



Cisco NDFC SAN コントローラ 構成ガイド、リリース 12.1.x

初版：2022年7月7日

最終更新：2022年8月1日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ www.cisco.com/jp/go/safety_warning/ ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



目次

Full Cisco Trademarks with Software License ?

第 1 章

概要 1

Web UI を理解する 1

ユーザフィードバック 3

Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング 4

第 2 章

新機能と更新情報 7

新規および変更情報 7

第 3 章

ダッシュボード 9

概要 9

ホスト 12

ホスト ラックの表示 14

CPU とメモリおよびディスク I/O チャートの表示 15

ストレージ 16

ストレージエンクロージャの表示 17

SAN Insights 18

SAN Insights の表示 19

カスタムグラフの表示 22

カスタムグラフとテーブルの表示 23

メトリックのモニタリング 25

IT ペアの表示 27

第 4 章	トポロジ	29
	トポロジの検索	30
	トポロジの表示	30
	SAN トポロジの要素の表示	32
	ズーム、パン、ドラッグ	33
	レイアウト	34
	ステータス	34

第 1 部 :	SAN	37
---------	------------	-----------

第 5 章	ファブリック	39
	ファブリック	39
	ファブリックの追加	41
	ファブリックの編集	42
	ファブリックを削除しています	42
	ファブリックの再検出	43
	ファブリックの消去	43
	パフォーマンスの設定	44
	SAN Insights	45
	前提条件	45
	永続的な IP アドレスの設定	46
	注意事項と制約事項	46
	SAN Insights のサーバープロパティ	47
	SAN Insights の設定	50
	ファブリック バックアップの構成	56
	ゴールデン バックアップ	57
	ファブリックの概要	58
	ファブリック サマリ	58
	スイッチ	58
	モジュール	60

インターフェイスの表示	60
VSAN	62
デフォルトの VSAN 設定	63
VSAN の作成ウィザード	64
VSLAN の削除	67
VSAN のフィールドと説明	68
デバイス エイリアス	73
デバイスエイリアスの設定	74
CFS	76
イベント分析	77
バックアップアクションの実行	77
ポートの使用の表示	79
メトリック	79
輻輳分析	81
輻輳可視化	82
DIRL	83

第 6 章

スイッチ	87
スイッチ	87
デバイス マネージャ	88
テクニカル サポート	88
CLI の実行	89
拡張されたロールベースのアクセス制御	90
Nexus Dashboard のセキュリティ ドメイン	95
スイッチの概要	97
スイッチの概要の表示	97
モジュール	97
インターフェイスの表示	98
スイッチライセンスの表示	100
イベント分析	100
バックアップの表示	100

ブートフラッシュのコピー	101
設定ファイルの比較	102
Export Configuration	103
ポートの使用の表示	104
ブートフラッシュの表示	104
デバイス マネージャ	105
ブレード	105

第 7 章**SAN リンク 107**

SAN リンク	107
ISL およびポートチャネル	107
FCIP の設定	107
ポート チャネル	109
[Create Port Channel] ウィザード	123
既知のポートチャネルの編集	125
NPV Links	125

第 8 章**インターフェイス 127**

インターフェイス	127
FC ポート	127
FC ポートのインベントリ情報の表示	127
FC ポートのパフォーマンス情報の表示	128
FC ポートのトランシーバ情報の表示	129
FC FICON ポートの表示	131
イーサネットポートに関するパフォーマンス情報の表示	132
ポートグループに関するパフォーマンス情報の表示	133
ポートグループメンバー	134
オプティクスのパフォーマンス情報の表示	135
カスタムポートグループ	137
カスタムポートグループのパフォーマンスの表示	138
カスタムポートグループの設定	138

第 9 章	エンドデバイス 141
	デバイス 141
	ラック 142
	インベントリエンクロージャ 143
	インベントリ ホストエンクロージャ 143
	インベントリ ストレージエンクロージャ 144
	パフォーマンスエンクロージャ 144
	パフォーマンス ホストエンクロージャ 144
	パフォーマンス ストレージエンクロージャ 145
	エンクロージャメンバー 146

第 10 章	ホストパスの冗長性 147
	ホストパスの冗長性 147
	診断テスト 147
	ホストパスエラー 148
	無視されたホスト 149
	無視されたストレージ 150
	無視されたホストストレージペア 150

第 11 章	ポート監視 153
	ポートモニタリングポリシー 153
	SFP カウンタの設定 159

第 12 章	アクティブゾーン 161
	通常ゾーン 161
	IVR ゾーン 162

第 13 章	ストレージ 163
	ストレージアレイ 163
	storageName エンクロージャ 163

ストレージ SMI-S プロバイダー 165

SMI-S プロバイダーの追加 166

第 II 部 : 仮想的な管理 169

第 14 章 ゾーン分割 171

ゾーン分割 171

拡張ゾーン分割 173

CFS 175

ゾーンセット 178

ゾーン 180

FC エイリアス 182

メンバー 183

第 15 章 仮想インフラストラクチャ マネージャ 187

仮想インフラストラクチャ マネージャ 187

Cisco UCS B シリーズ ブレードサーバーのサポート 188

ルート IP アドレスの設定 190

vCenter の可視化の追加 190

第 III 部 : 設定 193

第 16 章 [サーバ設定 (Server Settings)] 195

サーバ設定 195

第 17 章 Feature Manager 197

Feature Manager 197

フィーチャ セットの選択 197

各ペルソナの機能 198

機能セット全体での変更 198

第 18 章 クレデンシャル管理 201

SAN クレデンシャル管理 201

第 IV 部 : 操作 203

第 19 章 イベント分析 205

アラーム 205

発行されたアラーム 205

クリアされたアラーム 207

アラーム ポリシーの監視と追加 208

新しいアラーム ポリシーの作成 210

イベント 215

イベントのセットアップ 216

アカウンティング 220

リモートクラスタ 220

第 20 章 イメージ管理 223

イメージ管理 223

概要 224

イメージのステージング 225

イメージの検証 226

イメージのアップグレード 226

モードの変更 228

グループの変更 229

ポリシーの変更 230

コンプライアンスの再計算 231

レポートの実行 231

製品イメージ 232

イメージのアップロード 234

イメージ ポリシー 235

イメージ ポリシーの作成 236

履歴 238

第 21 章	プログラム可能レポート	239
	レポートの作成	240
	レポート テンプレート	241
	レポート定義	242
	レポート	244

第 22 章	ライセンス管理	247
	概要	247
	NDFC サーバ ライセンス	248
	スマートライセンス	250
	スイッチ ライセンス	253
	CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング	255
	スイッチ ライセンス ファイル	256
	スイッチ ライセンス ファイルの追加	257

第 23 章	テンプレート (Templates)	259
	テンプレート (Templates)	259
	新規テンプレートの作成	262
	テンプレートの編集	264
	テンプレートのインポート	265
	POAP テンプレートのインストール	266
	テンプレート構造	267
	テンプレートの形式	267
	テンプレート変数	276
	可変メタ プロパティ	279
	可変注釈	289
	テンプレートの内容	293
	高度な機能	295
	レポート テンプレート	297

第 24 章	バックアップと復元 301
	スケジューラ 302
	Restore (復元) 304
	今すぐバックアップ 305

第 25 章	NXAPI 証明書 309
	証明書の生成と管理 309
	スイッチ証明書 311
	CA 証明書 313

第 V 部 :	サービスの統合 315
---------	--------------------

第 26 章	ワン ビュー ダッシュボード 317
	ワン ビュー ダッシュボード 317

第 27 章	デバイス マネージャ 319
	デバイス マネージャ 319
	物理 319
	インベントリ 319
	Modules - ステータスと構成 319
	電源 320
	温度センサー 321
	ファン 321
	スイッチ 322
	ISL 323
	NP リンク 323
	ISL の統計 324
	ホスト 325
	ラック 325
	デバイスマネージャ - プリファレンス 326

インターフェイス	327
仮想インターフェイス グループ	327
仮想 FC インターフェイス	327
イーサネット インターフェイス	329
仮想 FC イーサネット	330
クイック構成ツール	330
イーサネット インターフェイス	331
Ethernet Interfaces iSCSI	333
Ethernet Interfaces iSCSI TCP	333
イーサネット インターフェイス VLAN	334
イーサネット VLAN	335
FC インターフェイス モニタリング トラフィック。	335
FC インターフェイス モニタリング プロトコル	336
FC インターフェイスでの破棄数モニタリング	337
FC インターフェイス モニタ リンク エラー	337
FC インターフェイス モニタ フレーム エラー	337
FC インターフェイス モニタ クラス 2 トラフィック	338
FC インターフェイス モニタ クラス 2 エラー	338
FC インターフェイス モニタ FICON	339
オーバーサブスクリプションの確認	339
仮想 FC インターフェイス モニタリング トラフィック	339
仮想 FC インターフェイス モニタ 廃棄数	340
仮想 FC インターフェイス モニタ エラー	340
イーサネット インターフェイス Dot3Stats	340
インターフェイス モニタ	341
イーサネット ポートチャネル	342
Ethernet Interface Monitor iSCSI Connections	343
イーサネット インターフェイス モニタリング TCP	343
FCIP Monitor	344
SVC インターフェイスのモニタ	344
SVC NPorts のモニタリング	345

SVC セッション FCP のモニタリング	345
SVC セッション モニタリング その他	346
FCIP インターフェイス	346
システム タイムアウト	347
インターフェイス ライセンス	348
全般	348
FC インターフェイス 全般	348
FC インターフェイス Rx BB クレジット+	354
FC の他のインターフェイス	355
FC インターフェイス FLOGI	355
FC インターフェイス ELP	357
FC インターフェイスのトランク構成	359
FCIP Interfaces Trunk Failures	360
FC インターフェイス IP	360
FC インターフェイスの物理的特徴	360
FC インターフェイス機能	361
FC インターフェイス FICON ピア	361
インターフェイス NPorts (SVC)	362
インターフェイス セッション	362
IP 統計 TCP	362
ポート チャネルイーサネット インターフェイス	363
ポート チャネル FC インターフェイス	363
ポート チャネル 全般	364
FlexAttach グローバル	365
FlexAttach 仮想 PWWN	365
FlexAttach 物理 WWN から仮想 WWN へ	366
FIPS	367
FCIP FICON Configuration	367
ポート チャネルの自動作成	367
SPAN セッション	367
SPAN グローバル	368

SPAN 送信元インターフェイス	368
ポート トラッキングの依存関係	368
ポート トラック強制シャットダウン	368
ポートガード	369
帯域幅予約 : 48-ポート 96-Gbps ファイバ チャンネル モジュール	369
帯域幅予約 : 48 ポート 48 Gbps ファイバチャンネル モジュール	369
帯域幅予約 : 24 ポート 48 Gbps ファイバチャンネル モジュール	370
帯域幅予約 : 48 ポート 256 Gbps ファイバー チャンネル モジュール	370
帯域幅予約 : 32 ポート 256 Gbps ファイバ チャンネル モジュール	371
DS-X9448-768K9 (Luke) ラインカード帯域幅の予約	371
FC	371
VSAN 全般	372
VSAN Membership	372
VSAN Interop-4 WWN	373
VSAN タイマー	373
VSAN デフォルト ゾーン ポリシー	374
IVR ローカル トポロジ	374
IVR ファブリック ID	374
IVR デフォルト ファブリック ID	374
IVR のアクション	374
IVR RDI VSAN	375
IVR アクティブトポロジ	375
IVR Zoneset ステータス	375
IVR の不一致	377
IVR ドメイン	377
IVR FCID	377
IVR Zoneset アクティブ ゾーン	377
IVR ゾーンセット アクティブ ゾーン属性	378
IVR ゾーンセット名	378
DPVM アクション	379
DPVM 構成データベース	379
DPVM アクティブ データベース	380

ドメイン マネージャを実行	380
Domain Manager の設定	380
ドメイン マネージャ ドメイン	382
ドメイン マネージャの統計	382
ドメイン マネージャ インターフェイス	383
ドメイン マネージャ 永続 FcId	383
ドメイン マネージャ 許可 DomainId	384
ゾーンセットのアクティブ ゾーン	384
Zoneset ゾーンなし	384
Zoneset Status	385
Zoneset ポリシー	385
Zoneset のアクティブ ゾーン属性	386
ゾーンセットを拡張	386
Zoneset 読み取り専用違反	387
Zoneset 統計	387
Zoneset LUN ゾーニング統計	388
Zoneset メンバー	388
ファブリック構成サーバーの検出	389
ファブリック構成サーバー インターコネクト要素	389
Fabric Config Server プラットフォーム (エンクロージャ)	389
ファブリック構成サーバー ファブリック ポート	390
FC ルート	390
FDMI HBAs	391
FDMI ポート	391
FDMI バージョン	392
フロー統計	392
FCC	392
診断	393
FSPF 全般	393
FSPF インターフェイス	395
FSPF インターフェイスの統計	396

SDV 仮想デバイス	397
SDV リアルデバイス	398
LUN の検出	398
LUN ターゲット	399
LUN	399
デバイス エイリアス	399
デバイス エイリアス構成	399
デバイス エイリアスのモード	400
デバイス エイリアスの不一致	400
ネームサーバー全般	400
ネームサーバーの詳細	401
ネームサーバー プロキシ	402
ネームサーバー統計情報	402
優先パス マップとルート	402
Preferred Path Maps Active	403
優先パスすべての一致基準	403
優先パスのアクティブな一致基準	404
優先パスのすべての設定	405
RSCN Nx の登録	405
RSCN Multi-PID サポート	405
RSCN イベント	405
RSCN 統計情報	406
マルチキャストルート	406
QoS ポリシーマップ	406
QoS クラス マップ	406
QoS マッチ ステートメント	407
ポリシー マップによる QoS クラスマップ	407
VSAN による QoS ポリシー マップ	408
QoS DWRR	408
QoS レート制限	408
タイマーとポリシー	408

WWN マネージャ	409
NPV トラフィック マップ	410
NPV ロードバランサ	410
NPV 外部インターフェイスの使用状況	411
NP リンク	411
FCoE	412
設定	412
VSAN-VLAN マッピング	412
VLAN-VSAN マッピング	412
FCoE 統計	413
Ficon	414
FICON VSAN	414
FICON VSAN ファイル	415
グローバル	415
FICON ポート属性	416
FICON ポートの構成	417
FICON ポート番号	417
FICON VSANs Director 履歴	418
ファブリック バインド アクション	418
ファブリック バインド構成データベース	419
ファブリック バインドアクティブ データベース	419
ファブリック バインドデータベースの差異	419
ファブリック バインド違反	420
ファブリック バインド 統計	421
ファブリック バインド EFMD 統計	421
IP ストレージ	422
FCIP Profiles	422
FCIP Tunnels	423
FCIP Tunnels (Advanced)	424
FCIP Tunnels (FICON TA)	425
FCIP Tunnels Statistics	425
FCIP XRC Statistics	425

iSCSI Connection	426
iSCSI イニシエータ	427
iSCSI Session Initiators	428
Module Control	428
iSCSI Global	428
iSCSI Session Statistics	429
iSCSI Targets	429
iSCSI iSLB VRRP	430
iSCSI Initiator Access	430
Initiator Specific Target	431
iSCSI Initiator PWWN	431
iSCSI Sessions	432
iSCSI Sessions Detail	432
IP サービス	433
IP Routes	433
IP Statistics ICMP	433
IP Statistics IP	435
IP Statistics SNMP	436
IP Statistics UDP	437
mgmt0 Statistics	438
TCP UDP TCP	438
TCP UDP UDP	438
VRRP General	438
VRRP IP Addresses	440
VRRP 統計情報	440
CDP General	441
CDPネイバー	441
iSNS Profiles	442
iSNS Servers	442
iSNS Entities	442
iSNS Cloud Discovery	442
iSNS Clouds	443
iSNS Cloud Interfaces	443
Monitor Dialog Controls	444

iSNS Details iSCSI Nodes	445
iSNS Details Portals	445
セキュリティ	446
セキュリティ ロール	446
セキュリティ ロールルール	446
機能グループ マネージャ	447
AAA LDAP サーバー	447
AAA サーバグループ	448
AAA 検索マップ	449
AAA アプリケーション	449
AAA のデフォルト	450
AAA 全般	451
AAAの統計情報	451
iSCSI User	455
共通ロール	455
SNMP セキュリティ ユーザ	456
SNMP セキュリティ コミュニティ	457
セキュリティ ユーザ グローバル	457
FC-SP 全般/パスワード	458
FC-SP インターフェイス	458
FC-SP ローカル パスワード	459
FC-SP リモート パスワード	459
FC-SP 統計	459
FC-SP SA (セキュリティ アソシエーション)	460
FC-SP ESP インターフェイス	460
PKI 全般	460
PKI RSA キーペア	461
PKI トラスト ポイント	461
PKI 信頼ポイント アクション	462
PKI LDAP	463
PKI 認定マップ	464

PKI 認定マップ - アプリケーション	464
PKI 信頼ポイントの詳細	464
IKE グローバル	466
IKE 事前共有認証キー	466
IKE ポリシー	466
IKE 発信側バージョン	467
IKE トンネル	467
IPSEC グローバル	468
IPSEC トランスフォームセット	468
IPSEC クリプトマップセット エントリ	468
IPSEC インターフェイス	469
IPSEC トンネル	470
IP ACL プロファイル	470
IP ACL インターフェイス	470
IP フィルタ プロファイル	471
SSH/Telnet	474
ポートセキュリティのアクション	474
ポートセキュリティ コンフィギュレーション データベース	477
ポートセキュリティ アクティブ データベース	477
ポートセキュリティ データベースの相違点	478
ポートセキュリティ違反	478
ポートセキュリティ統計情報	479
IPsec	479
イベント	479
Call Home 一般	479
Call Home 宛先	480
Call Home 電子メール セットアップ	480
Call Home アラート	481
Call Home HTTP プロキシ サーバ	481
Call Home SMTP サーバ	481
Call Home ユーザ定義コマンド	482

遅延トラップ	482
Call Home プロファイル	482
イベント宛先アドレス	482
イベント宛先セキュリティ (詳細)	483
イベント フィルター一般	483
イベント フィルタ インターフェイス	485
イベント フィルタ制御	485
リンク インシデント履歴	485
RMON しきい値制御	486
RMON しきい値 64 ビットアラーム	486
RMON しきい値 32 ビットアラーム	488
RMON しきい値イベント	489
RMON しきい値ログ	489
管理者	489
設定のコピー	489
フラッシュファイル	490
コンパクトフラッシュ	490
ライセンス機能	490
ライセンス マネージャ キー	491
ライセンス マネージャのインストール	491
ライセンス マネージャの使用状況	494
ポート ライセンス	494
機能セット	494
[機能制御 (Feature Control)]	494
NTPサーバ	495
NTP 全般	496
実行中のプロセス	496
起動時/実行構成の表示	496
EPLD のバージョンの表示	497
フラッシュ ファイルのコピー	497
TAC Pac ファイルの生成	498

技術サポートの表示	498
イメージのバージョンの表示	499
オンボード ログの表示 (Show Onboard Log)	499
一覧ビュー	499
RLIR ERL	501
優先ホスト	501
優先経路 (Preferred Path)	502
Edit iSCSI Advertised Interfaces	502
DNS 全般	502
DNS サーバ (DNS Servers)	502
Cisco Fabric Services (CFS) の機能	503
Cisco Fabric Services (CFS) の IP マルチキャスト	505
Cisco Fabric Services (CFS) IP 静的ピア	506
Cisco Fabric Services (CFS) のリージョンごとの機能	506
Cisco Fabric Services (CFS) のすべてのリージョン	507
Cisco Fabric Services (CFS) のオーナー	507
Cisco Fabric Services (CFS) のマージ	507
ログ	507
SysLog (リブート以降)	507
SysLog (重大なイベント)	508
アカウントティング ログ	508
スイッチ ロギング	508
syslog 重大度レベル	509
Syslogサーバ	509
エンド デバイス - ホスト	509
インテリジェント機能 - サマリ	510
データ モビリティ マネージャー モジュール	510
ストレージ メディア暗号化	511
メンバー	511
インターフェイス	512
ホスト	512

SSM 機能	512
概要	512
FCWA	513
SSM	513
MSM	513
SANTap CVT	514
SANTap DVT	514
NASB	515
NASB ターゲット	515
Virtual Initiator	516
DMM レート	516
FCWA Config Status	516
統計のステータス	517
I/O トラフィック統計	517
統計 I/O トラフィックの詳細	517
統計 SCSI コマンド	518
SCSI エラーの統計情報	519
統計 SCSI 検知エラー	519
コンパクト	520



第 1 章

概要

- [Web UI を理解する \(1 ページ\)](#)
- [ユーザフィードバック \(3 ページ\)](#)
- [Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング \(4 ページ\)](#)

Web UI を理解する

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI を初めて起動すると、**[機能管理 (Feature Management)]** ウィンドウが開きます。展開タイプを選択すると、左側のペインにパーソナリティに関連するメニューが表示されます。

上部ペインには、次の UI 要素が表示されます。

- **[ホーム (Home)]** アイコン：クリックして Nexus ダッシュボードセットアップの 1 つのビューを表示します。
- **[Nexus ダッシュボード (Nexus Dashboard)]**：クリックして、Nexus ダッシュボードセットアップの 1 つのビューを表示します。
- **フィードバック**：Cisco Nexus ダッシュボード ファブリック コントローラ に関するフィードバックを提供できます。この説明については、[ユーザフィードバック \(3 ページ\)](#) を参照してください。
- **[ヘルプ (Help)]**：[ヘルプ (Help)] をクリックすると、次のオプションを含むドロップダウンリストが表示されます。
 - **Nexus ダッシュボードについて**：Cisco Nexus ダッシュボード ファブリック コントローラ が導入されている Cisco Nexus ダッシュボードのバージョンを表示します。
 - **ウェルカム画面**：最新情報を表示します。Web UI を起動するたびに、このページを表示するかどうかを選択できます。
 - **[ヘルプセンター (Help Center)]**：クリックすると、[ヘルプセンター (Help Center)] ページが表示されます。このページからさまざまな製品ドキュメントにアクセスできます。

ページの最後までスクロールして、Nexus Dashboard にインストールされているサービスを表示します。サービスをクリックして **[ヘルプセンター (Help Center)]** を表示します。

- **[ユーザーロール (User Role)]** : 現在ログインしているユーザーのロール (**admin**など) が表示されます。ユーザー名をクリックすると、次のオプションを含むドロップダウンリストが表示されます。
 - **[ユーザー設定 (User Preferences)]** : ログインするたびにウェルカム画面を表示するかどうかを設定できます。
 - **[パスワードの変更 (Change Password)]** : 現在のログインユーザのパスワードを変更できます。
ネットワーク管理者ユーザの場合、他のユーザのパスワードを変更できます。
 - **[API キーの管理 (Manage API Keys)]** : クリックして API キーを管理します。 **[API キーの追加 (Add API Key)]** をクリックして、API キーを生成します。 **[編集 (Edit)]** アイコンをクリックして、名前を指定し、API キーを変更します。 **[保存 (Save)]** をクリックします。
 - **[ログアウト (Logout)]** : Web UI を終了し、ログイン画面に戻ります。
- **[Cisco Nexusダッシュボードファブリックコントローラ Persona]** : 展開ペルソナを指定します - ファブリックコントローラ、SAN コントローラ、またはファブリック検出。
- **[アラームの表示 (View Alarms)]** : ベルアイコンをクリックしてアラームを表示します。このページは、左ペインの **[操作 (Operations)]** > **[イベント分析 (Event Analytics)]** > **[アラーム (Alarms)]** から表示できます。
- **[ヘルプ (Help)]** アイコン : クリックすると、ヘルプページまたは Cisco NDFC に関する情報が表示されます。
 - **[ヘルプ (Help)]** を選択して、UI ページの状況依存ヘルプを表示します。
 - **[NDFC の詳細 (About NDFC)]** を選択して、バージョン情報と著作権情報を表示します。

UI の一般的なアイコン :

- **ハンバーガー アイコン** - ホーム画面の製品名の横にあるハンバーガー アイコンをクリックすれば、ホーム画面のメニュー項目を最小化することや、メニュー項目を詳細に表示することができます。
- **更新 アイコン** : 更新アイコンをクリックすると、画面が更新されます。

ユーザフィードバック

Cisco Nexus ダッシュボード ファブリック コントローラ では、アプリケーションに関するフィードバックを提供できます。この機能を使用して、新しい機能/拡張機能を要求できます。要求は Cisco Nexus ダッシュボード ファブリック コントローラ のマーケティング エンジニアに送信されます。エンジニアは要件を評価し、今後のリリースに機能または拡張機能を含めます。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI を使用してフィードバックを提供するには、次の手順を実行します。

手順

ステップ 1 [フィードバック (Feedback)] をクリックします。これは Nexus ダッシュボード ファブリック コントローラ アプリケーションの右上隅にあります。

これを初めて使用する場合は、Cisco Nexus ダッシュボードで DNS とプロキシサーバーを設定する必要があります。

ステップ 2 接続を確立するには、ブラウザで [Cisco Nexus ダッシュボード (Cisco Nexus Dashboard)] に移動し、次の手順を実行します。

a) Cisco Nexus ダッシュボードの Web UI で、[インフラストラクチャ (Infrastructure)] > [クラスタ設定 (Cluster Configuration)] を選択します。

[クラスタ設定全般 (Cluster Configuration General)] タブが表示されます。

- b) [プロキシ設定 (Proxy Configuration)] 領域で、[編集 (Edit)] アイコンをクリックします。
- c) [サーバー (Servers)] 領域で、[サーバーの追加 (Add Server)] をクリックします。
- d) プロトコルのタイプとして、[HTTP] または [HTTPS] を選択します。
- e) [サーバー (Server)] フィールドに、IP アドレスを入力します。
- f) [ユーザー名 (Username)] と [パスワード (Password)] をそれぞれのフィールドに入力します。
- g) 「チェック」アイコンをクリックして確定します。削除するには、「間違い」アイコンをクリックします。
- h) [無視するホスト (Ignore Hosts)] 領域で、[無視するホストの追加 (Add Ignore Host)] をクリックします。
- i) [ホスト名 (Hostname)] を入力し、「チェック」アイコンをクリックして確定します。削除するには、「間違い」アイコンをクリックします。
- j) [保存 (Save)] をクリックして、プロキシサーバーを設定します。

(注) プロキシ設定が Nexus ダッシュボード ファブリック コントローラ アプリケーションに反映されるまで、最大 5 分間待ってください。

ステップ 3 Cisco Nexus ダッシュボード ファブリック コントローラ Web UI で、[フィードバック (Feedback)] をクリックします。

- ステップ4 [フィードバック (Feedback)] パネルで、星をクリックして Nexus ダッシュボード ファブリック コントローラ についての感想をお聞かせください。
- ステップ5 [提案する (Make a suggestion)] フィールドに、提案/フィードバックを入力します。
- ステップ6 フィードバックについてシスコと連絡を取ることにした場合は、[シスコからフィードバック についての連絡を受けてもよい (Cisco may contact me about my Feedback)] チェックボックス をオンにします。
- ステップ7 [名前 (Name)] と [電子メール (Email)] のフィールドに名前と電子メールを入力します。

Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング

リリース 12.1.1e 以降、NDFC と Nexus Dashboard Insights を同じ Nexus Dashboard クラスタで管理モードでホストしてファブリックを管理し、Nexus Dashboard Insights をホストして同じファブリックをモニタリングできます。NDFC リリース 12.0.2f では、ファブリック ディスカバリ モードの NDFC、つまり、同じ Nexus Dashboard クラスタ上の NDI を使用したモニタモードがサポートされていることに注意してください。これには、最大 50 のスイッチの最大規模の 4 つの物理的な Nexus Dashboard ノードが必要でした。この機能は、対応するペアの Nexus Dashboard Insights リリース 12.1.1e を備えた NDFC リリースでもサポートされています。



- (注) KVM に展開された Nexus Dashboard は、同じ Nexus Dashboard クラスタでの NDFC と Insights サービスの共同ホスティングをサポートしていません。



- (注) 同じ Nexus Dashboard クラスタで NDFC と Insights を共同ホスティングするには、Nexus Dashboard ノードがレイヤ 2 で隣接している必要があります。共同ホスティング導入のためのレイヤ 3 隣接のサポートは、将来のリリースで展開される予定です。

次の表は、Nexus Dashboard とサービスの互換性のあるバージョンを示しています。

[サービス (Services)]	互換性バージョン
Nexus ダッシュボード	2.2.1h
Nexus ダッシュボード Insights	6.1.2
Nexus Dashboard Fabric Controller	12.1.1e

次の表は、Nexus Dashboard のシステム要件を示しています。

仕様	サポートされるスケール
物理的な Nexus Dashboard ノードの数	5
サポートされるスイッチの数	50
Nexus Dashboard Insights でサポートされるフローの数	10000

同じ Nexus Dashboard への NDFC と NDI のインストール

Cisco NDFC は、同じ Nexus Dashboard で Nexus Dashboard Insights と共同主催できます。

はじめる前に

- Cisco Nexus Dashboard の必要なフォームファクタがインストールされていることを確認します。手順については、『[Cisco Nexus Dashboard Deployment Guide](#)』を参照してください。
- 『[Cisco NDFC インストールおよびアップグレードガイド、リリース 12.1.1e](#)』の「前提条件」セクションに記載されている要件とガイドラインを満たしていることを確認してください。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、『[Nexus Dashboard ユーザーガイド](#)』を参照してください。
- DC のアプリケーションセンターへの接続を確立できない場合は、このセクションをスキップして、『[Nexus Dashboard ファブリックコントローラサービスを手動でインストールする](#)』で説明されている手順に従ってください。
- Cisco Nexus Dashboard で、サービスに IP プールアドレスが割り当てられていることを確認します。詳細については、『[Cisco Nexus Dashboard ユーザーガイド](#)』の「クラスタの設定」の項を参照してください。

Nexus Dashboard Insights のインストール

Cisco Nexus Dashboard の必要なフォームファクタがインストールされていることを確認します。手順については、『[Cisco Nexus Dashboard Deployment Guide](#)』を参照してください。

NDFC のインストール

『[Cisco Nexus Dashboard ファブリックコントローラのインストール](#)』を参照してください。

Nexus Dashboard で NDFC サイトを設定します。手順については、『[Cisco Nexus Dashboard ユーザーガイド](#)』の「サイトの追加」セクションを参照してください。

NDI のインストール

同じ Nexus Dashboard セットアップで、Nexus Dashboard Insights サービスをインストールします。詳細については、『[Cisco Nexus Dashboard Insights 導入ガイド](#)』を参照してください。

インストール後

NDFC と NDI の互換性のあるバージョンを 5 ノードの物理 Nexus ダッシュボードにインストールした後、NDFC をファブリック (LAN) コントローラとして起動します。ファブリックを作成し、NDFC ファブリックでスイッチを検出してインポートします。Nexus Dashboard は、NDFC ファブリックと [サイト (Sites)] ページのリストをエンティティとして自動的に識別します。



(注) Nexus Dashboard サイトマネージャで、各サイトのパスワードを指定する必要があります。



第 2 章

新機能と更新情報

- [新規および変更情報 \(7 ページ\)](#)

新規および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能の中には、一部、この表に記載されていないものもあります。

次の表に、Cisco NDFC の新機能および変更された機能に関する情報を示します。

表 1: NDFC リリース 12.1.1e のすべてのペルソナの新機能と強化された機能

機能	説明	参照先
KVM 上の Nexus Dashboard で NDFC をサポート	NDFC は、KVM ハイパーバイザ上で実行されている仮想 Nexus Dashboard クラスタにインストールできます。これは、ファブリック コントローラ、ファブリック ディスカバリ、および SAN コントローラ モードでサポートされます。	Cisco Nexus Dashboard 導入ガイド

表 2: Cisco NDFC リリース 12.1.1e の SAN ファブリックの新機能および拡張機能

機能	説明	参照先
SAN 展開用に RHEL で提供される NDFC	Nexus Dashboard は Red Hat Enterprise Linux に展開でき、NDFC SAN コントローラ ペルソナをインストールできます。	Cisco Nexus Dashboard 展開ガイド

機能	説明	参照先
DIRL 輻輳管理の可視化	リリース 12.1.1e 以降、NDFC は DIRL 情報の視覚化を提供して、SAN ファブリック内の輻輳ポイントを強調表示します。	DIRL (83 ページ)
複数の SAN コントローラを 1 つのビューで表示	この機能は、複数の NDFC SAN コントローラインスタンスを単一の画面で表示できるようにします。複数のコントローラにわたるスイッチ、ポート、およびファブリックのステータスに関する情報を提供します。	ワンビューダッシュボード (317 ページ)
CLI コマンド実行のためのインターフェイス	このリリースでは、NDFC は、複数の Cisco MDS 9000 シリーズスイッチで同時に CLI コマンドを実行するためのインターフェイスを提供します。	CLI の実行 (89 ページ)
Cisco MDS 9000 シリーズスイッチのポリシーサポートを使用したスマートライセンス	NDFC を使用すると、ポリシーを使用してスマートライセンスが構成されている Cisco MDS 9000 シリーズスイッチを検出できます。	Cisco NDFC でのポリシーを使用したスマートライセンス
エンドポイントの可視性	ファイバチャネルインターフェイスでトランシーバ情報を表示できるようになりました。	FC ポートのトランシーバ情報の表示 (129 ページ)
SAN Insights の機能強化	<ul style="list-style-type: none"> • 拡張された SAN Insights スケールは、最大 500K ITL/ITN をサポートするようになりました。 • 64G モジュールでの SAN Insights のサポート 	ファブリック (39 ページ)



第 3 章

ダッシュボード

ダッシュボードの目的は、ネットワーク管理者とストレージ管理者がデータセンタースイッチングの健全性とパフォーマンスに関する特定の領域に集中できるようにすることです。この情報は、24 時間のスナップショットとして提供されます。

Cisco SAN コントローラ Web UI で使用できるさまざまなスコープは次のとおりです。

- [概要 \(9 ページ\)](#)
- [ホスト \(12 ページ\)](#)
- [ストレージ \(16 ページ\)](#)
- [SAN Insights \(18 ページ\)](#)

概要

デフォルトでは、使用可能なダッシュレットのサブセットがダッシュボードの概要に自動的に表示されます。

左側のメニューバーから **[ダッシュボード (Dashboard)]** > **[概要 (Overview)]** を選択します。

[概要 (Overview)] ウィンドウに次のダッシュレットが表示されます。

[概要 (Overview)] ダッシュボードウィンドウに表示されるデフォルトのダッシュレットは次のとおりです。

ダッシュレット	説明
ファブリック	ファブリックの名前、状態、ヘルスステータスなどのファブリックの詳細を表示します。 ファブリックの詳細を表示するには、ファブリック名 (リンク) をクリックして [ファブリック (Fabric)] スライドインペインを開きます。 [起動 (Launch)] アイコンをクリックします。または、ファブリック名をダブルクリックします。

ダッシュレット	説明
	[ファブリックの概要 (Fabric Overview)] ウィンドウが表示されます。
イベント分析	<p>重大、メジャー、マイナー、および警告の重大度を持つイベントを表示します。</p> <p>円グラフの重大度レベルまたはセクターをクリックして、イベントおよびアラームの重大度に関する詳細情報を [イベント分析 (Event Analytics)] ウィンドウに表示します。</p>
Links	データセンターで送受信するための Inter-Switch Link (ISL) および NPV リンクの図を表示します。円グラフのセクターをクリックして、[SAN リンク (SAN Links)] ウィンドウに詳細情報を表示します。
スイッチ	<p>スイッチの状態：スイッチのヘルスステータスを、括弧内にスイッチの総数とともに色とヘルス状態名を含むグラフの形式で表示します。</p> <p>色とその意味を次のリストに示します。</p> <ul style="list-style-type: none"> • 緑：要素が正常に機能し、意図したとおりに機能していることを示します。 • 黄：要素が警告状態にあり、それ以上の問題を防ぐために注意が必要であることを示します。 • 赤：要素が重大な状態にあり、すぐに対処する必要があることを示します。 • グレー：要素を特定するための情報がなにか、要素が検出されたことを示します。 <p>スイッチステータス：スイッチのステータスを表示します。</p> <p>スイッチリリースバージョン：スイッチリリースバージョンを表示します。</p> <p>スイッチモデル：スイッチのモデルを表示します。</p> <p>円グラフのセクター、重大度、ステータス、バージョン、またはモデルをクリックして、</p>

ダッシュレット	説明
	[スイッチ (Switches)] ウィンドウに詳細情報を表示します。
モジュール	モジュールが検出されたスイッチ、モデル名、カウントを表示します。
ポートの使用	ポートインベントリに関する要約情報を表示します。
パフォーマンスコレクタ	パフォーマンスコレクション情報を表示します。 [更新 (Refresh)] アイコンをクリックしてデータを更新します。 [コレクタの再始動 (Restart collector)] をクリックして、パフォーマンス収集情報を再始動します。 [コレクタの停止 (Stop collector)] をクリックして、パフォーマンス収集情報を停止します。
上位の ISL	パフォーマンス上位 10 位 ISL のデータを表示します。各エントリーはデバイス名を示し、Rx トラフィックと Tx トラフィックの平均をパーセンテージで指定します。 デバイス名の隣にある [チャート (chart)] アイコンをクリックして、詳細を表示します。
上位の SAN エンドポート	パフォーマンスが高い上位 10 位までの SAN ホストおよびストレージポートのパフォーマンスデータを表示します。各エントリーには、現在の受信と送信の割合が表示され、各リンクが現在設定されているしきい値を超えて費やした時間の割合を示すグラフが表示されます。 デバイス名の隣にある [チャート (chart)] アイコンをクリックして、詳細を表示します。
上位の FICON エンドポート	上位 10 位の FICON ホストおよびコントロールユニットのデータを表示します。各エントリーは、スイッチインターフェイスのポートトラフィックを示し、FICON ポートが接続されているデバイスを指定し、Rx トラフィックと Tx トラフィックの平均、および超過したパーセンテージ値を指定します。

ダッシュレット	説明
	デバイス名の隣にある[チャート (chart)]アイコンをクリックして、詳細を表示します。
上位の FCIP ISL	FCIP ISL を実行している上位 10 位のデータを表示します。各エントリはデバイス名を示し、Rx トラフィックと Tx トラフィックの平均、および超過したパーセンテージ値を指定します。 [チャート (chart)]アイコンをクリックして、詳細を表示します。
上位のオプティクス	上位 10 位のオプティクスのデータを表示します。最も高温の SPF、最も低温の SPF、低い受信出力、最も低い送信出力でオプティクスを並べ替えることができます。 スイッチインターフェイスの隣にある[チャート (chart)]アイコンをクリックして、詳細を表示します。
上位の CPU/温度	上位の CPU のデータとスイッチの温度の詳細を表示します。 スイッチの隣にある[チャート (chart)]アイコンをクリックして、詳細を表示します。
上位のエラーと破棄	選択したインターフェイスで破棄された上位のエラーパケットを表示します。 [チャート (chart)]アイコンをクリックして、詳細を表示します。

ホスト

UI パス : [ダッシュボード (Dashboard)] > [ホスト (Host)]

ホストダッシュボード : ホストダッシュボードでは、検出されたすべての SAN ホストおよび仮想ホストに関連するすべての情報を確認できます。ホストダッシュボードには、仮想ホストの上位に設定された個々のホストおよび仮想マシンに関する I/O トラフィック、ディスク遅延、CPU、メモリの統計情報、トポロジ、およびイベントなど、ネットワークに関連する非常に詳細な情報が表示されます。[ホスト (Host)]ダッシュボードは、次の 4 つのパネルで構成されます。

- [エンクロージャ (Enclosures)] パネル : ホストとそのネットワーク属性を一覧表示します。

関連するホスト エンクロージャの **[i]** アイコンをクリックして、SAN Insights モニタリングページを表示します。詳しくは「[メトリックのモニタリング](#)」を参照してください。

- **[トラフィックチャート (Traffic Chart)]** : 個々のホストまたは仮想マシンに関する I/O 統計情報、CPU とメモリの情報、およびディスク遅延を示します。
- **[イベントテーブル (Event Table)]** タブ : 特定のホストエンクロージャ内に設定されたすべてのスイッチポートのイベント情報を示します。
- **[トポロジ (Topology)]** パネル : ホストエンクロージャとストレージエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。検出された仮想マシンが表示され、仮想マシンを選択すると、SAN データソースへのパスが表示されます。このビューを切り替えて、すべてのデータパスを一覧表示できます。
- **[ホスト名 (Host Name)]** をクリックすると、スライドインパネルが表示されます。以下のフィールドを表示できます。

次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
[IPアドレス (IP Address)]	スイッチの IP アドレスを表示します。
Mac アドレス	MAC アドレスを表示します。
WWN	ポート WWN を表示します。
FCID	関連する FCID を指定します。
OS	OS の詳細を表示します。
#VMs	VM の数を表示します。
VHost 名	仮想ホストの名前が表示されます。
VHost IP	仮想ホストの IP アドレスの名前を表示します。
VCluster	仮想クラスタの名前を表示します。
マルチパス	マルチパスの詳細を表示します。
プロトコル	ホストが SCSI プロトコルトラフィックまたは NVMe プロトコルトラフィックをストリーミングしているかどうかを指定します。 この列には、SAN Insights を使用して Nexus ダッシュボードファブリックコントローラにデータがストリーミングされるホストのデータのみが表示されます。



- (注) vCenter 設定の収集レベルによって、収集されてグラフに表示されるデータの量が決まります。レベル1は、すべての収集間隔のデフォルトの収集レベルです。ディスク I/O 履歴データを収集するには、vCenter 統計設定をレベル2以上に変更します。

ホストラックの表示

SAN コントローラの Web UI からホストエンクロージャを表示するには、次の手順を実行します。

手順

ステップ1 [ダッシュボード (Dashboards)] > [ホスト (Hosts)] を選択します。

ホストエンクロージャテーブルのホストのリストが表示されます。

ステップ2 ホストエンクロージャの [i] アイコンをクリックします。

[SAN Insights モニタリング (SAN Insights Monitor)] ウィンドウが表示されます。

ステップ3 [SAN Insights モニタリング (SAN Insights Monitor)] ウィンドウで、必要なホスト名をクリックします。

ホストエンクロージャのスライドインペインが表示されます。

ステップ4 [起動 (Launch)] アイコンをクリックして、[ホストエンクロージャ (Host Enclosure)] ページを表示します。

ホストエンクロージャ ウィンドウが表示されます。

[ホストエンクロージャ] ウィンドウには、選択したホストのイニシエータとターゲット (IT) のペア、トポロジ、平均 ECT/DAL/読み取り/書き込み時間、およびスイッチインターフェイスが表示されます。

- **イニシエータターゲットペア** : このテーブルには、選択したホストのすべてのイニシエータとターゲットのペアが一覧表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、中止、失敗などに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **トポロジ** : ホストエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。カードの [表示 (View)] で、[+] または [-] をクリックしてズームインおよびズームアウトします。同様に、マウスのスクロールホイールを使用して、拡大および縮小ができます。トポロジ表示を更新するには、[更新 (Refresh)] をクリックします。[レイアウトの選択 (Select layout)] ドロップダウンリストを選択して、トポロジを表示します。これは、階層的 (Hierachical) または階層的左 - 右 (Hierachical Left-Right) ビューのいずれかです。

- フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、IOPS、スループットなどに関するすべてのメトリックの詳細が、1時間の平均値とベースライン情報とともに表示されています。
- **スイッチインターフェイス**：このテーブルには、選択したインターフェイスに対して選択された過去1時間のデータが表示されます。スイッチ名とインターフェイス名は、スイッチインターフェイステーブルの上部に表示されます。

CPU とメモリおよびディスク I/O チャートの表示

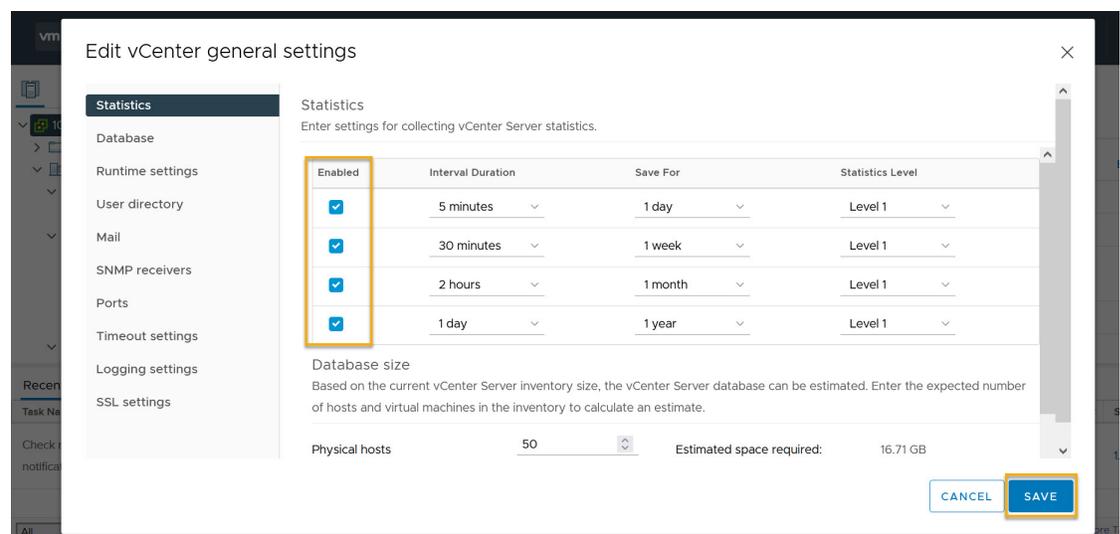
NDFC SAN コントローラ Web UI から SAN ホストエンクロージャを表示するには、次の手順を実行します。

始める前に

[CPU とメモリ (CPU & Memory)] と [ディスク I/O (Disk I/O)] の VM チャートを表示するには、vSphere vCenter で vCenter 設定を編集し、統計を手動で有効にする必要があります。

vSphere vCenter で統計情報を手動でイネーブルにするには、次の手順を実行します。

1. vSphere vCenter にログインします。（適切な [ホスト (Host)] をクリックします）
2. [設定 (Configure)] > [編集 (EDIT)] をクリックします。[vCenter の一般設定の編集 (Edit vCenter general settings)] 画面が表示されます。
3. [統計 (Statistics)] タブで、すべてのチェックボックスをオンにして、[保存 (SAVE)] をクリックします。



手順

ステップ1 [ダッシュボード (Dashboards)] > [ホスト (Hosts)] を選択します。

[エンクロージャ (Enclosures)] テーブルのホストのリストが表示されます。

ステップ2 ホスト名をクリックします。

[ホスト (Host)] のスライドインペインには、一般的な情報が表示されます。

ステップ3 [#VMs] をクリックして VM を表示します。

[SAN ホスト VM 画面 (SAN Host VM Screen)] が表示されます。

エンクロージャを選択して、右側のペインに [CPU とメモリ (CPU & Memory)] と [ディスク I/O (Disk I/O)] のチャートを表示します。

ストレージ

ストレージダッシュボードにアクセスするには、[ダッシュボード (Dashboard)] > [ストレージ (Storage)] を選択します。

ストレージダッシュボードは、次の4つのパネルで構成されます。

- [エンクロージャ (Enclosures)] エリア：ストレージとそのネットワーク属性を一覧表示します。
関連するホストエンクロージャの [i] アイコンをクリックして、SAN Insights モニタリングページを表示します。詳しくは「[メトリックのモニタリング](#)」を参照してください。
- [トポロジ (Topology)] エリア — ホストエンクロージャとストレージエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。検出された仮想マシンが表示され、仮想マシンを選択すると、SAN データソースへのパスが表示されます。このビューを切り替えて、すべてのデータパスを一覧表示できます。
- [トラフィックチャート (Traffic Chart)] エリア：個々のホストまたは仮想マシンに関する I/O 統計情報、CPU とメモリの情報、およびディスク遅延を示します。
- [イベントテーブル (Event Table)] エリア：特定のホストエンクロージャ内に設定されたすべてのスイッチポートのイベント情報を示します。
- [ストレージ名 (Storage Name)] をクリックすると、スライドインパネルが表示されます。以下のフィールドを表示できます。

次の表では、この画面のフィールドについて説明します。

フィールド	説明
[IPアドレス (IP Address)]	スイッチの IP アドレスを表示します。
Mac アドレス	MAC アドレスを表示します。
WWN	ポート WWN を表示します。
FCID	関連する FCID を指定します。
OS	OS の詳細を表示します。
#VMs	VM の数を表示します。
VHost 名	仮想ホストの名前が表示されます。
VHost IP	仮想ホストの IP アドレスの名前を表示します。
VCluster	仮想クラスタの名前を表示します。
マルチパス	マルチパスの詳細を表示します。
プロトコル	ホストが SCSI プロトコルトラフィックまたは NVMe プロトコルトラフィックをストリーミングしているかどうかを指定します。 この列には、SAN Insights を使用してデータが SAN コントローラにストリーミングされるホストのデータのみが表示されます。

ストレージエンクロージャの表示

SAN コントローラを使用すると、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights メトリックを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は[設定 (Settings)]>[サーバー設定 (Server Settings)]>[Insights]から変更できます。新しいプロパティを使用するには、SAN Insights サービスを再起動してください。

SAN コントローラの Web UI からストレージエンクロージャを表示するには、次の手順を実行します。

手順

ステップ 1 ダッシュボード (Dashboards) > [ストレージ (Storage)]を選択します。

ストレージエンクロージャ テーブルのストレージのリストが表示されます。

ステップ 2 [i] アイコンをクリックして、SAN Insights モニタリングページを表示します。SAN Insights モニタリングウィンドウで、必要なストレージ名をクリックします。詳しくは「[メトリックのモニタリング](#)」を参照してください。

[SAN Insights モニタリング (SAN Insights Monitor)] が表示されます。

ステップ 3 [起動 (Launch)] アイコンをクリックして、[ストレージエンクロージャ (Storage Enclosure)] ウィンドウを表示します。

ストレージエンクロージャ ウィンドウが表示されます。

[ストレージエンクロージャ] ウィンドウには、選択したホストのイニシエータとターゲット (IT) のペア、トポロジ、平均 ECT/DAL/読み取り/書き込み時間、およびスイッチインターフェイスが表示されます。

- **イニシエータターゲットペア**：このテーブルには、選択したストレージのすべてのイニシエータとターゲットのペアが一覧表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、中止、失敗などに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **トポロジ**：ホストエンクロージャ間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。カードの **[表示 (View)]** で、**[+]** または **[-]** をクリックしてズームインおよびズームアウトします。同様に、マウスのスクロールホイールを使用して、拡大および縮小ができます。トポロジ表示を更新するには、**[更新 (Refresh)]** をクリックします。**[レイアウトの選択 (Select layout)]** ドロップダウンリストを選択して、トポロジを表示します。これは、**階層的 (Hierachical)** または **階層的左 - 右 (Hierachical Left-Right)** ビューのいずれかです。
- フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、IOPS、スループットなどに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **スイッチインターフェイス**：このテーブルには、選択したインターフェイスに対して選択された過去 1 時間のデータが表示されます。スイッチ名とインターフェイス名は、スイッチインターフェイス テーブルの上部に表示されます。

SAN Insights

SAN Insights は、ファブリックレベルの情報をエンドツーエンドの全体像で視覚的に表示します。

SAN Insights ダッシュボードページで、プロトコル、ファブリック、およびスイッチをプロトコル、ファブリック、およびスイッチのドロップダウンリストから選択できます。ダッシュレットには、選択した範囲に基づいたインサイトデータが表示されます。

ダッシュボードには、過去 72 時間のデータが表示されます。ただし、フローサマリとエンクロージャ サマリ ドーナツには、最新の更新時刻からの最後の 15 分が表示されます。

SAN コントローラを使用すると、ファブリック、スイッチ、および 2 つのプロトコル (SCSI と NVMe) に基づいて SAN Insights メトリックを表示できます。

SAN コントローラの SAN Insights 機能が有効になっていることを確認します。[設定 (Settings)] > [機能管理 (Feature Management)] を選択し、[SAN Insights] チェックボックスをオンにします。

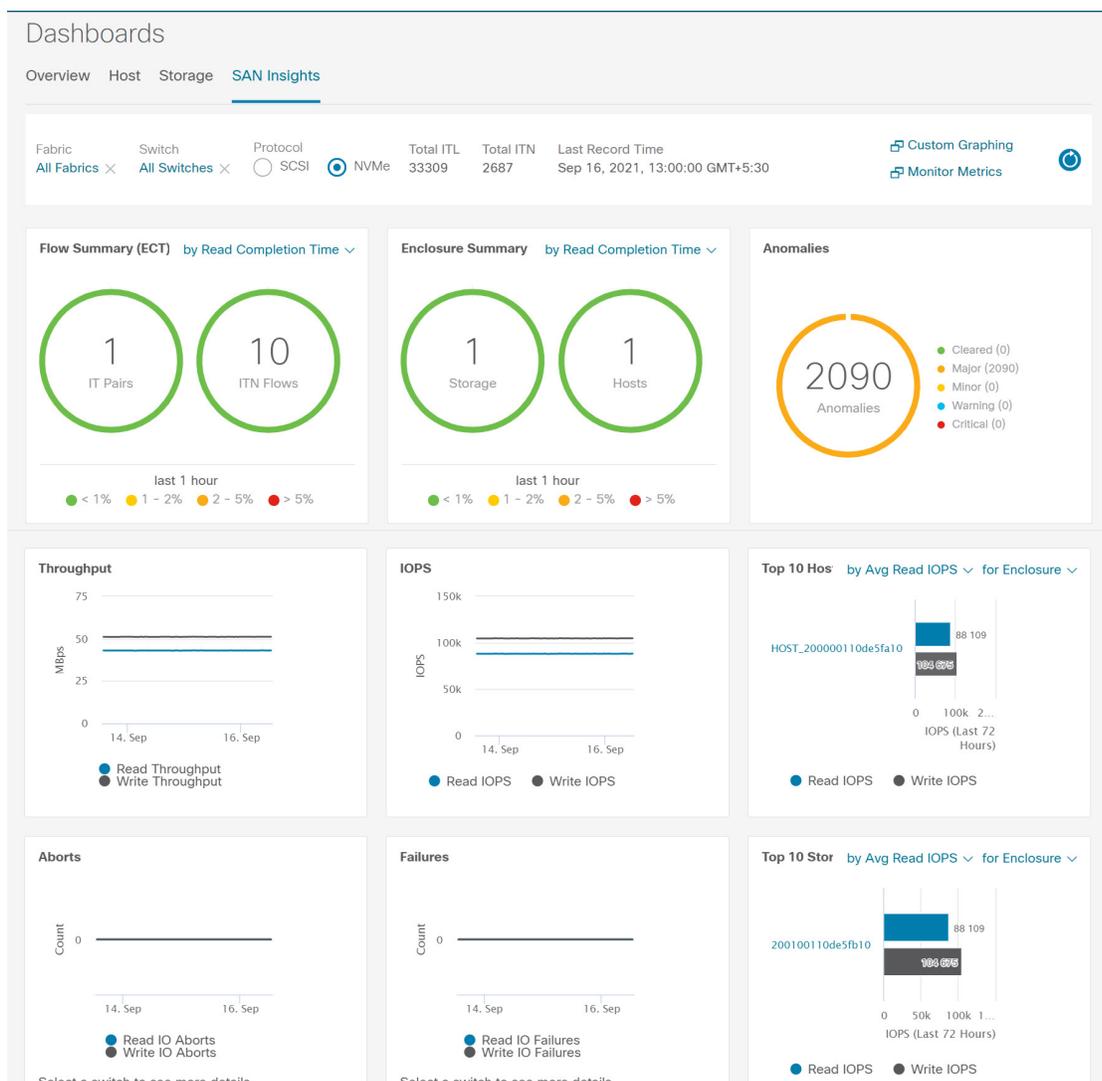
ダッシュボードに情報を表示するために、SAN Insights が構成されていることを確認します。「[SAN Insights の設定 \(50 ページ\)](#)」を参照してください。

SAN Insights の表示

SAN Insights ダッシュボードを表示するには、[ダッシュボード (Dashboard)] > [SAN Insights] を選択します。SAN Insights ダッシュボードは、全体的な読み取り/書き込み IO 操作/遅延を可視化することができます。

表 3: SAN Insights ダッシュボード

フィールド	説明
ファブリック	[ファブリック (Fabric)] をクリックして必要なファブリックを選択し、[保存 (Save)] をクリックします。
スイッチ	[スイッチ (Switch)] をクリックして、必要なスイッチを選択します。
プロトコル	[SCSI] または [NVMe] チェックボックスを選択して、必要なプロトコルを選択します。 デフォルトでは、 SCSI プロトコルが選択されます。
合計 ITL	選択したオプションの合計 ITL 値を表示します。
合計 ITN	選択したオプションの合計 ITN 値を表示します。
最終記録時間	選択したオプションの最終記録時間を表示します。
カスタムグラフ	[カスタムグラフ (Custom Graphing)] をクリックすると、SAN Insights メトリックの [カスタムグラフ (Custom Graphing)] ウィンドウが表示されます。詳細については、 カスタムグラフの表示 を参照してください。
メトリクスをモニター	[メトリックのモニタリング (Monitor Metrics)] をクリックすると、SAN Insights モニタリングウィンドウが表示されます。詳細については、「 メトリックのモニタリング 」を参照してください。
リフレッシュ	[更新 (Refresh)] アイコンをクリックすると、ロード画面が更新されます。



新しいプロパティを使用するには、SAN Insights サービスを再起動してください。

トレーニングされたベースラインからの個別の ITL カウントと ITN カウントの合計は、ダッシュボードの右上隅に表示されます。ドーナツには、過去 15 分間のアクティブな ITL/ITN カウントのみが表示されます。ただし、ITL と ITN の合計数には、選択したスコープのすべての ITL と ITN の数が表示されます。

SAN Insights ダッシュボードには、次のダッシュレットが含まれています。

- フローサマリ (ECT)

ドロップダウンリストから、[読み取り完了時間] または [書き込み完了時間] を選択します。これに基づいて、ドーナツに IT ペアと ITL フローが表示されます。これらのデータポイントは、Elasticsearch で利用可能な最後の 15 分間のデータに基づいて計算されます。

- エンクロージャの概要 (ECT)

ドロップダウンリストから、[読み取り完了時間]または[書き込み完了時間]を選択します。これに基づいて、ドーナツにストレージとホストが表示されます。これらのデータポイントは、Elasticsearch で利用可能な最後の 15 分間のデータに基づいて計算されます。

- 異常

異常ポリシーの数とその重大度を円グラフとリストで表示します。円グラフには重大度レベルがさまざまなカラーモードで表示され、グラフの横のリストには重大度レベルとそのレベルの異常ポリシーの数が表示されます。

これらの異常を編集、管理、表示、確認、および消去することができます。[操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] の順に選択します。

- スループット

読み取りおよび書き込みのスループットレートを表示します。グラフにマウスを合わせると、そのインスタンスの値が表示されます。これらの折れ線グラフのメトリックは、過去 72 時間のデータに基づいて計算されます。

- IOPS

読み取りおよび書き込み IOP のトレンドを表示します。これらの折れ線グラフのメトリックは、過去 72 時間のデータに基づいて計算されます。

- 中断

読み取りおよび書き込み中止のトレンドを表示します。これらの折れ線グラフのメトリックは、過去 72 時間のデータに基づいて計算されます。このメトリックは、Cisco MDS SAN 分析インフラストラクチャによって報告される **read_io_aborts** および **write_io_aborts** メトリックに基づいて計算されます。

詳細については、スイッチを選択して、ダッシュボードページで選択されているスイッチ IP アドレスの読み取り IO 中止/失敗のカスタムグラフを表示します。

- 障害

読み取りおよび書き込み失敗のトレンドを表示します。これらの折れ線グラフのメトリックは、過去 72 時間のデータに基づいて計算されます。このメトリックは、Cisco MDS SAN 分析インフラストラクチャによって報告される **read_io_failures** および **write_io_failures** メトリックに基づいて計算されます。

詳細については、スイッチを選択して、ダッシュボードページで選択されているスイッチ IP アドレスの読み取り IO 中止/失敗のカスタムグラフを表示します。

- 上位 10 件のホスト

ドロップダウンリストで選択したメトリックに基づいて、選択したプロトコル/ファブリック/スイッチスコープの上位 10 件のホストエンクロージャ/WWN/デバイスエイリアスを表します。データは、読み取り/書き込み IOPS、スループット、Exchange 完了時間、データアクセス遅延でソートできます。

- 上位 10 件のストレージ

ドロップダウンリストで選択したメトリックに基づいて、選択したプロトコル/ファブリック/スイッチスコープの上位 10 件のストレージエンクロージャ/WWN/デバイスエイリアスを表します。データは、読み取り/書き込み IOPS、スループット、Exchange 完了時間、データアクセス遅延でソートできます。



- (注) 上位 10 件のホストと上位 10 件のストレージは、選択したプロトコル、ファブリック、およびスイッチについて収集された 1 時間ごとのデータに基づいて、過去 72 時間にわたって計算されます。特定の WWPN のエンクロージャ名を変更すると、古いエンクロージャ名の名前は、データが 72 時間後にエージアウトするまで表示されます。

[ダッシュボード (Dashboard)] > [SAN Insights] ウィンドウの上部に、[高 NPU 負荷が検出されました (HIGH NPU LOAD Detected)] と警告メッセージが表示されます。この警告は、前の週に 1 つ以上のスイッチに未確認の Syslog イベントがあることを意味します。このイベントは、保存または表示される分析データの可用性に影響を与える可能性があります。警告を削除するには、これらのイベントを確認する必要があります。

[ダッシュボード (Dashboard)] > [SAN Insights] ウィンドウの上部に、[高 ITL 負荷が検出されました (HIGH ITL LOAD Detected)] と警告メッセージが表示されます。

NPU および ITL ロードをキャプチャするために、SAN コントローラ デバイス マネージャで Syslog が設定されていることを確認します。[SAN > スイッチ (SAN Switch)] を選択します。スイッチをクリックすると、スライドパネルが表示されます。[起動 (Launch)] アイコンをクリックしてスイッチ情報を表示し、[デバイスマネージャ (Device Manager)] をクリックします。[デバイスマネージャ (Device Manager)] タブで、[ログ (Logs)] > [Syslog] > [セットアップ (Setup)] をクリックします。[作成 (Create)] をクリックします。必須パラメータを入力します。[ファシリティ (Facility)] エリアで [syslog] オプションボタンを選択していることを確認してください。[作成 (Create)] をクリックして、SAN コントローラサーバーで Syslog を有効にします。

高 NPU 負荷および高 ITL 負荷を解決するには、[高 NPU 負荷が検出されました (HIGH NPU LOAD Detected)] または [高 ITL 負荷が検出されました (HIGH ITL LOAD Detected)] リンクをクリックします。[モニタリング (Monitor)] > [スイッチ (Switch)] > [イベント (Events)] ページが表示されます。イベントのリストは、タイプ: HIGH_NPU_LOAD およびタイプ: HIGH_ITL_LOAD でフィルタ処理されます。すべてのスイッチを選択し、[確認 (Acknowledge)] をクリックします。これにより、[高 NPU 負荷が検出されました (HIGH NPU LOAD Detected)] および [高 ITL 負荷が検出されました (HIGH ITL LOAD Detected)] 警告が削除されます。

カスタムグラフの表示

SAN Insights メトリックを表示するには、[Dashboard] > [SAN Insights] を選択します。[SAN Insights Dashboard] ページが表示されます。[カスタムグラフの表示 (View Custom Graphing)] をクリックして、SAN Insights メトリックの [カスタムグラフ (Custom Graphing)] ウィンドウを表示します。

ダッシュボードには、過去 72 時間のデータが表示されます。ただし、フローの概要とエンクロージャの概要ドーナツには、最新の更新時刻からの過去 1 時間の集計が表示されます。上位 10 位のホスト/ストレージ、スループット、IOPS、アバート、障害、グラフはそれぞれのデータを表示します。



Note カスタムグラフページの更新間隔は 5 分です。[再生 (Play)] アイコンをクリックすると、5 分ごとに自動的に更新されます。

Cisco SAN Controller を使用すると、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights メトリックを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は、[Web UI] > [設定 (Settings)] > [サーバー設定 (Server Settings)] > [Insights] から変更できます。

新しいプロパティを使用するには、SAN Insights サービスを再起動してください。

カスタムグラフとテーブルの表示

これはフリースタイルダッシュボードで、複数のメトリックを選択でき、選択したメトリックのリアルタイムデータが 5 分ごとに更新されるように構成された複数線グラフで表示され、対応する生データがデータテーブルに表示されます。

右上の [グラフの追加 (Add Graph)] をクリックして、比較のために複数のグラフを追加することもできます。



(注) 自動更新オプションはデフォルトで無効になっています。自動更新機能を有効にするには、[再生 (Play)] アイコンをクリックする必要があります。

SAN Insights メトリックには 2 つのタブがあります。

- グラフ
- 表

グラフ



グラフは、開始日と終了日が選択された対応するメトリックとともにプロットされます。データは5分ごとに更新でき、一時停止ボタンを使用して静的グラフに変換できるため、本質的に動的です。[**グラフの追加 (Add Graph)**] をクリックします。このページでは、一度に最大3つのグラフを追加できます。

SAN コントローラを使用すると、ユーザーは2週間以上（デフォルトの最大90日まで）データを表示できます。この時間枠は、サーバーのプロパティで設定できます。[**時間範囲 (Time Range)**] の横にあるドロップダウンボタンをクリックし、日付を選択します。

カスタムグラフのメトリックが拡張され、ドロップダウンメトリックリストに書き込みIOエラー、読み取りIOエラー、書き込みIOの中断、読み取りIOの中断が含まれるようになります。

各ITLフロー（読み取りおよび書き込み）のECTベースラインは、トレーニング期間にわたって継続的に学習された加重平均を使用して計算されます。

- ECT ベースラインの計算は、トレーニング期間と再調整時間の2つの部分で構成されます。
- ECT ベースラインのトレーニング期間は、デフォルトで7日間です（設定可能）。
- トレーニングの完了後、ECTベースラインは、デフォルトで7日後に再キャリブレーションがトリガーされるまで同じままです（設定可能）。
- デフォルトでは、14日ごとにトレーニングが7日間（周期的に）実行されます。
- パーセント（%）偏差は、ECT ベースラインと比較した現在の正規化された ECT の偏差を示します。

テーブル

Filter: HOST_200000110de5fa10 Metrics: Read IOPs x Write IOPs x Write Throughput x Apply Select up to 4 metrics

Graph **Table**

Filter by attributes

Initiator Enc	Initiator	Target Enc	Target	Namespace ID	Switch IP Address	Port	Timestamp	Read IOPs	Write IOPs	Write Through... (MB/s)
HOST_20000011	20:00:00:11:0d:e	200100110de5fb	20:01:00:11:0d:e	8	172.25.174.146	fc6/4	2021-09-14 12:25:00	8844	10130	4.9466
HOST_20000011	20:00:00:11:0d:e	200100110de5fb	20:01:00:11:0d:e	9	172.25.174.146	fc6/4	2021-09-14 12:25:00	8913	10131	4.9471
HOST_20000011	20:00:00:11:0d:e	200100110de5fb	20:01:00:11:0d:e	3	172.25.174.146	fc6/4	2021-09-14 12:25:00	8704	10695	5.2225

5 Rows Page 1 of 20 << < 1-5 of 100 > >>

[メトリック (Metrics)] ドロップダウンリストから失敗または中止を選択すると、テーブルリストがフィルタ処理され、選択した失敗または中止のメトリックの少なくとも1つをゼロ以外のエントリとして持つ行のみが表示されます。テーブルには 100 レコードのみが表示されます。ただし、ゼロ以外のエラーを見つけやすくするために、テーブルをフィルタ処理して、ゼロ以外の中止または失敗を持つ最後の 100 レコードを表示することができます。失敗または中止を選択すると、テーブルラベルがこの動作を表すように変更されます。

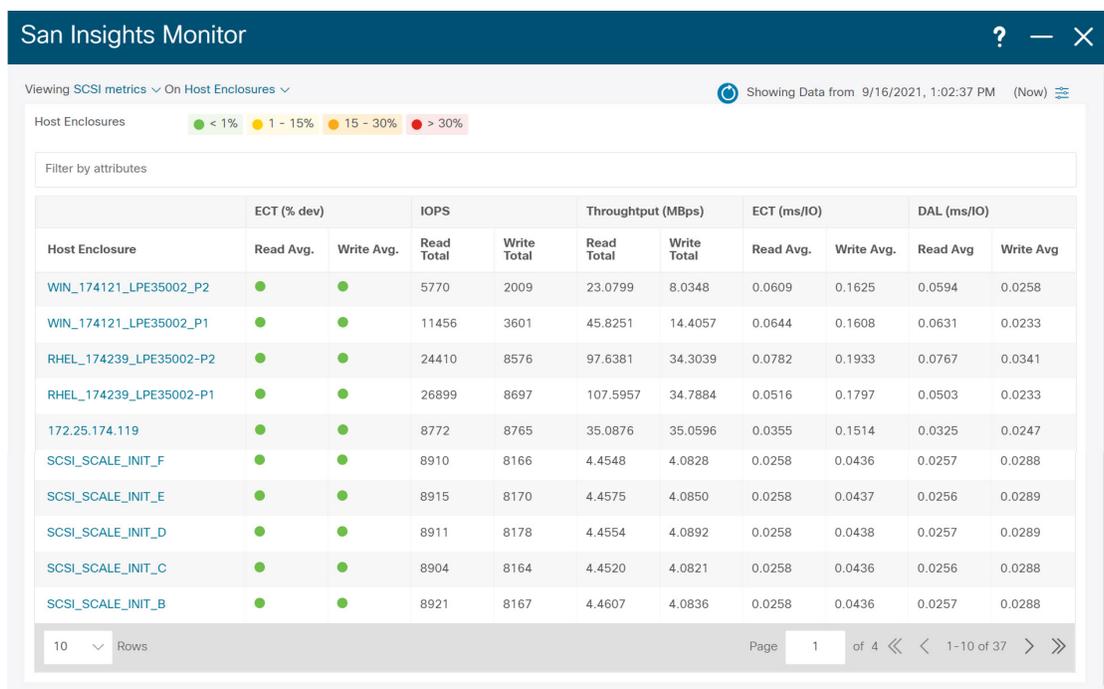
表示するには、属性別フィルタ処理フィールドに 7 つのディメンション (イニシエータ Enc、イニシエータ、ターゲット Enc、ターゲット、LUN、スイッチ IP アドレス、ポート、タイムスタンプ、読み取り IOP、書き込み IOP) のいずれかを入力し (コンマで区切って)、関連するメトリックを選択します。

メトリックのモニタリング

UI パス : [ダッシュボード (Dashboard)] > [SAN Insights] > [メトリックのモニタリング (Monitor Metrics)]

[SAN Insights モニタ (SAN Insights Monitor)] ページには、環境内の問題をすばやく特定できるように、インターフェイスにヘルス関連のインジケータが表示されます。ヘルスインジケータを使用して、ファブリックのどこに問題があるかを理解できます。

SAN コントローラを使用すると、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights モニタを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は [設定 (Settings)] > [サーバー設定 (Server Settings)] > [Insights] から変更できます。



リリース 12.0.1a から、ダッシュボードに SAN Insights モニタリングを表示できます。SAN コントローラ Web UI から、次の手順を実行します。

手順

ステップ 1 [Dashboard] > [SAN Insights] を選択します。

ステップ 2 [メトリックのモニタリング (Monitor Metrics)] をクリックします。

[SAN Insights モニタリング (SAN Insights Monitor)] ウィンドウが表示されます。

ステータスの色は、それぞれのイニシエータターゲットペアの読み取り偏差と書き込み偏差の時間平均です。

ステップ 3 [表示 (Viewing)] ドロップダウンリストを使用して **SCSI** または **NVMe** メトリックを選択して表示し、データタイプを選択します。

ステップ 4 [オン (On)] ドロップダウンリストを使用して、[ホストエンクロージャ (Host Enclosure)]、[ストレージエンクロージャ (Storage Enclosure)]、または [IT ペア (IT Pairs)] を選択して、必要なデータを表示します。

ステップ 5 [更新 (Refresh)] アイコンをクリックして、現在の時刻を表示します。

ウィンドウの右隅にシステム時刻が表示されます。

時間設定アイコンを使用して時間間隔を指定します。[設定 (Setting)] アイコンをクリックし、適切な時間を時間単位で入力し、[適用 (Apply)] をクリックして、選択した時間のデータを表示します。

トポロジページのスイッチで緑色の円のアイコンを選択すると、スイッチ インターフェイス カウンタが表示されます。

ステップ 6 必要な名前をクリックして詳細を表示します。

関連する IT ペアがスライドインパネルに表示されます。

ステップ 7 **[起動 (Launch)]** アイコンをクリックして、ウィンドウを表示します。

同様に、名前を 3 回クリックすると、詳細ビューに移動できます。

[SAN Insights モニタ (SAN Insights Monitor)] ページには、選択したエンクロージャまたは IT ペアのイニシエータとターゲットのペアが表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、ECT (%dev)、IOPS、スループット情報に関するすべてのメトリックの詳細が表示されます。

同様に、ダッシュボードのホストおよびストレージタブから SAN Insights モニタを表示できます。

- **[ダッシュボード (Dashboard)]** > **[ホスト (Host)]** を選択し、必要なホスト名の **[i]** アイコンをクリックします。ホストエンクロージャの詳細については、[ホスト](#) セクションを参照してください。
- **[ダッシュボード (Dashboard)]** > **[ストレージ (Storage)]** を選択し、必要なストレージ名の **[i]** アイコンをクリックします。ストレージエンクロージャの詳細については、[ストレージ](#) セクションを参照してください。

イニシエータとターゲット (IT) のペアの詳細については、「[IT ペアの表示 \(27 ページ\)](#)」セクションを参照してください。

IT ペアの表示

Cisco Nexusダッシュボード ファブリック コントローラ では、SCSI と NVMe の 2 つのプロトコルに基づいて SAN Insights メトリックを表示できます。デフォルトでは、SCSI プロトコルが選択されます。ただし、この設定は**[設定 (Settings)]** > **[サーバー設定 (Server Settings)]** > **[Insights]** から変更できます。新しいプロパティを使用するには、SAN Insights サービスを再起動してください

Cisco Nexusダッシュボード ファブリック コントローラ Web UI から IT ペアを表示するには、次の手順を実行します。

始める前に

UI パス : **[ダッシュボード (Dashboard)]** > **[SAN Insights]** > **[メトリックのモニタリング (Monitor Metrics)]**

手順

ステップ 1 [ダッシュボード (Dashboard)] > [SAN Insights] > [メトリックのモニタリング (Monitor Metrics)] を選択します

SAN Insights モニタリングページが表示されます。詳しくは「[メトリックのモニタリング](#)」を参照してください。

ステップ 2 [表示 (Viewing)] ドロップダウンリストを使用して **SCSI** または **NVMe** メトリックを選択して表示し、データタイプを選択します。

ステップ 3 データを表示するには、[オン (On)] ドロップダウンリストを使用して [IT ペア (IT Pairs)] を選択します。

ステップ 4 必要な IT ペア名をクリックします。

IT ペアのスライドインパネルが表示されます。

ステップ 5 [起動 (Launch)] アイコンをクリックして、IT ペアウィンドウを表示します。

IT ペアのウィンドウが表示されます。

IT ペアウィンドウには、選択した IT ペアのイニシエータとターゲット (IT) ペア、トポロジ、平均 ECT/DAL/読み取り/書き込み時間、およびスイッチインターフェイスが表示されます。

- **イニシエータターゲットペア** - このテーブルには、選択した IT ペア名のすべての IT ペアが一覧表示されます。フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、中止、失敗などに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **トポロジ** : IT ペア間のエンドツーエンドのトポロジレイアウトおよびパス情報を示します。カードの [表示 (View)] で、[+] または [-] をクリックしてズームインおよびズームアウトします。同様に、マウスのスクロールホイールを使用して、拡大および縮小ができます。トポロジ表示を更新するには、[更新 (Refresh)] をクリックします。[レイアウトの選択 (Select layout)] ドロップダウンリストを選択して、トポロジを表示します。これは、階層的 (Hierarchical) または階層的左 - 右 (Hierarchical Left-Right) ビューのいずれかです。
- フローテーブルには、ECT/DAL/読み取り/書き込み時間、アクティブ I/O、IOPS、スループットなどに関するすべてのメトリックの詳細が、1 時間の平均値とベースライン情報とともに表示されています。
- **スイッチインターフェイス** : このテーブルには、選択したインターフェイスに対して選択された過去 1 時間のデータが表示されます。スイッチ名とインターフェイス名は、スイッチインターフェイス テーブルの上部に表示されます。



第 4 章

トポロジ

UI ナビゲーション : [トポロジ (Topology)] をクリックします。

[トポロジ (Topology)] ウィンドウには、スイッチ、リンク、ファブリックエクステンダ、ポートチャネル設定、仮想ポートチャネルなど、さまざまなネットワーク要素に対応する色分けされたノードとリンクが表示されます。このウィンドウを使用して、次のタスクを実行します。

- これらの各要素の詳細を表示するには、対応する要素の上にカーソルを移動します。
- トポロジのナビゲーションを表示するには、上部のパンくずリストを表示します。
- デバイスまたは要素をクリックすると、右側にスライドインペインが表示され、デバイスまたは要素に関する詳細情報が表示されます。トポロジの詳細を表示するには、ノードをダブルクリックしてノードトポロジを開きます。たとえば、[トポロジ (Topology)] ウィンドウでファブリックトポロジとそのコンポーネントを表示するには、ファブリックノードをダブルクリックしてから、表示する要素（ホスト、マルチキャストグループ、マルチキャストフローなど）をダブルクリックし、ファブリックタイプを表示します。
- ファブリックのファブリックサマリを表示する場合は、ファブリックノードをクリックします。[ファブリックサマリ (Fabric Summary)] スライドインペインから、[ファブリックの概要 (Fabric Overview)] ウィンドウを開きます。または、ファブリックを右クリックして [詳細表示 (Detailed View)] を選択し、[ファブリックの概要 (Fabric Overview)] ウィンドウを開きます。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、[ファブリックの概要 \(58 ページ\)](#) を参照してください。
- 同様に、スイッチをクリックすると、設定されたスイッチ名、IP アドレス、スイッチモデル、およびステータス、シリアル番号、正常性、最後にポーリングされた CPU 使用率、最後にポーリングされたメモリ使用率などのその他のサマリ情報が [スイッチ (Switch)] スライドインペインに表示されます。-in ペイン。詳細を表示するには、[起動 (Launch)] アイコンをクリックして、[スイッチの概要 (Switch Overview)] ウィンドウを開きます。[スイッチの概要 (Switch Overview)] ウィンドウの詳細については、[スイッチの概要 \(97 ページ\)](#) を参照してください。

SAN スwitch の役割は、コア ルータ と エッジ ルータ の 2 つ だけ です。

- **[アクション (Actions)]** ドロップダウンリストからアクションを選択し、トポロジで選択した要素に基づいてさまざまなアクションを実行します。
- トポロジ内の要素に対してアクションを実行するには、アクションドロップダウンリストにリストされている要素以外の要素を右クリックします。これにより、適切なウィンドウが開き、要素に基づいてタスクを実行できます。たとえば、ファブリックを右クリックすると、さまざまな設定、ファブリックの削除、バックアップと復元などのタスクを実行できます。

この項の内容は、次のとおりです。

- [トポロジの検索 \(30 ページ\)](#)
- [トポロジの表示 \(30 ページ\)](#)

トポロジの検索

効果的な検索を行うには、検索バーで検索属性と検索条件の組み合わせを使用します。検索属性と検索条件の組み合わせを検索バーに入力すると、対応するデバイスがトポロジ内で強調表示されます。

等号 (=)、不等号 (!=)、次を含む (**contains**)、次を含まない (!**contains**) などの検索条件を適用できます。

SAN ファブリックに使用できる検索属性はファブリック名です。

トポロジにデバイスが表示されたら、そのデバイスをダブルクリックしてトポロジ内をさらに移動します。たとえば、検索したファブリックがトポロジに表示されている場合は、ファブリック (クラウドアイコン) をダブルクリックしてトポロジ内を移動します。さらに、ファブリックがトポロジに表示された後、条件とスイッチ名、IPアドレス、モデル、シリアル、ソフトウェアバージョン、およびアップタイムなどの条件とさまざまな検索持続性に基づいて検索を続行できます。



(注) トポロジの特定のレベルではフィルタのみが許可されます。つまり、フィルタは検索の代わりに使用されます。これらのレベルのトポロジリストには、限られた数のエンティティが表示されます。

トポロジの表示

移動するには、空白の任意の場所をクリックしたまま、カーソルを上下左右にドラッグします。スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

スイッチを複数選択する場合、マウสดラッグを放してスイッチの選択を終了する前に、修飾キー (cmd/ctrl) を放す必要があります。

[表示 (View)] ペインでは、デバイスとリンクに関する次の情報を表示できます。

- レイアウトオプション：画面に合わせてレイアウトを拡大、縮小、または調整できます。トポロジを更新したり、トポロジへの変更を保存したりすることもできます。詳細については、[ズーム、パン、ドラッグ \(33 ページ\)](#) を参照してください。
- [レイアウトの選択 (Select Layout)] ドロップダウンリスト：このドロップダウンリストからトポロジのレイアウトを選択し、レイアウトオプションで **[トポロジレイアウトの保存 (Save Topology Layout)]** をクリックします。詳細については、[レイアウト \(34 ページ\)](#) を参照してください。
- ステータス：すべてのデバイスまたはリンクのステータスが異なる色で表示されます。LAN トポロジの構成ステータスと動作ステータスも表示できます。詳細については、[ステータス \(34 ページ\)](#) を参照してください。

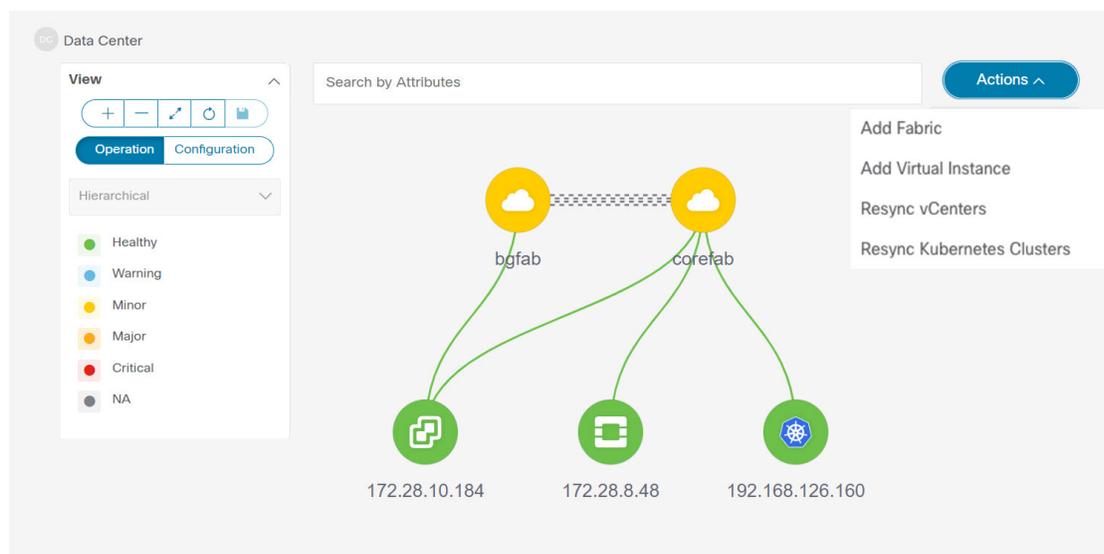
ノードのトポロジは、複数のスコープで表示されます。各スコープは、階層順に表示されません。スコープ階層はトピックパス (パンくずリスト) として表示され、必要なスコープに移動できます。スコープは次のとおりです。

- Data Center
- クラスタ (VCenter)
- リソースリスト (DVS、コンピューティング、および VM)
- Resource



- (注)
- **[トポロジ (Topology)]** ウィンドウでは、FEX の操作と構成ステータスが計算されないため、FEXはグレー (**[未知 (Unknown)]**) または **[該当なし (NA)]** で表示されます。
 - あるポートから別のポートにケーブルを移動した後、古いファブリックリンクは **[トポロジ (Topology)]** ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。削除が意図的なものであった場合は、リンクを右クリックして削除します。スイッチを手動で再検出すると、そのスイッチへのすべてのリンクが削除され、再学習されます。

マルチサイトドメイン (MSD) ファブリックが子ファブリックとともに展開されている場合、マルチサイトトポロジを表示するには、ファブリックノードをダブルクリックしてから MSD スコープを選択するか、灰色の MSD ノードをダブルクリックして MSD トポロジを表示します。



SAN トポロジの要素の表示

UI ナビゲーション : [トポロジ (Topology)] をクリックします。

ここでは、SAN ファブリックの [トポロジ (Topology)] ウィンドウに表示されるさまざまな要素またはエンティティについて説明します。

VSAN

[トポロジ (Topology)] ウィンドウで、ファブリックをダブルクリックしてファブリック トポロジを表示します。SAN ファブリックには、VSAN ノードとスイッチが含まれます。VSAN ノードには、カッコ内に数字が表示され、ファブリック内の VSAN の数を示します。VSAN ノード トポロジ内の個々の VSAN を表示するには、VSAN ノードをダブルクリックします。

VSAN トポロジには、VSAN に接続されているゾーンとスイッチが表示されます。VSAN をダブルクリックして VSAN トポロジを開き、ゾーンとスイッチを表示します。ただし、スイッチには VSAN が設定され、VSAN メンバーシップを持つリンクが必要です。

ゾーン

VSAN ノードをダブルクリックすると、VSAN ゾーンが表示されます。その VSAN およびゾーンノードのスイッチは、ゾーンの数を示します。そのゾーンノードをダブルクリックすると、個々のゾーンノードが表示されます。ゾーンノードをダブルクリックすると、そのゾーンのスイッチと、選択したゾーンのメンバーであるエンドデバイスとの接続 (ISL) が表示されます。

ホストとストレージ

ゾーン トポロジには、ゾーンに関連し、スイッチに接続されているホストとストレージデバイスが表示されます。[トポロジ (Topology)] ウィンドウで、ゾーンをダブルクリックしてホストとストレージデバイスを表示します。

または、スイッチトポロジを表示するには、ファブリックトポロジ内のスイッチを直接クリックします。スイッチトポロジには、スイッチに接続されているホストとストレージデバイスが表示されます。

ホスト

ホストデバイスをクリックすると、スライドインペインにホストに関する詳細情報が表示されます。スライドインペインから、ホストダッシュボードを開くことができます。または、ホストデバイスを右クリックし、**[詳細表示 (Detailed View)]** をクリックしてホストダッシュボードを開くこともできます。

ストレージ

ストレージデバイスをクリックすると、ストレージの詳細情報がスライドインペインに表示されます。スライドインペインから、ストレージダッシュボードを開くことができます。または、ストレージデバイスを右クリックして **[詳細ビュー (Detailed View)]** をクリックし、ストレージダッシュボードを開きます。

Links

スイッチトポロジで、2つのデバイス（スイッチとストレージなど）を接続するリンクをクリックして、**[リンク (Link)]** スライドインペインを開きます。このペインには、パフォーマンスデータの最後のポーリングに関する詳細が表示されます。ただし、**[パフォーマンスデータ収集設定 (Performance Data Collection Settings)]** でファブリックのパフォーマンスモニタリングを設定しておく必要があります。これにより、Nexusダッシュボードファブリックコントローラはトラフィック情報を収集でき、集約された情報がトラフィック使用率を示すグラフとともに表示されます。Nexusダッシュボードファブリックコントローラは、ファブリック内のすべてのスイッチのすべてのポート、リンクなどについて、5分ごとに最後のポーリングメトリックを更新します。このペインに表示される日時が最新の場合、最後のポーリングメトリックの詳細は最新です。このスライドインペインに表示される詳細は次のとおりです。

- リンク キャパシティ、VSAN、ステータスなどの一般情報。
- 平均、最大、および最小の Rx および Tx などの詳細を含む、過去 24 時間のトラフィックに関する情報（バイト単位）。
- Time、Rx、Tx などの最後のポーリングメトリックは、**[グラフ (Graph)]** タブのグラフと **[テーブル (Table)]** タブのテーブル形式で表示できます。テーブルがページ分割されていることに注意してください。

ズーム、パン、ドラッグ

ズームインまたはズームアウトするには、ウィンドウの左下にあるコントロールを使用するか、マウスのホイールを使用します。

移動するには、空白の任意の場所をクリックしたまま、カーソルを上下左右にドラッグします。

スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

レイアウト

トポロジは、トポロジの配置方法を記憶する [レイアウトの保存 (Save Layout)] オプションとともに、さまざまなレイアウトをサポートします。

- **[Hierarchical]** および **[Hierarchical Left-Right]** : トポロジのアーキテクチャ ビューを提供します。CLOS トポロジの設定方法に関するノードを示すさまざまなスイッチロールを定義できます。



Note 大規模なセットアップを実行する場合、リーフ層のすべてのスイッチを簡単に表示できるようになるのは困難です。これを軽減するために、Nexus ダッシュボード ファブリック コントローラ は 16 のスイッチごとにリーフ層を分割します。

- **Circular** および **Tiered-Circular** : ノードを円形または同心円状に描画します。
- **[ランダム (Random)]** : ノードはウィンドウにランダムに配置されます。Nexus ダッシュボード ファブリック コントローラ は、推測を行い、近接するノードをインテリジェントに配置しようとします。
- **カスタム保存レイアウト** : ノードは、必要に応じてドラッグできます。必要に応じて配置した後、**[保存 (Save)]** をクリックして位置を保持します。次回トポロジにアクセスすると、Nexus ダッシュボード ファブリック コントローラ により最後に保存したレイアウト位置に基づいてノードが描画されます。

レイアウトを選択する前に、Nexus ダッシュボード ファブリック コントローラ はカスタムレイアウトが適用されているかどうかを確認します。カスタムレイアウトが適用されている場合は、それを使用します。Nexus ダッシュボード ファブリック コントローラ カスタムレイアウトが適用されていない場合は、Nexus ダッシュボード ファブリック コントローラ はスイッチが異なる階層に存在するかどうかを確認し、階層レイアウトまたは階層左右レイアウトを選択します。他のすべてのレイアウトが失敗した場合は、強制指向レイアウトが選択されます。

ステータス

各ノードとリンクの色分けは、その状態に対応しています。動作の色とその意味を次のリストに示します。

- 緑 : 要素が正常に機能し、意図したとおりに機能していることを示します。
- 青 : 要素が警告状態にあり、それ以上の問題を防ぐために注意が必要であることを示します。
- 黄色 : 要素に小さな問題があることを示します。
- オレンジ : 要素に重大な問題があり、それ以上の問題を回避するには注意が必要であることを示します。

- 赤：要素が重大な状態にあり、すぐに対処する必要があることを示します。
- グレー：要素を特定するための情報がないか、要素が検出されたことを示します。

設定の色とその意味を次のリストに示します。

- 緑：要素が目的の設定と同期していることを示します。
- 青：要素に保留中の展開があることを示します。
- 黄色：アクティブな展開が進行中であることを示します。
- 赤：要素が意図した構成と同期していないことを示します。
- グレー：情報が不足しているか、設定の同期計算がサポートされていないことを示します。



Note

- [トポロジ (Topology)] ウィンドウでは、FEXの操作と構成ステータスが計算されないため、FEXはグレー ([不明 (Unknown)] または [n/a]) で表示されます。
 - あるポートから別のポートにケーブルを移動した後、古いファブリックリンクは[トポロジ (Topology)] ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。削除が意図的なものであった場合は、リンクを右クリックして削除します。スイッチを手動で再検出すると、そのスイッチへのすべてのリンクが削除され、再学習されます。
-



第 I 部

SAN

- ファブリック (39 ページ)
- スイッチ (87 ページ)
- SAN リンク (107 ページ)
- インターフェイス (127 ページ)
- エンドデバイス (141 ページ)
- ホストパスの冗長性 (147 ページ)
- ポート監視 (153 ページ)
- アクティブゾーン (161 ページ)
- ストレージ (163 ページ)



第 5 章

ファブリック

- [ファブリック \(39 ページ\)](#)
- [ファブリックの概要 \(58 ページ\)](#)

ファブリック

リリース 12.0.1a から、SAN コントローラを使用して SAN ファブリックを作成できるようになりました。

次の表では、[SAN コントローラ (SAN Controller)] > [SAN] > [ファブリック (Fabrics)] > [ファブリック (Fabrics)] で表示されるフィールドについて説明します。

フィールド	説明
Fabric Name (ファブリック名)	ファブリックの名前を指定します。
シードスイッチ	ファブリック内のスイッチを検出するために使用されるシードスイッチを指定します。
状態	ファブリックの状態を指定します。
SNMPv3 / SSH	SNMP および SSH アクセスを許可するかどうかを指定します。
ユーザー/コミュニティ	ファブリックを作成したユーザーのロールを指定します。
認証/プライバシー	認証タイプを表示します。
ライセンス有効	ファブリック内のすべてのスイッチにライセンスがあるかどうかを指定します。
ヘルス (Health)	ファブリックのヘルスを表示します。
パフォーマンス収集	ファブリックでパフォーマンス収集を有効にするか無効にするかを指定します。
更新時刻	ファブリックが作成または更新された時刻を指定します。

フィールド	説明
含める VSANS	ファブリックに含まれる VSANS を指定します。
除外する VSANS	除外する VSANS を指定します。

次の表で、[SAN]>[ファブリック (Fabrics)]>[ファブリック (Fabrics)]で表示される [アクション (Actions)] メニュー ドロップダウンリストのアクション項目について説明します。

アクション項目	説明
ファブリックの追加	[アクション (Actions)] ドロップダウンリストで、[ファブリックの追加 (Add Fabric)] を選択します。手順については、 ファブリックの追加 (41 ページ) を参照してください。
ファブリックの編集	編集するファブリックを選択します。[アクション (Actions)] ドロップダウンリストで、[ファブリックの編集 (Edit Fabrics)] を選択します。必要な変更を行って、[適用 (Apply)] をクリックします。手順については、 ファブリックの編集 (42 ページ) を参照してください。
ファブリックの削除	削除する 1 つ以上のファブリックを選択します。[アクション (Actions)] ドロップダウンリストで、[ファブリックの削除 (Delete Fabrics)] を選択します。[確認 (Confirm)] をクリックして、ファブリックを削除します。手順については、 ファブリックを削除しています (42 ページ) を参照してください。
ファブリックの再検出	ファブリックに関連付けられたスイッチ、リンク、およびエンドデバイスを再検出できます。再検出する 1 つ以上のファブリックを選択します。[アクション (Actions)] ドロップダウンリストで、[ファブリックの再検出 (Rediscover Fabrics)] を選択します。[状態 (State)] 列の進捗バーに、再検出の進行状況が表示されます。手順については、 ファブリックの再検出 (43 ページ) を参照してください。
ファブリックの消去	ファブリックの存在しないスイッチ、リンク、およびエンドデバイスを消去できます。消去する 1 つ以上のファブリックを選択します。[アクション (Actions)] ドロップダウンリストで、[ファブリックの消去 (Purge Fabrics)] を選択します。手順については、 ファブリックの消去 (43 ページ) を参照してください。

アクション項目	説明
パフォーマンスの設定	<p>ファブリックに関連付けられたリンク、スイッチインターフェイス、およびエンドデバイスのパフォーマンスモニタリングを有効にすることができます。パフォーマンスモニタリング用に1つ以上のファブリックを選択します。[アクション (Actions)] ドロップダウンリストで、[パフォーマンスの設定 (Configure Performance)] を選択します。必要な変更を行って、[適用 (Apply)] をクリックします。</p> <p>詳細な手順については、パフォーマンスの設定を参照してください。</p>
SAN Insights の設定	<p>選択したファブリックで SAN Insights を設定できます。</p> <p>詳細については、SAN Insights の設定を参照してください。</p>
バックアップの設定	<p>ファブリックデータのバックアップを設定およびスケジュールできます。</p> <p>手順については、ファブリックバックアップの構成 (56 ページ)を参照してください。</p>

この章は、次の項で構成されています。

ファブリックの追加

Cisco SAN コントローラ Web UI を使用してファブリックを作成するには、次の手順を実行します。

手順

- ステップ 1 [SAN] > [ファブリック (Fabrics)] > [SAN ファブリック (SAN Fabrics)] を選択します。
 - ステップ 2 [アクション (Actions)] > [ファブリックの追加 (Add Fabrics)] を選択します。
 - ステップ 3 [ファブリック名 (Fabric Name)] フィールドに一意のファブリック名を入力します。
 - ステップ 4 [ファブリックシードスイッチ (Fabric Seed Switch)] テキストボックスにシードスイッチの IP アドレスを入力します。
- シードスイッチの DNS 名を入力することもできます。
- ステップ 5 アクセスを有効にするには、SNMPv3/SSH チェックボックスをオンにします。
 - ステップ 6 [認証/プライバシー (Authentication/Privacy)] ドロップダウンリストから、スイッチの検出に適切な認証を選択します。

- ステップ 7** シードスイッチにアクセスするためのユーザー名とパスワードを適切なフィールドに入力します。
- ステップ 8** VSANのみを使用してスイッチを検出するには、[VSANによる検出の制限 (Limit Discovery by VSAN)] チェックボックスをオンにします。
- VSANに関連付けられているスイッチまたは関連付けられていないスイッチを検出することを選択できます。
- ステップ 9** (任意) UCS ログイン情報を使用してスイッチを検出することもできます。
- ステップ 10** [追加 (Add)] をクリックして、ファブリックを追加します。

ファブリックの編集

Cisco SAN コントローラ Web UI ファブリックを編集するには、次の手順を実行します。

手順

- ステップ 1** [SAN] > [ファブリック (Fabrics)] > [SAN ファブリック (SAN Fabrics)] を選択します。
- ステップ 2** チェックボックスをオンにして、必要なファブリック名を編集し、[アクション (Actions)] > [ファブリックの編集 (Edit Fabrics)] を選択します。
- ステップ 3** [ファブリックの編集 (Edit Fabrics)] ウィンドウが表示されます。一度に編集できるファブリックは1つだけです。
- ステップ 4** 新しいファブリックの [ファブリック名 (Fabric Name)] を入力します。
- ステップ 5** (任意) [SNMPV3] チェックボックスをオンにします。SNMPV3 をオンにすると、[コミュニティ (Community)] フィールドが [ユーザー名 (User Name)] および [パスワード (Password)] に変わります。
- ステップ 6** [ユーザー名 (Username)] と [パスワード (Password)]、プライバシーを入力し、いずれかのステータスオプションを選択することで、SAN コントローラ Web クライアントでファブリックを管理する方法を指定します。
- ステップ 7** ステータスを [管理 (Managed)]、[非管理 (Unmanaged)]、または [継続的に管理 (Managed Continuously)] に変更します。
- ステップ 8** (任意) [UCS ログイン情報を使用 (Use UCS Credentials)] チェックボックスをオンにします。UCS ログイン情報を変更する場合。
- ステップ 9** [ユーザー名 (Username)] と [パスワード (Password)] を入力します。
- ステップ 10** [適用 (Apply)] をクリックし、変更を保存します。

ファブリックを削除しています

SAN コントローラ Web UI を使用してファブリックを削除するには、次の手順を実行します。

手順

-
- ステップ 1** [SAN]>[ファブリック (Fabrics)]>[SAN ファブリック (SAN Fabrics)]を選択します。
- ステップ 2** [アクション (Actions)]>[ファブリックの削除 (Delete Fabrics)]を選択して、データソースからファブリックを削除し、そのファブリックのデータ収集を中止します。
-

ファブリックの再検出

Cisco SAN コントローラ Web UI を使用してファブリックを削除するには、次の手順を実行します。

手順

-
- ステップ 1** [SAN]>[ファブリック (Fabrics)]>[SAN ファブリック (SAN Fabrics)]を選択します。
- ステップ 2** チェックボックスを選択して必要なファブリック名を再検出し、[アクション (Actions)]>[ファブリックの再検出 (Rediscover Fabrics)]を選択します。
- ステップ 3** ポップアップ ウィンドウで [Yes] をクリックします。
- ファブリックウィンドウの [状態 (State)] 列には、選択したファブリックの再検出の進行状況が表示されます。
- ファブリックが再検出されました。
-

ファブリックの消去

[消去 (パージ)] オプションを使用して、ファブリック 検出テーブルをクリーニングおよび更新できます。

手順

-
- ステップ 1** [SAN]>[ファブリック (Fabrics)]を選択します。
- ステップ 2** 消去するファブリックの横にあるチェックボックスをオンにします。
- ステップ 3** [アクション (Actions)]>[ファブリックの消去 (Purge Fabrics)]を選択します。
- ファブリックは消去されます。

SAN コントローラリリース 12.0.1a から、トポロジウィンドウでファブリックを消去できます。

- [トポロジ (Topology)] を選択し、ファブリックを選択し、ファブリックを右クリックして、[ファブリックを消去する (Purge Down Fabric)] を選択します。

ファブリックは消去されます。

パフォーマンスの設定

パフォーマンスマネージャを使用してファブリックを管理する場合は、ファブリック上でフローおよび収集の初期セットを設定する必要があります。SANコントローラを使用してパフォーマンス収集の追加や削除を実行できます。スイッチのコレクションを作成する前に、スイッチにライセンスを付与し、**managedContinuously**状態に維持します。このウィンドウには、ライセンスを受けたファブリックのみが表示されます。

手順

- ステップ1 [SAN]>[ファブリック (Fabrics)]を選択します。
- ステップ2 パフォーマンス収集を設定するファブリックの横にあるチェックボックスをオンにします。
- ステップ3 [アクション (Actions)]>[パフォーマンスの設定 (Configure Performance)]を選択します。
[パフォーマンスデータ収集設定 (Performance Data Collection Settings)]ウィンドウが表示されます。
- ステップ4 他のチェックボックスを有効にするには、[パフォーマンス収集 (Performance Collection)]チェックボックスをオンにします。
- ステップ5 必要な ISL/NPV リンク、ホスト、ストレージ、および FC イーサネットを選択するか、[すべて選択 (Select All)]ボックスを選択して、これらのデータタイプのパフォーマンス収集を有効にします。
 - a) SAN デバイスの温度データを収集するには、[設定 (Settings)]>[サーバー設定 (Server Settings)]>[PM]を選択します。
 - b) [PM] タブで、[SAN センサー検出を有効にする (Enable SAN Sensor Discovery)]および [SAN スwitchの温度を収集する (Collect Temperature for SAN Switches)]のチェックボックスをオンにします。
- ステップ6 [Apply] をクリックして、設定を保存します
- ステップ7 確認ダイアログボックスで、[はい (Yes)] をクリックしてパフォーマンスコレクタを再起動します。

次のタスク

Nexusダッシュボードファブリックコントローラにアップグレードした後、復元された古いパフォーマンスマネージャと高チャートデータを表示するには、ファブリックごとにパフォーマンスマネージャを手動で有効にする必要があります。ただし、古い温度データは復元されません。

アップグレードされた Nexus ダッシュボード ファブリック コントローラ セットアップで温度データの収集を開始するには、[設定 (Settings)] > [サーバー設定 PM (Server Settings PM)] タブに移動します。[LAN スイッチの温度を収集 (Collect Temperature for LAN Switches)] チェックボックスをオンにして、[保存 (Save)] をクリックします。[LAN センサー検出を有効にする (Enable LAN Sensor Discovery)] チェックボックスはデフォルトで有効になっていることに注意してください。

SAN Insights

SAN Insights 機能を使用すると、ファブリック内のフロー分析を設定、モニタリング、および表示できます。SAN コントローラの SAN Insights 機能を使用すると、インターフェイスでヘルス関連のインジケータを可視化できるため、ファブリックの問題をすばやく特定できます。また、ヘルスインジケータにより、ファブリックの問題を理解することができます。SAN Insights 機能は、ホストから LUN へのより包括的なエンドツーエンドのフローベースのデータも提供します。

SAN コントローラは、コンパクトな GPB トランスポートを使用して SAN テレメトリストリーミング (STS) をサポートし、テレメトリのパフォーマンスを向上させ、SAN Insights の全体的な拡張性を向上させます。

SAN Insights のストリーミングの安定性とパフォーマンスについては、SAN コントローラの展開に [SAN Insights のサーバープロパティ](#) を参照してください。SAN Insights の展開にシステム RAM、vCPU、および SSD が使用されていることを確認します。SAN コントローラとスイッチ間の時刻同期を維持するには、NTP の使用をお勧めします。カウンタ統計を表示するための PM 収集を有効にします。

リリース 12.0.1a から、SAN ITL/ITN フローのポリシーベースのアラーム生成を作成できるようになりました。Web UI から、[操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] > [アラームポリシー (Alarm Policies)] を選択してポリシーを作成します。

前提条件

- SAN Insights は、仮想データノードと物理ノードでサポートされています。
- SAN Insights 機能は、Nexus Dashboard のアプリノード展開ではサポートされていません。
- Nexus Dashboard の単一ノードおよび 3 ノードの展開は、SAN Insights の展開でサポートされています。
- 11.2(1) より古いバージョンの Cisco SAN Insights を使用して、SAN Insights ストリーミングが KVGPB エンコーディングで設定されている場合、スイッチは、SAN Insights バージョン 11.2(1) 以降でストリーミングを設定している間も、KVGPB エンコーディングでストリーミングを継続します。SAN Insights のコンパクトな GPB ストリーミング設定は、SAN コントローラ 11.2(1) 以降でサポートされています。Compact GPB を使用してストリーミングするには、アップグレード後に SAN Insights を新しく設定する前に、古い KVGPB ストリーミングを無効にします。分析とテレメトリを無効にするには、Cisco SAN コントローラ Web UI で、[SAN] > [ファブリック (Fabrics)] を選択し、ファブリックを選択し、[ア

クシオン (Actions)] > [SAN Insights の設定 (Configure SAN Insights)] を選択して、[次へ (Next)] をクリックします。[スイッチの設定 (Switch Configuration)] 画面で、必要なスイッチを選択し、[アクション (Actions)]、>[分析を無効にする (Disable Analytics)] の順に選択して、選択したスイッチのすべての分析およびテレメトリ設定をクリアします。

- SAN Insights 機能は、Cisco MDS NX-OS リリース 8.3(1) 以降でサポートされています。

永続的な IP アドレスの設定

SAN コントローラリリース 12.1.1e をインストールまたはアップグレードする前に、Cisco Nexus ダッシュボードで永続的な IP アドレスを設定する必要があります。

Cisco Nexus Dashboard で、サービスに IP プールアドレスが割り当てられていることを確認します。詳細については、『Cisco Nexus Dashboard User Guide』の「Cluster Configuration」の項を参照してください。



Note SAN コントローラ導入用に 1 つのノードで SAN Insights を構成するには、SAN Insights 受信者に使用可能な永続的 IP が 1 つ必要です。同様に、SAN コントローラを導入するために 3 つのノードで SAN Insights を構成するには、3 つの使用可能な永続的 IP アドレスが必要です。

Cisco Nexus ダッシュボードで永続的 IP アドレスを設定するには、次の手順を実行します。

Procedure

- ステップ 1** [インフラストラクチャ (Infrastructure)] > [クラスタ設定 (Cluster Configuration)] を選択します。
- ステップ 2** [全般 (General)] タブの [外部サービスプール (External Service Pools)] カードで、[編集 (Edit)] アイコンをクリックします。
[外部サービスプール (External Service Pools)] ウィンドウが表示されます。
- ステップ 3** SAN コントローラの IP アドレスを設定するには、データサービス IP で、[IP アドレスの追加 (Add IP Address)] をクリックし、必要な IP アドレスを入力して、[チェック (check)] アイコンをクリックします。
- ステップ 4** [保存 (Save)] をクリックします。

注意事項と制約事項

- SAN Insights 機能を展開するために、SAN コントローラおよびサポートされているスイッチの時間の設定がローカル NTP サーバーに同期されていることを確認します。

- 適用可能な夏時間の設定は、スイッチと SAN コントローラ全体で一貫している必要があります。
- ストリーミング間隔を変更するには、スイッチから CLI を使用して、インストールされている SAN コントローラのクエリを削除します。SAN コントローラサーバーのプロパティで **san.telemetry.streaming.interval** プロパティを変更します。間隔の許容値は 30 ~ 300 秒です。デフォルト値は 30 秒です。デフォルト値に問題がある場合、または値を増やす場合は、デフォルト値を 60 秒に設定します。デフォルト値は、SAN Insights の設定中に変更できます。[スイッチの設定ウィザード (Switch Configuration)] の [間隔 (Interval(s))] 列で、ドロップダウンリストから必要な値を選択します。
- スイッチ側のポート サンプリング ウィンドウには、すべてのポートが含まれている必要があります (デフォルト)。
- ISL クエリインストールタイプは、ストレージが接続されているスイッチ (ストレージエッジスイッチ) にのみ使用します。
- ISL クエリインストールタイプの場合、SAN Insights の設定ウィザードで、非 MDS プラットフォームスイッチへのポートチャネル ISL のメンバーであるインターフェイスで分析を有効にすることはできません。
- スイッチベースの FM_Server_PKG ライセンスをインストールした後、SAN Insights の設定ウィザードがインストールされたライセンスを検出するまでに最大 5 分かかる場合があります。

SAN Insights ダッシュボードについては、[SAN Insights](#) を参照してください。

SAN Insights の設定については、[SAN Insights の設定](#) を参照してください。

SAN Insights のサーバープロパティ

サーバー設定値を変更するには、Web UI の [設定 (Settings)] > [サーバー設定 (Server Settings)] > [Insights] に移動します。



- (注) サーバーのプロパティを変更する場合は、新しいプロパティ値を使用するように SAN コントローラを再起動してください。

次の表で、フィールド名、説明、およびそのデフォルト値について説明します。

表 4: SAN Insights のサーバープロパティ

フィールド名	説明	デフォルト値
テレメトリページのデフォルトプロトコル scsi/nvme	対応するデータを表示するために、SAN Insights UI ページで必要なデフォルトのプロトコル選択を指定します (SCSI または NVMe)。	SCSI

フィールド名	説明	デフォルト値
SAN Insights ECT スレッド数	ECT クエリに使用するスレッドの数を指定します。	4
最大集計バケットサイズ	集計クエリに使用するバケットの最大数を指定します。	40,000
データテーブルダウンロードサイズ	テーブルダウンロードのレコード数を指定します。	1000
ECT データ制限	ECT データ制限を指定します。	14 (注) ECT データ制限の値は、SAN テレメトリ保持ポリシー（ベースライン/後処理）の値以下である必要があります。
SAN テレメトリ偏差の低しきい値	通常と低の変化点となる値を指定します。	1
SAN テレメトリ偏差中しきい値	低と中の変化点となる値を指定します。	15
SAN テレメトリ偏差の高しきい値	中と高の変化点となる値を指定します。	30
NVMe の SAN テレメトリ偏差の低しきい値	NVMe の通常と低の変化点となる値を指定します。	1
NVMe の SAN テレメトリ偏差の中しきい値	NVMe の低と中の変化点となる値を指定します。	2
NVMe の SAN テレメトリ偏差の高しきい値	NVMe の中高間の変化点となる値を指定します。	5
SAN テレメトリトレーニングのタイムフレーム	フロー ECT ベースラインのトレーニングタイムフレームを指定します。	7 日
SAN テレメトリトレーニングのリセットタイムフレーム	日数後に ECT ベースライントレーニングを定期的に再開する期間を指定します。	14 日
SAN テレメトリ保持ポリシー：ベースライン/後処理	保持ポリシー（ベースライン/後処理）を指定します。	14

フィールド名	説明	デフォルト値
SAN テレメトリ保持ポリシー：時間ごとのロールアップ	保持ポリシーを指定します：時間ごとのロールアップ	90
テレメトリギャップリセット間隔	レコード間の最大有効時間ギャップを指定します（ドロップ前）。時間は秒単位です	750
アクティブな異常キャプチャ	ポストプロセッサごとにアクティブに追跡される異常の最大数を指定します。	500
ベースライントレーニングには NOOP フレームが含まれます	ベースライン学習が noop フレームを参照する必要があるかどうかを指定します。	未選択
ベースライントレーニングには負の偏差が含まれます	ベースライン偏差に負の偏差を含めるかどうかを指定します。	オン
テレメトリギャップリセット間隔を使用する	レコード間の時間ギャップに基づいて使用テレメトリリセットを指定します	オン

次の表では、SAN コントローラのインストールのシステム要件について説明します。

表 5: SAN Insights を使用する SAN コントローラに必要なシステムメモリ

ノードタイプ	vCPU の数	メモリ	ストレージ
仮想データノード	32	128 GB	3 TB SSD
物理データノード	40	256 GB	4*2.2 TB HDD、370G SSD、1.5 TB NVMe

表 6: SAN Insights 展開の検証済み制限

展開タイプ	検証済み制限 ^{1,2}
Cisco Virtual Nexus Dashboard (1 ノード)	80K ITLs/ITNs
Cisco Physical Nexus Dashboard (1 ノード)	120K ITLs/ITNs
Cisco Virtual Nexus Dashboard (3 ノード)	150K ITLs/ITNs
Cisco Physical Nexus Dashboard (3 ノード)	250K ITLs/ITNs

¹ Initiator-Target-LUNs (ITLs)

² Initiator-Target-Namespace ID (ITNs)

SAN Insights の設定

SAN コントローラリリース 12.0.1a から、ファブリックウィンドウでの構成とは別に、トポロジウィンドウで SAN ファブリックを構成できます。

トポロジウィンドウで、SAN ファブリックを右クリックし、**[SAN Insights の構成 (Configure SAN Insights)]** を選択し、手順に従って構成します。

SAN Controller Web UI で SAN Insights を構成するには、次の手順を実行します。

Before you begin

SAN Insights を構成する前に、永続的な IP アドレスを構成していることを確認してください。[永続的な IP アドレスの設定](#)を参照してください。

SAN コントローラの SAN Insights 機能が有効になっていることを確認します。**[設定 (Settings)]** > **[機能管理 (Feature Management)]** を選択し、**[SAN Insights]** チェックボックスをオンにします。



Note 十分なシステム要件と IP アドレスで構成する必要があります。スケール制限の詳細については、[SAN Insights のサーバープロパティ](#)で、SAN 展開に必要なシステムメモリの表を参照してください。

Procedure

- ステップ 1** **[SAN]** > **[ファブリック (Fabrics)]** を選択します。
- ステップ 2** 必要なファブリックを選択し、**[アクション (Actions)]** > **[SAN Insights の設定 (Configure SAN Insights)]** をクリックします。
- [SAN Insights の設定 (SAN Insights Configuration)]** ウィザードが表示されます。

ステップ 3 [SAN Insights の設定 (SAN Insights Configuration)] ウィザードで、[次へ (Next)] をクリックします。

[スイッチの設定 (Switches Configuration)] ウィザードが表示されます。

ステップ 4 以下に示すようにドロップダウンリストから適切な値を選択した後、SAN Insights 分析とテレメトリストリーミングを構成する必要があるスイッチを選択します。

Switch Name	Fabric Name	Model	Release	Licensed	Switch Time	Subscriptions	Install Query	Interv...	Receiver
MDS9132T-174139	MONTREAL_DC-174146	DS-C9132T-K9	8.4(2)	Yes	9/14/2021, 12:56:36 PM	None	Host	30	172.25.174.252
MDS9706-174146	MONTREAL_DC-174146	DS-C9706	9.2(1)	Yes	9/14/2021, 12:56:42 PM	SCSI & NVMe	Storage	30	172.25.174.252

スイッチに SAN Insights ライセンスがない場合、[ライセンス済み (Licensed)] 列のステータスは [いいえ (インストールライセンス) (No (install licenses))] と表示されます。[ライセンスのインストール (Install licenses)] をクリックして、ライセンスをスイッチに適用します。

Note SAN コントローラの時間はこの UI に表示され、スイッチ時間が SAN コントローラの時間とずれていることがわかった場合、スイッチ時間は赤でマークされます。

最後の列で選択された SAN コントローラ受信者の場合、受信者はテレメトリをサブスクライブできます：SCSI のみ、NVMe のみ、SCSI と NVMe の両方、またはなし。これにより、SCSI テレメトリを受信するように 1 つの SAN コントローラサーバーを設定し、NVMe テレメトリを受信するように別の SAN コントローラサーバーを設定できます。

SAN コントローラの展開では、eth0 または eth1 に割り当てられた IP アドレスを使用して、スイッチからの SAN Insights ストリーミングを受信できます。ただし、それぞれのスイッチからの IP 到達可能性を持つ SAN コントローラインターフェイスにストリーミングが設定されていることを確認します。[受信者 (Receiver)] 列には、検出されたすべてのインターフェイスが一覧表示されます。スイッチから分析データをストリーミングするための SAN コントローラのインストール中に設定された、対応するインターフェイス IP アドレスを選択します。

SAN コントローラをブートストラップするためのファブリックアクセスに管理 IP eth0 とデータ IP eth1 を提供できます。したがって、ストリーミングは、データ IP サブネットに割り当てられた永続的な IP に設定する必要があります。詳細については、[永続的な IP アドレスの設定](#) セクションを参照してください。

NDFC を仮想 Nexus Dashboard (vND) インスタンス上で実行するには、外部サービス IP アドレスが指定されている Nexus Dashboard インターフェイスに関連付けられているポートグループで無差別モードを有効にする必要があります。vND は、Nexus Dashboard 管理インターフェイスとデータインターフェイスで構成されています。デフォルトでは、LAN 展開では、Nexus Dashboard 管理インターフェイスサブネットに 2 つの外部サービス IP アドレスが必要です。したがって、関連付けられたポートグループの無差別モードを有効にする必要があります。インバンド管理またはエンドポイントロケータ (EPL) が有効になっている場合は、Nexus Dashboard データインターフェイスサブネットでも外部サービス IP アドレスを指定する必要があります。また、Nexus ダッシュボードデータ/ファブリック インターフェイス ポートグループの無差別モードを有効にする必要があります。NDFC SAN コントローラの場合、無差別モードは、ポートグループに関連付けられた Nexus Dashboard データインターフェイスでのみ有効にする必要があります。NDFC SAN コントローラの場合、無差別モードは、ポートグループに関連付けられた Nexus Dashboard データインターフェイスでのみ有効にする必要があります。詳細については、[Cisco Nexus ダッシュボード導入ガイド](#)を参照してください。

同じポートグループで複数の永続的な IP に到達できるように無差別モードを設定するには。詳細については、『*Nexus Dashboard User Guide*』の「*Cluster Configuration*」の項を参照してください。

[サブスクリプション (Subscription)] 列では、受信者がサブスクライブするプロトコルを指定できます。ドロップダウンリストから、SCSI、NVMe、両方、またはなしから選択できます。

Note [サブスクリプション (Subscription)] で [なし (None)] を選択すると、続行する前に適切なサブスクリプションを選択するよう警告メッセージが表示されます。サブスクリプションに必要なプロトコルを選択します。

[スイッチ名 (Switch Name)] 列の [i] アイコンをクリックして、スイッチから分析およびテレメトリ機能の設定の詳細を取得できます (分析クエリおよびテレメトリ機能が構成されている場合)。

```

Show Telemetry Transport
-----
Session Id      IP Address      Port      Encoding      Transport      Status
-----
1               172.25.174.178  33000     GPB-compact   gRPC           Connected
0               172.25.174.244  33000     GPB-compact   gRPC           Connected
3               172.25.174.252  33000     GPB-compact   gRPC           Connected
-----

Retry buffer Size:          10485760
Event Retry Messages (Bytes): 0
Timer Retry Messages (Bytes): 0
Total Retries sent:        0
Total Retries Dropped:     0
  
```

Cancel

いずれかのタイプ (dcnminitITL、dcnmtgtITL、dcnmislpclITL、dcnminitITN、dcnmtgtITN、または dcnmislpclITN) の分析クエリがスイッチで設定されていない場合、テレメトリの設定は表示されません。

Note クラスタモードの例に複数の受信者がいる場合は、受信者の横にあるドロップダウンアイコンをクリックして、必要なレシーバーを選択します。

ステップ 5 [次へ (Next)]をクリックします。ストリーミング分析が可能なスイッチは、[スイッチの選択 (Select Switches)]ページに一覧表示されます。

ステップ 6 SAN Insights を設定する必要があるスイッチを選択します。

Note [スイッチの選択 (Select Switches)]ページに移動すると、SAN コントローラとスイッチの両方の時間が記録され、表示されます。これは、SAN コントローラとスイッチのクロックが同期していることを確認するのに役立ちます。

単一または複数のスイッチを選択し、[アクション (Actions)]>[分析を無効にする (Disable Analytics)]の順にクリックして、選択したスイッチのすべての分析およびテレメトリの設定をクリアします。

SAN Insights のコンパクトな GPB ストリーミングの設定がサポートされています。コンパクト GPB を使用してストリーミングするには、アップグレード後に新たに SAN Insights を設定する前に、古い KVGPB ストリーミングを無効にして削除する必要があります。

[クエリのインストール (Install Query)]列に、スイッチごとのポートのタイプが表示されます。ポートタイプは、[ISL]、[ホスト (host)]、または[ストレージ (storage)]です。

- [ホスト (host)]: スイッチ上でホストまたはイニシエータが接続されているすべてのポートを一覧表示します。
- [ストレージ (storage)]: スイッチ上でストレージまたはターゲットが接続されているすべてのポートを一覧表示します。
- [ISL]: スイッチ上のすべての ISL およびポートチャネル ISL ポートを一覧表示します。
- [なし (None)]: クエリがインストールされていないことを示します。

次のクエリが使用されます。

- dcnmtgtITL/dcnmtgtITN : これはストレージのみのクエリです。
- dcnminittITL/dcnminittITN : これはホストのみのクエリです。
- dcnmislpcITL/dcnmislpcITN : これは ISL および pc-member のクエリです。

Note ストレージに接続されているスイッチ (ストレージエッジスイッチ) に ISL クエリインストールタイプを使用する場合は、ISL ベースのクエリを追加する必要があります。

Note SAN コントローラは、重複した ITLs/ITNs を管理しません。ホストクエリとストレージクエリの両方を (ホストとストレージがそれぞれ接続されているスイッチで) 設定すると、データは同じ ITL/ITN に対して複製されます。これにより、計算されたメトリックに矛盾が生じます。

管理者が構成ウィザードで ISL\Host\Storage を選択すると、それぞれのポートがフィルタ処理され、次の手順で一覧表示されます。

ステップ 7 [次へ (Next)]をクリックします。

前のビューで選択したスイッチで分析がサポートされているすべてのモジュールが表示され、最後の列にそれぞれの瞬間的な NPU 負荷が表示されます。このステップでは、モジュールのポートサンプリング構成 (オプション) とポートサンプリングのローテーション間隔を指定できます。スイッチのデフォルト設定では、分析のためにスイッチ上のすべての分析対応ポートをモニタリングします。

Note ISL クエリがインストールされている複数の ISL ポートでポートサンプリングが有効になっている場合、メトリックの集計は正確ではありません。すべての交換が同時に利用できるわけではないため、メトリックの集計は正確ではありません。複数の ISL がある ISL クエリでは、ポートサンプリングを使用しないことをお勧めします。

ステップ 8 [モジュール設定 (Module Configuration)]タブで、SAN Insights 機能のモジュールを設定します。

リリース 12.1.1e 以降、Cisco NDFC は 64G モジュールの検出をサポートし、SAN Insights の設定中に選択できます。これらのモジュールではポートサンプリングがサポートされておらず、NPU ロードは 64G SAN 分析には適用されません。したがって、64G モジュールのサンプルウィンドウとローテーション間隔を設定することはできません。

Switch Name	Fabric Name	Module	Slot	Description	Ports	Sample Window (ports)	Rotation Interval (s)	NPU Load %
MDS9700-206	Fabric_Hindon	DS-X9648-1536K9	1	4/8/16/32 Gbps Advanced FC Module	48	4	30	0
MDS9700-206	Fabric_Hindon	DS-X9748-3072K9	2	8/16/32/64 Gbps Advanced FC Module	48	Not supported	Not supported	Not supported
MDS9700-206	Fabric_Hindon	DS-X9648-1536K9	5	4/8/16/32 Gbps Advanced FC Module	48	12	30	7

[サンプルウィンドウ (ポート) (Sample Window (ports))]および[ローテーション間隔 (秒) (Rotation Interval (seconds))]の値を変更するには、行をクリックして必要な値を入力します。

- 変更を破棄するには、[キャンセル (Cancel)]をクリックします。
- 変更を保存するには、[保存 (Save)]をクリックします。

[NPU ロード (NPU Load)]列には、モジュール内のネットワーク処理ユニット (NPU) が表示されます。

ステップ 9 [次へ (Next)]をクリックします。

ステップ 10 [インターフェイスの選択 (Interface Selection)]タブで、ファブリック内で分析データを生成するインターフェイスを選択します。

Choose the switch interfaces that will generate analytics data

Filter by attributes

Switch Name	Fabric Name	Module	S...	Interf...	Connected To	Type	SCSI Metrics	NVMe Metrics	Pending Change
MDS9706-174146	MONTREAL_DC-174146	DS-X9648-1536K9	1	fc1/30	SCSI_SCALE_TARG2	storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MDS9706-174146	MONTREAL_DC-174146	DS-X9648-1536K9	1	fc1/4	SBT11_NVMe_TARG_02	storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MDS9706-174146	MONTREAL_DC-174146	DS-X9648-1536K9	6	fc6/4	20:01:00:11:0d:e5:fb:00	storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MDS9706-174146	MONTREAL_DC-174146	DS-X9648-1536K9	6	fc6/18	IBM_F9100_P1	storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MDS9706-174146	MONTREAL_DC-174146	DS-X9648-1536K9	6	fc6/17	IBM_DS8870_P1	storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

10 Rows Page 1 of 1 1-5 of 5

Previous Next

インターフェイスごとに、メトリックを有効化または無効化できます。[SCSI メトリックと NVMe メトリック (SCSI Metrics and NVMe Metrics)] 列のチェックボックスを選択して、目的のポートでの分析を有効または無効にします。

ステップ 11 [次へ (Next)] をクリックし、行った変更を確認します。

Review and enable SAN Insights

Filter by attributes

Switch Name	Fabric Name	Ta... Ty...	Task	Status
MDS9706-174146	MONTREAL_DC-174146	Switch	Install query and configure telemetry. Copy r s. Query: Storage, Receiver: 172.25.174.252, Subscriptions: all, interval:30	

10 Rows Page 1 of 1 1-1 of 1

Previous Commit

ステップ 12 [確定する (Commit)] をクリックします。CLI はスイッチで実行されます。

ステップ 13 結果を確認し、応答が成功したことを確認します。

Note 一部の SAN Insights ウィンドウでは、データが表示されるまでに最大 2 時間かかる場合があります。

ステップ 14 [閉じる (Close)] をクリックして、ホームページに戻ります。

[閉じる (Close)] アイコンは、スイッチですべての CLI コマンドが実行された後にのみ表示されます。

再度 [SAN]>[ファブリック (Fabrics)] または [トポロジ (topology)] ページに移動して、SAN Insights の設定を変更します。

ファブリックバックアップの構成

選択したファブリックのバックアップを [ファブリック (Fabric)] ウィンドウから設定できます。同様に、[ファブリックの概要 (Fabric Overview)] ウィンドウでバックアップを設定できます。メインウィンドウで [ファブリックの概要 (Fabric Overview)] > [アクション (Actions)] を選択し、[バックアップの構成 (Configure Backup)] をクリックします。

すべてのファブリック設定とインテントを自動または手動でバックアップできます。インテントである SAN コントローラの設定を保存できます。インテントは、スイッチにプッシュされる場合とされない場合があります。

SAN コントローラは、次のファブリックをバックアップしません。

- モニタ専用モードの外部ファブリック：モニタ専用モードの外部ファブリックのバックアップを作成できますが、復元はできません。外部ファブリックがモニタ専用モードでない場合は、このバックアップを復元できます。
- 親 MSD ファブリック：MSD ファブリックのバックアップを作成できます。親ファブリックからバックアップを開始すると、バックアッププロセスはメンバーファブリックにも適用されます。ただし、SAN コントローラは、メンバーファブリックと MSD ファブリックのすべてのバックアップ情報を 1 つのディレクトリにまとめて保存します。

バックアップされた構成ファイルは、ファブリック名を持つ対応するディレクトリにあります。ファブリックの各バックアップは、手動または自動のどちらでバックアップされたかに関係なく、異なるバージョンとして扱われます。バックアップのすべてのバージョンは、対応するファブリックディレクトリにあります。

ファブリック設定およびインテントのスケジュールバックアップを有効にできます。

バックアップには、ファブリック上の使用済みリソースに関するリソースマネージャの状態に加えて、インテントとファブリック設定に関連する情報が含まれます。SAN コントローラは、設定プッシュがある場合にのみバックアップされます。SAN コントローラは、最後の設定プッシュ後に手動バックアップをトリガーしなかった場合にのみ、自動バックアップをトリガーします。

ゴールデンバックアップ

アーカイブの制限に達した後でも、削除しないバックアップにマークを付けることができます。これらのバックアップはゴールデンバックアップです。ファブリックのゴールデンバックアップは削除できません。ただし、SAN コントローラは、最大 10 個のゴールデンバックアップのみをアーカイブします。ファブリックの復元中に、バックアップをゴールデンバックアップとしてマークできます。バックアップをゴールデンバックアップとしてマークするには、Web UI から次の手順を実行します。

手順

ステップ 1 ファブリックを選択し、**[Fabrics] > [Fabric Overview] > [Backup]** の順に選択します。

[バックアップ (Backup)] タブが表示されます。

ステップ 2 メイン ウィンドウで、**[アクション (Actions)] > [バックアップの構成 (Configure Backup)]** を選択します。

[スケジュールされたアーカイブ (Scheduled Archive)] ウィンドウが表示されます。

ステップ 3 バックアップを選択する期間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y** および **All** です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報 (1 ヶ月) が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 バックアップをクリックして、ゴールデンとしてマークするバックアップを選択します。

自動または手動バックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの概要 (Fabric Overview)]** ウィンドウの **[バックアップ (Backup)]** タブから開始します。手動バックアップを開始するには、**[バックアップ (Backup)]** タブの **[アクション (Actions)]** ペインで **[今すぐバックアップ (Backup Now)]** をクリックします。

ステップ 5 スイッチウィンドウに移動し、必要なスイッチ名のチェックボックスを選択し、**[スイッチ (Switch)] > [スイッチの概要 (Switch Overview)] > [バックアップ (Backup)] > [アクション (Backup Actions)]** を選択して、**> [ゴールデンバックアップとしてマーク (Mark as golden backup)]** を選択します。

確認用のダイアログボックスが表示されます。

ステップ 6 [はい (Yes)] をクリックします。

ステップ 7 「ファブリックの復元」の項に記載されている残りのファブリック復元手順を続行するか、ウィンドウを終了します。

ファブリックの概要

ファブリック レベルの [アクション (Actions)] ドロップダウンリストでは、バックアップを設定できます。詳細については、[ファブリック バックアップの構成 \(56 ページ\)](#) を参照してください。

[ファブリックの概要 (Fabric Overview)] には、ファブリックで次の操作を表示および実行できるタブがあります。

ファブリック サマリ

[ファブリック (Fabric)] をクリックして、サイドキック パネルを開きます。次のセクションでは、ファブリックの概要を表示します。

ヘルス：ファブリックのヘルスを示します。

アラーム：カテゴリに基づいてアラームを表示します。

ファブリック情報：このセクションでは、ファブリックに関する基本情報を提供します。

インベントリ：このセクションでは、スイッチの設定とスイッチの状態に関する情報を提供します。

右上隅にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。

スイッチ

次の表で、[スイッチ (Switches)] ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
[IPアドレス (IP Address)]	スイッチの IP アドレスを指定します。
Fabric Name (ファブリック名)	スイッチに関連付けられているファブリック名を指定します。
ステータス	スイッチのステータスを指定します。

フィールド	説明
ヘルス (Health)	スイッチの正常性ステータスを指定します。正常性ステータスは次のとおりです。 <ul style="list-style-type: none"> • 正常 • 深刻 • 警告 • OK
Ports	スイッチのポートの合計数を指定します。
使用済みポート	スイッチで使用されるポートの合計数を指定します。
モデル	スイッチ モデルを指定します。
シリアル番号 (Serial Number)	スイッチのシリアル番号を指定します。
リリース	スイッチのリリース番号を指定します。
稼働時間	スイッチアップ時間の詳細を指定します。

次の表に、[アクション (Actions)]メニューのドロップダウンリストで、[LAN]>[スイッチ (Switch)]>[スイッチ (Switch)]に表示されるアクションメニューを示します。

アクション項目	説明
Device Manager	必要なスイッチのデバイスマネージャにログインできます。[デバイスマネージャ (Device Manager)]ログインウィンドウが表示され、ログイン情報を入力してログインします。 Cisco MDS 9000 デバイスマネージャの説明と使用方法については、 デバイスマネージャ (319 ページ) を参照してください。
テクニカル サポート	ログの収集を開始できます。詳細については、 テクニカル サポート (88 ページ) を参照してください。
CLI の実行	複数のスイッチで複数の CLI コマンドを実行し、各スイッチの出力を zip 形式のテキストファイルとして収集できます。詳細については、 CLI の実行 (89 ページ) を参照してください。

モジュール

SAN コントローラ Web UI からモジュールのインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 [SAN]、[スイッチ (Switch)]、[スイッチの概要 (Switch Overview)]、[モジュール (Modules)] の順に選択します。同様に、ファブリックの概要ウィンドウで、[SAN] > [ファブリック (Fabric)] > [ファブリックの概要 (Fabric Overview)] > [Modules] の順に表示できます。

[モジュール (Modules)] タブに、選択した範囲のすべてのスイッチとその詳細のリストが表示されます。

テーブルに必要な情報を表示し、[属性によるフィルタ (Filter by Attributes)] に詳細を入力できます。

ステップ 2 次の情報が表示されます。

- [名前 (Name)] にはモジュール名が表示されます。
- [モデル (Model)] にモデル名が表示されます。
- [シリアル番号 (Serial Number)] 列には、シリアル番号が表示されます。
- [タイプ (Type)] 列には、モジュールのタイプが表示されます。
- **Oper. Status** 列には、デバイスの動作状態が表示されます。
- [スロット (Slot)] 列には、スロット番号が表示されます。
- [ハードウェア リビジョン (HW Revision)] 列には、モジュールのハードウェアバージョンが表示されます。
- [ソフトウェア リビジョン (Software Revision)] 列には、モジュールのソフトウェアバージョンが表示されます。
- [アセット ID (Asset ID)] カラムには、モジュールのアセット ID が表示されます。

インターフェイスの表示

UI Path: SAN > スイッチ > スイッチの概要 > インターフェイス

同様に、ファブリック概要ウィンドウでインターフェイスを表示できます。

SAN > ファブリック > ファブリックの概要 > インターフェイス

次の表では、[インターフェイス (Interfaces)] タブに表示されるフィールドについて説明します。

フィールド	説明
名前	インターフェイス名を指定します。
Admin. ステータス	インターフェイスの管理ステータスを指定します。
Oper. ステータス	インターフェイスの動作ステータスを指定します。
理由	失敗の理由を指定します。
スピード	Gb でインターフェイスの速度を指定します。
モード	インターフェイスのモードを指定します。
スイッチ	スイッチの名前を示します。
VSAN	接続された VSAN の名前を指定します。
接続先	接続の詳細を指定します。
接続先のタイプ	接続のタイプを指定します。
説明	インターフェイスの詳細を指定します。
オーナー	ポートの所有者を指定します。
[ポートグループ (Port Group)]	インターフェイスが接続されているポートグループ番号を指定します。

インベントリタブでさまざまな操作を実行するには、次の手順に従います。

手順

- ステップ 1** インターフェイスに対してシャットダウンを実行しない場合は、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[シャットダウンな (No Shutdown)] をクリックします。

警告ウィンドウが表示されたら、[確認 (Confirm)] をクリックします。
- ステップ 2** インターフェイスをシャットダウンするには、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[シャットダウン (Shutdown)] をクリックします。

警告ウィンドウが表示されたら、[確認 (Confirm)] をクリックします。
- ステップ 3** インターフェイスのポート所有者を割り当てるには、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[所有者 (Owner)] をクリックします。
- ステップ 4** [ポート所有者の設定 (Set Port Owner)] ウィンドウが表示され、必要な名前を入力して [適用 (Apply)] をクリックします。

- ステップ 5** インターフェイスの診断をリンクするには、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)] > [リンク診断 (Link Diagnostics)] をクリックします。

VSAN

Cisco Nexus ダッシュボード ファブリック コントローラ の仮想 SAN (VSAN) を構成および管理できます。メニューから、[仮想的な管理 (Virtual Management)] > [VSANS] を選択して、VSAN 情報を表示します。検出されたファブリックの VSAN を、[管理可能 (Manageable)] または [継続的に管理 (Manage Continuously)] ステータスで表示または設定できます。選択したファブリックでは、VSAN スコープツリーが左側のパネルに表示されます。

Cisco データセンタースイッチおよび Cisco MDS 9000 シリーズスイッチで仮想 SAN (VSAN) を使用すると、ファイバチャネル ファブリックでより高度なセキュリティと高い安定性を得ることができます。VSAN は同じファブリックに物理的に接続されたデバイスを分離します。VSAN では、一般の物理インフラストラクチャで複数の論理 SAN を作成できます。各 VSAN には最大 239 台のスイッチを組み込みます。それぞれの VSAN は、異なる VSAN で同じファイバチャネル ID (FC ID) を同時に使用できる独立したアドレス領域を持ちます。



- (注) Cisco Nexus ダッシュボード ファブリック コントローラ は、一時停止された VSAN を検出せず、表示もしません。

[VSANS] タブには次のフィールドが表示されます。

フィールド	説明
VSAN 名	<p>VSAN 名を表示します。</p> <p>選択した VSAN の範囲に関連付けられている情報が右側のパネルに表示されます。VSAN がセグメント化されている場合、セグメント化された個々の VSAN はそれぞれ VSAN の範囲です。選択したすべての VSAN の範囲について、タブに情報を表示できます。</p> <ul style="list-style-type: none"> • [Switches] タブ • [ISLs] タブ • [ホストポート] タブ • [ストレージポート] タブ • [属性 (Attributes)] タブ • [ドメイン ID] タブ • [VSAN メンバーシップ] タブ

フィールド	説明
VSAN ID	VSAN ID を指定します。
セグメント	この VSAN のセグメントを指定します。 セグメントをクリックしてスライドインペインを開き、各セグメントに関する概要情報を表示します。
ステータス	VSAN が[アップ (Up)]か[ダウン (Down)]かを指定します。

次の表に、[アクション (Actions)]メニューのドロップダウンリストで、[ファブリックの概要 (Fabric Overview)]>[VSANs]に表示されるアクション項目を示します。

アクション項目	説明
VSAN を作成します。	ウィザードを起動して VSAN を作成できます。詳細については、 VSAN の作成ウィザード (64 ページ) をクリックしてください。
VSLAN の削除	VSAN を選択し、[VSAN の削除 (Delete VSAN)]をクリックして VSAN を削除します。詳細については、 VSLAN の削除 (67 ページ) をクリックしてください。



- (注) Nexus ダッシュボード ファブリック コントローラ でスイッチポートの VSAN を変更すると、ポートが隔離された VSAN に関連付けられていた場合、前の VSAN 列は空白になります。

タブに表示されるすべてのフィールドの説明については、「[VSAN のフィールドと説明 \(68 ページ\)](#)」を参照してください。

このセクションは、次のトピックで構成されています。

デフォルトの VSAN 設定

次の表に、設定されたすべての VSAN のデフォルト設定を示します。

パラメータ	デフォルト
デフォルト VSAN	VSAN 1
状態	アクティブ状態

パラメータ	デフォルト
名前	VSAN と VSAN ID を表す 4 桁のストリングを連結したものです。たとえば、VSAN 3 は VSAN0003 です。
ロード バランシング属性	OX ID (src-dst-ox-id)

VSAN の作成ウィザード

VSAN 作成ウィザードのワークフローには次のものが含まれます。

- VSAN ID と名前を指定します。
- スイッチを選択します。
- VSAN 属性を指定します。
- VSAN ドメインを指定します。
- VSAN メンバーを指定します。

[仮想管理 (Virtual Management)] > [VSANS] を選択します。ドロップダウンリストからファブリックを選択したら、[新しい VSAN の作成 (Create New VSAN)] アイコンをクリックします。ウィザードのようこそ画面が表示されます。



(注) VSAN がまだ作成されていないことを確認します。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI を使用して VSAN を作成して設定するには、次の手順を実行します。

始める前に

VSAN を作成する前には、VSAN に対してアプリケーション特有のパラメータを設定できません。

VSAN がまだ作成されていないことを確認します。中断状態の VSAN を作成しないでください。



(注) 中断状態の VSAN は管理されません。

手順

ステップ 1 [VSAN ID と名前 (VSAN ID and Name)] ウィンドウで、次の手順を実行します。

- a) ファブリックが [ファブリック (Fabric)] フィールドに対して正しいことを確認します。
- b) [VSAN ID] フィールドで、ドロップダウンリストから VSAN ID を選択します。
範囲は 2 ~ 4094 です。ファブリック内の少なくとも 1 つのスイッチで VSAN ID のリストを作成します。VSAN 4079 は予約済み VSAN ID です。
- c) [VSAN 名前 (VSAN Name)] フィールドに、VSAN の名前を入力します。
(注) このフィールドが空白の場合、スイッチはデフォルトの名前を VSAN に割り当てます。
- d) [FICON] チェックボックスをオンにして、スイッチで FICON を有効にします。
- e) [次へ (Next)] をクリックします。

ステップ 2 [スイッチの選択 (Select Switches)] 画面で、[スイッチ名 (Switch Name)] の横にあるチェックボックスをオンにして、VSAN を作成します。

スイッチ名がグレー表示されている場合は、そのスイッチがすでに VSAN の一部であることを示しています。また、前の手順で FICON がオンにされている場合、スイッチで FICON 機能が有効になっていないことを意味する場合があります。

[次へ (Next)] をクリックします。

ステップ 3 [VSAN 属性の設定 (Configure VSAN Attributes)] 画面で、VSAN 属性を設定します。

(注) 中断状態の VSAN を作成した場合、中断状態の VSAN は管理されないため、Cisco Nexus ダッシュボード ファブリック コントローラ には表示されません。

- a) [ロードバランシング (Load Balancing)] で、VSAN で使用するロードバランシングタイプを選択します。

次のタイプを使用できます。

- Src ID/Dest ID : 送信元 ID (Src_ID) と接続先 ID (Dest_ID) のみに基づいています。
- Src ID/Dest ID/Ox ID (デフォルト) : Src_ID および Dest_ID に加えて、発信元交換 ID (Ox_ID) もロードバランシングに使用されます。Ox_ID は、ターゲットインターコネクトポートとの交換のために発信元インターコネクトポートによって割り当てられた交換 ID です。

(注) Src ID/Dest ID/Ox ID は非 FICON VSAN のデフォルトのロードバランシングタイプであり、FICON VSAN では使用できません。Src ID/Dest ID は FICON VSAN のデフォルトです。

- b) [相互運用性 (InterOp)] で、相互運用性の値を選択します。

相互運用性の値は、異なるベンダーのデバイスと相互運用するために使用されます。次のいずれかを選択できます。

- デフォルト : 相互運用性が無効であることを意味します。
- InterOp-1 : VSAN がすべてのファイバチャネルベンダーデバイスと相互運用できることを意味します。

- **InterOp-2** : VSAN が基本的な機能から高度な機能まで、特定のファイバチャネルベンダー デバイスと相互運用できることを意味します。
- **InterOp-3** : VSAN が基本的な機能から高度な機能まで、特定のファイバチャネルベンダー デバイスと相互運用できることを意味します。
- **InterOp-4** : VSAN が基本的な機能から高度な機能まで、特定のファイバチャネルベンダー デバイスと相互運用できることを意味します。

(注) 相互運用性は FICON VSAN ではサポートされていません。

c) [管理状態 (Admin State)] で、この VSAN の設定可能な状態を選択します。

- **アクティブ** : VSAN が設定され、この VSAN のサービスがアクティブであることを意味します。
- **一時停止** : VSAN は設定されていますが、この VSAN のサービスは非アクティブ化されていることを意味します。

ファブリック全体のすべての VSAN パラメータを事前設定するには、この状態を選択します。

(注) Nexus ダッシュボード ファブリック コントローラ は一時停止された VSAN を管理しないため、VSAN 範囲には表示されません。

d) 順序どおりの配信を許可するには、[順序どおりの配信 (InOrder delivery)] チェック ボックスをオンにします。

fcInorderDelivery の値が変更されると、このオブジェクトの値はそのオブジェクトの新しい値に設定されます。

e) FICON VSAN のファブリックバインドを有効にする場合は、[ファブリックバインド DB の追加 (Add Fabric Binding DB)] チェックボックスをオンにします。

このチェックボックスをオンにすると、選択したスイッチのすべてのピアが、選択したリストの各スイッチに追加されます。

f) FICON VSAN のすべてのポートを禁止する場合は、[すべてのポートを禁止 (All Port Prohibited)] チェックボックスをオンにします。

チェックボックスが選択されている場合、FICON VSAN は、デフォルトですべてのポートが禁止されているものとして作成されます。

g) [次へ (Next)] をクリックします。

ステップ 4 [VSAN ドメインの設定 (Configure VSAN Domain)] 画面で、FICON VSAN の静的ドメイン ID を設定します。

- a) [静的ドメイン ID を使用する (Use Static Domain IDs)] チェックボックスをオンにして、VSAN 内のスイッチのドメイン ID を設定します。
- b) [使用可能なドメイン ID (Available Domain IDs)] フィールドには、ファブリックで使用可能なすべてのドメイン ID が表示されます。

[使用可能なドメイン ID を自動的に適用 (Automatically apply available domain IDs)] をクリックして、VSAN の一部として選択されたすべてのスイッチにドメイン ID を割り当てます。

- c) テーブル内のすべてのスイッチについて、使用可能なドメイン ID のリストからドメイン ID を入力します。
- d) [次へ (Next)] をクリックします。

ステップ 5 [ポートメンバーシップの設定 (Configure Port Membership)] 画面で、VSAN 内のすべてのスイッチについて、インターフェイスを新しい VSAN のメンバーとして設定します。

(注) ポート VSAN を変更すると、インターフェイスの I/O に影響する場合があります。

[次へ (Next)] をクリックします。

ステップ 6 [レビュー (Review)] 画面で、VSAN が正しく設定されているかどうかを確認します。

[前へ (Previous)] をクリックして前の画面に移動し、設定を変更します。

[完了 (Finish)] をクリックして確認し、VSAN を設定します。ウィンドウ下部に VSAN の作成結果が表示されます。

(注) VSAN の作成後、新しい VSAN が VSAN 範囲ツリーに表示されるまで数分かかります。

(注) スイッチポートが隔離された VSAN に関連付けられている場合、以前の VSAN 情報は空白になります。

VSLAN の削除

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI から VSAN とその属性を削除するには、次の手順を実行します。

手順

ステップ 1 [仮想管理 (Virtual Management)] > [VSANS] を選択します。

[VSANS] ウィンドウが表示されます。

ステップ 2 [ファブリックの選択] ドロップダウンリストから、VSAN が関連付けられているファブリックを選択します。

選択したファブリックの VSAN スコープツリーが VSANS エリアに表示されます。

ステップ 3 ファブリックを展開し、VSAN の横にある削除アイコンをクリックします。

[VSAN の削除] 画面が表示され、VSAN に関連付けられたスイッチが表示されます。

(注) セグメント化された VSAN は削除できません。

ステップ 4 VSAN を削除するスイッチのチェックボックスを選択します。

[VSANの削除 (Delete VSAN)] をクリックします。

確認ウィンドウが表示されます。

ステップ 5 削除を確認する場合は **[確認 (Confirm)]** をクリックするか、**[キャンセル (Cancel)]** をクリックして VSAN を削除しないでダイアログボックスを閉じます。

(注) VSAN が削除された後、新しい VSAN が VSAN スコープツリーから消えるまで数分かかります。

VSAN のフィールドと説明

[仮想管理 (Virtual Management)] > [VSANS] に表示されるすべてのタブのフィールドと説明は、次の表で説明されています。

[Switches] タブ

このタブには、VSAN スコープのスイッチが表示されます。スイッチ名をクリックして、スイッチの概要情報を表示します。次の表では、[スイッチ] タブに表示されるフィールドについて説明します。

表 7: [スイッチ] タブのフィールドと説明

フィールド	説明
名前	VSAN のスイッチの名前を指定します。 名前をクリックして、スイッチの概要を表示します。 詳細を表示するには、 [詳細の表示 (View Details)] をクリックしてください。
ドメイン ID	永続的なドメイン ID を指定します。
VSAN WWN	VSAN の World Wide Name (WWN) を指定します。
プリンシパル WWN	スイッチの World Wide Name (WWN) を指定します。 (注) 主要スイッチの場合、値は <i>self</i> です。
モデル	スイッチのモデル名を指定します。
リリース	スイッチの NX-OS バージョンを指定します。
稼働時間	スイッチが起動する時間を指定します。

[ISLs] タブ

このタブには、VSAN スコープ内のスイッチに関する ISL の情報が表示されます。次の表では、ISL タブに表示されるフィールドについて説明します。VSAN が ISL 全体の両方のスイッチで設定されていて、VSAN が ISL で有効になっていない場合、Nexus ダッシュボード ファブリック コントローラ では、VSAN はセグメント化されていると見なされます。したがって、VSAN を ISL 全体のトランク VSAN に追加して、警告メッセージをクリアします。または、この警告メッセージを無視することもできます。

表 8: [ISL] タブのフィールドと説明

フィールド	説明
VSAN	この ISL がトラフィックを実行するすべての VSAN。
スイッチから	リンクのソーススイッチ。
送信元インターフェイス	リンクのソース E_port のポートインデックス。
スイッチに	リンクのもう一方の端にあるスイッチ。
インターフェイスへ	リンクの宛先 E_port のポートインデックス。
スピード	この ISL の速度。
ステータス	リンクの動作ステータス。
ポートチャンネルメンバー	ISL がポートチャンネルの場合は、ポートチャンネルのメンバー。
追加情報	TE/TF/TNP ISL など、この ISL に関する追加情報。

[ホストポート] タブ

このタブには、VSAN スコープ内のスイッチのホストポートに関する情報が表示されます。次の表では、[ホストポート] タブに表示されるフィールドについて説明します。

表 9: [ホストポート] タブのフィールドと説明

フィールド	説明
エンクロージャ	エンクロージャの名前
デバイスエイリアス	このエントリのデバイスエイリアス。
ポートWWN	このホストに割り当てられた PWWN。
Fcid	このホストに割り当てられた FC ID。
スイッチ インターフェイス	エンドデバイスに接続されているスイッチのインターフェイス。
リンクステータス	リンクの動作ステータス。

フィールド	説明
ベンダー	ベンダーの名前を指定します。
シリアル番号 (Serial Number)	エンクロージャのシリアル番号を指定します。
モデル	モデルの名前を指定します。
ファームウェア	この HBA によって実行されるファームウェアのバージョン。
要因	この HBA によって実行されるドライバのバージョン。
追加情報	この HBA に対応する情報一覧です。

【ストレージポート】タブ

このタブには、VSAN スコープ内のスイッチのストレージポートに関する情報が表示されます。次の表では、【ストレージポート】タブに表示されるフィールドについて説明します。

表 10:【ストレージポート】タブのフィールドと説明

フィールド	説明
エンクロージャ	エンクロージャの名前
デバイス エイリアス	このエントリのデバイスエイリアス。
ポートWWN	このホストに割り当てられた PWWN。
Fcid	このホストに割り当てられた FC ID。
スイッチ インターフェイス	エンドデバイスに接続されているスイッチのインターフェイス。
リンクステータス	リンクの動作ステータス。

【属性 (Attributes)】タブ

このタブには、VSAN スコープ内のすべてのスイッチの属性が表示されます。次の表では、【属性】タブに表示されるフィールドについて説明します。

表 11: [属性] タブのフィールドと説明

フィールド	説明
編集	<p>[編集 (Edit)] をクリックして、VSAN の属性を変更し、同じ VSAN 属性を選択したスイッチにプッシュします。</p> <p>選択したいずれかのスイッチで VSAN が FICON VSAN の場合、次のフィールドは FICON VSAN では変更できないため、UI に表示されません。</p> <ul style="list-style-type: none"> • vsanLoadBalancing • 相互運用性 • 順序どおりの配信 <p>属性を変更したら、[保存 (Save)] をクリックして変更を保存するか、[キャンセル (Cancel)] をクリックして破棄します。</p>
スイッチ名	VSAN に関連付けられているスイッチの名前を表示します。
VSAN 名	VSAN の名前を表示します。
Admin	<p>Admin の状態がアクティブであるか一時停止であるかを指定します。</p> <ul style="list-style-type: none"> • [アクティブ (Active)] は、VSAN が設定され、VSAN のサービスがアクティブ化されていることを意味します。 • [ダウン (Down)] は、VSAN が設定されていることを意味します。ただし、VSAN のサービスは非アクティブ化されています。set this state を使用すると、CLI のみを使用して、すべての VSAN パラメータを事前設定できます。 <p>(注) VSAN を一時停止すると、Cisco Nexus ダッシュボード ファブリック コントローラ から削除されます。</p>
Oper	VSAN の動作状態。
MTU	スイッチの MTU を表示します。

フィールド	説明
ロード バランシング	VSAN で使用されるロードバランシングタイプを指定します。 VSAN で使用されるロードバランシングの種類です。 <ul style="list-style-type: none"> • srcId/DestId — パス選択にソース ID と接続先 ID を使用 • srcId/DestId/Oxid — ソース、接続先、交換 ID を使用
相互運用性	この VSAN のローカルスイッチの相互運用モード。 <ul style="list-style-type: none"> • デフォルト • 相互運用性 - 1 • 相互運用性 - 2 • 相互運用性 - 3
順序どおりの配信	デバイスの順序どおりの配信保証フラグ。true の場合、順序どおりの配信が保証されます。false の場合、保証されません。
FICON	VSAN が FICON 対応の場合は true。

[ドメイン ID] タブ

このタブには、VSAN ドメインとそのパラメータに関する情報が表示されます。次の表では、ドメイン ID タブのフィールドについて説明します。

表 12: [ドメイン ID] タブのフィールドと説明

フィールド	説明
編集	スイッチを選択し、[編集] アイコンをクリックして、選択したスイッチのドメイン ID 情報を変更します。
スイッチ名	VSAN のスイッチ名を指定します。 (注) NPV スイッチは、この列には表示されません。ただし、NPV スイッチはこの VSAN ファブリックに存在します。
状態	スイッチのステータスを指定します。
有効	ドメイン ID を有効にするか無効にするかを指定します。
Running	実行中のドメインを指定します。
設定	設定を指定します。

フィールド	説明
設定タイプ	ドメイン ID タイプの使用方法を [優先 (preferred)] または [静的 (static)] に指定します。
アイコン	
Total	テーブルの隣の番号は、このタブの下のエントリを指定します。
更新アイコン	更新アイコンをクリックしてエントリを更新します。

[VSAN メンバーシップ] タブ

このタブには、VSAN を形成するスイッチのインターフェイスに関する情報が表示されます。次の表では、[VSAN メンバーシップ] タブのフィールドについて説明します。

表 13: [VSAN メンバーシップ] タブのフィールドと説明

フィールド	説明
編集	<p>スイッチを選択し、[編集] アイコンをクリックして、選択した VSAN および選択したスイッチのポート VSAN メンバーシップを変更します。</p> <p>ポート VSAN メンバーシップは、FC (物理)、ポートチャネル、FCIP、iSCSI、VFC (スロット/ポート)、VFC (ID)、VFC チャネル、VFC FEX、および VFC ブレイクアウトを含むさまざまなタイプによって提供されます。PortChooser は、選択したスイッチに存在するすべてのインターフェイスを表示し、ユーザーが選択できるようにタイプごとに提供されます。</p> <p>(注) 動作中のトランキングポートまたはポートチャネルメンバーのポスト VSAN メンバーシップを変更すると、警告が表示されます。デバイスマネージャを使用して、トランキングインターフェイスの許可 VSAN リストを変更します。</p>
スイッチ名	スイッチの名前
インターフェイス	VSAN の FC ポート

デバイス エイリアス

デバイスエイリアスは、ポート WWN のわかりやすい名前です。デバイスエイリアス名は、ゾーン分割、QoS、ポートセキュリティなどの機能を設定するときに指定できます。デバイス

エイリアスアプリケーションは Cisco Fabric Services (CFS) インフラストラクチャを使用して、効率的なデータベースの管理およびファブリック全体への配布を実現します。

次の表では、[デバイスエイリアス (Device Aliases)] タブの下に表示されるフィールドについて説明します。

フィールド	説明
スイッチ	デバイスエイリアススイッチ名を表示します。
デバイスエイリアス	スイッチから取得したエイリアスを表示します。
pWWN	ポート WWN を表示します。

この項の内容は、次のとおりです。

デバイスエイリアスの設定

ファブリックテーブルから必要なファブリックをクリックすると、スライドインパネルが表示されます。[起動 (Launch)] アイコンをクリックして、[ファブリックの概要 (Fabric Overview)] ウィンドウを表示し、[デバイスエイリアス (Device Alias)] タブをクリックします。

デバイスエイリアス設定を実行する前に、CFS タブでステータスをチェックして、ステータスが [成功 (success)] であることを確認します。



- (注) SAN コントローラ Web UI からデバイスエイリアス設定を実行するには、ファブリックをデバイスエイリアス拡張モードとして設定する必要があります。

デバイスエイリアスを追加、編集、または削除するには、次の手順を実行します。

手順

- ステップ 1** デバイスエイリアスを追加する必要があるスイッチ列の横にあるチェックボックスをオンにします
- [アクション (Actions)] > [デバイスエイリアスの追加 (Add device alias)] をクリックします。
[デバイスエイリアスの追加 (Add device alias)] ウィンドウが表示されます。
プロビジョニングされたすべてのポート WWN がテーブルに入力されます。
 - [デバイスエイリアス (Device Alias)] フィールドにデバイスエイリアス名を入力して、選択した pWWN のデバイスエイリアスを作成することを示します。
 - [保存 (Save)] をクリックして、インラインエディタモードを終了します。
 - [適用 (Apply)] をクリックして、デバイスエイリアスをスイッチに割り当てます。

プロビジョニングされていないポート WWN を使用してデバイスエイリアスを作成することもできます。

- a) 事前プロビジョニングデバイスエイリアスの **[+]** アイコンをクリックして、インラインエディタモードで新しいテーブル行を作成します。
- b) **[pWWN]** フィールドに、プロビジョニングされていないポートの WWN と、新しいエイリアスのデバイスエイリアスを入力します。
- c) **[保存 (Save)]** をクリックして、インラインエディタモードを終了します。
- d) **[適用 (Apply)]** をクリックして、デバイスエイリアスと関連付けられた pWWN をスイッチに割り当てます。

(注) デバイスエイリアスをスイッチに適用する前に **[デバイスエイリアスの追加 (Add device alias)]** ウィンドウを閉じると、変更は破棄され、デバイスエイリアスは作成されません。

ステップ 2 デバイスエイリアスを編集するには、スイッチ列の横にあるチェックボックスをオンにしてから、**[アクション (Actions)]** > **[デバイスエイリアスの編集 (Edit device aliases)]** をクリックします。

(注) 複数のスイッチを選択して、デバイスエイリアスを編集できます。

[デバイスエイリアスの編集 (Edit device alias)] ウィンドウが表示されます。

選択したすべてのポート WWN がテーブルに入力されます。

- a) **[pWWN]** 列の横にある **[編集 (Edit)]** アイコンをクリックします。
- b) **[デバイスエイリアス (Device Alias)]** フィールドに必要なデバイスエイリアス名を入力し、**[チェックマーク (tick)]** アイコンをクリックして名前を保存します。
- c) 同じ手順を繰り返して、他のデバイスエイリアス名を編集します。
- d) **[適用 (Apply)]** をクリックして、編集したデバイスエイリアスをスイッチに保存します。

(注) デバイスエイリアスの名前を変更すると、デバイスエイリアスを編集するとトラフィックが中断され、ゾーンメンバータイプを確認するよう求める警告メッセージが表示されます。Cisco NX-OS リリースの場合：

- 7.x リリース : 7.3(0) リリースより前
- 6.x リリース : 6.2(15) リリースより前

- e) **[キャンセル (Cancel)]** をクリックして変更内容を破棄するか、または **[確認 (Confirm)]** をクリックして変更内容を保存します。

ステップ 3 デバイスエイリアスを削除する必要があるスイッチ列の横にあるチェックボックスをオンにします。

- a) **[アクション (Actions)]** > **[デバイスエイリアスの削除 (Delete device alias)]** をクリックします。

確認ウィンドウが表示されます。

(注) デバイスエイリアスを削除すると、トラフィックが中断する可能性があります。

b) **[はい (Yes)]** をクリックして、デバイスエイリアスを削除します。

ステップ 4 サービスプロファイルが添付されたエンドデバイスの場合、サービスプロファイル名が **[デバイスエイリアス (Device Alias)]** フィールドに入力されます。これにより、サービスプロファイル名をそれらのデバイスのデバイスエイリアス名として使用できます。

デバイスエイリアスの作成は、**[適用 (Apply)]** をクリックした後に CFS 自動コミットされます。**[CFS]** タブをクリックして、デバイスエイリアスの作成後に CFS が適切に実行されているかどうかを確認します。失敗した場合は、トラブルシューティングを行い、問題を修正する必要があります。

CFS

ファブリック内のすべての適格なスイッチの CFS 情報が一覧表示されます。デバイスエイリアス設定を実行する前に、**CFS** タブでステータスをチェックして、ステータスが **[成功 (success)]** であることを確認します。CFS が別のユーザーによってロックされている場合、または前の操作が失敗した場合は、CFS セッションがロック解除されていることを確認してください。

次の表では、**CFS** タブに表示される列について説明します。

フィールド	説明
スイッチ	スイッチの名前を示します。
機能	スイッチの機能を指定します。
直前のアクション	スイッチで最後に実行されたアクションを指定します。
結果	実行されたアクションが成功または失敗であることを指定します。
所有者スイッチのロック	スイッチがロックされているかどうかを指定します。
所有者ユーザーのロック	スイッチがロックされている場合のユーザーロール名を指定します。
結合ステータス	スイッチのマージステータスを指定します。

SAN コントローラ Web UI から CFS 情報を表示するには、次の手順を実行します。

手順

ステップ 1 CFS 設定をコミットするには、**スイッチオプションボタン**を選択し、**コミット**をクリックします。

このスイッチの CFS 設定はコミットされています。

ステップ 2 CFS 設定を中止するには、**スイッチオプションボタン**を選択し、**中止**をクリックします。

このスイッチの CFS 設定は中止されます。

ステップ 3 CFS 設定のロックをクリアするには、**スイッチオプションボタン**を選択し、**ロックのクリア**をクリックします。

CFS が別のユーザーによってロックされている場合、または前の操作が失敗した場合は、CFS セッションがロック解除されていることを確認してください。

イベント分析

イベント分析には、次のトピックが含まれます。

- [アラーム \(205 ページ\)](#)
- [イベント \(215 ページ\)](#)
- [アカウンティング \(220 ページ\)](#)

バックアップアクションの実行

次の表で、**[バックアップ (Backup)]** タブに表示される列について説明します。

フィールド	説明
スイッチ	スイッチの名前を示します。
バックアップ日	バックアップの日付を指定します。
バックアップタグ	バックアップ名を指定します。
バックアップのタイプ	バックアップタイプがゴールデンバックアップであるかどうかを指定します。
設定ファイル	設定ファイルを指定します。

次の表では、**[アクション (Action)]** に表示されるフィールドおよび説明について記述します。

アクション	説明
今すぐバックアップ	<ul style="list-style-type: none"> • [今すぐバックアップ (Backup now)] を選択します。 <p>[バックアップの新規作成 (Create new backup)] ウィンドウが表示されます。</p> <ul style="list-style-type: none"> • [バックアップタグ (Backup tag)] フィールドに名前を入力します。必要に応じて、[バックアップをゴールデンとしてマークする (Mark backup as golden)] チェックボックスをオンにします。 <p>ゴールデンバックアップの詳細については、「ゴールデンバックアップ (57 ページ)」を参照してください。</p> <ul style="list-style-type: none"> • [OK] をクリックします。
ブートフラッシュにコピー	<p>[ブートフラッシュにコピー (Copy to bootflash)] を選択します。確認ウィンドウが表示されます。[OK] をクリックします。</p> <p>ブートフラッシュの詳細については、「ブートフラッシュのコピー (101 ページ)」をチェックしてください。</p>
比較	<p>スイッチの設定を比較するために必要なスイッチ名を選択し、[比較 (Compare)] を選択します。</p> <p>インスタンスで選択できるスイッチは2つだけです。</p> <p>[設定の比較 (Compare Config)] ウィンドウが表示され、2つの設定ファイルの違いが表示されます。</p> <p>ソースおよびターゲットの設定ファイルの内容は、2つの列に表示されます。</p> <p>設定ファイルの違いは、凡例とともに表に示されています。</p> <ul style="list-style-type: none"> • 赤：削除された設定の詳細。 • 緑：新しく追加された設定の詳細。 • 青：変更された設定の詳細。
エクスポート	<p>[Export] をクリックします。</p> <p>ファイルがローカルシステムにダウンロードされます。サードパーティのファイル転送ツールを使用して、これらのファイルを外部サーバーに転送できます。</p>
タグの編集	<p>[タグの編集 (Edit tag)] をクリックして、バックアップタグ名を変更します。</p>
ゴールデンとしてマーク	<p>既存のバックアップをゴールデンバックアップとしてマークするには、[ゴールデンとしてマーク] を選択します。確認ウィンドウが表示されたら、[確認 (Confirm)] をクリックします。</p>

アクション	説明
ゴールデンとして削除	ゴールデンバックアップから既存のバックアップを削除するには、[ゴールデンとして削除 (Remove as gold)]を選択します。確認ウィンドウが表示されたら、[確認 (Confirm)]をクリックします。
Delete	<p>既存のバックアップを削除するには、[削除 (Delete)]を選択します。確認ウィンドウが表示されたら、[確認 (Confirm)]をクリックします。</p> <p>(注)</p> <ul style="list-style-type: none"> バックアップをゴールデンバックアップとしてマークしている場合。ゴールデンバックアップが削除されていることを確認してください。そうしないと、既存のバックアップを削除できないというエラーが表示されます。 一度に1つのバックアップを削除できます。

ポートの使用の表示

[ポートの使用 (Port Usage)] タブで次の情報を表示できます。

- [ポート速度 (Port Speed)] 列にはポートの速度が表示されます。
- [使用済みポート (Used Ports)] 列には、前述のポート速度の合計ポートが表示されます。
- [使用可能なポート (Available Ports)] 列には、ポート速度で使用可能なポートが表示されます。
- [ポートの合計 (Total Ports)] 列には、上記の速度のポートの合計が表示されます。
- [推定残り日数 (Estimated Day Left)] 列には、ポートの推定残り日数が表示されます。

[属性別フィルタ処理 (Filter by attribute)] を使用して、必要な情報を表示できます。

表を更新するには、[更新 (Refresh)] アイコンをクリックします。

[使用済みポート (Used ports)] には、選択したスイッチの使用済みポートの合計が表示されます。[ポートの合計 (Total ports)] には、選択したスイッチで使用可能なポートの合計が表示されます。

メトリック

[メトリック (Metric)] タブには、インフラストラクチャの正常性とステータスが表示されます。CPU 使用率、メモリ使用率、トラフィック、および温度、の詳細を表示できます。

次の表では、[CPU] および [メモリ (Memory)] タブでの列の表示について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
IP アドレス	スイッチの IP アドレスを指定します。
最小値 (Low Value (%))	スイッチの最小 CPU 使用率の値を示します。
平均値 (Avg. Value (%))	スイッチの平均 CPU 使用率の値を示します。
最大値 (High Value (%))	スイッチの最大 CPU 使用率の値を示します。
範囲プレビュー (Range Preview)	線形範囲のプレビューを示します。
前回の更新時刻	スイッチが最後に更新された日時を表示します。
最終日の表示 (Show last day)	[最終日の表示 (Show last day)] をクリックすると、選択した日、週、月、年のデータが表示されます。

次の表では、**[トラフィック (Traffic)]** タブに表示される列について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
平均Rx	平均 Rx 値を示します。
ピーク Rx (Peak Rx)	ピーク Rx 値を示します。
平均Tx	平均 Tx 値を示します。
ピーク Tx (Peak Tx)	ピーク Tx 値を示します。
平均Rx+Tx	Rx および Tx 値の平均を示します。
平均Errors	平均エラー値を示します。
ピーク エラー (Peak Errors)	ピーク エラー値を示します。
平均破棄	平均廃棄値を示します。
ピーク 廃棄 (Peak Discards)	ピーク 廃棄値を示します。
前回の更新時刻	最後に更新された日時を示します。
最終日の表示 (Show last day)	[最終日の表示 (Show last day)] をクリックすると、選択した日、週、月、年のデータが表示されます。

次の表では、**[温度 (Temperature)]** タブに表示される列について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
IP アドレス	平均 Rx 値を指します。

フィールド	説明
モジュール温度 (Temperature Module)	ピーク Rx 値を指します。
最低値 (Low Value (C))	最低温度の値を示します。
平均値 (Avg. Value (C))	平均温度の値を示します。
最高値 (High Value (C))	最高温度の値を示します。
最終日の表示 (Show last day)	[最終日の表示 (Show last day)] をクリックすると、選択した日、週、月、年のデータが表示されます。

輻輳分析

輻輳分析では、スイッチレベルおよびポートレベルで低速ドレインの統計を表示できます。任意の期間内で低速ドレインの問題をモニタリングできます。データをチャート形式で表示し、分析のためにデータをエクスポートできます。また、txwait、ドロップ、クレジット損失回復、使用率の超過、およびポートモニタイベントの高レベルビューを提供するトポロジを表示することもできます。

輻輳統計はキャッシュメモリに保存されます。したがって、サーバーが再起動されるか、新しい診断リクエストが発行されると、統計は失われます。



Note ログオフした後でも、ジョブはバックグラウンドで実行されます。

Procedure

- ステップ 1 [SAN] > [ファブリック (Fabrics)] を選択します。
- ステップ 2 ファブリックのリストから、[ファブリック (Fabrics)] をダブルクリックしてファブリックの概要を表示します。
[輻輳分析 (Congestion Analysis)] タブをクリックします。
- ステップ 3 [ファブリック (Fabric)] ドロップダウンリストからファブリック名を選択します。
- ステップ 4 [期間 (Duration)] ドロップダウンリストから、スケジュールされたジョブに対して [1 回 (Once)] または [毎日 (Daily)] を選択します。[1 回 (Once)] は、10 分、30 分、1 時間、カスタム時間などの間隔を含み、ジョブをすぐに実行します。[毎日 (Daily)] では、開始時刻を選択し、選択した間隔でジョブを実行できます。オプションボタンを使用して、データを収集する間隔を選択します。
- ステップ 5 [分析の開始 (Start Analysis)] をクリックして、ポーリングを開始します。
サーバーは、ユーザーが定義した範囲に基づいて低速ドレインの統計を収集します。[残り時間 (Time Remaining)] はページの右側に表示されます。

- ステップ 6** [分析の停止 (Stop Analysis)] をクリックして、ポーリングを停止します。
- サーバーは、新しい診断リクエストが行われるまで、カウンタをキャッシュに保持します。時間切れになる前にポーリングを停止できます。
- ステップ 7** 各ファブリックの [ファブリック (Fabric)]、[ポーリングのステータス (Status of polling)]、[開始 (Start)]、[終了 (End)]、および [期間 (Duration)] 列が表示されます。
- ステップ 8** ファブリックを選択し、[すべて削除 (Delete All)] または [停止 (Stop)] をクリックして、ジョブを削除または停止します。
- ファブリック名をクリックすると、ファブリックの詳細ビューが表示され、ファブリックの輻輳の詳細が表示されます。詳細については、「[輻輳可視化, on page 82](#)」を参照してください。
- ステップ 9** [デバイスインターフェイス (Device Interfaces)] テーブルの [スイッチ名 (Switch Name)] 列でスイッチ名をクリックして、スイッチの状態を表示します。
- ステップ 10** [デバイスインターフェイス (Device Interfaces)] テーブルの [インターフェイス (Interface)] 列でインターフェイス名をクリックして、スイッチポートの低速ドレイン値をチャート形式で表示します。
- [属性別フィルタ処理 (Filter by attributes)] オプションを使用して、各列に定義された値に基づいて詳細を表示します。
- [データのある行のみ (Only Rows With Data)] オプションを選択して、統計内のゼロ以外のエントリをフィルタ処理して表示します。

輻輳可視化

ファブリック名をクリックすると、選択したファブリックのトポロジが表示され、ファブリックの輻輳の詳細が表示されます。トポロジウィンドウには、さまざまなネットワーク要素に対応するノードとリンクが色分けされて表示されます。各要素について、カーソルを合わせると詳細情報を取得できます。リンクとスイッチは色分けされています。パフォーマンスコレクションと SNMP トラップを有効にして、トポロジの輻輳情報を表示します。

次の表に、リンクとスイッチに関連する色の説明を示します。

Table 14: 色の説明

カラー	名前	説明
ブルー (ライト)	高使用率	高使用率 tx-datarate >= 80%
緑	標準	輻輳は見つかりませんでした
赤	レベル 3	クレジット損失回復
オレンジ	レベル 2	ドロップ
黄 (ダーク)	レベル 1.5	txwait >= 30%

カラー	名前	説明
黄 (薄)	レベル 1	txwait < 30%
グレー (ライト)	データがありません	データがありません

スイッチの色は、スイッチへのリンクで検出される最高レベルの輻輳を表します。最大値は 3、最小値は 1 です。過剰使用の場合は、スイッチは 2 色になります。スイッチの右半分のライトブルーは、過剰使用を表します。スイッチの数字は、輻輳が発生している F ポートの数を表します。数字の周りの色は、スイッチの F ポートで検出される最高レベルの輻輳を表します。スイッチをクリックすると、輻輳の詳細が表示されます。

リンクの輻輳を表すために、2 本の平行線が使用されています。リンクは双方向であるため、各方向には、輻輳の最高レベルを表す色があります。リンクにカーソルを合わせると、送信元と接続先のスイッチとインターフェイス名が表示されます。リンクをクリックすると、そのリンクのみに関連する輻輳データが表示されます。



Note リンクが持つことができる最高の輻輳レベルは、[レベル 3 (Level 3)] です。リンクの有効な色は、緑、赤、オレンジ、黄 (ダーク)、黄 (ライト)、グレー (ライト) です。

DIRL

ダイナミック入力レート制限 (DIRL) は、入力コマンドおよびその他のトラフィックのレートを自動的に制限して、出力方向で発生している輻輳を軽減または排除するために使用されます。DIRL は、IO 勧誘によって生成されるデータが、輻輳を引き起こすことなくデータを処理するエンドデバイスの能力と一致するように、IO 勧誘のレートを下げることによってこれを行います。勧誘されたデータの量を処理するデバイスの能力が変化すると、DIRL は、動的に調整して、エンドデバイスが輻輳を引き起こすことなく、可能な最大量のデータをデバイスに供給しようとしています。エンドデバイスが輻輳から回復すると、DIRL はスイッチポートに送信されるトラフィックの制限を自動的に停止します。

ドレインが低速で使用率が過剰な場合、IO 勧誘リクエストのレートが低下すると、勧誘されてエンドデバイスに送信されるデータの量が対応して減少することが想定されます。データの量を減らすことで、低速ドレインと過剰使用の両方のケースを解決できます。

DIRL は 2 つの機能で構成されており、低速ドレインと過剰使用の両方によって引き起こされる輻輳に対しても同様に適切に実行できます。

- **ポートモニタ** : 低速ドレインと過剰使用状態を検出し、ポートガードアクションが DIRL に設定されている場合は、FPM に通知します。ポート モニタ ポート ガードアクション DIRL は、次のカウンタで設定できます。

- **txwait** : 低速ドレインの検出に使用します。
- **tx-datarate** : 過剰使用の検出に使用されます。
- **tx-datarate-burst** : 過剰使用の検出に使用します。

- **FPM** : DIRL アクションは、ポートモニタからの通知に従って FPM によって実行されます。ポートモニタから上昇しきい値を検出すると、FPM はレートを低下させ、入力トラフィックのレートを低下させます。DIRL 回復間隔で継続的に下限しきい値を下回っているカウンタの値を検出すると、FPM はレート回復を行います。

ポートモニタリングポリシーが DIRL ポートガードアクションで構成され、アクティブ化されると、デフォルトではないすべての F ポートがデフォルトでモニタリングされ、これらのポートのいずれかで輻輳が検出されると、FPM に通知されます。ただし、特定のインターフェイスをモニタリング対象から手動で除外できます。

以下は、DIRL のさまざまな遷移状態です。

- **正常** : ポートが正常に機能している状態で、DIRL レート削減に入る前の状態。完全に回復すると、ポートは正常状態に戻ります。
- **DIRL レート削減** : イベント上昇しきい値が DIRL レート削減プロセスをトリガーする状態。
- **DIRL レート削減の最大値** : DIRL レート削減が最大値に達しており、より多くの上昇しきい値イベントが検出された状態。
- **DIRL ステータス** : 上昇しきい値を下回り、下降しきい値を超えるイベントが検出された状態。設定された回復間隔で下限しきい値を下回るイベントが検出されると、この状態は DIRL 回復状態に移行します。
- **DIRL レート回復** : 設定された回復間隔の下限しきい値を下回るイベントを検出すると、DIRL レート回復が発生する状態。ポートが DIRL から完全に回復した後、この状態は正常状態に移行します。

この状態は繰り返し発生する状態であり、ポートが DIRL から完全に回復する前に、複数のレート回復が発生します。上昇しきい値を下回り、下限しきい値を超えるイベントが検出されると、この状態は DIRL 状態に遷移します。

ポートで検出されたイベントのタイプに応じて、DIRL によって開始されるアクションは次のとおりです。



(注) イベントは、最新のイベントを上にして、時刻順にリストされています。

- ポートでイベント上昇しきい値が検出され、ポートに対して DIRL が開始されます。ポート入力トラフィックレートは、現在のレートの 50% に削減されます。
- 次のポーリング間隔では、上昇しきい値を検出せずに回復間隔が終了します。ポート入力トラフィックは、現在の容量の 25% 増加します。
- 次のポーリング間隔では、上昇しきい値を検出せずに回復間隔が終了します。ポートの入力トラフィックは、現在の容量の 25% 増加します。
- 次のポーリング間隔では、上昇しきい値を検出せずに回復間隔が終了します。ポート入力トラフィックは、現在の容量の 25% 増加します。

- 次のポーリング間隔では、上昇しきい値を検出せずに回復間隔が終了します。ポート入力トラフィックは、現在の容量の 25% 増加します。
- 次のポーリング間隔で、ポートでイベント上昇しきい値が検出され、ポートに対して DIRL が開始されます。ポート入力トラフィックは、現在のレートの 50% に再び削減されます。

DIRL 輻輳管理の可視化

ダイナミック入力レート制限 (DIRL) 分析は、選択したファブリックに基づいて実行されるオンデマンドジョブです。ファブリック内のすべてのスイッチの DIRL ステータスとイベントを表示します。以下のコマンドがスイッチで実行され、出力がスナップショットとして収集されます。

- `show fcpm ingress-rate-limit status`
- `show fpm ingress-rate-limit events`



(注) DIRL 可視化は、リリース 9.2(1) の Cisco MDS シリーズスイッチでサポートされています。

Cisco NDFC SAN コントローラ UI で DIRL 分析を表示するには、次の手順を実行します。

1. [SAN] > [ファブリック (Fabrics)] を選択します。
2. ファブリックのリストから、[ファブリック (Fabrics)] をダブルクリックしてファブリックの概要を表示します。
[DIRL] タブをクリックします。
3. [DIRL ステータス (DIRL Status)] をクリックして収集を開始します。

収集が進行中であることを示すステータスメッセージが表示されます。また、分析が開始されたタイムスタンプも表示されます。分析が完了すると、下の表に情報が入力されます。収集が完了したことを示すステータスメッセージが表示されます。また、分析が完了したタイムスタンプも表示されます。

下の表のエントリは、次のフィールドを示しています。

フィールド	説明
スイッチ	分析が収集されるスイッチを指定します。 [スイッチ] をクリックして、概要を表示するスライドインペインを表示します。[起動 (Launch)] アイコンをクリックして、[スイッチの概要 (Switch Overview)] を表示します。

フィールド	説明
インターフェイス	分析が収集されるインターフェイスを指定します。 インターフェイスをクリックして、[レート制限イベント (Rate Limit events)] を表示します。表には、CLI コマンド出力からのこのインターフェイスのイベントが表示されます show fpm ingress-rate-limit events 。
現在のレート制限 (%)	現在のレート制限を示す % を指定します。
前のアクション	レート制限を制御するために実行された前のアクションを指定します。
最終更新時刻	イベントが発生したタイムスタンプを表示します。

[DIRL 履歴の表示 (View DIRL History)] をクリックして、現在の DIRL インターフェイスを除く、このファブリック内のすべてのインターフェイスの DIRL イベントを表示します。表には、CLI コマンド出力からのイベントが表示されます **show fpm ingree-rate-limit events**。



第 6 章

スイッチ

- [スイッチ \(87 ページ\)](#)
- [スイッチの概要 \(97 ページ\)](#)

スイッチ

次の表で、[**スイッチ (Switches)**] ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
[IPアドレス (IP Address)]	スイッチの IP アドレスを指定します。
Fabric Name (ファブリック名)	スイッチに関連付けられているファブリック名を指定します。
ステータス	スイッチのステータスを指定します。
ヘルス (Health)	スイッチの正常性ステータスを指定します。正常性ステータスは次のとおりです。 <ul style="list-style-type: none">• 正常• 深刻• 警告• OK
Ports	スイッチのポートの合計数を指定します。
使用済みポート	スイッチで使用されるポートの合計数を指定します。
モデル	スイッチ モデルを指定します。
シリアル番号 (Serial Number)	スイッチのシリアル番号を指定します。

フィールド	説明
リリース	スイッチのリリース番号を指定します。
稼働時間	スイッチアップ時間の詳細を指定します。

次の表に、[アクション (Actions)] メニューのドロップダウンリストで、**[LAN] > [スイッチ (Switch)] > [スイッチ (Switch)]** に表示されるアクションメニューを示します。

アクション項目	説明
Device Manager	必要なスイッチのデバイスマネージャにログインできます。 [デバイスマネージャ (Device Manager)] ログインウィンドウが表示され、ログイン情報を入力してログインします。 Cisco MDS 9000 デバイスマネージャの説明と使用方法については、 デバイスマネージャ (319 ページ) を参照してください。
テクニカル サポート	ログの収集を開始できます。詳細については、 テクニカル サポート (88 ページ) を参照してください。
CLI の実行	複数のスイッチで複数の CLI コマンドを実行し、各スイッチの出力を zip 形式のテキストファイルとして収集できます。詳細については、 CLI の実行 (89 ページ) を参照してください。

デバイスマネージャ

Cisco MDS 9000 Device Manager の説明と使用方法については、[デバイスマネージャ \(319 ページ\)](#) 章を参照してください。



(注) **[スイッチの概要 (Switch Overview)]** 画面で別のタブに移動すると、Device Manger セッションが終了します。

テクニカル サポート

[アクション (Actions)] ドロップダウンリストから、**[テクニカルサポート (Tech Support)]** を選択してログ収集を開始します。ウィンドウが表示されます。

- **[セッションタイムアウト (Session timeout)]** フィールドに時間を分単位で入力します。デフォルトの時間は 20 分です。

- **[コマンド (Command)]** テキストフィールドにコマンドを入力し、**[実行 (Run)]** をクリックします。
- データが正常に送信され、テクニカルサポートが開始されました (Data submitted successfully, tech support starting) という確認ウィンドウが表示され、**[確認 (Confirm)]** をクリックしてステータスが **[完了 (Completed)]** に変わります。
- レポートをダウンロードするには、**[テクニカルサポートのダウンロード (Download Tech Support)]** をクリックします。

CLI の実行

リリース 12.1.1e 以降、Cisco NDFC SAN コントローラを使用すると、スイッチで CLI コマンドを実行できます。各スイッチの .zip ファイル内の CLI コマンドからの出力を収集できます。

スイッチで CLI コマンドを実行するには、次の手順を実行します。

1. Cisco NDFC UI で、**[SAN] > [スイッチ (Switches)] > [スイッチ (Switches)]** を選択します。
2. CLI コマンドを実行するスイッチを選択します。
複数のスイッチを選択して、一連の CLI コマンドを同時に実行できます。
3. **[アクション (Actions)]** ドロップダウンリストから、**[CLI の実行 (Execute CLI)]** を選択します。
[スイッチ CLI の実行 (Execute Switch CLI)] 画面が表示されます。
4. **[設定 (Configure)]** タブで、**[選択されたスイッチ (Selected Switches)]** の下のハイパーリンクをクリックして、CLI が実行される選択されたスイッチを表示します。
5. **[CLI コマンド (CLI Commands)]** テキストボックスに、スイッチで実行する CLI コマンドを入力します。
1 行に 1 つのコマンドを入力するようにしてください。
6. **[実行 (Execute)]** をクリックします。
成功 (Success) 確認メッセージが表示されます。
7. **[実行 (Execute)]** タブで、テーブルには、スイッチ、関連するファブリック、および CLI の実行ステータスが表示されます。
8. **[出力のダウンロード (Download output)]** をクリックして、コマンド出力をダウンロードします。



(注) CLI 経由でスイッチに到達できない場合、zip ファイルの出力にエラーが表示されます。

拡張されたロールベースのアクセス制御

SAN コントローラリリース 12.0.1(a) からは、すべての RBAC が Nexus ダッシュボードにあります。ユーザーロールとアクセスは、NDFC 上のファブリックの Nexus ダッシュボードから定義されます。

Nexus ダッシュボードの管理者ロールは、NDFC のネットワーク管理者ロールと見なされます。

DCNM には、さまざまなアクセスと操作を実行するための 5 つのロールがありました。ユーザーがアクセスする場合、ネットワークステージロールを持つファブリックは、ネットワークステージロールとして他のすべてのファブリックにアクセスできます。したがって、ユーザー名は DCNM でのロールによって制限されます。

Cisco NDFC リリース 12.0.1(a) には同じ 5 つのロールがありますが、Nexus ダッシュボードの統合により詳細な RBAC を実行できます。ユーザーがネットワークステージロールとしてファブリックにアクセスする場合、同じユーザーは、管理者またはオペレーターロールなどの他のユーザーロールを使用して別のファブリックにアクセスできます。したがって、ユーザーは NDFC のさまざまなファブリックでさまざまなアクセス権を持つことができます。

NDFC RBAC は、次のロールをサポートします。

- NDFC アクセス管理者
- NDFC デバイス アップグレード管理者
- NDFC ネットワーク管理者
- NDFC ネットワーク オペレータ
- NDFC ネットワーク ステージャ

次の表では、NDFC でのユーザーロールとその権限について説明します。

ロール	権限
NDFC アクセス管理者	読み取り/書き込み 参照先
NDFC デバイス アップグレード管理者	読み取り/書き込み
NDFC ネットワーク管理者	読み取り/書き込み
NDFC ネットワーク オペレータ	読み取り
NDFC ネットワーク ステージャ	読み取り/書き込み

DCNM では、下位互換性のために次のロールがサポートされています。

- SAN 管理者 (ネットワーク管理者にマッピング)
- グローバル管理者 (ネットワーク管理者にマッピング)
- SAN ネットワーク管理者 (ネットワーク管理者にマッピング)

- サーバー管理者（ネットワーク管理者にマッピング）



- (注) どのウィンドウでも、ログインしているユーザーロールで実行できないアクションはグレー表示されます。

NDFC ネットワーク管理者

NDFC ネットワーク管理者ロールを持つユーザは、SAN コントローラですべての操作を実行できます。

Cisco Nexus ダッシュボードファブリック コントローラ リリース 12.1.1e から、このロールを持つユーザーは、ネットワークおよびVRFのMSDファブリックのすべての操作を実行できます。

NDFC ネットワーク管理者ロールを持つユーザーは、SAN コントローラの特定のファブリックまたはすべてのファブリックをフリーズできます。



- (注) スイッチの検出または追加のスイッチを行うスイッチ ユーザーのロール、またはNDFCのLANクレデンシャルには、`network-admin` ロールが必要であることを確認してください。

NDFC デバイス アップグレード管理者

NDFC デバイス アップグレード管理者ロールを持つユーザは、[イメージ管理 (Image Management)]ウィンドウでのみ操作を実行できます。

詳細については、「[イメージ管理](#)」の項を参照してください。

NDFC アクセス管理者

NDFC アクセス管理者ロールを持つユーザは、すべてのファブリックの[インターフェイス マネージャ (Interface Manager)]ウィンドウでのみ操作を実行できます。

NDFC アクセス管理者は、次のアクションを実行できます。

- レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。
- ホスト vPC、およびイーサネット インターフェイスを編集します。
- 管理インターフェイスからの保存、プレビュー、および展開。
- LAN クラシックおよび IPFM ファブリックのインターフェイスを編集します。

nve、管理、トンネル、サブインターフェイス、SVI、インターフェイス グループ、およびループバック インターフェイスを除く

ただし、SAN コントローラ アクセス ロールを持つユーザは、次のアクションを実行できません。

- レイヤ 3 ポートチャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。
- レイヤ 3、ST FEX、AA FEX のメンバー インターフェイスおよびポート チャネルは編集できません。
- Easy ファブリック用に、アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。
- ピア リンク ポート チャネルを編集できません。
- 管理インターフェイスを編集できません。
- トンネルを編集できません。



(注) ファブリックまたはSAN コントローラが展開フリーズモードの場合、このロールのアイコンとボタンはグレー表示されます。

NDFC ネットワーク ステージャ

NDFC ネットワーク ステージャ ロールを持つユーザは、SAN コントローラで設定を変更できます。NDFC ネットワーク 管理者 ロールを持つユーザは、これらの変更を後で展開できます。ネットワーク ステージャは、次のアクションを実行できます。

- インターフェイス構成の編集
- ポリシーの表示または編集
- インターフェイスの作成
- ファブリック設定の変更
- テンプレートの編集または作成

ただし、ネットワーク ステージャは次のアクションを実行できません。

- スイッチに設定を展開できません。
- SAN コントローラ Web UI または REST API から展開関連のアクションを実行できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。
- メンテナンス モードの切り替えはできません。
- 展開フリーズモードでファブリックを移動したり、展開モードから解放したりすることはできません。
- パッチをインストールします。

- スイッチをアップグレードできません。
- ファブリックを作成または削除できません。
- スイッチをインポートまたは削除できません。

NDFC ネットワーク オペレータ

ネットワーク オペレータは、ファブリックビルダー、ファブリック設定、構成のプレビュー、ポリシー、およびテンプレートを表示できます。ただし、ネットワーク オペレータは次の操作を実行できません。

- ファブリック内のスイッチの予期される構成を変更できません。
- スイッチに構成を展開できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。

ネットワーク オペレータとネットワーク ステージャの違いは、ネットワーク ステージャとして、既存のファブリックのインテントのみを定義できますが、それらの設定を展開できないことです。

ネットワーク ステージャロールを持つユーザがステージングした変更および編集を展開できるのは、ネットワーク管理者だけです。

デフォルトの認証ドメインの選択

Nexus ダッシュボードのデフォルトのログイン画面では、認証用のローカルドメインが選択されます。ドロップダウンリストから利用可能なドメインを選択することで、ログイン時にドメインを変更できます。

Nexus ダッシュボードは、ローカルおよびリモート認証をサポートしています。Nexus ダッシュボードのリモート認証プロバイダーには、RADIUS と TACACS が含まれます。認証のサポートの詳細については、<https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-211.pdf>を参照してください。

次の表に、DCNM アクセスと NDFC アクセス間の RBAC の比較を示します。

DCNM 11.5(x)	NDFC 12.0.x および 12.1.x
<ul style="list-style-type: none"> • ユーザーのロールは1つです。 • すべての API とリソースは、この1つのロールでアクセスされます。 	<ul style="list-style-type: none"> • ユーザーは、セキュリティドメインの Nexus ダッシュボードごとに異なるロールを持つことができます。 • セキュリティドメインには単一の Nexus ダッシュボードが含まれ、各 Nexus ダッシュボードには単一の NDFC ファブリックが含まれます。

DCNM 11.5(x)	NDFC 12.0.x および 12.1.x
DCNM のオプションへのアクセスを無効化または制限することにより、単一のロールがユーザーに関連付けられます。	単一のロールでは、選択したページに特権リソースのみが表示され、NDFC のその他のオプションでは、選択したリソースに関連付けられたセキュリティドメインに基づいて、制限されたアクセスがグレー表示されます。
シェル、ロール、およびオプションのアクセス制約を含む DCNM AV ペア形式。	シェル、ドメインを含む Nexus ダッシュボード AV ペアフォーマット。
展開タイプ LAN、SAN、または PMN に基づいてサポートされるロール。	network-admin、network-operator、device-upg-admin、network-stager、access-admin などのサポートされているロールは NDFC にあります。 下位互換性のためのレガシーロールのサポート。DCNM のネットワーク管理者としての Nexus ダッシュボード管理ロール。

次の表では、DCNM 11.5(x) AV ペアの形式について説明します。

Cisco DCNM Role	RADIUS Cisco-AV-Pair の値	TACACS+ シェル Cisco-AV-Pair ペアの値
network-operator	shell:roles = "network-operator" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"

次の表では、NDFC 12.x AV ペアの形式について説明します。

ユーザー ロール	AVPair 値
NDFC アクセス管理者	アクセス管理者
NDFC デバイス アップグレード管理者	Device-upg-admin
NDFC ネットワーク管理者	network-admin
NDFC ネットワーク オペレータ	network-operator
NDFC ネットワーク ステージャ	Network-stager

AV ペア文字列の形式は、特定のユーザーに対して読み取り/書き込みロールを設定するか、読み取り専用ロールを設定するか、または読み取り/書き込みロールと読み取り専用ロールの組み合わせを設定するかによって異なります。通常の文字列にはドメインが含まれており、その

後にスラッシュ (/) で区切って読み取り専用ロールからは切り離された読み取り/書き込みロールが続きます。個々のロールはパイプ (|) で区切られています。

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

Nexus Dashboard のセキュリティ ドメイン

ユーザ ログインに関するアクセス制御情報には、ユーザ ID、パスワードなどの認証データが含まれます。認証データに基づいて、リソースに適宜アクセスできます。Nexus ダッシュボードの管理者は、セキュリティ ドメインを作成し、さまざまなリソース タイプ、リソース インスタンスをグループ化し、それらをセキュリティ ドメインにマッピングできます。管理者は各ユーザの AV ペアを定義します。これにより、Nexus ダッシュボードのさまざまなリソースに対するユーザのアクセス権限が定義されます。ファブリックを作成すると、Nexus ダッシュボードに同じファブリック名でサイトが作成されます。これらのサイトは、**[Nexus ダッシュボード (Nexus Dashboard)] > [サイト (Sites)]** で作成および表示できます。

SAN コントローラ REST API は、この情報を使用して、認可を確認することによってアクションを実行します。

SAN コントローラ リリース 11.x からアップグレードすると、各ファブリックは同じ名前の自動生成サイトにマッピングされます。これらすべてのサイトは、Nexus ダッシュボードのすべてのセキュリティ ドメインにマッピングされます。

すべてのリソースは、他のドメインに割り当てられたりマッピングされたりする前に、すべてのドメインに配置されます。すべてのセキュリティ ドメインには、Nexus ダッシュボードで使用可能なすべてのセキュリティ ドメインは含まれません。

AV ペア

セキュリティ ドメインのグループと各ドメインの読み取りおよび書き込みロールは、AV ペアを使用して指定されます。管理者は、各ユーザの AV ペアを定義します。AV ペアは、Nexus ダッシュボードのさまざまなリソースに対するユーザのアクセス権限を定義します。

AV ペアの形式は次のとおりです。

```
"avpair": "shell:domains = security-domain / write-role-1 | write-role-2, security-domain / write-role-1 | write-role2 / read-role-1 | read-role-2 "
```

例: "avpair":

```
"shell:domains=all/network-admin/app-user|network-operator" 「all/admin/」はユーザをスーパーユーザにするため、all/admin/ を使用した例を避けるのが最善です。
```

write ロールには read ロールも含まれます。したがって、all/network-admin/ と all/network-admin/network-admin は同じです。



- (注) SAN コントローラ リリース 12.0.1a から、SAN コントローラ リリース 11.x で作成した既存の AV ペア形式がサポートされます。ただし、新しい AV ペアを作成する場合は、上記の形式を使用します。shell:domains にスペースが含まれていないことを確認します。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバ上で VSA cisco-AV-pair を使用して、次の形式で Cisco NX-OS デバイスのユーザーロールマッピングを指定できます。

```
shell:roles="roleA roleB ..."
```

cisco-AV-pair 属性にロールオプションを指定しなかった場合のデフォルトのユーザーロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシープロトコルに指定できるオプションは、AES-128 と DES です。cisco-AV-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュリティ ドメインの作成

Cisco Nexus Dashboard からセキュリティ ドメインを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. [管理 (Administrative)] > [セキュリティ (Security)] の順に選択します。
3. [セキュリティ ドメイン (Security Domain)] タブに移動する
4. [セキュリティ ドメインの作成 (Create Security Domain)] をクリックします。
5. 必要な詳細を入力し、[作成 (Create)] をクリックします。

ユーザの作成

Cisco Nexus Dashboard からユーザを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. [管理 (Administrative)] > [ユーザー (Users)] の順に選択します。
3. [ローカル ユーザーの作成 (Create Local User)] をクリックします。
4. 必要な詳細を入力し、[セキュリティ ドメインの追加 (Add Security Domain)] をクリックします。
5. ドロップダウン リストからドメインを選択します。
6. 適切なチェックボックスをオンにして、SAN コントローラ サービスの読み取りまたは書き込みロールを割り当てます。
7. [保存 (Save)] をクリックします。

スイッチの概要

UIパス：[SAN]>[スイッチ]>[スイッチの概要]

[スイッチの概要 (Switch Overview)]メニューには、次のサブメニューがあります。

スイッチの概要の表示

[スイッチの概要 (Switch Overview)]タブでは、スイッチの概要とともにスイッチに関する情報を表示できます。[SAN]>[スイッチ (Switches)]を移動し、必要なスイッチをクリックします。スライドインペインが表示されます。[起動 (Launch)]アイコンをクリックして、[スイッチの概要 (Switch Overview)]ウィンドウを表示します。

[概要 (Summary)]タブに表示されるデフォルトのカードは次のとおりです。

カード	説明
スイッチ情報	名前、正常性ステータス、IPアドレス、モデル、バージョン、その他のスイッチ情報など、スイッチの詳細を表示します。
イベント分析	重大、メジャー、マイナー 、および警告の重大度を持つイベントを表示します。詳細については、このカードで[起動 (Launch)]アイコンをクリックして[イベント (events)]タブに移動します。
関連資料	スイッチのリソース使用率をグラフ形式で表示します。
モジュール	モジュールが検出されたスイッチ、モデル名、カウントを表示します。
インターフェイス	スイッチインターフェイスに関する要約情報を表示します。
ポートの使用	ポートインベントリに関する要約情報を表示します。

モジュール

SAN コントローラWeb UI からモジュールのインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 [SAN]、[スイッチ (Switch)]、[スイッチの概要 (Switch Overview)]、[モジュール (Modules)] の順に選択します。同様に、ファブリックの概要ウィンドウで、[SAN]>[ファブリック (Fabric)]>[ファブリックの概要 (Fabric Overview)]>[Modules] の順に表示できます。

[モジュール (Modules)] タブに、選択した範囲のすべてのスイッチとその詳細のリストが表示されます。

テーブルに必要な情報を表示し、[属性によるフィルタ (Filter by Attributes)] に詳細を入力できます。

ステップ 2 次の情報が表示されます。

- [名前 (Name)] にはモジュール名が表示されます。
- [モデル (Model)] にモデル名が表示されます。
- [シリアル番号 (Serial Number)] 列には、シリアル番号が表示されます。
- [タイプ (Type)] 列には、モジュールのタイプが表示されます。
- **Oper. Status** 列には、デバイスの動作状態が表示されます。
- [スロット (Slot)] 列には、スロット番号が表示されます。
- [ハードウェアリビジョン (HW Revision)] 列には、モジュールのハードウェアバージョンが表示されます。
- [ソフトウェアリビジョン (Software Revision)] 列には、モジュールのソフトウェアバージョンが表示されます。
- [アセット ID (Asset ID)] カラムには、モジュールのアセット ID が表示されます。

インターフェイスの表示

UI Path: SAN > スイッチ > スイッチの概要 > インターフェイス

同様に、ファブリック概要ウィンドウでインターフェイスを表示できます。

SAN > ファブリック > ファブリックの概要 > インターフェイス

次の表では、[インターフェイス (Interfaces)] タブに表示されるフィールドについて説明します。

フィールド	説明
名前	インターフェイス名を指定します。
Admin. ステータス	インターフェイスの管理ステータスを指定します。

フィールド	説明
Oper. ステータス	インターフェイスの動作ステータスを指定します。
理由	失敗の理由を指定します。
スピード	Gb でインターフェイスの速度を指定します。
モード	インターフェイスのモードを指定します。
スイッチ	スイッチの名前を示します。
VSAN	接続された VSAN の名前を指定します。
接続先	接続の詳細を指定します。
接続先のタイプ	接続のタイプを指定します。
説明	インターフェイスの詳細を指定します。
オーナー	ポートの所有者を指定します。
[ポートグループ (Port Group)]	インターフェイスが接続されているポートグループ番号を指定します。

インベントリタブでさまざまな操作を実行するには、次の手順に従います。

手順

-
- ステップ 1** インターフェイスに対してシャットダウンを実行しない場合は、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[シャットダウンなし (No Shutdown)]をクリックします。
- 警告ウィンドウが表示されたら、[確認 (Confirm)]をクリックします。
- ステップ 2** インターフェイスをシャットダウンするには、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[シャットダウン (Shutdown)]をクリックします。
- 警告ウィンドウが表示されたら、[確認 (Confirm)]をクリックします。
- ステップ 3** インターフェイスのポート所有者を割り当てるには、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[所有者 (Owner)]をクリックします。
- ステップ 4** [ポート所有者の設定 (Set Port Owner)]ウィンドウが表示され、必要な名前を入力して[適用 (Apply)]をクリックします。
- ステップ 5** インターフェイスの診断をリンクするには、必要なインターフェイスのチェックボックス名を選択し、[アクション (Actions)]>[リンク診断 (Link Diagnostics)]をクリックします。
-

スイッチライセンスの表示

[ライセンス (Licenses)] タブで次の情報を表示できます。

- [機能 (Feature)] 列には、選択したスイッチの機能名が表示されます。
- [ステータス (Status)] 列には、ライセンスのステータスが表示されます。ステータスは、[使用中 (In Use)] または [未使用 (Unused)] のいずれかになります。
- [タイプ (Type)] 列には、ライセンスのタイプが表示されます。
- [警告 (Warnings)] 列には、ライセンスの猶予期間とその有効期限が表示されます。

[属性別フィルタ処理 (Filter by attribute)] を使用して、必要な情報を表示できます。

表を更新するには、[更新 (Refresh)] アイコンをクリックします。

イベント分析

イベント分析には、次のトピックが含まれます。

- [アラーム \(205 ページ\)](#)
- [イベント \(215 ページ\)](#)
- [アカウンティング \(220 ページ\)](#)

バックアップの表示

[バックアップ (Backup)] タブで次の情報を表示できます。

- [スイッチ (Switch)] 列にはスイッチの名前が表示されます。
- [バックアップ日 (Backup Date)] 列には、バックアップ日が表示されます。
- [バックアップタグ (Backup Tag)] 列には、バックアップタグ名が表示されます。
- [バックアップの種類 (Backup Type)] 列には、バックアップの種類が表示されます。
- [設定ファイル (Configuration File)] 列には、そのデバイス用にアーカイブされた設定ファイルが表示されます。

[属性別フィルタ処理 (Filter by attribute)] を使用して、必要な情報を表示できます。

表を更新するには、[更新 (Refresh)] アイコンをクリックします。

次の表では、このタブで実行できるアクションについて説明します。

アクション	説明
ブートフラッシュにコピー	ブートフラッシュのコピー (101 ページ) を参照してください。

アクション	説明
比較	設定ファイルの比較を参照してください。
エクスポート	Export Configurationを参照してください。
タグの編集	スイッチのタグを編集するには。必要なスイッチのチェックボックスをオンにし、[アクション (Actions)]>[タグの編集 (Edit tag)]を選択して、[OK]をクリックします。
ゴールデンとしてマーク	スイッチをゴールデンバックアップとしてマークするには。必要なスイッチのチェックボックスをオンにし、[アクション (Actions)]>[ゴールデンとしてマーク (Mark as golden)]を選択します。確認ウィンドウが表示されます。[確認 (Confirm)]をクリックします。 詳細については、「ゴールデンバックアップ」の項を参照してください。
ゴールデンとして削除	ゴールデンバックアップからスイッチを削除するには。必要なスイッチのチェックボックスをオンにし、[アクション (Actions)]>[ゴールデンとして削除 (Remove as golden)]を選択します。確認ウィンドウが表示されます。[確認 (Confirm)]をクリックします。
Delete	バックアップからスイッチを削除するには。必要なスイッチのチェックボックスをオンにし、[アクション (Actions)]>[削除 (Delete)]を選択します。確認ウィンドウが表示されます。[確認 (Confirm)]をクリックします。

この項の内容は、次のとおりです。

ブートフラッシュのコピー

設定ファイルは、同じデバイス、別のデバイス、または複数のデバイスに同時にコピーできます。

タスクのステータスを表示するには、次のタスクを実行します。

手順

- ステップ 1 SAN コントローラのホームページから、[SAN]>[スイッチ (Switch)]>[スイッチの概要 (Switch Overview)]>[バックアップ (Backup)]を選択します。

ステップ 2 [ブートフラッシュにコピー (Copy to bootflash)] をクリックします。

[ブートフラッシュにコピー (Copy to bootflash)] ページが表示され、[送信元設定のプレビュー (Source Configuration Preview)] エリアおよび [選択したデバイス (Selected Devices)] エリアが表示されます。

[送信元のプレビュー (Source Preview)] エリアには、デバイスにコピーされた実行/起動/バージョン設定ファイルの内容が表示されます。

ステップ 3 [選択されたデバイス (Selected Devices)] エリアで、デバイス名のチェックボックスをオンにして、設定をデバイスにコピーします。

(注) 複数の接続先デバイスを選択して、設定をコピーできます。

選択されたデバイスエリアには、次のフィールドが表示されます。

- [デバイス名 (Device Name)] : 送信元設定のコピー先のターゲットデバイス名を指定します。
- [IP アドレス (IP Address)] : 接続先デバイスの IP アドレスを指定します。
- [グループ (Groups)] : デバイスが属しているグループ。
- [ステータス (Status)] : デバイスのステータスを示します。

ステップ 4 [コピー (Copy)] をクリックします。

確認ウィンドウが表示されます。

ステップ 5 [はい (Yes)] をクリックして、設定を接続先デバイス設定にコピーします。

設定ファイルの比較

この機能を使用すると、設定ファイルを同じデバイスの別のバージョンまたは別のデバイスの設定ファイルと比較できます。

設定ファイルを比較するには、次のタスクを実行します。

手順

ステップ 1 チェックボックスをオンにして、比較する 2 つの設定ファイルを選択します。

選択した最初のファイルはソースとして指定され、2 番目の設定ファイルはターゲットファイルとして指定されます。

ステップ 2 [SAN] > [スイッチ (Switch)] > [スイッチの概要 (Switch Overview)] > [比較 (Compare)] に移動します。

ステップ 3 [設定の比較 (Compare Configuration)] をクリックします。

[設定の差分の表示 (View Config Diff)] ページが表示され、2つの設定ファイルの違いが表示されます。

ソースおよびターゲットの設定ファイルの内容は、2つの列に表示されます。右上隅のドロップダウンリストから[すべて (All)] を選択して、設定全体を表示します。[変更済み (Changed)] を選択して、設定ファイルの設定の違いを表示することもできます。

設定ファイルの違いは、凡例とともに表に示されています。

- [赤 (Red)] : 差分設定の詳細。
- 緑 : 新しく追加された設定の詳細。
- 青 : 変更された設定の詳細。

ステップ 4 [ターゲットにコピー (Copy to Target)] をクリックして、送信元設定をターゲット設定ファイルにコピーします。[キャンセル (Cancel)] をクリックして、[設定の詳細 (configuration details)] ページに戻ります。

[設定のコピー (Copy Configuration)] ウィンドウには、送信元設定のプレビューと接続先設定のターゲットデバイスが表示されます。選択されたデバイスエリアには、次のフィールドが表示されます。

- [デバイス名 (Device Name)] : 送信元設定のコピー先のターゲットデバイス名を指定します。
- [IP アドレス (IP Address)] : 接続先デバイスの IP アドレスを指定します。
- [グループ (Groups)] : デバイスが属しているグループ。
- [適切な設定 (Golden Config)] : 接続先設定のバージョンを指定します。
- [ステータス (Status)] : デバイスのステータスを示します。

ステップ 5 [はい (Yes)] をクリックして、設定を接続先デバイス設定にコピーします。

Export Configuration

SAN コントローラ サーバーから設定ファイルをエクスポートできます。設定ファイルをエクスポートするには、次のタスクを実行します。

手順

ステップ 1 SAN コントローラのホームページから、[設定 (Configure)] > [バックアップ (Backup)] を選択し、エクスポートする設定を選択します。

ステップ 2 [Export Configuration] をクリックします。

ファイルがローカルシステムにダウンロードされます。サードパーティのファイル転送ツールを使用して、これらのファイルを外部サーバーに転送できます。

ポートの使用の表示

[ポートの使用 (Port Usage)] タブで次の情報を表示できます。

- [ポート速度 (Port Speed)] 列にはポートの速度が表示されます。
- [使用済みポート (Used Ports)] 列には、前述のポート速度の合計ポートが表示されます。
- [使用可能なポート (Available Ports)] 列には、ポート速度で使用可能なポートが表示されます。
- [ポートの合計 (Total Ports)] 列には、上記の速度のポートの合計が表示されます。
- [推定残り日数 (Estimated Day Left)] 列には、ポートの推定残り日数が表示されます。

[属性別フィルタ処理 (Filter by attribute)] を使用して、必要な情報を表示できます。

表を更新するには、[更新 (Refresh)] アイコンをクリックします。

[使用済みポート (Used ports)] には、選択したスイッチの使用済みポートの合計が表示されます。[ポートの合計 (Total ports)] には、選択したスイッチで使用可能なポートの合計が表示されます。

ブートフラッシュの表示

[ブートフラッシュ (Bootflash)] タブで次の情報を表示できます。

- [プライマリ ブートフラッシュ サマリ (Primary Bootflash Summary)] カードには、合計、使用済み、および使用可能な領域が表示されます。
- [セカンダリ ブートフラッシュ サマリ (Secondary Bootflash Summary)] カードには、合計、使用済み、および使用可能な領域が表示されます。
- [ディレクトリ リスト (Directory List)] 領域に、プライマリ ブートフラッシュとセカンダリ ブートフラッシュのチェックボックスが表示されます。

この領域には、スイッチのブートフラッシュ上のすべてのファイルとディレクトリのファイル名、サイズ、および最終変更日が表示されます。[アクション (Actions)] > [削除 (Delete)] を順に選択してファイルを削除し、スイッチで使用可能なスペースを増やします。

デバイス マネージャ

Cisco MDS 9000 Device Manager の説明と使用方法については、[デバイス マネージャ \(319 ページ\)](#) 章を参照してください。



(注) **[スイッチの概要 (Switch Overview)]** 画面で別のタブに移動すると、Device Manger セッションが終了します。

ブレード

UCS スイッチのインターフェイスは、SAN コントローラ Web UI で、**[SAN] > [スイッチ (Switches)] > [スイッチの概要 (Switch Overview)]** から表示できます。



(注) UCS スイッチが SAN コントローラに一覧表示されており、これらのスイッチのステータスが正しいことを確認します。これらのタブは、UCS スイッチについてのみ表示できます。

[ブレード (Blades)] タブには、UCS FI に接続されているすべてのサーバーブレードの情報が表示されます。

UCS には次の 3 つのタブがあります。

- ブレード
- vNIC
- vHBA

[ブレード (blades)] タブには、すべてのブレード情報がカードとして表示されます。各ブレードエリアの **[詳細 (More Details)]** アイコンをクリックして、選択したブレードのサイドパネルに詳細を表示します。

[すべて折りたたむ (Collapse All)] または **[すべて展開 (Expand All)]** アイコンをクリックして、すべてのブレードエリアをそれぞれ折りたたむか、すべて展開することができます。

[ブレード (Blades)] タブには、UCS FI に接続されているすべてのサーバーブレードの情報が表示されます。冗長セットアップのプライマリ UCS FI またはスタンドアロン UCS FI のみが表示されます。

vNIC

[vNICs] タブには、その UCS FI の vNIC のリストが表示されます。グラフアイコンをクリックすると、vNIC の 24 時間のトラフィックが表示されます。

vHBA

[vHBA] タブには、その特定の UCS FI の vHBA のリストが表示されます。グラフアイコンをクリックして、vHBA の 24 時間のトラフィックを表示します。



第 7 章

SAN リンク

- [SAN リンク \(107 ページ\)](#)

SAN リンク

Cisco SAN コントローラを使用すると、SAN ファブリックで FCIP、ポートチャネルを設定できます。Cisco Web Nexus ダッシュボード ファブリック コントローラ UI から ISL トラフィックとエラーをモニタリングし、NPV リンクのパフォーマンスを表示することもできます。

ここでは、次の内容について説明します。

ISL およびポートチャネル

ISL トラフィックとエラーウィンドウが表示されます。この表は、SAN ファブリック設定された ISL とポートチャネルを示しています。ドロップダウンを使用して、24 時間、週、月、および年でビューをフィルタ処理できます。

[名前 (Name)] 列のトレンドアイコンをクリックして、グラフィカルな表現を表示します。

[アクション (Actions)] ドロップダウンリストから、次の操作を実行できます。

FCIP の設定

FCIP を設定するには、次の手順を実行します。

手順

- ステップ 1** [アクション (Actions)] ドロップダウンリストから [FCIP の設定 (Configure FCIP)] を選択します。

このページには、FCIP ウィザードを使用して FCIP を設定するためのタスクが表示されます。

(注) FCIP は、Cisco MDS 9000 24/10-Port SAN 拡張モジュールではサポートされていません。

- ステップ 2** [スイッチペアの選択 (Select Switch Pair)] 画面で、FCIP 経由で接続する 2 つの MDS スイッチをドロップダウンリストから選択します。
- 各スイッチが正しく機能するには、IP ネットワークに接続されたイーサネットポートが必要です。注フェデレーションセットアップの場合、両方のスイッチは、同じサーバーによって検出または管理されるファブリックに属している必要があります。
- ステップ 3** [次へ (Next)] をクリックして、イーサネットポートを選択します。
- ステップ 4** 選択したスイッチ間の FCIP ISL で使用するイーサネットポートを選択します。
- 正常に機能するには、ダウンポートを有効にする必要があります。未設定の 14+2、18+4、9250i、および SSN16 イーサネットポートにセキュリティを適用できます。
- ステップ 5** イーサネットポートの IP アドレスを入力し、ポートアドレスが別のサブネットにある場合は IP ルートを指定します。
- (注) [次へ (Next)] をクリックして、変更を IP アドレスと IP ルートに適用します。
- ステップ 6** [次へ (Next)] をクリックして、トンネルのプロパティを指定します。
- ステップ 7** TCP 接続をトンネリングするには、次のパラメータを指定します。
- パラメータを入力します。
- [最大帯域幅 (Max Bandwidth)] : 1 ~ 10000 の数値を入力します。単位は [Mb] です。
 - [最小帯域幅 (Min Bandwidth)] : 最小帯域幅の値を入力します。単位は [Mb] です。
 - [推定 RTT (ラウンドトリップ時間)] : 0 ~ 300000 の数値を入力します。単位は [us] です。[測定 (Measure)] をクリックして、ラウンドトリップ時間を測定します。
 - [書き込みアクセラレーション (Write Acceleration)] : チェックボックスをオンにして、書き込みアクセラレーションをイネーブルにします。
- (注) 書き込みアクセラレーションが有効になっている場合は、フローが複数の ISL 間で負荷分散しないようにします。
- [最適な圧縮をイネーブルにする (Enable Optimum Compression)] チェックボックスをオンにして、最適な圧縮をイネーブルにします。
 - [XRC エミュレータをイネーブルにする (Enable XRC Emulator)] チェックボックスをオンにして、XRC エミュレータをイネーブルにします。
 - [接続数 (Connections)] : 0 から 100 までの接続数を入力します。
- ステップ 8** [次へ (Next)] をクリックして、FCIP ISL を作成します。
- ステップ 9** スイッチペアの[プロファイル ID (Profile ID)] と[トンネル ID (Tunnel ID)] を入力し、ドロップダウンリストから [FICON ポートアドレス (FICON Port Address)] を選択します。
- ステップ 10** [設定の表示 (View Configured)] をクリックして、[プロファイル (Profiles)] と[トンネル (Tunnels)] の情報を表示します。

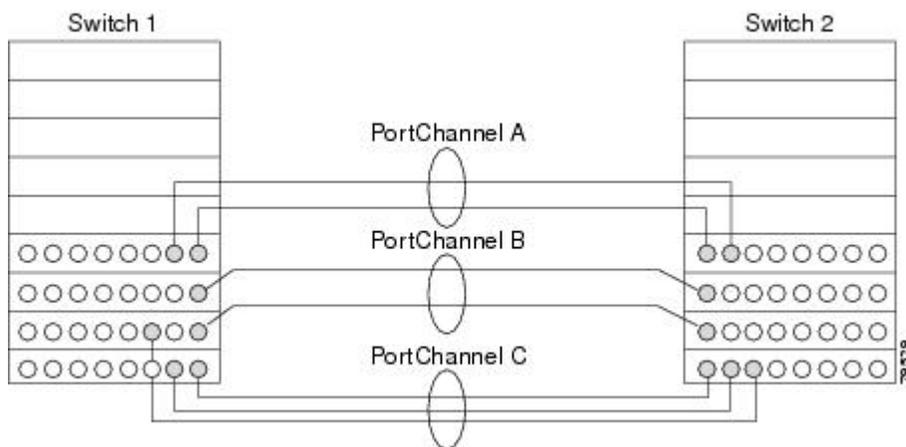
- ステップ11 トランクモード (Trunk Mode) を [非トランク (non-Trunk)]、[トランク (trunk)]、[自動 (auto)] から選択します。[Port VSAN (Port VSAN)] を [非トランク (non-Trunk)] および [自動 (auto)] に指定し、許可 VSAN リスト (VSANList) をトランクトンネルに指定します。
- ステップ12 [次へ (Next)] をクリックして最後の [概要 (Summary)] ページを表示します。
[概要 (Summary)] ビューには、前の手順で選択したものが表示されます。
- ステップ13 [終了 (Finish)] をクリックして FCIP を設定します。

ポートチャネル

ポートチャネルの概要

ポートチャネルは、複数の物理インターフェイスを1つの論理インターフェイスに集約し、より精度の高い集約帯域幅、ロードバランシング、およびリンク冗長性を提供する機能です (下図を参照)。ポートチャネルはスイッチングモジュール間のインターフェイスに接続することができるため、スイッチングモジュールで障害が発生してもポートチャネルのリンクがダウンすることはありません。

図 1: ポートチャネルの柔軟性



Cisco MDS 9000 ファミリスイッチのポートチャネルは柔軟に設定できます。これは、3つの可能なポートチャネル設定を示しています。

- ポートチャネル A は、接続の両端が同一のスイッチングモジュール上にある、2つのインターフェイスの2つのリンクを集約します。
- ポートチャネル B も2つのリンクを集約しますが、各リンクは別々のスイッチングモジュールに接続されています。スイッチングモジュールがダウンしても、トラフィックは影響されません。
- ポートチャネル C は3つのリンクを集約します。そのうち2つのリンクは両端が同一のスイッチングモジュール上にあり、1つのリンクはスイッチ1で別々のスイッチングモジュールに接続されています。

ポートチャネルおよびトランキング

トランキングは、ストレージ業界で一般的に使用されている用語です。ただし、Cisco NX-OS ソフトウェアおよび Cisco MDS 9000 ファミリー スイッチでは、トランキングとポートチャネルを次のように実装します。

- ポートチャネルでは、複数の物理リンクを1つの集約論理リンクに組み合わせることができます。
- トランキングでは、EISL 形式のフレームを送信しているリンクで複数の VSAN トラフィックを伝送（トランク）できます。たとえば、E ポートでトランキングを動作させると、その E ポートは TE ポートになります。TE ポートは、Cisco MDS 9000 ファミリー スイッチ特有のもので、業界標準の E ポートは他のベンダーのスイッチにリンクでき、非トランキングインターフェイスと呼ばれます（[図 2: トランキングだけ](#)（110 ページ） および [図 3: ポートチャネルおよびトランキング](#)（110 ページ）を参照）。

図 2: トランキングだけ

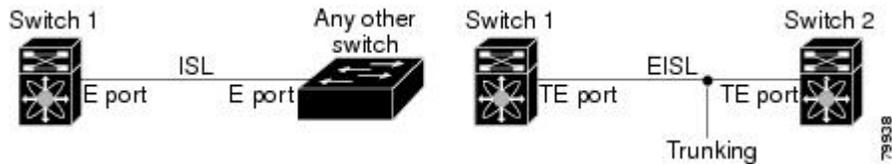
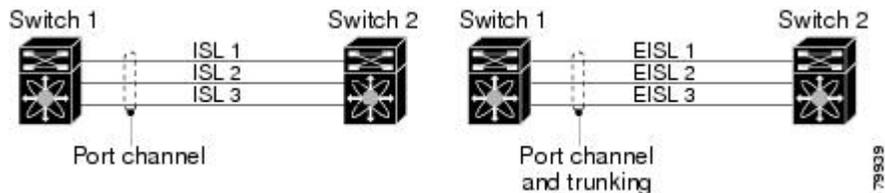


図 3: ポートチャネルおよびトランキング



ポートチャネルとトランキングは、ISL で別々に使用されます。

- ポートチャネル：次のポートの組み合わせの間でインターフェイスをチャネリングできます。
 - E ポートおよび TE ポート
 - F ポートおよび NP ポート
 - TF ポートおよび TNP ポート
- トランキング：トランキングでは、スイッチ間で複数の VSAN のトラフィックが伝送されます。
- TE ポート間では、EISL でポートチャネルとトランキングを使用できます。

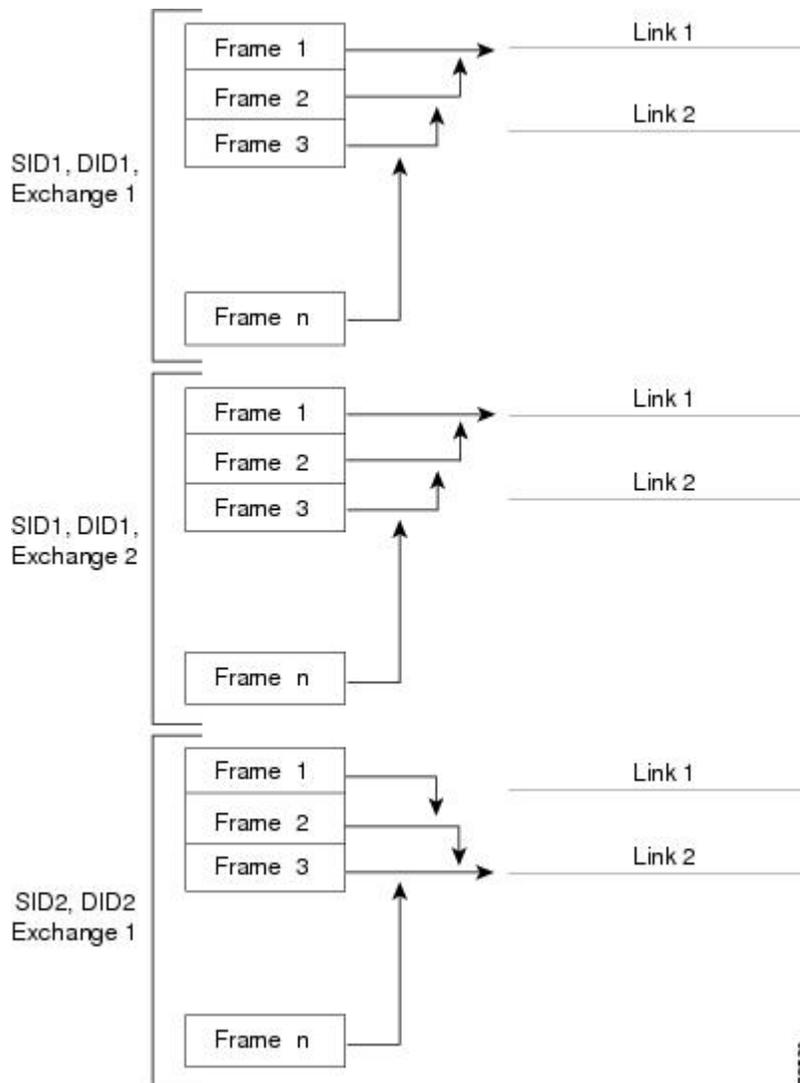
ロードバランシング

次の 2 つの方法でロードバランシング機能がサポートされます。

- フローベース：送信元と接続先間のすべてのフレームが所定のフローで同一のリンクをたどります。つまり、フローの最初のエクスチェンジで選択されたリンクが、後続のすべてのエクスチェンジで使用されます。
- エクスチェンジベース：エクスチェンジの最初のフレームがリンクを選択し、エクスチェンジのその後のフレームは同じリンクを流れます。ただし、後続のエクスチェンジは、別のリンクを使用できます。これにより、やり取りごとにフレームの順序を維持しながら、より細かいロードバランシングが可能になります。

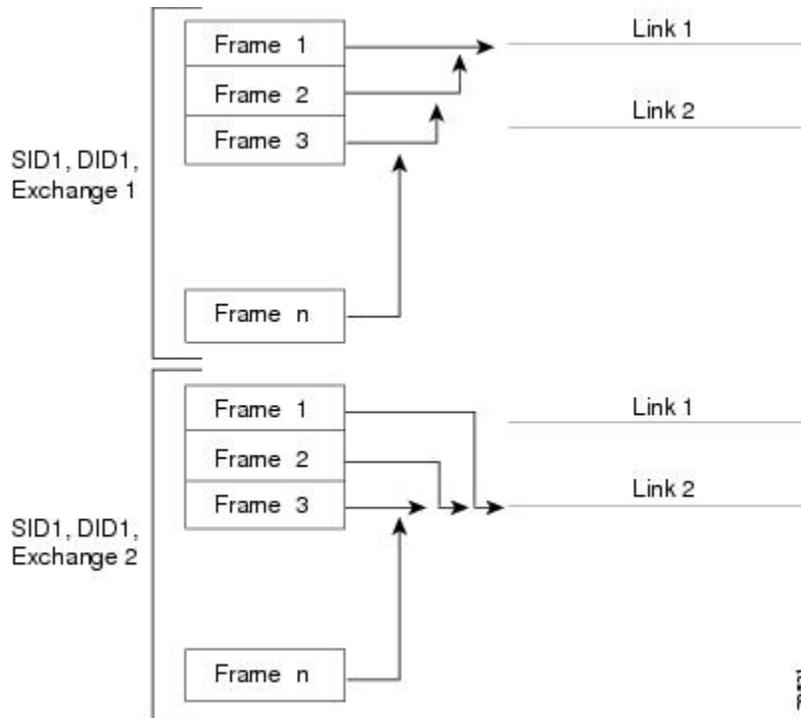
次の図に、送信元 ID 1 (SID1) と接続先 ID1 (DID1) を基準とするロードバランシングの動作を示します。フローの最初のフレームが転送のためにインターフェイスで受信されると、リンク 1 が選択されます。そのフローの各後続のフレームが、同一のリンク上に送信されます。SID1 および DID1 のフレームは、リンク 2 を使用しません。

図 4: SID1 および DID1 を基準としたロードバランシング



次の図は、エクスチェンジベースのロードバランシングがどのように機能するかを示しています。エクスチェンジで最初のフレームが転送用にインターフェイスで受信されると、リンク 1 がハッシュアルゴリズムによって選択されます。その特定のエクスチェンジにある残りすべてのフレームが同一のリンクに送信されます。エクスチェンジ 1 では、リンク 2 を使用するフレームはありません。次のエクスチェンジでは、ハッシュアルゴリズムによってリンク 2 が選択されます。ここではエクスチェンジ 2 のすべてのフレームが、リンク 2 を使用します。

図 5: SID1、DID1、およびエクスチェンジベースのロードバランシング



ポートチャネルモード

チャネルグループのモードパラメータで各ポートチャネルを設定し、このチャネルグループのすべてのメンバーポートでポートチャネルプロトコル動作を決めることができます。チャネルグループモードに指定できる値は、次のとおりです。

- **ON (デフォルト)** : メンバーポートはポートチャネルの一部として動作するか、非アクティブになります。このモードでは、ポートチャネルプロトコルは起動されません。ただし、ポートチャネルプロトコルフレームをピアポートから受信した場合、ソフトウェアはネゴシエーション不能ステータスを示します。このモードには、チャネルグループモードが暗黙的に ON になっている Release 2.0(1b) 以前で、既存のポートチャネルの実装と下位互換性があります。4763 Cisco MDS SAN-OS Release 1.3 以前で使用可能なポートチャネルモードは ON モードだけです。オンモードで設定されたポートチャネルでは、ポートチャネルの設定に対してポートの追加または削除を行う場合、各端のポートチャネルメンバーポートを明示的にイネーブルおよびディセーブルに設定する必要があります。また、ローカルポートおよびリモートポートが相互に接続されていることを物理的に確認する必要があります。

- **ACTIVE** : ピアポートのチャネルグループモードに関係なく、メンバーポートはピアポートとポートチャネルプロトコルネゴシエーションを始めます。チャネルグループで設定されているピアポートがポートチャネルプロトコルをサポートしていない場合、またはネゴシエーション不可能なステータスを返す場合、デフォルトでオンモードの動作に設定されます。ACTIVEポートチャネルモードでは、片側でポートチャネルメンバーのポートの有効化および無効化を明示的に行わなくても、自動回復が可能です。

次の表は、ONモードとACTIVEモードを比較したものです。

表 15: チャネルグループ設定の相違点

ON モード	ACTIVE モード
プロトコルは交換されません。	ピアポートとポートチャネルプロトコルネゴシエーションを行います。
動作値にポートチャネルとの互換性がない場合、インターフェイスは中断状態になります。	動作値にポートチャネルとの互換性がない場合、インターフェイスは分離状態になります。
ポートチャネルメンバーポート設定の追加または変更を行うとき、片側のポートチャネルメンバーポートのディセーブル化 (shut) およびイネーブル化 (no shut) を明示的に行う必要があります。	ポートチャネルインターフェイスを追加または変更すると、SANポートチャネルは自動的に復旧します。
ポートの起動は同期化されません。	すべてのピアスイッチで、チャネル内のすべてのポートの起動が同時に行われます。
プロトコルが交換されないため、すべての誤設定が検出される訳ではありません。	ポートチャネルプロトコルが使用され、誤設定が確実に検出されます。
誤設定ポートを中断ステートに移行します。各端でメンバーポートを明示的にディセーブル (shut) およびイネーブル (no shut) に設定する必要があります。	誤設定を修正するために、誤設定ポートを隔離ステートに移行します。誤設定を修正すれば、プロトコルによって自動的に復旧されます。

ポートチャネルの削除

ポートチャネルを削除すると、対応するチャネルメンバーシップも削除されます。削除したポートチャネルのすべてのインターフェイスは、個別の物理リンクに変換されます。ポートチャネルの削除後、使用するモード (ACTIVE および ON) に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します。

あるポートのポートチャネルを削除すると、削除したポートチャネル内の各ポートは互換性のあるパラメータ設定 (速度、モード、ポート VSAN、許可されている VSAN、ポートセキュリティ) を維持します。これらの設定は、必要に応じて、明示的に変更できます。

- スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブモードを使用する場合、ポートチャネルポートは削除から自動的に回復します。

ポートチャネルのインターフェイス

既存ポートチャネルで物理インターフェイス（またはある範囲のインターフェイス）の追加または削除を行うことができます。設定で互換性があるパラメータはポートチャネルにマッピングされます。ポートチャネルにインターフェイスを追加すると、ポートチャネルのチャネルサイズおよび帯域幅が増加します。ポートチャネルからインターフェイスを削除すると、ポートチャネルのチャネルサイズおよび帯域幅が減少します。

ここでは、ポートチャネルのインターフェイス設定について説明します。ここで説明する内容は、次のとおりです。

ポートチャネルへのインターフェイスの追加

既存ポートチャネルに物理インターフェイス（またはある範囲のインターフェイス）を追加できます。設定で互換性があるパラメータはポートチャネルにマッピングされます。ポートチャネルにインターフェイスを追加すると、ポートチャネルのチャネルサイズおよび帯域幅が増加します。

ポートとポートチャネルで次の構成が同じ場合にのみ、ポートを静的ポートチャネルのメンバーとして構成できます。

- スピード
- モード
- レート モード
- ポート VSAN
- トランッキング モード
- 許可 VSAN リストまたは VF-ID リスト

メンバーの追加後、使用するモード（ACTIVE および ON）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します（12 ページの「第 1 世代ポートチャネルの制限事項」セクションを参照）。

互換性チェック

互換性チェックでは、チャネルのすべての物理ポートで同一のパラメータ設定が確実に使用されるようにします。そうでない場合、ポートがポートチャネルに所属できません。互換性チェックは、ポートをポートチャネルに追加する前に実施します。

互換性チェックでは、ポートチャネルの両側で次のパラメータと設定が一致していることを確認します。

- 機能パラメータ（インターフェイスのタイプ、両端のギガビットイーサネット、両端のファイバチャネル）。
- 管理上の互換性パラメータ（速度、モード、レートモード、ポート VSAN、許可 VSAN リスト、およびポートセキュリティ）



(注) 共有レートモードのポートではポートチャネルやトランキン
グポートチャネルを形成できません。

- 動作パラメータ（リモートスイッチ WWN およびトランキングモード）

リモートスイッチの機能パラメータと管理パラメータおよびローカルスイッチの機能パラメータと管理パラメータに互換性がない場合、ポートは追加できません。互換性チェックが正常であれば、インターフェイスは正常に動作し、対応する互換性パラメータ設定がこれらのインターフェイスに適用されます。

中断および隔離ステート

動作パラメータに互換性がない場合、互換性チェックは失敗し、インターフェイスは設定されたモードに基づいて中断ステートまたは隔離ステートになります。

- インターフェイスは、ON モードに設定されている場合、一時停止状態になります。
- インターフェイスは、ACTIVE モードに設定されている場合、分離状態になります。

インターフェイスの強制追加

ポートチャネルにより、ポート設定の上書きを強制することができます。この場合、インターフェイスはポートチャネルに追加されます。

- スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- ACTIVE モードを使用する場合、ポートチャネルポートは追加から自動的に回復します。



(注) インターフェイス内からポートチャネルを作成するときは、force オプションを使用できません。

メンバーの強制追加後、使用するモード（ACTIVE および ON）に関係なく、片側のポートは正常にダウンします。これは、インターフェイスがダウンしてもフレームが失われないことを示します。

ポートチャネルからのインターフェイスの削除

物理インターフェイスをポートチャネルから削除すると、チャネルメンバーシップは自動的に更新されます。削除されたインターフェイスが最後の動作可能なインターフェイスである場合は、ポートチャネルのステータスは、ダウン状態に変更されます。ポートチャネルからインターフェイスを削除すると、ポートチャネルのチャネルサイズおよび帯域幅は減少します。

- スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。これらのポートは再度明示的にイネーブルにする必要があります。
- アクティブモードを使用する場合、ポートチャネルポートは削除から自動的に回復します。

メンバーを削除すると、使用されているモード（アクティブおよびオン）に関係なく、各端のポートが正常にシャットダウンされます。これは、インターフェイスのシャットダウン時にフレームが失われないことを意味します。

ポートチャネルプロトコル

Cisco SAN-OS の前バージョンでは、ポートチャネルで同期をサポートするために管理作業がさらに必要となっていました。Cisco NX-OS ソフトウェアには、強力なエラー検出機能および同期機能があります。チャネルグループを手動で設定できますが、自動的に作成することもできます。どちらの場合でも、チャネルグループの機能および設定可能なパラメータは同じです。対応付けられたポートチャネルインターフェイスに適用される設定の変更は、チャネルグループ内のすべてのメンバーに伝播されます。

ポートチャネル設定をやり取りするプロトコルは、すべての Cisco MDS スイッチで使用できます。この追加機能により、非互換 ISL でのポートチャネル管理が簡単になります。追加された自動作成モードでは、互換性のあるパラメータを持つ ISL でチャネルグループを自動的に作成でき、手動での作業は必要ありません。

デフォルトではポートチャネルプロトコルがイネーブルになっています。

ポートチャネルプロトコルにより、Cisco MDS スイッチにおけるポートチャネル機能モデルが拡張されます。ポートチャネルプロトコルは、Exchange Peer Parameters (EPP) サービスを使用して、ISL のピアポート間の通信を行います。各スイッチは、ピアポートから受信した情報、およびローカル設定と動作値を使用し、それがポートチャネルの一部であるかどうかを判断します。このプロトコルでは、一連のポートが確実に同一ポートチャネルの一部になります。すべてのポートが互換性のあるパートナーを持つ場合だけ、ポート一式が同一のポートチャネルに属せます。

ポートチャネルプロトコルでは、次の 2 つのプロトコルが使用されます。

- 起動プロトコル：自動的に誤設定を検出するため、これらを修正できます。このプロトコルでは両側でポートチャネルが同期されるので、特定フローのすべてのフレーム（送信元 FC ID、宛先 FC ID、OX_ID によって識別）は両方向で同一の物理リンクによって伝送されます。これにより、書き込みアクセラレーションのようなアプリケーションが、FCIP リンクでポートチャネル用に動作するようになります。
- 自動作成プロトコル：互換性があるポートがポートチャネルに自動的に集約されます。

ここでは、ポートチャネルプロトコルの設定方法について説明します。ここで説明する内容は、次のとおりです。

チャネルグループの作成



- (注) HP c-Class BladeSystem 用シスコ ファブリック スイッチおよび IBM BladeSystem 用シスコ ファブリック スイッチの内部ポートでは、チャネルグループがサポートされません。

リンク A1-B1 が最初にアップすると仮定すると (図 1-9 を参照)、そのリンクは個別のリンクとして動作します。次のリンク (たとえば A2-B2) がアップすると、ポートチャネルプロトコルは、このリンクがリンク A1-B1 と互換性があるかどうかを識別し、それぞれのスイッチでチャネルグループ 10 および 20 を自動的に作成します。リンク A3-B3 がチャネルグループ (ポートチャネル) に参加できるということは、それぞれのポートに互換性の設定があるということです。リンク A4-B4 が個別リンクとして動作するという事は、このチャネルグループのその他のメンバーポートとの互換性が、2つのエンドポート設定にないということです。

チャネルグループ番号は動的に選択され、片側でチャネルグループを形成するポートの管理上の設定は、新しく作成されるチャネルグループに適用可能となります。動的に選択されるチャネルグループ番号は、スイッチでポートが初期化される順序に基づくので、同一セットのポートチャネルでも、リポートすると異なることがあります。

次の表に、ユーザー設定のチャネルグループと自動設定のチャネルグループの相違点を示します。

ユーザ設定のチャネルグループ	自動設定のチャネルグループ
ユーザが手動で設定します。	2つの互換性のあるスイッチ間で互換性のあるリンクがアップしたときに自動的に作成されます (両端のすべてのポートでチャネルグループの自動作成がイネーブルになっている場合)。
メンバーポートはチャネルグループの自動作成には参加できません。自動作成機能は設定できません。	これらのポートは、ユーザー設定のチャネルグループのメンバーにはなりません。
チャネルグループのポートのサブセットでポートチャネルを形成できます。互換性がないポートは、ON モード設定または ACTIVE モード設定により、一時停止状態か分離状態になります。	チャネルグループに組み込まれるすべてのポートがポートチャネルに参加します。メンバーポートが分離状態や一時停止状態になることはありません。リンクに互換性がない場合、そのメンバーポートはチャネルグループから削除されます。
ポートチャネルで行った管理上の設定はチャネルグループのすべてのポートに適用され、ポートチャネルインターフェイスの設定は保存できます。	ポートチャネルで行った管理上の設定はチャネルグループのすべてのポートに適用されますが、メンバーポートの設定は保存され、ポートチャネルインターフェイスの設定は保存されません。このチャネルグループは、必要に応じて明示的に変更できます。

ユーザ設定のチャネルグループ	自動設定のチャネルグループ
任意のチャネルグループの削除およびチャネルグループへのメンバの追加が可能です。	チャネルグループは削除できません、メンバーの追加や削除もできません。メンバポートが存在しない場合、チャネルグループは削除されます。

自動作成

自動作成プロトコルには次の機能があります。

- 自動作成機能をイネーブルにした場合、ポートはポートチャネルの一部として設定できません。これらの2つの設定を同時に使用できません。
- 自動作成は、ポートチャネルをネゴシエーションするため、ローカルポートとピアポートの両方でイネーブルにする必要があります。
- 集約は、次の2通りの方法で実行されます。
 - 互換性のある自動作成ポートチャネルにポートが集約されます。
 - 互換性がある別のポートにポートが集約され、新しいポートチャネルが形成されます。
- 新しく作成されたポートチャネルは、可用性に基づいて大きいものから順に最大のポートチャネル（第1世代スイッチまたは第1世代スイッチと第2世代スイッチの組み合わせの場合は128、第2世代スイッチの場合は256）から割り当てられます。128または256の番号すべてが使用されている場合、集約は行われません。
- メンバーシップの変更または自動作成されたポートチャネルの削除はできません。
- 自動作成を無効化すると、すべてのメンバーポートは自動作成ポートチャネルから削除されます。
- 最後のメンバーが自動作成ポートチャネルから削除されると、チャネルは自動的に削除され、番号は解放されて再利用されます。
- 自動作成ポートチャネルは、リブート後に維持されません。自動作成されたポートチャネルは、手動で設定することにより、永続的なポートチャネルと同じように表示させることができます。ポートチャネルを持続させた場合、自動作成機能はすべてのメンバーポートでディセーブルになります。
- 自動作成機能は、ポート単位またはスイッチ内のすべてのポートに対して、イネーブルまたはディセーブルに設定できます。この設定がイネーブルの場合、チャネルグループモードはアクティブと見なされます。このタスクのデフォルトはディセーブルです。
- インターフェイスに対してチャネルグループの自動作成がイネーブルになっている場合、最初に自動作成をディセーブルにしてから、以前のソフトウェアバージョンにダウングレードするか、または手動設定されたチャネルグループでインターフェイスを設定する必要があります。



- (注) Cisco MDS 9000 ファミリの任意のスイッチで自動作成をイネーブルにする場合は、スイッチ間の最低 1 つの相互接続ポートで自動作成を設定しないことを推奨します。2 つのスイッチ間のすべてのポートを自動作成機能で同時に設定すると、自動作成ポートチャネルにポートが追加されるとき、ポートが自動的にディセーブルになって再度イネーブルになるので、この 2 つのスイッチ間でトラフィックが混乱することがあります。

手動設定チャネルグループ

ユーザによって設定されたチャネルグループを自動作成チャネルグループに変更できません。ただし、自動作成されたチャネルグループから手動チャネルグループへの変更は可能です。このタスクは、実行すると元に戻すことはできません。チャネルグループ番号は変化しませんが、メンバーポートは手動設定チャネルグループのプロパティに従って動作し、チャネルグループの自動作成はすべてのメンバーポートで暗黙的にディセーブルになります。



ヒント 持続をイネーブルにする場合は、ポートチャネルの両側でイネーブルにしてください。

ポートチャネルの設定の前提条件

ポートチャネルを設定する前に、次の注意事項を守ってください。

- スイッチングモジュール間でポートチャネルを設定し、スイッチングモジュールのリブートまたはアップグレードの際の冗長性を実装してください。
- 1 つのポートチャネルをさまざまなセットのスイッチに接続しないでください。ポートチャネルでは、同一セットのスイッチ間におけるポイントツーポイント接続が必要です。

第 1 世代スイッチングモジュールを含むか、第 1 世代および第 2 世代のスイッチングモジュールを含むスイッチでは、最大で 128 のポートチャネルを設定できます。第 2 世代スイッチングモジュールを含むか、第 2 世代および第 3 世代のスイッチングモジュールを含むスイッチでは、最大で 256 のポートチャネルを設定できます。

ポートチャネルの設定を誤った場合は、誤設定メッセージを受信することがあります。このメッセージを受信した場合、エラーが検出されたため、ポートチャネルの物理リンクはディセーブルになります。

ポートチャネルのエラーは、次の要件を満たしていない場合に検出されます。

- ポートチャネルの両端のスイッチが、同じ数のインターフェイスに接続されている必要があります。
- 各インターフェイスは、対応する反対側のインターフェイスに接続される必要があります（無効な設定例については、図 1-11 を参照してください）。
- ポートチャネルの設定後に、ポートチャネルのリンクは変更できません。ポートチャネルの設定後にリンクを変更する場合は、ポートチャネル内のインターフェイスにリンクを再接続してリンクを再びイネーブルにします。

3 つすべての条件が満たされていない場合、そのリンクはディセーブルになっています。

そのインターフェイスに `show interface` コマンドを入力して、ポートチャネルが設定どおりに機能していることを確認します。

ポートチャネルの設定に関するガイドラインと制約事項

この項では、この機能のガイドラインと制限事項について説明します。

Cisco MDS 9000 シリーズスイッチの一般的なガイドライン

Cisco MDS 9000 ファミリスイッチは、スイッチごとに次の数のポートチャネルをサポートします。

- 第 1 世代のスイッチングモジュールのみを含むスイッチは、F ポートチャネルおよび TF ポートチャネルをサポートしません。
- 第 1 世代スイッチングモジュールを含むか、第 1 世代および第 2 世代のスイッチングモジュールを含むスイッチでは、最大で 128 のポートチャネルがサポートされます。第 2 世代のポートのみをポートチャネルに組み込むことができます。
- 第 2 世代のスイッチングモジュールを含むか、第 2 世代および第 3 世代のスイッチングモジュールを含むスイッチでは、ポートチャネルごとに最大で 16 インターフェイスで 256 のポートチャネルがサポートされます。
- ポートチャネル番号は、各チャネルグループの一意の識別番号です。この番号の範囲は 1 ~ 256 です。

第 1 世代ポートチャネルの制限事項

ここでは、次の第 1 世代ハードウェアのポートチャネルにポートチャネルメンバーを作成および追加する場合の制約事項について説明します。

- 32 ポートの 2 Gbps または 1 Gbps スイッチングモジュール
- MDS 9140 および 9120 スイッチ。

第 1 世代ハードウェアのホスト最適化ポートを設定する場合は、ポートチャネルに関する次の注意事項が適用されます。

- 32 ポート スイッチングモジュールで `write erase` コマンドを実行し、`no system default switchport shutdown` コマンドを含むテキストファイルからスイッチに保存済み設定をコピーする場合、手動設定せずに E ポートをアップさせるには、テキストファイルをスイッチに再度コピーする必要があります。
- Cisco MDS 9100 シリーズの任意の（またはすべての）フル回線レートポートをポートチャネルに組み込むことができます。
- Cisco MDS 9100 シリーズのホスト最適化ポートは、32 ポート スイッチングモジュールと同じポートチャネルのルールに従います。各 4 ポートグループの最初のポートだけがポートチャネルに組み込まれます。

- 各 4 ポートのグループの最初のポートだけを E ポートとして設定できます (ポート 1 ~ 4 の最初のポート、ポート 5 ~ 8 の 5 のポートなど)。そのグループの最初のポートがポートチャネルとして設定された場合は、各グループのその他 3 つのポート (ポート 2 ~ 4、6 ~ 8 など) は使用できず、シャットダウンステートのままになります。
- その他 3 つのポートのいずれかがシャットダウンステート以外で設定されている場合は、最初のポートをポートチャネルとして設定できません。その他 3 つのポートは、引き続きシャットダウンステート以外になります。

F および TF ポートチャネルの制限事項

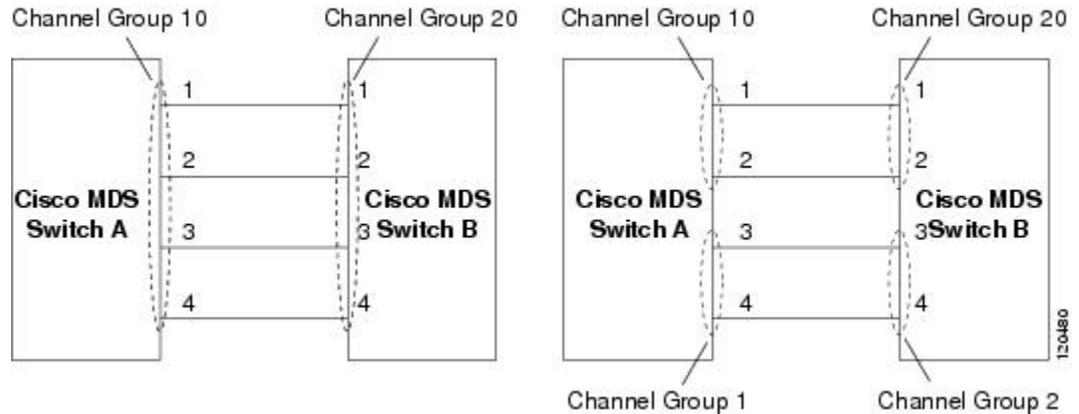
F ポートチャネルおよび TF ポートチャネルには、次の注意事項と制約事項が適用されます。

- ポートを F モードとしておく必要があります。
- 自動作成はサポートされません。
- 複数の FCIP インターフェイスを WA でグループ化する場合は、ポートチャネル インターフェイスが ACTIVE モードである必要があります。
- ON モードはサポートされません。サポートされるのは ACTIVE-ACTIVE モードだけです。デフォルトでは、NPV スイッチのモードは ACTIVE です。
- MDS スイッチの F ポートチャネル経由でログインしたデバイスは、IVR の非 NAT 設定でサポートされません。このデバイスをサポートするのは IVR NAT 設定だけです。
- ポートセキュリティルールは、物理 pWWN だけで単一リンクレベルで実行されます。
- FC-SP では、ポートチャネルのメンバーごとに最初の物理 FLOGI だけを認証します。
- FLOGI ペイロードは VF ビットだけを伝送して FLOGI 交換後にプロトコルの使用をトリガーするため、このビットは上書きされます。NPV スイッチの場合は、コアに Cisco WWN が設定されているので PCP プロトコルの開始を試行します。
- F ポートチャネル経由でログインする N ポートのネームサーバー登録では、ポートチャネル インターフェイスの fWWN を使用します。
- DPVM 設定はサポートされません。
- ポートチャネルのポート VSAN は DPVM を使用して設定できません。
- Dynamic Port VSAN Management (DPVM) データベースの問い合わせは各メンバーの最初の物理 FLOGI についてだけ行われるため、ポート VSAN は自動的に設定されます。
- DPVM では FC_ID を VSAN にバインドしませんが、pWWN を VSAN にバインドします。問い合わせが行われるのは物理 FLOGI についてだけです。

有効なポートチャネルと無効なポートチャネルの例

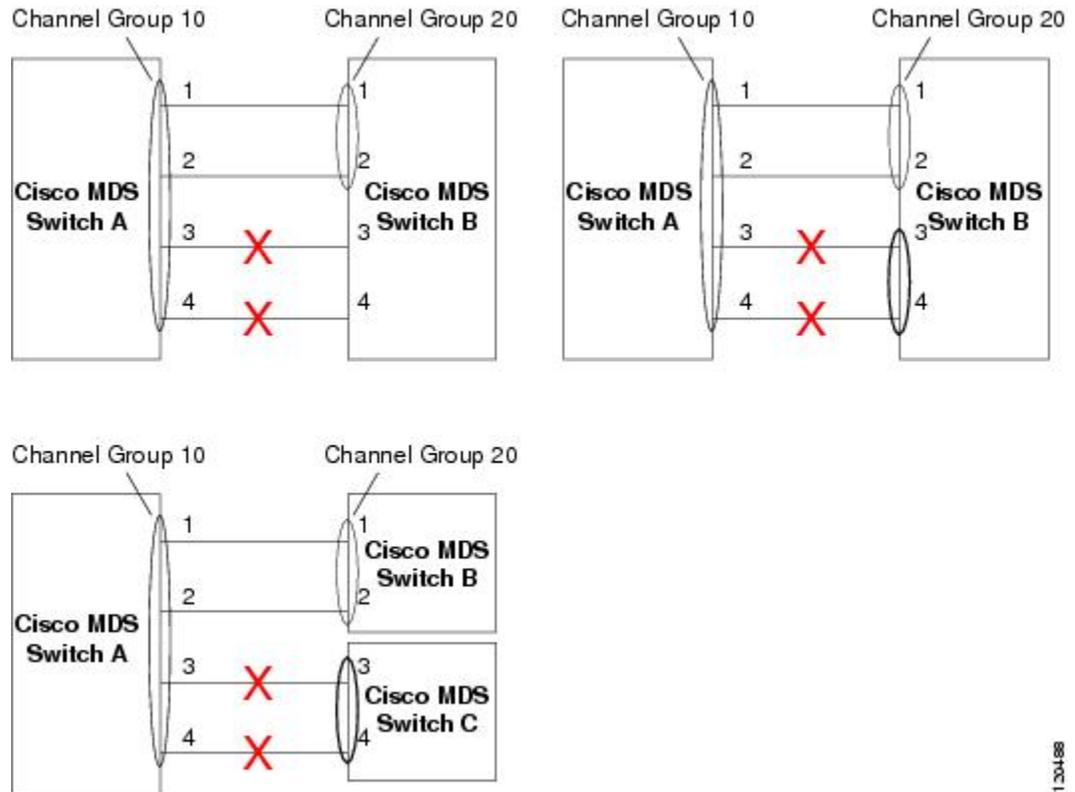
ポートチャネルは、デフォルト値で作成されます。その他の物理インターフェイスと同じように、このデフォルト設定を変更できます。次の図は、有効なポートチャネルの設定例を示しています。

図 6: 有効なポートチャネルの設定



次の図は、有効な設定例を示しています。リンクが1、2、3、4の順番でアップした場合、ファブリックの設定が誤っているため、リンク3および4は動作上ダウンします。

図 7: 誤った設定



デフォルト設定

次の表に、ポートチャネルのデフォルト設定を示します。

表 16: デフォルト SAN ポートチャネルパラメータ

パラメータ	デフォルト
ポートチャネル	FSPF はデフォルトでイネーブルになっています。
ポートチャネルの作成	管理上のアップ状態
デフォルトポートチャネルモード	ON モード (非 NPV スイッチおよび NPIV コア スイッチ)。 ACTIVE モード (NPV スイッチ)
自動作成	ディセーブル

[Create Port Channel] ウィザード

Nexusダッシュボードファブリックコントローラ Web UI で新しいポートチャネルの作成ウィザードを使用してポートチャネルを作成するには、次の手順を実行します。

手順

- ステップ 1** [新しいポートチャネルの作成 (Create a new Port Channel)] を [アクション (Actions)] ドロップダウンリストから選択します。
- [新しいポートチャネルの作成 (Create New Port Channel)] をクリックして、ポートチャネルの作成ウィザードを起動します。
- ステップ 2** [スイッチペアの選択 (Select Switch Pair)] 画面で、次の手順を実行します。
- [ファブリック (Fabric)] ドロップダウンから適切なファブリックを選択します。
このリストには、ポートチャネルにまだ存在しない、間に ISL があるファブリック内のスイッチペアが含まれています。
 - FC ポートチャネルでリンクするスイッチペアを選択します。
NPIV コアと NPV スイッチの間に NPV リンクがある場合、スイッチペアと NPV リンクの数を表示するには、NPIV スイッチで **feature fport-channel-trunk** コマンドを使用して F ポートトランッキングとチャネリングプロトコルを有効にする必要があります
 - [次へ (Next)] をクリックします。
- ステップ 3** [ISL の選択 (Select ISLs)] 画面で、1 つ以上の ISL またはリンクを選択して、スイッチペア間に新しいチャネルを作成します。
- [利用可能 (Available)] エリアの ISL のリストから、右矢印を選択してクリックし、ISL を [選択済み (Selected)] エリアに移動します。
 - [次へ (Next)] をクリックします。

ステップ4 [チャンネルの設定 (Configure Channel)] 画面で、チャンネル属性を定義または編集します。

- a) [チャンネルID (ChannelID)] フィールドには、次の未使用のチャンネルIDが入力されます。必要に応じて、各スイッチのチャンネルIDまたは説明を変更します。
チャンネルIDの範囲は1～256です。
- b) FICONポートアドレスは、スイッチでFICONが有効になっている場合にのみ有効です。ドロップダウンリストから、スイッチの適切なFICONポートアドレスを選択します。ポートチャンネルポートに割り当てるポートアドレスを選択します。
- c) [Channel Attributes (チャンネル属性)] エリアで、速度を設定するには、適切なオプションボタンをクリックします。
- d) 適切な[トランクモード (Trunk Mode)] オプションボタンを選択して、ポートチャンネルのリンクでトランキングを有効にします。
 - TEポート間にリンクが存在する場合は、[トランク (trunk)] を選択します。
 - Eポート間にリンクが存在する場合は、[nonTrunk] を選択します。
 - 不明な場合は、[自動 (auto)] を選択します。
- e) [ポートVSAN (Port VSAN)] フィールドに、トランキングが有効になっていない場合に使用する必要があるポートVSANのインターフェイスIDを入力します。
トランキングが有効になっている場合でも、すべてのインターフェイスにはポートVSANが必要です。トランキングが有効になっている場合、このポートVSANは使用されません。ただし、トランキングが無効になっている場合に、ネットワークがデフォルトで使用するVSANを認識できるように、スイッチはポートを設定する必要があります。
- f) VSANリストフィールドには、ポートチャンネルがトランキングに使用できるようにするVSANのリストが表示されます。
トランクモードが[nonTrunk]または[自動 (auto)]に設定されている場合、このフィールドは無効になります。
- g) [コアスイッチ帯域幅 (Core Switch Bandwidth)] フィールドで、専用または共有オプションボタンを選択して、スイッチの帯域幅を割り当てます。
この帯域幅は、NPIVスイッチとNPVスイッチ間のポートチャンネルにのみ適用されます。
- h) [管理の強制 (Force Admin)]、[トランク (Trunk)]、[速度 (Speed)]、および[VSAN属性を一致させる (VSAN attributes to be identical)] チェックボックスをオンにして、チャンネルのすべての物理ポートで同じパラメータ設定が使用されるようにします。これらの設定が同じでない場合、ポートはポートチャンネルに属することができません。

ステップ5 [前へ (Previous)] をクリックして前の画面に戻り、設定を編集します。[新しいポートチャンネルの作成 (Create New Port Channel)] をクリックして、ポートチャンネルを設定します。

処理が正常に完了したことを知らせるメッセージが表示されます。

既知のポートチャネルの編集

Nexusダッシュボード ファブリック コントローラ Web UI でポートチャネルの編集ウィザードを使用してポートチャネルを編集するには、次の手順を実行します。

手順

-
- ステップ 1** [ポートチャネルの編集 (Edit Port Channel)] を [アクション (Actions)] ドロップダウンリストから選択します。
- [ポートチャネルの編集 (Edit Port Channel)] をクリックして、ポートチャネルの作成ウィザードを起動します。
- ステップ 2** [スイッチペアの選択 (Select Switch Pair)] 画面で、次の作業を実行します。
- [ファブリック (Fabric)] ドロップダウンリストから適切なファブリックを選択します。
間にポートチャネルがあるスイッチペアは、以下のエリアにリストされています。
 - ポートチャネルを編集するスイッチペアを選択します。
 - [次へ (Next)] をクリックします。
- ステップ 3** [ポートチャネルの選択 (Select Port Channel)] 画面で、編集するポートチャネルを選択します。
- [次へ (Next)] をクリックします。
- ステップ 4** [ポートチャネルの編集 (Edit Port Channel)] 画面で、目的の ISL を選択します。
- 左右の矢印をクリックして、使用可能な ISL を選択します。
(注) 変更を保存すると、選択した ISL がポートチャネルに含まれます。選択した ISL リストが空の場合、[ポートチャネルの削除が空です (Delete Port Channel is Empty)] チェックボックスが有効になります。
 - ISL を選択しない場合は、[ポートチャネルが空の場合、削除する (Delete Port Channel If Empty)] チェックボックスをオンにして、ポートチャネルを削除します。
 - [管理の強制 (Force admin)]、[トランク (Trunk)]、[速度 (speed)]、[VSAN 属性を同一にする (VSAN attributes to be identical)] チェックボックスをオンにして、管理、トランク、速度、および VSAN 属性に同一の値を選択します。
 - [次へ (Next)] をクリックします。
- ステップ 5** [ポートチャネルの保存 (Save port channel)] をクリックして変更を適用します。
-

NPV Links

NPV リンクウィンドウが表示されます。この表は、SAN ファブリック上の NPV リンクのパフォーマンスを示しています。ドロップダウンを使用して、24時間、週、月、および年でビューをフィルタ処理できます。

ドロップダウンを使用して、**24 時間、週、月、および年**でビューをフィルタ処理できます。

[名前 (Name)]列の**[チャート (chart)]**アイコンをクリックし、過去 24 時間のトラフィックのリストを表示します。

他にもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行して NPV リンクの詳細情報を表示することもできます。

- この情報の時間範囲を変更するには、右上の隅のドロップダウンリストから選択します。
- 期間を指定して詳細情報を表示するには、スライダーコントロールをドラッグして、表示する期間を指定します。
- チャートアイコンを使用して、さまざまなビューでトラフィックチャートを表示します。アイコンを使用して、データを **[追加 (Append)]**、**[予測 (Predict)]**、および **[補間 (Interpolate)]**することもできます。
- スプレッドシートにデータをエクスポートするには、右上の隅の**[エクスポート (Export)]**アイコンをクリックしてから**[保存 (Save)]**をクリックします。
- リアルタイム情報を表示するには、**[チャート (Chart)]**メニューの**[リアルタイム (Real Time)]**を選択します。



第 8 章

インターフェイス

・ [インターフェイス \(127 ページ\)](#)

インターフェイス

このセクションでは、FC ポート、イーサネットポート、ポートグループなどの SAN インターフェイスに関する情報を提供します。

FC ポート

[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)] を選択して、FC ポートに関する情報を表示します。

FC ポートのインベントリ情報の表示

[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[インベントリ (Inventory)] タブを選択して、ファイバチャネルインターフェイスのリストを表示します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[インベントリ (Inventory)] に表示されるフィールドについて説明します。

フィールド	説明
ステータス	インターフェイスのステータスを指定します。
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
エンクロージャ	エンクロージャを指定します。

フィールド	説明
デバイス名 (Device Name)	デバイス名を指定します。
VSAN	インターフェイスが属する VSAN を指定します。
スイッチインターフェイス	インターフェイス名を指定します。
Type	インターフェイス タイプを指定します。
ポートWWN	ポートの世界ワイド名 (pWWN) を指定します。
スピード	インターフェイスの速度を指定します。
FCID	インターフェイス FCID を指定します。

FC ポートのパフォーマンス情報の表示

[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[パフォーマンス (Performance)] タブを選択して、ファイバチャネルインターフェイスのパフォーマンスを表示します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[パフォーマンス (Performance)] に表示されるフィールドについて説明します。[最終日を表示 (Show last day)] ドロップダウンリストから[日、週、月 (Day, Week, Month)]、および[年 (Year)] オプションを使用して、データをフィルタ処理できます。[ホストポートの表示 (Show Host Ports)] ドロップダウンリストを使用して、[ホストポート (Host Ports)] と [ストレージポート (Storage Ports)] をフィルタ処理することもできます。

パフォーマンスを有効にするには、[ファブリック (Fabric)] ウィンドウに移動し、必要なファブリックを選択して、[アクション (Actions)]>[パフォーマンスの設定 (Configure Performance)] を選択します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある[起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。

フィールド	説明
名前	インターフェイス名を指定します。[名前 (Name)]列のグラフアイコンをクリックして、選択したタイムラインに従ってそのデバイスのトラフィックのグラフを表示します。 [日 (Day)]、[週 (Week)]、[月 (Month)]、および[年 (Year)]オプションを使用してデータをフィルタ処理できます。
VSAN	インターフェイスが属する VSAN を指定します。
スイッチインターフェイス	インターフェイス名を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

FC ポートのトランシーバ情報の表示

[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[トランシーバ (Transceiver)]タブを選択して、ファイバチャネルインターフェイスのトランシーバを表示します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[トランシーバ (Transceiver)]に表示されるフィールドについて説明します。

フィールド	説明
エンクロージャ	エンクロージャ名を指定します。
デバイス エイリアス	スイッチから取得したエイリアスを表示します。 デバイスエイリアスは、ポート WWN のわかりやすい名前です。デバイスエイリアス名は、機能を設定するときに指定できます。
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
ポートWWN	ポートのワールドワイド名 (pWWN) を指定します。
Fcid	関連するインターフェイス FCID を指定します。
スイッチインターフェイス	インターフェイス名を指定します。
リンクステータス	リンクの動作ステータスを表示します。
ベンダー	ベンダーの名前を指定します。
シリアル番号 (Serial Number)	エンクロージャのシリアル番号を指定します。
モデル	モデルの名前を指定します。
ファームウェア	この HBA によって実行されるファームウェアのバージョン。
要因	この HBA によって実行されるドライバのバージョン。
追加情報	この HBA に対応する情報一覧です。

FC FICON ポートの表示

[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[FICON] タブを選択して、ファイバチャネル FICON インターフェイスのリストを表示します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[FC ポート (FC Ports)]>[FICON] に表示されるフィールドについて説明します。[最終日の表示 (Show last day)]メニュードロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある[起動 (Launch)]アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)]ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
スイッチインターフェイス	スイッチインターフェイスを指定します。
説明	インターフェイスの説明を指定します。
FCID	関連するインターフェイス FCID を指定します。
モード (Mode)	インターフェイス モードを指定します。
FICON ID	FICON ID を指定します。
接続先	インターフェイスの接続先を指定します。
VSAN	インターフェイスが属する VSAN を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。

フィールド	説明
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

イーサネットポートに関するパフォーマンス情報の表示

[SAN]>[インターフェイス (Interfaces)]>[イーサネット (Ethernet)]タブを選択して、イーサネット インターフェイスのリストを表示します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[イーサネット (Ethernet)]に表示されるフィールドについて説明します。[最終日の表示 (Show last day)]メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ペインの右上にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
名前	インターフェイス名を指定します。[名前 (Name)] 列のグラフアイコンをクリックして、選択したタイムラインに従ってそのデバイスのトラフィックのグラフを表示します。[日 (Day)]、[週 (Week)]、[月 (Month)]、および[年 (Year)] オプションを使用してデータをフィルタ処理できます。

フィールド	説明
説明	インターフェイスの説明を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

ポートグループに関するパフォーマンス情報の表示

[SAN] > [インターフェイス (Interfaces)] > [ポートグループ (Port Groups)] タブを選択して、ポートグループのリストを表示します。

次の表では、[SAN] > [インターフェイス (Interfaces)] > [ポートグループ (Port Groups)] に表示されるフィールドについて説明します。[過去 24 時間の表示 (Show last 24 hours)] メニューのドロップダウンリストを使用して、24時間、週、月、および年でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ページの右上にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
ポート グループ名	ポートグループ名を指定します。名前をクリックすると、ポートグループのメンバーが表示されます。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
最終更新日	情報が最後に更新された日時を指定します。

ポートグループメンバー

[SAN]>[インターフェイス (Interfaces)]>[ポートグループ (Port Groups)]を選択し、ポートグループ名をクリックして、ポートグループのメンバーを表示します。

次の表では、[ポートグループメンバー (Port Group Member)]に表示されるフィールドについて説明します。

フィールド	説明
ポートグループメンバー	ポートグループメンバーを指定します。チャートアイコンをクリックして、選択したタイムラインに基づくポートグループメンバーのトラフィックのグラフを表示します。[日 (Day)]、[週 (Week)]、[月 (Month)]、および[年 (Year)] オプションを使用してデータをフィルタ処理できます。
スピード	ポートグループメンバーを指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
最終更新日	情報が最後に更新された日時を指定します。

オプティクスのパフォーマンス情報の表示

[SAN]>[インターフェイス (Interfaces)]>[オプティクス (Optics)] タブを選択して、光ファイバのリストを表示します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[オプティクス (Optics)] に表示されるフィールドについて説明します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ページの右上にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
スイッチ	スイッチ名を指定します。
インターフェイス	インターフェイス名を指定します。[インターフェイス (Interfaces)] 列のチャートアイコンをクリックして、選択したタイムラインに従って、そのデバイスの光学パラメータのグラフを表示します。[日 (Day)]、[週 (Week)]、[月 (Month)]、および[年 (Year)] オプションを使用してデータをフィルタ処理できます。
温度 (C)	平均、最低、最高温度を指定します。
電流 (mA)	各パラメータの平均値を指定します。
OPRxPower	平均、最小、および最大の光受信出力を指定します。
OPTxPower	平均、最小、および最大の光送信出力を指定します。
Voltage	平均、最小、および最大電圧を指定します。

Cisco Web NexusダッシュボードファブリックコントローラUIからすべてのFCポートに接続されているデバイスの光メトリック情報を表示するには、次の手順を実行します。

1. **[SAN] > [インターフェイス (Interfaces)] > [オプティクス (Optics)]** を選択します。
[オプティクス (Optics)] ウィンドウが表示されます。
2. **[属性でフィルタ (Filter by attributes)]** フィールドを使用してテーブルを並べ替えると、ファブリック、スイッチ、インターフェイス、温度、電流、電力、および電圧によるフィルタ処理を有効にすることができます。
3. **[最終日の表示 (Show last day)]** ドロップダウンを使用して、日、週、月、および年でビューをフィルタ処理できます。

4. ファブリック名をクリックすると、ページの右側にファブリックの正常性ステータスが表示されます。
5. ファブリックウィンドウの[起動 (Launch)]アイコンをクリックして、ファブリックの概要ページに移動します。

カスタムポートグループ

[SAN]>[インターフェイス (Interfaces)]>[カスタムポートグループ (Custom Port Groups)] タブを選択して、カスタムポートグループを表示および作成します。

次の表では、[SAN]>[インターフェイス (Interfaces)]>[カスタムポートグループ (Custom Port Groups)] に表示されるフィールドについて説明します。

フィールド	説明
グループ名 (Group Name)	ポートグループ名を指定します。名前をクリックしてパフォーマンスを表示し、ポートグループを設定します。詳細については、 カスタムポートグループのパフォーマンスの表示 (138 ページ) および カスタムポートグループの設定 (138 ページ) を参照してください。
デバイス	デバイスの番号を指定します。
インターフェイス	インターフェイスの番号を指定します。

次の表で、[SAN]>[インターフェイス (Interfaces)]>[カスタムポートグループ (Custom Port Group)] で表示される [アクション (Actions)] メニュー ドロップダウンリストのアクション項目について説明します。

アクション項目	説明
ポートグループの作成	テーブルからポートグループを選択し、[ポートグループの作成 (Create Port Group)] を選択してポートグループ名を指定し、[保存して終了 (Save & Exit)] をクリックしてカスタムポートグループを作成します。
ポートグループの編集	テーブルからポートグループを選択し、[ポートグループの編集 (Edit port group)] を選択してポートグループを編集します。
Delete	テーブルからポートグループを選択し、[削除 (Delete)] を選択してポートグループを削除します。

カスタムポートグループのパフォーマンスの表示

[SAN]>[インターフェイス (Interfaces)]>[カスタムポートグループ (Custom Port Groups)] を選択し、ポートグループ名をクリックして、ポートグループのパフォーマンスを表示します。

次の表では、カスタムポートの [パフォーマンス (Performance)] タブに表示されるフィールドについて説明します。

フィールド	説明
デバイス	デバイス名を指定します。
接続先	インターフェイスの接続先を指定します。
スピード	インターフェイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
Rx + Tx	Rx と Tx 速度の合計を指定します。
エラー/破棄	
平均	着信エラーまたは破棄の平均を指定しました。
ピーク	着信エラーまたは破棄のピークを指定しました。
最終更新日	情報が最後に更新された日時を指定します。

[最終日の表示 (Show last day)] メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

カスタムポートグループの設定

[SAN]>[インターフェイス (Interfaces)]>[カスタムポートグループ (Custom Port Groups)] を選択し、ポートグループ名をクリックして、[設定 (Configuration)] タブをクリックして、カスタムポートグループを設定します。

次の表では、カスタムポートの [設定 (Configuration)] タブに表示されるフィールドについて説明します。

フィールド	説明
デバイス	デバイス名を指定します。デバイス名をクリックすると、ページの右側にデバイスの状態が表示されます。
接続先	インターフェイスの接続先を指定します。
説明	インターフェイスの説明を指定します。

次の表では、[設定 (Configuration)] タブに表示される [アクション (Actions)] メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
Add Interfaces	[インターフェイスを追加する (Add Interfaces)] を選択してポートグループにインターフェイスを追加します。[インターフェイスを追加する (Add Interfaces)] ウィンドウでデバイスを選択し、[次の手順-インターフェイスを追加する (Next Step - Add Interfaces)] をクリックします。ポートグループに追加するインターフェイスを選択して、[保存して終了 (Save & Exit)] をクリックします。
Delete	テーブルからポートグループを選択し、[削除 (Delete)] を選択してポートグループを削除します。



第 9 章

エンド デバイス

- [デバイス \(141 ページ\)](#)
- [ラック \(142 ページ\)](#)

デバイス

[SAN]>[エンドデバイス (End Devices)]>[デバイス (Devices)] タブを選択して、ホストおよびストレージデバイスのリストを表示します。

次の表では、[SAN]>[エンドデバイス (End Devices)]>[デバイス (Devices)] に表示されるフィールドについて説明します。[最終日の表示 (Show last day)] メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。[ホストポートの表示 (Show Host Ports)] メニューのドロップダウンリストを使用して、ホストポートとストレージポートでビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。ファブリック名をクリックすると、ページの右側にファブリックのステータスが表示されます。ページの右上にある [起動 (Launch)] アイコンをクリックして、ファブリックの概要を表示します。[ファブリックの概要 (Fabric Overview)] ウィンドウの詳細については、「 ファブリックの概要 (58 ページ) 」を参照してください。
エンクロージャ名	エンクロージャ名を指定します。

フィールド	説明
デバイス エイリアス	デバイスエイリアスを指定します。[デバイスエイリアス (Device Alias)] 列のグラフアイコンをクリックして、選択したタイムラインに従ってそのデバイスのトラフィックのグラフを表示します。[日 (Day)]、[週 (Week)]、[月 (Month)]、および[年 (Year)] オプションを使用してデータをフィルタ処理できます。
FCID	関連する FCID を指定します。
スイッチインターフェイス	スイッチインターフェイスを指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
エラー/破棄	
入力平均	着信エラーまたは破棄の平均を指定しました。
出力平均	送信エラーまたは破棄の平均を指定しました。
入力ピーク (In Peak)	着信エラーまたは破棄のピークを指定しました。
出力ピーク (Out Peak)	送信エラーまたは破棄のピークを指定しました。

ラック

[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)] タブを選択して、ホストとストレージエンクロージャを表示します。

Cisco Nexus ダッシュボード ファブリック コントローラ は、ファブリックの可視性をサーバーまで拡張し、ネットワークに接続されているエンドデバイス、SAN ストレージエンクロージャ、およびストレージシステムを検出および検索できるようにします。

エンクロージャの詳細を表示するには、表内のエンクロージャ名をクリックします。
このセクションは、次のトピックで構成されています。

インベントリエンクロージャ

[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[インベントリ (Inventory)]>[ホストエンクロージャ (Host Enclosures)]タブを選択して、ホストおよびストレージインベントリエンクロージャを表示します。

このセクションは、次のトピックで構成されています。

インベントリ ホスト エンクロージャ

次の表では、[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[インベントリ (Inventory)]>[ホストエンクロージャ (Host Enclosures)]に表示されるフィールドについて説明します。

フィールド	説明
エンクロージャ	エンクロージャ名を指定します。詳細については、エンクロージャ名をクリックしてください。
OS	OSの詳細を指定します。
[IPアドレス (IP Address)]	スイッチのIPアドレスを指定します。
WWN	World Wide Name (WWN) の数を指定します。

次の表では、[アクション (Actions)]メニューのドロップダウンリストで、[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[インベントリ (Inventory)]>[ホストエンクロージャ (Host Enclosures)]に表示されるアクション項目について説明します。

アクション項目	説明
編集	テーブルからエンクロージャを選択し、[編集 (Edit)]を選択してエンクロージャ情報を更新します。
ストレージエンクロージャに変更	テーブルからエンクロージャを選択し、[ストレージエンクロージャに変更 (Change to Storage Enclosure)]を選択して、選択したエンクロージャをストレージエンクロージャに変更します。

インベントリストレージエンクロージャ

次の表では、[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[インベントリ (Inventory)]>[ストレージエンクロージャ (Storage Enclosures)]に表示されるフィールドについて説明します。

フィールド	説明
エンクロージャ	エンクロージャ名を指定します。詳細については、エンクロージャ名をクリックしてください。
[IPアドレス (IP Address)]	スイッチの IP アドレスを指定します。
WWN	World Wide Name (WWN) の数を指定します。

次の表では、[アクション (Actions)]メニューのドロップダウンリストで、[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[インベントリ (Inventory)]>[ストレージエンクロージャ (Storage Enclosures)]に表示されるアクション項目について説明します。

アクション項目	説明
編集	テーブルからエンクロージャを選択し、[編集 (Edit)]を選択してエンクロージャ情報を更新します。
ホストエンクロージャに変更	テーブルからエンクロージャを選択し、[ホストエンクロージャに変更 (Change to Host Enclosure)]を選択して、選択したエンクロージャをホストエンクロージャに変更します。

パフォーマンスエンクロージャ

[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[パフォーマンス (Performance)]>[ホストエンクロージャ (Host Enclosures)]タブを選択して、ホストおよびストレージパフォーマンスエンクロージャを表示します。

このセクションは、次のトピックで構成されています。

パフォーマンスホストエンクロージャ

次の表では、[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[パフォーマンス (Performance)]>[ホストエンクロージャ (Host Enclosures)]に表示されるフィールドについて説明します。[最終日の表示 (Show last day)]メニュードロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

フィールド	説明
エンクロージャ名	エンクロージャ名を指定します。エンクロージャ名をクリックして、詳細を表示します。チャートアイコンをクリックして、選択したタイムラインに基づくそのデバイスのトラフィックのグラフを表示します。[日 (Day)]、[週 (Week)]、[月 (Month)]、および[年 (Year)] オプションを使用してデータをフィルタ処理できます。
受信/送信/エラー/破棄	
平均	受信、送信、エラーまたは破棄の平均速度を指定します。
ピーク	受信、送信、エラーまたは破棄のピーク使用率を指定します。
Rx + Tx	受信速度と送信速度の合計を指定します。
最終更新日	最後に更新された日時を示します。

パフォーマンス ストレージ エンクロージャ

次の表では、[SAN] > [エンドデバイス (End Devices)] > [エンクロージャ (Enclosures)] > [インベントリ (Inventory)] > [ストレージエンクロージャ (Storage Enclosures)] に表示されるフィールドについて説明します。

フィールド	説明
エンクロージャ名	エンクロージャ名を指定します。
受信/送信/エラー/破棄	
平均	受信、送信、エラーまたは破棄の平均速度を指定します。
ピーク	受信、送信、エラーまたは破棄のピーク使用率を指定します。
最終更新日	最後に更新された日時を示します。

[最終日の表示 (Show last day)] メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

エンクロージャメンバー

次の表では、[SAN]>[エンドデバイス (End Devices)]>[エンクロージャ (Enclosures)]>[パフォーマンス (Performance)]に表示されるフィールドについて説明します。エンクロージャメンバーは、ホストおよびストレージのパフォーマンスエンクロージャについて表示できます。[最終日の表示 (Show last day)]メニュー ドロップダウンリストを使用して、日、週、月、および年でビューをフィルタ処理します。

フィールド	説明
ファブリック	ファブリック名を指定します。名前をクリックすると、ページの右側にファブリックの状態に関する情報が表示されます。
デバイス	デバイス名を指定します。
スピード	デバイスの速度を指定します。
Rx/Tx	
平均	受信または送信の平均速度を指定します。
平均 %	受信または送信速度の平均パーセンテージを指定します。
ピーク	受信または送信速度のピーク使用率を指定します。
ピーク %	受信または送信速度のピーク使用率パーセンテージを指定します。
エラー/破棄	
平均	平均エラーまたは破棄速度を指定します。
ピーク	エラーまたは破棄速度のピーク使用率を指定します。
最終更新日	最後に更新された日時を示します。



第 10 章

ホストパスの冗長性

- [ホストパスの冗長性 \(147 ページ\)](#)

ホストパスの冗長性

SAN ホストパスの冗長性チェックでは、非冗長ホストストレージパスを表示できます。これは、エラーを修正するための解決策とともに、ホストエンクロージャのエラーを特定するのに役立ちます。



- (注) 検出されたすべてのファブリックにライセンスが必要です。そうでない場合、この機能は Cisco Nexus ダッシュボード ファブリック コントローラ Web クライアントで無効になります。この機能を無効にすると、ライセンスのないファブリックが検出されたことを示す通知が表示されます。

ホストパスの冗長性は、NDFC に表示されるエンクロージャ名を使用して、ポートが同じエンクロージャの一部であると判断します。エンクロージャ名が完全に同じでない場合、それらは別個のデバイスとして表示されます。名前が完全に同じでない場合、ホストパスの冗長性と他の機能がそれらと同じデバイスと見なせるようにするため、ユーザーは NDFC のエンクロージャ編集ダイアログで名前を手動で変更する必要があります。

[SAN] > [ホストパスの冗長性 (Host Path Redundancy)] を選択します。

このセクションは、次のトピックで構成されています。

診断テスト

手順

- ステップ 1 [SAN] > [Host Path Redundancy (ホストパス冗長性)] > [Diagnostic Test (診断テスト)] を選択します。

- ステップ 2** **[診断テスト (Diagnostic Test)]** タブで、チェックボックスを使用してホスト冗長性のオプションチェックを選択します。
- ステップ 3** チェッカーの定期的な実行を有効にするには、**[24 時間ごとにテストを自動的に実行する (Automatically run tests every 24 hours)]** チェックボックスをオンにします。チェッカーは、サーバーが起動してから 10 分後から 24 時間ごとに実行されます。
- ステップ 4** **[Limit by VSANs (VSAN による制限)]** チェックボックスをオンにして、**[包含 (inclusion)]** または **[除外 (exclusion)]** を選択します。テキストフィールドに VSAN または VSAN 範囲を入力して、冗長性チェックから VSAN に属するホストエンクロージャを含めるかスキップします。
- ステップ 5** 他のオプションのチェックをオンにして、関連するチェックを実行します。
- ステップ 6** **[結果をクリア (Clear Results)]** をクリックして、表示されているすべてのエラーをクリアします。
- ステップ 7** **[今すぐテストを実行 (Run Tests Now)]** をクリックして、いつでもチェックを実行します。
- ステップ 8** 結果は、**[診断テスト (Diagnostic Test)]** タブの隣にある関連するタブに表示されます。

ホストパスエラー

[SAN]>[ホストパス冗長性 (Host Path Redundancy)]>[ホストパスエラー (Hostpath Errors)] タブを選択して、ホストパス冗長性エラーテーブルを表示します。テーブルの上部には、**[良好 (Good)]**、**[エラー (Errored)]**、および**[スキップ (Skipped)]** の状態のホストエンクロージャの数が色付きで表示されます。

次の表では、[SAN]>[ホストパス冗長性 (Host Path Redundancy)]>[ホストパスエラー (Hostpath Errors)] に表示されるフィールドについて説明します。

フィールド	説明
ホストエンクロージャ	エラーを含むホストを指定します。これらは、エラーが発生したホストエンクロージャ内の各パスの数です。
ストレージエンクロージャ	エラーが発生しているコネクテッドストレージを指定します。
説明	エラーの説明を指定します。
[Fix]	エラーを修正するソリューションを指定します。エラーをポイントして、エラーを修正するソリューションを表示します。
最初の確認日時 (First Seen)	エラーが最初に発生した時期を指定します。

次の表では、**[アクション (Actions)]** メニュードロップダウンリストで、[SAN]>[ホストパス冗長性 (Host Path Redundancy)]>[ホストパスエラー (Hostpath Errors)] に表示されるアクション項目について説明します。

アクション項目	説明
無視するホスト	テーブルから行を選択し、[ホストを無視 (Ignore Host)] を選択して、選択した行のホストエンクロージャを除外リストに追加します。そのホストからのエラーは報告されなくなり、現在のエラーはデータベースから削除されます。
ストレージを無視する	テーブルから行を選択し、[ストレージを無視 (Ignore Storage)] を選択して、選択した行のストレージエンクロージャを除外リストに追加します。
ホストストレージペアを無視	テーブルから行を選択し、[ホストストレージペアを無視 (Ignore Host Storage Pair)] を選択して、選択した行のホストストレージペアエンクロージャを除外リストに追加します。
結果の消去	テーブルから行を選択し、[結果の消去 (Clear Results)] を選択して結果をクリアします。

無視されたホスト

[SAN]>[ホストパスの冗長性 (Host Path Redundancy)]>[無視されたホスト (Ignored Host)] タブを選択して、冗長性チェックによってスキップまたは無視されたホストエンクロージャのリストをスキップの理由とともに表示します。

次の表では、[SAN]>[ホストパスの冗長性 (Host Path Redundancy)]>[無視されたホスト (Ignored Host)] に表示されるフィールドについて説明します。ホストエンクロージャを選択し、[無視を解除 (Unignore)] をクリックしてホストを無視リストから削除し、無視することを選択したホストに関するエラーの受信を開始します。

フィールド	説明
ホストエンクロージャ	エラーを含むホストを指定します。

フィールド	説明
理由を無視する	<p>ホストが無視された理由を指定します。</p> <p>次の理由が表示される場合があります。</p> <ul style="list-style-type: none"> • [スキップ : エンクロージャには HBA が 1 つしかありません。 (Skipped: Enclosure has only one HBA.)] • [ホストはユーザーによって無視されました。 (Host was ignored by the user.)] • [複数のフェデレーションサーバーによって管理されるホストポート。チェックを実行できません。 (Host ports managed by more than one federated servers. Check can't be run.)] • [スキップ : ストレージへのパスが見つかりません。 (Skipped: No path to storage found.)]

無視されたストレージ

[SAN] > [ホストパス冗長性 (Host Path Redundancy)] > [無視されたストレージ (Ignored Storage)] タブを選択して、冗長性チェック中に無視するように選択されたストレージエンクロージャのリストを表示します。

次の表では、[SAN] > [ホストパス冗長性 (Host Path Redundancy)] > [無視されたストレージ (Ignored Storage)] に表示されるフィールドについて説明します。ストレージエンクロージャを選択し、[無視の解除 (Unignore)] をクリックして、無視するリストからストレージを削除し、無視することを選択したストレージに関するエラーの受信を開始します。

フィールド	説明
ストレージエンクロージャ	エラーが発生しているコネクテッドストレージを指定します。
理由を無視する	ストレージが無視された理由を指定します。

無視されたホストストレージペア

[SAN] > [ホストパス冗長性 (Host Path Redundancy)] > [無視されたホストストレージペア (Ignored Host Storage Pair)] タブを選択して、冗長性チェック中に無視するように選択されたホストストレージペアのリストを表示します。

次の表では、[SAN] > [ホストパス冗長性 (Host Path Redundancy)] > [無視されたホストストレージペア (Ignored Host Storage Pair)] に表示されるフィールドについて説明します。行を

選択し、[無視の解除 (Unignore)] をクリックして、ホストストレージペアを無視されたリストから削除します。

フィールド	説明
ホストエンクロージャ	エラーを含むホストを指定します。
ストレージエンクロージャ	エラーが発生しているコネクテッドストレージを指定します。
理由を無視する	ストレージが無視された理由を指定します。



第 11 章

ポート監視

- [ポートモニタリングポリシー \(153 ページ\)](#)
- [SFP カウンタの設定 \(159 ページ\)](#)

ポートモニタリングポリシー

この機能により、カスタム ポート モニタリング ポリシーを Cisco SAN コントローラデータベースに保存できます。選択したカスタムポリシーを 1 つ以上のファブリックまたは Cisco MDS 9000 シリーズスイッチにプッシュできます。このポリシーは、スイッチでアクティブなポートモニタポリシーとして指定されています。

この機能は Cisco MDS 9000 SAN スイッチでのみサポートされているため、Cisco SAN コントローラのユーザーは、ポリシーをプッシュする MDS スイッチを選択できます。

Cisco SAN コントローラには、ポリシーをカスタマイズするための 12 のテンプレートが用意されています。ユーザー定義のポリシーは、Cisco SAN コントローラデータベースに保存されます。任意のテンプレートまたはカスタマイズされたポリシーを選択して、目的のポートタイプで選択したファブリックまたはスイッチにプッシュできます。

Cisco SAN コントローラリリース 12.0.1a から、新しいポートモニタリングリソース `[fabricmon_edge_policy]` が追加されました。



(注) ユーザー定義のポリシーのみを編集できます。

次の表では、Cisco ファブリックコントローラ[`SAN`] > [ポートモニタリング (Port Monitoring)] で表示されるフィールドについて説明します。

フィールド	説明
選択したポートモニタリングポリシー	<p>このドロップダウンリストには、ポリシーの次のテンプレートが表示されます。</p> <ul style="list-style-type: none"> • Normal_edgePort • Normal_allPort • Normal_corePort • Aggressive_edgePort • Aggressive_allPort • Aggressive_corePort • Most-Aggressive_edgePort • Most-Aggressive_allPort • Most-Aggressive_corePort • デフォルト • slowdrain • fabricmon_edge_policy
論理型	<p>選択したポリシーのポートのタイプを指定します。使用可能なポートタイプは次のとおりです。</p> <ul style="list-style-type: none"> • コア • エッジ • すべて
保存	<p>ユーザー定義ポリシーの変更を保存できます。</p> <p>(注) デフォルトテンプレートの構成変更を保存することはできません。</p>

フィールド	説明
名前を付けて保存	<p>既存のポリシーを別の名前の新しいポリシーとして保存できます。</p> <p>これにより、テンプレートにカスタムポリシーとして別の項目が作成されます。カスタマイズされたポリシーは、このカテゴリの下に保存されます。</p> <p>ポリシーの編集中に [名前を付けて保存 (Save As)] をクリックすると、カスタマイズされたポリシーが保存されます。</p> <p>新しいポリシーを作成するには。</p> <ul style="list-style-type: none">必要なポートモニタリングポリシーを選択し、[名前を付けて保存 (Save As)] をクリックします。 <p>[新しいポートモニタリングポリシー (New Port Monitoring Policy)] ウィンドウが表示されます。</p> <ul style="list-style-type: none">新しいポリシー名を入力し、必要な論理タイプを選択して、[保存 (Save)] をクリックします。
Delete	すべてのユーザー定義のポリシーを削除できます。

フィールド	説明
スイッチにプッシュ	

フィールド	説明
	<p>ファブリックまたはスイッチを選択し、選択したポリシーを目的のポートタイプにプッシュできます。</p> <p>次のポリシーは、コアポリシータイプを選択します。</p> <ul style="list-style-type: none"> • Normal_corePort • Aggressive_corePort • Most-Aggressive_corePort <p>次のポリシーは、エッジポリシータイプを選択します。</p> <ul style="list-style-type: none"> • Normal_edgePort • Aggressive_edgePort • Most-Aggressive_edgePort • fabricmon_edge_policy • slowdrain <p>次のポリシーは、すべてのポリシータイプを選択します。</p> <ul style="list-style-type: none"> • Normal_allPort • Aggressive_allPort • Most-Aggressive_allPort • デフォルト <p>パラメータを選択し、[プッシュ (Push)] をクリックして、ファブリック内のスイッチにポリシーをプッシュします。</p> <p>リリース 12.0.1a の SAN コントローラの場合、事前定義されたポートとは別に、選択したポリシーに必要なポートタイプを変更できます。</p> <ul style="list-style-type: none"> • 必要なポリシーを選択し、[スイッチにプッシュ (Push to Switches)] をクリックします。 <p>[スイッチにプッシュ (Push to Switches)] ポップアップウィンドウが表示されます。</p> <ul style="list-style-type: none"> • 必要なポートタイプを選択し、[プッシュ (Push)] をクリックします。 <p>同じまたは共通のポートタイプを持つアクティブなポリシーがある場合、push コマンドは選択したデバイスに同じポリシーを設定します。このポリシーは、既存のアクティブポリシーを同じまたは共通のポートタイプに置き換えます。</p>

フィールド	説明
	<p>既存のポリシーを置き換える警告メッセージが表示されます。[確認 (Confirm)] をクリックしてポリシーを書き換えます。</p> <p>スイッチにプッシュされたポリシーの確認メッセージが表示されます。[ログの表示 (View logs)] をクリックしてスイッチのログの詳細を表示するか、[OK] をクリックしてホームページに戻ります。</p> <p>ポリシーの編集集中に [スイッチにプッシュ (Push to Switches)] をクリックすると、カスタマイズされたポリシーは保存されません。</p> <p>SAN コントローラは、FPIN または DURL ポートガードを使用してエッジ論理タイプポリシーをプッシュしてアクティブ化すると、ファブリック パフォーマンス モニタ (FPM) 機能を有効にします。</p> <p>(注) FPIN または DURL 機能カウンタを使用するポリシーに Cisco MDS 9250i マルチサービス ファブリック スイッチを選択すると、警告ウィンドウが表示されます。</p>
説明	<p>詳細情報を表示するには、説明の横にある「i」アイコンにポインタを移動します。</p> <p>SAN コントローラ リリース 12.0.1a 以降、次の新しいカウンタが導入されました。</p> <ul style="list-style-type: none"> • Rx データレートバースト • Tx データレートバースト • SFP Rx 電力低下警告 • SFP Tx 電力低下警告 • 入力エラー
上昇しきい値	カウンタタイプの上限しきい値を指定します。
上昇イベント	上昇しきい値に達したとき、または超えたときに生成されるイベントのタイプを指定します。
下降しきい値	カウンタタイプの下限しきい値を指定します。
アラート	<p>ポートのアラートのタイプを指定します。アラートは、syslog、rmon、および oblf です。</p> <p>アラートは、リリース 8.5(1) の Cisco MDS スイッチにのみ適用されます。</p>
ポーリング間隔	カウンタ値をポーリングする時間間隔を指定します。

フィールド	説明
警告しきい値	上限しきい値よりも低く、下限しきい値よりも高いオプションのしきい値を設定して、syslog を生成できます。 範囲は 0 ～ 9223372036854775807 です。
ポートガード	ポートガードを有効にするか無効にするかを指定します。値は、false、flap、または errorisable にすることができます。デフォルト値は「false」です。 Cisco SAN コントローラリリース 12.0.1a から、新しいポートガード FPIN 、 DIRL 、および cong-isolate-recover がエッジポートタイプにのみ追加されます。 (注) DIRL は、Cisco SAN コントローラ 12.0.1a のプレビュー機能です。実稼働環境での使用は推奨されません。
輻輳信号警報	ポート間の輻輳の増加を示します。これは、 TxWait (%) カウンタでのみ使用できます。
輻輳信号 アラーム	ポート間のクリティカルな輻輳を示します。これは、Tx-Wait カウンタでのみ使用できます。
モニターリング	true または false の値を示します。
編集	クリックして各行の上記の詳細を編集し、チェックマークをクリックして構成の変更を保存します。 (注) 各行の構成を編集するときに、[保存 (Save)] および [名前を付けて保存 (Save As)] オプションを使用して保存された構成の変更を上書きできます。

SFP カウンタの設定

Cisco MDS NX-OS リリース 8.5(1)以降、SFP カウンタを使用すると、SFP の送信電力および受信電力の警告下限しきい値を設定できます。これらのしきい値が設定値を下回ると、syslog を受信します。

SFP は 10 分に 1 回モニターリングされます。上昇しきい値は、受信電力または送信電力回数のカウントです。この電力時間は、SFP の受信電力または送信電力低警告しきい値にパーセンテージを掛けた値以下となります。したがって、10 分ごとに上昇しきい値を増やすことができます。ポーリング間隔の 600 倍を超える上昇しきい値を設定すると、エラーが表示されます。

たとえば、ポーリング間隔が 1200 の場合、上昇しきい値は 2 (1200/600) になり、2 より大きくする必要があります。SFP カウンタはデフォルトポリシーに含まれておらず、使用可能なアラートアクションは syslog のみです。port monitor counter コマンドを使用して、ポーリング間隔を設定できます。

次のいずれかを選択して SFP カウンタを設定し、次のオプションを実行できます。

- 警告下限しきい値のパーセンテージを 100% に設定すると、Rx 電力が SFP の Rx 電力警告下限しきい値以下の場合に、このカウンタがトリガーされます。
- 警告の下限しきい値のパーセンテージを 100% 未満に設定すると、Rx 電力が SFP の Rx 電力の警告下限しきい値を超えると、このカウンタがトリガーされます。
- 低警告しきい値のパーセンテージを 100% より大きく設定すると、Rx 電力が SFP の Rx 電力低警告しきい値（低警告と低アラームの間）を下回ると、このカウンタがトリガーされます。

SFP カウンタは次のとおりです。

- **sfp-rx-power-low-warn**

SFP のポートが SFP の Rx 電力の警告下限しきい値のパーセンテージに達した回数を指定します。このしきい値は、SFP のタイプ、速度、および製造元によって異なり、`show interface transceiver details` コマンドで表示されます。この値は、個々の SFP の Rx 電力警告下限しきい値のパーセンテージであり、完全な値ではありません。このパーセンテージを 50 ~ 150% の範囲で構成して、Rx 電力の警告下限しきい値未満または受信電力警告警告の下限しきい値を超える値でアラートを送信できるようにすることができます。これは完全な値であり、50% から 150% の間で変化します。警告下限しきい値は、SFP の実際の警告下限しきい値に指定されたパーセンテージを掛けた値として計算されます。Rx 電力が警告下限しきい値以下の場合、このカウンタが増分します

- **sfp-tx-power-low-warn**

SFP のポートが SFP の送信電力の警告下限しきい値の割合に達した回数を指定します。このしきい値は、SFP のタイプ、速度、および製造元によって異なり、`show interface transceiver details` コマンドで表示されます。この値は、個々の SFP の Tx 電力低警告しきい値のパーセンテージであり、完全な値ではありません。このパーセンテージを 50 ~ 150% の範囲で構成して、Tx 電力の警告下限しきい値未満または送信電力警告警告の下限しきい値を超える値でアラートを送信できるようにすることができます。これは完全な値であり、50% から 150% の間で変化します。警告下限しきい値は、SFP の実際の警告下限しきい値に指定されたパーセンテージを掛けた値として計算されます。Tx 電力が警告下限しきい値以下の場合、このカウンタが増分します。

Cisco MDS NX-OS リリース 8.5(1) 以降、データレート バースト カウンタは、データレートが設定されたしきい値データレートを超える回数を 1 秒間隔でモニタリングします。数値が上昇しきい値に設定された数値を超えると、条件が満たされると、設定されたアラートアクションが実行されます。データレート バースト カウンタは毎秒ポーリングされます。データレート バースト カウンタは、デフォルトポリシーに含まれていません。データレート バースト カウンタの設定については、『*Cisco MDS 9000 Series Interfaces Configuration Guide*』の「*Configuring a Port Monitor Policy*」セクションを参照してください。



第 12 章

アクティブゾーン

- [通常ゾーン \(161 ページ\)](#)
- [IVR ゾーン \(162 ページ\)](#)

通常ゾーン

SAN コントローラで設定されているすべての通常ゾーンを表示できます。[SAN]>[アクティブゾーン (Active Zones)]>[通常のゾーン (Regular Zones)] タブを選択します。次の表では、この画面のフィールドについて説明します。

表 17:

フィールド	説明
グループ	ファブリック名を指定します。
VSAN	このゾーンで設定されている VSANS の数を指定します。
ゾーン セット	ゾーンが属するゾーンセットの名前を指定します。
ゾーン	このメンバーが存在するゾーンを表示します。
スイッチインターフェイス/WWN	ゾーンメンバーが接続されているスイッチのスイッチインターフェイスまたは WWN を指定します。
PWWN	スイッチに関連付けられた pWWN を指定します。
メンバー名	ゾーンメンバーの名前を表示します。
ゾーン分割のタイプ	ゾーン分割のタイプを表示します。WWN、FCID、fcAlias、iSCSI などのゾーン分割のタイプで検索できます。

IVR ゾーン

SAN コントローラで設定されているすべての IVR ゾーンを表示できます。[SAN]>[アクティブゾーン (Active Zones)]>[IVR ゾーン (IVR Zones)] タブを選択します。次の表では、この画面のフィールドについて説明します。

表 18:

フィールド	説明
グループ	ファブリック名を指定します。
VSAN	このゾーンで設定されている VSANS の数を指定します。
ゾーンセット	ゾーンが属するゾーンセットの名前を指定します。
ゾーン	このメンバーが存在するゾーンを表示します。
スイッチインターフェイス/WWN	ゾーンメンバーが接続されているスイッチのスイッチインターフェイスまたは WWN を指定します。
PWWN	スイッチに関連付けられた pWWN を指定します。
メンバー名	ゾーンメンバーの名前を表示します。
ゾーン分割のタイプ	ゾーン分割のタイプを表示します。WWN、FCID、fcAlias、iSCSI などのゾーン分割のタイプで検索できます。



第 13 章

ストレージ

- [ストレージアレイ \(163 ページ\)](#)
- [ストレージ SMI-S プロバイダー \(165 ページ\)](#)

ストレージアレイ

このタブには、ストレージアレイに関する情報が表示されます。

次の表では、[SAN]>[ストレージ (Storage)]>[ストレージアレイ (Storage Arrays)]に表示されるフィールドについて説明します。

フィールド	説明
storageName	ストレージ名を指定します。 [storageName] をクリックして、[ストレージエンクロージャ (Storage Enclosure)] の詳細を表示します。表示されるタブの詳細については、「 storageName エンクロージャ (163 ページ) 」を参照してください。
WWN	スイッチの World Wide Name (WWN) を指定します。 ファブリック検出によって検出されたストレージアレイの PWWN のみが表示されます。ただし、ストレージアレイには、ここで指定されているよりも多くのポートがある場合があります。

storageName エンクロージャ

[storageName] アイテムをクリックして、各ストレージアレイに関する詳細情報を表示します。

ストレージアレイの詳細は、検出されたアレイのタイプと、プロバイダーが SMI-S 標準に準拠しているかどうかによって異なります。アレイをクリックして、概要タブから始まるインベントリページ、およびアレイのタイプに基づいた他のコンテキスト固有のタブを読み込みます。

以下のドキュメントには、追加の関連情報が記載されています。

- **概要**

この表は、プロバイダーに関する情報を提供します。ストレージアレイのシリアル番号、ストレージタイプ、およびアレイ内の物理ディスクの数も表示されます。

- **コンポーネント**

このタブには、ストレージ内のすべてのコンポーネントが一覧表示されます。

コンポーネントの名前をクリックして、合計ストレージ容量、使用状況の詳細、および物理ディスクの詳細を表示します。

- **プール**

このタブには、すべてのプール、そのステータス、およびRaw容量が一覧表示されます。[プール名 (POOL Name)] をクリックして、プールの詳細を表示します。

- **LUN**

このタブには、ストレージアレイ内のすべてのLUNが一覧表示されます。各LUNのLUN ID、WWN、ステータス、および容量の詳細を提供します。[LUN名 (LUN Name)] をクリックして、各LUNの詳細を表示します。[LUNの詳細 (LUN Detail)] ビューで[ホストLUNアクセス (Host LUN Access)] 情報を表示することもできます。

ホストLUNアクセステーブルのホストポートPWWN、ホストインターフェイス、ゾーニング、およびストレージインターフェイスの値は、このLUNにアクセスするホストがNDFCで検出されたファブリックの一部である場合にのみ表示されます。

- **ホスト**

このタブには、選択したストレージ内のすべてのホストが一覧表示されます。これは、ストレージアレイ内の各ホストのホスト名、ノードWWN、およびWWNの詳細を提供します。[ホスト名 (Host Name)] をクリックして、ホストに関する詳細を表示します。[ホストの詳細 (Host Detail)] ビュー内の[LUN]タブと[ポート (Ports)]タブで、関連する詳細を表示できます。

LUNタブ>ホストLUNアクセステーブルのホストインターフェイス、ゾーン分割、およびストレージインターフェイスの値は、このLUNにアクセスするホストがNDFCで検出されたファブリックの一部である場合にのみ表示されます。

ホストポートテーブルのファブリックとホストインターフェイスの値は、ホストポートWWNがNDFCで検出されたファブリックの一部である場合にのみ表示されます。

- **プロセッサ**

このタブには、すべてのプロセッサとそのステータスが一覧表示されます。各プロセッサのアダプタの数も表示されます。詳細を表示するには、[プロセッサ名 (Processor Name)] をクリックします。

- **ポート**

このタブには、ストレージレイ内のすべてのポートが一覧表示されます。ポートの詳細を表示するには、ポート名をクリックします。

ホスト LUN アクセステーブルのホストインターフェイス、ゾーン分割、およびストレージインターフェイスの値は、LUN ID 列の LUN にアクセスするホストが NDFC で検出されたファブリックの一部である場合にのみ表示されます。

ストレージ SMI-S プロバイダー

このタブには、SMI-S プロバイダーの情報が表示されます。

次の表では、[SAN]>[ストレージ (Storage)]>[ストレージ SMIS プロバイダー (Storage SMIS Provider)] に表示されるフィールドについて説明します。

フィールド	説明
ベンダー	ベンダーを指定します。 Cisco NDFC は、次のベンダーをサポートしています。 <ul style="list-style-type: none"> • EMC • NetApp • IBM • HDS • PureStorage • HP • その他
プロバイダーの URL	SMI-S プロバイダーの URL を指定します。
名前空間	名前空間を指定します。
相互運用名前空間	相互運用名前空間を指定します。
[ポート (Port)]	ポートを指定します。
ステータス	ステータスを指定します。
セキュア	安全な接続かどうかを指定します。
検出ステータス	検出ステータスを指定します。
最終更新時刻	最後に更新された日時を示します。

次の表で、SAN > [ストレージ (Storage)] > [ストレージ SMIS プロバイダー (Storage SMIS Provider)] で表示される [アクション (Actions)] メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
プロバイダの追加	SMI-S プロバイダーを追加します。手順については、「 SMI-S プロバイダーの追加 (166 ページ) 」。
プロバイダの編集	テーブルからプロバイダーを選択し、[プロバイダーの編集 (Edit Provider)] を選択してプロバイダー情報を更新します。
プロバイダーの削除	テーブルからプロバイダーを選択し、[プロバイダーの削除 (Delete Provider)] を選択してプロバイダーを削除します。
プロバイダーの再検出	テーブルからプロバイダーを選択し、[プロバイダーの再検出 (Rediscover Provider)] を選択して変更をスキャンします。これにより、通常の定期的なポーリング以外で検出サイクルがトリガーされます。
プロバイダーの消去	テーブルからプロバイダーを選択し、[プロバイダーの消去 (Purge Provider)] を選択してプロバイダー情報を消去します。これにより、存在しなくなった要素が検出から削除されます。

SMI-S プロバイダーの追加

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI から SMI-S プロバイダーを追加するには、次の手順を実行します。

手順

ステップ 1 [SAN] > [ストレージ (Storage)] > [ストレージ SMIS プロバイダー (Storage SMIS Provider)] を選択します。

[ストレージ SMIS プロバイダー (Storage SMIS Provider)] タブが表示されます。

ステップ 2 [アクション (Actions)] メニューのドロップダウンリストをクリックし、[プロバイダーの追加 (Add Provider)] をクリックします。

[SMI-S の追加 (Add SMI-S)] ウィンドウが表示されます。

ステップ3 ドロップダウンを使用して **[ベンダー (Vendor)]** を選択します。

サポートされているすべてのベンダーがドロップダウンリストに表示されます。ドロップダウンの **[その他 (Other)]** のベンダーオプションを使用して、「ベストエフォート」ハンドラーを通じて、より多くの SMI-S ストレージベンダーが検出されます。

(注) SMI-S ストレージ検出用のデータソースを追加する前に、少なくとも 1 つの有効な Nexus ダッシュボード ファブリック コントローラ ライセンスをプロビジョニングする必要があります。

ステップ4 SMI-S サーバーの IP、ユーザー名、およびパスワードを指定します。

ステップ5 名前空間と相互運用名前空間を指定します。

ステップ6 デフォルトでは、ポート番号は事前に入力されています。

[セキュア (Secure)] チェックボックスをオンにすると、デフォルトのセキュアポート番号が入力されます。

EMC でセキュアモードを使用する場合、デフォルト設定は相互認証です。詳細については、トラストストアへの SSL 証明書の追加に関する EMC のドキュメントを参照してください。また、*Security_Settings.xml* 構成ファイルで `SSLClientAuthentication` 値を *None* に設定し、ECOM サービスを再起動することもできます。

ステップ7 **[Add]** をクリックします。

ログイン情報が検証され、ログイン情報が有効な場合はストレージの検出が開始されます。ログイン情報チェックに失敗した場合は、有効なログイン情報を入力するように求められます。



第 II 部

仮想的な管理

- [ゾーン分割 \(171 ページ\)](#)
- [仮想インフラストラクチャ マネージャ \(187 ページ\)](#)



第 14 章

ゾーン分割

- ・ [ゾーン分割 \(171 ページ\)](#)

ゾーン分割

ゾーン分割により、ストレージデバイス間またはユーザーグループ間でアクセスコントロールの設定ができます。ファブリックで管理者権限を持つユーザーは、ゾーンを作成してネットワークセキュリティを強化し、データ損失またはデータ破壊を防止できます。ゾーン分割は、送信元/宛先 ID フィールドを検証することによって実行されます。

SAN コントローラ リリース 12.0.1a 以降、通常のゾーンと IVR ゾーンが単一のゾーン分割ページにマージされます。



- (注) Web UI のゾーン分割にデバイスエイリアスが使用されている場合、エンドデバイスはファブリックにログインする必要があるため、Web GUI はデバイスエイリアスを使用してゾーン分割を設定できます。エンドノードにログインしていない場合は、ゾーン分割に PWWN を使用できます。

次の表では、SAN コントローラの [仮想管理 (Virtual Management)] > [ゾーン分割 (Zoning)] タブに表示されるフィールドとアイコンについて説明します。

フィールド	説明
ゾーン分割のタイプ	[通常 (Regular)] または [IVR] の横にあるオプションボタンを選択して、必要なゾーン分割タイプを選択します。
ファブリック	[ファブリック (Fabric)] ドロップダウンリストから、ゾーン分割を設定または表示するファブリックを選択できます。 管理者ロールがファブリックをロックしている場合、ファブリックフィールドの隣にロックアイコンが表示されます。

フィールド	説明
VSAN	<p>通常のゾーン分割タイプを選択して、VSAN フィールドを表示します。</p> <p>VSAN ドロップダウンリストから、通常のゾーンを設定する VSAN を選択できます。</p>
地域ID	<p>リージョン ID フィールドを表示するには、IVR ゾーン分割タイプを選択します。</p> <p>[リージョン ID (Region ID)]ドロップダウンリストから、IVR ゾーンを設定するリージョン名を選択できます。</p>
拡張ゾーン分割	<p>[VSAN] テキストフィールドの横にある [設定 (Configurations)] アイコンをクリックして、拡張ゾーン分割ウィンドウを表示します。</p> <p>(注) 拡張ゾーン分割は通常ゾーンでのみサポートされています。</p> <p>詳細については、拡張ゾーン分割セクションを参照してください。</p>
Cisco Fabric Services (CFS)	<p>[リージョン ID (Region ID)] フィールドの横にある [セットアップアシスタント (set-up assistant)] アイコンをクリックして、CFS ウィンドウを表示します。</p> <p>(注) CFS は、IVR ゾーン分割でのみサポートされます。</p> <p>詳細については、CFSの項を参照してください。</p>
スイッチ	<p>[スイッチ (Switch)] ドロップダウンリストから、設定するスイッチを選択します。</p>
Action	<p>[ゾーン分割 (Zoning)] フィールドで、[アクション (Actions)] をクリックして以下を表示します。</p> <ul style="list-style-type: none"> • 変更 • データベース • サーバーキャッシュを消去 • 検出同期

フィールド	説明
変更	<p>[ゾーン分割 (Zoning)] フィールドで、[アクション (Actions)] > [変更 (Changes)] の順にクリックします。</p> <ul style="list-style-type: none"> • スマートゾーン分割を有効にする：すべてのスイッチのスマートゾーン分割設定を有効にします。 • 変更のコミット：ゾーン分割設定の変更をすべてのスイッチにコミットします。このフィールドは、ゾーンが拡張モードまたはスマートモードの場合にのみ適用されます。 • 保留中の破棄：保留中の変更の破棄を実行中です。
データベース	<p>[ゾーン分割 (Zoning)] フィールドで、[アクション (Actions)] > [データベース (Database)] をクリックします。</p> <ul style="list-style-type: none"> • データベースのバックアップ：[データベースのバックアップ (Backup Database)] を選択すると、[データベースのバックアップ (Backup Database)] ウィンドウが表示されます。名前を入力し、[バックアップ (Backup)] をクリックします。 • データベースの復元：[データベースの復元 (Restore Database)] を選択すると、[データベースの復元 (Restore Database)] ウィンドウが表示されます。適切なファイルをアップロードし、[復元 (Restore)] をクリックします。
サーバーキャッシュを消去	<p>[ゾーン分割] エリアで、[アクション (Actions)] > [サーバーキャッシュのクリア (Clear Server Cache)] の順に選択します。</p> <p>サーバー上のキャッシュをクリアします。</p>
検出同期	<p>[ゾーン分割 (Zoning)] エリアで、[アクション (Actions)] > [検出同期 (Discovery Sync)] を選択します。</p> <p>ゾーン分割モジュールを検出と同期するには。</p>

この章は、次の項で構成されています。

拡張ゾーン分割

SAN コントローラリリース 12.0.1a から、通常のゾーン分割タイプに拡張ゾーン分割機能が追加されました。

拡張ゾーン分割では、すべての設定が単一の設定セッション内で実行されます。セッションを開始すると、スイッチは変更を行うファブリック全体をロックします。

ゾーン分割タイプで[通常 (Regular)] オプションボタンを選択し、[VSAN] フィールドの横にある[設定 (Configurations)] アイコンをクリックして、[拡張ゾーン分割 (Enhanced zoning)] ウィンドウを表示します。

[拡張ゾーン分割 (Enhanced Zoning)] ウィンドウには、次のフィールドとその説明があります。

フィールド	説明
スイッチ	スイッチの IP アドレスを指定します。
モード	次のいずれかのスイッチのモードを表示します。 <ul style="list-style-type: none"> • Basic • Enhanced
結果	次のいずれかのアクティベーション結果を表示します。 <ul style="list-style-type: none"> • 成功 • 失敗
以下によってロックされた設定 DB	ロックされた設定データベースのロール名を表示します。
Action	次のいずれかのスイッチのアクションを表示します。 <ul style="list-style-type: none"> • オペレーションなし • 変更を確定します。 • クリーンアップ <p>最後の列の [編集 (edit)] アイコンをクリックして必要なアクションを選択し、[チェックマーク (check mark)] アイコンをクリックして保存します。</p>
最後のアクション結果	最後の設定データベースのステータスを表示します。
完全な DB マージを強制する	ステータスを有効または無効に表示します。最後の列の [編集 (edit)] アイコンをクリックして必要なアクションを選択し、[チェックマーク (check mark)] アイコンをクリックして保存します。 <p>これを有効にすると、アクティブゾーンとローカルゾーンの両方がマージされ、VSAN のすべてのスイッチで同一になります。</p>

フィールド	説明
続きを読む	<p>拡張ゾーンまたはIVRCFS対応ゾーンの場合、スイッチのゾーン分割DBに変更が加えられると、commitコマンドが発行されるまで、すべてのゾーンデータが保留中のデータベースにプッシュされます。</p> <p>このフラグは、ユーザーが保留中のゾーンDB（コピーDB）または通常のゾーンDB（有効なDB）からデータを取得するのに役立ちます。</p> <p>最後の列の [編集 (edit)] アイコンをクリックして必要なアクションを選択し、[チェックマーク (check mark)] アイコンをクリックして保存します。</p>
アクティブ化された日付	ゾーンセットがアクティブ化された日付を指定します。

SAN コントローラ Web UI の [拡張ゾーン分割 (Enhanced Zoning)] ウィンドウでさまざまな操作を実行するには、次の手順を実行します。

Procedure

- ステップ 1 [仮想管理 (Virtual Management)] > [ゾーン分割 (Zoning)] を選択し、必要な [ゾーンタイプ (Zone Type)]、[ファブリック (Fabric)]、および [VSAN] を選択します。
- ステップ 2 [VSAN] フィールドの隣にある [設定 (configurations)] アイコンをクリックします
[拡張ゾーン分割 (Enhanced Zoning)] ウィンドウが表示されます。
- ステップ 3 [続きを読む (Read from)] 列の横にある [編集 (Edit)] アイコンをクリックして必要なデータベースを選択し、[チェックマーク (Tick)] アイコンをクリックして保存します。
- ステップ 4 モードを基本から拡張に変更するには、[アクション (Actions)] > [モードを拡張に設定 (Set Mode to Enhanced)] を選択し、[適用 (Apply)] をクリックします。
- ステップ 5 同じ手順に従って、モードを拡張から基本に設定し、[アクション (Actions)] > [モードを基本に設定 (Set Mode to Basic)] を選択して、[適用 (Apply)] をクリックします。

CFS

Cisco Fabric Service (CFS) は、IVR ゾーン分割のファブリック内で自動的に設定を同期化するための、共通のインフラストラクチャを提供します。CFS が 1 つのスイッチで設定されていて、同じプロパティを他のスイッチで送信できる場合、スイッチで IVR を有効または無効にすることができます。さらに、選択したスイッチで CFS とグローバル CFS の両方を有効または無効にすることができます。

ゾーン分割タイプで[IVR]オプションボタンを選択し、[VSAN]フィールドの隣にある[セットアップアシスタント (set-up assistant)] アイコンをクリックして、CFS ウィンドウを表示します。

CFS ウィンドウでは、以下のタブを表示できます。

- Control
- IVR
- Action

次の表では、[コントロール (Control)] タブに表示されるフィールドについて説明します。

フィールド	説明
スイッチ	スイッチの IP アドレスを指定します。
IVR ステータス	スイッチで IVR が有効または無効であるかを表示します。
編集	[編集 (Edit)] アイコンをクリックしてスイッチの IVR を有効または無効にし、チェックマークをクリックして変更を保存します。
リフレッシュ	表を更新するには、更新 アイコンをクリックします。
適用	[適用 (Apply)] をクリックして、スイッチの変更ごとに変更を保存します。
完了	[完了 (Done)] をクリックしてすべての変更を保存し、CFS ウィンドウを終了します。

次の表では、[IVR] タブに表示されるフィールドおよび説明について記述します。

フィールド	説明
スイッチ	スイッチの IP アドレスを指定します。
CFS ステータス	CFS ステータスを有効にするか無効にするかを指定します。
グローバル CFS	スイッチでこの機能を有効にするか無効にするかを指定します。
続きを読む	ステータスを指定します。 <ul style="list-style-type: none"> • 有効な DB • DB をコピー
ロック所有者 (Lock Owner)	スイッチが管理者によってロックされていることを指定します。
結合ステータス	発生したファブリックマージを指定します。
地域ID	スイッチのリージョン ID を指定します。

フィールド	説明
編集	[編集 (Edit)] アイコンをクリックして、選択した行の [続きを読む (Read from)] 列および [リージョン ID (Region ID)] 列の変更を実行します。
適用	[適用 (Apply)] をクリックして、スイッチの変更ごとに変更を保存します。
リフレッシュ	表を更新するには、 更新 アイコンをクリックします。
完了	[完了 (Done)] をクリックしてすべての変更を保存し、CFS ウィンドウを終了します。

SAN コントローラ Web UI から IVR タブのスイッチでさまざまな操作を実行するには、次の手順を実行します。

Procedure

- ステップ 1** スイッチを選択し、**[アクション (Actions)]** > **[コミット (Commit)]** の順に選択し、**[適用 (Apply)]** をクリックして、スイッチで IVR を有効にします。
Note 変更をコミットできるのは、選択したスイッチで CFS が有効になっている場合だけです。
- ステップ 2** スイッチを選択し、**[アクション (Actions)]** > **[中止 (Abort)]** の順に選択し、**[適用 (Apply)]** をクリックしてスイッチの IVR を無効にします。
- ステップ 3** スイッチを選択し、**[アクション (Actions)]** > **[クリア (Clear)]** を選択し、**[適用 (Apply)]** をクリックして、スイッチの IVR 情報をクリアします。
- ステップ 4** スイッチを選択し、**[アクション (Actions)]** > **[CFS の有効化 (Enable CFS)]** の順に選択し、**[適用 (Apply)]** をクリックしてスイッチで CFS を有効にします。
- ステップ 5** スイッチを選択し、**[アクション (Actions)]** > **[グローバル CFS を無効にする (Disable Global CFS)]** を選択し、**[適用 (Apply)]** をクリックして、スイッチで CFS をグローバルに有効にします。

次の表では、**[アクション (Action)]** に表示されるフィールドおよび説明について記述します。

アクション	説明
スイッチ	スイッチの IP アドレスを指定します。
アクティブ	スイッチのアクティブステータスが true または false であることを指定します。
アクティベーション時間	アクティベーションの日付と時刻を指定します。
IVR NAT ステータス	IVR ステータスを有効にするか無効にするかを指定します。
自動検出トポロジ	自動検出トポロジステータスが true か false かを指定します

アクション	説明
編集	[編集 (Edit)] アイコンをクリックして、選択した行の IVR NAT ステータス列と自動検出トポロジ列の変更を実行します。
地域ID	スイッチのリージョン ID を指定します。
編集	[編集 (Edit)] アイコンをクリックして、選択した行の [続きを読む (Read from)] 列および [リージョン ID (Region ID)] 列の変更を実行します。
適用	[適用 (Apply)] をクリックして、スイッチの変更ごとに変更を保存します。
リフレッシュ	表を更新するには、 更新 アイコンをクリックします。
完了	[完了 (Done)] をクリックしてすべての変更を保存し、CFS ウィンドウを終了します。

ゾーンセット

選択したファブリック、VSAN、およびスイッチに基づいて、[ゾーンセット (Zoneset)] エリアには、設定されたゾーンセットとそのステータスが表示されます。ゾーンセットを作成、コピー、削除、または編集できます。さらに、ゾーンセットはアクティブ化または非アクティブ化できます。

次の表では、SAN コントローラの [**仮想管理 (Virtual Management)**] > [**ゾーン分割 (Zoning)**] [ゾーンセット (Zonesets)] タブに表示されるフィールドと説明について説明します。

フィールド	説明
ゾーンセット名	選択したゾーンセットの下で設定されているすべての名前を一覧表示します。
変更日	ゾーンセットが変更されているかどうかを表示します。
ゾーン	選択したゾーンセットの下に設定されているすべてのゾーンを一覧表示します。
メンバー	選択したゾーンに存在するメンバーを一覧表示します。
アクティブ化された日付	ゾーンセットがアクティブ化された日付を指定します。

手順

ステップ 1 SAN コントローラ Web UI からゾーンセットを作成するには、[アクション (Actions)] > [ゾーンセットの作成 (Create Zoneset)] の順に選択します。

[ゾーンセットの作成 (Create Zoneset)] ウィンドウが表示されます。

ステップ 2 ゾーンセットの有効な名前を入力し、[ゾーンセットの作成 (Create zoneset)] をクリックします。

ゾーンセットが作成され、[ゾーンセット (Zoneset)] エリアに表示されます。

ステップ 3 ゾーンセットをコピー/複製するには、オプションボタンを選択し、[アクション (Actions)] > [ゾーンセットのコピー/複製 (Copy/Clone Zoneset)] を選択するか、必要なゾーン名の最後の列にある [楕円 (ellipse)] アイコンをクリックします。

[ゾーンセットのコピーまたは複製 (Clone or Copy Zoneset)] ウィンドウには 2 つのオプションが表示されます。

適切なオプションボタンを選択します。次のいずれかを選択できます。

- **[コピー (Copy)]** : 初期ゾーンセットのゾーンのコピーで構成される新しいゾーンセットを作成します。
 - コピーされたゾーンセットを識別するために、文字列を先頭または末尾に追加できます。[タグ (Tag)] フィールドに有効な文字列を入力し、[名前の負荷 (Prepend names)] または [名前の追加 (Append names)] オプションボタンを選択します。
 - **[複製 (Clone)]** : ソースゾーンセットと同じゾーンで構成される新しい名前での新しいゾーンセットを作成します。

[名前 (Name)] フィールドに、新しいゾーンセットの有効な名前を入力します。

- **[ゾーンセットのコピー (Copy zoneset)]** をクリックして、ゾーンセットを複製またはコピーします。

複製またはコピーされたゾーンセットが [ゾーンセット (Zoneset)] エリアに表示されません。

ステップ 4 ゾーンセットを削除するには、[ゾーンセット名 (Zoneset Name)] 列の横にある [ゾーンセット (zoneset)] オプションボタンを選択し、[アクション (Actions)] > [ゾーンセットの削除 (Delete Zoneset)] の順に選択します。

確認ウィンドウが表示されます。[はい (Yes)] をクリックして、ゾーンセットを削除します。

ステップ 5 ゾーン名を編集するには、[ゾーンセット名 (Zoneset Name)] 列の横にあるゾーンオプションボタンを選択し、[アクション (Actions)] > [ゾーンとメンバーの編集 (Edit zones & member)] を選択するか、必要なゾーン名の最後の列にある [楕円 (ellipse)] アイコンをクリックします。

選択したファブリックの [ゾーンセット (Zoneset)] ページが表示されます。

[ゾーン名 (Zone Name)] 列の横にあるチェックボックスをオンにして、[アクション (Actions)]>[ゾーン名の変更 (Rename zone)]の順に選択します。

ゾーンセットの新しい名前を入力します。[Rename] をクリックします。

ステップ 6 ゾーンセットを非アクティブ化するには、[ゾーンセット名 (Zoneset Name)] 列の横にある [ゾーンセット] オプションボタンを選択し、[アクション (Actions)]>[非アクティブ化 (Deactivate)] をクリックします。

確認ウィンドウが表示されます。[はい (Yes)] をクリックして、ゾーンセットを非アクティブにします。

ステップ 7 ゾーンセットをアクティブにするには、[ゾーンセット名 (Zoneset Name)] 列の横にあるオプションボタンを選択し、[アクティブ化 (Activate)] をクリックします。

[ゾーンセットの差異 (Zoneset Differences)] ウィンドウには、以前にアクティブ化されてからゾーンセットに加えられた変更が表示されます。[Activate] をクリックします。

ゾーン

UIパス : [仮想管理 (Virtual Management)]> ゾーン分割 (Zoning) 。ゾーンメンバーを選択すると、スライドインパネルが表示されます。[起動 (Launch)] アイコンをクリックして、[ゾーン (Zones)] ウィンドウを表示します。

選択したゾーンセットに基づいて、そのゾーンセットの下に構成されているゾーンが [ゾーン (Zones)] エリアに表示されます。[ゾーン (Zones)] タブを表示するには、ゾーンセットのオプションボタンをクリックし、[アクション (Actions)]>[ゾーンとメンバーの編集 (Edit zones & members)] を選択します。[ゾーンセット (Zoneset)] ウィンドウが表示されます。また、VSANに有効になっているスマートゾーンがある場合にのみ、true または false が表示されます。

ゾーンを作成、コピー、削除、または複製し、名前を変更することができます。また、VSANに有効になっているスマートゾーンがある場合にのみ、true または false が表示されます。さらに、選択したゾーンセットにゾーンを追加または削除できます。ゾーンテーブルでスマートゾーンを有効または無効にすることもできます。

ゾーンエリアには、次のフィールドとその説明があります。

フィールド	説明
属性別フィルタ処理	必要なゾーン名またはゾーンセットとメンバーを指定して検索できます。
ゾーンセットに追加	ゾーン名を選択し、[ゾーンセットに追加 (Add to zoneset)] をクリックします。
リフレッシュ	表を更新するには、更新 アイコンをクリックします。

フィールド	説明
Zone Name	ゾーンの名前を表示します。 ゾーン名を指定して検索できます。
ゾーンセット内	ゾーンがゾーンセットの一部であるかどうかを指定します。 ゾーンがゾーンセットの一部である場合は true を表示します。それ以外の場合は、 false を表示します。 [ゾーンセット内 (In Zoneset)] ドロップダウンリストから true または false を選択して検索できます。
メンバー	ゾーンのゾーンメンバーを指定します。 メンバーを指定して検索できます。

Procedure

- ステップ 1** ゾーンを作成するには、**[仮想的な管理 (Virtual Management)] > [ゾーン分割 (Zoning)]** を選択します。
- ステップ 2** **[ゾーンセット (Zonesets)]** エリアで、必要なゾーンセット名を選択します。
スライドインパネルが表示されます。
- a) **[ゾーニングの編集 (Edit Zoning)]** または **[起動 (launch)]** アイコンをクリックして、**[ゾーンセット (Zoneset)]** ウィンドウを表示します。
デフォルトでは、**[ゾーン (Zones)]** タブが表示されます。
- ステップ 3** ゾーンを作成するには、**[アクション (Actions)] > [新しいゾーンの作成 (Create new zone)]** を選択します。
- a) **[新しいゾーンの作成 (Create new zone)]** で、ゾーンの有効な名前を入力し、**[作成 (Create)]** をクリックします。
- b) **[新しいゾーンの作成 (Create new zone)]** をクリックします。
- c) **[スマートゾーン分割 (Smart Zoning)]** の横にある選択ボックスを選択して、新しいゾーンのスマートゾーン分割を有効にします。
ゾーンが作成され、**[ゾーン (Zones)]** エリアに一覧表示されます。
- ステップ 4** スマートゾーンを有効にするには、**[ゾーン名 (Zone Name)]** の横にある必要なチェックボックスをオンにして、**[アクション (Actions)] > [スマートゾーンを有効にする (Enable smart zoning)]** を選択します。
スマートゾーン列は、VSANでスマートゾーン分割が有効になっている場合にのみ表示できます。

ステップ 5 スマートゾーンを無効にするには、[ゾーン名 (Zone Name)] の横にある必要なチェックボックスをオンにして、[アクション (Actions)]、>[スマートゾーンを無効にする (Disable smart zoning)] の順に選択します。

ステップ 6 ゾーンを複製するには、[構成 (Configure)] > [SAN] > [ゾーン分割 (Zoning)] > [ゾーン (Zones)] を選択し、[ゾーン (Zone)] オプションボタンを選択して [ゾーンの複製 (Clone Zone)] アイコンをクリックします。

[ゾーンの複製 (Clone Zone)] ウィンドウが表示されます。

a) [名前 (Name)] フィールドに、新しいゾーンセットの有効な名前を入力します。

b) [クローン (Clone)] をクリックして、ゾーンを複製します。

複製されたゾーンが [ゾーン (Zones)] エリアに表示されます。

ステップ 7 ゾーンセットからゾーンの名前を変更するには、[ゾーン名 (Zone Name)] の横にある必要なチェックボックスをオンにして、[アクション (Actions)]、>[ゾーン名の変更 (Rename zone)] の順に選択します。

[名前 (Name)] フィールドに、ゾーンの新しい名前を入力して、[名前の変更 (Rename)] をクリックします。

ステップ 8 ゾーンセットからゾーンを削除するには、[ゾーン名 (Zone Name)] の横にある必須チェックボックスをオンにして、[アクション (Actions)]、>[ゾーンセットから削除 (Remove from zoneset)] の順に選択します。

選択したゾーンセットからゾーンが削除されます。ゾーン名の横にある緑色のチェックマークが消え、ゾーンがゾーンセットから削除されたことを示します。

ステップ 9 ゾーンセットからゾーンを削除するには、[ゾーン名 (Zone Name)] の横にある必要なチェックボックスをオンにして、[アクション (Actions)]、>[ゾーンの削除 (Delete zone)] の順に選択します。

単一または複数のゾーンを選択して、すぐに削除できます。

Note 選択したゾーンセットのメンバーであるゾーンは削除できません。ゾーンを削除するには、ゾーンセットからゾーンを削除します。

FC エイリアス

ナビゲーションパス : 仮想管理 > > ゾーン分割 > ゾーンセット > メンバー

SAN コントローラリリース 12.0.1a 以降、FC エイリアス機能は通常のゾーンでサポートされます。これは、1 つ以上の pWWN を必要な名前に関連付けるために使用されます。ゾーンメンバーを追加すると、FC エイリアスを追加したり、既存の FC エイリアスを削除したりできます。[FC エイリアス (FC Aliases)] タブには、以下のフィールドが表示されます。

- [FC エイリアス (FC Aliases)] : FC エイリアスの名前を指定します。
- [メンバー (Member)] : FC エイリアスに関連付けられたメンバーを指定します。

FC エイリアス操作を行うには、次の手順を実行します。

Procedure

- ステップ 1** [仮想的な管理 (Virtual Management)] > [通常ゾーン (Regular Zones)] を選択し、必要なゾーンセット名をクリックします。

スライドインパネル ウィンドウが表示されます。
- ステップ 2** [ゾーン分割の編集 (Edit Zoning)] または [起動 (launch)] アイコンをクリックして、[ゾーンセット (Zoneset)] ページを表示します。

ゾーンセットウィンドウが表示されます。
- ステップ 3** [FC エイリアス (FC Aliases)] タブをクリックして、[FC エイリアス (FC Aliases)] エリアを表示します。
- ステップ 4** 新しい FC エイリアスを作成するには、[アクション (Actions)] > [新しい FC エイリアスの作成 (Create new FC Alias)] の順に選択します。

[新しい FC エイリアスの作成 (Create new FC Alias)] ウィンドウが表示されます。

 - a) テキストフィールドに有効な名前を入力し、[FC エイリアスの作成 (Create FC Alias)] をクリックします。

FC エイリアスが作成され、[FC エイリアス (FC Aliases)] エリアに一覧表示されます。
- ステップ 5** 新しい FC エイリアスを削除するには、[FC エイリアス (FC Aliases)] 列の横にある必要なチェックボックスをオンにして、[アクション (Actions)] > [FC エイリアスの削除 (Delete FC Alias)] の順に選択します。

メンバー

UIパス : [仮想管理 (Virtual Management)] > [ゾーン分割 (Zoning)] > [ゾーンセット (Zon Sets)] > [メンバー (Members)]

選択したゾーンセットとゾーンに基づいて、[メンバー (Members)] エリアにゾーンメンバーとそのステータスが表示されます。メンバーの詳細を表示するには、[属性別フィルタ処理 (Filter by attributes)] テキストフィールドに必要なフィールド名を入力します。

メンバーエリアには、次のフィールドとその説明があります。

フィールド	説明
Parent	ゾーンメンバーの名前を表示します。 ゾーン名を指定して検索できます。
メンバー	ゾーンのメンバー名を表示します。

フィールド	説明
スイッチ	ゾーンメンバーがリンクされているスイッチを指定します。 スイッチを指定して検索できます。
インターフェイス	ゾーンメンバーが接続されているインターフェイスを指定します。 インターフェイスを指定して検索できます。
ステータス	ゾーンの状態を指定します。
ゾーン分割のタイプ	ゾーン分割のタイプを表示します。 WWN、FCID、FC エイリアス、または iSCSI、FQDN、デバイスエイリアス、IP サブネットなどのゾーン分割のタイプで検索できます。
FCID	ゾーンメンバーに関連付けられた FCID を指定します。 ゾーンメンバーに関連付けられている FCID を指定して検索できます。
pWWN	スイッチの pWWN を指定します。 スイッチの WWN を指定して検索できます。

ゾーンセットのメンバーを追加または削除できます。さらに、既存のメンバーを追加したり、既存の FC エイリアスをメンバーに追加したりすることもできます。

SAN コントローラ Web UI から、[仮想管理 (Virtual Management)] > [ゾーン分割 (Zoning)] > [ゾーンセット (Zoneset)] > [メンバー (Members)] を選択して、[ゾーンセット (Zoneset)] ウィンドウのメンバーエリアを表示します。

ゾーンセットとゾーンを選択して、ゾーンメンバーのリストを表示します。

Procedure

ステップ 1 新しいメンバーを作成するには、[メンバー (Members)] 領域で、[アクション (Actions)] > [新しいメンバーの作成 (Create new member)] の順に選択します。

[新しいメンバーの作成と追加 (Create and Add a new Member)] ウィンドウで、適切なゾーンのオプションボタンを選択します。

テキストフィールドに有効な名前を入力し、[メンバーの作成 (Create Member)] をクリックします。

オプションボタンセクションによるゾーンに基づいて、新しい名前は、すべてのゾーンではなく、選択されたゾーンのみにつけられます。たとえば、WWN ゾーンを選択した場合、テキストフィールドの名前は WWN ゾーンの名前です。同様に、[ドメインとポートゾーン (Domain & Port zone by)] を選択すると、ドメイン ID 番号とスイッチインターフェイス名になります。

[新しいメンバーの作成 (Create new Member)] では、現在ファブリックに存在しないゾーンにメンバーを追加できます。この機能は、デバイス検出ですべてのデバイスが検出されなかった場合に利用できます。追加可能な機能を使用すると、検出されたデバイスをゾーンに追加できます。

ステップ 2 ゾーンメンバーを削除するには、[親 (Parent)] 列の横にあるチェックボックスをオンにして、[アクション (Actions)] > [ゾーンからメンバーを削除 (Remove Member from zone(s))] をクリックします。

インスタンス内の複数のゾーンを選択して削除できます。

ステップ 3 既存のメンバーを追加するには、[アクション (Actions)] > [既存のメンバーの追加 (Add existing members)] の順に選択します。

[既存のメンバーの追加 (Add existing members)] ウィンドウが表示されます。

このウィンドウには、次のフィールドとその説明があります。

フィールド	説明
Zone By	[Zone by] 機能は、デバイス WWN またはデバイスエイリアスを使用して、デバイスをゾーンに追加する必要があるかどうかを決定します。 [Zone by : エンドポート (Zone By: End Ports)] を選択した場合、デバイスは WWN によってゾーンに追加されます。 同様に、デバイスエイリアスと FC エイリアスの場合、デバイスはそれぞれデバイスエイリアスと FC エイリアスによってゾーンに追加されます。選択した Zone by に基づいて、デバイスが表示されます。
メンバー名	ゾーンの名前を表示します。 ゾーン名を指定して検索できます。
Type	スイッチがストレージまたはホストであることを指定します。
スイッチ	ゾーンメンバーがリンクされているスイッチを指定します。 スイッチを指定して検索できます。
インターフェイス	ゾーンメンバーが接続されているインターフェイスを指定します。 インターフェイスを指定して検索できます。
pWWN	スイッチの pWWN を指定します。 スイッチの pWWN を指定して検索できます。
VSAN	ゾーンメンバーが属する VSAN を指定します。

ステップ 4 オプションで適切な [Zone by] を選択し、必要な [メンバー名 (Member Name)] を選択します。

ステップ 5 [メンバーの追加 (Add Members)] をクリックします。

Note 複数のゾーンを選択できます。ゾーンテーブルで現在選択されているすべてのゾーンのリストを示すダイアログが表示されます。



第 15 章

仮想インフラストラクチャ マネージャ

- [仮想インフラストラクチャ マネージャ \(187 ページ\)](#)
- [vCenter の可視化の追加 \(190 ページ\)](#)

仮想インフラストラクチャ マネージャ

UIパス : [仮想管理 (Virtual Management)]>[仮想インフラストラクチャ マネージャ (Virtual Infrastructure Manager)]



- (注) Cisco Nexus Dashboard ファブリックコントローラの仮想マシンのネットワーク可視化機能が有効になっていることを確認します。

次の表では、[仮想インフラストラクチャ マネージャ (Virtual Infrastructure Manager)] ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
[サーバ (Server)]	サーバー IP アドレスを指定します。
管理対象 (Managed)	管理対象または管理対象外のクラスタのステータスを指定します。
ステータス	追加されたクラスタの状態を指定します。
ユーザー (User)	クラスタを作成したユーザーを指定します。
最終更新時刻	クラスタの最終更新時刻を指定します。



- (注) **[更新 (Refresh)]** アイコンをクリックして、仮想インフラストラクチャ マネージャ テーブルを更新します。

次の表では、[アクション (Actions)] メニューのドロップダウンリストで、[仮想インフラストラクチャ マネージャ (Virtual Infrastructure Manager)] に表示されるアクション項目について説明します。

アクション項目	説明
インスタンスの追加	[アクション (Actions)] ドロップダウンリストから [インスタンスの追加 (Add Instance)] を選択します。詳細については、「インスタンスの追加」を参照してください。 (注) ルート上で同じ IP アドレスを設定していることを確認します。「ルート IP アドレスの設定」を参照してください。
インスタンスの編集	編集するインスタンスを選択します。[アクション (Actions)] ドロップダウンリストから [インスタンスの編集 (Edit Instance)] を選択します。必要な変更を行って、[保存 (Save)] をクリックします。[キャンセル (Cancel)] をクリックして、変更を破棄します。
インスタンスの削除	削除する1つ以上の必要なインスタンスを選択します。[アクション (Actions)] ドロップダウンリストから、[削除 (Delete)] を選択します。[確認 (Confirm)] をクリックしてインスタンスを削除します。[キャンセル (Cancel)] をクリックしてこの削除を破棄します。
インスタンスの再検出	再検出する1つ以上の必要なインスタンスを選択します。[アクション (Actions)] ドロップダウンリストから、[インスタンスの再検出 (Rediscover Instance(s))] を選択します。確認メッセージが表示されます。

詳細については、次を参照してください。

Cisco UCS B シリーズ ブレードサーバーのサポート

NDFC は、ファブリックインターコネクットの背後にある UCS タイプ B (シャーシ UCS) で実行されているホストをサポートします。この機能を使用するには、Cisco UCSM で vNIC の CDP を有効にする必要があります。



(注) デフォルトでは、CDP は Cisco UCSM で無効になっています。

参考のために、VMM-A と VMM-B の2つの VMM について考えてみましょう。Cisco UCS UCS B シリーズブレードサーバーの検出後、トポロジに青色の VMM-A と VMM-B がファブリックインターコネクット ノードであることが表示されます。トポロジの例を下図に示します。

UCSM で CDP を有効にするには、次の手順を使用して新しいネットワーク制御ポリシーを作成する必要があります。

1. USCM で、**[LAN]** を選択し、ポリシーを展開します。
2. **[ネットワーク制御ポリシー (Network Control Policies)]** を右クリックして、新しいポリシーを作成します。
3. **[名前 (Name)]** フィールド、にポリシーの名前を **EnableCDP** と入力します。
4. CDP の有効なオプションを選択します。



The screenshot shows a 'Create Network Control Policy' dialog box. The 'Name' field is filled with 'EnableCDP'. The 'CDP' section has 'Enabled' selected. The 'MAC Register Mode' has 'Only Native Vlan' selected. The 'Action on Uplink Fail' has 'Link Down' selected. The 'MAC Security' section has 'Forge' set to 'Allow'. There are 'OK' and 'Cancel' buttons at the bottom right.

5. **[OK]** をクリックしてポリシーを作成します。

新しいポリシーを ESX NIC に適用するには、次の手順を実行します。

- 更新された vNIC テンプレートを使用している場合は、ESXi vNIC の各 vNIC テンプレートを選択し、[ネットワーク制御ポリシー] ドロップダウンリストから EnableCDP ポリシーを適用します。
- vNIC テンプレートを使用していない場合は、更新されたサービス プロファイルテンプレートを使用します。各サービス プロファイルテンプレートに EnableCDP ポリシーを適用します。
- 1 回限りのサービスプロファイルを使用している場合（つまり、各サーバーが独自のサービスプロファイルを使用している場合）、すべてのサービスプロファイルに移動し、すべての vNIC で EnableCDP ポリシーを有効にする必要があります。

Cisco UCSM の詳細については、『[Cisco UCSM ネットワーク管理ガイド](#)』を参照してください。

ルータ IP アドレスの設定

IP アドレスを vCenter に追加する前に、Cisco Nexus ダッシュボードで同じ IP アドレスを設定する必要があります。

Cisco Nexus ダッシュボードでルータを設定するには、次の手順を実行します。

手順

-
- ステップ 1** [インフラストラクチャ (Infrastructure)] > [クラスタ設定 (Cluster Configuration)] を選択します。
- ステップ 2** [全般 (General)] タブの [ルータ (Routes)] カードで、[編集 (Edit)] アイコンをクリックします。
- [ルータ (Routes)] ウィンドウが表示されます。
- ステップ 3** IP アドレスを設定するには、[管理ネットワーク ルータの追加 (Add Management Network Routes)] をクリックし、必要な IP アドレスを入力して、[チェック (check)] アイコンをクリックします。
- ステップ 4** [保存 (Save)] をクリックします。

ルータ設定は、次の 2 つのシナリオによって管理されます。

1. アプリケーションサーバーである vCenter の場合、通常は管理ネットワーク経由で到達可能です。
2. vCenter によって管理される ESXi サーバーと、K8s インスタンスや OpenStack インスタンスをホストするベアメタルサーバーは、ファブリックネットワークに直接接続されます。したがって、それらはデータネットワークを介して到達可能です。

vCenter の可視化の追加

[仮想的な管理 (Virtual Management)] > [仮想インフラストラクチャ マネージャ (Virtual Infrastructure Manager)] に表示される [アクション (Actions)] メニューのドロップダウンリストで、さまざまなアクションを実行できます。

手順

-
- ステップ 1** [アクション (Actions)] [インスタンスの追加 (Add Instance)] を選択します。
- [インスタンスの追加 (Add Instance)] ウィンドウが表示されます。

Add Instance

Select Type

vCenter

Virtual Center Server IP Address or Domain*

192.168.1.1

Enter a valid IP Address or Domain

Username*

administrator@vsphere.local

Password*

.....

Cancel Add

- ステップ 2** [タイプの選択 (Select Type)] ドロップダウン リストから **[vCenter]** を選択します。
- 必要な IP アドレスまたはドメイン名とパスワードをそれぞれのフィールドに入力します。
- ステップ 3** [Add] をクリックします。
- 追加された vCenter クラスタは、**[仮想インフラストラクチャ マネージャ (Virtual Infrastructure Manager)]** ウィンドウで表示できます。
- ステップ 4** インスタンスを編集するには、必要な vCenter を選択して、**[アクション (Actions)] > [インスタンスの編集 (Edit Instance)]** を選択して、**[保存 (Save)]** をクリックします。
- 選択済みの vCenter クラスタのパスワードをアップデートし、ステータスを「管理対象」または「管理対象外」に変更できます。
- (注) 管理対象外ステータスの vCenter クラスタの場合、ダッシュボードでトポロジと vCenter クラスタの詳細を表示できません。
- ステップ 5** 1 つ以上の vCenter クラスタを削除するには、必要な vCenter を選択し、**[アクション (Actions)] > [インスタンスの削除 (Delete Instance(s))]** を選択して、**[変更の確認 (Confirm changes)]** をクリックします。
- (注) クラスタを削除すると、すべてのデータが削除されます。クラスタは、トポロジビューからも削除されます。
- ステップ 6** 1 つ以上の vCenter クラスタを再検出するには、必要な vCenter を選択して、**[アクション (Actions)] > [インスタンスの再検出 (Rediscover Instance(s))]** を選択します。
- 確認メッセージが表示されます。



第 III 部

設定

- [\[サーバ設定 \(Server Settings\)\] \(195 ページ\)](#)
- [Feature Manager \(197 ページ\)](#)
- [クレデンシャル管理 \(201 ページ\)](#)



第 16 章

[サーバ設定 (Server Settings)]

- [サーバ設定 \(195 ページ\)](#)

サーバ設定

デフォルト値として入力されるパラメータを設定できます。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI から Nexus ダッシュボード ファブリック コントローラ サーバのパラメータを設定するには、次の手順を実行します。

1. [設定 (Settings)] > [サーバ設定 (Server Settings)] を選択します。
サーバ設定はさまざまなタブに分類され、
2. 要件に基づいて設定を変更します。
3. [保存 (Save)] をクリックして設定を適用します。



第 17 章

Feature Manager

- [Feature Manager \(197 ページ\)](#)

Feature Manager

Cisco DCNM リリース 11.x では、DCNM のインストール時にインストール モードを選択する必要があります。リリース 12.0.1a 以降、Cisco Nexus ダッシュボード ファブリック コントローラでは Nexus Dashboard にサービスをインストールできます。Nexus ダッシュボード ファブリック コントローラ UI を起動すると、[機能管理 (Feature Management)] ページに 3 つの異なるインストールモードが表示されます。

Nexus ダッシュボード ファブリック コントローラ 12 では、機能セットを動的に有効にし、アプリケーションを拡張できます。[設定 (Settings)] > [機能管理 (Feature Management)] の順に選択して、インストーラタイプを選択し、選択した展開でいくつかの機能を有効または無効にします。

Cisco Nexus Dashboard から Nexus ダッシュボード ファブリック コントローラ を初めて起動すると、[機能管理 (Feature Management)] 画面が表示されます。機能セットを選択する前に、バックアップと復元の操作のみを実行できます。

[機能管理 (Feature Management)] ページで、次のインストール モードのいずれかを選択できます。

- ファブリック 検出
- ファブリック コントローラ
- SAN コントローラ

機能セットを選択した後、Nexus Dashboard から Cisco Nexus ダッシュボード ファブリック コントローラ を起動すると、次のログインから Dashboard ページが開きます。

フィーチャ セットの選択

Cisco Nexus ダッシュボード ファブリック コントローラ 12 を初めて起動すると、どのフィーチャセットも有効になりません。この状態で、バックアップと復元を実行して、DCNM 11.5(x)

データをNexusダッシュボードファブリックコントローラ 12に復元できます。Nexusダッシュボードファブリックコントローラはバックアップファイルからデータを読み取り、それに応じてインストーラタイプを選択します。

Cisco Nexusダッシュボードファブリックコントローラ Web UI からフィーチャセットを展開するには、次の手順を実行します。

手順

ステップ 1 [設定 (Settings)] > [機能管理 (Feature Management)] を選択します。

ステップ 2 ペルソナを選択して、デフォルトの機能セットを表示します。

Cisco NDFC ペルソナで使用できる機能については、「[各ペルソナの機能 \(198 ページ\)](#)」を参照してください。

ステップ 3 次の表で、機能セットで使用可能な機能名に対してチェックボックスをオンにします。

ステップ 4 [Apply] をクリックします。

フィーチャセットが展開されます。選択したアプリケーションが有効になります。フィーチャセットがインストールされていることを示すメッセージが表示されます。有効にするには更新する必要があります。

ステップ 5 ブラウザを更新して、選択したフィーチャセットとアプリケーションでNexusダッシュボードファブリックコントローラを展開します。

左側のペインには、展開されたフィーチャセットで特にサポートされている機能が表示されます。

各ペルソナの機能

次の表に、Cisco NDFC リリース 12.1.1e で使用可能な機能に関する情報を示します。

表 19: SAN コントローラペルソナで利用可能な機能

機能名	説明
パフォーマンス モニタリング	環境とインターフェ이스の統計をモニタリングする
SAN Insights	SAN 分析の可視化
VMM ビジュアライザ	仮想マシンのネットワーク可視化

機能セット全体での変更

Nexusダッシュボードファブリックコントローラ 12では、ある機能セットから別の機能セットに切り替えることができます。[設定 (Settings)] > [機能管理 (Feature Management)] を選

択します。次の表で、目的の機能セットとアプリケーションを選択します。[保存して続行 (Save and Continue)] をクリックします。ブラウザを更新して、新しい機能セットとアプリケーションでシスコ Nexus ダッシュボード ファブリック コントローラ の使用を開始します。

特定の展開でサポートされる機能/アプリケーションがいくつかあります。機能セットを変更すると、これらの機能の一部は新しい展開でサポートされません。次の表に、機能セットを変更できる前提条件と基準の詳細を示します。

表 20: 展開間でサポートされるスイッチング

送信元/宛先	ファブリック検出	ファブリック コントローラ	SAN コントローラ
ファブリック検出	-	ファブリック検出の展開では、モニタモードファブリックのみがサポートされます。機能セットを変更すると、ファブリック コントローラ 導入でファブリックを使用できません。	サポート対象外
ファブリック コントローラ	ファブリックセットを変更する前に、既存のファブリックを削除する必要があります。	Easy Fabric から IPFM ファブリック アプリケーションに変更する場合は、既存のファブリックを削除する必要があります。	サポート対象外
SAN コントローラ	サポート対象外	サポート対象外	-



第 18 章

クレデンシャル管理

- [SAN クレデンシャル管理, on page 201](#)

SAN クレデンシャル管理

[設定 (Settings)] [SAN クレデンシャル管理 (SAN Credentials Management)] を選択して、ファブリックシードスイッチへの SNMP アクセスの詳細を表示します。ユーザがすべてのファブリックへのアクセスを検証した場合は、ファブリックのすべてのシードスイッチの SNMP クレデンシャルが表示されます。

Cisco Nexus ダッシュボードファブリックコントローラのスイッチクレデンシャルウィンドウには、次のフィールドがあります。

フィールド	説明
シードスイッチ	スイッチの IP アドレス。
ユーザ名	Cisco Nexus ダッシュボードファブリックコントローラのユーザのユーザ名を指定します。
[パスワード (Password)]	スイッチ SNMP ユーザの暗号化形式を表示します。
SNMPv3 / SSH	SNMP プロトコルが検証されるかどうかを指定します。 デフォルト値は false です。
認証/プライバシー	認証プロトコルを指定します。 デフォルト値は [NOT_SET] です。
ステータス	スイッチのステータスを表示します。

Cisco Nexus ダッシュボードファブリックコントローラユーザが SNMP を使用してファブリックを設定する前に、ユーザはファブリックのシードスイッチに SNMP クレデンシャルを提供

し、検証する必要があります。ユーザがファブリック シード スイッチの有効なクレデンシャルを提供しない場合、[スイッチクレデンシャル (Switch Credentials)]テーブルに SNMPv3/SSH および AuthPrivacy フィールドのデフォルト値が表示されます。

次の表では、[アクション (Actions)]メニューのドロップダウンリストで、[設定 (Settings)] > [SAN クレデンシャル管理 (SAN Credentials Management)]に表示されるアクション項目について説明します。

アクション項目	説明
編集	テーブルから行を選択し、[編集 (Edit)]を選択してスイッチ クレデンシャル情報を更新します。
クリア (Clear)	スイッチ クレデンシャルをクリアします。
検証	スイッチ クレデンシャルを再検証します。



第 **IV** 部

操作

- イベント分析 (205 ページ)
- イメージ管理 (223 ページ)
- プログラム可能レポート (239 ページ)
- ライセンス管理 (247 ページ)
- テンプレート (Templates) (259 ページ)
- バックアップと復元 (301 ページ)
- NXAPI 証明書 (309 ページ)



第 19 章

イベント分析

ここでは、次の内容について説明します。

- [アラーム \(205 ページ\)](#)
- [イベント \(215 ページ\)](#)
- [アカウンティング \(220 ページ\)](#)
- [リモートクラスタ \(220 ページ\)](#)

アラーム

このタブには、さまざまなカテゴリに対して生成されたアラームが表示されます。このタブには、ID (オプション)、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、最終更新日 (オプション)、ポリシー、メッセージなどの情報が表示されます。このタブで [更新間隔 (Refresh Interval)] を指定できます。1 つ以上のアラームを選択し、[ステータスの変更 (Change Status)] ドロップダウンリストを使用して、アラームのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除 (Delete)] ボタンをクリックしてアラームを削除できます。

発行されたアラーム

UI パス : [操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] の順に選択します。

1. 新しいアラーム ポリシーを作成した後、[発生したアラーム (Alarms Raised)] タブに移動し、[更新 (Refresh)] アイコンをクリックして、作成したアラームを表示します。
新しく作成されたアラームが表示されます。
2. [アラーム (Alarms)] テーブルの [重大度 (Severity)] をクリックすると、同じ ITL/ITN フローで同じポリシーによって発生したアラームの履歴が表示されます。
3. [ポリシー (Policy)] 列の [ポリシー名 (Policy name)] をクリックして、チャートを表示します。
スライドイン ペインが表示され、内部にグラフが表示されます。

4. グラフを表示するには、ドロップダウン リストから必要なメトリックを選択します。



(注) これらのメトリックは、SAN Insights Anomaly Policy でのみ表示できます。

次の表では、[操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] > [発生したアラーム (Alarms Raised)] に表示されるフィールドについて説明します。

フィールド	説明
重大度	アラームの重大度を指定します
送信元	送信元の名前を指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
ポリシー	アラームのポリシーを指定します。
Message	メッセージを表示します。
Ack User	アラームを確認したユーザのユーザ名。

次の表では、[発行されたアラーム (Alarms Raised)] タブに表示される [アクション (Actions)] メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
確認応答あり	1つまたは複数のアラームを選択し、 確認 を選択します。アラームをブックマークし、[確認済み (Acknowledged)] の列に Ack User 名を追加できます。
未確認	1つまたは複数のアラームを選択し、 未確認 を選択して、ブックマークされたアラームを削除します。 (注) 確認済みアラームのみを未確認にすることができません。
クリア	アラームを選択し、 消去 を選択して、アラームポリシーを手動で消去します。 消去されたアラームは、[消去されたアラーム (Alarm Cleared)] タブに移動します。
アラームの削除	アラームを選択し、 削除 を選択してアラームを削除します。

クリアされたアラーム

UI パス : 操作 > イベント分析 > アラーム > クリアされたアラーム

[クリアされたアラーム (Alarms Cleared)] タブには、[発行されたアラーム (Alarms Raised)] タブでクリアされたアラームのリストがあります。このタブには、ID (オプション)、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、クリア時 (オプション)、クリア

元、ポリシー、メッセージなどの情報が表示されます。最大 90 日間、クリアされたアラームの詳細を表示できます。

1 つ以上のアラームを選択し、[アクション (Actions)] > [削除 (Delete)] をクリックしてそれらを削除できます。

次の表では、[発行されたアラーム (Alarms Raised)] タブに表示されるフィールドについて説明します。

フィールド	説明
重大度	アラームの重大度を指定します
送信元	送信元アラーム IP アドレスを指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
クリアされた時間	アラームがクリアされた時刻を指定します。
クリアしたユーザ	アラームをクリアしたユーザを指定します。
ポリシー	アラームのポリシーを指定します。
Message	アラームの CPU 使用率およびその他の詳細を指定します。
Ack User	確認応答されたユーザ ロール名を指定します。

次の表では、[発行されたアラーム (Alarms Raised)] タブに表示される [アクション (Actions)] メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
アラームの削除	アラームを選択し、[削除 (Delete)] を選択して、クリアされたアラームを削除します。

アラーム ポリシーの監視と追加

SAN コントローラでアラームを有効にし、[操作 (Operations)] > [イベント分析 (Analytics)] > [アラーム (Alarms)] に移動し、垂直タブの [アラーム ポリシー (Alarm Policies)] をクリックします。[外部アラームの有効化] チェックボックスが選択されていることを確認します。これを有効にするには、SAN Controller Server を再起動する必要があります。

SAN コントローラの登録済みSNMPリスナーにアラームを転送できます。Cisco SAN コントローラ Web UI から、[設定 (Settings)] > [サーバ設定 (Server Settings)] > [アラーム (Alarms)] を選択し、[外部アラームの有効化 (Enable external alarms)] チェックボックスがオンになっていることを確認します。これを有効にするには、SAN Controller Server を再起動する必要があります。

SANコントローラの登録済みSNMPリスナーにアラームを転送できます。Cisco SANコントローラ Web UIから、[設定 (Settings)] > [サーバ設定 (Server Settings)] > [アラーム (Alarms)] を選択し、alarm.trap.listener.address フィールドに外部ポートアドレスを入力し、[変更の適用 (Apply Changes)] をクリックして、SAN コントローラを再起動します。



- (注) [アラーム ポリシーの作成 (Alarm Policy creation)] ダイアログ ウィンドウで [転送 (Forwarding)] チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

次の表では、[操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] > [アラーム ポリシー (Alarms Policies)] に表示されるフィールドについて説明します。

フィールド	説明
名前	アラーム ポリシーの名前を指定します
説明	アラーム ポリシーの名前を指定します
ステータス	アラーム ポリシーのステータスを指定します。 <ul style="list-style-type: none"> • アクティブ • 非アクティブ
ポリシータイプ	ポリシーのタイプを指定します。 <ul style="list-style-type: none"> • デバイスのヘルス ポリシー • インターフェイスのヘルス ポリシー • syslog アラームポリシー • SAN Insights の異常ポリシー
Devices	アラーム ポリシーを適用するデバイスを指定します。
インターフェイス	インターフェイスを指定します。
詳細	ポリシーの詳細を指定します。

次の表では、[操作 (Actions)] メニュー ドロップダウン リストのアクション項目について説明します。この項目は、[操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] > [アラーム ポリシー (Alarms Policies)] に表示されます。

アクション項目	説明
新しいアラーム ポリシーの作成	新しいアラーム ポリシーを作成することを選択します。「 新しいアラーム ポリシーの作成 」の項を参照してください。
編集	アラーム ポリシーを編集するには、ポリシーを選択し、[編集 (Edit)] を選択します。

アクション項目	説明
削除	アラーム ポリシーを削除するには、ポリシーを選択し、 [削除 (Delete)] を選択します。
アクティブ化 (Activate)	アラーム ポリシーをアクティブ化して適用するには、ポリシーを選択し、 [アクティブ化 (Activate)] を選択します。
非アクティブ化	アラーム ポリシーを無効にして非アクティブにするには、ポリシーを選択し、 [非アクティブ化 (Deactivate)] を選択します。
インポート	.csv ファイルからアラーム ポリシーを一括でインポートする場合に選択します。
エクスポート	アラーム ポリシーを .csv ファイルから一括でエクスポートする場合に選択します。

次のアラーム ポリシーを追加できます。

- **デバイスヘルスポリシー**：デバイスヘルスポリシーを使用すると、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。
- **インターフェイスヘルスポリシー**：インターフェイスヘルスポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。
- **Syslog アラームポリシー**：Syslog アラームポリシーは、Syslog メッセージ形式のペアを定義します。1 つはアラームを発生させ、もう 1 つはアラームをクリアします。
- **San Insights Anomaly Policy**：San Insights Anomaly Policy では、SAN Insight データを使用して、ファブリック内の問題を特定するためのカスタマイズされたアラームを作成できます。

新しいアラーム ポリシーの作成

次のアラーム ポリシーを追加できます。

- デバイスのヘルス ポリシー
- インターフェイスのヘルス ポリシー
- syslog アラームポリシー
- SAN Insights の異常ポリシー

デバイスのヘルス ポリシー

デバイスヘルスポリシーを使用すると、デバイス ICMP 到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。

ポリシーを作成するデバイスを選択します。ポリシー名、説明、CPU使用率パラメータ、メモリ使用率パラメータ、環境温度パラメータ、デバイスの可用性」を参照してください。

インターフェイスのヘルス ポリシー

インターフェイスヘルスポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- **ポリシー名**：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- **説明**：このポリシーの簡単な説明を指定します。
- **転送**：Cisco Nexus DashboardファブリックコントローラSANコントローラの登録済みSNMPリスナーにアラームを転送できます。Web UI から、**[設定 (Settings)] > [サーバ設定 (Server Settings)] > [イベント (Events)]** を選択します。



(注) [アラームポリシーの作成 (Alarm Policy creation)] ダイアログウィンドウで**[転送 (Forwarding)]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- **電子メール**：アラームが作成、クリア、または重大度を変更されたときに、アラームイベントの電子メールを受信者に転送できます。SAN コントローラ Web UI から、**[設定 (Settings)] > [サーバ設定 (Server Settings)] > [イベント (Events)]** を選択します。SMTPパラメータを設定し、**[保存 (Save)]** をクリックして、SAN コントローラサービスを再起動します。
- **リンクステート**：リンクステートオプションを選択して、インターフェイスリンクのアップまたはダウンを確認します。リンクダウンの場合、アラームを発生させることができ、リンクアップでアラームをクリアできます。
- **帯域幅 (イン/アウト) :**
 - インバウンドエラー
 - アウトバウンドエラー
 - インバウンド破棄
 - アウトバウンド破棄

Syslog アラーム

Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。1つはアラームを発生させ、もう1つはアラームをクリアします。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- デバイス：このポリシーの範囲を定義します。このポリシーを適用する個々のデバイスまたはすべてのデバイスを選択します。
- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboard ファブリックコントローラ SAN コントローラの登録済み SNMP リスナーにアラームを転送できます。Web UI から、**[設定 (Settings)]** > **[サーバ設定 (Server Settings)]** > **[イベント (Events)]** を選択します。



(注) [アラームポリシーの作成 (Alarm Policy creation)] ダイアログ ウィンドウで **[転送 (Forwarding)]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。SAN コントローラ Web UI から、**[設定 (Settings)]** > **[サーバ設定 (Server Settings)]** > **[イベント (Events)]** を選択します。SMTP パラメータを設定し、**[保存 (Save)]** をクリックして、SAN コントローラ サービスを再起動します。
- 重大度：この syslog アラーム ポリシーの重大度レベルを定義します。選択肢は、Critical、Major、Minor、および Warning です。
- 識別子：発生およびクリア メッセージの識別子部分を指定します。
- Raise Regex：syslog 発生メッセージの形式を定義します。構文は次のとおりです。
Facility-Severity-Type：メッセージ
- Clear Regex：syslog クリアメッセージの形式を定義します。構文は次のとおりです。
Facility-Severity-Type：メッセージ

正規表現の定義は単純な式ですが、完全な正規表現ではありません。テキストの可変領域は、\$(LABEL) 構文を使用して示されます。各ラベルは、1つ以上の文字に対応する正規表現キャプチャグループ (+) を表します。2つのメッセージを関連付けるために、raise メッセージと clear メッセージの両方にある可変テキストが使用されます。識別子は、両方のメッセージに表示される1つ以上のラベルのシーケンスです。識別子は、ckearsyslog メッセージをアラームを発生させた syslog メッセージと照合するために使用されます。テキストがメッセージの1つだけに表示される場合は、ラベルを付けて識別子から除外できます。

例：「値」が「ID1-ID2」のポリシー

```
"syslogRaise": "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"
"syslogClear": "SVC-5-UP: $(ID1) module $(ID2) is up."
```

この例では、ID1 および ID2 ラベルをアラームとして検出するための識別子としてマークできます。この識別子は、対応する syslog メッセージで見つかります。ラベル「REASON」は昇格ですが、クリアメッセージにはありません。このラベルは、アラームをクリアする syslog メッセージに影響しないため、識別子から除外できます。

表 21: 例 1

識別子	ID1-ID2
正規表現を上げる	ETHERPORT-5-IF_ADMIN_UP : インターフェイス Ethernet15/1 で admin が起動されています。
正規表現のクリア	ETHERPORT-5-IF_DOWN_NONE : インターフェイス Ethernet15/1 がダウンしています (トランシーバ欠落)

上記の例では、正規表現は端末モニタに表示される syslog メッセージの一部です。

表 22: 例 2

Identifier	ID1-ID2
正規表現を上げる	ETH_PORT_CHANNEL-5-PORT_DOWN : \$ (ID1) : \$ (ID2) がダウンしています
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP : \$ (ID1) : \$ (ID2) が起動しています

表 23: 例 3:

Identifier	ID1-ID2
正規表現を上げる	ETHERPORT-5-IF_SFP_WARNING : Interface \$ (ID1) 、 High Rx Power Warning
Clear Regex	ETHERPORT-5-IF_SFP_WARNING : Interface \$ (ID1) 、 High Rx Power Warning clear

San Insights Anomaly ポリシー

Cisco Nexus Dashboard SAN コントローラリリース 12.0(1)から、新しいポリシータイプ saninsights が追加されました。この新しいポリシータイプは、問題を特定するためにカスタマイズできます。分析のために間隔データごとに保持する特定のフローに基づいて、アラームポリシーを作成できます。選択したフローがアラームポリシーと一致する場合は、ポリシーで定義されたパラメータに基づいてフローを維持します。

手順

-
- ステップ 1** [操作 (Operations)] > [イベント分析 (Event Analytics)] > [アラーム (Alarms)] の順に選択します。
- ステップ 2** [アラーム (Alarms)] タブで [アラーム ポリシー] を選択します。
- ステップ 3** [アクション (Actions)] > [新規アラーム ポリシーの作成 (Create new alarm policy)] の順に選択します。
- ステップ 4** [San Insights の異常ポリシー (San Insights Anomaly Policy)] オプションボタンを使用します。
- ステップ 5** 次のパラメータの詳細を指定します。
- [ポリシー名 (Policy Name)] : このポリシーの名前を指定します。一意の名前を指定する必要があります。
 - [説明 (Description)] : ポリシーの簡単な説明。
 - [転送 (Forwarding)] : 外部 SNMP リスナーへの転送アラームを有効にします。
 - [電子メール (Email)] : このポリシーのメール更新をメール ID に送信するには、チェックボックスを選択します。
- ステップ 6** ドロップダウン リストから時間を選択して、**キャプチャ時間**と**保持時間**を定義します。
- [キャプチャ時間 (Capture Time)] : 特定のポリシーに一致する各フローの間隔ごとのデータをキャプチャする時間の長さを指定します。
 - [保持時間 (Retention Time)] : (削除する前に) そのデータを保持する時間の長さを指定します。
- ステップ 7** ドロップダウン リストから時間または間隔を選択して**分析レベル**を定義し、ドロップダウン リストから**重大度**レベルを選択してこのポリシーの重大度を定義します。
- [分析レベル (Analysis Level)] : 特定のポリシーでチェックする必要があるフローデータの集約を指定します。中止ポリシーや失敗ポリシーなどの一部のポリシータイプは、即座に発生する場合に照合するロジックです (間隔レベル)。一部のポリシータイプは、しきい値を超えて維持されると異常ポリシーとして表示されます。たとえば、レベルの瞬間的な ECT または DAL のスパイクはアラームではありませんが、同じスパイク レベルが一定期間 (5 分または 1 時間) 続く場合は、調査する必要があります。
 - [重大度 (Severity)] : このポリシーが原因で発生するアラームに関連付けられる重大度を指定します。
- ステップ 8** 新しいルールを定義し、[新規ルールの追加 (Add new rule)] をクリックして必須フィールドを指定し、[新規ポリシーの作成 (Create new policy)] をクリックします。

- (注)
- 1つ以上の新しいルールと一致基準を定義して、フローを識別し、新しいポリシーを作成できます。
 - すべてのポリシーは、スイッチからレシーバにストリーミングされる各 ITL/ITN フロー レコードと照合されます。

作成されたアラームは、[アラーム (Alarms)] タブで確認できます。

イベント

このタブには、スイッチに対して生成されたイベントが表示されます。このタブには、Ack、確認済みユーザ、グループ、スイッチ、重大度、ファシリティ、タイプ、カウント、最終確認、説明などの情報が表示されます。1つ以上のイベントを選択し、[ステータスの変更 (Change Status)] ドロップダウンリストを使用して、そのステータスを確認または確認解除できます。また、1つ以上のアラームを選択し、[削除 (Delete)] ボタンをクリックしてアラームを削除できます。すべてのイベントを削除する場合は、[すべてを削除 (Delete All)] ボタンをクリックします。

次の表で、[操作 (Operations)] > [イベント分析 (Event Analytics)] > [イベント (Events)] に表示されるフィールドについて説明します。

フィールド	説明
グループ	ファブリックを指定します。
スイッチ	スイッチのホスト名を指定します。
重大度	イベントの重大度を指定します。
施設	イベントを作成するプロセスを指定します。 イベント ファシリティには、NDFC と syslog ファシリティとの2つのカテゴリがあります。Nexusダッシュボードファブリックコントローラファシリティは、Nexusダッシュボードファブリックコントローラ内部サービスによって生成されたイベントと、スイッチによって生成されたSNMPトラップを表します。syslogファシリティは、syslogメッセージを作成したマシンプロセスを表します。
タイプ	スイッチ/ファブリックの管理方法を指定します。
数	イベントが発生した回数を提供します。
作成時刻	イベントが作成された時刻を指定します。
前回の検出	イベントが最後に実行された時刻を指定します。

フィールド	説明
説明	イベントに提供される説明を指定します。
Ack	イベントを確認するかどうかを指定します。

次の表では、**[操作 (Actions)]**メニュー ドロップダウンリストで、**[操作 (Operations)]** > **[イベント分析 (Event Analytics)]** > **[イベント (Events)]** に表示されるアクション項目について説明します。

アクション項目	説明
確認応答あり	テーブルから1つ以上のイベントを選択し、 [確認 (Acknowledge)] アイコンを選択して、ファブリックのイベント情報を確認します。 ファブリックのイベントを確認すると、確認アイコンが [グループ (Group)] の横の [Ack] 列に表示されます。
未確認	テーブルから1つ以上のイベントを選択し、 [確認解除 (Unacknowledge)] アイコンを選択して、ファブリックのイベント情報を確認します。
削除	イベントを選択し、 [削除 (Delete)] をクリックします。
イベントのセットアップ	では新しいイベントを設定できます。詳細については、 イベントのセットアップ (216ページ) を参照してください。

イベントのセットアップ

Cisco Nexusダッシュボードファブリックコントローラ Web UI を使用してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 **[操作 (Operations)]** > **[イベント分析 (Event Analytics)]** > **[イベントのセットアップ (Event Setup)]** の順に選択します。**[アクション (Actions)]** ドロップダウンメニューから、**[イベントのセットアップ (Event Setup)]** を選択します。

ステップ 2 **[レシーバ (Receiver)]** タブで、次の手順を実行します。

- この機能を有効にするには、トグル ボタンを使用します。
- [Syslog メッセージを DB にコピー (Copy Syslog Messages to DB)]** を選択し、**[適用 (Apply)]** をクリックして syslog メッセージをデータベースにコピーします。このオプションを選択しない場合、イベントは Web クライアントのイベント ページに表示されません。2 番目のテーブルの列には、次の情報が表示されます。

- トラップを送信するスイッチ
- syslog を送信するスイッチ
- syslog アカウンティングを送信するスイッチ
- 遅延トラップを送信するスイッチ

c) [送信元 (Sources)] タブのテーブルには、関連付けられているファブリックとスイッチが表示されます。また、トラップと syslog に関する情報も表示されます。

ステップ 3 Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からシステムメッセージの通知転送を追加および削除するには、次の手順を実行します。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI は、電子メールまたは SNMPv1 トラップを介してファブリック イベントを転送します。一部の SMTP サーバでは、Nexus ダッシュボード ファブリック コントローラ から SMTP サーバに送信される電子メールに認証パラメータを追加する必要があります。Nexus ダッシュボード ファブリック コントローラ により認証を必要とする任意の SMTP サーバに送信される電子メールに認証パラメータを追加できます。この機能は、[設定 (Settings)] > [サーバ設定 (Server Settings)] > [イベント (Events)] タブで有効にします。

- a) [設定 (Settings)] > [サーバ設定 (Server Settings)] > [イベント (Events)] を選択します。イベント転送を有効にするには、[イベント転送を有効にする (Enable Event forwarding)] チェックボックスをオンにします。イベントの転送範囲、レシーバの電子メールアドレス、イベントの重大度、およびイベントのタイプが表示されます。説明の [正規表現 (Regex)] フィールドは、転送送信元がイベント フォワーダの追加時に転送元が Syslog として選択されている場合にのみ適用されます。
- b) SMTP サーバの詳細と送信元電子メールアドレスを指定します。スヌーズおよびイベントカウント フィルタを設定します。
- c) [Save (保存)] をクリックします。
- d) [操作 (Operations)] > [イベント分析 (Event Analytics)] の順に選択します。[操作 (Actions)] ドロップダウン リストから [ルールの追加 (Add Tags)] を選択します。
- e) [転送メソッド (Forwarding Method)] で、[電子メール] または [トラップ (Trap)] を選択します。

[トラップ (Trap)] を選択した場合は、ダイアログボックスに [アドレス (Address)] と [ポート (Port)] フィールドが追加されます。

- f) 電子メール転送メソッドを選択する場合は、[電子メールアドレス (Email Address)] フィールドに IP アドレスを入力します。トラップメソッドを選択する場合は、[アドレス (Address)] フィールドにトラップ レシーバの IP アドレスを入力し、ポート番号を指定します。

[アドレス (Address)] フィールドに IPv4 または IPv6 アドレスまたは DNS サーバ名を入力できます。

- g) [ファブリック (Fabric)] フィールドで、通知するすべてのグループまたは特定のファブリックを選択します。SAN インストーラの場合は、[VSAN 範囲 (VSAN Scope)] を選択

します。[すべて (All)] または [リスト (List)] オプションを選択できます。リストを選択した場合は、通知用の VSAN のリストを指定します。

h) [送信元] フィールドで、Nexus ダッシュボード ファブリック コントローラ または [Syslog] を選択します。

- Nexus ダッシュボード ファブリック コントローラ を選択すると、次のようになります。

1. [タイプ (Type)] ドロップダウン リストから、イベント タイプを選択します。
2. [ストレージポートのみ (Storage Ports Only)] チェックボックスをオンにして、ストレージポートのみを選択します。
3. [最低重大度 (Minimum Severity)] ドロップダウン リストで、受信するメッセージの重大度を選択します。
4. [追加 (Add)] をクリックして、通知を追加します。

- [Syslog] を選択した場合：

1. [ファシリティ (Facility)] リストから、syslog のファシリティを選択します。
2. syslog タイプを指定します。
3. [説明の正規表現 (Description Regex)] フィールドで、イベントの説明と一致する説明を指定します。
4. [最低重大度 (Minimum Severity)] ドロップダウン リストで、受信するメッセージの重大度を選択します。
5. [追加 (Add)] をクリックして、通知を追加します。

(注) [最低重大度 (Minimum Severity)] オプションは、[イベントタイプ (Event Type)] が [すべて (All)] に設定されている場合のみ使用できます。

Cisco Nexus ダッシュボード ファブリック コントローラが送信するトラップは、重大度タイプに対応しています。重大度タイプとともにテキストによる説明も提供されます。

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

i) [ルールの追加 (Add Rule)] をクリックします。

ステップ 4 Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からイベント抑制にルールを追加するには、次の手順を実行します。

Cisco Nexusダッシュボードファブリックコントローラでは、ユーザ指定のサブプレッサールールに基づいて、指定されたイベントを抑制することができます。このようなイベントは、Cisco Nexusダッシュボードファブリックコントローラ Web UIおよびSANクライアントには表示されません。イベントはNexusダッシュボードファブリックコントローラデータベースに保持されず、電子メールまたはSNMPトラップを介して転送されません。

テーブルからサブプレッサールールを表示、追加、変更、および削除できます。既存のイベントテーブルからサブプレッサールールを作成できます。テンプレートとして特定のイベントを選択し、ルールダイアログウィンドウを呼び出します。イベントの詳細は、イベントテーブルで選択したイベントから、ルール作成ダイアログウィンドウの入力フィールドに自動的に移植されます。

(注) Cisco Nexusダッシュボードファブリックコントローラ Web UI から EMC Call Home イベントを抑制することはできません。

- a) ルールの名前を指定します。
- b) イベント送信元に基づくルールに必要な**[範囲 (Scope)]**を選択します。

[範囲 (Scope)] ドロップダウンリストには、LANグループとポートグループが個別に表示されます。**[SAN/LAN]**、**[ポートグループ (Port Groups)]**、または**[任意 (Any)]**を選択できます。SANおよびLANの場合は、ファブリックまたはグループまたはスイッチレベルでイベントの範囲を選択します。ポートグループスコープのグループのみを選択できます。範囲として**[任意 (Any)]**を選択すると、サブプレッサールールがグローバルに適用されます。

- c) ファシリティ名を入力するか、SAN/LANスイッチイベントファシリティリストから選択します。

ファシリティを指定しない場合は、ワイルドカードが適用されます。

- d) ドロップダウンリストから**[イベントタイプ (Event Type)]**を選択します。

イベントタイプを指定しない場合は、ワイルドカードが適用されます。

- e) **[説明の照合 (Description Matching)]** フィールドで、一致する文字列または正規表現を指定します。

ルール照合エンジンは、Javaパターンクラスでサポートされている正規表現を使用して、イベントの説明テキストとの一致を検索します。

- f) **[アクティブ範囲 (Active Between)]** ボックスをオンにして、イベントが抑制される有効な時間範囲を選択します。

デフォルトでは、時間範囲は有効になっていません。つまり、ルールは常にアクティブです。

(注) 一般に、アカウンティングイベントを抑制しないでください。アカウンティングイベントの抑制ルールは、アカウンティング イベントが Nexusダッシュボードファブリック コントローラ またはソフトウェアのスイッチのアクションによって生成される特定のまれな状況でのみ作成できます。たとえば、Nexusダッシュボードファブリック コントローラと管理対象スイッチ間のパスワード同期中に、多数の「sync-snmp-password」AAA syslog イベントが自動的に生成されます。アカウンティング イベントを抑制するには、[サプレッサ (Suppressor)]テーブルに移動し、[イベント サプレッサ ルールの追加 (Add Event Suppressor Rule)]ダイアログ ウィンドウを呼び出します。

g) [ルールの追加 (Add Rule)]をクリックします。

アカウンティング

Cisco Nexusダッシュボードファブリック コントローラ Web UI でアカウンティング情報を表示できます。

次の表では、[操作 (Operations)]>[イベント分析 (Event Analytics)]>[アカウンティング (Accounting)]>に表示されるフィールドについて説明します。

フィールド	説明
ソース (Source)	送信元 SGT を指定します。
User Name	ユーザ名を指定します。
時間	イベントが作成された時刻を指定します。
説明	説明を表示します。
グループ	グループの名前を指定します。

次の表では、[操作 (Actions)]ドロップダウンリストのアクション項目について説明します。これらの項目は、[操作 (Operations)]>[イベント分析 (Event Analytics)]>[アカウンティング (Accounting)]に表示されます。

アクション項目	説明
削除	リストからアカウンティング情報を削除するには、行を選択して[削除 (Delete)]を選択します。

リモートクラスタ

このタブには、セットアップの各クラスタ内のクラスタとファブリックの数が表示されます。

クラスタ名をクリックして概要情報を表示します。起動アイコンをクリックして、クラスタの詳細な概要を表示できます。



第 20 章

イメージ管理

- ・イメージ管理 (223 ページ)

イメージ管理

デバイスを最新のソフトウェアバージョンに手動でアップグレードすると、時間がかかり、エラーが発生しやすくなります。迅速で信頼性の高いソフトウェアアップグレードを実現するために、イメージ管理はアップグレードの計画、スケジューリング、ダウンロード、およびモニタリングに関連する手順を自動化します。イメージ管理は、Cisco Nexus スイッチでのみサポートされます。



- (注) アップグレードする前に、Cisco Nexus 9000 シリーズ スイッチおよび Cisco Nexus 3000 シリーズ スイッチの POAP ブート モードが無効になっていることを確認します。POAP を無効にするには、スイッチ コンソールで `[no boot poap enable]` コマンドを実行します。ただし、アップグレード後に有効にすることができます。

[イメージ管理 (Image Management)] ウィンドウには次のタブがあり、[アクション (Actions)] 列にリストされている操作を実行できます。

タブ	アクション
概要	イメージのステージング イメージの検証 イメージのアップグレード ポリシーの変更 コンプライアンスの再計算
製品イメージ	イメージのアップロード 削除

タブ	アクション
イメージポリシー	イメージポリシーの作成 削除
履歴	履歴 (238 ページ)

ユーザ ロールが **network-admin** または **device-upg-admin** であり、次の操作を実行するために Nexus ダッシュボード ファブリック コントローラをフリーズしていないことを確認します。

- イメージをアップロードまたは削除します。
- イメージのインストール、削除、またはイメージのインストールを終了します。
- パッケージおよびパッチをインストールまたはアンインストールします。
- パッケージおよびパッチをアクティブ化または非アクティブ化します。
- イメージ管理ポリシーを追加または削除します (**network-admin** ユーザ ロールにのみ適用)。
- 管理ポリシーを表示します。

ユーザ ロールが **network-admin**、**network-stager**、**network-operator**、または **device-upg-admin** の場合は、任意のイメージインストールまたはデバイスアップグレードタスクを表示できます。Nexus ダッシュボード ファブリック コントローラがフリーズ モードの場合は、それらを表示することもできます。

スイッチ イメージをアップグレードするプロセスを次に示します。

1. Nexus ダッシュボード ファブリック コントローラへのスイッチを検出します。
2. イメージをアップロードします。
3. イメージ ポリシーを作成します。
4. イメージ ポリシーをスイッチに適用します。
5. スイッチでイメージをステージングします。
6. (任意) スイッチが中断のないアップグレードをサポートしているかどうかを検証します。
7. 適切にスイッチをアップグレードします。

概要

[概要 (Overview)] ウィンドウには、シスコ Nexus ダッシュボード ファブリック コントローラ で検出されたすべてのスイッチが表示されます。スイッチの現在のバージョン、スイッチに接続されているポリシー、ステータス、およびその他のイメージ関連情報などの情報を表示できます。エントリをフィルタリングおよびソートできます。

Nexusダッシュボード ファブリック コントローラ UI ナビゲーション

- [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。[アクション (Actions)] をクリックして、さまざまな操作を実行します。

実行するアクションに基づいて、[理由 (Reason)] 列の値が更新されます。

[概要 (Overview)] ウィンドウで以下のアクションを実行できます。

イメージのステージング

イメージポリシーをスイッチに適用した後、イメージをステージングします。イメージをステージングすると、ファイルがブートフラッシュにコピーされます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からイメージをステージングするには、次の手順を実行します。

始める前に

- デバイスでイメージをステージングする前に、選択したデバイスにポリシーをアタッチする必要があります。
- SAN コントローラでサポートされる NX-OS イメージの最小バージョンは 6.1(2)I1(1) です。

上記のバージョンより前の NX-OS バージョンを実行している Nexus 9000 または Nexus 3000 スイッチでイメージをステージングするには、**Use KSTACK to SCP on N9K, N3K** 値を False に設定する必要があります。Web UI で、[設定 (Settings)] > [サーバー設定 (Server Settings)] > [SSH] タブを選択します。[N9K, N3K で SCP に KSTACK を使用する (Use KSTACK to SCP on N9K, N3K)] チェックボックスをオフにします。サポートされているイメージバージョンをステージングする場合は、このチェックボックスをオンにします。

手順

ステップ 1 [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

(注) 複数のスイッチを選択してイメージをステージングできます。

ステップ 3 [アクション (Actions)] をクリックし、[イメージのステージング (Stage Image)] を選択します。

[インストールするイメージの選択 (Select Images to Install)] ウィンドウが表示されます。

このウィンドウでは、スイッチで使用可能な容量と必要な容量を確認できます。

- ステップ4** (任意) [ステー징するファイル (Files For Staging)] 列の下のハイパーリンクをクリックして、ブートフラッシュにコピーされるファイルを表示します。
- ステップ5** [ステージ (Stage)] をクリックします。
- [イメージ管理 (Image Management)] ウィンドウの [概要 (Overview)] タブに戻ります。
- ステップ6** (任意) [ステー징するイメージ (Image Staged)] 列でステータスを確認できます。
- ステップ7** (任意) ログを表示するには、[理由 (Reason)] 列の下のハイパーリンクをクリックします。

イメージの検証

スイッチをアップグレードする前に、中断のないアップグレードがサポートされているかどうかを検証できます。Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からイメージを検証するには、次の手順を実行します。

手順

- ステップ1** [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。
- ステップ2** チェックボックスをオンにしてスイッチを選択します。
- (注) 複数のスイッチを選択してイメージをステーキングできます。
- ステップ3** [アクション (Actions)] をクリックして [検証 (Validate)] を選択します。
- [検証 (Validate)] ダイアログボックスが表示されます。
- ステップ4** 破損のないアップグレードチェックボックスで [確認 (Confirm)] にチェックします。
- ステップ5** [Validate] をクリックします。
- [イメージ管理 (Image Management)] ウィンドウの [概要 (Overview)] タブに戻ります。
- ステップ6** (任意) [検証済み (Validated)] 列でステータスを確認できます。
- ステップ7** (任意) ログを表示するには、[理由 (Reason)] 列の下のハイパーリンクをクリックします。

イメージのアップグレード

スイッチをアップグレードまたはアンインストールできます。アップグレード グループ オプションを使用すると、複数のスイッチでイメージのアップグレードを瞬時にトリガーできます。このオプションは、アップグレード/ダウングレードオプションで選択できます。



- (注) 最大 12 個のスイッチを一度にアップグレードすることをお勧めします。12 個を超えるスイッチを選択した場合、アップグレードは順番に実行されます。

NX-OS スイッチのアップグレードオプション

- 中断：中断を伴うアップグレードの場合は、このオプションを選択します。
- [非中断を許可 (Allow Non-disruptive)]：中断のないアップグレードを許可する場合を選択します。[非中断を許可 (Allow Non Disruptive)] オプションを選択し、スイッチが非中断アップグレードをサポートしていない場合、中断アップグレードが実行されます。[強制中断なし (Force Non Disruptive)] を選択し、選択したスイッチが中断なしアップグレードをサポートしていない場合、スイッチの選択を確認するよう求める警告メッセージが表示されます。スイッチを選択または削除するには、チェックボックスを使用します。
- ロールが異なる複数のスイッチをアップグレード対象として選択すると、警告メッセージが表示され、スイッチの選択を確認するか、[確認 (Confirm)] をクリックしてアップグレードするか、[キャンセル (Cancel)] をクリックします。

同じグループにデバイスを追加するときに、以下の制限が適用されることを確認してください。そうでない場合、スイッチの選択を確認するための警告メッセージが表示されません。

- ファブリック内のすべてのピア、スパイン、ボーダー、ボーダーゲートウェイ、RP、または RR (ファブリック内で複数のスイッチが同じ役割を持つ場合)。



(注) 接続されたデバイスが作成またはアップグレードまたは変更グループから切り離された場合、アップグレードグループは自動的に削除されます。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からスイッチ イメージをアップグレードするには、次の手順を実行します。

手順

- ステップ 1** [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。
- ステップ 2** チェックボックスをオンにしてスイッチを選択します。
- ステップ 3** [アクション (Actions)] をクリックし、[アップグレード (Upgrade)] を選択します。
[アップグレード/アンインストール (Upgrade / Uninstall)] ウィンドウが表示されます。
- ステップ 4** チェックボックスをオンにして、アップグレードのタイプを選択します。
有効なオプションは、NXOS、EPLD、およびパッケージ (RPM / SMU) です。
- ステップ 5** NXOS、EPLD、またはパッケージを選択します。
 - a) アップグレードする方法に基づいて、ドロップダウンリストからアップグレードオプションを選択します。
 - b) (任意) [BIOS 適用 (BIOS Force)] チェックボックスをオンにします。

すべてのデバイスの検証ステータスを表示できます。

- c) [ゴールデン (Golden)] チェックボックスをオンにして、ゴールデンアップグレードを実行します。
- d) [モジュール番号 (Module Number)] フィールドにモジュール番号を入力します。

このフィールドの下にモジュールのステータスが表示されます。

- (注) • [パッケージ (Packages)] を選択すると、パッケージの詳細も表示できます。
- [アンインストール (Uninstall)] オプション ボタンを選択して、パッケージをアンインストールできます。

ステップ 6 [アップグレード (Upgrade)] をクリックします。

- (注) 複数のスイッチをアップグレードする場合、アップグレードステータスの更新には 30 ～ 40 分かかります。

モードの変更

デバイスのモードを変更できます。Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からデバイスのモードを変更するには、次の手順を実行します。

手順

ステップ 1 [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。

ステップ 2 チェックボックスをオンにして、モードを変更するスイッチを選択します。

- (注) 複数のスイッチを選択できます。

ステップ 3 [アクション (Actions)] > [モードの変更 (Change Mode)] をクリックします。

[モードの変更 (Change Mode)] ダイアログボックスが表示されます。

ステップ 4 ドロップダウン リストからモードを選択します。

有効なオプションは [標準 (Normal)] と [メンテナンス (Maintenance)] です。

ステップ 5 [保存して続Save and Deploy Now] または [Save and Deploy Later] をクリックします。

[Image Management] ウィンドウの [Overview] タブに戻ります。

グループの変更

Cisco NDFC リリース 12.1.1e から、[概要 (Overview)] ページのスイッチごとのグループ指定の変更で、接続または接続解除できます。

[グループの変更 (Modify Group)] を使用すると、任意のスイッチのセットを選択して、同じインスタンスでイメージ管理操作を実行できます。NDFC 管理者ロールは、アップグレードグループを構成できます。admin ロールは、必要なスイッチをアップグレードグループに追加できます。これらのアップグレードグループを使用して、イメージ管理を実行できます。

グループの変更でアタッチまたは分離することができます。すべてのスイッチをグループに接続することも、必要なスイッチだけをグループに接続することもできます。

グループにアタッチするために、スパイン、ボーダー、ボーダー ゲートウェイ、RP、RR など、さまざまなロールを持つ複数のスイッチを選択した場合、スイッチの選択を確認するための警告メッセージが表示されます。[確認 (Confirm)] をクリックしてグループにアタッチするか、[キャンセル (Cancel)] をクリックします。

デバイスグループを作成するには、次の手順を実行します。

手順

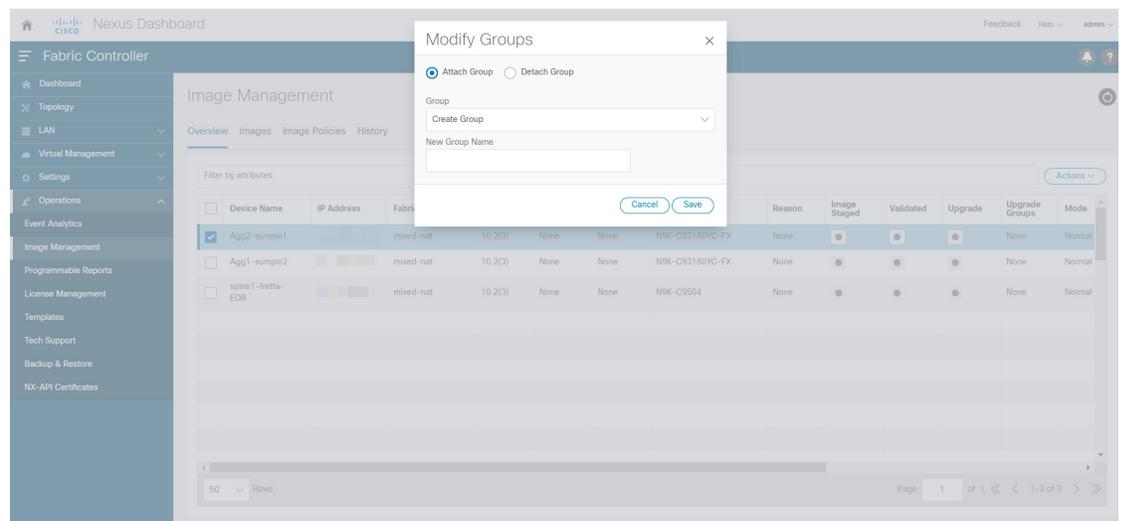
ステップ 1 [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。

ステップ 2 チェックボックスをオンにして、グループをアップグレードするデバイス名を選択します。

(注) 複数のデバイス名を選択して、同じグループに追加できます。

ステップ 3 [アクション (Actions)] > [グループの変更 (Modify Groups)] をクリックします。

[グループの変更 (Modify Groups)] ダイアログボックスが表示されます。



ステップ 4 選択したデバイス名のグループをアタッチするには。

- a) **[グループのアタッチ (Attach Group)]** オプションボタンを選択し、**[グループ (Group)]** ドロップダウンリストから **[グループの作成 (Create Group)]** を選択します。

[新しいグループ名 (New Group Name)] テキストフィールドが表示されます。

- b) テキストフィールドに必要な名前を入力し、**[保存 (Save)]** をクリックします。

全てのスイッチをグループにアタッチすることも、必要なスイッチだけをグループにアタッチすることもできます。スイッチの選択を確認するための警告メッセージが表示されます。**[確認 (Confirm)]** をクリックしてアタッチするか、**[キャンセル (Cancel)]** をクリックします。

以下のインスタンスのグループにデバイスが追加されると、警告メッセージが表示されます。

- 同じグループ内のファブリックで特定の役割を持つすべてのデバイスの場合
- ファブリック内のすべての RR が同じグループにある場合
- ファブリック内のすべての RP が同じグループにある場合
- 両方の vPC ピアが同じグループにある場合
- 同じグループのすべてのインバンドシードデバイスの場合

[概要 (Overview)] タブの **[グループのアップグレード (Upgrade group)]** 列で、アタッチされたグループ名を表示できます。

ステップ 5 デバイス名をグループから分離するには。

- a) 必要なデバイス名を選択し、**[アクション (Actions)]** > **[グループの変更 (Modify Groups)]** をクリックします。

[グループの変更 (Modify Groups)] ダイアログボックスが表示されます。

- a) **[グループの分離 (Detach Group)]** オプションボタンを選択し、**[分離 (Detach)]** をクリックします。

確認ウィンドウが表示されます。

- b) **[OK]** をクリックします。

ポリシーの変更

スイッチにアタッチしたイメージポリシーは更新できます。複数のスイッチのイメージポリシーを同時に変更することができます。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からスイッチにアタッチされたイメージポリシーをアタッチまたは変更するには、次の手順を実行します。

手順

- ステップ 1 [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。
- ステップ 2 チェックボックスをオンにしてスイッチを選択します。
- ステップ 3 [アクション (Actions)] をクリックし、[ポリシーの適用 (Apply Policy)] を選択します。
[ポリシーの変更 (Modify Policy)] ダイアログボックスが表示されます。
- ステップ 4 ポリシーをアタッチまたはアタッチ解除するには、必要なチェックボックスを選択します。
- ステップ 5 ドロップダウンリストからポリシーを選択します。
- ステップ 6 必要に応じて [アタッチ (Attach)] または [アタッチ解除 (Detach)] を選択します。
- ステップ 7 (任意) 変更を表示するには、[理由 (Reason)] 列の下のハイパーリンクをクリックします。
- ステップ 8 (任意) [ステータス (Status)] 列の下のハイパーリンクをクリックして、現在のイメージのバージョンと予期されるイメージのバージョンを表示します。
スイッチが **Out-Of-Sync** ステータスの場合は、予期されるイメージのバージョンを表示し、それに応じてスイッチをアップグレードします。

コンプライアンスの再計算

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からスイッチの設定コンプライアンスを再計算するには、次の手順を実行します。

手順

- ステップ 1 [オペレーション (Operations)] > [イメージ管理 (Image Management)] > [概要 (Overview)] を選択します。
- ステップ 2 チェックボックスをオンにしてスイッチを選択します。
- ステップ 3 [アクション (Actions)] をクリックし、[コンプライアンスの再計算 (Recalculate Compliance)] を選択します。
- ステップ 4 変更を表示するには、[理由 (Reason)] 列の下のハイパーリンクをクリックします。

レポートの実行

[レポート (Reports)] [レポート定義 (Report Definitions)] を選択します。

再度生成する必要があるレポートの横にあるチェックボックスをオンにします。[アクション (Actions)] ドロップダウンリストから [レポートの再実行 (Re-run Report)] を選択して、レポートジョブを再度実行します。レポートジョブが再実行されたことを示すポップアップウィンドウが表示されます。

[レポートの再実行 (Re-run Report)] を使用すれば、スケジュールされた実行時間の前にレポートを生成できます。オンデマンドジョブの場合は、[レポートの再実行 (Re-run Report)] をクリックしてレポートを生成します。

製品イメージ

このタブで、イメージとプラットフォームの詳細を表示できます。デバイスにイメージをアップロードまたは削除できます。

次の表で、[操作 (Operations)] > [イメージ管理 (Image Management)] > [イメージ (Images)] に表示されるフィールドについて説明します。

フィールド	説明
プラットフォーム	<p>プラットフォームの名前を指定します。イメージ、RPM、または SMU は、次のように分類されます。</p> <ul style="list-style-type: none"> • N9K/N3k • N6K • N7K • N77K • N5K • その他 • サードパーティ <p>N9K プラットフォームと N3K プラットフォームのイメージは同じです。</p> <p>アップロードされたイメージが既存のプラットフォームのいずれにもマッピングされていない場合、プラットフォームは [その他 (Other)] になります。</p> <p>プラットフォームは RPM の [サードパーティ (Third Party)] になります。</p>
ビット	イメージのビットを指定します。
イメージ名	アップロードしたイメージ、RPM、または SMU のファイル名を指定します。
イメージのタイプ	イメージ、EPLD、RPM、または SMU のファイルタイプを指定します。

フィールド	説明
イメージサブタイプ	イメージ、EPLD、RPM、またはSMUのファイルタイプを指定します。 ファイルタイプEPLDは[epld]です。イメージのファイルタイプは、[nxos]、[system]または[kickstart]です。RPMのファイルタイプは[feature]で、SMUのファイルタイプは[patch]です。
NXOSバージョン	CiscoスイッチのみのNXOSイメージバージョンを指定します。
イメージバージョン	Cisco以外のデバイスを含むすべてのデバイスのイメージバージョンを指定します。
サイズ (バイト)	イメージ、RPM、またはSMUファイルのサイズをバイト単位で指定します。
Checksum	イメージのチェックサムを指定します。チェックサムは、イメージ、RPM、またはSMUのファイルに破損がないかどうかをチェックします。CiscoのWebサイトからダウンロードしたファイルと[イメージのアップロード (Image Upload)]ウィンドウでアップロードしたファイルのチェックサム値が同じかどうかを確認することで、信頼性を検証できます。

次の表に、[アクション (Actions)]メニューのドロップダウンリストで、[操作 (Operations)] > [イメージ管理 (Image Management)] > [イメージ (Images)]に表示されるアクション項目を示します。

アクション項目	説明
更新	イメージテーブルを更新します。
アップロード	クリックして新しいイメージをアップロードします。この説明については、 イメージのアップロード (234 ページ) を参照してください。

アクション項目	説明
削除	<p>イメージをリポジトリから削除できます。</p> <p>イメージを選択して、[アクション (Actions)]、[削除 (Delete)] を選択します。確認ウィンドウが表示されます。[はい (Yes)] をクリックして、イメージを削除します。</p> <p>(注) イメージを削除する前に、イメージにアタッチされているポリシーがどのスイッチにもアタッチされていないことを確認してください。</p>

イメージのアップロード

32 ビットおよび 64 ビットのイメージをアップロードできます。Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からサーバにさまざまなタイプのイメージをアップロードするには、次の手順を実行します。



(注) デバイスは、POAP またはイメージのアップグレード中にこれらのイメージを使用します。すべてのイメージ、RPM、および SMU が [イメージポリシー (Image Policies)] ウィンドウで使用されます。

イメージをアップロードするには、ユーザーロールが **network-admin** または **device-upg-admin** である必要があります。 **network-stager** ユーザーロールでは、この操作を実行できません。

手順

ステップ 1 [操作 (Operations)]、[イメージ管理 (Image Management)]、[イメージ (Images)] の順に選択します。

ステップ 2 [アクション (Actions)] をクリックし、[アップロード (Upload)] を選択します。

[アップロード イメージ (Upload Image)] ダイアログ ボックスが表示されます。

ステップ 3 [ファイルの選択 (Choose file)] をクリックして、デバイスのローカル リポジトリからファイルを選択します。

ステップ 4 ファイルを選択し、[OK] をクリックします。

ZIP または TAR ファイルもアップロードできます。シスコ Nexus ダッシュボード ファブリック コントローラ はイメージファイル进行处理して検証し、それに応じて既存のプラットフォームで分類します。 **N9K/N3K**、**N6K**、**N7K**、**N77K**、または **N5K** プラットフォームに該当しない場合、イメージファイルは **サードパーティ** または **その他のプラットフォーム** に分類されます。 **サードパーティ** プラットフォームは、RPM にのみ適用されます。

ステップ 5 [OK] をクリックします。

EPLD イメージ、RPM、および SMU は、`/var/lib/dcnm/upload/<platform_name>` のリポジトリにアップロードされます。

(注) EPLD ファイルのみがアップロードされている場合、EPLD イメージの [リリース (Release)] ドロップダウンリストが空であるため、ポリシーを作成できません。

すべての NX-OS、キックスタートおよびシステム イメージは、`/var/lib/dcnm/images and /var/lib/dcnm/upload/<platform_name>` のパスのリポジトリにアップロードされます。

ファイル サイズとネットワーク帯域幅によっては、アップロードに時間がかかります。

(注) すべての Cisco Nexus シリーズ スイッチのイメージをアップロードできます。

Cisco Nexus 9000 シリーズ スイッチの EPLD イメージのみをアップロードできます。

ネットワークの速度が遅い場合は、Cisco Nexus ダッシュボード ファブリック コントローラの待機時間を 1 時間に増やして、イメージのアップロードを完了します。Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からの待機時間を増やすには、次の手順を実行します。

- a) [設定 (Settings)] > [サーバ設定 (Server Settings)] を選択します。
- b) **csrf.refresh.time** プロパティを検索し、値を **60** に設定します。
値は分単位です。
- c) [Apply Changes] をクリックします。
- d) Nexus ダッシュボード ファブリック コントローラ サーバを再起動します。

イメージポリシー

イメージ管理ポリシーには、RPM または SMU とともに NX-OS イメージの目的の情報が含まれます。ポリシーは特定のプラットフォームに属することができます。スイッチに適用されたポリシーに基づいて、Cisco Nexus ダッシュボード ファブリック コントローラでは必要な NXOS と RPM または SMU がスイッチに存在するかどうかを確認されます。スイッチ上のポリシーとイメージの間に不一致があると、ファブリック警告が生成されます。

次の表では、[アクション (Actions)] メニューのドロップダウンリストで、[操作 (Operations)] > [イメージ管理 (Image Management)] > [イメージポリシー (Images Policies)] に表示されるアクション項目について説明します。

アクション項目	説明
作成 (Create)	イメージに適用できるポリシーを作成できます。 イメージポリシーの作成 (236 ページ) を参照してください。

アクション項目	説明
Delete	<p>ポリシーを削除できます。</p> <p>ポリシーを選択して、[アクション (Actions)]、[削除 (Delete)]を選択します。確認ウィンドウが表示されます。[確認 (Confirm)]をクリックしてポリシーを削除します。</p> <p>(注) デバイスにアタッチされているポリシーを削除しようとする、エラーメッセージが表示されます。</p>
編集	ポリシーを編集できます。

イメージポリシーの作成

Cisco Web UI からイメージポリシーを作成するには、次の手順を実行します。Nexusダッシュボードファブリックコントローラ



(注) MDSプラットフォームおよびSAN展開のポリシーを作成する際に、一部のフィールドがグレー表示されます。

始める前に

イメージポリシーを作成する前に、[イメージ (Images)]タブでイメージをアップロードします。イメージのアップロードの詳細については、[を参照してください。イメージのアップロード \(234 ページ\)](#)

手順

ステップ 1 [操作 (Operations)] > [イメージ管理 (Image Management)] > [イメージポリシー (Image Policies)] の順に選択します。

ステップ 2 [アクション (Actions)] > [作成 (Create)] をクリックします。

[イメージ管理ポリシーの作成 (Create Image Management Policy)] ダイアログボックスが表示されます。

ステップ 3 必要なフィールドに情報を入力します。

[イメージ管理ポリシーの作成 (Create Image Management Policy)] ダイアログボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名	ポリシー名を入力します。

フィールド	アクション
プラットフォーム	プラットフォームドロップダウンリストからプラットフォームを選択します。オプションは、[イメージ (Images)] ウィンドウでアップロードしたイメージに基づいて入力されます。[リリース (Release)] ドロップダウンリストのオプションは、選択したプラットフォームに基づいて自動的に入力されます。
リリース	[リリース (Release)] ドロップダウンリストから NX-OS バージョンを選択します。 64 ビット イメージのリリース バージョンでは、イメージ名に 64 ビットが付加されます。 (注) EPLD ファイルのみがアップロードされている場合、EPLD イメージの [リリース (Release)] ドロップダウンリストが空であるため、ポリシーを作成できません。
パッケージ名	(任意) パッケージを選択します。特定のプラットフォーム (バージョンに依存しない) にアップロードされたすべてのパッケージを表示するには、[パッケージ (Packages)] を選択してから、[すべてのパッケージを表示 (View All Packages)] チェックボックスをオンにします。
[ポリシーの説明 (Policy Description)]	(任意) ポリシーの説明を入力します。
EPLD	(任意) ポリシーが EPLD イメージ用の場合は、[EPLD] チェックボックスをオンにします。
EPLD を選択します	(任意) EPLD イメージを選択します。
RPM の無効化	(任意) パッケージをアンインストールするには、このチェックボックスをオンにします。
アンインストールする RPM	(任意) アンインストールするパッケージをカンマで区切って入力します。[RPM 無効化 (RPM Disable)] チェックボックスをオンにした場合にのみ、パッケージ名を入力できます。

ステップ 4 [Save (保存)] をクリックします。

次のタスク

デバイスにポリシーをアタッチします。詳細については、[ポリシーの変更 \(230 ページ\)](#) セクションを参照してください。

履歴

すべてのイメージ管理操作の履歴は、[操作 (Operations)] [イメージ管理 (Image Management)] [履歴 (History)] タブで確認できます。

次の表では、この画面のフィールドについて説明します。

フィールド	説明
ID	ID 番号を指定します。
デバイス名 (Device Name)	デバイス名を指定します。
バージョン	デバイスのイメージバージョンを指定します。
ポリシー名	イメージにアタッチされるポリシー名を指定します。
ステータス	操作が成功したか失敗したかを表示します。
理由	操作の失敗の理由を示します。
操作タイプ	実行した操作のタイプを指定します。
Fabric Name (ファブリック名)	ファブリックの名前を指定します。
作成者	操作を実行したユーザー名を指定します。
タイムスタンプ	操作が実行された時刻を指定します。



第 21 章

プログラム可能レポート

[プログラム可能レポート (Programmable Reports)] アプリケーションでは、Python 2.7 スクリプトを使用してレポートを生成できます。レポートジョブは、レポートを生成するために実行されます。各レポートジョブは複数のレポートを生成できます。特定のデバイスまたはファブリックに対して実行するレポートをスケジュールできます。これらのレポートは、デバイスに関する詳細情報を取得するために分析されます。

[REPORT] テンプレートタイプは、[プログラム可能レポート (Programmable Reports)] 機能をサポートするために使用されます。このテンプレートには、[UPGRADE] と [GENERIC] の 2 つのテンプレート サブタイプがあります。REPORT テンプレートについては、[レポート テンプレート \(297 ページ\)](#) を参照してください。レポート生成を簡素化するために Python SDK が提供されています。この SDK は Nexus ダッシュボード ファブリック コントローラにバンドルされています。



- (注) Jython テンプレートは 100k バイトの最大ファイル サイズをサポートします。いずれかのレポート テンプレートがこのサイズを超えると、Jython の実行が失敗する可能性があります。

Nexus ダッシュボード ファブリック コントローラ UI ナビゲーション

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI でプログラム可能なレポートを起動するには、[オペレーション (Operations)] [プログラム可能レポート (Programmable Reports)] を選択します。 >

[レポート (Reports)] ウィンドウが表示されます。このウィンドウには、[レポート定義 (Report Definitions)] タブと [レポート (Reports)] タブがあります。[レポートの作成 (Create Report)] をクリックすると、両方のタブからレポートを作成できます。レポートジョブの作成については、「レポート ジョブの作成」を参照してください。[更新 (Refresh)] アイコンをクリックしてウィンドウを更新します。



(注) Cisco DCNM 11.5(x) から Nexus ダッシュボード ファブリック コントローラ リリース 12.0.1a にアップグレードした場合、レポートジョブおよび SAN ユーザー定義レポートは移行されません。手動で再度作成する必要があります。

この章は、次の項で構成されています。

- [レポートの作成 \(240 ページ\)](#)
- [レポート定義 \(242 ページ\)](#)
- [レポート \(244 ページ\)](#)

レポートの作成

[操作 (Operations)] > [プログラマブル レポート (Programmable Reports)] を選択します。
[Create Report] をクリックします。[レポートの作成 (Create Report)] ウィザードが表示されます。

レポート ジョブを作成するには、次の手順を実行します。

手順

ステップ 1 [レポート名 (Report Name)] フィールドにレポート ジョブの名前を入力します。

ステップ 2 [Select Template (テンプレートの選択)] をクリックします。

ステップ 3 ドロップダウンリストからレポートテンプレートを選択し、[選択 (Select)] をクリックします。

選択したテンプレートに基づいて、画面に表示されるフィールドに必要な値を入力します。

ステップ 4 [次へ (Next)] をクリックして、[ソースと繰り返し (Source & Recurrence)] のステップに進みます。

ステップ 5 レポート ジョブを実行する頻度を選択します。

次の表に、使用可能なオプションとそれらの説明を示します。

使用可能な方法	説明
現在	レポートは直ちに生成されます
毎日	レポートは、開始日と終了日の間の指定された時刻に毎日生成されます。
毎週	レポートは、開始日と終了日の間に指定された時刻に週に1回生成されます。
毎月	レポートは、開始日と終了日の間に指定された時刻に月に1回生成されます。

使用可能な方法	説明
Periodic	レポートは、指定された開始日と終了日の間の期間に定期的に生成されます。レポート間の時間間隔は、分単位または時間単位で指定できます。

(注) 定期的な NVE VNI カウンタ レポートを作成する場合は、レポート生成の間隔を 60 分以上に設定する必要があります。間隔が 60 分未満の場合は、エラーメッセージが表示されます。

ステップ 6 レポートを電子メールで送信する場合は、[電子メールレポート先 (Email Report To)] フィールドに電子メールの ID またはメーラーの ID を入力します。

[設定 (Settings)] [サーバ設定 (Server Settings)] [SMTP] タブで SMTP を設定する必要があります。データ サービスの IP アドレスがプライベート サブネットにある場合は、SMTP サーバーのスタティック管理ルートを Cisco Nexus Dashboard クラスタ設定に追加する必要があります。

ステップ 7 [デバイスの選択 (Select device(s))], [ファブリックの選択 (Select fabric(s))], または [VSAN の選択 (Select VSAN(s))] エリアでデバイス、ファブリック、または VSAN を選択します。

(注) 選択したテンプレートに基づいて、デバイス、ファブリック、または VSAN が読み込まれます。

ステップ 8 [Save (保存)] をクリックします。

新しいレポートが作成され、[レポート (Reports)] タブに表示されます。

レポート テンプレート

各レポート テンプレートには、いくつかのデータが関連付けられています。Nexus ダッシュボード ファブリック コントローラ で有効にした機能に応じて、使用可能なレポート テンプレートの一部は次のとおりです。

- Inventory_Report
- Performance_Report
- Switch_Performance_Report
- fabric_cloudsec_oper_status
- fabric_macsec_oper_status
- fabric_nve_vni_counter
- fabric_resources
- sfp_report

- switch_inventory

上記のテンプレートに加えて、作成した他のテンプレートもここに表示されます。デフォルトテンプレートとカスタマイズされたテンプレートの作成の詳細については、「テンプレートライブラリ」を参照してください。テンプレートは、関連するタグに基づいてリストされます。

Inventory_Report、**Performance_Report**、**Switch_Performance_Report** は、パフォーマンス管理レポートに使用されます。

レポート定義

[レポート定義 (**Report Definitions**)] タブには、ユーザが作成したレポートジョブが表示されます。

このタブで次の情報を表示できます。

フィールド	説明
タイトル (Title)	レポートジョブのタイトルを指定します。
テンプレート	テンプレート名を指定します。
範囲	レポートの範囲を指定します。
スコープタイプ	デバイスまたはファブリックのレポートを生成するかどうかを指定します。
ステータス	レポートのステータスを指定します。ステータスメッセージは次のとおりです。 <ul style="list-style-type: none"> • 正常：レポートが正常に生成されました。 • スケジュール済み：レポート生成スケジュールが設定されています。 • 実行中：レポートジョブが実行中です。 • 失敗：1つ以上の選択されたスイッチ/ファブリックでレポートの実行に失敗したか、レポートジョブの実行中に問題が発生しました。 • 不明：ジョブの状態を特定できませんでした。
スケジュール	レポートの実行をスケジュールする時刻を指定します。
前回の実行時間 (Last Run Time)	レポートが最後に生成された時刻を指定します。

フィールド	説明
ユーザ	レポート生成を開始したユーザを指定します。
繰り返し	レポートが生成される頻度を指定します。
内部	レポートがユーザによって生成されるか、ユーザまたは Nexus ダッシュボード ファブリック コントローラ によって生成されるかを指定します。レポートがユーザによって生成された場合、値は false です。

このタブで次のアクションを実行できます。



(注) 内部レポート定義に対してこれらのアクションを実行することはできません。

アクション	説明
編集	レポートを編集できます。 (注) レポート名とテンプレートは変更できません。
レポートの再実行	レポートを再実行できます。再実行オプションを使用して、スケジュールされた実行時間の前にレポートを生成できます。
履歴	レポート ジョブ履歴を表示できます。 [ジョブ履歴 (Job History)] ウィンドウが表示されます。レポート ジョブごとに複数のエントリを表示できます。 (注) 表示される定義の数は、 [設定 (Settings)] > [サーバ設定 (Server Settings)] > [レポート (Reports)] タブの次の設定によって定義されます。これらの値に基づいて、レポートと履歴が消去されます。 <ul style="list-style-type: none"> レポート定義全体の履歴の最大数 レポート定義あたりの最大レポート数
削除	レポート ジョブを削除できます。

レポート

[レポート (Reports)] タブには、ユーザが実行したレポートが表示されます。

このタブで次の情報を表示できます。

フィールド	説明
タイトル (Title)	<p>レポートのタイトルを指定します。</p> <ul style="list-style-type: none"> レポートのタイトルを1回クリックすると、サマリーパネルにスライドが表示されます。 レポートのタイトルをダブルクリックすると、[詳細とコマンド (Details and Commands)] ウィンドウが開きます。
テンプレート	テンプレート名を指定します。
範囲	レポートの範囲を指定します。
スコープタイプ	デバイスまたはファブリックのレポートを生成するかどうかを指定します。
ステータス	<p>レポートのステータスを指定します。ステータスメッセージは次のとおりです。</p> <ul style="list-style-type: none"> 完了 成功 実行中 FAILED 警告 スケジュール済み 不明ファイル
ユーザ	レポート生成を開始したユーザを指定します。
繰り返し	レポートが生成される頻度を指定します。
作成時刻	レポートをいつ作成するかを指定します。
内部	レポートがユーザによって作成されたかどうかを指定します。Nexusダッシュボードファブリックコントローラレポートがユーザによって作成された場合、値は <code>false</code> です。

このタブで次のアクションを実行できます。

アクション	説明
削除	レポートを削除できます。 (注) 内部レポートは削除できません。
比較 (2 レポート)	2つのレポートを並べて比較できます。レポートの詳細は、論理的にセクションにグループ化されます。 コマンドは、デバイスでコマンドを実行するために使用されるテンプレートと API に基づいて表示されます。たとえば、[switch_inventory] テンプレートでは、show version、show inventory、および show license usage コマンドを実行して情報を取得します。コマンドは、show_and_store API を使用してデバイスでコマンドを実行する場合にのみ表示されることに注意してください。
ダウンロード	レポートをダウンロードできます。ダウンロードするレポートを複数選択することはできません。



第 22 章

ライセンス管理

Cisco Nexus ダッシュボード ファブリック コントローラ リリース 12.0.1a 以降、次のものからサポートが削除されます。

- 評価ライセンスの状態はサポートされていません。
- サーバライセンスファイルはサポートされていません。

Cisco Smart Software Manager (CSSM) で既存のサーバライセンスファイルをスマートライセンスに変換する必要があります。詳細については、『[Cisco Smart Software Manager](#)』を参照してください。

この章は次のトピックで構成されています。

- [概要 \(247 ページ\)](#)
- [NDFC サーバライセンス \(248 ページ\)](#)
- [スマートライセンス \(250 ページ\)](#)
- [スイッチライセンス \(253 ページ\)](#)
- [スイッチライセンスファイル \(256 ページ\)](#)

概要

[操作 (Operations)] > [ライセンス管理 (License Management)] > [概要 (Overview)] を選択して、既存の Cisco Nexus ダッシュボード ファブリック コントローラのライセンスを表示できます。次のタブでライセンスを表示して割り当てることができます。

- NDFC
- スマート
- スイッチライセンス ファイル



(注) デフォルトでは、[概要 (Overview)] タブが表示されます。

[概要 (Overview)] タブには、NDFC、Switch、および Smart の 3 つのカードがあります。これらのカードには、購入するライセンスの総数と期限切れになるライセンスの総数が表示されます。

スマート ライセンシングを有効にするには、[スマート ライセンシングの設定 (Setup Smart Licensing)] をクリックします。スマート ライセンシングの詳細については、「スマートライセンス」の項を参照してください。

NDFC サーバライセンス

NDFC タブでは、各スイッチの NDFC ライセンスのステータスを確認できます。これらのライセンスは、デバイス、スマートライセンス、または名誉ライセンスまたはライセンスのないデバイスでプロビジョニングできます。

1 つまたは複数のスイッチを選択し、[アクション (Actions)]、>[割り当て (Assign)] または [すべて割り当て (Assign All)] をクリックします。

ライセンスをデバイスに割り当てると、NDFC ライセンスサービスは、デバイスの可用性、スマートライセンスのステータス、およびその他の要因に基づいて、使用可能なライセンスを割り当てます。

サーバベースのスマートライセンスは、Cisco MDS スイッチ、Nexus 9000、3000 7000、および 5000 シリーズのスイッチでサポートされます。

ローカルディレクトリからライセンスを追加するには、次の手順を実行します。

1. [ライセンスの追加 (Add license)] をクリックします。
[ライセンス ファイルの追加 (Add License File)] ウィンドウが表示されます。
2. [ライセンス ファイルの選択 (Select License File)] をクリックし、ローカルディレクトリから適切なファイルを選択します。
3. [アップロード (Upload)] をクリックし、[更新 (Refresh)] アイコンをクリックしてテーブルを更新し、アップロードされたライセンス ファイルを表示します。

ライセンスファイル名、ライセンスのタイプ、および有効期限の詳細がインポートされたライセンスファイルから抽出され、テーブルに表示されます。

次の表に、ライセンス管理 > NDFC に表示されるフィールドを示します。

フィールド	説明
スイッチ名	スイッチの名前が示されます。

フィールド	説明
License Type	次のいずれかの、スイッチのライセンス ステータスが示されます。 <ul style="list-style-type: none"> • スイッチ • スマート • スイッチ スマート
ステータス	次のいずれかの、スイッチのライセンス ステータスが示されます。 <ul style="list-style-type: none"> • 永続 • Unlicensed • スマート • Expired • N/A • 無効
期限日 (Expiration Date)	ライセンスの有効期限を指定します。
WWN/シャーシ ID	World Wide Name またはシャーシ ID を表示します。
モデル	デバイスのモデルが示されます。DS-C9124 や N5K-C5020P-BF など。
ファブリック	ファブリックの名前を指定します。

ライセンスを追加するには

次の表では、[アクション (Actions)] メニューのドロップダウン リストで、[ライセンス管理] > [NDFC] に表示されるアクション項目について説明します。

アクション項目	説明
割り当て	スイッチを選択し、[アクション (Actions)] ドロップダウン リストから [割り当て (Assign)] を選択します。 確認メッセージが表示されます。
割り当て解除	スイッチを選択し、[アクション (Actions)] ドロップダウン リストから [割り当て解除 (UnAssign)] を選択します。 確認メッセージが表示されます。

アクション項目	説明
すべて割り当て	<ul style="list-style-type: none"> • テーブル内のすべてのスイッチにライセンスを割り当てるには、[Actions] ドロップダウンリストから [Assign All] を選択します。 • 確認メッセージが表示されます。 • 表を更新するには、OK をクリックします。
すべて割り当て解除	<ul style="list-style-type: none"> • テーブル内のすべてのスイッチにライセンスを割り当て解除するには、[アクション (Actions)] ドロップダウンリストから [すべて割り当て解除 (UnAssign All)] を選択します。 • 確認メッセージが表示されます。 • 表を更新するには、OK をクリックします。

スマートライセンス

Cisco Nexus ダッシュボード ファブリック コントローラ では、スマートライセンスを設定することができ、スマートライセンス機能を使用してデバイスレベルでライセンスを管理し、必要に応じてライセンスを更新できます。

スマートライセンシングの概要

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements (MCE) は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります (<https://software.cisco.com/software/cs/ws/platform/home>)。

シスコライセンスの詳細な概要については、<https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html> を参照してください。

スマートなライセンス管理

Cisco NDFC リリース 12.0.2 から、スマートライセンスポリシーが導入されました。このポリシーはライセンスマイクロサービスで実行され、CSSMを使用してNDFCの高度な機能のライセンスを管理する機能を提供します。このリリースから、スマートライセンスの OnPrem またはオフラインモードを登録できます。

インターネットアクセスを使用してNDFCにスマートライセンスを直接登録すると、Cisco Nexus Dashboard は、ホスト名の代わりにIPアドレスを使用してスマートライセンスにアクセスし、エラーを表示します。

<https://smartreceiver.cisco.com> の IP アドレスのサブネットが、Cisco Nexus Dashboard のルーティング IP アドレスに追加されていることを確認します。

IPアドレスを追加するには、Cisco Nexus ダッシュボード Web UI で、[管理コンソール (Admin Console)] の [インフラストラクチャ (Infrastructure)] > [クラスタ構成 (Cluster Configuration)] > [ルート (Routes)] 領域に移動します。編集アイコンをクリックし、[管理ネットワーク ルート (Management Network Routes)] の IP アドレスを追加します。[保存 (Save)] をクリックして確認します。

[Smart] ページには、次のカードが表示されます。

- **スマートライセンシングの有効化**

トグルスイッチを使用して、スマートライセンシングを有効にします。有効にすると、スマートライセンスは、**信頼の確立**または**オフラインモード**の2つの方法で割り当てることができます。

- **信頼ステータス**

[**信頼を確立する (Establish Trust)**] をクリックして信頼を確立します。トランスポートゲートウェイ - CSLU を備えたオンプレミスを使用し、CSSM を介して Cisco のライセンスサーバーと直接接続するか、**プロキシ - 中間 HTTP または HTTPS プロキシ経由のプロキシ**を経由して接続するかの2つのオプションを表示することができます。

[Smart Licenseの信頼の確立]ウィンドウで、スマートライセンスエージェントとの信頼を確立するときに使用する転送タイプを選択します。

- シスコ ライセンシング サーバと直接通信するには、[**デフォルト (Default)**] を選択します。

- [**トランスポートゲートウェイ - CSLU を備えたオンプレミス (Transport Gateway - OnPrem with CSLU)**] を選択し、適切な URL を入力します。

ライセンスを有効にするために信頼トークンは必要ありません。CSSM とオンプレミス CSLU の間で信頼が確立されます。NDFC およびオンプレミス CSLU から、ローカル接続であることが予想されるため、信頼は一定です。

- プロキシサーバーを使用して転送するには、[**プロキシ - 中間 HTTP または HTTPS プロキシ経由のプロキシ (Proxy - Proxy via intermediate HTTP or HTTPS proxy)**] を選択します。プロキシサーバー経由でアクセスするための URL とポートの詳細を入力します。詳細については、[CSSM との信頼を確立するためにポリシーを使用したスマートライセンシング \(255 ページ\)](#) を参照してください。

デフォルトの転送を使用する場合は、CSSM から取得した登録トークンを入力します。



- (注) スマート ライセンシングを登録したら、既存のスイッチにライセンスを手動で割り当てる必要があります。登録後に検出されたすべてのスイッチについて、スマート ライセンシングが自動的にスイッチに割り当てられます。

• オフライン モード

オフラインモードでは、NDFC インスタンスと CSSM の間で代替的にデータを共有できません。エアギャップまたは切断された環境で動作している場合、オフラインモードを使用すると、状態をエクスポートして CSSM にアップロードし、応答を NDFC にインポートして戻すことができます。

ライセンスデータをエクスポートし、CSSM からの応答をインポートするには、以下の手順に従ってください。

1. [信頼ステータス (Trust Status)] で [オフラインモードに切り替える (Switch to Offline mode)] をクリックして、オフラインモードを有効にします。
2. 1つまたは複数のライセンスが割り当てられているオフラインモードで、[ライセンスデータのエクスポート (Export License Data)] をクリックします。
3. <https://software.cisco.com/software/cs/ws/platform/home> で、スマートライセンスセクションに移動し、[レポート (Reports)] タブをクリックして、後続の使用状況データファイルタブを選択します。NDFC からの使用状況レポートをアップロードし、数分後に応答をダウンロードして NDFC にインポートできます。
4. [ライセンスデータのインポート (Import License Data)] をクリックし、CSSM 確認応答ファイルを NDFC にアップロードします。

• ライセンスステータス

NDFC のライセンスのステータスを指定します。スマート ライセンシングが有効になっていない場合、値は **UNCONFIGURED** です。登録せずにスマート ライセンシングを有効にすると、値は **NO LICENSES IN USE** に設定されます。値は、ライセンスを登録して割り当てると、**IN USE** または **NOT IN USE** に設定されます。[ライセンス認証の詳細 (License Authorization Details)] ポップアップ ウィンドウで、最後のアクション、最後の認証試行、次の認証試行、および認証の有効期限を表示するには、ライセンス ステータスをクリックします。

ポリシーの詳細 をクリックして、スマートライセンスポリシーの詳細を表示します。最初の 90 日間のデフォルトのスマートライセンスポリシーと、そのレポートから 365 日以内の現在利用可能なレポートを表示できます。



- (注) 最初の登録から 30 日後にレポートを表示できます。

Resync

NDFC ライセンスの総数が CSSM ライセンスカウントと同じでない場合は、**[再同期 (Resync)]** をクリックしてライセンスカウントを更新します。

再同期により、スイッチインベントリ内の NDFC ライセンスのローカル監査が実行され、レポート用にスマートライセンス数が更新されます。

CSSM はスマートライセンスへの従来のライセンスの変換を可能にします。手順については、[「https://www.cisco.com/c/dam/en/us/products/se/2020/8/Collateral/brownfield-conversion-qrg.pdf](https://www.cisco.com/c/dam/en/us/products/se/2020/8/Collateral/brownfield-conversion-qrg.pdf)

ポリシーを使用してスマート ライセンシングからスマート ライセンシングに移行するには、Cisco Nexus Dashboard ファブリック コントローラを起動します。Web UI で、**[オペレーション (Operations)]** > **[ライセンス管理 (License Management)]** > **[スマート (Smart)]** タブの順に選択します。SLP を使用して CCSM との信頼を確立します。手順については、「[CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング \(255 ページ\)](#)」。

次の表で、「**スイッチ ライセンス**」の項に表示されるフィールドについて説明します。

フィールド	説明
名前	ライセンス名を指定します。
数	使用するライセンスの数を指定します。
ステータス	使用されているライセンスのステータスを指定します。有効な値は、 IN USE および NOT IN USE です。
説明	ライセンスのタイプと詳細を指定します。

ライセンスレポートをアップロードまたはダウンロードするには、<https://software.cisco.com/> に移動し、**[スマート ソフトウェア ライセンシング (Smart Software Licensing)]** > **[Reports (レポート)]** に移動します。**[使用状況データファイル (Usage Data Files)]** タブで、**[使用状況データのアップロード (Upload Usage Data)]** をクリックして、NDFC から使用状況レポートをアップロードします。レポートをアップロードしてから数分後、**[確認応答 (Acknowledgment)]** 列の **[ダウンロード (Upload Usage Data)]** をクリックして、NDFC に戻されてインポートされた応答をダウンロードします。

スイッチ ライセンス

スイッチがスマートライセンスで事前設定されている場合、Nexus ダッシュボード ファブリック コントローラ はスイッチのスマート ライセンスを検証して割り当てます。Nexus ダッシュボード ファブリック コントローラ Cisco UI を使用してスイッチにライセンスを割り当てるには、**[操作 (Operations)]** > **[ライセンス管理 (License Management)]** > **[スマート (Smart)]** を選択します。スマートライセンスを有効にするには、**[スマートライセンスの有効化 (Enable Smart Licensing)]** をクリックします。

スイッチベースのスマートライセンスは、MDS スイッチ、Nexus 9000、および 3000 シリーズのスイッチでサポートされます。



(注) 管理対象モードのスイッチの場合は、スイッチのスマートライセンスを Nexus ダッシュボード ファブリック コントローラ を介して割り当てる必要があります。

スイッチのスマート ライセンスを有効にするには、Nexus ダッシュボード ファブリック コントローラ の手順を実行します。

- 自由形式の CLI 設定を使用して、スイッチでスマート ライセンス機能を有効にします。
- スイッチで `feature license smart` または `license smart enable` コマンドを使用して、スマート ライセンシングを構成します。
- `license smart register id token` コマンドを使用して、デバイスのトークンをスマート アカウントにプッシュします。トークンをプッシュするには、Nexus ダッシュボード ファブリック コントローラ で **EXEC** オプションを使用します。

表を更新するには、**更新** アイコンをクリックします。

次の表に、**ライセンス管理 > スイッチ** に表示されるフィールドを示します。

フィールド	説明
スイッチ	スイッチの名前が表示されます。
機能	スイッチの機能を表示します。
ステータス	スイッチが使用中かどうかのステータスを表示します。 <ul style="list-style-type: none"> • 未使用 • 使用中 • 非準拠
タイプ	次のいずれかの、スイッチのライセンス ステータスが表示されます。 <ul style="list-style-type: none"> • 一時的 • 永続 • スマート • カウンター 永続 • Unlicensed • カウント
Warnings	有効期限など、ライセンスに関する警告を指定します。
グループ	ファブリック名または LAN 名を指定します。

CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング

Cisco Nexus Dashboard ファブリック コントローラのポリシーを使用してスマートライセンスを使用する CSSM との信頼を確立するには、次の手順を実行します。

始める前に

- Cisco Nexus Dashboard と CSSM の間にネットワーク到達可能性があることを確認します。ネットワーク到達可能性を設定するには、**Cisco Nexus Dashboard Web UI** を起動します。**[管理コンソール (Admin Console)]** で、**[インフラストラクチャ (Infrastructure)]** > **[クラスタ構成 (Cluster Configuration)]** > **[全般 (General)]** タブの順に選択します。**[ルート (Routes)]** 領域で、編集アイコンをクリックし、データ ネットワーク ルートの IP アドレスを追加します。**[保存 (Save)]** をクリックして確認します。
- CSSM からトークンを取得していることを確認します。

手順

- ステップ 1** **[操作 (Operations)]** > **[ライセンス管理 (License Management)]** > **[Smart]** タブの順に選択します。
- ステップ 2** スマートライセンスを有効にするには、**[スマートライセンスの有効化 (Enable Smart Licensing)]** をクリックします。
- ステップ 3** **[信頼ステータス (Trust Status)]** カードで、**[信頼の確立 (Establish Trust)]** をクリックします。
[スマートライセンスの信頼の確立 (Establish Trust for Smart License)] ウィンドウが表示されます。
- ステップ 4** スマートライセンス エージェントを登録するには、**[トランスポート (Transport)]** オプションを選択します。

次のオプションがあります。

- **デフォルト** : NDFC はシスコのライセンス サーバーと直接通信します
このオプションは、次の URL を使用します。 <https://smartreceiver.cisco.com/licservice/license>
- **トランスポートゲートウェイ** : CSLU オプションを備えたオンプレミス
CSLU トランスポート URL を入力します。
(注) CSLU トランスポート URL を使用するには、製品にライセンススマート URL を設定する必要があります。
- **プロキシ** : 中間 HTTP または HTTPS プロキシ経由のプロキシ
このオプションを選択する場合は、URL とポートを入力します。

ステップ 5 [トークン (Token)] フィールドに、CSSM から取得したトークンを貼り付けて、スマート ライセンスの信頼を確立します。

ステップ 6 [信頼の確立 (Establish Trust)] をクリックします。

確認メッセージが表示されます。

ステータスが UNTRUSTED から TRUSTED に変わります。スイッチ ライセンスの名前、数、およびステータスが表示されます。

[TRUSTED] をクリックして詳細を表示します。スイッチの詳細は、[ライセンス割り当て (License Assignments)] タブの [スイッチ/VDC (Switches/VDCs)] セクションで更新されます。スマート ライセンス オプションを使用してライセンスが付与されたスイッチのライセンス タイプとライセンス状態は Smart です。

ステップ 7 [NDFC] タブをクリックします。

ステップ 8 [アクション (Actions)] ドロップダウン リストから、[すべての割り当て (Assign All)] を選択します。

サーバー ライセンスの [ステータス (Status)] に [コンプライアンス内 (InCompliance)] が表示されます。

ステータスが [コンプライアンス外 (OutOfCompliance)] になっている場合は、CSSM ポータルにアクセスして必要なライセンスを取得します。

これ以外のすべてのステータスについては、シスコテクニカルアシスタンスセンター (TAC) にお問い合わせください。

スイッチ ライセンス ファイル

Cisco Nexusダッシュボードファブリック コントローラ では、1つのインスタンスで複数のライセンスをアップロードできます。Nexusダッシュボードファブリック コントローラ はライセンスファイルを解析し、スイッチのシリアル番号を抽出します。検出されたファブリックにライセンスファイルのシリアル番号をマッピングして、各スイッチにライセンスをインストールします。ライセンス ファイルがブート フラッシュに移動され、インストールされます。

次の表では、このタブのフィールドについて説明します。

フィールド	説明
スイッチ	スイッチ名を指定します。
IPのスイッチ	スイッチの IP アドレスを指定します。
ライセンスファイル	ライセンス ファイルのタイプを指定します。
ステータス	ライセンスのステータスを指定します。
Result Message	ライセンスの詳細を指定します。

フィールド	説明
最終アップロード時刻	サーバにアップロードされた日時を指定します。
機能	ライセンス機能を指定します。

スイッチ ライセンス ファイルの追加

Cisco Nexusダッシュボードファブリック コントローラ Web Client UI でスイッチにライセンスを一括インストールするには、次の手順を実行します。

手順

-
- ステップ 1** [操作 (Operations)] > [ライセンス管理 (License Management)] > [スイッチ ライセンス ファイル (Switch License Files)] を選択します。
- [スイッチ ライセンス ファイル (Switch License File)] ウィンドウが表示されます。
- ステップ 2** [スイッチ ライセンス ファイル (Switch License File)] タブで、[ライセンスの追加 (Add License)] をクリックして適切なライセンス ファイルをアップロードします。
- [ライセンス ファイルの追加 (Add License File)] ウィンドウが表示されます。
- ステップ 3** [ライセンスファイルの追加] で、[ライセンスファイルの選択] をクリックします。
- ローカルディレクトリにある適切なライセンス ファイルに移動して選択します。
- ステップ 4** [アップロード (Upload)] をクリックします。
- ライセンス ファイルが Nexusダッシュボードファブリック コントローラ にアップロードされています。次の情報がライセンス ファイルから抽出されます。
- スイッチ IP : このライセンスが割り当てられているスイッチの IP アドレス。
 - ライセンス ファイル : ライセンス ファイルのファイル名
 - 機能リスト : ライセンス ファイルでサポートされている機能のリスト
- ステップ 5** アップロードし、それぞれのスイッチにインストールするライセンスのセットを選択します。
- ライセンス ファイルは、単一の特定のスイッチに適用されます。
- ステップ 6** [アクション (Actions)] > [インストール (Install)] をクリックして、ライセンスをインストールします。
- 選択したライセンスがアップロードされ、それぞれのスイッチにインストールされます。問題やエラーを含むステータスメッセージは、ファイルが完了するたびに更新されます。
- ステップ 7** ライセンスがそれぞれのデバイスと一致し、インストールされると、[ステータス (Status)] 列にステータスが表示されます。
-



第 23 章

テンプレート (Templates)

- [テンプレート \(Templates\)](#) , on page 259

テンプレート (Templates)

UI ナビゲーション

- [オペレーション (Operations)] > [テンプレート (Templates)] を選択します。

Cisco Nexus ダッシュボード ファブリック コントローラ Web クライアントを使用して、異なる Cisco Nexus、IOS-XE、IOS-XR、および Cisco MDS プラットフォームで設定されているテンプレートを追加、編集、または削除できます。Cisco Nexus ダッシュボード ファブリック コントローラ Web クライアントで設定されているテンプレートごとに、次のパラメータが表示されます。テンプレートは JavaScript をサポートします。テンプレートの JavaScript 関数を使用して、テンプレートの構文で算術演算と文字列操作を実行できます。

Table 24: テンプレート テーブルのフィールドと説明

フィールド	説明
名前	テンプレート名を指定します。
サポートされるプラットフォーム	テンプレートがサポートするプラットフォームを指定します。
タイプ	テンプレート タイプを指定します。
サブタイプ	テンプレート サブタイプを指定します。
変更日	テンプレート変更の日時を指定します。
タグ (Tags)	テンプレートがファブリックまたはデバイスにタグ付けされているかどうかを指定します。
説明	テンプレートの説明を指定します。
参照カウント	テンプレートが使用される回数を指定します。

テーブルヘッダーをクリックすると、そのパラメータのアルファベット順にエントリがソートされます。



Note エラーのあるテンプレートは、[テンプレート (Templates)] ウィンドウに表示されません。エラーがあるテンプレートはインポートできません。このようなテンプレートをインポートするには、エラーを修正してインポートします。

次の表では、[テンプレート (Templates)] ウィンドウに表示される [アクション (Actions)] ドロップダウンリストのアクション項目について説明します。

Table 25: テンプレートのアクションと説明

Actions	説明
新しいテンプレートの作成	新しいテンプレートを作成できるようにします。詳細については、 新規テンプレートの作成 , on page 262を参照してください。
テンプレートのプロパティの編集	テンプレートのプロパティを編集できるようにします。一度に編集できるテンプレートは1つだけです。詳細については、 テンプレートの編集 , on page 264を参照してください。
テンプレートの内容の編集	テンプレートの内容を編集できるようにします。一度に編集できるテンプレートは1つだけです。詳細については、 テンプレートの編集 , on page 264を参照してください。
テンプレートの複数	<p>選択したテンプレートを別の名前で複製できるようにします。必要に応じて、テンプレートを編集できます。一度に複製できるテンプレートは1つだけです。</p> <p>テンプレートを複製するには、複製するテンプレートの横にあるチェックボックスをオンにし、[テンプレートの複製 (Duplicate template)] を選択します。[テンプレートの複製 (Duplicate template)] ウィンドウが表示されます。複製されるテンプレートの名前を指定します。複製されたテンプレートの詳細については、テンプレートの編集, on page 264を参照してください。</p>

Actions	説明
テンプレートの削除	<p>テンプレートを削除できるようにします。1つのインスタンスで複数のテンプレートを削除できます。</p> <p>ユーザ定義テンプレートを削除できます。ただし、事前定義されたテンプレートは削除できません。</p> <p>テンプレートを削除するには、削除するテンプレートの横にあるチェックボックスをオンにし、[テンプレートの削除 (Delete template)] を選択します。警告メッセージが表示されます。テンプレートを削除する場合は、[確認 (Confirm)] をクリックします。削除しない場合は、[キャンセル (Cancel)] をクリックします。テンプレートが使用中であるか、出荷テンプレートである場合は、削除できず、エラーメッセージが表示されます。</p> <p>Note 複数のテンプレートを選択して、同じインスタンスで削除します。</p> <p>テンプレートを完全に削除するには、ローカルディレクトリ Cisco Systems\dcn\ndfc\data\templates\にあるテンプレートを削除します。</p>
インポート	<p>ローカルディレクトリからテンプレートを1つずつインポートできます。詳細については、テンプレートのインポート, on page 265を参照してください。</p>

Actions	説明
Zip としてインポート	<p>.zip形式でバンドルされた複数のテンプレートを含む .zip ファイルをインポートできます</p> <p>ZIPファイル内のすべてのテンプレートが抽出され、個々のテンプレートとしてテーブルにリストされます。</p> <p>詳細については、「テンプレートのインポート, on page 265」を参照してください。</p> <p>Note Nexusダッシュボードファブリックコントローラ 仮想アプライアンス (OVAまたはISO) のPOAPテンプレートをインストールするには、POAPテンプレートのインストール, on page 266 を参照してください。</p> <p>。</p>
エクスポート	<p>ローカルディレクトリの場所にテンプレート設定をエクスポートできます。一度にエクスポートできるテンプレートは1つだけです。</p> <p>テンプレートをエクスポートするには、テンプレートの横にあるチェックボックスを使用して選択し、[エクスポート (Export)] を選択します。テンプレートファイルを保存するローカルシステムディレクトリの場所を選択します。[Save (保存)] をクリックします。テンプレートファイルがローカルディレクトリにエクスポートされます。</p>

network-operator ロールを持つテンプレートのみを表示できます。このロールでテンプレートを作成、編集、または保存することはできません。ただし、**network-stager** ロールを使用してテンプレートを作成または編集できます。

この項の内容は、次のとおりです。

新規テンプレートの作成

NexusダッシュボードファブリックコントローラUIナビゲーション

- **[オペレーション (Operations)]** > **[テンプレート (Templates)]** を選択します。

Cisco Nexusダッシュボードファブリックコントローラ Web UI からユーザ定義のテンプレートを作成し、ジョブをスケジュールするには、次の手順を実行します。

Procedure

ステップ 1 [テンプレート (Templates)] ウィンドウで、[アクション (Actions)] ドロップダウン リストから [新規テンプレートの作成 (Create new template)] を選択します。

[テンプレートの作成 (Create Template)] ウィンドウが表示されます。

ステップ 2 ウィンドウの [テンプレート プロパティ (Template Properties)] ページで、テンプレート名、説明、タグを指定し、新しいテンプレートのサポート対象プラットフォームを選択します。次に、ドロップダウン リストからテンプレート タイプとサブテンプレート タイプを選択します。ドロップダウン リストからテンプレートのコンテンツ タイプを選択します。

Note 基本テンプレートは CLI テンプレートです。

ステップ 3 [次へ (Next)] をクリックしてテンプレートの編集を続行するか、[キャンセル (Cancel)] をクリックして変更を破棄します。

編集したテンプレートのプロパティは、[テンプレートの編集 (Edit Template)] ウィンドウの [テンプレート コンテンツ (Template Content)] ページに表示されます。構成テンプレートの構造については、「テンプレートの構造」の項を参照してください。

ステップ 4 [検証 (Validate)] をクリックして、テンプレートの構文を検証します。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行 (Start Line)] 列の下に行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 5 [ヘルプ (Help)] をクリックして、右側の [エディタ (Help)] ペインを開きます。

このウィンドウには、テンプレートの作成に使用された形式、変数、コンテンツ、およびデータ型に関する詳細情報が表示されます。[エディタのヘルプ (Editor Help)] ペインを閉じます。

ステップ 6 リンクが表示されたら、エラーおよび警告をクリックします。エラーまたは警告がない場合、リンクは使用できません。エラーまたは警告が表示されている場合にリンクをクリックすると、右側に [エラーおよび警告 (Errors & Warnings)] ペインが表示され、エラーと警告が表示されます。[エラーおよび警告 (Errors & Warnings)] ペインを閉じます。

ステップ 7 テンプレート コンテンツを作成するには、必要なテーマ、キー バインディング、およびフォント サイズをドロップダウン リストから選択します。

ステップ 8 [完了 (Finish)] をクリックしてテンプレートの編集を完了し、[キャンセル (Cancel)] をクリックして変更を破棄し、[前へ (Previous)] をクリックして [テンプレート プロパティ (Template Properties)] ページに移動します。

テンプレートが作成されたことを示すメッセージのページが表示されます。このページには、テンプレート名、タイプ、サブタイプ、およびプラットフォームも表示されます。[別のテンプレートの作成 (Create another template)] をクリックしてもう 1 つのテンプレートを作成す

るか、[**Edit <template name> template**] をクリックして編集したばかりのテンプレートを編集します。

- ステップ 9** [テンプレートの編集 (**Edit Template**)] ウィンドウを閉じるか、[テンプレート ライブラリに戻る (**Back to template library**)] をクリックして[テンプレート (**Templates**)] ウィンドウに戻ります。

テンプレートの編集

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- [オペレーション (**Operations**)] > [テンプレート (**Templates**)] を選択します。

ユーザ定義のテンプレートを編集できます。ただし、定義済みのテンプレートおよびすでに公開されているテンプレートは編集できません。

[テンプレートの編集 (**Edit Template**)] ウィンドウを使用して、最初にテンプレートのプロパティを編集し、次にテンプレートの内容を編集します。さらに、[テンプレート プロパティの編集 (**Edit Template Properties**)] アクションを使用してテンプレート プロパティのみを編集するか、[テンプレート コンテンツの編集 (**Edit template content**)] アクションを使用してテンプレート コンテンツのみを編集できます。つまり、あるインスタンスでテンプレートのプロパティを編集してから、別のインスタンスでテンプレートの内容を編集できます。このウィンドウを使用して、テンプレートのプロパティとコンテンツを表示することもできます。

テンプレートのプロパティを編集し、テンプレートの内容を編集するには、次の手順を実行します。

Procedure

- ステップ 1** [テンプレート (**Templates**)] ウィンドウで、テンプレートを選択します。[アクション (**Actions**)] ドロップダウンリストから、[テンプレート プロパティの編集 (**Edit Template Properties**)] を選択します。
- [テンプレートの編集 (**Edit Template**)] ウィンドウが表示されます。
- ステップ 2** ウィンドウの [テンプレート プロパティ (**Template Properties**)] ページに、テンプレートの名前、その説明、サポートされるプラットフォーム、タグ、およびコンテンツタイプが表示されます。テンプレートの説明とタグを編集できます。サポートされているプラットフォームを編集するには、選択したチェックボックスをオフにして他のスイッチを選択します。次に、ドロップダウンリストからテンプレート タイプとサブテンプレート タイプを選択します。
- ステップ 3** [次へ (**Next**)] をクリックしてテンプレートの編集を続行するか、[キャンセル (**Cancel**)] をクリックして変更を破棄します。
- 編集したテンプレートのプロパティは、[テンプレートの編集 (**Edit Template**)] ウィンドウの [テンプレート コンテンツ (**Template Content**)] ページに表示されます。

ステップ4 [検証 (Validate)] をクリックして、テンプレートの構文を検証します。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行 (Start Line)] 列の下に行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ5 [ヘルプ (Help)] をクリックして、右側の [エディタ (Help)] ペインを開きます。

このウィンドウには、テンプレートの作成に使用された形式、変数、コンテンツ、およびデータ型に関する詳細情報が表示されます。[エディタのヘルプ (Editor Help)] ペインを閉じます。

ステップ6 リンクが表示されたら、エラーおよび警告をクリックします。エラーまたは警告がない場合、リンクは使用できません。エラーまたは警告が表示されている場合にリンクをクリックすると、右側に[エラーおよび警告 (Errors & Warnings)] ペインが表示され、エラーと警告が表示されます。[エラーおよび警告 (Errors & Warnings)] ペインを閉じます。

ステップ7 テンプレート コンテンツを作成するには、必要なテーマ、キーバインディング、およびフォントサイズをドロップダウンリストから選択します。

ステップ8 [完了 (Finish)] をクリックしてテンプレートの編集を完了し、[キャンセル (Cancel)] をクリックして変更を破棄し、[前へ (Previous)] をクリックして[テンプレート プロパティ (Template Properties)] ページに移動します。

テンプレートが保存されたことを示すメッセージが表示されたページが表示されます。このページには、テンプレート名、タイプ、サブタイプ、およびプラットフォームも表示されます。[別のテンプレートの作成 (Create another template)] をクリックしてもう1つのテンプレートを作成するか、[Edit <template name> template] をクリックして編集したばかりのテンプレートを編集します。

ステップ9 [テンプレートの編集 (Edit Template)] ウィンドウを閉じるか、[テンプレート ライブラリに戻る (Back to template library)] をクリックして[テンプレート (Templates)] ウィンドウに戻ります。

テンプレートのインポート

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- [オペレーション (Operations)] > [テンプレート (Templates)] を選択します。

zip形式のテンプレートをインポートする場合も、同じ手順に従います。



Note テンプレート内の「\n」は、インポートおよび編集されると改行文字と見なされますが、ZIPファイルとしてインポートされると正常に機能します。



Note Nexusダッシュボードファブリック コントローラ 仮想アプライアンス (OVAまたはISO) のPOAPテンプレートをインストールできます。詳細については、[POAPテンプレートのインストール, on page 266](#)を参照してください。

Cisco Nexusダッシュボードファブリック コントローラ Web UI からテンプレートをインポートするには、次の手順を実行します。

Procedure

ステップ 1 [テンプレート (Templates)] ウィンドウで、[アクション (Actions)] ドロップダウンリストから [テンプレートのインポート (Import template)] を選択します。

[テンプレートのインポート (Import Template)] ウィンドウが表示されます。

ステップ 2 コンピュータに保存されているテンプレートを参照して選択します。

ステップ 3 [OK] をクリックしてテンプレートをインポートするか、[キャンセル (Cancel)] をクリックしてテンプレートを破棄します。

Note 圧縮されたテンプレート ファイルをインポートすると、成功またはエラー メッセージが表示されます。[OK] をクリックします。

ステップ 4 必要に応じて、テンプレートパラメータとコンテンツを編集できます。詳細については、[テンプレートの編集 , on page 264](#)を参照してください。

Note 圧縮されたテンプレート ファイルをインポートすると、[テンプレートの編集 (Edit Template)] ウィンドウが表示されないことがあります。ただし、必要に応じて [テンプレートの編集 (Edit Template)] アクションを使用して、テンプレートパラメータとコンテンツを編集できます。

ステップ 5 テンプレートのプロパティまたはコンテンツを編集しない場合は、[次へ (Next)]、[完了 (Finish)]、[テンプレート ライブラリに戻る (Back to template library)] の順にクリックして、[テンプレート (Templates)] ウィンドウに戻ります。

POAP テンプレートのインストール

UI ナビゲーション

- [オペレーション (Operations)] > [テンプレート (Templates)] を選択します。

Cisco Nexusダッシュボードファブリック コントローラ では、異なる Cisco Nexus プラットフォームで設定されているユーザ定義テンプレートを追加、編集、または削除できます。Cisco Nexusダッシュボードファブリック コントローラ Release 10.0(x)以降、シスコ定義のFabricPath および IP VXLAN Programmable Fabric POAP テンプレートは、シスコの公式 Web サイトから

個別にダウンロードできます。これらのテンプレートは、Nexus 2000、Nexus 5000、Nexus 6000、Nexus 7000、およびNexus 9000 シリーズスイッチで使用する Nexusダッシュボードファブリック コントローラ 仮想アプライアンス（OVAまたはISO）で使用できます。

シスコ定義のテンプレートは、<https://software.cisco.com/download/release.html> からダウンロードできます。

Cisco Nexusダッシュボードファブリック コントローラ から POAP テンプレートをインストールするには、次のタスクを実行します。

手順

ステップ 1 <https://software.cisco.com/download/release.html> に移動し、ファイルをダウンロードします。

次のいずれかを選択できます。

- `ndfc_ip_vxlan_fabric_templates.10.0.1a.zip`
- `ndfc_fabricpath_fabric_templates.10.0.1a.zip` ファイル

ステップ 2 ファイルを解凍し、コンピューターのローカルディレクトリに抽出します。

ステップ 3 [アクション (Actions)] ドロップダウンリストから [テンプレートのインポート (Import Template)] をクリックします。

ステップ 4 コンピュータに保存されているテンプレートを参照して選択します。必要に応じて、テンプレートパラメータを編集できます。

ステップ 5 これらのテンプレートを POAP テンプレートとして指定するには、[POAP and Publish] チェックボックスをオンにします。

ステップ 6 [テンプレート構文の検証] をクリックして、テンプレートを検証します。

ステップ 7 [保存 (Save)] をクリックしてテンプレートを保存するか、[保存して終了 (Save and Exit)] をクリックしてテンプレートを保存して終了します。

テンプレート構造

構成テンプレートの内容は、主に4つの部分で構成されます。テンプレートのコンテンツの編集については、[テンプレート コンテンツ (Template Content)] の横にある [ヘルプ (Help)] アイコンをクリックします。

この項の内容は、次のとおりです。

テンプレートの形式

ここでは、テンプレートの基本情報について説明します。次の表に、使用可能なフィールドの詳細を示します。

プロパティ名	説明	有効な値	任意かどうか
名前 (name)	テンプレートの名前	テキスト	いいえ
説明	テンプレートに関する簡単な説明	テキスト (Text)	はい
userDefined	ユーザがテンプレートを作成したかどうかを示します。ユーザが作成した場合、値は「true」です。	「true」または「false」	はい
supportedPlatforms	この設定テンプレートをサポートするデバイスプラットフォームのリスト。すべてのプラットフォームをサポートするには、[All]を指定します。	N1K、N3K、N3500、N4K、N5K、N5500、N5600、N6K、N7K、N9K、MDS、VDC、N9K-9000v、IOS-XE、IOS-XR、その他、すべてのNexusスイッチのリストがカンマで区切られています。	いいえ

プロパティ名	説明	有効な値	任意かどうか
templateType	使用するテンプレートのタイプを指定します。	<ul style="list-style-type: none"> • CLI • POAP <p>Note POAP オプションは、Cisco Nexus ダッシュボードファブリックコントローラ LAN ファブリックの展開には適用されません。</p> <ul style="list-style-type: none"> • ポリシー • SHOW • プロファイル • ファブリック • [抽象 (ABSTRACT)] • レポート 	はい

プロパティ名	説明	有効な値	任意かどうか
templateSubType	テンプレートに関連付けられたサブタイプを指定します。		

プロパティ名	説明	有効な値	任意かどうか
		<ul style="list-style-type: none"> • CLI <li style="padding-left: 20px;">• なし • POAP <li style="padding-left: 20px;">• なし <li style="padding-left: 20px;">• VXLAN <li style="padding-left: 20px;">• FABRICPATH <li style="padding-left: 20px;">• VLAN <li style="padding-left: 20px;">• PMN <p>Note POAP オプションは、Cisco Nexus ダッシュボード ファブリックコントローラ LAN ファブリックの展開には適用されません。</p> <ul style="list-style-type: none"> • ポリシー <li style="padding-left: 20px;">• VLAN <li style="padding-left: 20px;">• interface-vlan <li style="padding-left: 20px;">• INTERFACE_VPC <li style="padding-left: 20px;">• INTERFACE_FHRNET <li style="padding-left: 20px;">• INTERFACE_BD <li style="padding-left: 20px;">• INTERFACE_CHANNEL 	

プロパティ名	説明	有効な値	任意かどうか
		<ul style="list-style-type: none"> • INTERFACE_FC • NIERFACE_MGMT • NIERFACE_COBACK • INTERFACE_NVE • INTERFACE_VFC • NIERFACE_CHANNEL • DEVICE • FEX • NIRA_FABCINK • NIER_FABCINK • INTERFACE • SHOW <ul style="list-style-type: none"> • VLAN • interface-vlan • INTERFACE_VFC • NIERFACE_ETHNET • INTERFACE_BD • NIERFACE_CHANNEL • INTERFACE_FC • NIERFACE_MGMT • NIERFACE_COBACK • INTERFACE_NVE • INTERFACE_VFC • NIERFACE_CHANNEL • DEVICE • FEX • NIRA_FABCINK • NIER_FABCINK • INTERFACE 	

プロパティ名	説明	有効な値	任意かどうか
		<ul style="list-style-type: none"> • プロファイル <ul style="list-style-type: none"> • VXLAN • ファブリック <ul style="list-style-type: none"> • 該当なし • [抽象 (ABSTRACT)] <ul style="list-style-type: none"> • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHNET • INTERFACE_BD • INTERFACE_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_OOB • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_PFC • DEVICE • FEX • INTERFACE_FABRIC • INTERFACE_FABRIC • INTERFACE • レポート <ul style="list-style-type: none"> • アップグレード • GENERIC 	

プロパティ名	説明	有効な値	任意かどうか
contentType			はい

プロパティ名	説明	有効な値	任意かどうか
		<ul style="list-style-type: none"> • CLI <ul style="list-style-type: none"> • TEMPLATE_CLI • POAP <ul style="list-style-type: none"> • TEMPLATE_CLI Note POAP オプション ション は、 Cisco Nexus ダッ シュ ボード ファブ リック コント ローラ LAN ファブ リック の展開 には適 用され ませ ん。 • ポリシー <ul style="list-style-type: none"> • TEMPLATE_CLI • PYTHON • SHOW <ul style="list-style-type: none"> • TEMPLATE_CLI • プロファイル <ul style="list-style-type: none"> • TEMPLATE_CLI • PYTHON • ファブリック <ul style="list-style-type: none"> • PYTHON 	

プロパティ名	説明	有効な値	任意かどうか
		<ul style="list-style-type: none"> • [抽象 (ABSTRACT)] • TEMPLATE_CLI • PYTHON • レポート • PYTHON 	
実装 (Implement)	抽象テンプレートを実装するために使用されます。	テキスト (Text)	はい
依存関係	スイッチの特定の機能を選択するために使用されます。	テキスト (Text)	はい
公開	テンプレートを読み取り専用としてマークし、変更を回避するために使用されます。	「true」または「false」	はい

テンプレート変数

このセクションには、テンプレートに使用されるパラメータの宣言された変数、データ型、デフォルト値、および有効な値の条件が含まれます。これらの宣言された変数は、動的コマンド生成プロセス中にテンプレート コンテンツ セクションの値の置換に使用されます。また、これらの変数は、意思決定およびテンプレート コンテンツ セクションの反復ブロックで使用されます。変数には事前定義されたデータ型があります。変数に関する説明を追加することもできます。次の表に、使用可能なデータ型の構文と使用方法を示します。

変数の型	有効値	反復可能?
boolean	true false	いいえ
enum	Example: running-config, startup-config	いいえ
浮動	浮動小数点形式	いいえ
floatRange	Example: 10.1, 50.01	はい
整数型 (Integer)	任意の数値	いいえ

変数の型	有効値	反復可能?
integerRange	「-」で区切られた連続する番号 「,」で区切られた個別の番号 Example: 1-10,15,18,20	はい
インターフェイス	形式: <if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	いいえ
interfaceRange	Example: eth10/1/20-25, eth11/1-5	はい
IPアドレス	IPv4 または IPv6 アドレス	いいえ
ipAddressList	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: 2001:0cb8:85a3:0000:0000:8a2e:0370:7334, 2001:0cb8:85a3:0000:0000:8a2e:0370:7335, 2001:0cb8:85a3:1230:0000:8a2f:0370:7334 Example 3: 172.22.31.97, 172.22.31.99, 2001:0cb8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254	はい
ipAddressWithoutPrefix	Example: 192.168.1.1 または Example: 1:2:3:4:5:6:7:8	いいえ
ipV4Address	IPv4 アドレス	いいえ
ipV4AddressWithSubnet	Example: 192.168.1.1/24	いいえ
ipV6Address	[IPv6 アドレス (IPv6 address)]	いいえ

変数の型	有効値	反復可能?
ipV6AddressWithPrefix	Example: 1:2:3:4:5:6:7:8 22	いいえ
ipV6AddressWithSubnet	IPv6アドレスとサブネット	いいえ
ISISNetAddress	Example: 49.0001.00a0.c96b.c490.00	いいえ
long	Example: 100	いいえ
MAC アドレス	14 または 17 文字長の MAC アドレス形式	いいえ
string	変数の説明などに使用される自由テキスト Example: string scheduledTime { regularExpr="^([01]\d 2[0-3]):([0-5]\d)\$"; }	いいえ
string[]	Example: {a,b,c,str1,str2}	はい
構造体	単一の変数にバンドルされているパラメータのセット。 <pre>struct <structure name declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; } [<structure_inst1>] [, <structure_inst2>] [, <structure_array_inst3 []>;</pre> <pre>struct interface_detail { string inf_name; string inf_description; ipAddress inf_host; enum duplex { validValues = auto, full, half; }; }myInterface, myInterfaceArray[];</pre>	いいえ Note 構造体変数が配列として宣言されている場合、変数は反復型です。

変数の型	有効値	反復可能?
wwn (Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントでのみ使用 可能)	Example: 20:01:00:08:02:11:05:03	いいえ

例：テンプレート変数

```
##template variables
integer VSAN_ID;
string SLOT_NUMBER;
integerRange PORT_RANGE;
integer VFC_PREFIX;
##
```

可変メタ プロパティ

テンプレート変数セクションで定義されている各変数には、一連のメタ プロパティがあります。メタ プロパティは、主に変数に定義されている検証ルールです。

次の表に、使用可能な変数タイプに適用されるさまざまなメタ プロパティを示します。

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
boolean	ブール値。 Example: true	はい											
enum			はい										
浮動	符号付き実数。 Example: 75.56, -8.5	はい	はい	はい	はい	はい							

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
frRng	符号付き実数の範囲 Example: 50.5 - 54.75	はい	はい	はい	はい	はい							
integer	符号付き実数 Example: 50, -75	はい	はい		はい	はい							
intRng	符号付き実数の範囲 Example: 50-65	はい	はい		はい	はい							
インターフェイス	インターフェイス/ポートを指定します Example: Ethernet 5/10	はい	はい				はい	はい	はい	はい			
intRng		はい	はい				はい	はい	はい	はい			

変数の型	説明	可変メタプロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
IPアドレス	IPv4またはIPv6形式のIPアドレス	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
<code>ipAcls</code>		はい											

変数の型	説明	可変メタプロパティ										
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長
	<p>IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。</p> <p>Example 1: 172.23.9, 172.23.9, 172.23.15, 172.23.10</p> <p>Example 2: 172.11.237, 172.11.237, 172.23.15,172.23.10</p> <p>Example 3: 172.23.9, 172.23.9, 172.11.237, 172.23.23</p> <p>Note</p>	リス										

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
		ト内のアドレスは、ハイフンではなくカンマで区切ります。											

変数の型	説明	可変メタプロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
ip4	IPv4 または IPv6 アドレス (プレフィックス/サブネットは不要)。												
ip4	IPv4 アドレス	はい											
ip4	IPv4 アドレスとサブネット	はい											
ip6	[IPv6 アドレス (IPv6 adrs)]	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
IPv6	プレフィックス付き IPv6 アドレス	はい											
IPv6	IPv6 アドレスとサブネット	はい											
IPv6	Example: 4008:6660												
long	Example: 100	はい			はい	はい							
MAC	MAC アドレス												
string	リテラル文字列 Example for string Regular expression string string { 01234 }	はい									はい	はい	はい

変数の型	説明	可変メタプロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
string[]	カンマ (,) で区切られた文字列リテラル Example: {string1, string2}	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
構造体	単一の変数にバンドルされているパラメータのセット。 struct <structure name definition > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ... } <struct1> [, <struct2> [, <struct3> [1]>;												
wwn	WWN アドレス												

例：メタ プロパティの使用

```

##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
string inf_name;
string inf_description;
ipAddress inf_host;
enum duplex {
validValues = auto, full, half;
};
}myInterface;

##

```

可変注釈

注釈を使用して変数をマーキングする変数プロパティを設定できます。



Note 可変注釈は、POAP でのみ使用できます。ただし、注釈はテンプレートタイプ「CLI」には影響しません。

テンプレート変数セクションでは、次の注釈を使用できます。

注釈キー	有効な値	説明
AutoPopulate	テキスト (Text)	あるフィールドから別のフィールドに値をコピーします。
DataDepend	テキスト	
説明	[テキスト (Text)]	ウィンドウに表示されるフィールドの説明
DisplayName	テキスト (Text) Note スペースがある場合は、テキストを引用符で囲みます。	ウィンドウに表示されるフィールドの表示名

注釈キー	有効な値	説明
列挙体	Text1、Text2、Text3 など	選択するテキストまたは数値をリストします
IsAlphaNumeric	「true」または「false」	文字列には、英数字を使用します。
IsAsn	「true」または「false」	
IsDestinationDevice	「true」または「false」	
IsDestinationFabric	「true」または「false」	
IsDestinationInterface	「true」または「false」	
IsDestinationSwitchName	「true」または「false」	
IsDeviceID	「true」または「false」	
IsDot1qId	「true」または「false」	
IsFEXID	「true」または「false」	
IsGateway	「true」または「false」	IPアドレスがゲートウェイかどうかを検証します。
IsInternal	「true」または「false」	フィールドを内部にし、ウィンドウに表示しません。 Note この注釈は、ipAddress変数にのみ使用します。
IsManagementIP	「true」または「false」 Note この注釈は、変数「ipAddress」に対してのみマークする必要があります。	

注釈キー	有効な値	説明
is_mandatory	「true」 または 「false」	値をフィールドに強制的に渡す必要があるかどうかを検証します
IsMTU	「true」 または 「false」	
IsMultiCastGroupAddress	「true」 または 「false」	
IsMultiLineString	「true」 または 「false」	文字列フィールドを複数行の文字列テキスト領域に変換します
IsMultiplicity	「true」 または 「false」	
IsPassword	「true」 または 「false」	
IsPositive	「true」 または 「false」	値が正であるかどうかを確認します。
IsReplicationMode	「true」 または 「false」	
IsShow	「true」 または 「false」	ウィンドウのフィールドを表示または非表示にします
IsSiteId	「true」 または 「false」	
IsSourceDevice	「true」 または 「false」	
IsSourceFabric	「true」 または 「false」	
IsSourceInterface	「true」 または 「false」	
IsSourceSwitchName	「true」 または 「false」	
IsSwitchName	「true」 または 「false」	
IsRMID	「true」 または 「false」	
IsVPCDomainID	「true」 または 「false」	
IsVPCID	「true」 または 「false」	
IsVPCPeerLinkPort	「true」 または 「false」	
IsVPCPeerLinkPortChannel	「true」 または 「false」	

注釈キー	有効な値	説明
IsVPCPortChannel	「true」または「false」	
[パスワード (Password)]	テキスト (Text)	パスワードフィールドを検証します
UsePool	「true」または「false」	
UseDNSReverseLookup		
ユーザ名	テキスト (Text)	ウィンドウにユーザ名フィールドを表示します。
警告	テキスト (Text)	Description 注釈をオーバーライドするテキストを提供します。

例 : AutoPopulate 注釈

```
##template variables
string BGP_AS;
@(AutoPopulate="BGP_AS")
string SITE_ID;
##
```

例 : DisplayName注釈

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
ipAddress hostAddress;
##
```

例 : IsMandatory注釈

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

例 : IsMultiLineString注釈

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow注釈

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual", Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to
true or false
```

例：警告の注釈

```
##template variables
@(Warning="This is a warning msg")
string SITE_ID;
##
```

テンプレートの内容

この項には、テンプレートで使用する構成コマンドと、すべてのパラメータが含まれています。これらのコマンドには、テンプレート変数セクションで宣言された変数を含めることができます。コマンド生成プロセス中に、変数の値がテンプレートの内容に適切に置き換えられます。



Note 使用するコマンドは、任意のデバイスのグローバル構成コマンドモードで入力するのと同じように指定する必要があります。コマンドを指定するときは、コマンドモードを考慮する必要があります。

テンプレートの内容は、変数の使用によって決まります。

- スカラ変数：反復に使用できない値の範囲または配列を取得しません（変数タイプテーブルでは、`iterate-able`が「No」としてマークされています）。スカラ変数はテンプレートの内容内で定義する必要があります。

```
Syntax: $$<variable name>$$
Example: $$USER_NAME$$
```

- 反復変数：ブロックの反復に使用されます。これらのループ変数は、次に示すように、繰り返しブロック内でアクセスする必要があります。

```
Syntax:@<loop variable>
Example:
foreach val in $$INTEGER_RANGE_VALUE$$ {
@val
}
```

- スカラー構造体変数：構造体メンバー変数は、テンプレートの内容からアクセスできません。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

- 配列構造変数：構造体のメンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

テンプレート変数に加えて、次のステートメントを使用して、条件付きコマンドと反復コマンドの生成を使用できます。

- **if-else if-else** ステートメント：その中の変数に割り当てられた値に基づいて、設定コマンドのセットの包含/除外を論理的に決定します。

```
Syntax: if(<operand 1> <logical operator> <operand 2>){
command1 ..
command2..
..
}
else if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

- **foreach** ステートメント：コマンドのブロックを反復するために使用されます。反復は、割り当てられたループ変数値に基づいて実行されます。

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
```

```
foreach ports in $$MY_INF_RANGE$${
interface @ports
no shut
}
```

- オプションパラメータ：デフォルトでは、すべてのパラメータが必須です。パラメータをオプションにするには、パラメータに注釈を付ける必要があります。

変数セクションには、次のコマンドを含めることができます。

- **@(IsMandatory=false)**

- **Integer frequency;**

テンプレートの内容の項では、「if」条件チェックを使用せずに、パラメータに値を割り当てることで、コマンドを除外または含めることができます。オプションのコマンドは、次のように構成できます。

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

高度な機能

次に、テンプレートの構成に使用できる高度な機能を示します。

- 割り当て操作

構成テンプレートは、テンプレートコンテンツセクション内の変数値の割り当てをサポートします。変数の宣言されたデータ型の値が検証されます。不一致がある場合、値は割り当てられません。

割り当て操作は、次のガイドラインに従って使用できます。

- 左側の演算子は、テンプレートパラメータまたは for ループパラメータのいずれかである必要があります。
- 正しい値の演算子は、テンプレートパラメータ、ループパラメータ、引用符で囲まれたリテラル文字列値、または単純な文字列値のいずれかの値です。

ステートメントがこれらのガイドラインに従っていない場合、またはこの形式に適合しない場合は、割り当て操作とは見なされません。これは、他の通常の行と同様に、コマンド生成時に置き換えられます。

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
```

```
foreach vlanID in $$vlan_range$${
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

• Evaluate メソッド

設定テンプレートは、Java ランタイムが提供する Java スクリプト環境を使用して、算術演算（ADD、SUBTRACT など）、文字列操作などを実行します。

テンプレートリポジトリパスで JavaScript ファイルを見つけます。このファイルには、算術文字列関数の主要なセットが含まれています。カスタム JavaScript メソッドを追加することもできます。

これらのメソッドは、次の形式の設定テンプレート コンテンツ セクションから呼び出すことができます。

```
Example1:
$$somevar$$ = evalscript(add, "100", $$anothervar$$)
```

また、次のようなif条件の内部で *evalscript* を呼び出すことができます。

```
if($$range$$ > evalscript(sum, $$vlan_id$$, -10)){
do something...
}
```

Java スクリプト ファイルのバックエンドにあるメソッドを呼び出すことができます。

• 動的な決定

構成テンプレートは、特殊な内部変数 `LAST_CMD_RESPONSE` を提供します。この変数には、コマンド実行中のデバイスからの最後のコマンド応答が格納されます。これは、デバイスの状態に基づいてコマンドを提供するための動的な決定を行うために、構成テンプレートのコンテンツで使用できます。



Note ifブロックの後には、空の場合もある新しい行で `else` ブロックを続ける必要があります。

VLAN がデバイス上に存在しない場合の VLAN の作成例。

```
Example: Create VLAN
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
else{
}
##
```

この特別な暗黙的変数は、「IF」ブロックでのみ使用できます。

• テンプレート参照

すべての変数を定義した基本テンプレートを作成できます。この基本テンプレートは、複数のテンプレートにインポートできます。基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。インポートしたテンプレートパラメータと内容は、拡張テンプレート内でアクセスできます。

```
Example: Template Referencing
Base template:
##template properties
name =a vlan base;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
timestamp = 2015-07-14 16:07:52;
imports = ;
##
##template variables
integer vlan_id;
##
##template content
vlan $$vlan_id$$
##

Derived Template:
##template properties
name =a vlan extended;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
timestamp = 2015-07-14 16:07:52;
imports = a vlan base,template2;
##
##template variables
interface vlanInterface;
##
##template content
<substitute a vlan base>
interface $$vlanInterface$$
<substitute a vlan base>
##
```

拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

レポート テンプレート

REPORT テンプレートのテンプレートタイプは `python` で、2 つのサブタイプ (UPGRADE と GENERIC) があります。

アップグレード

UPGRADE テンプレートは、ISSU 前後のシナリオに使用されます。これらのテンプレートは、ISSU ウィザードに表示されます。

ISSU 前後の処理の詳細については、Nexus ダッシュボード ファブリック コントローラ にパッケージ化されているデフォルトのアップグレードテンプレートを参照してください。デフォルトのアップグレードテンプレートは `issu_vpc_check` です。

GENERIC

GENERIC テンプレートは、リソース、スイッチ インベントリ、SFP、NVE VNI カウンタに関する情報の収集など、一般的なレポートシナリオに使用されます。このテンプレートを使用して、トラブルシューティング レポートを生成することもできます。

リソース レポート

このレポートには、特定のファブリックのリソース使用状況に関する情報が表示されます。

[**サマリ (Summary)**] セクションには、すべてのリソース プールと現在の使用率が表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロールバーを使用します。

POOL NAME : プールの名前を指定します。

POOL RANGE : プールの IP アドレス範囲を指定します。

SUBNET MASK : サブネット マスクを指定します。

MAX ENTRIES : プールから割り当て可能な最大エントリ数を示します。

USAGE INSIDE RANGE : プール範囲内に割り当てられている現在のエントリ数を指定します。

USAGE OUTSIDE RANGE : プール範囲外に設定されている現在のエントリ数を指定します。

USAGE PERCENTAGE : これは、(範囲内での使用数/最大エントリ数) *100 という式を使用して計算されます。

[**詳細の表示 (View Details)**] をクリックして、各リソース プールに割り当てられた、または設定されたリソースのビューを表示します。たとえば、SUBNET の詳細セクションには、サブ ネット内で割り当てられたリソースに関する情報が含まれます。

スイッチ インベントリ レポート

このレポートは、スイッチ インベントリに関する概要を提供します。

[**詳細の表示 (View Details)**] をクリックして、モジュールとライセンスに関する詳細情報を表示します。

SFP レポート

このレポートは、ファブリックおよびデバイス レベルでの SFP の使用率に関する情報を提供します。



(注) スイッチ インベントリ および SFP レポートは、Cisco Nexus デバイスでのみサポートされます。

トラブルシューティング レポート

これらのレポートは、トラブルシューティングのシナリオに役立つように生成されます。現在、定義済みのトラブルシューティング レポートは **NVE VNI** カウンタ レポートのみです。**NVE VNI カウンタ** レポートの生成では、ネットワーク トラフィックに基づいて上位ヒットの

VNIを特定するための定期的なチェックが実行されます。大規模なセットアップでは、レポートの生成頻度を 60 分以上に制限することをお勧めします。

NVE VNI カウンタ レポート

このレポートは、ファブリック内の各 VNI の **show nve vni counters** コマンド出力を収集します。

最も古いレポートと最新のレポートを比較すると、[サマリ (Summary)] セクションには上位 10 件のヒット VNI が表示されます。上位ヒット VNI は、次のカテゴリに表示されます。

- ユニキャスト トラフィック用の L2 または L3 VNI
- マルチキャスト トラフィック用の L2 または L3 VNI
- ユニキャスト トラフィック用の L2 のみの VNI
- マルチキャスト トラフィック用の L2 のみの VNI
- ユニキャスト トラフィック用の L3 のみの VNI
- マルチキャスト トラフィック用の L3 のみの VNI

最も古いレポートは、現在のレポートタスクで保存された最初のレポートを参照します。現在のレポートと比較する必要がある最初のレポートとして特定のレポートを選択する場合は、選択したレポートが最初で最も古いレポートになるように、選択したレポートよりも古いすべてのレポートを削除します。

たとえば、昨日の午前 8 時、午後 4 時、および午後 11 時に 3 つのレポートが実行されたとします。今日のレポートの最初の最も古いレポートとして午後 11 時にレポートを使用する場合は、昨日の午前 8 時と午後 4 時に実行されました。

定期レポートの場合、最も古いレポートは、期間の開始時刻に実行される最初のレポートです。日次および週次レポートの場合、現在のレポートが以前に生成されたレポートと比較されます。

[サマリ (Summary)] セクションには、送信された合計バイト数と VNI に関する情報を含むカラムごとのレポートが表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロールバーを使用します。



- (注) NVE VNI カウンタ レポートの [サマリ (Summary)] セクションでは、スイッチのリロード後またはスイッチのカウンタのクリア後にレポートが生成された場合、[合計送信バイト数 (TOTAL TX BYTES)] 列に負の数が表示されます。番号は、後続のレポートで正しく表示されます。回避策として、スイッチをリロードするか、カウンタをクリアする前に、古いレポートをすべて削除するか、新しいジョブを作成することを推奨します。

詳細については、[詳細の表示 (View Details)] をクリックしてください。このセクションでは、スイッチごとに NVE VNI とカウンタを示します。

レポートの表示方法の詳細については、「プログラム可能なレポート」の章を参照してください。



第 24 章

バックアップと復元

いつでも手動でバックアップできます。すべてのファブリック設定とインテントを自動または手動でバックアップするようにスケジューラを設定することもできます。

次のいずれかの形式を使用してバックアップおよび復元できます。

- **設定のみ**：設定のみのバックアップの方が小さくなります。これにはインテント、依存データ、検出情報、ログイン情報、およびポリシーが含まれています。このバックアップからの復元には、機能するファブリック、スイッチの検出、予期される設定、およびその他の設定が含まれています。
- **完全**：フルバックアップは大規模です。これには、現在のデータ、履歴データ、アラーム、ホスト情報、および設定のみのバックアップのすべてが含まれます。このバックアップからの復元には、機能的な履歴レポート、メトリックグラフ、およびすべての基本機能があります。

構成のみのバックアップまたは完全バックアップを復元できます。

バックアップを復元するときは、設定のみの復元または完全な復元を選択できます。設定のみの復元では、設定（インテント、検出情報、ログイン情報、ポリシー）のみが復元され、設定のみのバックアップと完全バックアップの両方を使用して実行できます。完全な復元は、設定と、現在および過去のデータ、チャートなどを復元し、完全バックアップのみを使用して実行できます。



- (注) 新規インストール後、バックアップデータを復元する前に、最低 20 分間待機してください。新しくインストールしたセットアップでバックアップをすぐに復元すると、一部のアプリケーションが動作しない場合があります。

アップグレード後の機能の互換性

次の表に、NDFC、リリース 12.1.1e へのアップグレード後に DCNM 11.5(x) バックアップから復元される機能に関連する警告を示します。



(注) 11.5(x)には、リリース 11.5(1)、11.5(2)、のみが含まれます。11.5(4)から 12.1.1e へのアップグレードはサポートされていません。

DCNM 11.5(x) の機能	アップグレードのサポート
vCenter による VMM の可視性	サポート対象
設定されたプレビュー フィーチャー	サポート対象外
SAN インストールの LAN スイッチ	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
SAN CLI テンプレート	11.5(x) から 12.1.1e に引き継がれない
イメージ/イメージ管理データの切り替え	11.5(x) から 12.1.1e に引き継がれない
低速ドレイン データ	11.5(x) から 12.1.1e に引き継がれない
アラーム ポリシーの設定	11.5(x) から 12.1.1e に引き継がれない
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。

このセクションの内容は次のとおりです。

- [スケジューラ \(302 ページ\)](#)
- [Restore \(復元\) \(304 ページ\)](#)
- [今すぐバックアップ \(305 ページ\)](#)

スケジューラ

スケジューラの目的は、システムを復元する必要がある場合にシステムのバックアップを取ることです。リモートロケーションにバックアップする必要があります。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からアプリケーションおよび設定データのバックアップをスケジュールするには、次の手順を実行します。

始める前に

スケジュールされたバックアップジョブがない場合は、[スケジュールが設定されていません (No Schedule set)] が表示されます。

手順

-
- ステップ 1** [スケジュール設定なし (No Schedule set)] をクリックします。
[Scheduler (スケジューラ)] ウィンドウが表示されます。
- ステップ 2** [スケジュールされたバックアップの有効化 (Enable Scheduled backups)] チェックボックスをオンにします。
- ステップ 3** [種類 (Type)] で、復元する形式を選択します。
• [構成のみ (Config only)] または [完全 (Full)] を選択します。
- ステップ 4** [接続先 (Destination)] フィールドで、をクリックして、ドロップダウンリストから [SCP サーバーにエクスポート (Export to SCP Server)] または [SFTP サーバーにエクスポート (Export to SFTP Server)] を選択します。
- ステップ 5** [サーバー (Server)] フィールドに、SCP サーバーの IP アドレスを入力します。
- ステップ 6** [ファイルパス (File Path)] フィールドに、バックアップ ファイルを保存するディレクトリの絶対パスを入力します。
- ステップ 7** バックアップディレクトリにユーザー名とパスワードを入力します。
- ステップ 8** バックアップ ファイルに対する暗号キーを入力します。
バックアップから復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。
- ステップ 9** [日単位で実行 (Run on days)] フィールドで、チェックボックスをオンにして、1 日以上のバックアップジョブをスケジュールします。
- ステップ 10** [開始時刻 (Start at)] フィールドで、タイムピッカーを使用して特定の時刻にバックアップをスケジュールします。
タイムピッカーは 12 時間制です。
- ステップ 11** [バックアップのスケジュール (Schedule backup)] をクリックして、スケジュールに従ってバックアップジョブを実行します。
-

Restore (復元)



- (注) 新規インストール後、バックアップデータを復元する前に、最低 20 分間待機してください。新しくインストールしたセットアップでバックアップをすぐに復元すると、一部のアプリケーションが動作しない場合があります。

ガイドライン

機能が有効になっていない、新しくインストールされた Nexus ダッシュボード ファブリック コントローラ でのみ復元を実行できます。

L2 HA から L3 HA に移行する場合は、[外部サービス IP 構成を無視する (Ignore External Service IP Configuration)] チェックボックスをオンにして、バックアップ内の永続的な IP が無視され、復元中に新しい IP が選択されるようにします。残りのデータは復元されます。



- (注) 災害復旧時に NDFC を使用した場合、バックアップが作成されたのと同じバージョンでのみ復元できます。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からアプリケーションおよび構成データを復元するには、次の手順を実行します。

手順

ステップ 1 [復元 (Restore)] をクリックします。

[今すぐ復元 (Restore now)] ウィンドウが表示されます。

ステップ 2 [種類 (Type)] で、復元する形式を選択します。

- [構成のみ (Config only)] または [完全 (Full)] を選択します。

ステップ 3 [送信元 (Source)] フィールドで、バックアップファイルを保存した適切な接続先をクリックして選択します。

- ファイルがローカル ディレクトリに保存されている場合は、[ファイルのアップロード (Upload File)] を選択します。

1. バックアップ ファイルが保存されるディレクトリ
2. バックアップファイルを [今すぐ復元 (Restore now)] ウィンドウにドラッグアンドドロップします。

または

[Browse]をクリックします。バックアップファイルが保存されるディレクトリに移動します。バックアップファイルを選択して、[開く (Open)]をクリックします。

3. バックアップファイルに対する**暗号キー**を入力します。

(注) バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

- バックアップファイルがリモートディレクトリに保存されている場合は、[SCP サーバーからインポート (Import from SCP Server)]または[SFTP サーバーからインポート (Import from SFTP Server)]を選択します。

1. [サーバー (Server)] フィールドに、SCP サーバーの IP アドレスを入力します。
2. [ファイルパス (File Path)] フィールドに、バックアップファイルへの相対ファイルパスを入力します。
3. ユーザ名とパスワードを該当するフィールドに入力します。
4. [暗号キー (Encryption Key)] フィールドにバックアップファイルに対する暗号キーを入力します。

(注) バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

ステップ 4 (オプション) [外部サービスの IP 設定を無視する (Ignore External Service IP Configuration)] チェックボックスをオンにします。

[外部サービスの IP 設定を無視する (Ignore External Service IP Configuration)] チェックボックスがオンになっている場合、外部サービスの IP 設定は無視されます。この選択により、システムでバックアップを作成し、それを別の管理サブネットやデータサブネットを持つ別のシステムに復元することができます。

このオプションは、Cisco DCNM 11.5(x) から Cisco NDFC へのアップグレード中には影響しません。

ステップ 5 [復元 (Restore)] をクリックします。

バックアップファイルが [バックアップと復元 (Backup & Restore)] ウィンドウの表に表示されます。復元に必要な時間は、バックアップファイルのデータによって異なります。

今すぐバックアップ

Cisco Nexus ダッシュボード ファブリック コントローラ Web UI からアプリケーションおよび設定データのバックアップを取得するには、次の手順を実行します。

手順

ステップ1 [今すぐバックアップ (Backup Now)] をクリックします。

ステップ2 [種類 (Type)] で、復元する形式を選択します。

- [構成のみ (Config only)] または [完全 (Full)] を選択します。

ステップ3 [接続先 (Destination)] フィールドで、バックアップファイルを保存する適切な接続先を選択します。

- ローカルディレクトリにバックアップを保存するには、[ローカルダウンロード (Local Download)] を選択します。

1. バックアップファイルに対する暗号キーを入力します。

(注) バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

2. [バックアップ (Backup)] をクリックします。

バックアップが完了すると、[バックアップと復元 (Backup & Restore)] 画面からバックアップファイルをダウンロードできます。

3. [アクション (Actions)] 列で、[ダウンロード (Download)] アイコンをクリックして、バックアップをローカルディレクトリに保存できます。

バックアップを削除するには、[削除 (Delete)] アイコンをクリックします。

(注) 割り当てられたディスク容量が限られているため、[ローカルダウンロード (Local Download)] オプションで取得したバックアップはできるだけ早く削除する必要があります。

- SCPサーバーへのエクスポートまたはSFTPサーバーへのエクスポートを選択して、バックアップファイルをリモートディレクトリに保存します。

1. [サーバー (Server)] フィールドに、SCPサーバーのIPアドレスを入力します。

2. [ファイルパス (File Path)] フィールドに、バックアップファイルへの相対ファイルパスを入力します。

3. ユーザ名とパスワードを該当するフィールドに入力します。

4. [暗号キー (Encryption Key)] フィールドにバックアップファイルに対する暗号キーを入力します。

(注) バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

5. [バックアップ (Backup)] をクリックします。

バックアップが完了すると、バックアップファイルがリモートディレクトリに保存されます。



第 25 章

NXAPI 証明書

Cisco NX-OS スイッチを NX-API HTTPS モードで機能させるには、SSL 証明書が必要です。SSL 証明書を生成し、CA によってそれに署名することができます。証明書は、スイッチ コンソールで CLI コマンドを使用して手動でインストールすること、または Cisco Nexus ダッシュボード ファブリック コントローラ を使用してスイッチにインストールすることができます。

Cisco Nexus ダッシュボード ファブリック コントローラ では、NX-API 証明書を Nexus ダッシュボード ファブリック コントローラ にアップロードするための Web UI フレームワークを提供しています。後で、Nexus ダッシュボード ファブリック コントローラ によって管理されるスイッチに証明書をインストールできます。



(注) この機能は、Cisco NXOS バージョン 9.2(3)以降で動作するスイッチでサポートされます。

- [証明書の生成と管理 \(309 ページ\)](#)

証明書の生成と管理

データセンター管理者は、スイッチごとに ASCII (base64) エンコードの証明書を生成します。この証明書は、次の 2 つのファイルで構成されます。

- 秘密キーを含む .key ファイル
- 証明書を含む .crt/.cer/.pem ファイル

Cisco Nexus ダッシュボード ファブリック コントローラ は、組み込みキー ファイル、つまり .crt/.cer/.pem ファイルを含む単一の証明書ファイルもサポートします。これには、.key ファイルの内容も含めることができます。

Nexus ダッシュボード ファブリック コントローラ は、バイナリ エンコードされた証明書はサポートしていません。つまり、.der 拡張子の証明書はサポートされません。キー ファイルは、暗号化用のパスワードで保護できます。Cisco Nexus ダッシュボード ファブリック コントローラ は暗号化を義務付けていません。ただし、これは Nexus ダッシュボード ファブリック

コントローラに保存されるため、キーファイルを暗号化することをお勧めします。NexusダッシュボードファブリックコントローラはAES暗号化をサポートしています。

CA署名付き証明書または自己署名証明書のいずれかを選択することができます。Cisco Nexusダッシュボードファブリックコントローラは署名を義務付けていません。ただし、セキュリティガイドラインでは、CA署名付き証明書を使用することを推奨しています。

複数のスイッチ用に複数の証明書を生成して、Nexusダッシュボードファブリックコントローラにアップロードすることができます。証明書に適したスイッチを選択できるように、証明書に適切な名前を付けてください。

1つの証明書と対応するキーファイルをアップロードすることも、複数の証明書とキーファイルを一括アップロードすることもできます。アップロードが完了したら、スイッチにインストールする前に、アップロードリストを確認することができます。組み込みキーファイルを含む証明書ファイルがアップロードされた場合、Nexusダッシュボードファブリックコントローラは自動的にキーを取得します。

証明書とキーファイルは同じファイル名である必要があります。たとえば、証明書ファイル名がmycert.pemの場合、キーファイル名はmycert.keyである必要があります。証明書とキーペアのファイル名が同じでない場合、Nexusダッシュボードファブリックコントローラはスイッチに証明書をインストールできません。

Cisco Nexusダッシュボードファブリックコントローラでは、スイッチに証明書を一括インストールできます。一括インストールでは同じパスワードが使用されるため、すべての暗号化キーは同じパスワードで暗号化する必要があります。キーのパスワードが異なる場合、証明書を一括モードでインストールすることはできません。一括モードインストールでは、暗号化されたキー証明書と暗号化されていないキー証明書を一緒にインストールできますが、すべての暗号化キーは同じパスワードを持つ必要があります。

スイッチに新しい証明書をインストールすると、既存の証明書が新しい証明書に置き換えられます。

同じ証明書を複数のスイッチにインストールすることができます。ただし、一括アップロード機能は使用できません。



- (注) Nexusダッシュボードファブリックコントローラは、提供される証明書またはオプションが有効であることを要求しません。この規則に従うかどうかは、ユーザーとスイッチの要件次第です。たとえば、スイッチ1のための証明書が生成されても、それがスイッチ2にインストールされた場合、Nexusダッシュボードファブリックコントローラは証明書の適用を強制しません。スイッチは、証明書のパラメータに基づいて証明書を受け入れるか、拒否するかを選択できます。

Cisco NexusダッシュボードファブリックコントローラによるNX-API証明書の検証

リリース12.0.1a以降、Cisco Nexusダッシュボードファブリックコントローラはスイッチによって提供されるNX-API証明書を検証する機能をサポートしています。Cisco Nexusダッシュボードファブリックコントローラが行うNX-APIリクエストにはSSL接続が必要です。ス

スイッチはSSLサーバーのように動作し、SSLネゴシエーションの一部としてサーバー証明書を提供します。対応するCA証明書が提供されている場合、Cisco Nexusダッシュボードファブリックコントローラはそれを確認できます。



- (注) デフォルトでは、NX-API証明書の検証は有効にされていません。これは、データセンター内のすべてのスイッチにCA署名付き証明書がインストールされている必要があり、Cisco Nexusダッシュボードファブリックコントローラには対応するすべてのCA証明書が供給されるためです。

Cisco NexusダッシュボードファブリックコントローラのNX-API証明書管理には、同じ対象を管理するためのスイッチ証明書とCA証明書という2つの機能があります。

スイッチ証明書

証明書のアップロード

証明書をNexusダッシュボードファブリックコントローラにアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切な証明書ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリックコントローラにアップロードする必要がある証明書キーペアを選択します。

拡張子が .cer/.crt/.pem および .key の証明書を個別に選択できます。

Cisco Nexusダッシュボードファブリックコントローラでは、埋め込みキーファイルを含む単一の証明書ファイルをアップロードすることもできます。キーファイルはアップロード後に自動的に取得されます。

3. **[アップロード (Upload)]** をクリックし、選択したファイルをNexusダッシュボードファブリックコントローラにアップロードします。

ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

テーブルには、ステータスが **UPLOADED** と表示されます。証明書がキーファイルなしでアップロードされた場合、ステータスは **KEY_MISSING** と表示されます。

スイッチの割り当てと証明書のインストール

Cisco Nexusダッシュボードファブリックコントローラ Web UIを使用してスイッチに証明書をインストールするには、次の手順を実行します。

1. 1つまたは複数の証明書のチェックボックスをオンにします。

2. **[アクション (Actions)]** ドロップダウンリストから、**[スイッチの割り当てとインストール (Assign Switch & Install)]** を選択します。
3. **[NX API 証明書クレデンシャル (NX API Certificate Credentials)]** フィールドに、証明書の生成時にキーを暗号化するために使用したパスワードを入力します。

[パスワード (Password)] フィールドは必須ですが、キーがパスワードを使用して暗号化されていない場合は、任意のランダムな文字列を入力できます（たとえば `test`、`install` など）。暗号化されていないファイルの場合、パスワードは使用されませんが、一括モードであるため、ランダムな文字列を入力する必要があります。



- (注) 1回の一括インストールで、暗号化されていないキーと暗号化されたキーおよび証明書をインストールできます。ただし、暗号化キーに使用するキーパスワードを指定する必要があります。

4. 証明書ごとに、**[割り当て (Assign)]** の矢印をクリックし、証明書に関連付けるスイッチを選択します。
5. **[証明書のインストール (Install Certificates)]** をクリックして、それぞれのスイッチにすべての証明書をインストールします。

証明書のリンク解除と削除

証明書をスイッチにインストールすると、NexusダッシュボードファブリックコントローラはNexusダッシュボードファブリックコントローラから証明書をアンインストールできません。ただし、スイッチにはいつでも新しい証明書をインストールできます。スイッチにインストールされていない証明書は削除できます。スイッチにインストールされている証明書を削除するには、スイッチから証明書のリンクを解除してから、Nexusダッシュボードファブリックコントローラから削除する必要があります。



- (注) スイッチから証明書のリンクを解除しても、スイッチの証明書は削除されません。証明書はまだスイッチに存在します。Cisco Nexusダッシュボードファブリックコントローラはスイッチの証明書を削除できません。

Nexusダッシュボードファブリックコントローラリポジトリから証明書を削除するには、次の手順を実行します。

1. 削除する必要がある証明書を選択します。
2. **[アクション (Actions)]** ドロップダウンリストから、**[リンク解除 (Unlink)]** を選択します。確認メッセージが表示されます。
3. **[OK]** をクリックして、選択した証明書をスイッチからリンク解除します。

ステータス カラムには [UPLOADED] と表示されます。[Switch] カラムには [NOT_INSTALLED] と表示されます。

4. [Switch] から、現在リンク解除されている証明書を選択します。
5. [アクション (Actions)] ドロップダウン リストから、[削除 (Delete)] を選択します。
証明書は Nexus ダッシュボード ファブリック コントローラ から削除されます。

CA 証明書

証明書のアップロード

証明書を Nexus ダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. [証明書のアップロード (Upload Certificate)] をクリックして、適切なライセンス ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexus ダッシュボード ファブリック コントローラ にアップロードする証明書とキーのペアを選択します。

ファイル拡張子が .cer/.crt/.pem ファイル拡張子をもつ証明書を個別に選択できます。



(注) CA 証明書は公開証明書であり、キーは含まれません。また、この操作にはキーは必要ありません。これは、スイッチが提供する NX-API 証明書を確認するために Cisco Nexus ダッシュボード ファブリック コントローラ が必要とする証明書です。つまり、CA 証明書は Cisco Nexus ダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

3. [アップロード (Upload)] をクリックし、選択したファイルを Nexus ダッシュボード ファブリック コントローラ にアップロードします。

ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

スイッチの割り当てと証明書のインストール

これらの CA 証明書は Cisco Nexus ダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

証明書のリンク解除と削除

CA 証明書はスイッチにインストールされないため、リンク解除する必要はありません。

CA 証明書は、特定の CA に新しい証明書を持ち込む必要があるため、削除できます。

[アクション (Actions)] ドロップダウンリストから、[削除 (Delete)] を選択します。証明書は Nexus ダッシュボード ファブリック コントローラ から削除されます。

NX-API 証明書検証の有効化

NX-API 証明書の検証は、[CA 証明書] ページのトグル ボタンを使用して有効にできます。ただし、これは、Cisco Nexus ダッシュボード ファブリック コントローラ が管理するすべてのスイッチに CA 署名付き証明書がインストールされ、対応する CA ルート証明書 (1つ以上) が Cisco Nexus ダッシュボード ファブリック コントローラ にアップロードされた後にのみ行う必要があります。これを有効にすると、Cisco Nexus ダッシュボード ファブリック コントローラ SSL クライアントはスイッチによって提供される証明書の検証を開始します。検証に失敗すると、NX-API コールも失敗します。



- (注)
- NX-API 証明書の検証は、スイッチごとに適用できません。all または none のいずれかです。したがって、すべてのスイッチに対応する CA 署名付き証明書がインストールされている場合にのみ、検証を有効にすることが重要です。
 - また、すべての CA 証明書が Cisco Nexus ダッシュボード ファブリック コントローラ にインストールされている必要があります。
 - 検証の問題が原因で特定のスイッチで NX-API コールが失敗した場合は、トグル ボタンを使用して適用を無効にできます。すべての結果は、以前の状態に戻ります。
 - 上記の点から、メンテナンス期間中に適用を有効にする必要があります。



第 **V** 部

サービスの統合

- [ワンビューダッシュボード \(317 ページ\)](#)
- [デバイスマネージャ \(319 ページ\)](#)



第 26 章

ワンビューダッシュボード

- ・ワンビューダッシュボード (317 ページ)

ワンビューダッシュボード

ワンビューダッシュボードには、すべてのサイトに関する概要情報を示す、多くのダッシュレットが表示されます。デフォルトでは、使用可能なダッシュレットのサブセットがダッシュボードの概要に自動的に表示されます。

左側のメニューバーから、[SAN コントローラ (SAN Controller)] > [ワンビュー (One View)] > [ワンビューダッシュボード (One View Dashboard)] を選択します。[概要 (Overview)] ウィンドウに次のダッシュレットが表示されます。更新アイコンをクリックして、ダッシュボードを手動で更新することもできます。

トップバーのワンビューアイコンをクリックして、[NDFC の選択 (Select NDFC)] 画面を表示します。[ワンビュー (One View)] をクリックして、コントローラの情報とそのステータスを表示します。左側のペインで各コントローラをクリックして、フェデレーション内のそのコントローラに関する特定の情報を表示します。

また、各統合ノードの NDFC サービスと Nexus Dashboard のステータスを表示することもできます。

[概要 (Overview)] ダッシュボードウィンドウに表示されるデフォルトのダッシュレットは次のとおりです。

ダッシュレット	説明
要約	以下を水平ペインに表示します。 <ul style="list-style-type: none">• フェデレーションセットアップ内の SAN コントローラの数• ファブリックの総数• 検出されたスイッチの総数

ダッシュレット	説明
ファブリックヘルス	ファブリックのヘルスステータスを、括弧内にファブリックの総数とともに色とヘルス状態の重大度を記した、グラフの形式で表示します。
スイッチの状態	スイッチのヘルスステータスを、括弧内にスイッチの総数とともに色とヘルス状態のシビラティ（重大度）を含むグラフの形式で表示します。
スイッチのリリースバージョン	NX-OS のバージョンを、各バージョンのスイッチの総数を括弧で囲んだ、色付きのグラフ形式で表示します。
スイッチのモデル	スイッチの PID を、各バージョンのスイッチの総数を括弧で囲んだ色付きのグラフ形式で表示します。
ファブリック	すべてのファブリックとそれに関連付けられたコントローラを表示します。また、各ファブリックの動作状態と健全性も表示されます。
スイッチ	すべてのスイッチと、それらに関連付けられたコントローラとファブリックを表示します。また、各スイッチの状態も表示されます。
コントローラ	フェデレーションセットアップ内の各コントローラのファブリックの健全性、スイッチの健全性、スイッチのリリースバージョン、およびスイッチモデルを表示します。



第 27 章

デバイス マネージャ

- [デバイス マネージャ \(319 ページ\)](#)

デバイス マネージャ

この章には、デバイス マネージャのヘルプ情報が含まれています。この章は、次の項で構成されています。

物理

このセクションには、DCNM SAN セットアップの物理属性が含まれています。

インベントリ

フィールド	説明
名前	現場交換可能ユニット (FRU) の名前。
ModelName	モデル名の識別子。
SerialNumber	プライマリおよびセカンダリ シリアル番号。
HardwareRevision	ハードウェア リビジョン
SoftwareRevision	Cisco NX-OS ソフトウェアのリリース バージョン。
Alias	ネットワーク マネージャによって指定されたエイリアス名。
AssetID	ネットワーク管理者によって指定された、ユーザーが割り当てた資産の追跡識別子。

Modules - ステータスと構成

フィールド	説明
名前	モジュールの説明。

フィールド	説明
モジュール	モジュール名の識別子。
OperStatus	モジュールの動作状態。
リセット	クリックしてモジュールを再起動します。
RateModeOverSubscriptionLimit	このオプションを選択して、それをサポートするモジュールのオーバーサブスクリプション比率の制限を制御します。デフォルトでは、制限は有効になっています。このオプションを無効にすると、使用可能な帯域幅に関係なく、モジュールのすべてのインターフェイスが最大管理速度で動作できるようになります。
BandwidthFairnessConfig	このオプションを選択して、それをサポートするモジュールの帯域幅の公平性を制御します。デフォルトでは、帯域幅の公平性が有効になっています。
BandwidthFairnessOper	帯域幅の公平性が有効か無効かを示します。デフォルトでは、帯域幅の公平性が有効になっています。
X2 xcvrFrequency Config	モジュールのトランシーバ周波数を指定します。 <ul style="list-style-type: none"> • notApplicable - モジュールがこの構成をサポートしていない場合は、これを選択します。 • xcvrFreqX2FC - モジュールの FC トランシーバ周波数を 10 ギガバイトに設定するには、これを選択します。 • xcvrFreqX2Eth - モジュールのイーサネット トランシーバ周波数を 10 ギガバイトに設定するには、これを選択します。
ResetReasonDescription	モジュールが最後にリセットされた理由。
ローカル スイッチング モード	ローカルスイッチングモジュールのステータスを表示します。
StatusLastChangeTime	OperStatus の変更時刻。
Power Admin	フィールド交換可能ユニット (FRU) の電源をオンまたはオフにすることができます。
Power Oper	フィールド交換可能ユニット (FRU) の動作電源状態。
電流	フィールド交換可能ユニット (FRU) によって供給される電流。

電源

フィールド	説明
名前	電源の場所。

フィールド	説明
TotalPowerAvailable	使用可能な電力を表示します。結合モードでは、総電力は2つの電源の容量のうち少ない方の2倍となります。
冗長/結合	選択して、電源装置の構成方法を決定します。冗長モードでは、1つが故障した場合にバックアップ電源を提供できますが、利用可能な総電力は少なくなります。
ModelName	モデル識別子。
OperStatus	電源動作の状態。
TotalAvailable	電源の使用に利用可能な総電力。モードが冗長の場合、使用可能な合計電力は、電源モジュールの電源容量よりも少ない電源容量です。モードが結合の場合、使用可能な合計電力は、動作中の電源のモジュールの少ない方の電源容量の2倍になります。
TotalReserved	電源が投入されている FRU に使用される合計電流。



- (注) Uros と Paradise への電力供給が中断またはオフになった場合、電力供給テーブルの OperStatus は「offEnvOther」と表示されます。ただし、電源が切断されたデバイスの対応するエントリは、インベントリ テーブルに残ります。

温度センサー

フィールド	説明
名前	センサーの位置。
Threshold Major	主要な温度しきい値。
Threshold Minor	副次的な温度しきい値。
電流	センサーによって認識された最新の測定値を報告します。
ステータス	センサーの現在の動作ステータス。

ファン

フィールド	説明
名前	ファンの場所。
ModelName	モデル識別子。

フィールド	説明
OperStatus	現在の運用状況。

スイッチ

フィールド	説明
説明	スイッチとソフトウェアの説明。
稼働時間	システムのネットワーク管理部分が最後に再初期化された以降の時間。
名前	この管理対象ノードの管理上割り当てられた名前。
Location	このノードの物理的な場所（例：電話ブース、3階）。
連絡先	このスイッチの連絡先担当者。この担当者への連絡方法に関する情報も含む。
SwitchWWN	このスイッチの World-Wide Name。
ClockDateAndTime	システムの現在のローカル日時。これを設定することは、自動化された時計と予定表を設定することと同じです。
タイムゾーン	システムの現在のローカルタイムゾーン。タイムゾーンは GMT の形式で入力する必要があります。タイムゾーンと GMT（グリニッジ標準時）との時間差です。
ProcessorRAM	プロセッサで使用可能な RAM の合計バイト数。
NVRAM	エンティティ内の NVRAM の合計バイト数。
NVRAMUsed	使用中の NVRAM のバイト数。
FIPSMODEACTIVATION	デバイスの FIPS モードを有効化または無効化します。FIPS 140-2 は暗号モジュールに関する一連のセキュリティ要件であり、暗号モジュールに対する米国政府の要求条件を詳細に記述しています。モジュールは、ハードウェアとソフトウェアの両方で構成されます（例：データセンターのスイッチングまたはルーティングモジュール）。FIP モードを有効にするための要求が受信され、その要求に応じて一連のセルフテストが正常に実行される場合、モジュールは FIPS 対応モードにあると言われます。セルフテストが失敗した場合は、適切なエラーが返されます。
CPUUtilization	アクティブ スーパーバイザでの CPU の平均使用率。
MemoryUtilization	アクティブ スーパーバイザでのメモリの平均使用率。
FlashPartitionSize	フラッシュパーティションサイズ。
FlashPartitionFreeSpace	フラッシュパーティション内の空き領域。

フィールド	説明
ステータス	スイッチ全体のステータス。
ベンダー	Cisco、McData、Brocade などのスイッチベンダーの名前。
モデル	MDS 9134 または MDS 9124 などのスイッチモデル名。
リリース	スイッチソフトウェアバージョン。
NumFCPorts	スイッチ内の物理 FC ポートの数。
WWN	検出されたイーサネット VDC の MAC アドレス。
VDCId	検出されたイーサネット VDC の一意の ID。
FCoE Enabled	true の場合、検出されたイーサネット VDC に対して FCoE が有効になります。

ISL

フィールド	説明
スイッチから	リンクのソーススイッチ。
送信元インターフェイス	リンクのソース E_port のポートインデックス。
スイッチに	リンクのもう一方の端にあるスイッチ。
インターフェイスへ	リンクの宛先 E_port のポートインデックス。
ステータス	リンクの動作ステータス。

NP リンク

フィールド	説明
NPIV (Core)	NPIV コアスイッチ。
F ポート	NPIV コアスイッチの接続された F ポート。
NPV	NPV スイッチ。
NP ポート	NPV スイッチの接続ポート。
ステータス	リンクの動作ステータス。

ISL の統計

フィールド	説明
説明	ネットワーク マネージャによって指定されたインターフェイスのエイリアス名。ポート チャネルと FCIP の場合、このフィールドは、メンバーが使用可能な場合は常にメンバーを表示します。FCIP の場合、圧縮されていれば、このフィールドには <code>compress</code> と表示されます。
VSAN(s)	VSAN メンバーシップ。
モード	ポートの動作モード> (凡例を参照)。
接続先	アタッチされたポート。これは、ホスト、ストレージ、またはスイッチポートである可能性があります。
スピード	最大帯域幅 (Gbps)
Rx	次のいずれかが必要です。 使用率 % バイト数 フレーム数 平均フレーム サイズ
Rx 圧縮	FCIP デバイスで受信したパケットの IP 圧縮比。
Tx	次のいずれかが必要です。 使用率 % バイト数 フレーム数 平均フレーム サイズ
Tx 圧縮	FCIP デバイスで送信したパケットの IP 圧縮比。
エラー	インターフェイス上の Rx および Tx エラーの総数。Rx エラーのタイプには、CRC エラー、フレームの分断化、サポートされていないクラスフレーム、Runt フレーム、Jabber フレーム、ジャイアント フレームなどがあります。Tx エラーのタイプは一般に CRC エラーですが、発生するのはまれです。[エラー (Errors)] フィールドが空でない場合は、Rx エラーが発生している可能性があります。エラー カウントの詳細な内訳については、適切なインターフェイスの [モニタ (Monitor)] ダイアログ ボックスを確認してください。

破棄	インターフェイスでの Rx と Tx の破棄の合計数。Rx フレームの破棄は、通常、プロトコルエラーが原因です。まれに、ハードウェアエラーなしでフレームが受信されたにもかかわらず、MACアドレスに設定されているフィルタリングルールの不一致により、フレームが破棄されることがあります。Txフレームが破棄された場合には、タイムアウトフレーム破棄（ポートがオフラインまたはアップしていない）か、スーパーバイザに返送されなかったタイムアウトフレーム（クラス F/2 フレーム）の可能性があります。[破棄 (Discards)]フィールドが空でない場合は、タイムアウト フレームが原因である可能性があります。
ログ	オンにすると、ポーリング間隔ごとにレコードをメッセージログに書き込みます。

ホスト

フィールド	説明
エンクロージャ名	エンクロージャの名前
Alias	このエントリのデバイスエイリアス。
ポートWWN	このホストに割り当てられた PWWN。
FcId	このホストに割り当てられた FC ID。
リンクステータス	リンクの動作ステータス。
シリアル番号	シリアル番号。
モデル	モデル名。
Firmware Ver	この HBA が実行しているファームウェアのバージョン。
Driver Ver	この HBA が使用しているドライバのバージョン。
情報	この HBA に対応する情報一覧です。
スイッチ インターフェイス	エンドデバイスに接続されているスイッチのインターフェイス。

ラック

フィールド	説明
[IPアドレス (IP Address)]	エンクロージャの IP アドレス。
Elem. Mgr Use HTTP	ローカル エンクロージャを起動するために HTTP を使用します。
Elem. Mgr URL/Path	ローカル エンクロージャを起動するために使用する URL
デバイスタイプ	ホストの場合は HBA です。ストレージの場合は SCSI ターゲットです。

フィールド	説明
ベンダー	ホストの場合は HBA です。ストレージの場合は SCSI ターゲットです。
モデル	ホストの場合は HBA です。ストレージの場合は SCSI ターゲットです。
Firmware Ver	この HBA が実行しているファームウェアのバージョン。
Driver Ver	この HBA を制御するドライバソフトウェアのバージョンレベル。
OS	この HBA を制御するオペレーティング システムのタイプとバージョン
他の情報:	この HBA に対応する情報一覧です。

デバースマネージャ - プリファレンス

フィールド	説明
Retry Requests # time(s) after #sec timeout	タイムアウト (秒) 後の再試行回数。
Enable Status Polling	オンにすると、(指定された) 秒数ごとにステータスポーリングが有効になります。
Trace SNMP packets in Message Log	オンにすると、メッセージログ内の SNMP パケットのトレースが有効になります。
Register for Events after Open, listen on Port 1163	オンにすると、イベントが自動的に登録されます。
Show WWN Vendor	オンにすると、WWN ベンダー名の表示が有効になります。 <ul style="list-style-type: none"> • Replace : 既存のベンダー名を新しいものに置き換えます。 • Prepend : 新しいベンダー名を現在のベンダー名の先頭に付けます。
Show Timestamps as Date/Time	オンにすると、タイムスタンプが日付/時刻形式で表示されます。
Telnet Path	Telnet クライアントへのパス。
Use Secure Shell instead of Telnet	セキュア シェルを使用する場合にオンにします。
CLI Session Timeout	CLI セッションの時間間隔 (秒単位)。CLI タイムアウトを無効にするには、0 を入力します。
Show Tooltips in Physical View	オンにすると、ツールチップが表示されます。

フィールド	説明
Label Physical View Ports with	<ul style="list-style-type: none"> • FICON : デバイス ビューのポートのラベルとしてFICONを表示します。 • インターフェイス : デバイス ビューのポートのラベルとしてインターフェイスを表示します。
表のエクスポート	<ul style="list-style-type: none"> • Tab-Delimited : テーブルをタブ区切りテキスト ファイルにエクスポートします。 • XML : テーブルをxml ファイルにエクスポートします。

インターフェイス

次の項を参照してください。

仮想インターフェイス グループ

テーブルの [バインドされたイーサネットインターフェイス (Bound Ethernet Interface)] フィールドは変更できます。残りのフィールドは情報提供のみを目的としています。

フィールド	説明
スイッチ	この仮想インターフェイス グループ (VIG) をホストするスイッチの名前。
VIG ID	仮想インターフェイス グループ ID。
Bound Eth Interface	この VIG に関連付けられた物理イーサネット インターフェイス。
Virtual Eth Interfaces	この VIG にバインドされた仮想イーサネット インターフェイス。
Virtual FC Interfaces	この VIG にバインドされた仮想 FC インターフェイス。
運用ステータス	VIG の現在の運用状態。
CreationTime	VIG が作成された日付と時刻。



(注) この表は、4.0(1a)より前のバージョンを実行しているN5kスイッチにのみ適用されます。

仮想 FC インターフェイス

テーブルの次のフィールドを変更できます: 説明、バインドタイプ、バインドインターフェイス、バインドMACアドレス、FCF優先度、VSAN IDポート、モード管理、ステータス管理。残りのフィールドは情報提供のみを目的としています。

フィールド	説明
スイッチ	このインターフェイスをホストするスイッチの名前。
Interface	インターフェイス名。
[説明 (Description)]	ネットワーク管理者によって指定されたインターフェイスのテキストによる説明。
VIG ID	この仮想 FC インターフェイスがバインドされる仮想インターフェイスグループ。
バインドタイプ	この仮想 FC インターフェイスに関連付けられているインターフェイスのタイプ - 物理イーサネット インターフェイスまたは FCoE ノード (ENode) の MAC アドレス。
Bind Interface	物理イーサネット インターフェイスまたはこの仮想 FC インターフェイスに関連付けられているイーサネット ポート チャンネル。
Bind MACAddress	FCoENode (ENode) または仮想 FC インターフェイスによって識別されるリモートのファイバチャンネル フォワーダ (FCF) の MAC アドレス
FCF Priority	FCF によって ENode にアダプタイズされる FCoE 初期化プロトコル (FIP) 優先度の値。
VSAN ID Port	インターフェイスが統計的に割り当てられている VSAN ID。
VSAN Id Dynamic	インターフェイスが統計的に割り当てられている VSAN の指数。
Mode Admin	ユーザーが構成したポート モード。仮想 FC インターフェイスは、ファブリック ポート (F ポート) モードのみをサポートします。
Rate Mode	インターフェイスを専用モードまたは共有モードとして指定します。
Speed Oper	動作速度。
Mode Oper	ポートの現在の動作モード。
Speed Admin	ユーザーが構成したポート速度。
Status Service	インターフェイスがイン サービスかアウト オブ サービスかを指定します。
Status Admin	インターフェイスの適切な状態。
Status Oper	インターフェイスの現在の動作状態。
Status FailureCause	ポートの現在の動作状態の原因。
Status LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカル ネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。



- (注) VIG Id フィールドは、4.0(1a) より前のバージョンを実行している N5k スイッチにのみ適用されます。

イーサネット インターフェイス

テーブルの[説明 (Description)]および[管理者 (fields)]フィールドは変更できます。残りのフィールドは情報提供のみを目的としています。

フィールド	説明
スイッチ	このインターフェイスをホストするスイッチの名前。
Interface	インターフェイス名。
[説明 (Description)]	ネットワーク管理者によって指定されたインターフェイスのテキストによる説明。
VIG ID	この仮想インターフェイスがバインドされる仮想インターフェイスグループ。
Bound Eth Interface	この仮想イーサネット インターフェイスに関連付けられた物理イーサネット インターフェイス。
Admin	インターフェイスの適切な状態。
Oper	インターフェイスの現在の動作状態。
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカルネットワーク管理サブシステムの前の初期化以前に現在の状態に移行した場合、この値は N/A です。
CDP (Enable)	Cisco 検出プロトコルがこのインターフェイスで実行されているかどうかを示します。
Duplex Status	MAC エンティティの現在の動作モード。ステータス「不明 (unknown)」は、現在の二重モードを判別できなかったことを示します。
Enable Link Trap	このインターフェイスに対してリンク アップ トラップまたはリンク ダウン トラップを生成するかどうかを指定します。



- (注) この表は、4.0(1a) より前のバージョンを実行している N5k スイッチにのみ適用されます。

仮想 FC イーサネット

フィールド	説明
スイッチ	このインターフェイスをホストするスイッチの名前。
インターフェイス	vFCインターフェイスの名前と、他のインターフェイスとの関連付けを表示します。
[説明 (Description)]	ネットワーク管理者によって指定されたインターフェイスのテキストによる説明。
Status Admin	インターフェイスの適切な状態。
Status Oper	インターフェイスの現在の動作状態。
Speed Oper	インターフェイスの動作速度
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカルネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。

クイック構成ツール

フィールド	説明
Show All Interfaces	このチェックボックスをオンにすると、vFC へのバインドに使用できないインターフェイスを含む、使用可能なすべてのインターフェイスが表示されます。
Auto Assign vFC Id	このチェックボックスをオンにすると、vFC ID が自動的に選択されます。このオプションをオンにしない場合は、有効な vFC ID を手動で入力する必要があります。
Switch Operational Type	スイッチでファイバー チャネル インターフェイスを構成していない場合は、[イーサネットスイッチ (Ethernet Switch)]をクリックします。ファイバーチャネルおよびFCoE インターフェイスを構成している場合は、[FCoE スイッチ (FCoE Switch)]をクリックします。
インターフェイス	物理的なイーサネット インターフェイスの名前。物理イーサネット インターフェイスにカーソルをホバーさせると、関連付けられている仮想インターフェイスがツールチップにディスプレイされます。
FCoE VLAN(VSAN)	インターフェイスで使用される FCoE VLAN (VSAN) マッピング。
管理モード	vFC インターフェイスの管理モード、つまり F または E
Eth のみ	物理イーサネットを仮想インターフェイス抜きで構成。列ヘッダーの [Eth のみ (Eth Only)] ボタンをクリックして、すべてのインターフェイスをこの値に設定します。

フィールド	説明
vEth Only	関連付けられた VIG と仮想イーサネットインターフェイスを持つように物理イーサネットを構成します。列ヘッダーの [vEth のみ (vEth Only)] ボタンをクリックして、すべてのインターフェイスをこの値に設定します。
vFC Only	関連付けられた VIG と仮想 FC インターフェイスを持つように物理イーサネットを設定します。列ヘッダーの [vFC のみ (vFC Only)] ボタンをクリックして、すべてのインターフェイスをこの値に設定します。
vFC	関連付けられた VIG と仮想 FC インターフェイスを持つように物理イーサネットを設定します。列ヘッダーの [vFC] ボタンをクリックして、すべてのインターフェイスをこの値に設定します。
vEth + vFC	関連付けられた VIG、仮想イーサネットインターフェイス、および仮想 FC インターフェイスを持つように物理イーサネットを設定します。列ヘッダーの [vEth + vFC] ボタンをクリックして、すべてのインターフェイスをこの値に設定します。
Configure Action Status	リクエストされた構成の変更の現在のステータスが表示されます。



(注) [vEth only]、[vFC only]、[vEth + vFC] 列は、バージョン 4.0(1a)N1 を実行している N5K スイッチには適用されません。



(注) バージョン 4.0(1a)N1 を実行している N5K スイッチには、[vFC] 列だけが適用されます。



(注) 以前に設定されたポートの場合、マッピングの詳細は [VLAN(VSAN)] マッピング列に表示されません。

イーサネットインターフェイス

フィールド	説明
説明	ネットワークマネージャによって指定されたインターフェイスの「エイリアス」名。
MTU	インターフェイスで送受信できる最大フレームのサイズ (バイト数)。
Speed Oper	インターフェイスの動作速度。

フィールド	説明
Speed Admin	<ul style="list-style-type: none"> • notApplicable - 速度の変更はそのポートには適用されません。 • oneGigSpeed - IPStorage ポートは 1G として構成されています。 • tenGigSpeed - IPStorage ポートは 10G として構成されています。
障害原因	失敗の原因
PhysAddress	インターフェイスの MAC アドレス。
Status Admin	インターフェイスの適切な状態。
Status Oper	インターフェイスの現在の動作状態。
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカルネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。
ConnectorPresent	コネクタが検出された場合は True。
CDP (Enable)	An indication of whether the Cisco Discovery Protocol is currently running on this interface.
IscsiAuthMethod	認証方式。
無差別モード	<p>このオプションのオンとオフにより、パケット/フレームの宛先が決まります。このオプションがオンの場合、このインターフェイスは、このステーション宛てのパケット/フレームを受け入れます。このオプションがオフの場合、ステーションによって受け入れられたパケットはメディアで送信されます。</p> <p>このオプションをオンまたはオフにしても、インターフェイスによるブロードキャストおよびマルチキャストパケット/フレームの受付には影響しません。</p>
自動ネゴシエーション	このオプションを選択すると、自動ネゴシエーションが有効になります。
ビーコンモード	ビーコンモードでは、識別のためにインターフェイス LED に点滅モードを割り当てます。ビーコンモードを有効にするには、このオプションを選択します。
IPAddress/Mask	インターフェイスの IP アドレスとサブネットマスク。



(注) SAN 管理ユーザーは、デバイス マネージャを使用して Cisco Nexus 5000 シリーズ スイッチのイーサネットインターフェイス設定を変更することができません。

Ethernet Interfaces iSCSI

フィールド	説明
説明	ネットワークマネージャによって指定されたインターフェイスのエイリアス名。
スピード	動作速度。
PhysAddress	インターフェイスの WWN。
Admin	インターフェイスの適切な状態。
Oper	インターフェイスの現在の動作状態。
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカルネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A になります。
PortVSAN	インターフェイスが属す VSAN。
ForwardingMode	HBA にパススルーで問題が発生する場合には、ストアアンドフォワードを使用します。
Initiator ID Mode	このインターフェイス上で発信側を識別する方法。iSCSI 名 (name) または IP アドレス (ipaddress) を使用します。
有効	このインターフェイス用の発信側プロキシモード。True の場合、このインターフェイスに接続するすべての発信側が、このインターフェイスで提供される発信側設定を使用します。発信側設定には、ポート WWN とノード WWN が含まれます。
割り当て	発信側プロキシモード FC アドレスを割り当てる方法。「自動」の場合、FC アドレスが自動的に割り当てられます。「手動」の場合、手動で設定する必要があります。
ポート WWN	発信側プロキシモードがオンの場合に、このインターフェイスで発信側が使用するポート FC アドレス。
Node WWN	発信側プロキシモードがオンの場合に、このインターフェイスで発信側が使用するノード FC アドレス

Ethernet Interfaces iSCSI TCP

フィールド	説明
ローカルポート	ローカル インターフェイスの TCP ポート。
SACK	選択的確認応答 (SACK) オプションがイネーブルかどうかを示します。
KeepAlive	この iSCSI インターフェイスの TCP キープアライブ タイムアウト。値が 0 の場合、キープアライブ タイムアウトは無効です。

フィールド	説明
MinTimeout	TCP 最小再送信時間。
最大	TCP 最大再送信回数。
SendBufferSize	TCP 送信バッファ サイズ。
MinBandwidth	TCP 最小帯域幅。
MaxBandwidth	TCP 最大帯域幅。
Estimated Round Trip	B-D 乗算に使用されるネットワーク パイプの推定ラウンドトリップ遅延。スイッチは、これを使用してアダプタイズする TCP ウィンドウを算出できます。
QoS	TCP QoS コード ポイント。
PMTU Enable	パス MTU ディスカバリ オプション オプションがイネーブルかどうかを示します。
PMTU Reset Timeout	PMTU リセット タイムアウト。
Connections Normal	通常の iSCSI 接続数。
Connections Discovered	ディスカバリ iSCSI 接続数。
CWM Enable	True の場合、輻輳ウィンドウ モニタリングがイネーブルされます。False の場合はディセーブルです。
CWM Burst Size	TCP 送信側の待機時間後に送信される最大バースト。
最大ジッター (Max Jitter)	このインターフェイスの TCP 接続で発生する可能性のある最大遅延変動 (輻輳が原因ではないもの)。
ポート	このインターフェイスのローカル TCP ポート。

イーサネット インターフェイス VLAN

フィールド	説明
スイッチ	スイッチ名。
インターフェイス	インターフェイスの名前。

フィールド	説明
VLAN モード	この VLAN が構成されているモード。 静的：単一の VLAN に直接割り当てられた静的 VLAN メンバーシップを持つポート。 ダイナミック：VMPS への VQP クエリを介してポートで受信したパケットの内容に基づく、単一の VLAN に割り当てられたダイナミック VLAN メンバーシップを持つポート。 multiVLAN：1 つ以上の VLAN に直接割り当てられた複数の VLAN メンバーシップを持つポート。
VLAN リスト	スイッチで許可されている VLAN のリスト。

イーサネット VLAN

フィールド	説明
スイッチ	スイッチ名。
ID	[スイッチID (Switch ID)]
トランク モード	モードがアクセスとトランクのどちらであるかを指定します。
トランク ステータス	ポートのトランッキング ステータス。
ネイティブ VLAN	ネイティブ VLAN
許可 VLAN リスト	ポートでの送受信が許可されている VLAN のリスト。
アクティブ VLAN リスト	スイッチ上でアクティブな VLAN のリストまたは範囲。

FC インターフェイス モニタリング トラフィック。

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
C3 Rx Bytes	このポートがアタッチしている Nx_Port から受信した、クラス 3 バイトの数。フレーム デリミタを含みます。
C3 Rx Frames	このポートがアタッチしている Nx_Port から受信した、クラス 3 フレームの数。フレーム デリミタを含みます。
C3 Tx Bytes	このポートがアタッチしている Nx_Port に送信した、クラス 3 バイトの数。フレーム デリミタを含みます。
C3 Tx Frames	このポートがアタッチしている Nx_Port に送信した、クラス 3 フレームの数。フレーム デリミタを含みます。

フィールド	説明
CF Rx Bytes	このポートがアタッチしている Nx_Port から受信した、クラス F バイトの数。フレーム デリミタを含みます。
CF Rx Frames	このポートがアタッチしている Nx_Port から受信した、クラス F フレームの数。フレーム デリミタを含みます。
CF Tx Bytes	このポートがアタッチしている Nx_Port に送信した、クラス F バイトの数。フレーム デリミタを含みます。
CF Tx Frames	このポートがアタッチしている Nx_Port に送信した、クラス F フレームの数。フレーム デリミタを含みます。

FC インターフェイス モニタリング プロトコル

[モニタ (Monitor)] ダイアログボックスには特別な **モニタ ダイアログ コントロール** があります。

フィールド	説明
LRRIn	FC ポートが受信したリンク リセット応答の数。
LRROut	FC ポートが送信したリンク リセット応答の数。
OlsIns	FC ポートが受信したオフライン シーケンス エラーの数。
OlsOuts	FC ポートが発行したオフライン シーケンス エラーの数。
NOSIn	FC ポートが受信した非動作シーケンスの数。
NOSOut	FC ポートが送信した非動作シーケンスの数。
LinkResetIns	アタッチされた FC ポートから FC ポートが受信したリンク リセット プロトコル エラーの数。
LinkResetOuts	アタッチされた FC ポートに対して FC ポートが発行したリンク リセット プロトコル エラーの数。
TxWaitCount	送信クレジットの不足のために FC ポートが待機した回数。
RxBBCredit	ログインした Nx_Port から受信したクラス 2、クラス 3 を保持するために使用可能な受信バッファの最大数。これは、ログインした Nx_Port から FC ポートへの着信方向のバッファ間フロー制御用です。
TxBBCredit	ログインした Nx_Port に送信されるクラス 2、クラス 3 フレームを保持するために使用可能なバッファの総数。これは、FC ポートから Nx_Port 方向のバッファ間フロー制御用です。
BBCreditTransitionFromZero	ゼロ状態からの BB クレジットの遷移の数。

FC インターフェイスでの破棄数モニタリング

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
Class2	このポートによって破棄されたクラス 2 フレームの数。
Class3	このポートによって破棄されたクラス 3 フレームの数。
classf	このポートによって破棄されたクラス F フレームの数。
EISL	FC ポートによって破棄された Enhanced Inter Switch Link (EISL) フレームの数。EISL フレームには、他の情報とともに VSAN を含む EISL ヘッダーが含まれます。
InDiscards	エラーが検出されなかったにもかかわらず、上位層プロトコルに配信されないようにするため、破棄することが選択された着信フレームの合計数。
OutDiscards	エラーが検出されなかったにもかかわらず、送信されないようにするため、破棄することが選択された発信フレームの合計数。

FC インターフェイス モニタ リンク エラー

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
LinkFailures	FC-Port によって検出されたリンク障害の数。
SigLosses	FC-Port によって検出された信号損失の数。
SyncLosses	FC-Port によって検出された同期喪失障害の数。
InvalidTxWords	FC-Port によって検出された無効な送信ワードの数。
DelimiterErrors	FC-Port によって検出されたデリミタ エラーの数。
AddressIdErrors	FC-Port によって検出されたアドレス識別子エラーの数。

FC インターフェイス モニタ フレーム エラー

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
InvalidCrcs	FC-Port によって検出された無効な CRC の数。ループポートは、モニタリング時に通過する CRC エラーをカウントしないことになっています。

フィールド	説明
ELPFailures	FC ポートによって検出された、エクステンジリンク パラメータ スイッチ ファブリックの内部リンク サービス リクエストの失敗数。これは、E_Port または B_Port である Interconnect_Port のみに適用されます。
[フラグ (Frag)]	FC ポートが受信したフラグメント化されたフレームの数。
Runts	FC ポートが受信したフレームのうち、許容される最小フレーム長よりも短いフレームの数。CRC が正しいかどうかには関係しません。
Jabber 数	FC ポートが受信したフレームのうち、最大フレーム長より長く、CRC エラーもあるフレームの数。
TooLongs	FC ポートが受信したフレームのうち、フレーム長が FLOGI/PLOGI で合意されたものよりも長いフレームの数。これは、フレームの終わりの区切り文字が失われたことが原因である可能性があります。
TooShorts	FC ポートが受信したフレームのうち、フレーム長がフレーム ヘッダーで示される最小値 (通常 24 バイト) よりも短いフレームの数ですが、オプションのヘッダーが存在しているはずであることを DFCTL フィールドが示している場合は、さらに多くなる可能性があります。
Unknowns	FC ポートが受信した、フラグメント化されたフレームの数。
EOFa	FC ポートが受信したフレームのうち、EOF アポートが伴っているフレームの数。
フレーミング (Framing)	フレーム エラーの数。これは、FC ポートがフレーム構造の不整合を検出したことを示しています。

FC インターフェイス モニタ クラス2トラフィック

[モニタ (Monitor)] ダイアログボックスには特別な **モニタ ダイアログ コントロール** があります。

フィールド	説明
In Octets/In Frames	アタッチされた Nx_Port からこのポートが受信したクラス2フレーム バイトおよびフレームの数。フレーム デリミタを含みます。
Out Octets/Out Frames	アタッチされた Nx_Port にこのポートを介して配信されたクラス2フレーム バイトおよびフレームの数。フレーム デリミタを含みます。

FC インターフェイス モニタ クラス2エラー

[モニタ (Monitor)] ダイアログボックスには特別な **モニタ ダイアログ コントロール** があります。

フィールド	説明
FBSY	ビジー フレーム応答の数。
FRJT	クラス 2 フレームに対してこのポートによって生成された F_RJT フレームの数。
PBSY	クラス 2 フレームをリンクのもう一方の端に配信できなかった結果として、ポート ビジー状態がこのポートに返された回数。これは、宛先 Nx_Port が一時的にビジーの場合に発生します。PBSY は、SOFC1 フレーム（接続を確立するフレーム）でのみ発生します。
PRJT	クラス 2 フレームが宛先 Nx_Port で拒否された結果として、ポート拒否がこのポートに返された回数。

FC インターフェイス モニタ FICON

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
FramePacingTime	クレジットがゼロのためにフレーム送信がブロックされる、2.5 マイクロ秒を単位とする数。
DispErrorsInFrame	ディスパリティ エラーのあるフレームの数。
EOFErr	EOF エラーのあるフレームの数。
DispErrsOutOfFrame	OOE エラーのあるフレームの数。
InvalidOrderSets	フレーム外の無効または認識できないオーダー セットの数。

オーバーサブスクリプションの確認

フィールド	説明
間隔	
Elapsed	経過時間。
インターフェイス	インターフェイスの名前
InOctectRate	
OutOctectRate	

仮想 FC インターフェイス モニタリング トラフィック

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
RxBytes	接続された N_Port からこのポートが受信したバイト数（フレーム デリミタを含む）。
[RxFrames]	接続された N_Port からこのポートが受信したフレームの数（フレーム デリミタを含む）。
TxBytes	このポートによって接続された N_Port に送信されたバイト数（フレーム デリミタを含む）。
[TxFrames]	このポートによって接続された N_Port に送信されたフレームの数（フレーム デリミタを含む）。

仮想 FC インターフェイス モニタ 廃棄数

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
InDiscards	エラーが検出されなかったにもかかわらず、上位層プロトコルに配信されないようにするため、廃棄することが選択された着信フレームの合計数。
OutDiscards	エラーが検出されなかったにもかかわらず、送信されないようにするため、廃棄することが選択された発信フレームの合計数。

仮想 FC インターフェイス モニタ エラー

[モニタリング (Monitor)] ダイアログボックスには特別な [モニタリング ダイアログ コントロール](#) があります。

フィールド	説明
InErrors	仮想 FC ポートによって検出された着信エラーの数。
OutErrors	仮想 FC ポートによって検出された発信エラーの数。

イーサネット インターフェイス Dot3Stats

フィールド	説明
インターフェイス	インターフェイスの名前。
Alignment Errors	長さがオクテットの整数倍であるものの、FCS チェックに合格しなかった、特定のインターフェイスでの受信フレームの数。

フィールド	説明
FCS エラー	長さがオクテットの整数倍であるものの、FCS チェックに合格しなかった、特定のインターフェイスでの受信フレームの数。この数には、フレームが長すぎる、またはフレームが短すぎるためにエラーが生じた受信フレームは含まれません。
シングルコリジョンフレーム	特定のインターフェイスで正常に送信されたものの、送信が1つのコリジョンだけによって妨げられたフレームの数。
マルチコリジョンフレーム	特定のインターフェイスで正常に送信されたものの、送信が2つ以上のコリジョンによって妨げられたフレームの数。
SQEテストエラー	特定のインターフェイスについて、SQE TEST ERROR メッセージが PLS サブレイヤによって生成された回数。
遅延送信	特定のインターフェイスでの最初の送信試行が、メディアがビジー状態のために遅延したフレームの数。
レイトコリジョン	パケットの送信の1スロット時間より後に、特定のインターフェイスでコリジョンが検出された回数。
過剰コリジョン	多数のコリジョンが生じたことによって、特定のインターフェイス上で送信が失敗したフレームの数。インターフェイスが全二重モードで動作している場合、このカウンタが増えることはありません。
内部 Mac 送信エラー	内部MACサブレイヤの送信エラーのために特定のインターフェイスで送信が失敗したフレームの数。
キャリア検知エラー	特定のインターフェイスでフレームを送信しようとしたときに、キャリア センス状態が失われたか、一度もアサートされなかった回数。
長すぎるフレーム	特定のインターフェイスで受信され、最大許可フレーム サイズを超えたフレームの数。
内部MAC受信エラー	内部MACサブレイヤ受信エラーが原因で、特定のインターフェイスでの受信に失敗したフレームの数。
Symbol Errors	100 Mb/s で動作するインターフェイスの場合、有効なキャリアが存在しながら無効なデータ シンボルがあった回数

インターフェイス モニタ

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
Rxバイト	インターフェイスで受信したバイト合計数 (フレーミング文字を含む)。

フィールド	説明
[RxFrames]	インターフェイスで受信したフレームの数。
Rx マルチキャスト フレーム (Rx Multicast Frames)	(Nexus 5000 シリーズのみ) インターフェイスで受信したマルチキャスト フレームの数。
Rx ブロードキャスト フレーム (Rx Broadcast Frames)	(Nexus 5000 シリーズのみ) インターフェイスで受信したブロードキャスト フレームの数。
TxBytes	インターフェイスが送信したバイトの合計数 (フレーミング文字を含む)。
[TxFrames]	このインターフェイスが送信したフレームの合計数。
Tx マルチキャスト フレーム (Tx Multicast Frames)	(Nexus 5000 シリーズのみ) このインターフェイスが送信したマルチキャスト フレームの数。
Tx ブロードキャスト フレーム (Tx Broadcast Frames)	(Nexus 5000 シリーズのみ) このインターフェイスが送信したブロードキャスト フレームの数。
RxErrors	エラーを含むために上位層のプロトコルに配信不可能だった着信フレームの数。
TxErrors	エラーのために送信できなかった発信フレームの数。
RxDiscards	エラーが検出されなかったにもかかわらず、上位層プロトコルに配信されないようにするために廃棄することが選択された着信フレームの合計数。
TxDiscards	エラーが検出されなかったにもかかわらず、送信されないようにするために廃棄することが選択された発信フレームの合計数。

イーサネット ポートチャネル

フィールド	説明
説明	ネットワーク マネージャによって指定されたインターフェイスのエイリアス名。
メンバー	このイーサネット ポートチャネルのメンバー。
動作速度	インターフェイスの動作速度。
MTU	インターフェイスで送受信できる最大フレームのサイズ (バイト数)。
PhysAddress	インターフェイスの MAC アドレス。
Status Admin	インターフェイスの適切な状態。
Status Oper	インターフェイスの現在の動作状態。

フィールド	説明
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカル ネットワーク 管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。

Ethernet Interface Monitor iSCSI Connections

フィールド	説明
RxBytes	iSCSI セッションで受信した合計バイト数。
TxBytes	iSCSI セッションで送信した合計バイト数。
IPSec	iSCSI 接続統計情報に関するオブジェクトのコレクション。

イーサネット インターフェイス モニタリング TCP

フィールド	説明
Opens	接続が開かれた回数。
受諾	接続が受け入れられた回数。
失敗しました	接続に失敗した回数。
RxResets	接続がリセットされた回数。
Est	接続が確立された回数。
RxSeg	確立したセグメントで受信したセグメントの合計数。エラーを受信したセグメントも含まれます。
TxSeg	送信されたセグメントの合計数。再送信されたバイトを含むものは除きます。
ReTxSegs	再送信されたセグメントの総数。
BadSegs	エラーを受信したセグメントの合計数 (例えば、悪いチェックサム)。
TxSegResets	「リセット」フラグを含む送信したセグメントの数。
SplitSeg	送信されたセグメントのうち、最小サイズ未満のもの数。
DupACK	受信された重複 ACK の数。
RxBytes	受信したヘッダーとデータのバイト数。
TxBytes	送信されたヘッダーとデータのバイト数。

FCIP Monitor

[モニタ (Monitor)] ダイアログボックスには特別な**モニタ ダイアログ コントロール**があります。

フィールド	説明
C3 Rx Bytes	データ トラフィックの着信バイト数。
C3 Tx Bytes	データ トラフィックの発信バイト数。
CF Rx Bytes	制御トラフィックの着信バイト数。
CF Tx Bytes	制御トラフィックの発信バイト数。
Rxエラー	エラーを含むために上位層のプロトコルに配信不可能だった着信フレームの数。
Txエラー	エラーのために送信できなかった発信フレームの数。
RxDiscard	エラーが検出されなかったにもかかわらず、上位層プロトコルに配信されないようにするために廃棄することが選択された着信フレームの合計数。
TxDiscard	エラーが検出されなかったにもかかわらず、送信されないようにするために廃棄することが選択された発信フレームの合計数。

SVC インターフェイスのモニタ

[モニタ (Monitor)] ダイアログボックスには特別な**モニタ ダイアログ コントロール**があります。

フィールド	説明
Rxバイト	着信バイト数。
Rx フレーム	着信フレームの数
Tx Bytes	発信バイト数。
Tx フレーム	発信フレーム数。
Rx Errors	着信エラーの数。
Tx Errors	発信エラーの数。
Rx廃棄	着信廃棄の数。
Tx廃棄	発信廃棄の数。

SVC NPorts のモニタリング

[モニタ (Monitor)] ダイアログボックスには特別な [モニタ ダイアログ コントロール](#) があります。

フィールド	説明
Rxバイト	この仮想 N ポートの着信バイト数。
Rx フレーム	この仮想 N ポートの着信フレーム数。
Tx Bytes	この仮想 N ポートの発信バイト数。
Tx フレーム	この仮想 N ポートの発信フレーム数。
Rxバイト	この仮想 N ポートの着信バイト数。
Rx フレーム	この仮想 N ポートの着信フレーム数。
Tx Bytes	この仮想 N ポートの発信バイト数。
Tx フレーム	この仮想 N ポートの発信フレーム数。

SVC セッション FCP のモニタリング

[モニタリング (Monitor)] ダイアログボックスには特別な [モニタリング ダイアログ コントロール](#) があります。

フィールド	説明
Cmnds	このセッションの着信 FCP コマンド フレームの数。
XferRdys	このセッションの着信 FCP 転送準備完了フレームの数。
DataFrames	着信 FCP Data フレームの数。
ステータス	着信 FCP ステータス フレームの数。
DataBytes	着信 FCP データのバイト数。
OverRuns	このセッションの着信 FCP オーバーランフレームの数。
UnderRuns	このセッションの着信 FCP アンダーランフレームの数。
Cmnds	このセッションの発信 FCP コマンド フレームの数。
XferRdys	このセッションの発信 FCP 転送準備完了フレームの数。
DataFrames	発信 FCP データ フレームの数。

フィールド	説明
ステータス	発信 FCP ステータス フレームの数。
DataBytes	発信 FCP データのバイト数。
OverRuns	このセッションの発信 FCP オーバーランフレームの数。
UnderRuns	このセッションの発信 FCP アンダーランフレームの数。

SVC セッション モニタリングその他

[モニタ (Monitor)] ダイアログボックスには特別な **モニタ ダイアログ コントロール** があります。

フィールド	説明
InELSFrames	このセッションの着信拡張リンク サービスフレームの数。
InBLSFrames	このセッションの着信基本リンク サービスフレームの数。
OutELSFrames	このセッションの発信拡張リンク サービスフレームの数。
OutBLSFrames	このセッションの発信基本リンク サービスフレームの数。
InAborts	このセッションで中止された着信フレームの数。
OutAborts	このセッションで中止された発信フレームの数。
OpenXchanges	このセッションのオープン交換の数。
InBadFc2Drops	このセッションでドロップされた FC2 フレームの数。
InBadFcPDrops	FCP ドロップされたフレームの数。
InFCPDataExcess	このセッションの FCP データ超過フレームの数。

FCIP インターフェイス

フィールド	説明
説明	ネットワーク マネージャによって指定されたインターフェイスのエイリアス名。
PortVsan	このインターフェイスが静的に割り当てられている VSAN ID。
Oper Mode	ポートの現在の動作モード。
AutoChannelCreate	選択すると、ポートチャネルを自動的に作成します。
Admin	インターフェイスの適切な状態。
動作ステータス	インターフェイスの現在の動作状態。

フィールド	説明
FailureCause	ポートの現在の動作状態の原因。
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカル ネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。
FICON Address	このポートの FICON ポート アドレス。

システム タイムアウト

スイッチに長期間存在するフレームは、輻輳ドロップと見なされます。継続的に tx/rx クレジットを受信していない場合、ノークレジット ドロップと見なされます。デバイスマネージャクライアントで、輻輳ドロップとノークレジット ドロップのタイムアウト値を設定できます。低速ポート モニタリングのタイムアウトを構成するには、**[管理 (Admin)] > [システム タイムアウト (System Timeout)]** に移動します。

フィールド	説明
E port Congestion Drop	E ポートの輻輳ドロップの時間を指定します。または、デフォルトをクリックしてデフォルト値を入力します。 単位はミリ秒です。
F ポート輻輳ドロップ	F ポートの輻輳ドロップの時間を指定します。または、デフォルトをクリックしてデフォルト値を入力します。 単位はミリ秒です。
F port NoCredit Drop	ノークレジット ドロップの時間を指定します。 tx/rx クレジットのないフレームをドロップすることを望まない場合は、無効をクリックするか、デフォルトをクリックしてデフォルト値を入力します。 単位はミリ秒です。
E Port slowport-monitor	E ポートの slowport-monitor タイムアウト値を指定します。 スローポートの監視を無効にするには、無効をクリックします。または、デフォルトをクリックしてデフォルト値を入力します。 単位はミリ秒です。
F Port slowport-monitor	F ポートの slowport-monitor タイムアウト値を指定します。 スローポートの監視を無効にするには、無効をクリックします。または、デフォルトをクリックしてデフォルト値を入力します。 単位はミリ秒です。



- (注) SANクライアントからの低速ポートモニタリングのタイムアウト値を構成するには、[物理属性 (Physical Attributes)] > [スイッチ (Switch)] > [システム (System)] > [タイムアウト (Timeout)] に移動します。

インターフェイス ライセンス

フィールド	説明
タイプ	特定のインターフェイスに対して取得できるライセンスを指定します。現在、ポート アクティベーション ライセンスを定義できます。
設定	インターフェイスが適格なライセンスを表示します。どのタイプのライセンスにも適格でないインターフェイスは表示されません。
Oper	インターフェイスのポート ライセンスの現在の状態が表示されます。

全般

フィールド	説明
説明	ネットワーク マネージャによって指定されたインターフェイスのエイリアス名。
MTU	インターフェイスで送受信できる最大フレームのサイズ (バイト数)。
Oper	動作速度
PhysAddress	インターフェイスの MAC アドレス。
Admin	管理者の状態。
Oper	インターフェイスの現在の動作状態。
LastChange	インターフェイスが現在の動作状態にいつ移行したか。
CDP	CDP を有効または無効にします。
デフォルト ゲートウェイ (Default Gateway)	デフォルト ゲートウェイの IP アドレス。

FC インターフェイス全般

PortVSAN、Port Mode Admin and Oper、Admin Speed、FailureCause 変数は、すべてのインターフェイスでサポートされているわけではありません。

フィールド	説明
説明	ネットワーク マネージャによって指定されたインターフェイスのエイリアス名。
VSAN Id Port	このインターフェイスが静的に割り当てられている VSAN ID。
VSAN Id Dynamic	このインターフェイスが動的に割り当てられている VSAN ID (DPVM を参照)。
CDP (Enable)	An indication of whether the Cisco Discovery Protocol is currently running on this interface.
無差別モード	<p>このオプションのオンとオフにより、パケット/フレームの宛先が決まります。このオプションがオンの場合、このインターフェイスは、このステーション宛てのパケット/フレームを受け入れます。このオプションがオフの場合、ステーションによって受け入れられたパケットはメディアで送信されます。</p> <p>このオプションをオンまたはオフにしても、interface9 によるブロードキャストおよびマルチキャストパケット/フレームの受け付けには影響しません。</p>
Auto Negotiate	このインターフェイスで速度と二重モードの自動ネゴシエーションを使用する必要があるかどうかの指示。
ビーコンモード	ビーコンモードでは、識別のためにインターフェイス LED に点滅モードを割り当てます。ビーコンモードを有効にするには、このオプションを選択します。

フィールド	説明
Mode Admin	

フィールド	説明
	<p>ユーザーが構成したポート モード。モードは次のとおりです。</p> <ul style="list-style-type: none"> • auto - ユーザーがポートを auto として構成した場合、ポートの初期化スキームによってポートのモードが決定されます。 • F Port - インターフェイスがファブリックポートとして機能します。このポートを N ポートとして動作する周辺装置（ホストまたはディスク）に接続できます。 • FL Port - ファブリック ループ モードでは、インターフェイスがファブリック ループ ポートとして機能します。このポートを1つまたは複数の NL ポート（他のスイッチの FL ポートを含む）に接続し、パブリック アービトラート型ループを形成することができます。 • E Port - 拡張ポートモードでは、インターフェイスがファブリック拡張ポートとして機能します。このポートを別の E ポートに接続し、2つのスイッチ間でスイッチ間リンク（ISL）を作成できます。E ポートはフレームをスイッチ間で伝送し、ファブリックを設定および管理できるようにします。 • FX Port - Fx ポートとして構成されたインターフェイスは、F ポートまたは FL ポートモードのいずれかで動作します。Fx ポートモードは、インターフェイスの初期化中に、接続された N ポートまたは NL ポートに応じて判別されます。この管理設定は、インターフェイスがその他のモードで動作するのを禁止します。たとえば、別のスイッチにインターフェイスが接続されるのを防ぎます。 • SD Port - SPAN 宛先ポートモードでは、インターフェイスがスイッチドポートアナライザ（SPAN）として機能します。SPAN 機能は、Cisco MDS 9000 ファミリスイッチに特有の機能です。ファイバチャンネルインターフェイスを通過するネットワークトラフィックをモニタします。 • TL Port -

フィールド	説明
	<p>トランスレーティブループポートモードでは、インターフェイスがトランスレーティブループポートとして機能します。1つまたは複数のプライベートループ装置に接続できます。TLポートモードはCisco MDS 9000 ファミリスイッチに特有で、FLポートとプロパティが似ています。</p> <ul style="list-style-type: none"> • ST Port - SPAN トンネルポート (STポート) モードでは、インターフェイスがRSPANファイバチャネルトンネルの送信元スイッチ内の入口ポートとして機能します。STポートモードとリモートSPAN (RSPAN) 機能は、Cisco MDS 9000 ファミリスイッチに特有の機能です。STポートモードに構成されている場合、インターフェイスを任意の装置に設定できないので、通常のファイバチャネルトランジックに使用できません。 • TE Port - トランキングEポートモード では、インターフェイスがトランキング拡張ポートとして機能します。別のTEポートに接続し、2つのスイッチ間でExtended ISL (EISL) を作成します。TEポートは、Cisco MDS 9000 ファミリスイッチに特有のポートです。 • B Port - Eポート が通常はファイバチャネルスイッチを相互接続するのに対して、シスコ製のPA-FC-1Gファイバチャネルポートアダプタなど、一部のSAN拡張装置は、ブリッジポートモデルを実装して地理的に分散したファブリックを接続します。このポートタイプの操作モードは「読み取り専用」であり、設定できません。 • TF - トランキング f_Port • TNPポート - Nポートバーチャライザー (NPV) にのみ適用されるトランキングNプロキシポートモード • NPポート - Nポートバーチャライザー (NPV) にのみ適用可能なNプロキシポートモード

フィールド	説明
Mode Oper	ポートの現在の動作モード。
SpeedGroup	特定のインターフェイスの現在の速度グループ構成を指定します。 <ul style="list-style-type: none"> • None : このインターフェイスにインターフェイス速度グループ設定は適用されません。読み取り専用の値です。 • 10G : このインターフェイスのインターフェイス速度グループ設定は 10G です。 • 1/2/4/8G : このインターフェイスでのインターフェイス速度グループ構成は 1G-2G-4G-8G です。
Speed Admin	ユーザーが構成したポート速度。ポートの速度値は [auto]、[1Gb]、[2Gb]、[4Gb]、[8Gb]、[10Gb]、[autoMax2G]、および [autoMax4G] のいずれかです。 注 Cisco NX-OS リリース 4.2(2) を実行する Cisco Nexus 5000 シリーズスイッチでは、M1060 スイッチモジュールでのみ 8 Gbps の管理速度を設定できます。Cisco NX-OS リリース 4.2(2) 以前のリリースを実行する Cisco Nexus 5000 シリーズスイッチでは、すべてのスイッチモジュールで速度を 1 Gbps、2 Gbps、または 4 Gbps に設定できます。
Speed Oper	動作速度。
RateMode	インターフェイスを専用モードまたは共有モードとして指定します。
Status Service	インターフェイスがインサービスかアウトオブサービスかを指定します。
Status Admin	インターフェイスの適切な状態。
Status Oper	インターフェイスの現在の動作状態。
Status FailureCause	ポートの現在の動作状態の原因。
StatusWasEnabled	true の場合、このポートはリンクの初期化を正常に完了しています。
Status LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカル ネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。

フィールド	説明
Port Owner	インターフェイス リソースの現在の所有者に管理上割り当てられた名前。

FC インターフェイス Rx BB クレジット+

フィールド	説明
Oper	動作ポートモード用に構成された受信バッファ間クレジット。
モデル	FC ポートで使用される BB_Credit モデル。代替の BB_Credit 管理モデルを調停ループ トポロジで使用して、現在のループ回路に参加している 2 つのポート間のフレーム フローを管理できます。これは物理ポートの特性であるため、ポートチャネルポートには適用されません。
Admin	このポートに設定された受信バッファ間クレジット。
拡張	FC ポートで構成できる拡張 BB クレジット (256 ~ 4095 の範囲)。許容値は、モジュールの他のポートの BB クレジット構成によって異なります。この値は、拡張 BB クレジット機能をサポートするモジュールでのみ変更できます。
AdminISL	このポートが xE_port モードで動作している場合に使用されるように構成された受信バッファ間クレジット。
AdminFx	このポートが Fx モードで動作している場合に使用されるように構成された受信バッファ間クレジット。
PerfBuffer Admin	このポート用に構成されたパフォーマンスバッファ。バッファ間クレジットに加えて、これらのバッファは、ポートのパフォーマンスを向上させるために使用されます。値 0 が設定されている場合、モジュールは組み込みアルゴリズムを使用して、使用するパフォーマンス バッファの数を計算します。
PerfBuffer Oper	パフォーマンス バッファは、現在このポートで動作しています。

フィールド	説明
Oper Rx	ピア <code>Interconnect_Port</code> から受信したクラス 2、クラス 3、クラス F フレームを保持するために使用できる受信バッファの最大数。
Oper Tx	ピア <code>Interconnect_Port</code> に送信されるクラス 2、クラス 3、クラス F フレームを保持するために使用可能なバッファの総数。
Current Rx	このポートの受信バッファ間クレジットの現在の値。
現在の送信	このポートの送信バッファ間クレジットの現在の値。
BbScn Notify	バッファ間状態変更番号 (<code>BB_SC_N</code>) モードが有効になっているかどうかを示します。オンにすると、 <code>BB_SC_N</code> モードが有効になります。オフにすると、 <code>BB_SC_N</code> モードが無効になります。

FC の他のインターフェイス

フィールド	説明
PortChannel Id	インターフェイスが属しているポートチャネル。
Fabric WWN	このインターフェイスに付けられたワールドワイドネーム。
Mtu bytes	インターフェイスで送受信できる最大フレームのサイズ (バイト数)。
RxDataFieldSize bytes	このポートで受信できる FT_1 フレームの最大 <code>Data_Field</code> サイズ。
HoldTime us	フレームを送信できない場合に、FC ポートがフレームを破棄する前に送信バッファに保持する最大時間。
Auto Port Channel	ポートチャネルを自動的に作成するかどうかを確認します。
FEC Admin	構成されたポート FEC 状態を指定します。
FEC Oper	ポートの現在の動作 FEC 状態を指定します。

FC インターフェイス FLOGI

フィールド	説明
FcId	ログインした <code>Nx_Port</code> に割り当てられたアドレス識別子。
PortName	ログインしている <code>Nx_Port</code> のワールドワイド名。

フィールド	説明
NodeName	ログインした Nx_Port が属するリモート ノードのワールド ワイド名。
Original PWWN	このインターフェースの元のポート WWN
バージョン	Fx_Port がファブリック ログインからサポートすることに同意した FC-PH のバージョン。
BBCredit Rx	ログインした Nx_Port から受信したクラス 2、クラス 3 を保持するために使用可能な受信バッファの最大数。これは、ログインした Nx_Port から FC-Port への着信方向のバッファ間フロー制御用です。
BBCredit Tx	ログインした Nx_Port に送信されるクラス 2、クラス 3 フレームを保持するために使用可能なバッファの総数。これは、FC-Port から Nx_Port 方向のバッファ間フロー制御用です。バッファ間フロー制御メカニズムは、それぞれの BbCreditModel で示されます。
CoS	ログインした Nx_Port が FC-Port にサポートを要求し、FC-Port が要求を許可したサービスのクラス。
Class2 RxDataSize	ログインした Nx_Port のクラス 2 受信データフィールド サイズ。Nx_Port で受信できる FT_1 フレームの最大データフィールド サイズを指定します。
Class2 SeqDeliv	FC-Port がファブリック ログイン中にクラス 2 の順次配信をサポートすることに同意したかどうか。これは、クラス 2 サービスが合意されている場合にのみ意味があります。これは、Fx_Ports にのみ適用されます。
Class3 RxDataSize	ログインした Nx_Port の Class3 受信データフィールド サイズ。Nx_Port が受信できる FT_1 フレームの最大データフィールド サイズを指定します。
Class3 SeqDeliv	FxPort がファブリック ログイン中にクラス 3 の順次配信をサポートすることに同意したかどうか。これは、クラス 3 サービスが合意されている場合にのみ意味があります。これは、Fx_Ports にのみ適用されます。

FC インターフェイス ELP

フィールド	説明
近接ポート	ピア Interconnect_Port のポート ワールド ワイド名。
Neighbor Switch	ピア ノードのノード ワールド ワイド名。
BBCredit Rx	ピアの Interconnect_Port から受信した保留クラス 2、クラス 3、クラス F フレームで使用できる受信バッファの最大数。これは、ピアの Interconnect_Port からローカルの Interconnect_Port への着信方向のバッファ間フロー制御用です。 バッファ間フロー制御メカニズムは、それぞれの BbCreditModel で示されます。
BBCredit Tx	ピアの Interconnect_Port に送信される保留クラス 2、クラス 3、クラス F フレームで使用できるバッファの最大数。これは、ローカルの Interconnect_Port からピアの Interconnect_Port への方向のバッファ間フロー制御用です。 バッファ間フロー制御メカニズムは、対応する BbCreditModel で示されます。
CoS	ピアの Interconnect_Port がローカルの Interconnect_Port にサポートを要求し、ローカルの Interconnect_Port が要求を許可したサービスのクラス。
Class2 SeqDeliv	ローカルの Interconnect_Port が、Exchange リンク パラメータ スイッチファブリック内部リンク サービス リクエスト中にクラス 2 の順次配信をサポートすることに同意したかどうか。これは、クラス 2 サービスが合意されている場合にのみ意味があります。
Class2 RxDataSize	ピア Interconnect_Port のクラス 2 受信データ フィールド サイズ。Interconnect_Port で受信できる FT_1 フレームの最大データ フィールド サイズを指定します。これは、クラス 2 サービスが合意されている場合にのみ意味があります。

フィールド	説明
Class3 SeqDeliv	ローカルの <code>Interconnect_Port</code> が、Exchange リンクパラメータスイッチファブリック内部リンクサービスリクエスト中にクラス3の順次配信をサポートすることに同意したかどうか。これは、クラス3サービスが合意されている場合にのみ意味があります。
Class3 RxDataSize	ピア <code>Interconnect_Port</code> のクラス3受信データフィールドサイズ。 <code>Interconnect_Port</code> で受信できる FT_1 フレームの最大データフィールドサイズを指定します。これは、クラス3サービスが合意されている場合にのみ意味があります。
ClassF X_ID	true の場合、このパラメータを提供するピア <code>Interconnect_Port</code> は、クラスFの X_ID 割り当て中にインターロックを使用する必要があることを示します。これは、クラスFサービスが合意されている場合にのみ意味があります。
ClassF RxDataSize	ピア <code>Interconnect_Port</code> のクラスF受信データフィールドサイズ。クラスFサービスは、常に2つの <code>Interconnect_Port</code> 間で合意されます。 <code>Interconnect_Port</code> で受信できる FT_1 フレームの最大データフィールドサイズを指定します。
ClassF ConSeq	シーケンス受信側としてシーケンスの進行状況を追跡するためのパラメータを提供する <code>Interconnect_Port</code> によって提供されるシーケンスステータスブロックの数。指定できる同時シーケンスの最大数は255です。このフィールドの N/A の値は予約されています。
ClassF EECredit	付随する ACK または <code>Link_Response</code> フレームを受信せずに <code>Interconnect_Port</code> によって送信できるクラスFデータフレームの最大数。エンドツーエンドクレジットの最小値は1です。指定されたエンドツーエンドのクレジットフィールドは、クラスFフレームの <code>Data_Field</code> を保持し、パラメータを提供する <code>Interconnect_Port</code> によってその <code>Data_Field</code> の内容を処理するために使用可能なバッファの数に関連付けられます。

フィールド	説明
ClassF OpenSeq	交換ごとのオープン シーケンスは、1 回の交換の Interconnect_Port のペア間で受信側で一度にオープンできるシーケンスの最大数を指定するものとします。この値は、交換とシーケンスの追跡に使用されます。

FC インターフェイスのトランク構成

フィールド	説明
Admin	ユーザーが構成したトランキング モード。 <ul style="list-style-type: none"> • nonTrunk に設定すると、ポートはネゴシエーションを行い、リンクを非トランキング モードに変換します。このポートとピアポートの OperTrunkMode は、複数の VSAN トラフィックを伝送しません。 • trunk に設定すると、ピアポートが trunk または auto の場合にのみ、ポートはネゴシエーションを行い、リンクをトランキング モードに変換します。 • auto に設定すると、ピアポートが trunk の場合にのみ、ポートはリンクをトランク リンクに変換します。
Oper	ポートの現在のトランキング モード。
Allowed VSANs	ポートがトランキング モードで動作しているときに、ポートで送受信できる VSAN のリスト。複数の VSAN に所属させることができるのは、トランク モードで動作しているポートだけです。
Up VSANs	このポートが関連付けられている、動作状態がアップの VSAN のリスト。複数の VSAN に関連付けさせることができるのは、トランク モードで動作しているポートだけです。これは、トランク モードで動作しているポートにのみ適用されます。

FCIP Interfaces Trunk Failures

フィールド	説明
FailureCause	指定された VSAN のトランク ステータスにエラーがある場合、このテーブルにエントリが表示されます。

FC インターフェイス IP

フィールド	説明
スイッチ	スイッチの名前。
イーサネット インターフェイス	イーサネット インターフェイスを識別する一意の値。
イーサネットのステータス	イーサネット インターフェイスの現在の動作状態。
Ethernet IP Address	このエンティティのインターネットアドレス。
ピアIPアドレス	このエンティティのインターネットアドレス
ポート	最新の CDP メッセージでレポートされたポート ID 文字列。
ピアインターフェイス	このリンクが関連するデバイスのピアインターフェイスを識別する一意の値。
Peer Device Id	最新の CDP メッセージでレポートされたピアデバイス ID 文字列。
IP Security Enabled	IP セキュリティをオンにするかどうかを指定します。

FC インターフェイスの物理的特徴

フィールド	説明
BeaconMode	有効にすると、インターフェイス LED が点滅モードに変わって、特定のインターフェイスを簡単に識別できるようになります。
ConnectorPresent	true の場合、物理コネクタがあります。
ConnectorType	ポート コネクタのモジュールタイプ。
TransmitterType	ポート トランシーバのテクノロジー。
ベンダー	コネクタ装置のベンダー。
PartNumber	コネクタ装置の部品番号。
リビジョン	コネクタ装置のポート リビジョン。
SerialNo	コネクタ装置のシリアル番号。

FC インターフェイス機能

フィールド	説明
FC-PH Vers Low	FC-Port がサポートできる FC-PH の最低バージョン。
FC-PH Vers High	FC-Port がサポートできる FC-PH の最高バージョン。
RxDataSize Min	FC ポートがアタッチされた FC ポートから受信できるフレーム内のデータ フィールドの最小サイズ (バイト単位)。
RxDataSize Max	FC ポートがアタッチされた FC ポートから受信できるフレーム内のデータ フィールドの最大サイズ (バイト単位)。
HoldTime Min	FC ポートがサポートできる最小保持時間 (マイクロ秒)。
HoldTime 最大	FC ポートがサポートできる最大保持時間 (マイクロ秒)。
CoS	FC ポートがサポートできる一連のサービス クラスを示すビット マスク。
ServiceStateCapable	このインターフェイスがサービス状態の変更を処理できるかどうかを示します。
PortRateMode Capable	このインターフェイスが専用または共有ポート レート モードとして構成できるかどうかを示します。
AdminRxBbCreditExtendedCapable	true の場合、インターフェイスの拡張バッファツープックアップクレジットを変更できます。ユーザーは、このインターフェイスでオブジェクト <code>fcIfAdminRxBbCreditExtended</code> を構成できます。
Class2Seq Deliv	FC-Port がクラス 2 シーケンシャル デリバリーをサポートできるかどうかを示すフラグ。
Class3Seq Deliv	FC-Port がクラス 3 シーケンシャル デリバリーをサポートできるかどうかを示すフラグ。

FC インターフェイス FICON ピア

フィールド	説明
TypeNumber	ピア ノードのタイプ番号。たとえば、タイプ番号は 002105 などになります。
SerialNumber	製造時にピア ノードに割り当てられたシーケンス番号です。たとえば、シリアル番号は 000000023053 などになります。
タグ	このポートに接続しているピア ノード内のポートの ID です。
FcId	NX-Port に割り当てられたアドレス識別子
ステータス	行のステータス (valid、invalid、old) を指定します。
名前	このポートの名前。

フィールド	説明
メーカー	ピアノードを製造した会社の名前。たとえば、製造元の情報は HTC などになります。
ModelNumber	ピアノードのモデル番号。たとえば、モデル番号は F20 などになります。
PlantOfMfg	ピアノードの製造工場を識別する工場コード。たとえば、製造工場コードは 00 などになります。
UnifType	このポートが通信しているピアノードのタイプ。
アラート	このインターフェイスで発生したリンク インシデントのタイプ。

インターフェイス NPorts (SVC)

フィールド	説明
Pwwn	仮想 N ポートの WWN (ワールドワイド名)。
FcId	仮想 N ポートのファイバチャネル ID。
ステータス	仮想 N ポートの動作状態。
DownReason	状態のインスタンスによって示されている N ポートの状態が「ダウン」である場合、この値は、この N ポートが「ダウン」である理由を示します。

インターフェイス セッション

フィールド	説明
NportPwwn	このセッションに属する N ポートの WWN。
PeerPwwn	このセッションのリモート N ポートの WWN。
PeerNwwn	このセッションのリモート N ポートの WWN。
PeerFcId	このセッションのリモートポートのファイバチャネル識別子。

IP 統計 TCP

フィールド	説明
AttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
InErrs	The total number of segments received in error (e.g., bad TCP checksums).
ActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

PassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
EstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
InSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	送信済みのセグメントの合計数。現在の接続上のセグメントなどを含むものの、再送信バイトだけを含むセグメントは除きます。
RetransSegs	再送信済みのセグメントの合計数。つまり、過去に1バイト以上送信したことがあるデータを含むTCPセグメントの数。
OutRsts	The number of TCP segments sent containing the RST flag.

ポートチャネルイーサネットインターフェイス

フィールド	説明
説明	ネットワークマネージャによって指定されたインターフェイスのエイリアス名。
MTU	インターフェイスで送受信できる最大フレームのサイズ（バイト数）。
PhysAddress	そのプロトコルでのインターフェイスのアドレス。
Admin	インターフェイスの適切な状態。
Oper	インターフェイスの現在の動作状態。
LastChange	インターフェイスが現在の動作状態にいつ移行したか。ローカルネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値はN/Aです。
IPAddress/Mask	インターフェイスのIPアドレスとマスク。
iSCSI AuthMethod	このインターフェイスの認証方法。
iSNS ProfileName	このインターフェイスのiSNSサーバープロファイル名。

ポートチャネルFCインターフェイス

フィールド	説明
PortVsan	インターフェイスが静的に割り当てられているVSAN。
[説明 (Description)]	ネットワークマネージャによって指定されたインターフェイスのエイリアス名。

フィールド	説明
管理モード	ユーザーが構成したポートモード。ユーザーがポートを auto(1) として構成した場合、ポートの初期化スキームによってポートのモードが決定されます。この場合、ユーザーは OperMode を調べて、ポートの現在の動作モードを判断できます。 auto(1) または ePort(4) のみが許可されます。
Oper Mode	ポートの現在の動作モード。
管理速度	ユーザーが構成したポート速度。
動作速度	インターフェイスの現在の帯域幅/秒。
Admin Status	インターフェイスの適切な状態。
動作ステータス	インターフェイスの現在の動作状態。
FailureCause	ポートの現在の動作状態の原因。
LastChange	インターフェイスが現在の動作状態に移行した時刻。プロキシエージェントの最後の再初期化に先立って現在の状態になった場合、この値は 0 または N/A です。

ポートチャネル全般

フィールド	説明
管理モード	ネットワーク管理者が希望するチャンネルモード。
動作モード (Oper Mode)	ポートの現在の動作チャンネルモード。
強制	<p>ポートチャネルポートにポートを追加する方法。</p> <ul style="list-style-type: none"> オフにすると、このポートチャネルに追加されるポートのパラメータに対して互換性チェックが実行されます。追加するポートには、ポートチャネルポートと同じ物理パラメータおよび構成パラメータが必要です。 オンにすると、物理パラメータのみで互換性チェックが実行されます。このポートチャネルポートに追加するポートには、同じ物理パラメータが必要です。操作は、物理パラメータが同じでない場合にのみ失敗します。追加されるポートの構成パラメータは、このポートチャネルポートの構成パラメータによって上書きされます。

フィールド	説明
MemberList By Interface	このポートチャネルポートのメンバーである E_port のリスト。
MemberList By FICON	このポートチャネルポートのメンバーである E_port のリスト。
MemberList LoadBalanced	PortChannel にアクティブに参加しているポート。
LastAction Status	ポートチャネルポートのメンバーリストを変更するために実行された最後の操作（メンバーの追加または削除）のステータス。ポートが追加されていないか、最後の操作が成功した場合、この値は成功になります。この値が失敗だった場合、ユーザーは LastAddStatusCause を調べて失敗の理由を見つけることができます。
LastAction FailureCause	ポートチャネルポートのメンバーリストを変更するために実行された最後の操作（メンバーの追加または削除）が失敗した原因。
LastAction Time	このエントリで最後にアクションが実行された時刻を示すタイムスタンプ。
CreationTime	このエントリの作成時刻のタイムスタンプ。
FICON Address	FICON のポートアドレス。空の場合、このチャネルは FICON によって使用されません。（この列は、FICON が有効な場合に表示されます。ポートチャネルが自動作成されたものである場合、この列はグレー表示されます）。

FlexAttach グローバル

フィールド	説明
VirtualPwwnauto	すべての F_port インターフェイスで仮想 WWN の自動生成を有効にします。VirtualPWWNauto の値が「true」に設定されている場合、VirtualWWN テーブルのすべてのエントリの VirtualWWN Auto の値は暗黙的に true に設定されます。

FlexAttach 仮想 PWWN

フィールド	説明
-------	----

仮想 pWWN	これは、このインターフェイスの仮想ポート WWN です。VirtualWwnAuto の値が「true」の場合、この仮想 pWWN の値はデバイスによって自動的に生成されます。この pWWN の値が明示的に設定した場合、VirtualWwnAuto の値は暗黙的に「false」に設定されます。pWWN の長さがゼロの場合、自動仮想 WWN 生成は無効になります。この pWWN は長さゼロに設定できません
自動	このインターフェイスでの仮想 WWN の自動生成を有効にします。VirtualWwnPwwn の値が明示的に設定されている場合、Auto の値は暗黙的に false に設定されます。また、この Auto が「true」に設定されている場合、VirtualWwnPwwn の値は自動生成された仮想ポート WWN で上書きされます。
LastChange	この仮想 WWN エントリが最後に変更されたときの sysUpTime の値。

FlexAttach 物理 WWN から仮想 WWN へ

フィールド	説明
virtual pWWN	これは、このデバイス ポート WWN の仮想ポート WWN です。WWN の衝突を最小限に抑えるために、この仮想 pWWN の 2 つのインスタンスに同じ値を持たせることはできません。 注: 対応するデバイスがログインしている場合、仮想 pWWN を変更することはできません。
LastChange	この仮想 WWN エントリが最後に変更されたときの sysUpTime の値。

FIPS

フィールド	説明
ModeActivation	<p>デバイスの FIPS モードをイネーブルまたはディセーブルにします。FIPS 140-2 は暗号モジュールに関する一連のセキュリティ要件であり、暗号モジュールに対する米国政府の要求条件を詳細に記述しています。モジュールは、ハードウェアとソフトウェアの両方で構成されます（たとえば、データセンターのスイッチングまたはルーティングモジュール）。</p> <p>FIPS モードをイネーブルにするための要求が受信され、その要求に応じて一連のセルフテストが正常に実行される場合、モジュールは FIPS 対応モードにあると言われます。セルフテストが失敗した場合は、適切なエラーが返されます。</p>

FCIP FICON Configuration

フィールド	説明
インターフェイス	このリンクに関連する FCIP デバイスのインターフェイスを識別する一意の値。
VSAN List Admin	Ficon テープ アクセラレーションが設定される VSAN（1 ～ 2047 の範囲）のリスト。存在する CISCO-FICON-MIB の cficonVsanEntry がある VSAN のみ、Ficon テープ アクセラレーション用に構成できます。
VSAN List Oper	Ficon テープ アクセラレーションの動作が「オン」になっている VSAN（1 ～ 2047 の範囲）のリスト。

ポート チャネルの自動作成

フィールド	説明
チャンネル	このポートチャネルのチャンネルグループモード。
永続	ポートチャネルが永続的である場合は true。

SPAN セッション

フィールド	説明
Dest Interface	SPAN 宛先ポート インターフェイス。

フィールド	説明
Filter VSAN List	このセッションに割り当てられる VSAN。
Status Admin	アクティブなセッションを一時停止にするか、非アクティブのセッションをアクティブにします。
Status Oper	セッションの現在の状態。
[説明 (Description)]	セッション ステータスの説明。
VSAN List	このセッションに割り当てられる VSAN。
Or Interface (Direction)	セッション用に設定される宛先ポート ID。
Inactive Reason	このセッションがアクティブになっていない理由の説明。

SPAN グローバル

フィールド	説明
MaxQueuedSpanPackets	このフィールドは、すべての SPAN セッションに対するドロップしきい値パケット数を指定します。[MaxQueuedSpanPackets] フィールドは、アクティブなセッションが存在しないときにのみ使用できます。

SPAN 送信元インターフェイス

フィールド	説明
[Interface]、[Direction]	セッション用に設定される宛先ポート ID、およびトラフィックの方向。

ポート トラッキングの依存関係

フィールド	説明
Linked, Destination Interfaces	追跡を行っているインターフェース。
VSAN Type	単一の VSAN とすべての VSAN のどちらを追跡しているか。
VSAN ID	単一の VSAN を追跡している場合、その VSAN の ID。

ポート トラック強制シャットダウン

フィールド	説明
インターフェイス	強制シャットダウン モードを構成するポートのインターフェイス。

フィールド	説明
強制シャットダウン	true の場合、ポートは管理上停止されるため、手動でポートを起動する必要があります。false の場合、ポートは運用上のみ停止するので、追跡対象のポートのいずれかが起動するとすぐに再び起動します。

ポートガード

フィールド	説明
インターフェイス	インターフェイスの名前
有効	インターフェイスがアップ状態とダウン状態の間で変化しないようにするか、状態を継続的に変化するのを許可するかを指定します。
Duration (sec)	ポートが状態を変更できる期間を指定します。
Number of Flaps	Duration で指定された時間内にポートがフラップできる回数を指定します。
Oper	インターフェイスの動作状態。

帯域幅予約：48-ポート 96-Gbps ファイバチャネル モジュール

RateMode 構成マクロ	[説明 (Description)]
各グループの最初のポートは 4 Gbps 専用ポートで、残りのポートは 8 Gbps を共有	各グループの最初のポートに 4 Gbps のレートモードと管理速度を割り当て、残りのポートは、ポートの動作速度に応じて 8 Gbps を共有
各グループの最初のポートは 8 Gbps 専用ポートで、残りのポートは 8 Gbps を共有	各グループの最初のポートに 8 Gbps のレートモードと管理速度を割り当て、残りのポートは、ポートの動作速度に応じて 8 Gbps を共有
すべてのポートで 8 Gbps を共有（初期設定およびデフォルト設定）	使用可能なすべてのポートに 8 Gbps のレートモードと管理速度を割り当てます。これがデフォルト設定です。

帯域幅予約：48 ポート 48 Gbps ファイバチャネル モジュール

RateMode 構成マクロ	[説明 (Description)]
各グループの最初のポートは 2 Gbps 専用ポートで、残りのポートは 4 Gbps を共有	各グループの最初のポートに 2 Gbps のレートモードと管理速度を割り当て、残りのポートはポートの動作速度に応じて 4 Gbps を共有
各グループの最初のポートは 8 Gbps 専用ポートで、残りのポートは 4 Gbps を共有	各グループの最初のポートに 8 Gbps のレートモードと管理速度を割り当て、残りのポートはポートの動作速度に応じて 4 Gbps を共有

RateMode 構成マクロ	[説明 (Description)]
すべてのポートで最大4Gbpsを自動共有 (初期設定およびデフォルト設定)	使用可能なすべてのポートに最大レートモードと4Gbpsの管理速度を割り当てます。これがデフォルト設定です。

帯域幅予約 : 24 ポート 48 Gbps ファイバチャネル モジュール

RateMode 構成マクロ	[説明 (Description)]
各グループの最初のポートは8 Gbps 専用ポートで、残りのポートは8 Gbps を共有	各グループの最初のポートにレートモードと8Gbpsの管理速度を割り当て、残りのポートはポートの動作速度に応じて8 Gbps を共有します
すべてのポートで自動を共有 (初期設定およびデフォルト設定)	使用可能なすべてのポートに8 Gbps のレートモードと管理速度を割り当てます。これがデフォルト設定です。

帯域幅予約 : 48 ポート 256 Gbps ファイバー チャネル モジュール

RateMode 構成マクロ	[説明 (Description)]
6 ポートの各ポートグループのうち、最初の4つのポートは8 Gbps 専用ポートで、残りのポートは8 Gbps を共有	各6ポートポートグループの最初の4ポートに8 Gbps のレートモードと管理速度を割り当て、残りのポートはポートの動作速度に応じて8 Gbps を共有します。
各グループの最初のポートは8Gbps専用ポートで、残りのポートは8 Gbps を共有	各グループの最初のポートに8 Gbps のレートモードと管理速度を割り当て、残りのポートはポートの動作速度に応じて8 Gbps を共有します。
Shared 8G On all ports	使用可能なすべてのポートに8 Gbps のレートモードと管理速度を割り当てます。これがデフォルト設定です。
Dedicated 4G On all ports	使用可能なすべてのポートに4Gbpsのレートモードと管理速度を割り当てます。
次のポートの専用 10G : <ul style="list-style-type: none"> • 4、5、6、7、8、10 (ポート 1、2、3、9、11、12 は無効) • 16、17、18、19、20、22 (ポート 13、14、15、21、23、24 は無効) • 28、29、30、31、32、34 (ポート 25、26、27、33、35、36 は無効) • 40、41、42、43、44、46 (ポート 37、38、39、45、47、48 は無効) 	次のポートに10Gbpsのレートモードと管理速度を割り当てます。

帯域幅予約：32ポート 256 Gbps ファイバチャネル モジュール

RateMode 構成マクロ	[説明 (Description)]
すべてのポートで専用の 8 Gbps	すべての使用可能なポートに、レートモードと 8 Gbps の管理速度を割り当てます。
すべてのポートで 8 Gbps を共有（初期設定およびデフォルト設定）	すべての使用可能なポートに、レートモードと共有の 8 Gbps の管理速度を割り当てます。
以下のポートには専用の 10 G があります。 <ul style="list-style-type: none"> • 2、3、4、5、6、8（ポート1および7は無効） • 10、11、12、13、14、16（ポート9および15は無効） • 18、19、20、21、22、24（ポート17および23は無効） • 26、27、28、29、30、32（ポート25および31は無効） 	指定されたポートに 10Gbps のレートモードと管理速度を割り当てます。

DS-X9448-768K9 (Luke) ラインカード帯域幅の予約

RateMode 構成マクロ	[説明 (Description)]
次のポートの専用 10G : <ul style="list-style-type: none"> • ポート 1 ~ 8 • ポート 9 ~ 16 • ポート 17 ~ 24 • ポート 25-32 • ポート 33 ~ 40 • ポート 41 ~ 48 	指定されたポートに 10 Gbps の専用レートモードと管理速度を割り当てます。
次のポートで 10G を構成解除します。 <ul style="list-style-type: none"> • ポート 1 ~ 8 • ポート 9 ~ 16 • ポート 17 ~ 24 • ポート 25-32 • ポート 33 ~ 40 • ポート 41 ~ 48 	指定されたポートでデフォルトのレートモードと管理速度に戻します。トランシーバの周波数は FC に設定されています。この操作は中断を伴います。

FC

このセクションの内容は次のとおりです。

VSAN 全般

フィールド	説明
名前	VSANの名前。デフォルト値は文字列 VSANxxxx であり、xxxx は vsanIndex の値を4桁で表したものであることに注意してください。たとえば、vsanIndex が23の場合、デフォルト値は VSAN0023 です。
MTU	VSAN の MTU。通常、これは 2112 です。
LoadBalancing	VSAN で使用されるロードバランシングの種類です。 <ul style="list-style-type: none"> • srcdst : パス選択に送信元 ID と接続先 ID を使用 • srcdst 0xld : 送信元、接続先、交換 ID を使用
相互運用性	この VSAN のローカルスイッチの相互運用モード。 <ul style="list-style-type: none"> • 標準 • 相互運用性 - 1 • 相互運用性 - 2 • 相互運用性 - 3
AdminState	この VSAN の状態。
OperState	VSAN の動作状態。
InOrderDelivery	デバイスの InOrderDelivery 保証フラグ。true の場合、順序どおりの配信が保証されます。false の場合、保証されません。
DomainID	永続的なドメイン ID を指定します。
FICON	VSAN が FICON 対応の場合は true。
ネットワーク遅延	この VSAN でのこのスイッチのネットワーク遅延。これは、送信された順序で配信されない場合にフレームがドロップされるまでの時間です。

VSAN Membership

フィールド	説明
スイッチ	スイッチの名前
ポート	VSAN の FC ポート

フィールド	説明
チャンネル	VSAN のポートチャンネル
FCIP	VSAN の FCIP インターフェイス
iSCSI	VSAN の iSCSI インターフェイス
FICON	FICON による VSAN のインターフェイス
FC 仮想インターフェイス	VSAN の仮想 FC インターフェイス

VSAN Interop-4 WWN

フィールド	説明
VSAN ID	McData スイッチを含む VSAN の ID。
WWN	McData スイッチの WWN。

VSAN タイマー

フィールド	説明
VSAN Id	VSAN の ID。
R_A_TOV	Recovery_Qualifier などの NxPort リソースをいつ再利用するかを決定するためのタイムアウト値として FxPort に使用される Resource_Allocation_Timeout 値。これは、E_D_TOV に、フレームがファブリック内で遅延しても配信される可能性のある最大時間の 2 倍を加えたものを表します。ファブリック内のすべてのスイッチは、このタイムアウトを同じ値で構成する必要があることに注意してください。
D_S_TOV	分散サービス リクエストが応答を待機する時間を示す Distributed_Services_Timeout 値。
E_D_TOV	エラー状態を検出するためのタイムアウト値として FxPorts で使用される Error_Detect_Timeout Value です。ファブリック内のすべてのスイッチは、このタイムアウトを同じ値で構成する必要があることに注意してください。値は D_S_TOV の値より小さくならないことに注意してください。
NetworkDropLatency	この VSAN でのこのスイッチのネットワーク遅延。

VSAN デフォルト ゾーン ポリシー

フィールド	説明
Zone Behavior	VSAN の作成時のデフォルト ゾーン動作の初期値を表します。VSAN が削除され、再度作成された場合、デフォルトのゾーン動作は、このオブジェクトに指定された値に設定されます。
[伝播モード (Propagation Mode)]	VSAN の作成時のゾーンセット伝播モードの初期値を表します。VSAN が削除され、再作成された場合、ゾーンセット伝播モードは、このオブジェクトに指定された値に設定されます。

IVR ローカル トポロジ

フィールド	説明
VSAN List	このデバイスの IVR トポロジの一部である構成済み VSAN のリスト。

IVR ファブリック ID

フィールド	説明
VSAN List	このデバイスの IVR トポロジの一部である構成済み VSAN のリスト。

IVR デフォルト ファブリック ID

フィールド	説明
Fabric Id	このスイッチの構成済みのデフォルト自律ファブリック ID。

IVR のアクション

フィールド	説明
Activate Local Topology	このオブジェクトをアクティブに設定すると、構成された IVR トポロジがこのデバイスでアクティブになるように要求されます。つまり、IVR トポロジの現在の構成が複製され、その複製がアクティブな IVR トポロジになります。

フィールド	説明
アクティブ	このオブジェクトは、IVR トポロジがアクティブかどうかを示します。true の場合、IVR トポロジはアクティブです。false の場合、IVR トポロジはアクティブではありません。
アクティベーション時間	IVR トポロジが最後にアクティブ化された日時。IVR トポロジがローカル ネットワーク管理サブシステムの前回の初期化以前に現在の状態に移行した場合、この値は N/A です。
IVR NAT を有効にします	VSAN 境界を越えた FCID および VSAN 識別子の変換を有効にします。true の場合、フレームが VSAN 境界を越えると、VSAN 識別子とエンドデバイスの FCID 全体が変更されます。
自動検出トポロジ	自動 VSAN トポロジディスカバリを有効にします。true の場合、自動 VSAN トポロジディスカバリがオンになります。IVR プロセスは相互に通信して、すべての IVR 対応スイッチに物理トポロジのグローバルビューを提供します。false の場合、自動 VSAN トポロジディスカバリ検出はオフになります。

IVR RDI VSAN

フィールド	説明
Add Virtual Domain to FC Domain List	このオブジェクトは、VSAN 内の仮想ドメインがその VSAN のドメイン リストに追加されている VSAN を一覧表示します。

IVR アクティブトポロジ

フィールド	説明
VSAN List	このデバイスの IVR トポロジの一部である VSAN のリスト。

IVR Zoneset ステータス

フィールド	説明
ステータス	この VSAN 上のアクティブな IV ゾーンセットのステータス。

- idle - アイドル
- active - アクティブ
- deactive - 非アクティブ
- defaultZoneDeny - デフォルトのゾーン動作が拒否であり、通常のアクティブゾーンセットがないため、アクティブ化に失敗。
- activationFailed - アクティブ化に失敗。
- deactivationFailed - 非アクティブ化に失敗。
- activationNotInitiated - アクティブ化が開始していない。
- activationFailedFabricChgFailed - ファブリックの変更に失敗したため、アクティブ化が失敗。
- deactivationNotInitiated - 非アクティブ化が開始していない。
- deactivationFailedFabChgFailed - ファブリックの変更に失敗したため、非アクティブ化に失敗。
- deactivationNotInitiated - 非アクティブ化が開始していない。
- deactivationFailedFabChgFailed - ファブリックが変更されたため、非アクティブ化に失敗。
- activating - アクティブ化が進行中。
- activatingWaitForLowestSwrn - アクティブ化が進行中。最小のスイッチ WWN のスイッチが IV ゾーンセットを通常のアクティブゾーンセットに追加するのを待機中。
- activatingFabricChanging - アクティブ化が進行中。ファブリックを変更中。
- deactivating - 非アクティブ化が進行中。
- deactivatingWaitForLowestSwrn - 非アクティブ化が進行中。最小のスイッチ WWN のスイッチが、IVR ゾーンセットを通常のアクティブゾーンセットから削除するのを待機中。
- deactivatingFabricChanging - 非アクティブ化が進行中。ファブリックを変更中。
- defaultZonePermit - デフォルトのゾーン動作が許可であるため、アクティブ化に失敗。
- defaultZonePermitNoForce - デフォルトのゾーンの動作が強制オプションなしの許可であるため、アクティブ化に失敗。
- defaultZonePermitActZsNoForce - デフォルトのゾーン動作が許可であり、通常のアクティブ化ゾーンセットがあり、強制オプションがないため、アクティブ化が失敗。
- denyNoActiveZoneset - アクティブなゾーンセットがないため、アクティブ化に失敗。
- activationFailedLowestWwnWait - 最小の WWN のスイッチがこのゾーンセットをアクティブ化するのを待機していて、アクティブ化に失敗。
- deactivationFailedLowestWwnWait - 最小の WWN のスイッチがこのゾーンセットを非アクティブ化するのを待機していて、非アクティブ化に失敗。
- activationFailedZoneNmCtnsIIChar - アクティブ化されているゾーンセット内のゾーン名の 1 つに不正な文字が含まれているため、アクティブ化に失敗。

IVR の不一致

フィールド	説明
不一致	強制された（アクティブな）IVゾーンセットのチェックサム。
RegionID	CFS 構成がサポートされているリージョンを識別します。

IVR ドメイン

フィールド	説明
ドメイン ID	VSAN を表すために使用される FC ドメイン ID。

IVR FCID

フィールド	説明
FCID	デバイスを表すために IVR が使用する FCID。

IVR Zoneset アクティブ ゾーン

フィールド	説明
VSAN Id	IVR VSAN ID。
ゾーン	アクティブな IVR ゾーン名。
Fabric Id	自律ファブリック ID。
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチ インターフェイス。
名前	ゾーンのメンバー名。
WWN	ゾーン メンバー WWN。
FcId	ゾーン メンバーの FC ID。
LUN	ゾーン メンバーの LUN。

フィールド	説明
ステータス	<ul style="list-style-type: none"> • ファブリック内不在：ゾーンメンバーがファブリック内に存在しない場合。 • VSAN内不在：ゾーンメンバーがVSAN内に存在しない場合。 • 該当なし：ステータスを判断できません。 <p>空：メンバーはファブリックと正しいVSANに存在しており、ゾーンの他のメンバーと通信できます。</p>

IVR ゾーンセット アクティブ ゾーン属性

フィールド	説明
ゾーン	アクティブな IVR ゾーン名。
QoS	QoS イネーブルの場合は true、そうでない場合は false です。
QoSの優先順位	QoS 優先度の値（低、中、または高）。
ブロードキャスト	この VSAN のこのデフォルトゾーンでブロードキャスト ゾーニングを有効にするかどうかを指定します。true の場合、有効になります。false の場合、無効になります。

IVR ゾーンセット名

フィールド	説明
VSAN Id	IVR VSAN ID。
ゾーン	アクティブな IVR ゾーン名。
Fabric Id	自律ファブリック ID。
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチ インターフェイス。
名前	ゾーンのメンバー名。
WWN	ゾーン メンバー WWN。
FcId	ゾーン メンバーの FC ID。
Luns	ゾーン メンバーの LUN。

フィールド	説明
ステータス	<ul style="list-style-type: none"> ファブリック内不在：ゾーンメンバーがファブリック内に存在しない場合。 VSAN内不在：ゾーンメンバーがVSAN内に存在しない場合。 該当なし：ステータスを判断できません。 <p>空：メンバーはファブリックと正しいVSANに存在しており、ゾーンの他のメンバーと通信できます。</p>

DPVM アクション

フィールド	説明
操作	一連のバインディングをアクティブ化するのに役立ちます。
結果	アクティブ化の結果を示します。
ステータス	アクティブ化の状態を示します。trueの場合は、最新の操作として、アクティブ化が試みられています。falseの場合は、最新の操作として、アクティブ化が試みられていません。
CopyActive to Config	copy(1)に設定すると、アクティブな（強制された）バインディングデータベースが構成バインディングデータベースにコピーされます。学習済みエントリもコピーされます。
Auto Learn Enable	すべてのポートでローカルデバイスにログインしているデバイスの構成と、それらが関連付けられているVSANを学習するのに役立ちます。
Auto Learn Clear	自動学習エントリのクリアを支援します。
Clear WWN	対応する自動学習エントリをクリアするために使用されるポートWWN (pWWN) を表します。

DPVM 構成データベース

フィールド	説明
スイッチ	スイッチ名。
タイプ	デバイスの対応するインスタンスのタイプを指定します。
WWN または Name または MAC	ログインデバイスアドレスを表します。値は、対応するデバイスタイプ (PWWN、NWWN、またはMAC) によって異なります。
VSAN Id	cdpvmLoginDev で表されるデバイスがログインするローカルデバイスのポートに関連付けられるVSANを表します。
スイッチ インターフェイス	デバイス エイリアスを表します。

DPVM アクティブ データベース

フィールド	説明
タイプ	cdpvmEnfLoginDev の対応するインスタンスのタイプを指定します。
WWN または Name または MAC	ログイン デバイス アドレスを表します。値は、対応するデバイス タイプ (PWWN、NWWN、または MAC) によって異なります。
VSAN Id	cdpvmEnfLoginDev で表されるデバイスがログインするローカル デバイス上のポートの VSAN を表します。
インターフェイス	デバイス エイリアスを表します。
IsLearnt	これが学習済みエントリかどうかを示します。true の場合、学習済みエントリです。false の場合、そうではありません。

ドメイン マネージャを実行

フィールド	説明
都道府県 (State)	この VSAN のローカルスイッチのドメインマネージャの状態。
DomainID	この VSAN のローカルスイッチのドメイン ID、またはドメイン ID が割り当てられていない場合は 0。
Local Switch WWN	この VSAN のローカルスイッチの WWN。
ローカル優先度	この VSAN のローカルスイッチの実行優先度。
プリンシパルスイッチ WWN	この VSAN のプリンシパルスイッチの WWN。プリンシパルスイッチの ID が不明な場合は空の文字列。
Principal Priority	この VSAN のプリンシパルスイッチの実行優先度。

Domain Manager の設定

フィールド	説明
[有効 (Enable)]	この VSAN でドメイン マネージャを有効にします。アクティブな VSAN で有効になっている場合、スイッチはプリンシパルスイッチの選択に参加します。無効にすると、スイッチはプリンシパルスイッチの選択にもドメイン割り当てにも参加しません。したがって、ドメイン ID は静的に構成する必要があります。

フィールド	説明
Running DomainId	<p>この VSAN のローカルスイッチの構成済みドメイン ID。ドメイン ID が構成されていない場合は 0 です。意味は DomainIdType に依存します。</p> <p>タイプが「preferred」の場合、構成されたドメイン ID は「優先ドメイン ID」と呼ばれます。有効な値は 0 ~ 239 です。このドメインを割り当てることができない状況では、任意のドメイン ID が受け入れられます。値「0」は、任意のドメイン ID を意味します。</p> <p>タイプが「static」（強く要求）の場合、ドメイン ID は「静的ドメイン ID」と呼ばれます。有効な値は 1 ~ 239 です。このドメインが 0 ではないものの、割り当てられない状況では、他のドメイン ID は受け入れられません。</p> <p>ドメインマネージャが VSAN で有効になっている場合、このドメイン ID を要求する RDI（リクエストドメイン ID）が送信されます。「優先」の場合にドメイン ID を付与できない場合、または構成された「静的」（強く要求する）ドメイン ID を付与できない場合は、エラー状態です。このエラーが発生すると、その VSAN の E_ports は分離されます。</p> <p>ドメインマネージャが有効になっていない場合でも、静的（強く要求する）ドメイン ID が（有効な数値に）構成されていれば、その ID が付与されると見なされます。この VSAN でいずれかのドメイン ID がゼロ以外の値で構成されておらず、ドメインマネージャが有効になっていない場合、スイッチはこの VSAN 上のすべての E_port を分離します。</p>
DomainId Type	構成されたドメイン ID のタイプ。
FabricName	この VSAN へのファブリックログインに使用される WWN。これは、[Enable] が false の場合にのみ使用されます。[Enable] が true の場合、プリンシパルスイッチの WWN が使用されます。長さゼロの値に設定すると、自動的にデフォルト値に設定されます。
プライオリティ	プリンシパルスイッチの選択プロセスで使用されるスイッチの優先度。
Contiguous Allocation	プリンシパルスイッチとして選択されたときのスイッチの動作を決定します。true の場合、スイッチは、RDI 内の連続していないドメイン ID を受け入れません。連続したドメイン ID の RDI を満たすことができない場合、リスト内のすべてのドメイン ID を連続したドメイン ID に置き換えようとしません。false の場合、スイッチはドメイン ID が連続していなくても、通常どおりにドメイン ID を付与します。
Auto Reconfigure	特定のエラー状態に対するスイッチの応答方法を決定します。これらのエラーの原因となる可能性があるのは、2 つの不整合なファブリックがマージされて、ドメイン ID リストがオーバーラップしていることです。true の場合、スイッチは RCF（ReConfigureFabric）を送信してファブリックを再構築します。false の場合、スイッチはエラーが発生した E_ports を分離します。

フィールド	説明
Persistent FcId	true の場合、この VSAN に割り当てられたすべての FC ID は、この VSAN で永続的になります。false の場合、PersistenceTable の VSAN 上のすべてのエントリが削除されます。
Purge FcIds?	FC ID 永続性データベース内のこの VSAN の FC ID を消去するようドメイン マネージャに指示します。
Restart?	ドメイン マネージャにドメイン ID ツリーを最初から再構築するように指示します。「disruptive」の場合、ファブリックをエラーから回復させるために、RCF (ReConfigure Fabric) が VSAN で生成されます。 「nonDisruptive」の場合、BF (Build Fabric) が VSAN で生成されます。
最適化	フィールドをクリックして、次のいずれかを選択する必要があります。ターボ モードを無効にするには、何も選択しないでください。 <ul style="list-style-type: none"> • Fast-Restart - 最適化タイプを高速再起動に設定します。 • Selective-Restart- 最適化タイプを選択的再起動に設定します。

ドメイン マネージャ ドメイン

フィールド	説明
SwitchWWN	特定の VSAN に DomainId の対応する値が現在割り当てられているスイッチの WWN。

ドメイン マネージャの統計

フィールド	説明
Prin. Sel Total	この VSAN で選択したプリンシパルスイッチの合計。
Prin. Sel ローカル	ローカルスイッチがこの VSAN のプリンシパルスイッチになった回数。
Fabric Builds (BF)	この VSAN で発生した BuildFabric (BF) の回数。
Fabric Reconfigures (Rcf)	この VSAN で発生した ReconfigureFabric (RCF) の回数。
FcIds Free	この VSAN で割り当てられていない FC ID の数。
FcIds Assigned	この VSAN に割り当てられている FC ID の数。
FcIds Reserved	この VSAN で予約されている FC ID の数。

ドメインマネージャインターフェイス

フィールド	説明
[役割 (Role)]	次のいずれかが必要です。 <ul style="list-style-type: none"> • nonPrincipal - 非プリンシパル インターフェイス • principalUpstream - アップストリーム プリンシパル インターフェイス • principalDownstream - ダウンストリーム プリンシパル インターフェイス • isolated - 隔離されたインターフェイス • down - ダウン インターフェイスが不明 • unknown - 不明のインターフェイス
RcfReject	この VSAN とインターフェイスで着信する ReConfigure Fabric (RCF) メッセージを受け入れるかどうかを決定します。true の場合、着信 RCF は拒否されます。false の場合、着信 RCF は受け入れられます。これは、このインターフェイスによって生成された発信 RCF には適用されないことに注意してください。

ドメイン マネージャ永続 FcId

フィールド	説明
FcId	この VSAN でこの WWN に割り当てられた FC ID。PersistenceNum の値が area の場合、3 番目のオクテットは 0x00 である必要があります。
マスク	この VSAN 上のこの WWN に静的または動的に割り当てられる、PersistenceFcId から始まる FC ID の数。値 1 は、1 つの FC ID のみが割り当てられることを意味します。値 area は、FcId の 2 番目のオクテットで指定されたエリア内のすべての FC ID が割り当てられることを意味します。通常、1 つのエリアに 256 個の FC ID が割り当てられます。[使用済み (Used)] の値が true の場合、この値は変更できません。
使用済み	この FC ID が使用されているかどうかを示します。
割り当て	この FC ID の永続性のタイプ。

ドメイン マネージャ 許可 DomainId

フィールド	説明
リスト	許可されているドメインのリストを提供します。対応するビットの値が1の場合、ドメインはこの VSAN で許可されています。長さが32 バイト未満の値の場合、表されていないドメインはリストに含まれているとは見なされません。このオブジェクトが長さゼロの文字列である場合、この VSAN ではドメインは許可されません。

ゾーンセットのアクティブ ゾーン

フィールド	説明
ゾーン	ゾーン名を指定します。
タイプ	ゾーン メンバー タイプ。
スイッチ インターフェイス	ゾーン メンバーが接続されているスイッチ インターフェイス。
名前	ゾーンのメンバー名。
WWN	ゾーン メンバー WWN。
FcId	ゾーン メンバーの FC ID。
LUN	ゾーン メンバーの LUN。
ステータス	<ul style="list-style-type: none"> ファブリック内がない：ゾーン メンバーがファブリック内に存在しない場合。 VSAN 内がない：ゾーン メンバーが VSAN 内に存在しない場合。 該当なし：ステータスを判断できません。 空：メンバーはファブリックと正しい VSAN に存在しており、ゾーンの他のメンバーと通信できます。

Zoneset ゾーンなし

フィールド	説明
名前	ゾーンのメンバー名。
WWN	ゾーン メンバー WWN。
FcId	ゾーン メンバーの FC ID。

Zoneset Status

フィールド	説明
ステータス	最新のアクティベーション/非アクティベーションの結果を示します。
アクティベーション時間	このエントリが最後にアクティブ化された時刻。ローカルネットワーク管理システムの前回の再初期化以前にこのエントリがアクティブ化されていた場合、この値は N/A です。
FailureCause	ゾーンセットのアクティブ化/非アクティブ化の失敗の理由。
FailedSwitch	Change Protocol の失敗の原因となったファブリック内のデバイスのドメイン ID。
Active == Local?	強制されたデータベースがこの VSAN のローカルデータベースと同じかどうかを示します。true の場合、それらは同じです。false の場合、それらは同じではありません。
Active Zoneset	強制された IV ゾーンセットの名前。
Hard Zoning	この VSAN でハードゾーニングが有効になっているかどうかを示します。ハードゾーニングは、ハードウェアでゾーニングを強制するメカニズムです。true の場合、この VSAN ではハードゾーニングが有効です。false の場合、この VSAN ではハードゾーニングが有効ではありません。

Zoneset ポリシー

フィールド	説明
Default Zone Behavior	この VSAN のデフォルトゾーンの動作を制御します。許可に設定されている場合、この VSAN のデフォルトゾーンのメンバーは相互に通信できます。拒否に設定されている場合、この VSAN のデフォルトゾーンのメンバーは相互に通信できません。
Default Zone ReadOnly	この VSAN で、SCSI ターゲットであるデフォルトゾーンのメンバーで SCSI 読み取り操作が許可されるかどうかを示します。true の場合、SCSI 読み取り操作のみが許可されます。したがって、このデフォルトゾーンは、この VSAN の読み取り専用のデフォルトゾーンになります。false の場合、SCSI の読み取り操作と書き込み操作の両方が許可されます。
Default Zone QoS	この VSAN のデフォルトゾーンの QoS 属性を有効にするかどうかを指定します。true の場合、この VSAN のデフォルトゾーンの QoS 属性が有効になります。false の場合、この VSAN のデフォルトゾーンの QoS 属性は無効になります。
Default Zone QoS Priority	QoS 優先順位を指定します。

フィールド	説明
Default Zone Broadcast	この VSAN のこのデフォルトゾーンでブロードキャストゾーンニングを有効にするかどうかを指定します。true の場合、有効になります。false の場合、無効になります。
伝播	この VSAN でのマージ/変更プロトコル中にゾーンセット情報が伝達される方法を制御します
Read From	管理ステーションが有効なデータベースから読み取るか、コピー データベースから読み取るかを指定します。

Zoneset のアクティブゾーン属性

フィールド	説明
名前	ゾーン名を指定します。
読み取り専用	この VSAN の SCSI ターゲットであるデフォルトゾーンのメンバーに、SCSI 読み取り操作のみが許可されるかどうかを示します。true の場合、SCSI 読み取り操作のみが許可されます。したがって、このデフォルトゾーンは、この VSAN の読み取り専用のデフォルトゾーンになります。false の場合、SCSI の読み取り操作と書き込み操作の両方が許可されます。
QoS	この VSAN のデフォルトゾーンの QoS 属性を有効にするかどうかを指定します。true の場合、この VSAN のデフォルトゾーンの QoS 属性が有効になります。false の場合、この VSAN のデフォルトゾーンの QoS 属性は無効になります。
QoS の優先順位	QoS 優先度の値（低、中、または高）を指定します。
ブロードキャスト	この VSAN のこのデフォルトゾーンでブロードキャストゾーンニングを有効にするかどうかを指定します。true の場合、有効になります。false の場合、無効になります。

ゾーンセットを拡張

フィールド	説明
操作	basic(1) に設定すると、ゾーンサーバーは FC-GS4 標準規格で定義されている基本モードで動作します。Enhanced(2) に設定すると、ゾーンサーバーは FC-GS4 標準規格で定義されている拡張モードで動作します。
結果	この VSAN 上のローカルゾーンサーバーの動作モードを設定した結果。
Config DB Locked By	このセッションの所有者を指定します。
Config DB Discard Changes	このセッションでのコピー データベースの内容のコミットまたはクリアを行えるよう支援します。

フィールド	説明
Config DB Result	czseSessionCntl の対応するインスタンスを commitChanges(1) に設定した結果を示します。
Enforce Full DB Merge	ゾーンのマージ動作を制御します。このオブジェクトが許可に設定されている場合、マージはマージルールに従って行われます。制限に設定されている場合、マージデータベースが完全に同一でない場合、デバイス間のスイッチ間リンク (ISL) は隔離されます。
Read From	管理ステーションが有効なデータベースから読み取るか、コピーデータベースから読み取るかを指定します。

Zoneset 読み取り専用違反

フィールド	説明
違反	ローカルゾーンサーバーによって送信された、データ保護されたチェック条件エラーレスポンスの数。

Zoneset 統計

フィールド	説明
Merge Req Tx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーに送信したマージ要求フレームの数。
Merge Req Rx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーから受信したマージ要求フレームの数。
Merge Acc Tx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーに送信したマージ受け入れフレームの数。
Merge Acc Rx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーから受信したマージ受け入れフレームの数。
Change Req Tx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーに送信した変更要求の数。
Change Req Rx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーから受信した変更要求の数。
Change Acc Tx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーに送信した変更応答の数。
Change Acc Rx	このゾーンサーバーがこの VSAN のファブリック内の他のゾーンサーバーから受信した変更応答の数。
GS3 Rej Tx	この VSAN のこのゾーンサーバーが拒否された GS3 要求の数。
GS3 Req Rx	この VSAN のこのゾーンサーバーが受信した GS3 要求の数。

Zoneset LUN ゾーニング統計

フィールド	説明
INQUIRY	ローカルゾーンサーバーが受信した SCSI INQUIRY コマンドの数。
REPORT LUN	ローカルゾーンサーバーが受信した SCSI Report LUN コマンドの数。通常、Report LUN コマンドは LUN 0 に対してのみ送信されます。
検知	ローカルゾーンサーバーが受信した SCSI SENSE コマンドの数。
Other Cmds	ローカルゾーンサーバーが受信した SCSI Read、Write、Seek などのコマンドの数。
BadInquiry Errors	ローカルゾーンサーバーによって送信された No LU エラー応答の数。
Illegal Errors	ローカルゾーンサーバーによって送信された Illegal Request Check Condition 応答の数。

Zoneset メンバー

フィールド	説明
ゾーン	デフォルトゾーン。
タイプ	FCID。
スイッチインターフェイス	ゾーンメンバーが接続されているスイッチインターフェイス。
名前	ゾーンのメンバー名。
WWN	ゾーンメンバー WWN。
FcId	ゾーンメンバーの FC ID。
Luns	ゾーンメンバーの LUN。
ステータス	<ul style="list-style-type: none"> ファブリック内にはない：ゾーンメンバーがファブリック内に存在しない場合。 VSAN内にはない：ゾーンメンバーが VSAN 内に存在しない場合。 該当なし：ステータスを判断できません。 <p>空：メンバーはファブリックと正しい VSAN に存在しており、ゾーンの他のメンバーと通信できます。</p>

ファブリック構成サーバーの検出

フィールド	説明
ステータス	ローカルスイッチの検出のステータス。最初にスイッチが起動したときには、これはすべての VSAN で <code>databaseInvalid</code> 状態に設定されます。これは、検出を行う必要があることを示しています。検出中、この VSAN の状態は <code>inProgress</code> に設定されます。この VSAN で検出が完了すると、これは <code>completed</code> に設定されます。指定された VSAN のリストの検出が完了すると、データは一定期間キャッシュされます。 この期間が経過すると、データは消失し、指定された VSAN のリストのデータベースは <code>databaseInvalid</code> に設定されます。
CompleteTime	この VSAN で直前の検出が完了した時刻。この値は、この VSAN での最初の検出が行われる前は N/A です。

ファブリック構成サーバー インターコネクト要素

フィールド	説明
タイプ	このインターコネクト要素のタイプ。
DomainID	このインターコネクト要素のドメイン ID。ドメイン ID が構成されていない場合、この値は 0 です。
MgmtId	このインターコネクト要素の管理識別子。インターコネクト要素がスイッチの場合、これはスイッチのドメインコントローラ識別子になります。
FabricName	このインターコネクト要素のファブリック名。
LogicalName	このインターコネクト要素の論理名。
ベンダー、モデル、リリース、WWN	このインターコネクト要素に対応する情報リスト。
MgmtAddrList	このインターコネクト要素に対応する管理アドレスリスト。

Fabric Config Server プラットフォーム (エンクロージャ)

フィールド	説明
名前	このプラットフォームの名前。

フィールド	説明
タイプ	このプラットフォームのタイプ。
ConfigSource	このエントリの構成のソース。GS3 経由で構成されたエントリは、SNMP 経由では削除できないことに注意してください。
NodeList	このプラットフォームに対応するノード名リスト。
MgmtAddrList	本プラットフォームに対応する管理アドレス一覧。

ファブリック構成サーバー ファブリック ポート

フィールド	説明
タイプ	このポートのタイプ。
TxType	このポートの TX タイプ。
ModuleType	このポートのモジュール タイプ。
インターフェイス	このポート エントリに対応する物理番号。
ステータス	このポートの状態。
AttachedPortList	このポートに対応する、アタッチされたポート名のリスト。

FC ルート

フィールド	説明
プリファレンス	同じ接続先への複数のルートが異なるプロトコル、ピア、または静的ルートから学習される場合に、あるルートを別のルートよりも優先して選択するために使用される値。プリファレンス値は、単一のルーティングデータベース (RIB) 内の同じ接続先へのルートの順序を決定するために使用される、任意に割り当てられた値です。最もプリファレンス値が小さなルートを、アクティブなルートとして選択します。
LastChangeTime	FCルートテーブルで行が最後に作成、変更、または削除された時刻。
DomainID	ネクスト ホップ スイッチのドメイン ID。ただし、読み取り時に、fcRouteProto の値がローカルだった場合、この値は N/A になる可能性があります。

フィールド	説明
メトリック	このルートのルーティングメトリック。使用方法は、使用する fcRouteProto に依存します。
タイプ	ルートのタイプ。 <ul style="list-style-type: none"> ローカル(1)：次のホップが最終目的地であるルートを指します。 リモート(2)：次のホップが最終目的地でないルートを指します。これは、マルチキャストおよびブロードキャストルートエントリには関係ありません。

FDMI HBAs

フィールド	説明
Sn	HBA のシリアル番号。
モデル	この HBA のモデル。
ModelDescr	モデルの説明
OSInfo	この HBA を制御するオペレーティングシステムのタイプとバージョン。
MaxCTPayload	この HBA を含むホストに常駐するアプリケーションソフトウェアによって送受信される可能性のある、すべての CT ヘッダーを含む (FC フレームヘッダーは含まない) 共通トランスポート (CT) ペイロードの最大サイズ。

FDMI ポート

フィールド	説明
SupportedFC4Type	この VSAN のこのポートに登録されている、サポートされている FC-4 タイプの属性。
SupportedSpeed	この VSAN のこのポートに登録されている、サポートされている速度。
CurrentSpeed	この VSAN のこのポートに登録されている現在の速度。
MaxFrameSize	この VSAN のこのポートに登録されている、最大フレームサイズの属性。
OsDevName	この VSAN のこのポートに登録されている OS デバイス名属性。

FDMI バージョン

フィールド	説明
HostName	このポートに関連付けられたホストの名前。

FDMI バージョン

フィールド	説明
ハードウェア	この HBA のハードウェア バージョン。
DriverVer	この HBA を制御するドライバソフトウェアのバージョン レベル。
OptROMVer	この HBA のオプション ROM または BIOS のバージョン。
ファームウェア	HBA が実行しているファームウェアのバージョン。

フロー統計

フィールド	説明
タイプ	フローを選択するための一致基準で、そのようなそのフローは入力トラフィックカウンターにより計測されるトラフィックに含まれる。
VsanId	VSAN の ID。
DestId	宛先ファイバチャネルのアドレス ID。
SrcId	送信元ファイバチャネルのアドレス ID。
マスク	送信元と宛先ファイバチャネルのアドレス ID のマスク。
フレーム	ネットワーク マネージャによって作成されたフローの受信フレーム数。
バイト	ネットワーク マネージャによって作成されたフローの受信フレームのバイト数。
CreationTime	行が作成または変更された時刻を示すタイムスタンプ。

FCC

フィールド	説明
[有効 (Enable)]	ファブリック輻輳制御の有効化
プライオリティ	優先度のレベルを指定します。

フィールド	説明
EdgeQuenchPktsRecd	このポートで受信および処理されたエッジクエンチパケットの数
EdgeQuenchPktsSent	輻輳の結果としてこのポートで生成されたエッジクエンチパケットの数。
PathQuenchPktsRecd	このポートで受信および処理されたパスクエンチパケットの数。
PathQuenchPktsSent	輻輳の結果としてこのポートで生成されたパスクエンチパケットの数。
CurrentCongestionState	輻輳の重大度を示す、このポートの現在のFCC輻輳状態。
LastCongestedTime	ポートの輻輳状態が他の値から noCongestion に変化した時刻。デバイスの最後の再起動以降、ポートの輻輳状態が noCongestion に移行していない場合は N/A です。
LastCongestionStartTime	ポートの輻輳状態が noCongestion から他の値に変化した時刻。
IsRateLimitingApplied	true の場合、レート制限は現在このポートに適用されています。

診断

フィールド	説明
値	センサーが検出した最新の測定値を表示します。
アラーム High and Low	温度、電圧、電流、光送信および受信電力に関するインターフェイスの SFP 診断情報の重大度レベルを表します。1～6の範囲で、6が最も重大度が高くなります。
Warnings High and Low	

FSPF 全般

フィールド	説明
AdminStatus	この VSAN での FSPF の望ましい状態。
OperStatus	この VSAN の FSPF の状態。

フィールド	説明
SetToDefault	これを有効にすると、この行のそれぞれの値がデフォルト値に変更されます。すべての構成パラメータがデフォルト値になっており、VSAN が一時停止している場合、行は自動的に削除されます。
RegionId	この VSAN 上のローカル スイッチの自律領域。
DomainID	この VSAN のローカル スイッチのドメイン ID。
SpfHoldTime	VSAN での 2 つの連続した SPF 計算間の最小時間。値が小さいほど、ルーティングは変更により速く反応しますが、CPU 使用率は高くなります。
SpfDelay	FSPF がトポロジアップデートを受信してから、この VSAN で最短パスファースト (SPF) 計算を開始するまでの時間。値が小さいほど、ルーティングは変更により速く反応しますが、CPU 使用率は高くなります。
MinLsArrival	この VSAN でリンク ステート レコード (LSR) を受け入れてから、同じ VSAN で同じ LSR の別の更新を受け入れるまでの最小時間。この時間間隔のために受け入れられなかった LSR 更新は破棄されます。
MinLsInterval	このスイッチがこの VSAN で LSR を送信してから、同じ VSAN で同じ LSR の別の更新を送信するまでの最小時間。
LsRefreshTime	この VSAN でのリフレッシュ LSR の送信間隔。
LSRMaxAge	LSR がこの VSAN の FSPF データベースに保持される最大経過時間。MaxAge に達すると、データベースから削除されます。
CreateTime	このエントリが最後に作成された時刻。
チェックサム	この VSAN 上のすべての LSR の合計チェックサム。

FSPF インターフェイス

フィールド	説明
SetToDefault	これを有効にすると、この行のそれぞれの値がそのデフォルト値に変更されます。すべての構成パラメータにデフォルト値になっており、インターフェイスがダウンしている場合、行は自動的に削除されます。
コスト	この VSAN のこのインターフェイスでフレームを送信するための管理コスト。値 0 は、コストが構成されていないことを意味します。値が構成されると、値を再び 0 にすることはできません。したがって、明らかに値を 0 に設定することはできません。値が 0 で、対応するインターフェイスがアップである場合、エージェントはインターフェイスの ifSpeed を使用して計算された値を設定します。それ以外の場合は、値がコストとして使用されます。 リンク コストの計算には、次の式が使用されます。 $\text{Link Cost} = \begin{cases} \text{fspflfCost} & \text{if fspflfCost} > 0 \\ (1.0625e12 / \text{Baud Rate}) & \text{if fspflfCost} == 0. \end{cases}$ ここで、Baud Rate はインターフェイスの ifSpeed です。
AdminStatus	この VSAN のこのインターフェイスでの FSPF の望ましい状態。
HelloInterval	リンクの健全性を確認するために、この VSAN のこのインターフェイスで定期的送信される HELLO メッセージの間隔。この値は、この VSAN のリンクの両端にある両方のインターフェイスで同じである必要があることに注意してください。
DeadInterval	この VSAN のこのインターフェイスで HELLO メッセージを受信できない最大時間。この時間が経過すると、インターフェイスは障害が発生していると思われ、データベースから削除されます。 この値は、この VSAN のこのインターフェイスで指定された HELLO 間隔より大きくなければならないことに注意してください。

フィールド	説明
RetransmitInterval	この VSAN のこのインターフェイスで、未確認のリンク アップデートが再送信されるまでの時間。
Neighbour State	FSPF のネイバー ステート マシンの状態。これは、このインターフェイスに接続されているネイバーのインターフェイスとの相互作用の動作状態です。
Neighbour DomainId	この VSAN のネイバーのドメイン ID。
Neighbour PortIndex	この VSAN 上のこのインターフェイスに接続されているネイバーのインターフェイスの、ネイバーによって認識されるインデックス。
CreateTime	このエントリが最後に作成された時刻。

FSPF インターフェイスの統計

フィールド	説明
CreateTime	このエントリが最後に作成された時刻。
ErrorRxPkts	エントリの作成以降、この VSAN のこのインターフェイスで受信した無効な FSPF 制御フレームの数。
InactivityExpirations	エントリの作成以降、この VSAN のこのインターフェイスで非アクティブ タイマーが期限切れになった回数。
LsuRxPkts	エントリの作成以降、この VSAN のこのインターフェイスで受信したリンクステート更新 (LSU) フレームの数。
LsuTxPkts	エントリの作成以降、この VSAN のこのインターフェイスで送信したリンクステート更新 (LSU) フレームの数。
RetransmittedLsuTxPkts	エントリの作成以降、この VSAN のこのインターフェイスで再送信した LSU フレームの数。
LsaRxPkts	エントリの作成以降、この VSAN のこのインターフェイスで受信したリンクステート確認応答 (LSA) フレームの数。

フィールド	説明
LsaTxPkts	エントリの作成以降、この VSAN のこのインターフェイスで送信したリンクステート確認応答 (LSA) フレームの数。
HelloTxPkts	エントリの作成以降、この VSAN のこのインターフェイスで送信した HELLO フレームの数。
HelloRxPkts	エントリの作成以降、この VSAN のこのインターフェイスで受信した HELLO フレームの数。

SDV 仮想デバイス

フィールド	説明
名前	この仮想デバイスの名前を表します。
仮想ドメイン	この仮想デバイスが属する必要があるファブリックの特定のパーティション (ドメイン) を示すための、仮想デバイスの永続的なドメイン ID のユーザー設定。
仮想 FCID	この仮想デバイスの永続的 FCID のユーザー設定。
ポート WWN	この仮想デバイスに割り当てられた PWWN。エージェントは、構成がコミットされるときにこの値を割り当てます。
Node WWN	この仮想デバイスに割り当てられた NWWN。エージェントは、構成がコミットされるときにこの値を割り当てます。
割り当てられた FCID	この仮想デバイスに割り当てられた FCID。エージェントは、構成がコミットされ、この仮想デバイスが仮想化する実際のデバイスがオンラインになったときに、この値を割り当てます。
リアルデバイス マップ リスト	この仮想デバイスがこの VSAN で仮想化する実デバイスのセット。

SDV リアル デバイス

フィールド	説明
タイプ	この仮想デバイスが仮想化する cFcSdvVirtRealDeviceId の対応するインスタンスの値によって表されるリアル デバイス識別子のタイプ。
名前	この仮想デバイスが仮想化するリアル デバイス ID を表します。
マップタイプ	実デバイス (イニシエータ/ターゲット) のマッピング関連付けタイプ。

LUN の検出

フィールド	説明
StartDiscovery	ローカルの場合、直接接続された SCSI ターゲットデバイス/ポートと、すべての VSAN でそれらに関連付けられた LUN のみが検出されます。リモートの場合、直接接続されているものを除き、ファブリック全体のすべての VSAN でそれらに関連付けられているすべての SCSI ターゲット デバイス/ポートおよび LUN が検出されます。
タイプ	ターゲットを選択すると、ターゲットのみが検出されます。NS を選択しないと、ターゲットと LUN の両方が検出されます。
OS	LUN を検出する必要があるオペレーティングシステムを指定します。
ステータス	ローカルスイッチでの LUN 検出の結果を示します。最新の検出のステータスが含まれています。 <ul style="list-style-type: none"> • inProgress(1) - ディスカバリがまだ進行中であることを示します。 • completed(2) - 発見が完了したことを示します。 • failure(3) - 発見が失敗したことを示します。
CompleteTime	最後の検出が完了した日時。最後のシステム再起動以降に検出が実行されていない場合、値はゼロまたは N/A になります。

LUN ターゲット

フィールド	説明
VsanId	このターゲットが属す VSAN。
ポートWWN	この許可された/検出されたターゲットデバイスまたはポートの名前。
DevType	SCSI ターゲットのデバイス タイプ。
VendorId	SCSI ターゲットのベンダー ID。
ProductId	SCSI ターゲットの製品 ID。
RevLevel	SCSI ターゲットの製品リビジョン レベル。
OtherInfo	INQUIRY コマンド応答データのバイト 0 ~ 7。

LUN

フィールド	説明
Id	この LUN の番号。
容量(MB)	この LUN の容量。
SerialNum	この LUN のシリアル番号。
OS	この LUN が検出されたオペレーティング システム。
FC ID	この LUN のファイバチャネル ID。

デバイス エイリアス

フィールド	説明
エイリアス (Alias)	このエントリのデバイスエイリアス。デバイスに設定できるエイリアスは1つだけです。
WWN	デバイスエイリアスが与えられたファイバチャネルデバイス。

デバイス エイリアス構成

フィールド	説明
デバイス エイリアス	このエントリのデバイスエイリアス。デバイスに設定できるエイリアスは1つだけです。

フィールド	説明
WWN	デバイスエイリアスが与えられたファイバチャネル デバイス。

デバイスエイリアスのモード

フィールド	説明
ConfigMode	デバイスエイリアスを構成できるモードを指定します。基本に設定されている場合、デバイスエイリアスは基本動作モードで動作します。基本モードがオンになっている場合、デバイスエイリアスを使用しているすべてのMIBは、それらを同等のpWWNに内部的に変換し、pWWNを使用します。この変換のために従うべきメカニズムは、実装固有です。拡張に設定されている場合、デバイスエイリアスは拡張動作モードで動作します。拡張モードがオンになっている場合、デバイスエイリアスを使用しているすべてのMIBは、変換せずにそのまま使用します。デバイスエイリアスは変換なしで直接使用されます。これはデバイスエイリアスのネイティブ動作モードです。

デバイスエイリアスの不一致

フィールド	説明
不一致	cfdaConfigTable および cfdaConfigMode オブジェクトによって表されるデータベースに対して計算されたチェックサムを表します。このオブジェクトは、上記のオブジェクトがローカル デバイスで変更されたかどうかを確認するために、ネットワーク マネージャによって使用されます。チェックサムの計算に使用される方法は、実装固有です。

ネームサーバー全般

フィールド	説明
VSAN ID / FcId	VSAN または FC の ID。
タイプ	このポートのポート タイプ。

フィールド	説明
PortName	この Nx_port のファイバー チャネル Port_Name (WWN)。
NodeName	この Nx_port のファイバチャネル Node_Name (WWN)。
FC4Type/Features	このポートに関連する FC-4 機能と FC-4 タイプ。形式は FC-GS3 の仕様を参照してください。
FC4 Features	このポートに関連付けられている FC-4 機能。
ProcAssoc	ファイバチャネルの初期プロセス アソシエータ。
FabricPortName	この Nx_port がアタッチされている Fx_port のファブリック ポート名 (WWN)。

ネーム サーバーの詳細

フィールド	説明
ClassOfSvc	サービス インジケータのクラス。
PortIpAddress	関連付けられたポートの IP アドレスが含まれています。
NodeIpAddress	送信した GS3 メッセージの Nx_Port によって示される、この Nx_port のノードの IP アドレス。
SymbolicPortName	このポートのユーザー定義名。
SymbolicNodeName	このポートのノードのユーザー定義名。
HardAddress	拡張リンク サービス (FC-PH-2)。ハードアドレスは 24 ビットの NL_Port 識別子であり、以下で構成されます。最上位バイトの 8 ビット：ドメイン ID、次のバイトの 8 ビット：エリア ID、最下位バイトの 8 ビット：NL_port が FC-AL 初期化中に取得を試みる AL-PA (任意ループの物理アドレス)。ポートが NL_Port ではない場合、または NL_Port であるがハードアドレスがない場合は、すべてのビットが 0 として報告されます。
ProcAssoc	ファイバチャネルの初期プロセス アソシエータ (IPA)。

フィールド	説明
PermanentPortName	この Nx ポートの永続的なポート名。複数のポート名が FDISC (F ポート サービス パラメータの検出) を介してこの Nx ポートに関連付けられている場合、ログイン時にこの Nx ポートに関連付けられた元のポート名が永続的なポート名になります。

ネーム サーバー プロキシ

フィールド	説明
PortName	この VSAN 上の他のポートを登録/登録解除できるプロキシポートの名前。ユーザーは、この値を設定することにより、サードパーティの登録を有効にすることができます。

ネーム サーバー 統計情報

フィールド	説明
Queries Rx	この VSAN のローカル スイッチが受信した Get 要求の総数。
Queries Tx	この VSAN のローカル スイッチが送信した Get 要求の総数。
Requests Rx Reg	この VSAN のローカル スイッチが受信した登録要求の総数。
Requests Rx DeReg	この VSAN のローカル スイッチが受信した登録解除要求の総数。
RSCN Rx	この VSAN のローカル スイッチが受信した RSCN コマンドの総数。
RSCN Tx	この VSAN のローカル スイッチが送信した RSCN コマンドの総数。
Rejects Tx	この VSAN のローカル スイッチが拒否した要求の総数。

優先パス マップとルート

フィールド	説明
VSAN Id、Route Id	この FC ルート マップの VSAN ID。この FC ルート マップ内のルートを識別する任意の整数値。

フィールド	説明
Map Active	FC ルート マップ内のすべてのルートのアクティブ化/非アクティブ化を許可します。true の場合、この FC ルート マップ内のすべてのルートがアクティブになります。false の場合、この FC ルート マップ内のすべてのルートが非アクティブになります。
Route Strict Preference	優先パス選択ロジックが優先パスを選択する方法を変更できます。これを true に設定した場合、cPrefPathRMapSetIntfPref を使用して設定された優先順位に厳密に従って発信インターフェイスを選択する優先パスが作成されます。false に設定した場合、優先パス選択ロジックは、現在の発信インターフェイスがダウンした場合にのみ選択を実行します。
Route Active	FC ルート マップ内のルートのアクティブ化/非アクティブ化を許可します。true の場合、ルートがアクティブになります。false の場合、ルートが非アクティブになります。
RouteActive	FC ルート マップ内のルートのアクティブ化/非アクティブ化を許可します。true の場合、ルートがアクティブになります。false の場合、ルートが非アクティブになります。

Preferred Path Maps Active

フィールド	説明
VSAN Id	この FC ルートマップの VSAN ID。
GlobalActive	FC ルートマップ内のすべてのルートのアクティブ化/アクティブ化解除を許可します。

優先パスすべての一致基準

フィールド	説明
VSAN Id、Route Id	この FC ルート マップの VSAN ID。この FC ルート マップ内のルートを識別する任意の整数値。
Source FcId	フロー分類のためにフレーム内の送信元アドレスとのマッチングが行われる FC ID。

フィールド	説明
出典情報	送信元アドレスに関連付けられたマスクを表します。
送信元シリアル番号	送信元のシリアル番号を表します。
Source Unit Type	送信元のユニットタイプ。
Source Tag	IP アドレスの一意の識別子。
宛先 FcId	フロー分類のためにフレーム内の宛先アドレスとのマッチングが行われる FC ID。
Dest Information	宛先アドレスに関連付けられたマスクを表します。
Dest Serial Number	宛先のシリアル番号を表します。
Dest Unit Type	宛先のユニットタイプ。
Dest Tag	宛先アドレスの一意の識別子。

優先パスのアクティブな一致基準

フィールド	説明
VSAN Id、Route Id	この FC ルート マップの VSAN ID。この FC ルート マップ内のルートを識別する任意の整数値。
Source FcId	フロー分類のためにフレーム内の送信元アドレスとのマッチングが行われる FC ID。
出典情報	送信元アドレスに関連付けられたマスクを表します。
送信元シリアル番号	送信元のシリアル番号を表します
Source Unit Type	送信元のユニットタイプ。
Source Tag	IP アドレスの一意の識別子。
宛先 FcId	フロー分類のためにフレーム内の宛先アドレスとのマッチングが行われる FC ID。
Dest Information	宛先アドレスに関連付けられたマスクを表します。
Dest Serial Number	宛先のシリアル番号を表します。
Dest Unit Type	ソースのユニットタイプ。
Dest Tag	宛先アドレスの一意の識別子。

優先パスのすべての設定

フィールド	説明
VSAN Id、Route Id、Preference	この FC ルートマップの VSAN ID。この FC ルートマップ内のルートを識別する任意の整数値。優先レベル。優先パスのメトリックまたはコストを示します。数値が低いほど優先度が高くなります。
インターフェイス	一致した、または分類されたフレームが転送されるローカルデバイス上のインターフェイスを表します。
IVR Nexthop VSAN	IVR ネクストホップ VSAN ID を表します。

RSCN Nx の登録

フィールド	説明
RegType	サブスクライバが希望する登録のタイプを示します。 <ul style="list-style-type: none"> 「fromFabricCtrlr」は、ファブリックコントローラによって生成された RSCN を示します。 「fromNxPort」は、Nx_Ports によって生成された RSCN を示します。 「fromBoth」は、ファブリックコントローラと Nx_Ports によって生成された RSCN を示します。

RSCN Multi-PID サポート

フィールド	説明
[有効 (Enable)]	この VSAN で multi-pid オプションを有効にするかどうかを指定します。

RSCN イベント

フィールド	説明
タイムアウト (ミリ秒) (TimeOut (msec))	RSCN イベントがタイムアウトするまでの時間 (秒単位)。

RSCN 統計情報

フィールド	説明
SCR Rx	この VSAN の Nx_Port から受信した SCR の数。
SCR RJT	この VSAN で拒否された SCR の数。
RSCN Rx	この VSAN で受信した Nx_Port からの RSCN の数。
RSCN Tx	この VSAN で送信された RSCN の総数。
RSCN RJT	この VSAN で拒否された RSCN の数。
SW-RSCN Rx	この VSAN で他のスイッチから受信したスイッチ間登録状態変更通知 (SW_RSCN) の数。
SW-RSCN Tx	この VSAN で他のスイッチに送信されたスイッチ間登録状態変更通知 (SW_RSCN) の数。
SW-RSCN RJT	この VSAN で拒否された SW_RSCN 要求の数。

マルチキャスト ルート

フィールド	説明
DomainID	この VSAN のマルチキャスト ルートのドメイン ID。
ConfigMode	この VSAN で構成されたマルチキャスト ルート モード。
動作モード	この VSAN の動作可能なマルチキャスト ルート モード。

QoS ポリシーマップ

フィールド	説明
名前	この分類子エントリの名前。名前は一意である必要があります。

QoS クラス マップ

フィールド	説明
名前	このフィルタ エントリの名前。名前は一意である必要があります。

フィールド	説明
一致	フィルタの適用方法を指定します。true の場合、このフィルタの一致が成功したと見なされるには、このフィルタに関連付けられているすべての一致ステートメントが満たされている必要があります。false の場合、このフィルタに関連付けられた条件のいずれか1つが満たされただけでも、フィルタの一致は成功したと見なされます。

QoS マッチ ステートメント

フィールド	説明
SrcAddr	FC フレーム内の送信元アドレスと一致する必要がある FC アドレス。
DstAddr	FC フレーム内の宛先アドレスと一致する必要がある FC アドレス。
インターフェイス	このフィルタによって分類されるためにフレームが到着する必要があるローカル デバイス上の FC インターフェイス。ゼロの値は、インターフェイスが構成されていないことを示します。
Wildcard	ワイルドカード オプションが設定されているかどうかを指定します。true の場合、ワイルドカード オプションが設定され、すべての FC トラフィックが対応するマルチフィールド分類子に一致すると見なされます。false の場合、ワイルドカード オプションは設定されません。

ポリシー マップによる QoS クラスマップ

フィールド	説明
クラスマップ ID	ファイバチャネルフィルタを識別します。
プライオリティ	プライオリティ値を指定します。

VSAN による QoS ポリシー マップ

フィールド	説明
VSAN ID、方向	この VSAN のトラフィック フローの方向を指定します。
ポリシー マップ ID (Policy Map Id)	この VSAN のトラフィックを処理する最初の差別化サービス分類子の要素を選択します。

QoS DWRR

フィールド	説明
重量	このキューに関連付けられた重み。

QoS レート制限

フィールド	説明
パーセント	このインターフェイスのレート制限係数を指定します。

タイマーとポリシー

フィールド	説明
R_A_TOV	Recovery_Qualifier などの NxPort リソースをいつ再利用するかを決定するためのタイムアウト値として FxPort に使用される Resource_Allocation_Timeout 値。
D_S_TOV	分散サービス リクエスト送信者が応答を待機する時間を示す Distributed_Services_Timeout 値。
E_D_TOV	エラー状態を検出するためのタイムアウト値として FxPorts で使用される Error_Detect_Timeout Value です。
F_S_TOV	ファブリック構成中にファブリックの安定性が達成されたことを確認するために使用される Fabric_Stability_Timeout 値。

フィールド	説明
Network Drop Latency	このスイッチのネットワーク遅延。これは送信された順番で受信されなかった場合にフレームがドロップされる時間間隔です。ネットワークの遅延は、常にスイッチの遅延よりも大きいことに注意してください。
Switch Drop Latency	このスイッチのスイッチレイテンシ。これは、いくつかのフレームをネクストホップに配信した後にリンクがダウンした場合、スイッチが未配信フレームをドロップするまでの時間間隔です。このようにして、利用可能なリンクがある場合、未配信のフレームを新しいリンクで送信できます。
InOrderDelivery	デバイスに順序どおりに配信されることを保証する InOrderDelivery フラグ。true の場合、順序どおりの InOrder 配信が保証されます。false の場合、保証されません。
TrunkProtocol	デバイスでトランキングプロトコルを有効または無効にします。トランキングプロトコルは、トランクモードのネゴシエーションと、EISL リンクでの動作可能な VSAN の計算に使用されます。また、ポート VSAN の整合性チェックも実行します。非トランキング ISL リンクでは、ポートの VSAN が異なる場合、E ポートが分離されます。この分離を回避するには、これを無効に設定する必要があります。

WWN マネージャ

フィールド	説明
SwitchWWN	このファブリック要素のワールドワイドネーム。これは 64 ビットの識別子であり、世界中で一意です。
タイプ 1 WWN	
最大	内部エンティティへの割り当てに使用できる NAA タイプ 1 WWN の最大数。
利用可能	内部エンティティへの割り当てに現在使用可能な NAA タイプ 1 WWN の数。

フィールド	説明
予約済み	内部用に予約されている NAA タイプ 1 WWN の数。
タイプ 2 および 5 の WWN	
最大	内部エンティティへの割り当てに使用できるタイプ NAA タイプ 2 およびタイプ 5 WWN の合計 WWN の最大数。
利用可能	内部エンティティへの割り当てに現在使用可能な NAA タイプ 2 およびタイプ 5 WWN の合計数。
予約済み	内部用に予約されたタイプ NAA タイプ 2 およびタイプ 5 WWN の合計 WWN の数。
[より多くの WWN が必要な場合はセカンダリを有効にする (Enable Secondary when more WWNs needed)]	
BaseMacAddress	スーパーバイザ MAC アドレスから生成された WWN のデフォルト範囲を使い果たした場合に、World Wide Name (WWN) の生成に使用される最初の MAC アドレス。
MacAddressRange	wwnmSecondaryBaseMacAddress から始まりこれを含むセカンダリ MAC アドレスの数。

NPV トラフィック マップ

フィールド	説明
スイッチ	スイッチの名前
サーバインターフェイス	サーバ インターフェイスの名前。
外部インターフェイス リスト	トラフィックをマッピングする必要があるインターフェイスのリスト。

NPV ロードバランサ

フィールド	説明
スイッチ	スイッチ名。
有効	サーバ インターフェイスごとの NPV 関連情報の表示を有効または無効にします。

NPV 外部インターフェイスの使用状況

フィールド	説明
スイッチ	スイッチの名前
サーバインターフェイス	ホストやディスクなどのエンドデバイスに接続する NPV デバイスのインターフェイス。F ポート モードで動作するため、F ポートとも呼ばれます。
使用中の外部インターフェイス	NPV コア スイッチに接続する NPV デバイスのインターフェイス。NP ポート モードで動作するため、NP ポートとも呼ばれます。

NP リンク

フィールド	説明
NPIV (core)	NPIV コア スイッチの名前。
F ポート	NPIV コア スイッチに接続されている F ポート
NPV	NPV スイッチの名前
スピード	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. オブジェクトが、値が「n」であると報告した場合、インターフェイスのスピードは「n-500,000」から「n+499,999」までの間です。
Rx Util%	受信トラフィックの使用率%、インターフェイスで構成された速度によりインターフェイスで受信されたオクテットの総数。フレーミング文字を含みます。
Rx Bytes	インターフェイスで受信されたオクテットの総数（フレーミング文字を含む）。
Tx Util%	再送信トラフィックの使用率%、インターフェイスで構成された速度によりインターフェイスから送信されたオクテットの総数。フレーミング文字を含みます。
Tx Bytes	インターフェイスから送信されたオクテットの総数（フレーミング文字を含む）。

FCoE

設定

フィールド	説明
FC Map	FCoE ノード (ENode) に関連付けるために使用される FCoE MAC アドレスのプレフィックス。
Default FCF Priority	ファイバチャネル フォワーダ (FCF) から ENode にアドバタイズされる、デフォルトの FCoE 初期化プロトコル (FIP) の優先順位。
FKA Adv. Period (sec)	FIP キープ アライブ (FKA) メッセージが ENode の MAC アドレスに送信される時間間隔。

VSAN-VLAN マッピング



(注) この表は、バージョン 4.0(1a) 以降を実行している N5k スイッチにのみ適用されます。

フィールド	説明
VSAN Id	VSAN の ID。
VLAN Id	VLAN の ID。
Oper State	この VLAN-VSAN アソシエーション エントリの動作状態を表示します。

VLAN-VSAN マッピング

フィールド	説明
VSAN Id	VSAN の ID。
VLAN Id	VLAN の ID。
Oper State	この VLAN-VSAN アソシエーション エントリの動作状態を表示します。

FCoE 統計

フィールド	説明
Alignment Errors	長さがオクテットの整数倍であるものの、FCS チェックに合格しなかった、特定のインターフェイスでの受信フレームの数。
FCS エラー	長さがオクテットの整数倍であるものの、FCS チェックに合格しなかった、特定のインターフェイスでの受信フレームの数。この数には、フレームが長すぎる、またはフレームが短すぎるためにエラーが生じた受信フレームは含まれません。
シングルコリジョンフレーム	特定のインターフェイスで正常に送信されたものの、送信が1つのコリジョンだけによって妨げられたフレームの数。
マルチコリジョンフレーム	特定のインターフェイスで正常に送信されたものの、送信が2つ以上のコリジョンによって妨げられたフレームの数。
SQEテストエラー	特定のインターフェイスについて、SQE TEST ERROR メッセージが PLS サブレイヤによって生成された回数。
遅延送信	特定のインターフェイスでの最初の送信試行が、メディアがビジー状態のために遅延したフレームの数。
レイトコリジョン	パケットの送信の1スロット時間より後に、特定のインターフェイスでコリジョンが検出された回数。
過剰コリジョン	多数のコリジョンが生じたことによって、特定のインターフェイス上で送信が失敗したフレームの数。インターフェイスが全二重モードで動作している場合、このカウンタが増えることはありません。
内部 Mac 送信エラー	内部 MAC サブレイヤの送信エラーのために特定のインターフェイスで送信が失敗したフレームの数。
キャリア検知エラー	特定のインターフェイスでフレームを送信しようとしたときに、キャリアセンス状態が失われたか、一度もアサートされなかった回数。
長すぎるフレーム	特定のインターフェイスで受信され、最大許可フレームサイズを超えたフレームの数。

フィールド	説明
内部MAC受信エラー	内部MACサブレイヤ受信エラーが原因で、特定のインターフェイスでの受信に失敗したフレームの数。
Symbol Errors	100 Mb/s で動作するインターフェイスの場合、有効なキャリアが存在しながら無効なデータシンボルがあった回数

Ficon

FICON VSAN

フィールド	説明
VSAN ID	ファブリック内の VSAN を一意に識別します。
Host Can Offline SW	true の場合、ホストはシステムをオフラインにすることができます。
Host Can Sync Time	true の場合、ホストはシステム時刻を設定できます。
Port Control by Host	true の場合、ホストは FICON Director 接続パラメータを変更できます。
Port Control by SNMP	true の場合、SNMP マネージャーは FICON ディレクターの接続パラメータを変更できます。
CUP Name	コントロールユニット デバイスの名前。
CUP Enable	コントロールユニット デバイスが有効かどうかを示します。
ドメイン ID	スイッチのドメイン ID を指定します。
CodePage	この VSAN で使用されるコード ページ。
文字セット (Character Set)	この VSAN で使用されるコード ページの文字セット。
Active=Saved	true の場合、「アクティブなら保存」モードが有効になります。すべての変更は NVRAM に保存されます。
User Alert Mode	true の場合、FICON 管理ステーションは変更時にプロンプトを表示します。

フィールド	説明
Device Allegiance	CUP がチャンネルへの従属状態にある場合、論理パスからのコマンドを受け入れることはできません。CUP は、チャンネルからコマンドを受け取ると従属状態になり、チャンネルプログラムが正常に完了するまで「従属関係」を形成します。その時点で、CUPは「ロック解除」モードになります。
VSAN Time	VSANのシステム時刻。これは、ホストによって設定されるか、FICON Director のデフォルトのグローバル時間である可能性があります。デフォルトのグローバル時間は、FICON Director のローカル時間です。
VSAN State	FICON 機能のコンテキストで、VSAN に属するポートの状態を制御します。
VSAN Serial Number	この VSAN の FICON ダイ렉タのシリアル番号。

FICON VSAN ファイル

フィールド	説明
説明	構成ファイルの説明。
CUP Name	コントロールユニット デバイスの名前。
ステータス	Locked は、変更が許可されていないことを示します。Unlocked は、変更が許可されていることを示します。
LastAccessed	このファイルが最後にアクセスされた時刻。
UserAlertMode	true の場合、ダイ렉タのユーザー アラートモードが有効になります。

グローバル

フィールド	説明
Default Port Prohibited	デフォルトのポートをブロックするには、このオプションをオンにします。

FICON ポート属性

フィールド	説明
TypeNumber	この FICON ダイレクタのタイプ番号。
SerialNumber	製造時にこの FICON ダイレクタに割り当てられたシーケンス番号。
タグ	これは、ピア ポートの識別子です。 <ul style="list-style-type: none"> ピア ポートのユニットタイプがチャンネルである場合、PortId はこのピア ポートを含むチャンネルパスの CHPID (チャンネルパス識別子) になります。 ピア ポートが controlUnit の場合、PortId は 0 になります。 ピア ポートがファブリックの場合、PortId はピア スイッチのインターフェイスのポート アドレスになります。
FcId	反対側のポートのファブリック ID (イニシエータ/ターゲット)。これは、ファブリックポートの場合にのみ入力されます。
ステータス	「有効 (valid)」 : この情報が最新の場合。 「古い (old)」 : この情報がキャッシュされている場合。 [古い属性をクリア (Clear Old Attributes)] をクリックして、キャッシュをクリアします。
名前	FICON のポート名。
メーカー	この FICON ダイレクタを製造した会社の名前。
ModelNumber	この FICON ダイレクタのモデル番号。
PlantOfMfg	この FICON ダイレクタの製造工場を識別する工場コード。
UnitType	このポートが通信しているポートのピア タイプ。 ==チャンネル - ホスト ==コントロールユニット - ディスク ==ファブリック - ISL

フィールド	説明
アラート	次のいずれかが表示されます。 <ul style="list-style-type: none"> • bitErrThreshExceeded, • lossOfSignalOrSync, • nosReceived, • primitiveSeqTimeOut, • invalidPrimitiveSeq <p>このアラートを確認してクリアするには、 [クリア (Clear)] をクリックします。</p>

FICON ポートの構成

フィールド	説明
Show Installed Ports Only	true の場合、物理的に使用可能なポートのみがテーブルにリストされます。
ESCON 形式	ESCON 形式のポート構成画面では、DM のポート構成テーブルに、ESCON 形式でポートが表示されます。表の A は使用可能なポートを表し、P は禁止されているポートを表します。
Port/ Prohibit	ポートの FICON アドレスと禁止リストを入力します。（これはテーブルグリッドの代替です）。
名前	このポートのポート名。
Block	true の場合、このポートは分離されます。
Prohibit Grid	グリッドをクリックして、ポートが相互に通信する機能を追加または削除します。

FICON ポート番号

フィールド	説明
モジュール	シャーシのモジュール番号
Reserved Port Numbers (Physical)	モジュール用に予約されたポート番号。
NumPorts	そのモジュール用に予約されているポートの数。
Module Name	モジュールの名前。

フィールド	説明
Reserved Port Numbers (Logical)	シャーシ スロットのポート番号。1つのシャーシ スロット用に予約されているポート番号。シャーシ内のスロットごとに、最大 64 個のポート番号を予約できます。

FICON VSANs Director 履歴

最新の FICON 情報を表示するには、[Refresh] ボタンをクリックする必要があります。

フィールド	説明
KeyCounter	キーカウンターです。
Ports Address Changed	KeyCounter の値の構成が変更されたポートのリスト。

ファブリック バインド アクション

フィールド	説明
VSANId	ファブリック内の VSAN に対する一意の識別子を指定します。
アクティブ化 (Activate)	<ul style="list-style-type: none"> • activate - この VSAN/VLAN 上の有効なポート バインドがアクティブ化されます。 • force activate - アクティブ化中にエラーが発生した場合でも強制的にアクティブ化が行われ、アクティブになったファブリック バインドがアクティブデータベースにコピーされます。 • deactivate - この VSAN/VLAN 上で現在アクティブになっている有効なファブリック バインド (ある場合) が非アクティブ化されます。アクティブ データベースに含まれていた現在アクティブなエントリ (ある場合) は削除されます。 • no-selection -
有効	この VSAN/VLAN のアクティベーションの状態。true の場合は、この VSAN/VLAN に対する最新の操作として、アクティベーションが試みられています。false の場合は、この VSAN/VLAN に対する最新の操作として、アクティベーションが試みられていません。
結果	最新のアクティベーション/非アクティベーションの結果を示します。

フィールド	説明
LastChange	この VSAN/VLAN 上の有効なポート バインドが最後にアクティブ化されたタイミング。エージェントの前の再初期化前に最後のアクティベーションが行われている場合、この値はN/Aになります。
CopyActToConfig	有効な場合、アクティブポートバインドデータベースがこのVSAN/VLANの構成のデータベースにコピーされます。学習済みエントリもコピーされます。

ファブリック バインド構成データベース

フィールド	説明
VSAN Id	ファブリック内の VSAN の一意の識別子を指定します。
Peer WWN (Name)	ファブリックの一部にすることができるスイッチのスイッチ WWN を指定します。
DomainID	永続的なドメイン ID を指定します。

ファブリック バインド アクティブ データベース

フィールド	説明
VSAN Id	ファブリック内の VSAN の一意の識別子を指定します。
Peer WWN	ファブリックの一部にすることができるスイッチのスイッチ WWN を指定します。
DomainID	スイッチの WWN の対応するインスタンスによって表されるスイッチの固定ドメインIDを指定します。

ファブリック バインド データベースの差異

フィールド	説明
VSAN	ドロップダウンリストから、比較する VSAN の番号を選択します。

フィールド	説明
比較	<p>比較するデータベースを選択します：</p> <ul style="list-style-type: none"> • Active - この VSAN/VLAN で構成データベースに関連してファブリック バインドアクティブ データベースを比較します。そのため、コンフィギュレーションデータベースがリファレンス データベースとなり、差演算の結果はコンフィギュレーションデータベースに対するものになります。 • Config - この VSAN/VLAN でアクティブデータベースに関連してファブリック バインド構成データベースを比較します。そのため、アクティブデータベースがリファレンス データベースとなり、差演算の結果はアクティブ データベースに対するものになります。
VSAN Id	ファブリック内の VSAN の一意の識別子を指定します。
Peer WWN	ファブリックの一部にすることができるデバイスのデバイス WWN を指定します。
DomainID	スイッチの WWN の対応するインスタンスによって表されるスイッチの固定ドメインIDを指定します。
Reason	このエントリに関する、比較しているデータベース間の相違点の理由を示します。

ファブリック バインド違反

フィールド	説明
VSAN Id	ファブリック内の VSAN の一意の識別子を指定します。
Peer WWN	ローカル デバイスのポートのいずれかでファブリックへのエントリが拒否されたデバイスの sWWN (switch WWN) です。

フィールド	説明
DomainID	ローカル デバイスのポートのいずれかでファブリックへのエントリが拒否されたデバイスのドメイン ID です。ゼロの値は、デバイスのスイッチ WWN が強制されたファブリック バインディングに存在しなかったことを示します。
DenialTime	拒否された時刻です。
DenialCount	このスイッチがローカル デバイスのポートのいずれかでファブリックへのエントリを拒否された回数。
DenialReason	デバイスがローカル デバイスのポートのいずれかでファブリックへのエントリを拒否された理由。

ファブリック バインド 統計

フィールド	説明
AllowedReqs	この VSAN/VLAN で、ファブリックの一部となるためにスイッチから出されて、許可された要求の数です。
DeniedReqs	この VSAN/VLAN で、ファブリックの一部となるためにスイッチから出されたものの、拒否された要求の数です。
クリア	Clear に設定すると、この VSAN/VLAN 上のファブリック バインド統計情報カウンタがクリアされます。

ファブリック バインド EFMD 統計

フィールド	説明
TxMergeReqs	ローカル デバイスがこの VSAN で送信した EFMD マージ要求の数。
RxMergeReqs	ローカル デバイスがこの VSAN で受信した EFMD マージ要求の数。
TxMergeAccs	ローカル デバイスがこの VSAN で送信した EFMD マージ受け入れの数。
RxMergeAccs	ローカル デバイスがこの VSAN で受信した EFMD マージ受け入れの数。

フィールド	説明
TxMergeRejs	ローカル デバイスがこの VSAN で送信した EFMD マージ拒否の数。
RxMergeRejs	ローカル デバイスがこの VSAN で受信した EFMD マージ拒否の数。
TxMergeBusys	ローカル デバイスがこの VSAN で送信した EFMD マージ ビジーの数。
RxMergeBusys	ローカル デバイスがこの VSAN で受信した EFMD マージ ビジーの数。
TxMergeErrs	ローカル デバイスがこの VSAN で送信した EFMD マージ エラーの数。
RxMergeErrs	ローカル デバイスがこの VSAN で受信した EFMD マージ エラーの数

IP ストレージ

FCIP Profiles

フィールド	説明
[IPアドレス (IP Address)]	このエンティティのインターネットアドレス。
ポート	FCIP エンティティが新しい TCP 接続要求を待ち受ける、FCIP の既知のポート番号以外の TCP ポート。
SACK	TCP 選択的受信確認オプションをイネーブルにし、受信側が複数の損失フレームを 1 つの ACK で確認応答し、高速な回復を可能にするかどうか。
KeepAlive (s)	このエンティティ内部のすべてのリンクの TCP キープアライブ タイムアウト。
ReTrans MinTimeout (ms)	このエンティティ内部のすべてのリンクに対する TCP 最小再送信 タイムアウト。
ReTrans Max	TCP 接続で同じデータ項目を再送信する最大回数。この再送信回数後に配信の確認応答がなかった場合、その接続は終了されます。
Send BufSize (KB)	このエンティティ内部のすべてのリンクのすべての TCP 接続に対する、集約 TCP 送信ウィンドウ。この値は出力フロー制御に使用されます。このエンティティ内部のすべての接続でキューに入れられたデータの合計がこの値に達すると、出力側でフロー制御が行われます。

フィールド	説明
Bandwidth Max (Kb)	アダプタイズする TCP 受信ウィンドウを算出するための、B-D 乗算に使用されるネットワーク パイプの推定帯域幅。
Bandwidth Min (Kb)	このエンティティ内部のリンクの TCP 接続に使用可能な最小帯域幅。
Est Round Trip Time (us)	アダプタイズする TCP 受信ウィンドウを算出するための、B-D 乗算に使用されるネットワーク パイプの推定ラウンドトリップ遅延。
PMTU Enable	パス MTU ディスカバリ。
PMTU ResetTimeout (sec)	MSS がネゴシエーションされた TCP 値に戻るまで、検出した pathMTU が有効となっている期間。
CWM Enable	True の場合、輻輳ウィンドウ モニタリングがイネーブルされます。
CWM BurstSize (KB)	TCP 送信側の待機時間後に送信される最大バースト。
最大ジッター (Max Jitter)	このインターフェイスの TCP 接続で発生する可能性のある最大遅延変動 (輻輳が原因ではないもの)。

FCIP Tunnels

フィールド	説明
インターフェイス	このリンクが関連するこの FCIP デバイスのインターフェイスを識別します。
サービス契約購入済み	この FCIP リンクが開始されたインターフェイス。
B Port Enable	True の場合、ローカル FCIP リンクで B ポートモードがイネーブルになります。
B Port KeepAlive	True の場合、ピアから受信した (ファイバチャネルの) ELS エコーフレームに対してメッセージが送信されます。一部の B ポート実装では、リンク キープアライブとして ELS エコー要求/応答フレームが使用されます。
リモート IP アドレス	リモート FCIP エンティティのインターネット アドレス。
Remote TCP Port	ローカル FCIP エンティティによってこのリンクの TCP 接続設定が開始された場合に、その FCIP エンティティの接続先となるリモート TCP ポート。
Spc Frames Enable	True の場合、TCP アクティブ オープナが FCIP 特殊フレームを開始し、TCP パッシブ オープナがその FCIP 特殊フレームに回答するようになります。False に設定すると、FCIP 特殊フレームは生成されず、応答もされません。

Spc Frames RemoteWWN	リモート FC ファブリック エンティティのワールドワイド名。長さゼロの文字列となっている場合は、このリンクがすべてのリモートエンティティからの接続を受け付けます。WWN が指定されると、このリンクはその WWN を持つリモートエンティティからの接続を受け付けます。
Spc Frames Remote Profile Id	リモート FCIP エンティティの ID。

FCIP Tunnels (Advanced)

フィールド	説明
インターフェイス	この FCIP リンクが開始されたインターフェイス。
Timestamp Enable	True の場合、FCIP ヘッダーのタイムスタンプが確認されます。
Timestamp Tolerance	ローカル時刻と、FCIP ヘッダーで受信したタイムスタンプ値の間で許容される時間差。デフォルトでは、この値が EDTOV/2 になります。EDTOV とは、エラー状態を検出するためのタイムアウト値としてファイバチャネルポートで使用される Error_Detect_Timeout Value です。
Number Connections	このリンクで許可される TCP 接続の最大数。
パッシブ	False の場合、このリンクエンドポイントはピアへの接続をアクティブに試行します。True の場合、このリンクエンドポイントはピアからの接続を待ちます。
QoS Control	TCP 制御接続用として IP ヘッダーの ToS フィールドに設定する値。
QoS Data	TCP データ接続用として IP ヘッダーの ToS フィールドに設定する値。
IP Compression	圧縮する場合に使用するアルゴリズム。
Write Accelerator	書き込みアクセラレータを使用すると SCSI 書き込みパフォーマンスを向上できます。
Tape Accelerator	True の場合、テープアクセラレータ（テープの書き込みパフォーマンスを向上可能）がイネーブルになります。
Tape Accelerator Oper	FCIP リンクの書き込みアクセラレーションをイネーブルにします。
TapeRead Accelerator Oper	テープアクセラレータ動作を有効にすると自動的にイネーブルになります。
FlowCtrlBufSize Tape (KB)	フロー制御バッファのサイズ（64 K ~ 32 MB）。0 に設定すると、フロー制御バッファのサイズがスイッチによって自動的に計算されます。
IPSec	このリンクで IP セキュリティがオンとオフのどちらになっているかを示します。

フィールド	説明
XRC Emulator	オンにすると、XRC エミュレータがイネーブルになります。この機能はデフォルトではディセーブルになっています。
XRC Emulator Oper	XRC エミュレータの動作状態を示します。

FCIP Tunnels (FICON TA)

フィールド	説明
インターフェイス	このリンクが関連する FCIP デバイスのインターフェイスを識別する一意の値。
VSAN List Admin	FICON テープ アクセラレーションが構成されている VSAN のリスト。
VSAN List Oper	FICON テープ アクセラレーションが動作している VSAN のリスト。

FCIP Tunnels Statistics

フィールド	説明
インターフェイス	このリンクが関連する FCIP デバイスのインターフェイスを識別する一意の値。
Rx IPCompRatio	FCIP デバイスで受信したパケットの IP 圧縮比。このオブジェクトの値は、小数点以下 2 桁までの浮動小数点数で示されます。
Tx IPCompRatio	FCIP デバイスで送信したパケットの IP 圧縮比。このオブジェクトの値は、小数点以下 2 桁までの浮動小数点数で示されます。

FCIP XRC Statistics

フィールド	説明
ProfileId	プロファイルの固有 ID。
インターフェイス	インターフェイスの名前。
RRSAccelerated	アクセラレーションされた読み取りレコードセット IU の数。
RRSForwarded	転送された読み取りレコードセット IU の数。
BusyStatus	コントロール ユニットから受信したビジー状態のインスタンスの数。

フィールド	説明
UnitCheckStatus	コントロールユニットから受信したユニットチェック状態のインスタンスの数。
cfmFcipLinkExtXRCEStatsSelReset	処理された選択的リセットの数。
BufferAllocErrors	バッファ割り当てエラーの数。

iSCSI Connection

フィールド	説明
LocalAddr	この接続で使用されるローカルインターネットネットワークアドレス。
RemoteAddr	この接続で使用されるリモートインターネットネットワークアドレス。
CID	この接続の iSCSI 接続 ID。
ステータス	<p>iSCSI ネゴシエーションから見た、この接続の現在の状態。</p> <ul style="list-style-type: none"> • login : トランスポート プロトコルで接続されているが、最終ビットが設定された有効な iSCSI ログイン応答が送信または受信されていません。 • full : 最終ビットが設定された有効な iSCSI ログイン応答が送信または受信されています。 • logout : 有効な iSCSI ログアウトコマンドが送信または受信されたが、トランスポート プロトコル接続がまだ閉じていません。
MaxRecvDSLen	この接続で使用されているコマンドまたはデータ PDU でサポートされる最大データペイロードサイズ。ネゴシエーションが 512K ブロック単位で行われていても、レポートされるサイズはバイト単位となります。
SendMarker	この接続で、発信データストリームにマーカーを挿入するかどうかを示します。
HeaderDigest	この接続で使用される iSCSI ヘッダーダイジェスト方式。
DataDigest	この接続で使用される iSCSI データ ダイジェスト方式。

iSCSI イニシエータ

フィールド	説明
Name or IP Address	このエントリで表されるノードのグローバルな固有識別子となる文字列。
VSAN Membership	このエントリで表されるノードがアクセス可能な設定済み VSAN のリスト。
ダイナミック	True の場合は、このエントリで表されるノードが自動的に検出されます。
イニシエータタイプ	ノードが、iSCSI ロード バランシングに使用されるホストかどうかを示します。
Persistent Node WWN	True の場合は、FC ドメイン内で同じノード名で表されるノードに、同じ FC アドレスが割り当てられます。ノードの FC アドレスは、自動割り当てでも手動割り当てでもかまいません。
SystemAssigned Node WWNN	True の場合、このノードに FC アドレスが自動的に割り当てられます。False の場合は、FC アドレスが手動で設定されます。
Node WWN	ノードの永続的な FC アドレス。
Persistent Port WWN	True の場合は、FC ドメイン内で同じノード名で表されるノードのポートに、同じ FC アドレスが割り当てられます。
ポート WWN	このノードに関連付けられたすべての FC ポート アドレス。
AuthUser	発信側がログイン時の使用を許可された唯一の CHAP ユーザ名です。
Target UserName	(任意) ログインに使用されるユーザ名。ユーザ名を指定しなかった場合は、グローバルユーザ名が使用されます。
Target Password	(任意) ログインに使用されるパスワード。パスワードを指定しなかった場合は、グローバルパスワードが使用されます。
Load Metric	iSCSI ロードバランシング用に、この iSCSI 発信側に設定されたロードメトリック。
Auto Zone Name	この発信側のターゲットリストに対する自動ゾーンをシステムが作成するときに使用されるゾーン名。

iSCSI Session Initiators

フィールド	説明
Name or IP Address	発信側ポートの名前または IP アドレス。
Alias	ログイン時に獲得した発信側のエイリアス。

Module Control

フィールド	説明
Module Id	モジュールの ID。
Admin Status	モジュールの iSCSI 機能をイネーブルまたはディセーブルにします。
OperStatus	モジュールの iSCSI インターフェイスがイネーブルか、ディセーブルかが表示されます。

iSCSI Global

フィールド	説明
AuthMethod	認証方式。
InitiatorIdleTimeout	ゲートウェイ (FC ターゲットを表すもの) が、最後の iSCSI セッションから iSCSI 発信側がダウンするまで待つ時間。この時間が経過すると、その iSCSI 発信側に関する情報をパーズします。
iSLB ZonesetActivate	このオプションをオンにすると、発信側ターゲットに関連付けられた自動ゾーン分割が実行されます。
DynamicInitiator	このフィールドは、ダイナミック iSCSI 発信側の作成方法を決定します。iSCSI オプション (デフォルト) を選択すると、ダイナミック iSCSI 発信側が作成されます。iSLB を選択すると、iSLB ダイナミック発信側が作成されます。拒否するオプションを選択すると、発信側のダイナミック作成が禁止されます。
Target UserName	ログインに使用するデフォルト ユーザ名。発信側のユーザ名を指定した場合は、代わりにそのユーザ名が使用されます。

フィールド	説明
Target Password	ログインに使用するデフォルトパスワード。発信側のパスワードを指定した場合は、代わりにそのパスワードが使用されます。

iSCSI Session Statistics

フィールド	説明
PDU Command	このセッションで転送されたコマンドPDUの数。
PDU Response	このセッションで転送された応答PDUの数。
Data Tx	このセッションでローカル iSCSI ノードから送信されたデータのバイト数。
Data Rx	このセッションでローカル iSCSI ノードで受信されたデータのバイト数。
Errors Digest	認証エラー。
Errors CxnTimeout	接続タイムアウト。

iSCSI Targets

フィールド	説明
Dynamically Import FC Targets	このオプションをオンにすると、FCターゲットが iSCSI ドメインに動的にインポートされます。iSCSI ドメイン内にすでに存在しているターゲットはインポートされません。
iSCSI名	このエントリで表されるノードの iSCSI 名。
ダイナミック	このエントリで表されるノードが、自動的に検出されたものか、手動で設定されたものかを示します。
Primary Port WWN	このターゲットの FC アドレス。
Secondary Port WWN	このターゲットのオプションのセカンダリ FC アドレス。この FC アドレスは、プライマリに到達できない場合に使用されます。
LUN Map iSCSI	この LU に構成されたデフォルトの論理ユニット番号。
LUN Map FC Primary	プライマリ ポートアドレスに対するリモート LU の論理ユニット番号。

フィールド	説明
LUN Map FC Secondary	セカンダリポートアドレスに対するリモートLUの論理ユニット番号。
Initiator Access All	Trueの場合、このターゲットの発信側許可リストになくても、すべての発信側がこのターゲットにアクセスできます。Falseの場合は、許可リストにある発信側だけがこのターゲットにアクセスを許可されます。
Initiator Access List	このエントリで表されるノードにアクセスを許可されたすべてのiSCSIノードのリスト。AllAllowedがFalseでリストの値が空の場合は、このターゲットにアクセスを許可される発信側がありません。
Advertised Interfaces	ターゲットがアダプタイズされるすべてのインターフェイスのリスト。
Trespass Mode	このノードのトレスパスモード。各iSCSIターゲットはFCターゲットの1つ以上のポートを表しています。Trueの場合は、プライマリポートがダウンしているときに、すべてのLUN I/O要求をセカンダリポートに渡すよう、ノードがFCノードに指示します。
RevertToPrimaryPort	FCターゲットがオンラインに復帰した場合に、プライマリポートに戻す必要があるかどうかを示します。

iSCSI iSLB VRRP

フィールド	説明
VrId、IpVersion	仮想ルータ番号およびIPバージョン（IPv4、IPv6、またはDNS）。
Load Balance	ロードバランシングがイネーブルになっているかどうかを示します。

iSCSI Initiator Access

フィールド	説明
イニシエータ名	iSCSIノード名。

Initiator Specific Target

フィールド	説明
名前	ノードのグローバルな固有識別子。
Port WWN(s) Primary	この iSCSI 発信側固有のターゲットに関連付けられた、ファイバチャネルターゲットのポートアドレス。
Port WWN(s) Secondary	この iSCSI 発信側固有のターゲットに関連付けられた、ファイバチャネルターゲットのポートアドレス。
LUN Map (Hex) iSCSI	この iSCSI 発信側固有のターゲットに関連付けられた、ファイバチャネルターゲットのポートアドレス。
LUN Map (Hex) FC Primary	この iSCSI 発信側固有のターゲットに関連付けられた、ファイバチャネルターゲットのポートアドレス。
LUN Map (Hex) FC Secondary	この iSCSI 発信側固有のターゲットに関連付けられた、ファイバチャネルターゲットのポートアドレス。
No AutoZone Creation	この iSCSI 発信側ターゲットおよび iSCSI 発信側に対して、ファイバチャネルゾーンが自動的に作成されるかどうかを示します。True の場合、ゾーンは自動的に作成されません。False (デフォルト) の場合、ゾーンは自動的に作成されます。
Trespass Mode	このノードのトレスパス モード。True の場合、プライマリ ポート (fcAddress) がダウンすると、FC ノードインスタンスはすべての LUN I/O 要求をセカンダリ ポート (fcSecondaryAddress) に渡します。
Revert to Primary Port	このノードのプライマリ モードに戻ります。True の場合、プライマリ ポートがオンラインに復帰すると、FC ノードインスタンスはすべての LUN I/O 要求をプライマリ ポート (fcAddress) に渡します。
Primary PWWN VSAN	この発信側ターゲットの自動ゾーンが配置される VSAN を示します。このオブジェクトが設定されていない場合、VSAN はネームサーバに照会することで決定されます。
Secondary PWWN VSAN	この発信側ターゲットの自動ゾーンが配置される VSAN を示します。このオブジェクトが設定されていない場合、VSAN はネームサーバに照会することで決定されます。

iSCSI Initiator PWWN

フィールド	説明
ポート WWN	このエントリの FC アドレス。

iSCSI Sessions

フィールド	説明
タイプ	iSCSI セッションのタイプ。 <ul style="list-style-type: none"> • normal : セッションは通常の iSCSI セッション • discovery -セッションは検出のためにのみ使用されます。
TargetName	方向が発信の場合は、ここにリモートターゲットの名前が格納されます。
Vsan ID	このセッションが属す VSAN。
ISID	iSCSI セッション ID の発信側で定義された部分。
TSIH	このセッション用にターゲットで定義された識別ハンドル。

iSCSI Sessions Detail

フィールド	説明
ConnectionNumber	このセッションに現在属している転送プロトコル接続の数。
ImmediateData	発信側とターゲットが、このセッションでの即時データのサポートに合意しているかどうか。
初期	True の場合、発信側は Ready-To-Transfer を待ってからターゲットに送信する必要があります。False の場合、発信側は FirstBurstSize で設定された制限内、および要求で予想されるデータ転送長の範囲内でデータをすぐに送信できます。
MaxOutstanding	このセッション中のタスクごとの未処理の Ready-To-Transfers の最大数。
最初	このセッション中に送信される割り込みデータでサポートされる最大長。
最大	受信データまたは送信データ PDU の 1 つのシーケンス中に送信可能な最大バイト数。

フィールド	説明
[シーケンス (Sequence)]	False の場合は、iSCSI データ PDU シーケンスが任意の順序で転送される可能性があることを示します。True の場合は、エラー回復時を除いて、連続的に増加するオフセットを使用してデータ PDU シーケンスを転送する必要があることを示します。
PDU	False の場合は、シーケンス中の iSCSI データ PDU が任意の順序でかまいません。True の場合は、シーケンス中のデータ PDU が、PDU 間にギャップやオーバーレイがなく、連続して増加するアドレスになっている必要があることを示します。

IP サービス

IP Routes

フィールド	説明
Routing Enabled	このチェックボックスをオンにすると、スイッチが IP ルータとして機能します。
Destination、Mask、Gateway	このルートのネクストホップに到達するために経由するローカルインターフェイスを識別する値。
メトリック	このルートのプライマリ ルーティング メトリック。
インターフェイス	このルートのネクストホップに到達するために経由するローカルインターフェイス。
アクティブ	ルートがアクティブかどうかを示します。

IP Statistics ICMP

フィールド	説明
InParmProbs	受信した ICMP パラメータ問題メッセージの数。
OutParmProbs	送信した ICMP パラメータ問題メッセージの数。
InSrcQuenchs	受信した ICMP ソースクエンチメッセージの数。
InRedirects	受信した ICMP リダイレクトメッセージの数。

フィールド	説明
InEchos	受信した ICMP エコー（要求）メッセージの数。
InEchoReps	受信した ICMP エコー応答メッセージの数。
InTimestamps	受信した ICMP タイムスタンプ（要求）メッセージの数。
InTimestampReps	受信した ICMP タイムスタンプ応答メッセージの数。
InAddrMasks	受信した ICMP アドレス マスク要求メッセージの数。
InAddrMaskReps	受信した ICMP アドレス マスク応答メッセージの数。
InDestUnreachs	受信した ICMP 宛先到達不能メッセージの数。
InTimeExcds	受信した ICMP 時間超過メッセージの数。
OutSrcQuenchs	送信した ICMP ソースクエンチメッセージの数。
OutRedirects	送信した ICMP リダイレクトメッセージの数。 ホストはリダイレクトを送信しないため、ホストではこの値が常に N/A となります。
OutEchos	送信した ICMP エコー（要求）メッセージの数。
OutEchoReps	送信した ICMP エコー応答メッセージの数。
OutTimestamps	送信した ICMP タイムスタンプ（要求）メッセージの数。
OutTimestampReps	送信した ICMP タイムスタンプ応答メッセージの数。
OutAddrMasks	送信した ICMP アドレス マスク要求メッセージの数。
OutAddrMaskReps	送信した ICMP アドレス マスク応答メッセージの数。
OutDestUnreachs	送信した ICMP 宛先到達不能メッセージの数。
OutTimeExcds	送信した ICMP 時間超過メッセージの数。

IP Statistics IP

フィールド	説明
InHdrErrors	チェックサムの誤り、バージョン番号の不一致、その他のフォーマットエラー、存続可能時間の超過、IP オプションの処理中に発見されたエラーなど、IP ヘッダーにエラーがあるため廃棄された入力データ グラムの数。
InAddrErrors	IP ヘッダーの宛先フィールドにある IP アドレスが、このエンティティで受信する有効なアドレスではないために廃棄された入力データ グラムの数。エンティティが IP ルータではなく、データ グラムを転送しない場合、このカウンタには宛先アドレスがローカルアドレスではないために廃棄されたデータ グラムが含まれます。
InUnknownProtos	正常に受信されたが、不明または未サポートのプロトコルであるために廃棄されたローカル アドレス宛データグラムの数。
InDiscards	処理の継続を妨げるような問題は発生していないにもかかわらず、(バッファ領域の不足などが原因で) 廃棄された入力 IP データ グラムの数。このカウンタには、再構成の待機中に廃棄されたデータグラムは含まれません。
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). このカウンタには、ipForwDatagrams でカウントされたデータグラムの中で、この (任意の) 廃棄基準と一致するすべてのフレームが含まれます。
OutNoRoutes	宛先に転送するためのルートが見つからなかったために廃棄された IP データグラムの数。このカウンタには、ipForwDatagrams でカウントされたフレームの中で、この「ルートなし」基準と一致するものすべてが含まれます。これには、すべてのデフォルトルートがダウンしているためにホストがルーティングできなかったすべてのデータグラムが含まれます。
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
ReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). 一部のアルゴリズム (特に RFC 815 のアルゴリズム) では、受信ごとにフラグメントを結合し、フラグメントの数を追跡しきれないため、これは廃棄された IP フラグメントの数とは限りません。
InReceives	受信エラーがあったものも含めて、インターフェイスから受信した入力データグラムの合計数。
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	転送要求の中でローカル IP ユーザー プロトコル (ICMP を含む) が IP に指定された、IP データ グラムの合計数。このカウンタには、ipForwDatagrams でカウントされたデータ グラムは含まれません。

フィールド	説明
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. IP ルータとして機能しないエンティティでは、このエンティティによってソースルーティングされ、ソースルートオプションが正常に処理されたフレームだけがこのカウンタに含まれます。
FragOKs	このエンティティで正常にフラグメント化された IP データグラムの数。
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully re-assembled.

IP Statistics SNMP

フィールド	説明
BadVersions	SNMP エンティティに配信されたが、サポートされていない SNMP バージョンだった SNMP メッセージの合計数。
BadCommunityNames	認識されない SNMP コミュニティ名を使用している SNMP エンティティに配信された SNMP メッセージの合計数。
BadCommunityUses	SNMP エンティティに配信され、メッセージで指定された SNMP コミュニティで許可されていない SNMP 処理を表す SNMP メッセージの合計数。
ASNParseErrs	受信した SNMP メッセージをデコードするときに、SNMP エンティティで発生した ASN.1 エラーまたは BER エラーの合計数。
TooBigs	SNMP プロトコルエンティティに配信され、エラー状態フィールドの値が tooBig だった SNMP PDU の合計数。
SilentDrops	SNMP エンティティに配信され、空の変数バインドフィールドを持つ代替 Response-PDU を含んだ応答のサイズが、ローカル制限または要求の発信元に関連する最大メッセージサイズよりも大きかったため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
ProxyDrops	SNMP エンティティに配信され、返信できた Response-PDU がなかった状態（タイムアウトを除く）でプロキシターゲットへのメッセージ（変換されたものを含む）の送信に失敗したため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
NoSuchNames	SNMP プロトコルエンティティに配信され、エラー状態フィールドの値が noSuchName だった SNMP PDU の合計数。

フィールド	説明
BadValues	SNMP プロトコル エンティティに配信され、エラー ステータス フィールドの値が badValue である SNMP PDU の総数。
ReadOnlys	SNMP プロトコルエンティティに配信され、エラー状態フィールドの値が readOnly だった有効な SNMP PDU の合計数。エラー状態フィールドに値 readOnly を含んだ SNMP PDU の生成は、誤った実装の SNMP を検出する手段として用意されたものであるため、これが生成されるのはプロトコルエラーです。
GenErrs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
Pkts	転送サービスから SNMP エンティティに配信されたメッセージの合計数。
GetRequests	SNMP プロトコルエンティティによって受け入れられ、処理された SNMP Get-Request PDU の合計数。
GetNexts	SNMP プロトコルエンティティによって受け入れられ、処理された SNMP Get-Next PDU の合計数。
SetRequests	SNMP プロトコルエンティティによって受け入れられ、処理された SNMP Set-Request PDU の合計数。
OutTraps	SNMP プロトコルエンティティで生成された SNMP Trap PDU の合計数。
OutGetResponses	SNMP プロトコル エンティティで生成された SNMP Get-Response PDU の合計数。
OutPkts	SNMP プロトコルエンティティから転送サービスに渡された SNMP メッセージの合計数。
TotalReqVars	有効な SNMP Get-Request と Get-Next PDU を受信した結果として、SNMP プロトコル エンティティによって正常に取得された MIB オブジェクトの合計数。
TotalSetVars	有効な SNMP Set-Request PDU を受信した結果として、SNMP プロトコルエンティティによって正常に変更された MIB オブジェクトの合計数。

IP Statistics UDP

フィールド	説明
InErrors	宛先ポートでアプリケーションが待ち受けていないこと以外の理由で配信できなかった、受信した UDP データグラムの数。
InDatagrams	UDP ユーザに配信された UDP データグラムの合計数。
OutDatagrams	このエンティティから送信された UDP データグラムの合計数。

フィールド	説明
NoPorts	宛先ポートでアプリケーションが待ち受けていなかった、受信したUDPデータグラムの合計数。

mgmt0 Statistics

フィールド	説明
InErrors	インターフェイスで受信したエラーの合計数。
OutErrors	インターフェイスで送信したエラーの合計数。
InDiscards	インターフェイスで受信した廃棄の合計数。
OutDiscards	インターフェイスで送信した廃棄の合計数。
TotalRxBytes	受信した合計バイト数。
TxBytes	送信した合計バイト数。
[RxFrames]	受信したフレームの合計数。
[TxFrames]	送信したフレームの合計数。

TCP UDP TCP

フィールド	説明
都道府県 (State)	この TCP 接続の状態。

TCP UDP UDP

フィールド	説明
ポート (Port)	このUDPリスナーのローカルポート番号。

VRRP General

フィールド	説明
IP Address Type、VrId、Interface	IP アドレスのタイプ (IPv4、IPv6、または DNS)、仮想ルータ ID、およびインターフェイス。
Admin	仮想ルータの管理状態 (active または notInService)。

フィールド	説明
Oper	<p>仮想ルータの現在の状態。定義済みの値は次の3つです。</p> <ul style="list-style-type: none"> • initialize : すべての仮想ルータがスタートアップイベントを待っていることを示しています。 • backup : 仮想ルータがマスタールータの可用性を監視していることを示しています。 • master : 仮想ルータが、このルータに関連付けられたIPアドレスにフレームを転送していることを示しています。
プライオリティ	<p>仮想ルータのマスター選択プロセスに使用されるプライオリティを指定します。値が大きいほどプライオリティが高くなります。マスタールータからプライオリティ0が送信された場合は、このルータがVRRPへの参加を終了しようとしているため、バックアップの仮想ルータが新しいマスターに移行する必要があります。プライオリティ255は、関連するIPアドレスを所有するルータに使用されます。</p>
AdvInterval	<p>アドバタイズメントメッセージの送信間隔（秒数）。VRRPアドバタイズメントを送信するのはマスタールータだけです。</p>
PreemptMode	<p>プライオリティの高い仮想ルータが、プライオリティの低いマスターと入れ替わるかどうかを制御します。</p>
稼働時間	<p>この仮想ルータが、「初期化済み状態」から変化するとき。</p>
バージョン	<p>このVRRPインスタンスが実行しているVRRPのバージョン。</p>
AcceptMode	<p>マスター状態の仮想ルータがIPv6アドレスを所有していない場合に、アドレス所有者のそのIPv6アドレス宛てのパケットをそのまま受け付けるかどうかを制御します。Trueの場合、マスター状態の仮想ルータは受け付けます。Falseの場合、マスター状態の仮想ルータは受け付けません。</p>

VRRP IP Addresses

フィールド	説明
Interface、VRRP ID、IP Address	インターフェイス、仮想ルータの冗長プロトコルID、および関連する IP アドレス。

VRRP 統計情報

フィールド	説明
IP Address Type、VrId、Interface	IP アドレスのタイプ (IPv4、IPv6、または DNS)、仮想ルータ ID、およびインターフェイス。
LastAdvRx	この仮想ルータが受信した VRRP アドバタイズメントの合計数。
Protocol Traffic MasterIpAddr	マスタールータの実際の (プライマリ) IP アドレス。この仮想ルータが前回受信した VRRP アドバタイズメントに送信元としてリストされた IP アドレスです。
Protocol Traffic BecomeMaster	仮想ルータの状態が MASTER に遷移した合計回数。
Priority 0 Rx	仮想ルータが受信した、プライオリティ「0」の VRRP フレームの合計数。
Priority 0Tx	仮想ルータが送信した、プライオリティ「0」の VRRP フレームの合計数。
AuthErrors InvalidType	不明な認証タイプで受信したフレームの合計数。
Other Errors dvIntervalErrors	ローカル仮想ルータに設定されたアドバタイズメント間隔とは異なる間隔で受信した VRRP アドバタイズメント フレームの合計数。
Other Errors IpTtlErrors	仮想ルータが受信した、IP TTL (存続可能時間) が 255 以外の VRRP フレームの合計数。
Other Errors InvalidTypePktsRcvd	仮想ルータが受信した、タイプ フィールドが無効な値の VRRP フレームの合計数。
Other Errors AddressListErrors	アドレス リストが仮想ルータにローカルで設定したリストと一致しない、受信したフレームの合計数。
OtherErrors PacketLengthErrs	フレーム長が VRRP ヘッダーよりも短い、受信したフレームの合計数。

フィールド	説明
RefreshRate	リフレッシュの時間間隔。

CDP General

フィールド	説明
[有効 (Enable)]	Cisco Discovery Protocol が実行されているかどうか。CDP がディセーブルになると CacheTable のエントリが削除されます。
MessageInterval sec	CDP メッセージが生成される間隔。デフォルト値は 60 秒です。
HoldTime sec	受信デバイスが CDP メッセージを保持している時間。デフォルト値は 180 秒です。
LastChange	キャッシュ テーブルが最後に変更されたのはいつか。
サポートされる DeviceId 形式	デバイスのデバイス ID 形式への互換性を示します。
デバイス ID 形式	サポートされているデバイスの中で対応しているインスタンスに入っているデバイス - ID のフォーマットの表示。

CDPネイバー

フィールド	説明
スイッチ	このエンティティのインターネットアドレス。
ローカルインターフェイス	このリンクが関連する FCIP デバイスのインターフェイスを識別する一意の値。
[DeviceName]	リモートデバイスの名前。規定では、デバイスの完全修飾ドメイン名です。
DeviceID	最新の CDP メッセージでレポートされたデバイス ID 文字列。
DevicePlatform	最新の CDP メッセージでレポートされたバージョン文字列。
インターフェイス	最新の CDP メッセージでレポートされたポート ID 文字列。
IPAddress	最近受信した CDP メッセージのアドレス TLV でレポートされた、デバイスの SNMP エージェントの（最初の）ネットワーク層アドレス。
NativeVLAN	最新の CDP メッセージでレポートされた、リモートデバイスのインターフェイスのネイティブ VLAN。値 0 は、最新の CDP メッセージでネイティブ VLAN フィールド (TLV) がレポートされなかったことを示します。

フィールド	説明
PrimaryMgmtAddr	最近受信した CDP メッセージでレポートされた、デバイスが SNMP メッセージを受け付ける（最初の）ネットワーク層アドレスを示します。
SecondaryMgmtAddr	最近受信した CDP メッセージでレポートされた、デバイスが SNMP メッセージを受け付ける代替ネットワーク層アドレスを示します。

iSNS Profiles

フィールド	説明
アドレス	iSNS サーバのアドレス。
ポート	iSNS サーバの TCP ポート。

iSNS Servers

フィールド	説明
名前	iSNS サーバの名前。
TcpPort	iSNS メッセージで使用される TCP ポート。このサーバで TCP がサポートされていない場合、値は 0 になります。
稼働時間	サーバがアクティブ状態を続けている時間。
ESI Non Response Threshold	エンティティが iSNS データベースから登録解除される前に送信されたため、応答を受信しない ESI メッセージの数。
# Entities	サーバの iSNS に登録されたエンティティの数。
# Portals	サーバの iSNS に登録されたポータル数。
# Portal Groups	サーバの iSNS に登録されたポータルグループの数。
# iSCSI Devices	サーバの iSNS に登録された iSCSI ノードの数。

iSNS Entities

フィールド	説明
エンティティ ID (Entity ID)	エンティティの iSNS エンティティ識別子。
最後のアクセス	エンティティが最後にアクセスされた時刻。

iSNS Cloud Discovery

フィールド	説明
AutoDiscovery	自動クラウド検出をオンするかどうか。

フィールド	説明
DiscoveryDelay	連続した IP クラウド検出を実行する継続時間。
検出	<p>実行する IP ネットワーク検出コマンド。</p> <ul style="list-style-type: none"> • all - ファブリック内のすべてのギガビットイーサネットインターフェイスに対して IP ネットワーク検出を実行する。 • noOp (デフォルト) - 何も実行しない。
CommandStatus	<p>ライセンスのインストール/アンインストール/更新動作の状態。</p> <ul style="list-style-type: none"> • success - 検出動作が正常に完了した。 • nProgress - 検出動作が進行中。 • none - 検出動作が実行されていない。 • NoIpNetworkNameSpecified - ipCloud 名が指定されていない。 • invalidNetworkName - ipCloud が構成されていない。 • NoIPSPortNameSpecified - gigE ポート ifindex が指定されていない • invalidIPSPortName - 無効な gigE ポートインターフェイス。 • generalISNSFailure - 一般的な iSNS サーバ障害。

iSNS Clouds

フィールド	説明
Id	IP クラウドの ID。
Switch WWN	このテーブル内のスイッチの WWN。

iSNS Cloud Interfaces

フィールド	説明
Name、Switch WWN、Interface、Address	クラウドの名前、スイッチの WWN、インターフェイス、およびアドレス。

Monitor Dialog Controls

フィールド	説明
折れ線グラフ	データを折れ線グラフで表した新しいウィンドウを開きます。
面グラフ	データを面グラフで表した新しいウィンドウを開きます。
棒グラフ	データを棒グラフで表した新しいウィンドウを開きます。
円グラフ	データを円グラフで表した新しいウィンドウを開きます。
Reset Cumulative Counters	[Column Data] の表示モードが [Cumulative] に設定されている場合に、カウンタを0にリセットします。
ファイルへのエクスポート	標準の [Save] ダイアログボックスを表示します。データは.TXTファイルで保存されます。
プリント	標準の [Print] ダイアログボックスを表示します。
更新頻度 (Update Frequency)	監視ダイアログ内でデータを更新する間隔。
列データ	監視ダイアログに表示されるデータのタイプを指定します。 <ul style="list-style-type: none"> • Absolute Value : スイッチを起動してからの合計量を表示します。これがエラー モニタリングのデフォルトです。 • Cumulative : ダイアログを表示してからの合計量を表示します。[Reset Cumulative Counters] ボタンをクリックしてカウンタをリセットすると、累積データの新しいセットを収集できます。 • Minimum/sec : リフレッシュ間隔ごとの1秒間の最小値を表示します。 • Maximum/sec : リフレッシュ間隔ごとの1秒間の最大値を表示します。 • Last Value/sec : リフレッシュ間隔ごとの1秒間の最新の値を表示します。これがトラフィック モニタリングのデフォルト設定です。

フィールド	説明
Elapsed	ダイアログが表示されてからの経過時間。 [Reset Cumulative Counters] ボタンをクリックしてこのカウンタをリセットすると、累積データの新しいセットを収集できます。

iSNS Details iSCSI Nodes

フィールド	説明
名前	ストレージノードに関連付けられたイニシエータまたはターゲットの iSCSI 名。
タイプ	この iSCSI ノードの機能を定義する Node Type ビットマップ。31 はターゲット、30 は発信側、29 は制御で、その他はすべて予約されています。
Alias	iSCSI ノードのエイリアス名。
ScnBitmap	ノードの State Change Notification (SCN) ビットマップ。
WWN Token	オプションのグローバルに固有な 64 ビット整数値。ファイバチャネルファブリック内での iSCSI デバイスのノードのワールドワイドノード名を表すために使用できます。
AuthMethod	この iSCSI ノードで有効な iSCSI 認証方法。

iSNS Details Portals

フィールド	説明
アドレス	このポータルのインターネットアドレス。
TcpPort	このポータルのポート番号。
SymName	このポータルのオプションのシンボリック名。
EsiInterval	このポータルの Entity Status Inquiry (ESI) 間隔。
TCP ESI	ESI モニタリングに使用される TCP ポート番号。
TCP Scn	iSNS サーバからの SCN メッセージの受信に使用される TCP ポート番号。
SecurityInfo	ポータルセキュリティビットマップ属性に登録されたポータルのセキュリティ属性設定。

セキュリティ

セキュリティ ロール

フィールド	説明
名前	ロールの名前。 [作成 (Create)] ボタンをクリックして、新しいロールを定義します。 [ルール (Rules)] ボタンをクリックして、このロールのルールを定義します。
[説明 (Description)]	ユーザー ロールのテキストの説明。
VSAN Scope Enable	ロールを指定された VSAN に制限する機能を有効にします。
VSAN Scope List	ロールがアクセスを許可されている VSAN のリストを指定します。
Interface Scope Enable	(Nexus 5000 シリーズのみ) ロールを指定されたインターフェイスに制限する機能を有効にします。
Interface Scope List	(Nexus 5000 シリーズのみ) ロールがアクセスを許可されているインターフェイスのリストを指定します。

セキュリティ ロール ルール



(注) この表は Nexus 5000 シリーズ スイッチにのみ適用されます。

フィールド	説明
ルールの順序	番号順にルールが適用されます。
許可するか?	ルールが操作を許可するか拒否するかを示します。
Rule Operation	ルールでは、操作での読み取り専用アクセスまたは読み取り/書き込みアクセスを指定できます。
Rule Element Type	ルールは、コマンド、機能、機能グループ、またはすべてに適用できます。 [すべて (all)] を選択すると、ルールはすべてのコマンドと機能に適用されます。
Rule Element	ルール要素。ルールが適用されるコマンド、機能、または機能グループを指定します。
Features/Groups	[機能/グループ (Features/Groups)] ボタンをクリックすると、機能グループ マネージャが開きます。

機能グループ マネージャ



(注) この表は Nexus 5000 シリーズ スイッチにのみ適用されます。

フィールド	説明
名前	機能グループの名前。
追加	新しい機能グループを作成するには、[名前 (Name)]フィールドに新しい機能グループ名を入力し、[追加 (Add)]をクリックします。
機能の追加	機能グループに機能を追加するには、機能グループ パネルで 1 つ以上の機能グループ名を選択し、機能パネルで機能を選択して、[機能の追加 (Add Feature)]をクリックします。
適用	変更を保存するには、[適用 (Apply)] ボタンをクリックします。

AAA LDAP サーバー

フィールド	説明
IP アドレスタイプ	IP アドレス タイプ (IPv4、IPv6、または DNS) 。
Name or IP Address	AAA サーバーの IP アドレス。
AuthPort	AAA サーバーの認証ポート。
TimeOut(s)	AAA サーバーへの再送信間の秒単位の時間。この値は、このサーバーの [機能 (Features)] タブで設定されたタイムアウトの設定値を上書きします。この値がゼロの場合、[機能 (Features)] タブで設定された値が使用されます。
再送信	サーバーへの試行を中止するまでに、AAA クライアントが AAA サーバーを試行する追加の回数。この値は、[機能 (Features)] タブで設定された値を上書きします。この値がゼロの場合、[機能] タブで設定された値が使用されます。
Idle Time (m)	システムがサーバーにテスト パケットを送信して定期的に AAA サーバーをテストする時間間隔 (分)。デフォルト値の 0 は、AAA サーバーの定期的なテストを行わないことを意味します。

フィールド	説明
TestUser	サーバーが要求に応答するかどうかをテストするために、AAAサーバーに送信されるテストパケットで使用されるユーザー名。
TestPassword	サーバーが要求に応答するかどうかをテストするために、AAAサーバーに送信されるテストパケットで使用されるパスワード。
RootDN	LDAP サーバー データベースへのアクセスの認証に使用されるルート名。
RootDNPasswordEncrType	RootDNPassword パスワードに使用される暗号化のタイプ。
RootDNPassword	ルート バインドを実行する場合に使用する RootDN パスワード。RootDN パスワードを入力しない場合、匿名バインドが実行されます。
SSL Mode	LDAP サーバーとのバインディングの前に、TLS トンネルを設定する必要があるかどうかを指定します。

AAA サーバグループ

フィールド	説明
名前	サーバグループの名前。
プロトコル	このサーバーグループが属する AAA プロトコル。
ServerIdList	これは、このサーバーグループを形成する AAA サーバーの順序付きリストを表します。値内のサーバーの順序によって、そのグループのサーバーの優先順位が決まります。最初のもは「プライマリ」で、残りはセカンダリ（その他）です。サーバーグループは、メンバーがいないと存在できません。

フィールド	説明
デッドタイム	AAA サーバー グループの DeadTime 設定。これは、AAA サーバーが認証要求に応答しない場合に、システムがサーバーをデッドとマークする時間の長さで、分単位で指定します。デッドタイムの間隔中に発生した認証要求は、デッドとしてマークされた AAA サーバーに送信されません。デフォルト値の 0 は、AAA サーバーが応答しない場合でも、そのサーバーがデッドとしてマークされないことを意味します。

AAA 検索マップ

フィールド	説明
BaseDN	許可要求の処理中に LDAP サーバーが検索を開始する LDAP 階層内の基本エントリの名前を指定します。
フィルタ	LDAP サーバー データベースでユーザー エントリを検索するために使用する LDAP フィルタの名前を指定します。
属性	ユーザー プロファイルのプライベート属性として使用する LDAP 属性を指定します。

AAA アプリケーション

フィールド	説明
ServerGroupIdList	これは、このアプリケーションが AAA 機能を実行するように設定されている AAA サーバーグループの順序付きリストを表します。値でのサーバー グループの順序によって、リスト内のサーバー グループの優先順位が決まります。
ローカル	「ローカル」AAA は、デバイスで提供されるローカル AAA サービスを使用して、すべての AAA 機能を実行することを意味します。有効にすると、サーバーグループリスト内のすべてのサーバー グループを試した後にのみ使用されます。

フィールド	説明
通常	<p>「トリビアル (Trivial) 」AAA は、すべてのサーバーグループと「ローカル」AAA (構成されている場合) を試した後にのみ使用されます。トリビアルAAA は、AAAFUNCTION の対応するインスタンスの値に基づいて、次のいずれかに対応します。</p> <ul style="list-style-type: none"> 「AAAFUNCTION」値が「authentication」の場合、ユーザー名ベースの認証 「AAAFUNCTION」値が「authorization」の場合、許可チェックなし 「AAAFUNCTION」値が「accounting」の場合、アカウントिंगなし。

AAA のデフォルト

フィールド	説明
KeyEncrType	サーバー鍵の暗号化タイプ。
AuthKey	AAA サーバーとクライアントの間で渡されるフレームの暗号化に使用されるキー。このキーは、サーバーで設定されているキーと一致する必要があります。
TimeOut	AAA サーバーへの再送信間隔を指定する秒数。
再送信	サーバーへの試行を中止するまでに、AAA クライアントが AAA サーバーを試行する追加の回数。
DirectReq	ログイン時の認証に AAA サーバーを選択できるかどうかを指定します。true の場合、ログイン時の認証にリモート AAA サーバーを指定できます。ログイン名を username@hostname として指定すると、認証要求は、username をユーザー名として、hostname というホスト名を持つリモート AAA サーバーに送信されます。false の場合、ログイン時の認証にリモート AAA サーバーを指定できません。

フィールド	説明
DeadTime (m)	AAA サーバー グループの DeadTime 設定。これは、AAA サーバーが認証要求に応答しない場合に、システムがサーバーをデッドとマークする時間の長さで、分単位で指定します。デッドタイムの間隔中に発生した認証要求は、デッドとしてマークされた AAA サーバーに送信されません。デフォルト値の 0 は、AAA サーバーが応答しない場合でも、そのサーバーがデッドとしてマークされないことを意味します。

AAA 全般

フィールド	説明
AuthTypeMSCHAP	ログイン時にリモート AAA サーバーを介してユーザーを認証するために MSCHAP 認証メカニズムを使用する必要があるかどうかを示します。true の場合、MSCHAP 認証が使用されます。false の場合は、デフォルトの認証メカニズムが使用されます。
AuthTypeMSCHAPv2	ログイン時にリモート AAA サーバーを介してユーザーを認証するために MSCHAPv2 認証メカニズムを使用する必要があるかどうかを示します。true の場合、MSCHAP 認証が使用されます。false の場合は、デフォルトの認証メカニズムが使用されます。



- (注) 一度に 1 つの認証メカニズムを変更することをお勧めします。そうしないと、エラーが発生する可能性があります。たとえば、MSCHAP を MSCHAPv2 に変更したい場合は、MSCHAP を選択して適用してから、MSCHAPv2 を選択して適用してください。

AAAの統計情報

フィールド	説明
認証	
要求	このサーバーがアクティブになってから送信された認証要求の数。リクエストのタイムアウトによる再送信は、別個のリクエストとしてカウントされます。

フィールド	説明
タイムアウト	サーバーがアクティブになってからタイムアウトになった認証要求の数。
Unexpected	このサーバーがアクティブになってから受信した予期しない認証応答の数。
エラー	このサーバーがアクティブになってから受信したサーバー ERROR の認証応答の数。
不正解	サーバーがアクティブになってから処理できなかった認証応答の数。
ResponseTime	システムの再初期化以降、このサーバーに送信された認証要求の平均応答時間（タイムアウトを除く）。
成果	このサーバーがアクティブになってから成功した、このサーバーとの認証トランザクションの数。タイムアウトが発生した場合、トランザクションには複数の要求の再送信が含まれる場合があります。サーバーが認証の成功または失敗のいずれかで応答した場合、トランザクションは成功したものとみなされます。
障害	このサーバーがアクティブになってから失敗した、このサーバーとの認証トランザクションの数。タイムアウトが発生した場合、トランザクションには複数の要求の再送信が含まれる場合があります。最大再送信数に達した場合、またはサーバーがトランザクションを中止した場合、トランザクションエラーが発生します。
許可	
要求	このサーバーがアクティブになってから送信された許可リクエストの数。リクエストのタイムアウトによる再送信は、別個のリクエストとしてカウントされます。
タイムアウト	サーバーがアクティブになってからタイムアウトになった許可リクエストの数。タイムアウトになると、リクエストが再送信されます。試行の最大数に達した場合、それ以上の再送信は試行されません。

フィールド	説明
Unexpected	このサーバーがアクティブになってから受信した予期しない許可応答の数。例としては、すでにタイムアウトしたリクエストへの遅延応答があります。
エラー	このサーバーがアクティブになってから受信したサーバー ERROR の許可応答の数。これらは、サーバー自体が許可操作でエラーを識別したことを示す応答です。
不正解	サーバーがアクティブになってから処理できなかった許可応答の数。理由には、応答を復号できなかった、無効なフィールドである、または応答が要求に基づいて無効であることが含まれます。
ResponseTime	システムの再初期化以降、このサーバーに送信された許可要求の平均応答時間（タイムアウトを除く）。
成果	このサーバーがアクティブになってから成功した、このサーバーとの許可トランザクションの数。タイムアウトが発生した場合、トランザクションには複数の要求の再送信が含まれる場合があります。サーバーが許可のパスした、または失敗のいずれかで応答した場合、トランザクションは成功したものとみなされます。
障害	このサーバーがアクティブになってから失敗した、このサーバーとの許可トランザクションの数。タイムアウトが発生した場合、トランザクションには複数の要求の再送信が含まれる場合があります。最大再送数に達した場合、またはサーバーがトランザクションを中止した場合、トランザクションエラーが発生します。
アカウンティング	
要求	システムの再初期化以降にこのサーバーに送信されたアカウンティング要求の数。リクエストのタイムアウトによる再送信は、別個のリクエストとしてカウントされます。

フィールド	説明
タイムアウト	システムの再初期化以降にタイムアウトになったアカウントング要求の数。タイムアウトになると、リクエストが再送信されます。試行の最大数に達した場合、それ以上の再送信は試行されません。
Unexpected	システムの再初期化以降に、このサーバーから受信した予期しないアカウントング応答の数。例としては、すでにタイムアウトしたリクエストへの遅延応答があります。
エラー	システムの再初期化以降に、このサーバーから受信したサーバー ERROR アカウントング応答の数。これらは、サーバー自体がアカウントング操作でエラーを識別したことを示す応答です。
不正解	システムの再初期化以降に処理できなかったアカウントング応答の数。理由には、応答を復号できなかった、無効なフィールドである、または応答が要求に基づいて無効であることが含まれます。
ResponseTime	タイムアウトを除くシステムの再初期化以降、このサーバーに送信されたアカウントング要求の平均応答時間。
成果	システムの再初期化以降に成功した、このサーバーとのアカウントング トランザクションの数。タイムアウトが発生した場合、トランザクションには複数の要求の再送信が含まれる場合があります。サーバーがアカウントングの成功または失敗のいずれかで応答した場合、トランザクションは成功したものとみなされます。
障害	システムの再初期化以降に失敗した、このサーバーとのアカウントング トランザクションの数。タイムアウトが発生した場合、トランザクションには複数の要求の再送信が含まれる場合があります。最大再送数に達した場合、またはサーバーがトランザクションを中止した場合、トランザクションエラーが発生します。
統計	

フィールド	説明
ステータス	サーバーの現在の状態です。 <ul style="list-style-type: none"> • アップ：サーバーはリクエストに応答します • デッド：サーバーが応答しませんでした サーバーは最大回数の再送信後に応答しない場合「デッド」とマークされます。待機期間後またはサーバーから応答があると、サーバーは再び「アップ」とマークされます。
現在の継続時間 (csec)	サーバーが現在の状態になってからの経過時間。
以前の継続時間 (csec)	このオブジェクトは、サーバーが最新の状態より前の状態にあった時間の長さを提供します。サーバーの状態が変化していない場合、この値はゼロです。
TotalDeadTime	システムの再初期化以降、このサーバーの状態の値がデッドだった時間の合計。
DeadCount	システムの再初期化以降、このサーバーがデッド状態になった回数

iSCSI User

フィールド	説明
iSCSI User	iSCSI ユーザの名前。
パスワード	iSCSI ユーザのパスワード。

共通ロール



(注) 共通ロールは、displayFCoE モードでは使用できません（セキュリティロールを使用してください）。

フィールド	説明
説明	共通ロールの説明。
有効	共通ロールに VSAN の制約があるかどうかを指定します。

フィールド	説明
リスト	ユーザが制限された VSAN のリスト。

SNMP セキュリティ ユーザ

フィールド	説明
[役割 (Role)]	セキュリティモデルに依存しない形式でのユーザ。
パスワード	一般ユーザのパスワード。SNMP の場合、このパスワードは、認証と機密保全の両方に使用されます。CLI と XML の場合、認証のみに使用されます。
ダイジェスト	使用されるダイジェスト認証プロトコルのタイプ。
Encryption	使用される暗号化認証プロトコルのタイプ。
ExpiryDate	このユーザの有効期限が切れる日付。
SSH Key File Configured	ユーザが SSH 公開キーで設定されているかどうかを指定します。
SSHキーファイル	<p>SSH 公開キーを保管しているファイルの名前。SSH 公開キーは、このユーザの SSH セッションを認証するために使用されます。これは、CLI ユーザに対してのみ適用されます。形式は次のいずれかになります。</p> <ul style="list-style-type: none"> • OpenSSH 形式の SSH 公開キー • IETF SECSH (商用の SSH 公開キー形式) の SSH 公開キー • 公開キーの抽出元となる PEM (Privacy-Enhanced Mail 形式) の SSH クライアント証明書 • 証明書ベースの認証用の SSH クライアント証明書 DN (識別名)

フィールド	説明
Creation Type	ユーザのクレデンシャルストアのタイプ。ユーザによってこのテーブルに行が作成されると、デバイスに対してローカルなクレデンシャルストアにユーザ エントリが作成されます。AAA サーバベースの認証などのリモート認証メカニズムの場合、資格情報は他の（リモートの）システムまたはデバイスに保管されません。
有効期限日	このユーザの有効期限が切れる日付。

SNMP セキュリティ コミュニティ

フィールド	説明
コミュニティ	コミュニティ スtring。
ロール	セキュリティ モデル名。

セキュリティ ユーザ グローバル

フィールド	説明
Enforce SNMP Privacy Encryption	SNMP エージェントにより、SNMPv3 メッセージに対する暗号化の使用がシステム内のすべてのユーザに対してグローバルに適用されるかどうかを指定します。
キャッシュタイムアウト	これにより、ローカル システム内でユーザ資格情報をキャッシュするための最大タイムアウト値が指定されます。



- (注) 管理者が Device Manager で新しいユーザを作成する場合または既存のユーザを削除する場合、プライバシー パスワードと認証パスワードが必要です。ただし、新しいユーザの作成時に管理者がこれらの資格情報を入力しなくても、Device Manager は、管理者の認証パスワードをプライバシー パスワードとして使用します。ユーザに対して定義されたプライバシー プロトコルが DES（デフォルト）ではない場合、MDS 内の SNMP エージェントはパケットを復号化できなくなり、SNMP エージェントはタイムアウトします。ユーザに対して定義されたプライバシー プロトコルが DES ではない場合、ユーザがログイン時にプライバシー パスワードとプロトコルの両方を入力する必要があります。

FC-SP 全般/パスワード

フィールド	説明
タイムアウト	FC-SP メッセージのタイムアウト時間
HashList	提案されたハッシュメカニズムが優先順に含まれています。先頭が最優先で、末尾が最も優先されません。
GroupList	「:」で区切られた各トークンには、Diffie-Hellman グループ識別子に対応する値が含まれます。
GenericPasswd	スイッチのパスワード

FC-SP インターフェイス

フィールド	説明
モード	<p>このインターフェイスの FC-SP モード。</p> <ul style="list-style-type: none"> • autoPassive の場合、ポートは FC-SP 認証交換を開始しません。ただし、相手側によって開始された FC-SP 認証交換には常に参加します。 • autoActive の場合、ポートは常に ESC の後に FC-SP 認証交換を開始しようとします。相手側が FC-SP 認証をサポートしていない場合でも、ポートはやはりアップになろうとします。 • オン の場合、ポートは常に FC-SP 認証交換を開始しようと、認証はポートがアップになる前に行われます。相手側が FC-SP 認証をサポートしていない場合、ポートはアップになりません。 • オフ の場合、ポートは FC-SP 認証交換を開始せず、反対側から開始された FC-SP 認証メッセージに拒否を送信しません。「オフ」でない場合には、ポートは少なくとも 1 つの FC-SP 認証プロトコルをサポートする必要があります。 <p>(注) DCNM からのタイムアウト エラーを回避するには、各スイッチで FC-SP DHCHAP モードを個別に設定する必要があります。</p>

フィールド	説明
Reauthenticate Interval (hr)	ポートが相手側の再認証を試みる前に待機しなければならない時間（時間単位）。
Reauthenticate Start	これが有効に設定されている場合、相手側を再認証します。
Auth Successes	このインターフェイスで FC-SP 認証が成功した回数。
Auth Fails	このインターフェイスで FC-SP 認証が失敗した回数。
Auth Bypasses	このインターフェイスで FC-SP 認証がバイパスされた回数。

FC-SP ローカルパスワード

フィールド	説明
Local WWN	ローカルホストのポートワールドワイド名。
パスワード	ローカルスイッチのパスワード。

FC-SP リモートパスワード

フィールド	説明
Remote WWN	リモートホストのワールドワイド名。
パスワード	リモートスイッチのパスワード。

FC-SP 統計

フィールド	説明
Auth Succeeded	このインターフェイスで FC-SP 認証が成功した回数。
認証失敗	このインターフェイスで FC-SP 認証が失敗した回数。
Auth ByPassed	このインターフェイスで FC-SP 認証がバイパスされた回数。
EspSpiMismatch	SPI が不一致だった受信フレームの数。

フィールド	説明
EspAuthFailed	ESP 認証チェックに失敗した受信フレームの数。

FC-SP SA (セキュリティ アソシエーション)

フィールド	説明
SPI	セキュリティパラメータインデックスの値を表示します。
ソルト	暗号化に使用されるソルト。
キー	暗号化と認証に使用されるキー。

FC-SP ESP インターフェイス

フィールド	説明
インターフェイス	インターフェイスの名前。
ESP Mode	ESP モードを次のいずれかとして指定します。 <ul style="list-style-type: none"> なし - ESP はリンク上で実行されていません。 Gcm- リンクは暗号化および認証する必要があります。 Gmac- リンクは認証が必要です
EgressSA	使用する出力セキュリティアソシエーションを指定します。有効な値は、256 ~ 65536 です。
IngressSA1	使用する入力セキュリティアソシエーションを指定します。有効な値は、256 ~ 65536 です。
IngressSA2	使用する入力セキュリティアソシエーションを指定します。有効な値は、256 ~ 65536 です。
EspFailureReason	失敗の理由を表示します。「なし (None)」は、エラーがないことを示します。

PKI 全般

フィールド	説明
スイッチ	スイッチ名。

フィールド	説明
CertStoreConfig	システムが認証に使用する証明書ストア構成。

PKI RSA キーペア

フィールド	説明
名前	キーペアの名前またはラベル。
サイズ	<p>キーのサイズ。次のモジュラスサイズが定義されています。</p> <ul style="list-style-type: none"> • 512 ビット、768 ビット、1024 ビット、1536 ビット、および 2048 ビット。 <p>作成後はサイズの変更はできません。行の削除によってキーペアを削除してから、エントリを別のサイズで再度作成してください。</p>
ファイル名	RSA 秘密鍵を保管するファイルの名前。このファイル名は、キーペア名から自動的に生成されます。これは、UNIX スタイルの「/」で区切られた文字列で、デバイスのファイルシステム内のファイルの絶対パスを表します。
エクスポート可能	キーペアは、 <code>exportpkcs12</code> PKI サポートアクションを介してエクスポートできます。作成後は、エクスポート可能フラグの値を変更することはできません。行の削除によってキーペアを削除してから、別のエクスポート可能フラグの値を使用して、エントリを再度作成してください。

PKI トラストポイント

フィールド	説明
名前	トラストポイントの名前またはラベル。
キーペア名	キーペアテーブルからの関連付けられたキーペアの名前。キーペアがまだ関連付けられていない場合、値は長さゼロの文字列になります。

フィールド	説明
Revoke CheckMethods	<p>この信頼ポイント エントリに対応する CA によって発行されたピア証明書を検証する際に使用される証明書失効チェック メソッドの順序付きリストである失効チェック メソッドリスト。このオブジェクトの値は、1つ以上の1オクテット値の順序付けられたリストであり、各1オクテット値は失効チェック メソッド列挙のメソッドに対応します。</p> <ul style="list-style-type: none"> • none (1) - 失効ステータスのチェックは必要ありません。代わりに、証明書は取り消されていないと見なしてください。 • crl (2) - CRL を使用して証明書の失効ステータスを確認します。 • ocsp (3) - 証明書の失効ステータスをチェックするために OCSP を使用します。 <p>リストに何も表示されない場合は、直前の値にする必要があります。順序付けられたリストの最後の値の後のオクテットは、ゼロオクテットでなければなりません。</p> <p>失効チェック メソッドがこのオブジェクトの値内で発生する順序は、ピア証明書の検証中に失効チェック メソッドが試行される順序を決定します。デフォルト値（行作成後）には、失効チェック メソッド crl のみが含まれます。</p>
OCSPUrl	<p>OCSP プロトコルを使用した証明書失効チェックのための外部 OCSP サーバーのコンタクト http URL。デフォルト値（行作成後）は、長さゼロの文字列です。</p>

PKI 信頼ポイントアクション

フィールド	説明
名前	信頼ポイントアクションの名前またはラベル。
コマンド	この信頼ポイント エントリに対してトリガーされる PKI サポート アクション。

フィールド	説明
Url	このエントリでトリガーされる PKI サポートアクションに必要な入力または出力証明書データを含むファイル名を示します。ファイル名は <code>bootflash:<filename></code> として指定する必要があります。また、トリガーされたアクションに応じて、ブートフラッシュで使用可能にするか、ブートフラッシュで作成する必要があります。
パスワード	トリガーされている PKI サポートアクションを実行するために必要なパスワードを示します。このパスワードは、 <code>certreq</code> 、 <code>importpkcs12</code> 、および <code>exportpkcs12</code> アクションに対してのみ指定する必要があります。セキュリティ上の理由から、値は、管理プロトコルによって取得されるときは常に、長さゼロの文字列です。
Last Command	最後に試行された PKI サポートアクション。最後に <code>cpkiAction</code> オブジェクトに設定しようとした値です。信頼ポイントの作成後にアクションがトリガーされていない場合、このオブジェクトの値を取得しても何も返されません。
結果	最後の PKI サポートアクションの実行結果。

PKI LDAP

フィールド	説明
スイッチ	スイッチ名。
Store Type	リモート証明書ストアのタイプ。
CRL Timer (hrs)	CA 証明書に対応する CRL が更新される時間間隔。CA 証明書と対応する CRL は、認証のためにリモート <code>certstore</code> から取得され、ローカル キャッシュに保存されます。後続の認証の時間遅延を回避するためです。
Server Group Name	リモートの <code>certstore</code> 操作に使用されるサーバーグループの名前。

PKI 認定マップ

フィールド	説明
スイッチ	スイッチの名前
フィルタ名	マッピング フィルタ処理の一意の名前。
Subject Name	CA 証明書のサブジェクト名。
Alternate Name Email	AltNameEmail は別の一意のフィールドであり、認証に使用されるサブジェクト名の一部です。
Alternate Name Universal Principal Name	UPN は別の一意のフィールドであり、認証に使用されるサブジェクト名の一部です。

PKI 認定マップ - アプリケーション

フィールド	説明
スイッチ	スイッチ名。
Purpose / Issuer Name	証明書発行者の名前。
Map Name 1	指定された権限と発行者名で証明書に適用される最初のフィルタリング マップの名前。
Map Name 2	特定の権限と発行者名で証明書に適用される 2 番目のフィルタリング マップの名前。

PKI 信頼ポイントの詳細

フィールド	説明
名前	キーペアの名前またはラベル。
IdCert FileName	ID 証明書を格納するファイルの名前。これは、デバイスのファイル システム内のファイルの絶対パスを表す UNIX スタイルの「/」で区切られた文字列です。まだアイデンティティ証明書を取得していない場合、値は長さゼロの文字列になります。
IdCert SubjName	アイデンティティ証明書のサブジェクト名。証明書または証明書にサブジェクト名がない場合、このオブジェクトの値は長さゼロの文字列になります。
IdCert SerialNum	アイデンティティ証明書のシリアル番号。証明書がない場合、このオブジェクトの値は長さゼロの文字列になります。

フィールド	説明
IdCert StartDate	証明書の notBefore フィールドに対応する、ID 証明書が有効になり始める時刻。証明書がない場合、このオブジェクトの値は長さゼロの文字列になります。
IdCert EndDate	証明書の notAfter フィールドに対応する、ID 証明書の有効期間が終了する時刻。証明書がない場合、このオブジェクトの値は長さゼロの文字列になります。
IdCert FingerPrint	16 進数文字列形式の ID 証明書の MD5 fingerprint。証明書がない場合、このオブジェクトの値は長さゼロの文字列になります。
IssuerCert FileName	発行者証明書を格納するファイルの名前。これは、デバイスのファイルシステム内のファイルの絶対パスを表す UNIX スタイルの「/」で区切られた文字列です。発行者証明書がまだ取得されていない場合、このオブジェクトの値は長さゼロの文字列になります。
IssuerCert SubjName	発行者名（発行者証明書のサブジェクト名。存在する場合、ID 証明書の発行者名と同じになります）。証明書がない場合、値は長さゼロの文字列になります。
IssuerCert SerialNum	発行者証明書のシリアル番号。証明書がない場合、値は長さゼロの文字列になります。
IssuerCert StartDate	証明書の notBefore フィールドに対応する、発行者証明書が有効になり始める時刻。証明書がない場合、値は長さゼロの文字列になります。
IssuerCert EndDate	証明書の notAfter フィールドに対応する、発行者証明書の有効期間が終了する時刻。証明書がない場合、値は長さゼロの文字列になります。
IssuerCert FingerPrint	発行者の証明書の MD5 フィンガープリント（HEX 文字列形式）。証明書がない場合、このオブジェクトの値は長さゼロの文字列になります。

IKE グローバル

フィールド	説明
RemIdentity	管理対象デバイスの IKE エンティティが、すべてのピアとともに、この概念的な行に対応する DOI に使用する、キープアライブ インターバルを秒単位で表示します。
キー	管理対象デバイスの IKE エンティティがすべてのピアとともに、この概念的な行に対応する DOI に使用するキープアライブのタイプを表示します。

IKE 事前共有認証キー

フィールド	説明
KeepAliveInterval (sec)	この事前共有キーがローカルエンティティ上で設定されたピアのフェーズ 1 ID。
IdentityType	この概念的な行に対応するピアの認証に使用される事前共有認証キー。

IKE ポリシー

フィールド	説明
プライオリティ	この ISAKMP ポリシー エントリのプライオリティ。小さい値を持つポリシーは、同じ DOI 内の高い値を持つポリシーよりも優先されます。
Encr	この ISAKMP ポリシー仕様によって指定された暗号化トランスフォーム。このポリシー項目を使用するインターネット KeyExchange (IKE) トンネル設定は、指定された暗号化トランスフォームを使用して ISAKMP PDU を保護します。
ハッシュ	この ISAKMP ポリシー仕様によって指定されたハッシュ トランスフォーム。このポリシー項目を使用する IKE トンネル設定は、指定されたハッシュ トランスフォームを使用して ISAKMP PDU を保護します。
Auth	この ISAKMP ポリシー仕様によって指定されたピア認証方式。このポリシー エンティティを選択してピアとネゴシエートする場合、ローカルエンティティは、このオブジェクトによって指定された方法でピアを認証します。

フィールド	説明
DHGroup	メイン モードでの Diffie-Hellman 交換に使用される Oakley グループを指定します。このポリシー項目を選択してメインモードを IKE ピアとネゴシエートする場合、ローカルエンティティは、このオブジェクトによって指定されたグループを選択して、ピアとの Diffie-Hellman 交換を実行します。
Lifetime (sec)	このポリシー仕様を使用して生成された IKE トンネルのライフタイムを秒単位で指定します。

IKE 発信側バージョン

フィールド	説明
アドレス	この概念的な行に対応するリモートピアのアドレス。このオブジェクトは、 <code>cicIkeCfgInitiatorStatus</code> の対応する値がアクティブに等しい間は変更できません。
バージョン	<code>cicIkeCfgInitiatorPAddr</code> で指定されたリモートピアに接続するときに使用される IKE プロトコルバージョン。このオブジェクトは、 <code>cicIkeCfgInitiatorStatus</code> の対応する値がアクティブに等しい間は変更できません。

IKE トンネル

フィールド	説明
LocalAddress	フェーズ 1 トンネルのローカルエンドポイントのアドレス。
RemoteAddress	フェーズ 1 トンネルのリモートエンドポイントのアドレス。
AuthMethod	この概念的な行に対応する制御トンネルのフェーズ 1 ネゴシエーションで使用される認証方式。
アクション	このトンネルに適用するアクション。 <code>clear</code> の場合は、このトンネルがクリアされます。 <code>re-key</code> の場合は、このトンネルに対してキーの再生成が強制されます。このオブジェクトの読み取り後に、値 <code>none</code> が返されます。

IPSEC グローバル

フィールド	説明
Lifetime (sec)	グローバルポリシーとして IPSEC トンネルに割り当てられたデフォルト ライフタイム (秒単位) (特定のクリプトマップ定義で上書きされる可能性がある)。
Lifesize (KB)	グローバルポリシーとして IPSEC トンネルに割り当てられたデフォルト ライフ サイズ (KBytes) (ただし、特定のクリプトマップ定義で上書きされる場合を除く)。

IPSEC トランスフォーム セット

フィールド	説明
Id	トランスフォーム セットを一意に識別するトランスフォームセットのシーケンス番号です。異なるトランスフォームセットは、異なるシーケンス番号を持つ必要があります。
プロトコル	このトランスフォーム セットのフェーズ 2 セキュリティプロトコルのスイートを表します。
ESP暗号化	ESP 暗号化に使用されるトランスフォームを表します。
ESP 認証	ESP プロトコルによる完全性チェックを実装するために使用されるトランスフォームを表します。
モード	トランスフォーム セットのカプセル化モードを表します。

IPSEC クリプト マップ セット エントリ

フィールド	説明
IpFilter	このクリプトマップエントリを使用して保護される IP プロトコルフィルタを指定します。長さ 0 のストリング値を持つ場合は、無効または適用不可です。

フィールド	説明
TransformSetIdList	この CipsStaticCryptomapEntry のメンバである cipsXformSetId のリスト。このオブジェクトの値は、0 個以上の 4 オクテット スtring を連結したものです。各 4 オクテット スtring は 1 つの 32 ビット cipsXformSetId 値を含みます（ネットワークバイトオーダー）。長さ 0 の String 値は、このリストにメンバが含まれないことを意味します。
AutoPeer	true の場合は、トンネルの作成中、宛先アドレスがピアアドレスであると見なされます。
ピアアドレス（Peer Address）	このクリプトマップエントリが現在接続されているピアの IP アドレス。
PFS	このポリシー項目に起因してインスタンス化されたトンネルで完全転送秘密（PFS）を使用するかどうかを識別し、使用する場合は、Oakley のどのグループを使用するかを識別します。
LifeTime	この IPsec ポリシー エントリを使用して作成された IPsec セキュリティ アソシエーション（SA）のライフタイムを指定します。
Lifesize Value	この IPsec ポリシー エントリを使用して作成された IPsec SA のライフサイズ（伝送される可能性がある最大トラフィック（バイト数））を識別します。この IPsec ポリシー エントリを使用してセキュリティ アソシエーション（SA）が作成された場合は、このオブジェクトの値をライフサイズとして取得します。

IPSEC インターフェイス

フィールド	説明
CryptomapName	スタティッククリプトマップテーブルのインデックス。この文字列の値は、クリプトマップセットを定義したときに NMS によって割り当てられた名前の文字列です。
InterfaceList	クリプトマップに属するインターフェイス。

IPSEC トンネル

フィールド	説明
ローカルアドレス (Local Address)	IPSec フェーズ 2 トンネルのローカルエンドポイントの IP アドレス。
RemoteAddress	IPSec フェーズ 2 トンネルのリモートエンドポイントの IP アドレスのタイプ。
ESP暗号化	IPSec フェーズ 2 トンネルのアウトバウンドセキュリティアソシエーションによって使用される暗号化アルゴリズム。
ESP Encryption KeySize	ceipSecTunOutSaEncryptAlgo により示されるアルゴリズムとともに使用されるネゴシエーションキーのキーサイズ (ビット単位)。DES および 3DES のキーサイズは、それぞれ 56 および 168 です。AES の場合は、ネゴシエートされたキーサイズを示します。
ESP 認証	IPSec フェーズ 2 トンネルにおけるインバウンドのカプセル化セキュリティペイロード (ESP) プロトコルのセキュリティアソシエーションによって使用される認証アルゴリズム。
LifeSize (KB)	IPSec フェーズ 2 トンネルのネゴシエートされたライフサイズ (KB 単位)。
LifeTime (sec)	IPSec フェーズ 2 トンネルのネゴシエートされたライフタイム (秒単位)。トンネルを手動で設定した場合、この MIB 要素の値は 0 となっている必要があります。
アクション	MIB テーブル行のステータス。

IP ACL プロファイル

フィールド	説明
名前	固有の IP プロトコルフィルタプロファイル識別子です。
タイプ	このオブジェクトは、このフィルタプロファイルの使用タイプを決定します。この使用タイプは、プロファイルの作成後には変更できません。

IP ACL インターフェイス

フィールド	説明
ProfileName	固有の IP プロトコルフィルタプロファイル識別子です。

IP フィルタ プロファイル

フィールド	説明
操作	deny に設定すると、このフィルタに一致するすべてのフレームが廃棄され、フィルタ リスト残りの部分のスキャンが中止されます。 permit に設定すると、後続のブリッジングまたはルーティング処理に対して、このフィルタに一致するすべてのフレームが許可されます。
プロトコル	このフィルタ プロトコル値は、フレーム内のインターネット プロトコル番号と照合されます。これらの IP 番号は、Network Working Group の Request for Comments (RFC) ドキュメントで定義されています。これを「-1」に設定すると、フィルタリングで任意の IP 番号が一致します。
アドレス	このフィルタで照合される送信元 IP アドレス。0を設定すると、すべての送信元アドレスが一致します。
マスク	一致する必要がある SrcAddress ビットに対するワイルドカードマスクです。このマスクの 0 ビットは、照合に成功するために一致する必要がある SrcAddress の対応するビットを示します。1 ビットは、照合に無関係のビットです。0 を設定すると、SrcAddress と同じ送信元アドレスの IP フレームだけが一致します。
PortLow	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の送信元ポート範囲の下限を指定します。それ以外の場合は、照合中に無視されます。この値は、この SrcPortHigh のエントリに指定した値以下である必要があります。
PortHigh	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の送信元ポート範囲の上限を指定します。それ以外の場合は、照合中に無視されます。この値は、この SrcPortLow のエントリに指定した値以上である必要があります。この値が「0」の場合は、照合中に UDP または TCP ポート番号が無視されます。

フィールド	説明
アドレス	このフィルタで照合される宛先 IP アドレス。 0を設定すると、すべての送信元アドレスが一致します。
マスク	一致させる必要がある DestAddress ビットに対するワイルドカードマスクです。このマスクの 0 ビットは、照合に成功するために一致する必要がある DestAddress の対応するビットを示します。1 ビットは、照合に無関係のビットです。0を設定すると、SrcAddress と同じ送信元アドレスの IP フレームだけが一致します。
PortLow	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の宛先ポート範囲の下限を指定します。それ以外の場合は、照合中に無視されます。この値は、PortHigh でこのエントリに指定した値以下である必要があります。
PortHigh	プロトコルが UDP または TCP の場合は、照合されるトランスポート層の宛先ポート範囲の上限を指定します。それ以外の場合は、照合中に無視されます。この値は、この DestPortLow のエントリに指定した値以上である必要があります。この値が「0」の場合は、照合中に UDP または TCP ポート番号が無視されます。

フィールド	説明
優先順位	<p>各フレーム内の IP トラフィックの優先度パラメータは、特定のネットワークを通じてデータグラムを送信するときに、実際のサービスパラメータの選択を案内するために使用されます。ほとんどのネットワークは、高い優先度のトラフィックを他のトラフィックよりも重要なものとして扱います。IP Precedence 値の範囲は「0」～「7」ですが、「7」が最も優先度が高く、「0」が最も優先度が低くなります。値「-1」は、任意の IP precedence のフレームと一致することを意味します。つまり、この値が「-1」の場合、IP precedence パラメータはチェックされません。優先レベルは次のとおりです。</p> <ul style="list-style-type: none"> • routine(0) : ルーティングトラフィックの優先度 • priority(1) : プライオリティトラフィックの優先度 • immediate(2) : 即時トラフィックの優先度 • flash(3) : フラッシュトラフィックの優先度 • flashOverride(4) : フラッシュ オーバーライドトラフィックの優先度 • critical(5) : クリティカルな優先度 • internet(6) : インターネットワーク制御トラフィックの優先度 • network(7) : ネットワーク制御トラフィックの優先度
TOS	<p>フレームのサービスタイプ (ToS) 。TOS 値の範囲は「0」～「15」です。値「-1」は、任意の TOS 値と一致します。</p>
ICMPType	<p>このフィルタは、照合される ICMP メッセージを指定します。この値を「-1」に設定すると、フィルタリングで任意の ICMP メッセージタイプが一致します。</p>
ICMPCode	<p>このフィルタは、照合される ICMP メッセージコードを指定します。この値を「-1」に設定すると、フィルタリングで任意の ICMP コードが一致します。</p>

フィールド	説明
TCPEstablished	このフィルタが true の場合は、TCP プロトコルで接続が確立されているときに、TCP データグラムが ACK、FIN、PSH、RST、SYN、または URG のコントロールビットセットを持っていると一致と見なされます。false の場合は、任意の TCP データグラムで一致と見なされません。
LogEnabled	フィルタリングサブシステムによってフィルタリングされたフレームが記録されるかどうかを指定します。true の場合は、すべてのフレームが記録されます。false の場合は、いずれのフレームも記録されません。

SSH/Telnet

フィールド	説明
Enable SSH/Telnet	チェックボックスをオンにして SSH または Telnet を有効にします。
NumBits	キーの生成に使用するビット数。これは、SSH によって生成されるキー文字列の長さを決定します。
キー	生成される SSH キー文字列。
LastCreationTime	キーが最後に作成された時刻。
有効	デバイスで Secure Shell (SSH) サービスを有効または無効にします。

ポートセキュリティのアクション

フィールド	説明
アクティベーション	

フィールド	説明
アクション	<ul style="list-style-type: none"> • activate - この VSAN/VLAN 上の有効なポート バインディングがアクティブになります。 • activate (Turn LearningOff) - この VSAN/VLAN 上の有効なポート バインディングがアクティブになり、アクティブ データベースにコピーされます。また、アクティブ化が完了すると、この VSAN/VLAN の自動学習がオフになります。 • force activate - アクティベーション中にエラーが発生した場合でも強制的にアクティベーションが行われ、アクティブになったポート バインディングがアクティブ データベースにコピーされます。 • force activate (Turn Learning Off) - 強制的にアクティベーションが行われ、アクティベーション後に自動学習がオフになります。また、アクティブになったポート バインディングがアクティブ データベースにコピーされます。 • deactivate - この VSAN/VLAN 上で現在アクティブになっている有効なポート バインディング (ある場合) が非アクティブ化されます。アクティブ データベースに含まれていた現在アクティブなエントリ (ある場合) は削除されます。 • 自動学習がイネーブルになっている場合、その VSAN 上でのアクティベーションは許可されません。
有効	この VSAN/VLAN のアクティベーションの状態。true の場合は、この VSAN/VLAN に対する最新の操作として、アクティベーションが試みられています。false の場合は、この VSAN/VLAN に対する最新の操作として、アクティベーションが試みられていません。
結果	最新のアクティベーション/非アクティベーションの結果を示します。

フィールド	説明
最終変更日	この VSAN/VLAN 上の有効なポート バインディングが最後にアクティブ化されたタイミング。エージェントの前の再初期化前に最後のアクティベーションが行われている場合、この値は N/A になります。
CopyActiveToConfig	イネーブルの場合、アクティブポートバインディングデータベースがこの VSAN/VLAN のコンフィギュレーションデータベースにコピーされます。学習済みエントリもコピーされます。
AutoLearn	そのすべてのポート上のローカルデバイスにログイン済みのデバイス/ポートの有効なポートバインディング設定の学習を支援し、前述のアクティブデータベースを同じ内容を入力します。一定期間にわたってローカルデバイスにログイン済みのデバイス/ポートの設定を「学習」して、設定を入力するこのメカニズムは、ユーザーにとって便利なメカニズムです。特定の VSAN でイネーブルになっている場合、その VSAN に対する後続のすべてのログイン (FLOGI) は、その VSAN 上で実行されている既存のポートバインディングと競合しないならば、実行されたポートバインディングデータベースに入力されます。ディセーブルの場合、学習メカニズムは停止します。ただし、学習済みエントリはアクティブデータベースに保存されます。
Clear AutoLearned	
アクション	<ul style="list-style-type: none"> VSAN をクリアすると、この VSAN 上のポートバインド自動学習済みエントリがクリアされます。 インターフェイスをクリアすると、この VSAN 上の指定されたインターフェイスのポートバインド自動学習済みエントリがクリアされます。
インターフェイス	ポートバインド自動学習済みエントリをクリアする必要があるインターフェイスを指定します。

ポートセキュリティ コンフィギュレーション データベース

フィールド	説明
Interface or fWWN	<p>指定したデバイスが FLOGI することができる、ローカル デバイス上のポートのアドレスを表します。</p> <ul style="list-style-type: none"> • fwwn の場合、値はローカルデバイス上のポートのファブリック WWN です。 • intfIndex の場合、ローカル デバイス上のポートはそのインターフェイスによって表されます。 • wildCard の場合、ワイルドカード エントリを表します。ワイルドカードは、ローカル デバイス上の任意のポートを表します。
タイプ	スイッチ ポートを特定するためのメカニズムです。
WWN	ログイン デバイス アドレスを表します。

ポートセキュリティ アクティブ データベース

フィールド	説明
Interface or fWWN	ローカルデバイス上のポートのアドレスです。
タイプ	<p>スイッチ ポートを識別するメカニズム ==</p> <p>fwwn : ローカルスイッチ ポートはファブリック WWN (fWWN) で識別されます。==</p> <p>intfIndex : ローカルスイッチ ポートは intfIndex で識別されます。==</p> <p>wildCard : ワイルドカード (ローカル デバイス上の任意のスイッチ ポート) 。</p>
WWN	ログイン デバイス アドレスを表します。
IsLearnt	このエントリが学習済みエントリかどうかを示します。

ポートセキュリティ データベースの相違点

フィールド	説明
CompareWith	<p>比較するデータベースを指定します。</p> <ul style="list-style-type: none"> • configDb - 構成データベースをこの VSAN/VLAN 上のアクティブ データベースと比較します。そのため、アクティブ データベースがリファレンス データベースとなり、差演算の結果はアクティブ データベースに対するものになります。 • activeDb - アクティブ データベースをこの VSAN/VLAN 上の構成データベースと比較します。そのため、コンフィギュレーション データベースがリファレンス データベースとなり、差演算の結果はコンフィギュレーション データベースに対するものになります。
VSANId	比較対象の VSAN の ID です。
Interface/fWWN	ローカルデバイス上のポートのアドレスです。
タイプ	<p>スイッチ ポートを特定するためのメカニズムです。</p> <ul style="list-style-type: none"> • fwwn - ローカルスイッチポートはファブリック WWN (fWWN) で識別されます。 • intfIndex - ローカルスイッチポートは ifIndex で識別されます。 • wildCard - ワイルドカード (ローカルデバイス上の任意のスイッチポート)。
WWN	ログイン デバイス アドレスを表します。
Reason	このエントリに関する、比較しているデータベース間の相違点の理由を示します。

ポートセキュリティ違反

フィールド	説明
インターフェイス	ログインが拒否されたローカル デバイス上のポートの fWWN です。
エンド デバイス	ローカル デバイスのポートのいずれかで FLOGI が拒否されたデバイスの pWWN です。

フィールド	説明
Or Switch	ローカルデバイスのポートのいずれかでエントリが拒否されたデバイスの sWWN です（デバイスがスイッチの場合）。
時間	ログインが拒否された時刻です。
応答数	この特定の pWWN/nWWN または sWWN が、この特定のローカルインターフェイスでログインを拒否された回数です。

ポートセキュリティ統計情報

フィールド	説明
AllowedLogins	この VSAN/VLAN で許可された FLOGI 要求の数です。
DeniedLogins	この VSAN/VLAN で拒否された FLOGI 要求の数です。
クリア	Clear に設定すると、この VSAN/VLAN 上のポートバインド統計情報カウンタがクリアされます。

IPsec

フィールド	説明
[Interface]、[CryptomapName]	管理対象エンティティのインターフェイスへ、クリプトマップセットのバインディングを設定します。

イベント

Call Home 一般

フィールド	説明
連絡先	このスイッチの連絡先担当者。この担当者への連絡方法に関する情報も含む。
PhoneNumber	連絡先担当者の電話番号。電話番号は、「+」で始まり、空白と「-」以外はすべて数字にする必要があります。+44 20 8332 9091、+45 44886556、+81-46-215-4678、+1-650-327-2600 などの電話番号が有効です。
EmailAddress	連絡先担当者の電子メールアドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などの電子メールアドレスが有効です。
StreetAddress	このスイッチの送付先住所です。
CustomerId	お客様を識別するための任意の適切な形式の文字列です。

フィールド	説明
ContractId	お客様とサポートパートナーの間のサポート契約を識別するための任意の適切な形式の文字列です。
SiteId	このデバイスのロケーション ID です。
DeviceServicePriority	デバイスのサービスプライオリティです。これにより、デバイスにサービスが提供される速さが決定されます。
有効	ローカルデバイスで CallHome インフラストラクチャを有効または無効にします。

Call Home 宛先

フィールド	説明
プロファイル名、ID	宛先プロファイルを識別する名前。
タイプ	送信方式のタイプ。
EmailAddress	この宛先プロファイルに関連付けられる電子メールアドレス。 raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
Http Url	この宛先プロファイルに関連付けられた HTTP URL。

Call Home 電子メール セットアップ

フィールド	説明
送信元	SMTP を使用して電子メールを送信する際に、[From] フィールドに使用される電子メールアドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
返信先	SMTP を使用して電子メールを送信する際に、[Reply-To] フィールドに使用される電子メールアドレス。raj@helpme.com、bob@service.com、mtom@abc.caview.ca.us などになります。
IP アドレスタイプ	IP アドレス タイプ (IPv4、IPv6、または DNS)。
Name or IP Address	SMTP サーバの名前または IP アドレス。
ポート	SMTP サーバの TCP ポート。

Call Home アラート

フィールド	説明
操作	[テスト (Test)] : Call Home メッセージを送信 TestWithInventory - インベントリの詳細付きメッセージを送信します。
ステータス	最後の callhome アクション呼び出しのステータス。
FailureCause	最後の callhome テスト呼び出しの失敗原因。
LastTimeSent	最後の CallHome アラートが送信された時刻。
NumberSent	送信された CallHome アラートの数。
すべて	定期的なソフトウェア インベントリ Call Home メッセージを送信するためのタイム フレーム。
Throttling Enable	オンの場合、システムに実装されているメッセージスロットリングメカニズムがイネーブルになり、一定のタイムフレーム内での特定のアラートタイプの callhome メッセージの数が制限されます。最大は2時間のタイムフレーム内で 30 件であり、それ以上のそのアラートタイプのメッセージは廃棄されます。
有効	オンの場合、システム上での定期的なソフトウェア インベントリ callhome メッセージの送信がイネーブルになります。

Call Home HTTP プロキシ サーバ

フィールド	説明
マスター	スイッチ名。
アドレスタイプ	HTTP プロキシ サーバー アドレスの値で表される HTTP プロキシ サーバーのタイプ。
アドレス	HTTP プロキシ サーバーのアドレス。
ポート	HTTP プロキシ サーバーのポート。
有効	HTTP 経由で callhome メッセージを送信するように構成された HTTP プロキシ サーバーの使用を有効または無効にします。

Call Home SMTP サーバ

フィールド	説明
[Address Type]、[Address]	SMTP サーバの IP アドレス。
ポート	SMTP サーバの TCP ポート。
プライオリティ	優先値

Call Home ユーザ定義コマンド

フィールド	説明
User Defined Command	callhome アラート グループ タイプのユーザー定義コマンドを構成します。

遅延トラップ

フィールド	説明
[有効 (Enable)]	遅延トラップを有効または無効にします。
遅延	分単位の遅延時間 (有効な値の範囲は1～60)

Call Home プロファイル

フィールド	説明
MsgFormat	XML、フルテキスト、またはショートテキスト。
MaxMsgSize	この宛先プロファイルで示される宛先に送信可能な最大メッセージサイズ。
MsgLevel	しきい値レベル。宛先に送信されるアラートメッセージのフィルタリングに使用されます。設定されたしきい値レベルよりも低い重大度の Callhome アラートメッセージは送信されなくなります。デフォルトのしきい値レベルはデバッグ (1) です。この場合、すべてのアラートメッセージが送信されます。
AlertGroups	この宛先プロファイルに設定されているアラートグループのリスト。

イベント宛先アドレス

フィールド	説明
Address/Port	イベントを送信する IP アドレスとポート。
[セキュリティ名 (Security Name)]	このアドレスに送信されるメッセージを生成する際に使用される SNMP パラメータ。
セキュリティモデル	このエントリを使用して SNMP メッセージを生成する際に使用されます。
Inform Type	<ul style="list-style-type: none"> • Trap : 未確認応答イベント • Inform : 確認応答イベント

フィールド	説明
Inform Timeout	アドレスと通信するためのこの予想最大往復時間。
RetryCount	生成したメッセージに対する応答が受信されない場合に行われる再試行の回数。
ステータス	<ul style="list-style-type: none"> • Active - ポートはアクティブです。 • NotInService - ポートはサービス停止中です。

イベント宛先セキュリティ (詳細)

フィールド	説明
MPModel	このエントリを使用して SNMP メッセージを生成する際に使用されるメッセージ処理モデル。
SecurityModel	このエントリを使用して SNMP メッセージを生成する際に使用されるセキュリティモデル。
SecurityName	このエントリを使用して SNMP メッセージが生成される対象者を識別します。
SecurityLevel	このエントリを使用して SNMP メッセージを生成する際に使用されるセキュリティレベル。

イベント フィルター 一般

フィールド	説明
FSPF - Nbr State Changes	ローカルスイッチが VSAN 上のインターフェイスでネイバーの状態 (FSPF ネイバー有限状態マシンの状態) の変化を検出したときに通知を発行するかどうかを指定します。
Domain Mgr - ReConfig Fabrics	ローカルスイッチが VSAN 上での ReConfigureFabric (RCF) の送受信時に通知を発行するかどうかを指定します。
Zone Server - Request Rejects	ゾーン サーバーが拒否時に通知を発行するかどうかを指定します。
Zone Server - Merge Failures	ゾーン サーバがマージ失敗時に通知を発行するかどうかを指定します。
Zone Server - Merge Successes	ゾーン サーバがマージ成功時に通知を発行するかどうかを指定します。
Zone Server - Default Zone Behavior Change	伝播ポリシーが変化した場合にゾーン サーバが通知を発行するかどうかを指定します。

フィールド	説明
Zone Server - Unsupp Mode	ゾーンサーバが unsupp モードの変化時に通知を発行するかどうかを指定します。
FabricConfigServer - Request Rejects	ファブリック コンフィギュレーションサーバが拒否時に通知を発行するかどうかを指定します。
RSCN - ILS Request Rejects	SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
RSCN - ILS RxRequest Rejects	SW_RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
RSCN - ELS Request Rejects	SCR または RSCN 要求が拒否されるときに RSCN モジュールが通知を生成するかどうかを指定します。
FRU Changes	false 値の場合、このシステムによって現場交換可能ユニット (FRU) の通知は生成されません。
SNMP - Community Auth Failure	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。
VRRP	VRRP 対応ルータがこの MIB に定義されているイベントに対して SNMP トラップを生成するかどうかを示します。
FDMI	登録要求が拒否されるときに FDMI が通知を生成するかどうかを指定します。
ライセンスマネージャ	システムが通知を生成するかどうかを示します。
Port/Fabric Security	ポート/ファブリックセキュリティの問題が発生したときにシステムが通知を生成するかどうかを指定します。
FCC	エージェントが通知を生成するかどうかを指定します。
ネーム サーバ	オンの場合、要求が拒否されたときにネームサーバが通知を生成します。オフの場合、通知は生成されません。

イベント フィルタ インターフェイス

フィールド	説明
EnableLinkTrap	このインターフェイスに対して linkUp/linkDown トラップが生成されるかどうかを示します。

イベント フィルタ 制御

フィールド	説明
変数	制御される通知を表します。
説明	通知に関する説明。
有効	オンにすると、コントロールの通知がイネーブルになります。コントロールのステータスを表示します。



(注) [説明 (Descr)] 列は、Cisco NX-OS Release 5.0以降が動作しているスイッチ上でのみ表示されます。

リンク インシデント履歴

フィールド	説明
Host Time	ホストのローカル時間。
Switch Time	スイッチのローカル時間。
ポート	リンク インシデントのポート番号。
インターフェイス	指定されたポートのファイバチャネルインターフェイス。
Link Incident	発生したインシデントのタイプ。

RMON しきい値制御

フィールド	説明
AlarmEnable	true の場合、RMON アラーム機能はイネーブルになります。RMON 機能をディセーブルにすると、RMON アラームに関連したポーリングはすべて停止されます。これは、RMON の CPU 使用率が悪影響を及ぼすことがないようにするために、RMON アラーム機能を一時的にディセーブルにする場合にのみ使用します。この機能を永続的にディセーブルにする場合は、alarmTable 内のすべてのエントリを削除することが推奨されます。
MaxAlarms	alarmTable の最大許容エントリ数。

RMON しきい値 64 ビット アラーム

フィールド	説明
間隔	データを上昇しきい値および下限しきい値と比較するためのデータのサンプリング間隔の秒数。deltaValue サンプリングの場合、この変数を設定する際に注意が必要です。サンプリングされた変数が 1 つのサンプリング間隔において $2^{31} - 1$ を上回る幅で増減することがないように、間隔を十分短く設定する必要があります。
変数	サンプリングされる変数です。INTEGER (INTEGER、Integer32、Counter32、Counter64、Gauge、または TimeTicks) の ASN.1 プリミティブ型になる変数のみがサンプリングされます。
SampleType	選択された変数のサンプリング方式、およびしきい値と比較される値の計算方式。この値が absoluteValue の場合、選択された変数の値は、サンプリング間隔の終了時にしきい値と直接比較されます。この値が deltaValue の場合、選択された変数の直前のサンプリング値が現在の値から減算され、その差がしきい値と比較されます。

フィールド	説明
値	最後のサンプリング期間の統計値。たとえば、サンプルタイプが <code>deltaValue</code> の場合、この値は、その期間の開始時のサンプルと終了時のサンプルの差となります。サンプルタイプが <code>absoluteValue</code> の場合、この値は、その期間の終了時にサンプリングされた値となります。この値が、上昇しきい値および下限しきい値と比較されます。現在のサンプリング期間の値は、その期間が完了すると使用可能になり、次の期間が完了するまで使用できます。
StartupAlarm	このエントリが初めて有効に設定されたときに送信されるアラーム。
上昇しきい値	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以上で、最後のサンプリング期間の値がこのしきい値未満であった場合、単一のイベントが生成されます。
Rising EventId	上昇しきい値を超えたときに使用される <code>eventEntry</code> の ID。
下降しきい値	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以下で、最後のサンプリング期間の値がこのしきい値を超えた場合、単一のイベントが生成されます。
Falling EventId	下限しきい値を下回ったときに使用される <code>eventEntry</code> の ID。このインデックスの値で識別される <code>eventEntry</code> は、そのインデックスと同じ値の <code>eventIndex</code> で識別されるものと同じです。 <code>eventTable</code> 内に対応するエントリがない場合、関連付けは存在しません。特に、この値が N/A の場合、N/A は有効なイベントインデックスではないので、関連するイベントが生成されることはありません。
FailedAttempts	アラーム変数がポーリングされ（アクティブ状態）、応答が受信されなかった回数。
オーナー	このエントリを設定したユーザの ID。

RMON しきい値 32 ビット アラーム

フィールド	説明
間隔	データを上昇しきい値および下限しきい値と比較するためのデータのサンプリング間隔の秒数。deltaValue サンプリングの場合、この変数を設定する際に注意が必要です。サンプリングされた変数が 1 つのサンプリング間隔において $2^{31} - 1$ を上回る幅で増減することがないように、間隔を十分短く設定する必要があります。
変数	サンプリングされる変数です。INTEGER (INTEGER、Integer32、Counter32、Counter64、Gauge、または TimeTicks) の ASN.1 プリミティブ型になる変数のみがサンプリングされます。
SampleType	選択された変数のサンプリング方式、およびしきい値と比較される値の計算方式。
値	最後のサンプリング期間の統計値。
StartupAlarm	このエントリが初めて有効に設定されたときに送信されるアラーム。
上昇しきい値	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以上で、最後のサンプリング期間の値がこのしきい値未満であった場合、単一のイベントが生成されます。
Rising EventId	上昇しきい値を超えたときに使用される eventEntry の ID。
下降しきい値	サンプリングされた統計値に対するしきい値。現在のサンプリング値がこのしきい値以下で、最後のサンプリング期間の値がこのしきい値を超えた場合、単一のイベントが生成されます。
Falling EventId	下限しきい値を下回ったときに使用される eventEntry の ID。
FailedAttempts	アラーム変数がポーリングされ (アクティブ状態)、応答が受信されなかった回数。
オーナー	このエントリを設定したユーザの ID。

RMON しきい値イベント

フィールド	説明
説明	このイベント エントリを説明しているコメント。
タイプ	プローブがこのイベントに関して行う通知のタイプ。ログの場合、イベントごとにエントリがログ テーブルに作成されます。SNMP トラップの場合、SNMP トラップが 1 つ以上の管理ステーションに送信されます。
コミュニティ	コミュニティ スtring。
LastTimeSent	このイベント エントリによりイベントが最後に送信された時刻。このエントリがイベントを 1 つも生成していない場合、この値は N/A になります。
オーナー	このエントリを設定したエンティティ。このエントリに割り当てられたリソースを使用します。

RMON しきい値ログ

フィールド	説明
時間	このログ エントリが作成された時刻。
[説明 (Description)]	このログ エントリをアクティブにしたイベントの説明。

管理者

設定のコピー

フィールド	説明
送信元	コピー元のファイルのタイプを指定します。
送信先	コピー先のファイルのタイプを指定します。
ServerAddress	構成ファイルのコピー元（またはコピー先）のサーバーの IP アドレス。
ファイル名	ファイルのファイル名（該当する場合はパスを含む）。
プロトコル	コピーに使用されるプロトコル。
UserName	リモート ユーザー名。
UserPassword	リモート ユーザーのパスワード
CopyState	この構成コピー要求の状態を指定します。このオブジェクトの値は、行がインスタンス化された後にのみインスタンス化されます。たとえば、CopyEntryRowStatus がアクティブになった後です。

フィールド	説明
CopyFailCause	config-copy 操作が失敗した理由。このオブジェクトは、このエントリの CopyState が失敗状態になった場合にのみインスタンス化されます。

フラッシュファイル

フィールド	説明
名前	ファイル内でコピーしているユーザーが指定したフラッシュファイル名。
Size (B)	ファイルのサイズ (バイト単位)。このサイズには、ファイルシステムのファイルヘッダーのサイズが含まれていないことに注意してください。
変更日	ファイルの最終変更日時。

コンパクトフラッシュ

フィールド	説明
デバイス	デバイスの名前。
パーティション (Partition)	パーティションを参照するために使用されるフラッシュパーティション名。
サイズ	パーティションのサイズ。

ライセンス機能

フィールド	説明
欠落	ローカルシステムに、この機能のライセンスを含む1つ以上のインストール済みライセンスファイルがない場合、この機能の不足している使用ライセンスの数を示します。通常の状態では、値は0です。
Installed Type	demo、permanent、counted、unlicensed、inGracePeriod ライセンスの組み合わせ。
Installed Count	このライセンス機能の最大同時使用数。これは、この機能のライセンス情報を含む、インストールされているすべてのライセンスファイルから取得した、この機能の累積ライセンス使用可能数です。
ステータス	このライセンスされた機能の現在の使用数を表します。
ExpiryDate	ライセンスされた機能の有効期限です。
GracePeriod	この機能の残りの猶予期間を表します (日/秒)。猶予期間は、ライセンスのない機能またはライセンスの期限が切れた機能の、実行が許可される時間です (秒単位)。
エラー	エラー (存在する場合)。

フィールド	説明
DefaultLicenses	デフォルトで含まれるこのライセンス機能の最大同時使用数。

ライセンス マネージャ キー

フィールド	説明
LastModified	ライセンス ファイルの内容が最後に変更された時刻を表します。
機能	インストールされたライセンス ファイル名を指定します。
バージョン	ライセンス ファイルのバージョン番号。
タイプ	<ul style="list-style-type: none"> • permanent - 永久ライセンスを示します。
応答数	<ul style="list-style-type: none"> • uncounted - この機能のカウントされないライセンス数を指定しました。 • counted - このライセンス機能の同時使用の最大数を示します。

ライセンス マネージャのインストール

フィールド	説明
ホストID	ローカル システムのライセンス ホスト ID が含まれます。このシステムのライセンスを要求するときに、ローカル システムを識別するために使用されます。
URI	インストール用にライセンス ファイルが選択されるローカル システム上の保存場所を表します。CISCO-CCO またはその他の方法 (CLI など) で入手したライセンス ファイルを、この場所にコピーしておく必要があります。たとえば、値は「bootflash:licfile1」のようになります。これは、「インストール」する前に有効な値に設定する必要があります。アンインストール操作の場合、値は関係ありません。
Target Filename	ライセンス ファイルのインストールに使用する名前、またはアンインストールするライセンス ファイルの名前を表します。

ステータス	
-------	--

ライセンスのインストール/アンインストール操作のステータス。

- **success (1)** : インストール/アンインストール操作が正常に完了しました。 **InProgress (2)** - ライセンスのインストール/アンインストール操作が進行中です。
- **corruptedLicenseFile (3)** - ライセンス ファイルの内容が無効/破損しています。
- **targetLicenseFileAlreadyExist (4)** - ターゲットライセンスファイル名がすでに存在しています。
- **invalidLicenseFileName (5)** - ライセンスファイルが存在しません。
- **duplicateLicense (6)** - ライセンスファイルは既にインストールされています。
- **licenseInUse (7)** - 使用中のライセンスファイルをアンインストールできません。
- **generalLicensingFailure (8)** - License Manager からの一般的なエラーです。
- **none (9)** - インストール/アンインストール操作は実行されません。
- **licenseExpiryConflict(10)** - 機能に対応した、有効期限の異なるライセンスが存在しています。
- **invalidLicenseCount(11)** - 機能に対応した、ライセンス数が無効です。
- **notThisHost (12)** - ライセンスファイルのライセンス ホスト ID が一致しません。
- **licenseInGraceMore(13)** - 猶予期間内のライセンス数がインストールライセンスファイル内の値を超えています。
- **licenseFileNotFound(14)** - インストール、アンインストール、または更新処理用のライセンスファイルが見つかりません。
- **licenseFileMissing (15)** - インストール済みライセンスファイルがないことがわかりました。
- **licenseFileMissing (15)** - インストール済みライセンスファイルがないことがわかりました。
- **invalidLicenseFileExtension (16)** - ライセンスファイルに .lic 拡張子がありません。
- **invalidURI (17)** - インストール処理で指定

	<p>したライセンス ファイル URI が無効です。</p> <ul style="list-style-type: none"> • noDemoLicenseSupport (18) - デモ ライセンスはサポートされていません。 • invalidPlatform (19) - 無効なプラットフォーム
--	--

ライセンス マネージャの使用状況

フィールド	説明
名前	機能をチェックアウトしたアプリケーションの名前を示します。
アプリケーション	機能をチェックアウトしたアプリケーション。

ポート ライセンス

フィールド	説明
Id	ローカルシステムのライセンス ホスト ID を表示します。ライセンスを要求するときに、ローカルシステムを識別するために使用されます。
最大	このライセンスの最大同時使用数。
使用済み	このライセンスされた機能の現在の使用数を表します。

機能セット

フィールド	説明
名前	機能制御セットの名前。
OpStatus	機能の現在の運用状況です。
アクション	機能セットに対して実行されるアクション。
LastCommand	機能に対してトリガーされるアクション。
結果	機能セットに適用された最後のアクションの結果。

[機能制御 (Feature Control)]

フィールド	説明
機能名	機能の名前。
ステータス	機能の現在の運用状況。
アクション	機能を有効または無効にします。

フィールド	説明
LastCommand	機能の最後のアクションの結果。
結果	機能に対してトリガーされた最後のアクションの実行が失敗した理由の説明。

NTPサーバ

フィールド	説明
IP アドレスタイプ	ピアの IP アドレス タイプ (IPv4 または IPv6)。
Name or IP Address	ピアの名前または IP アドレス。
モード	<p>NTP サーバーのアソシエーション モード。値は次のようにコーディングされます。</p> <p>ピア：このモードで動作しているホストは、ピアの到達可能性の状態や階層に関係なく、定期的にメッセージを送信します。このモードで動作することにより、ホスト（通常は LAN ワークステーション）は、ピアに基づいて同期される用意があることを通知しますが、ピアを同期させることはありません。</p> <p>サーバー：このタイプの関連付けは、通常、クライアント要求メッセージの到着時に作成され、その要求に応答するためにのみ存在します。その後、関連付けは解消されます。このモードで動作することにより、ホスト（通常は LAN タイム サーバー）は、ピアを同期させる用意があることを通知しますが、ピアに基づいて同期されることはありません。</p>
優先 (Preferred)	このピアが他のピアよりも優先されるかどうかを指定します。デフォルトでは、NTP は、ローカル システム上にあるピアで、時刻を同期するものを選択します。true の場合、NTP は、対応するピアを時刻の同期相手として選択します。複数のエントリが true の場合、NTP は最初に設定するエントリを選択します。

NTP 全般

フィールド	説明
LEAP	NTP 時間スケールへのうるう秒の挿入が間近に迫っていることを示す、2 ビット コードの警告です。
RootDelay	同期サブネットの起点にあるプライマリリファレンス ソースへのラウンドトリップ遅延 (秒単位) を示す符号付き固定小数点数。
RootDispersion	同期サブネットの起点にあるプライマリリファレンス ソースとの最大誤差 (秒単位) 。

実行中のプロセス

フィールド	説明
名前	このプロセスに関連付けられた名前。名前が 32 文字を超える場合、最初の 31 文字に切り捨てられ、最後の文字として「*」が追加されます。これにより、プロセス名が切り捨てられていることを示します。
MemAllocated (B)	このプロセスがシステムから動的に割り当てられているすべてのメモリの合計。これには、すでにシステムに返されたメモリが含まれている場合があります。
CPU Time (us)	プロセスが使用した CPU 時間 (ミリ秒)

起動時/実行構成の表示

フィールド	説明
新興企業	スイッチの起動時構成を、指定されたファイル名で別のコンピュータにバックアップします。
Running	スイッチの実行構成を、指定されたファイル名で別のコンピュータにバックアップします。
TCPタイムアウト	タイムアウトする前に TCP 接続の確立を待機する時間の値 (秒単位)。有効な値は 1 ~ 120 です。タイムアウトが発生すると、バックアップアクションは中止されます。
ファイル名	バックアップの詳細が保存されるファイルの名前を指定します。

フィールド	説明
ファイルの圧縮	[ファイルを圧縮 (Compress File)] チェックボックスをオンにして、バックアップ ログ ファイルを圧縮します。

EPLD のバージョンの表示

フィールド	説明
イメージ URI	イメージの URI。
結果	URI で指定されたイメージのバージョン。

フラッシュ ファイルのコピー

フィールド	説明
方向	ファイル転送の方向を指定します。
プロトコル	コピーに使用するプロトコル。
ServerAddress	使用するサーバー アドレス。
RemoteUserName	FTP、SFTP、および SCP プロトコルのリモート ユーザー名。
RemotePassword	FTP、SFTP、または SCP で使用されるリモート ユーザーのパスワード。
Server File	<p>コピーコマンドのタイプに応じて、フラッシュまたはサーバー上のサーバー ファイル名。必須。フラッシュからコピーする場合：ファイル名は [device>:[:]] の形式で指定する必要があります。FlashDeviceName から取得した値、FlashPartitionName から取得した値、フラッシュ内のファイル名を使用します。xFTP プロトコルを使用してファイルをコピーする場合、サーバー ファイルの場所は xFTP ルートパスからの相対パスで指定しなければならないことがあります。</p> <p>注 必要に応じて、ファイルパスを手動で変更する必要がある場合があります。</p>

フィールド	説明
スイッチ ファイル (Switch File)	スイッチのファイル名。フラッシュにコピーする場合：ファイル名は {device>:[:] の形式で指定する必要があります。FlashDeviceName から取得した値、FlashPartitionName から取得した値、および埋め込まれたコロン文字のない任意の文字列を使用します。

TAC Pac ファイルの生成

Tac-Pac は .zip形式のファイルとしてダウンロードできます。

フィールド	説明
プロトコル	
TCPタイムアウト	タイムアウトする前に TCP 接続の確立を待機する値 (分単位)。有効値は 1 ~ 60 です。タイムアウトは、バックアップアクションの打ち切りを導きます。
管理インターフェイス	インターフェイスのタイプを選択します。次のオプションを使用できます。 <ul style="list-style-type: none"> • デフォルト • vrf management • vrf default
ServerAddress	使用するサーバーアドレス。
UserName	リモート ユーザー名。
UserPassword	リモート ユーザーのパスワード
ファイル名	show tech support information がキャプチャされるファイルの名前。

技術サポートの表示

フィールド	説明
TCPタイムアウト	タイムアウトまでに CLI を待機する秒数。
ファイル名	show tech support information がキャプチャされるファイルの名前。
ファイルの圧縮	テキスト ファイルを ZIP ファイルに圧縮するには、チェックボックスをオンにします。

イメージのバージョンの表示

フィールド	説明
画像 URL	イメージの URL。
結果	指定された URL にあるイメージのバージョン。

オンボード ログの表示 (Show Onboard Log)

フィールド	説明
ログのフィルタ条件	
モジュール番号	シャーシに挿入されているカードのロット番号。
開始日	開始日時を指定します。
終了日	終了日時を指定します。
オンボードログ出力表示をファイルにキャプチャ	
TCPタイムアウト	ドロップダウンリストからタイムアウト間隔を指定します。
ファイル名	ログファイルの名前。
ファイルの圧縮	ログファイルを圧縮するには、[ファイルの圧縮 (Compress File)] チェックボックスをオンにします。

一覧ビュー

フィールド	説明
説明	ネットワーク マネージャによって指定されたインターフェイスのエイリアス名。ポートチャネルと FCIP の場合、このフィールドは、メンバーが使用可能な場合は常にメンバーを表示します。FCIP の場合、圧縮されていれば、このフィールドには <code>compress</code> と表示されます。
VSAN(s)	VSAN メンバーシップ。
モード	ポートの動作モード> (凡例を参照)。

フィールド	説明
接続先	<p>アタッチされたポート。これは、ホスト、ストレージ、またはスイッチポートである可能性があります。</p> <p>(注) デバイスマネージャは、一度に1つのスイッチを接続して管理します。NPVスイッチ接続情報を持つスイッチがコアスイッチに保存されており、NPVスイッチを表示するように選択した場合、[接続先情報 (Connected To)] は表示されません。</p>
スピード	最大帯域幅 (Gbps)
Rx	<p>次のいずれかが必要です。</p> <p>使用率 %</p> <p>バイト数</p> <p>フレーム数</p> <p>平均フレーム サイズ</p>
Tx	<p>次のいずれかが必要です。</p> <p>使用率 %</p> <p>バイト数</p> <p>フレーム数</p> <p>平均フレーム サイズ</p>
エラー	<p>インターフェイス上の Rx および Tx エラーの総数。Rx エラーのタイプには、CRC エラー、フレームの分断化、サポートされていないクラス フレーム、Runt フレーム、Jabber フレーム、ジャイアント フレームなどがあります。Tx エラーのタイプは一般に CRC エラーですが、発生するのはまれです。[エラー (Errors)] フィールドが空でない場合は、Rx エラーが発生している可能性があります。エラーカウンターの詳細な内訳については、適切なインターフェイスの [モニタ (Monitor)] ダイアログボックスを確認してください。</p>

フィールド	説明
破棄	インターフェイスでの Rx と Tx の破棄の合計数。Rx フレームの破棄は、通常、プロトコルエラーが原因です。まれに、ハードウェアエラーなしでフレームが受信されたにもかかわらず、MAC アドレスに設定されているフィルタリングルールの不一致により、フレームが破棄されることがあります。Tx フレームが破棄された場合には、タイムアウト フレーム破棄（ポートがオフラインまたはアップしていない）か、スーパーバイザに返送されなかったタイムアウト フレーム（クラス F/2 フレーム）の可能性があります。[破棄 (Discards)] フィールドが空でない場合は、タイムアウト フレームが原因である可能性があります。
ログ	オンにすると、ポーリング間隔ごとにレコードをメッセージ ログに書き込みます。

RLIR ERL

フィールド	説明
Vsan ID	ポートの VSAN 識別子。
FC ID	サブスクライブしている Nx_Port のファイバチャネル識別子。
フォーマット	Nx_Port が RLIR ELS を受信するデバイスタイプ。
RegType	サブスクライバの登録タイプ。 <ul style="list-style-type: none"> • ConditionalRx : VSAN 上の ERL からの他の受信者が選択されていない場合にのみ、Nx_Port はリンク インシデント レコードの受信者になります。 • AlwaysRx : Nx_Port は、常にリンク インシデント レコードの受信者として選択されます。

優先ホスト

フィールド	説明
Vsan ID	ポートの VSAN 識別子。

優先経路 (Preferred Path)

PreFcid	サブスクライブする Nx_Port の優先ファイバチャネル識別子。
---------	-----------------------------------

優先経路 (Preferred Path)

フィールド	説明
インターフェイス	一致した、または分類されたフレームが転送されるローカルデバイス上のインターフェイスを表します。
VSAN Id	この FC ルートマップの VSAN ID。この FC ルートマップ内のルートを識別する任意の整数値。優先レベル。優先パスのメトリックまたはコストを示します。数値が低いほど優先度が高くなります。
DestinationDomain	
FCID	フロー分類のソース アドレスと一致させる必要がある FC ID。
[説明 (Description)]	
プライマリ ISL	
セカンダリ ISL	

Edit iSCSI Advertised Interfaces

フィールド	説明
Num	iSCSI ターゲットの数。
インターフェイス	ターゲットをアダプタイズするインターフェイス。

DNS 全般

フィールド	説明
[有効 (Enable)]	DNS 構成を有効または無効にします。
ドメイン名	DNS サーバーが有効になっているドメインの名前。

DNS サーバ (DNS Servers)

フィールド	説明
[IP アドレス (IP Address)]	DNS サーバーの IP アドレス。

Cisco Fabric Services (CFS) の機能

フィールド	説明
Globally Enabled	このチェックボックスをオンにすると、このスイッチ上の CFS は機能の設定を他のスイッチに配信できるようになります。このチェックボックスをオフにすると、CFS は他のスイッチに設定を配信できなくなります。
機能	CFS 対応機能の名前。
ステータス	CFS 対応機能のステータス。
コマンド	機能に対してトリガーされるアクション。アクションには次のものがあります。 <ul style="list-style-type: none"> • noop - 操作なし。 • enable - スイッチでの CFS 配信を有効にします。 • disable - スイッチでの CFS 配信を無効にします。 • commit - セッション開始以降に行われた変更をコミットします。 • abort - 行われた変更を破棄し、セッションを閉じます。 • clear - 行われた変更を破棄しますが、セッションは閉じません。
タイプ	使用された最後の CFS 機能スコープタイプ。
VSAN Id	この機能が動作中の VSAN の ID。
RegionId	この CFS 対応機能がマッピングされている配信リージョン ID。このリージョンは、その使用よりも前に定義される必要があります。
View Config Changes As	変更が実行と保留のいずれであるかを決定します。保留コンフィギュレーションは、その機能に対してコミットまたは中断のアクションがトリガーされるまで存在します。この値が [running] の場合、この機能の後続のすべての設定取得は、ローカル デバイス上の実行コンフィギュレーションから行われます。この値が [pending] の場合、この機能の後続のすべての設定取得は、ローカル デバイス上の保留コンフィギュレーションから行われます。
LastCommand	この機能に対して実行された最後のアクション。

フィールド	説明
結果	CFS 対応機能に対して実行されたアクションの結果。
範囲	このオブジェクトの値は、CFS インフラストラクチャに登録されている CFS 対応機能の属性を表します。 <ul style="list-style-type: none"> • fcFabric - 機能の CFS ベースの配信が FC (ファイバチャネル) ファブリック全体にわたることを示します。 • ipNetwork - 機能の CFS ベースの配信が IP ネットワーク全体にわたることを示します。 • vsanScope - 機能の CFS ベースの配信が VSAN 単位で行われ、FC (ファイバチャネル) ファブリック内の特定の VSAN に制限されることを示します。
PendingConfOwnerAddr	機能に対する保留コンフィギュレーションが存在する、ファブリック内のデバイスのアドレス。
所有者スイッチのロック	この範囲内の機能に対する保留構成が存在する、ファブリック内のデバイスのアドレス。
Lock Owner UserName	この範囲内の機能に対する保留構成が存在する、ファブリック内のデバイスの名前。

フィールド	説明
結合ステータス	<p>システムのスコープタイプとスコープ値の組み合わせのコンテキスト内での、この機能の最後のファブリック マージの結果。結果は次のとおりです。</p> <ul style="list-style-type: none"> • Success : ファブリックのマージが正常に完了しました。 • InProgress : ファブリックのマージが進行中です。このステータスは、ファブリックの一部であるローカルデバイスが別のファブリックとのマージプロセスに関与している場合に発生することがあります。 • Failure : ファブリックのマージに失敗しました。 • Waiting : 競合が解消されている間、既存のマージが完了するのを待機しています。ファブリックの一部であるローカルデバイスが、ファブリック マージの新しいインスタンスを開始する前に、競合が解決されるのを待機している場合、このステータスが表示されることがあります。 • Other : ここに列挙した他のどの値にも該当しません。
マスター	CFS マスター スイッチを選択します。

Cisco Fabric Services (CFS) の IP マルチキャスト

フィールド	説明
IP アドレスタイプ	IP アドレスタイプ (IPv4、IPv6、または DNS)。

フィールド	説明
Multicast Address Domain	CFS 配信が制限されるマルチキャストアドレスドメイン。IP で CFS 対応スイッチを検出するためにキープアライブメッセージが送受信されるデフォルトのマルチキャストアドレスが IPv4 と IPv6 の両方に存在します。同じマルチキャストアドレスを持つすべてのスイッチが 1 つの CFS-over-IP ファブリックを構成します。IPv4 のデフォルトのマルチキャストアドレスは 239.255.70.83 で、サポートされる範囲は 239.255.0.0 ~ 239.255.255.255 です。IPv6 のデフォルトのマルチキャストアドレスは ff13::7743:4653 で、サポートされる範囲は [ff13::0000:0000 - ff13::ffff:ffff] です。
アクション	対応するタイプのインターネットアドレスを使用した配信について CFS で採用される現在の動作モードを指定します。このオブジェクトの値を [有効 (enable)] に設定すると、CFS は、対応するタイプのインターネットアドレスを使用してファブリック経由でアプリケーションデータを配信する機能を有効化します。このオブジェクトの値を [無効 (disable)] に設定すると、CFS は、対応するタイプのインターネットアドレスを使用してファブリック経由でデータを配信する機能を無効化します。

Cisco Fabric Services (CFS) IP 静的ピア

フィールド	説明
IP 静的ピア	配布対象の CFS ピア デバイスのアドレスを指定します。
DiscStatus	CFS 配信を目的としたユーザー定義のピアデバイスを指定します。

Cisco Fabric Services (CFS) のリージョンごとの機能

フィールド	説明
機能	配信リージョン内の CFS 対応機能の名前を特定します。
RegionId	CFS 配信リージョンを特定します。

Cisco Fabric Services (CFS) のすべてのリージョン

フィールド	説明
RegionId	CFS 配信リージョンを特定します。

Cisco Fabric Services (CFS) のオーナー

フィールド	説明
[Feature]、 [VSAN]	CFS 対応機能の名前、およびその機能のイネーブル化やコミットが行われる VSAN。
Name or IP Address	機能のイネーブル化やコミットが行われるスイッチの名前または IP アドレス。
UserName	機能のイネーブル化またはコミットを実行したユーザの名前。
タイプ	使用された最後の CFS 機能スコープタイプ。

Cisco Fabric Services (CFS) のマージ

フィールド	説明
機能	CFS 対応機能の名前。
CFS Merge Status Value	最後に行われたファブリック マージの結果。

ログ

SysLog (リポート以降)



(注) 最新のログを表示するには、ログ ダイアログを閉じて起動してください。「更新」オプションは、ページごとのダイアログでは使用できません。

フィールド	説明
スイッチ時間	スイッチのローカル時間。
ファシリティ	メッセージを生成したファシリティの名前。
重大度	The severity of the message.
イベント	ログに記録されているイベントの名前
VSAN Id	イベントが発生した VSAN。

SysLog (重大なイベント)

フィールド	説明
Host Time	ホストのローカル時間。
[説明 (Description)]	ログに記録されているイベントの説明。

SysLog (重大なイベント)

フィールド	説明
Switch Time	スイッチのローカル時間。
ファシリ ティ	メッセージを生成したファシリティの名前。
重大度	The severity of the message.
イベント	ログに記録されているイベントの名前
VSAN Id	イベントが発生した VSAN。
Host Time	ホストのローカル時間。
説明	ログに記録されているイベントの説明。

アカウントिंग ログ



(注) 最新のログを表示するには、ログ ダイアログを閉じて起動してください。「更新」オプションは、ページごとのダイアログでは使用できません。

フィールド	説明
スイッチ時間	スイッチのローカル時間。
アクション	発生したアクション (開始、停止、または更新)。
プロトコルと送信元	送信元スイッチのプロトコルと IP アドレス。
ユーザ	ユーザーの名前。
[説明 (Description)]	該当する場合、アクションの説明。

スイッチ ロギング

フィールド	説明
ConsoleEnable	Indicate whether the Syslog messages should be sent to the console.
ConsoleMsgSeverity	Minimum severity of the message that are sent to the Console.

フィールド	説明
TerminalEnable	Indicate whether the Syslog messages should be sent to the terminals.
TerminalMsgSeverity	Minimum severity of the message that are sent to the terminals.
LinecardEnable	Indicate whether the Syslog messages should be generated at the line cards.
LinecardMsgSeverity	Minimum severity of the message that are sent from linecards.
LogFileMsgSeverity	ログ ファイルに送信するメッセージの最小重大度。
SyslogLogFileName	Name of file to which the Syslog messages are logged.

syslog 重大度レベル

フィールド	説明
Facility	メッセージを生成するバッチ処理。
重大度	Minimum severity of the message that are generated by this Syslog message facility.

Syslogサーバ

フィールド	説明
IPAddress Type	IP アドレス タイプ (IPv4、IPv6、または DNS)。
Name or IP Address	The address of the Syslog server.
MsgSeverity	Minimum severity of the message that are sent to this Syslog server.
ファシリティ	The facility to be used when sending Syslog messages to this server.

エンド デバイス - ホスト

フィールド	説明
ホストエンクロージャ	ホスト エンクロージャの名前
名前	VMware の名前
IP アドレス	VMware の IP アドレス
CPU数	VMware の CPU 数
メモリサイズ	VMware のメモリ サイズ
ステータス	VMware の現在のステータス。
OS	VMwareのOS。

フィールド	説明
データストア	VMware データストアの名前。
前回の更新時刻	DCNM-SAN サーバーが VMware を最後に更新した時刻。

インテリジェント機能 - サマリ

フィールド	説明
スイッチ	スイッチの IP アドレス。
モジュール	モジュールの名前。
名前	スイッチ名。
IOA	IOA 機能が有効になっている場合、有効と表示されます。この機能が無効になっている場合、フィールドは空白になります。
DMM	DMM機能が有効になっている場合、有効と表示されます。この機能が無効になっている場合、フィールドは空白になります。
SANTap	SANTap 機能が有効になっている場合、有効と表示されます。この機能が無効になっている場合、フィールドは空白になります。

データ モビリティ マネージャ - モジュール

フィールド	ジョブ行の説明	セッション行の説明
名前	ジョブの名前。	このフィールドは空白になります。
ID	ジョブにシステムが割り当てた一意の識別子。	ジョブ内のセッション番号。
モード	サーバー モードまたはストレージ モード。	このフィールドは空白になります。
Existing Storage	既存ストレージのポートのエイリアス名。	既存ストレージの LUN 番号。
New Storage	新しいストレージのポートのエイリアス名。	新しいストレージの LUN 番号。

フィールド	ジョブ行の説明	セッション行の説明
ステータス	ジョブのステータス。作成またはスケジュールされたジョブはまだ開始されていません。進行中のジョブは現在移行中です。完了または検証済みのジョブは正常に終了しました。停止、失敗、またはリセットされたジョブは正常に終了しませんでした。	セッションのステータス。
時間	ジョブを開始するようにスケジュールされた日時。ジョブがスケジュールされていない場合、このフィールドは空白です。ジョブが進行中の場合、このフィールドにはジョブが開始された日時が表示されます。	セッションが進行中の場合、このフィールドには、セッションが完了するまでの推定残り時間が表示されます。それ以外の場合、フィールドは空白です。
SSM1	移行ジョブを実行しているSSMのスイッチ番号とスロット。	セッションがSSM 1で実行されている場合は、 OnSSM1 と表示されます。
SSM2	移行ジョブを実行しているSSMのスイッチ番号とスロット。	セッションがSSM 2で実行されている場合は、 OnSSM2 と表示されます。
タイプ	オンラインまたはオフラインの移行。	このフィールドは空白になります。
利率	ベストエフォート、低速、中速、高速。移行ジョブを構成するときにレートを設定します。	このフィールドは空白になります。

ストレージメディア暗号化

メンバー

フィールド	説明
Cluster	SME クラスタ名。
ステータス	SME クラスタの動作状態。

フィールド	説明
マスター	SME クラスター マスターの IP アドレスを識別します。
メンバー	SME クラスターのメンバーであるスイッチの IP アドレスを識別します。
IsLocal?	スイッチがこのクラスターのローカル メンバーかリモート メンバーかを識別します。

インターフェイス

フィールド	説明
Cluster	この SME インターフェイスが属するクラスターを識別します。
インターフェイス	SME インターフェイスを識別します。
ステータス	SME インターフェイスの動作状態。

ホスト

フィールド	説明
ホスト (Host)	ホスト Nx_Port のファイバチャネルポート名 (P_WWN)。
Cluster	このホスト ポートが属するクラスターを識別します。

SSM 機能

概要

フィールド	説明
スイッチ	インテリジェントモジュールのスイッチの名前。
モジュール	インテリジェント モジュールのロット番号。
名前	インテリジェント モジュールの名前。
IOA	インテリジェント モジュールの IOA 状態。
DMM	インテリジェント モジュールの DMM 状態。
SANTap	インテリジェント モジュールの SANTap 状態。
SE	インテリジェント モジュールの SE 状態。

FCWA

フィールド	説明
フローID	フロー ID を表します。
Init WWN	フロー内の発信側の pWWN を表します。
Init VSAN	フローが設定されている発信側の VSAN ID です。
Target WWN	フロー内のターゲットの pWWN を表します。
TargetVSAN	フローが設定されているターゲットの VSAN ID です。
WriteAcc	このフローに対して書き込みアクセラレーション機能がイネーブルになっているかどうかを指定します。true に設定すると、イネーブルになります。false に設定すると、ディセーブルになります。
BufCount	書き込みアクセラレーションに使用するバッファ数を指定します。
Stats Enable	このフローに対する統計情報収集をイネーブルにする必要があるかどうかを指定します。true に設定すると、イネーブルになります。false に設定すると、ディセーブルになります。
Stats Clear	このフローの統計情報のクリアを支援します。
Init Verification	SCSI フローに対応する発信側デバイスの検証ステータスです。
Init Module	SCSI フローの発信側デバイスがあるラインカードのステータスです。
Target Verification	SCSI フローに対応するターゲット デバイスの検証ステータスです。
Target Module	SCSI フローのターゲット デバイスがあるラインカードのステータスです。

SSM

フィールド	説明
[StartPort]、[EndPort]、 [Feature]	インターフェイスの機能関連情報を含んでいるテーブルです。このテーブルには、さまざまな機能に割り当てられているインターフェイスのリストがあります。サポートされているインターフェイスは、ファイバチャネルのタイプです。
PartnerImageURI	SSM 機能からインターフェイス マッピングに関連しているオブジェクトのコレクションです。

MSM

フィールド	説明
スイッチ	MSM モジュールのスイッチの名前。

フィールド	説明
Module、StartNode、EndNode、Feature	MSM モジュール番号、さまざまな機能に割り当てられるノード範囲など、機能に関連する情報を含むテーブル。



- (注) MSM (マルチサービス モジュール) と SSM (サービス モジュール) の違いは、SSM がカードのポート範囲ごとに機能を有効にできることです。MSM の場合、カード全体で有効にする必要があります。

SANTap CVT

フィールド	説明
Node WWN	モジュール上で作成された CVT のノードワールドワイド名を表します。
ポート WWN	モジュールで作成された CVT のポートワールドワイド名を表します。
名前	この CVT に管理上割り当てられた名前。

SANTap DVT

フィールド	説明
VSAN Id、Port WWN	作成された DVT のポート ワールドワイド名を表します。これは、データが複製される実際のターゲットのポートワールドワイド名と同じになります。
インターフェイス	DVT が作成されるモジュールのポートを表します。
Target VSAN Id	この DVT が作成されている実際のターゲットの VSAN を表します。
名前	この DVT に管理上割り当てられた名前。
LUNSize Handling	DVT が仮想 LUN の実際のターゲット LUN サイズを使用するか、それともサポートされる最大 LUN サイズである 2TB を使用するかを示します。
IO Timeout (sec)	DVT に関連付けられた IO タイムアウト値を表します。このオブジェクトは、DVT の作成時に設定する必要があり、後で変更することはできません。

フィールド	説明
Target IO Timeout (sec)	DVTに関連付けられたターゲット IO タイムアウト値を表します。

NASB

フィールド	説明
制御	TPCターゲットによって公開されるLUNのデバイスタイプを指定します。値1は、デバイスタイプをデフォルト値のディスクに設定します。値2は、デバイスタイプをストレージアレイコントローラに設定します。その他の値は、将来の変更のために予約されています。
マルチ	TPCターゲットが単一のLUNまたは複数のLUNモードで動作しているかどうかを指定します。値1は、単一のLUNであるデフォルトのモードを設定します。値2は、TPCターゲットが10のLUNを公開するマルチLUNモードを設定します。

NASB ターゲット

フィールド	説明
Module、VSAN Id、Processor Id	TPCターゲットに関連付けられた一意のID番号。このID番号は、TPCターゲットが構成されているVSAN内で一意です。
Virtual Target Node WWN	TPCターゲットのノードの世界ワイド名。
Virtual Target Port WWN	TPCターゲットのポートの世界ワイド名。
ステータス	TPCターゲットの現在の状態。
XCOPY Num	このターゲットが構成されているモジュールがオンラインになってから、TPCターゲットによって処理されたxcopyコマンドの総数。
XCOPY MinData (KB)	このターゲットが構成されているモジュールがオンラインになってから、単一のxcopyコマンドでTPCターゲットによって転送されたキロバイト単位の最小データ量。

フィールド	説明
XCOPY MaxData (KB)	このターゲットが構成されているモジュールがオンラインになってから、単一の xcopy コマンドで TPC ターゲットによって転送されたキロバイト単位の最大データ量。
XCOPY Avgthruput (KBps)	xcopy コマンドを処理する際の TPC ターゲットの 1 秒あたりの平均キロバイト スループット。

Virtual Initiator

フィールド	説明
Processor Id	DPP ID です。
制御	false の場合はデータ パスです。true の場合はコントロール パスです。

DMM レート

フィールド	説明
高速(MBps)	特定モジュールの高速属性の移行率の値を指定します。
中速(MBps)	特定モジュールの中速属性の移行率の値を指定します。
低速(MBps)	特定モジュールの低速属性の移行率の値を指定します。

FCWA Config Status

フィールド	説明
全体	このフローに対する書き込みアクセラレーション機能の設定ステータスです。
イニシエータ	このフローに対する書き込みアクセラレーション機能の発信側の設定ステータスです。
ターゲット言語	このフローに対する書き込みアクセラレーション機能のターゲットの設定ステータスです。

統計のステータス

フィールド	説明
全体	このフローに対する統計機能の構成ステータスです。
イニシエータ	このフローに対する統計機能のイニシエータ構成ステータスです。
ターゲット言語	このフローに対する統計機能のターゲット構成ステータスです。

I/O トラフィック統計

フィールド	説明
IO 読み取り	このフローでのこの LUN に対する SCSI 読み取り操作の総数。
IO 書き込み	このフローでのこの LUN に対する SCSI 書き込み操作の総数。
ブロック読み取り	このフローでこの LUN で読み取られたブロックの総数。
ブロック書き込み	このフローでこの LUN に書き込まれたブロックの総数。
Bytes Rx	このフローのこの LUN のリンク レベルフレームで受信されたオクテットの総数。
Bytes Tx	このフローのこの LUN のリンク レベルフレームで送信されたオクテットの総数。
フレーム Rx	このフローのこの LUN で受信されたリンク レベル FC フレームの総数。
フレーム Tx	このフローのこの LUN で送信されたリンク レベルフレームの総数。

統計 I/O トラフィックの詳細

フィールド	説明
Timeouts Read	このフローのこの LUN でタイムアウトした SCSI 読み取り操作の総数。
Timeouts Write	このフローのこの LUN でタイムアウトした SCSI 書き込み操作の総数。

フィールド	説明
MaxBlocks Read	このフローのこの LUN のすべての読み取り操作で読み取られたブロックの最大数。
MaxBlocks Write	このフローのこの LUN で書き込んだブロックの総数。
MaxTime Read	このフローのこの LUN のすべての読み取り操作に対する最大応答時間。
MaxTime Write	このフローのこの LUN に対するすべての書き込み操作に対する最大応答時間。
MinTime Read	このフローのこの LUN のすべての読み取り操作に対する最小応答時間。
MinTime Write	このフローのこの LUN に対するすべての書き込み操作に対する最小応答時間。
Active Read	このフローのこの LUN で現在アクティブな読み取り操作の数。
Active Write	このフローのこの LUN で現在アクティブな書き込み操作の数。

統計 SCSI コマンド

フィールド	説明
TestUnitRdys	このフローのこの LUN で送信されたテストユニット準備完了 SCSI コマンドの数。
RepLuns	このフローのこの LUN で送信されたレポート LUN SCSI コマンドの数。
Inquirys	このフローのこの LUN で送信された SCSI 照会コマンドの数。
RdCapacitys	このフローのこの LUN で送信された容量読み取り SCSI コマンドの数。
ModeSenses	このフローのこの LUN で送信されたモードセンス SCSI コマンドの数。
ReqSenses	このフローの LUN で送信されたリクエストセンス SCSI コマンドの数。

SCSI エラーの統計情報

フィールド	説明
BusyStatuses	このフローのこの LUN で受信したビジー状態の SCSI ステータスの数。
StatusResvConfs	このフローのこの LUN で受信した予約競合の SCSI ステータスの数。
TskSetFulStatuses	このフローのこの LUN で受信したタスクセットの完全な SCSI ステータスの数。
AcaActiveStatuses	このフローのこの LUN で受信した ACA アクティブ ステータスの数。

統計 SCSI 検知エラー

フィールド	説明
NotRdyErrs	このフローのこの LUN で受信した NOT READY SCSI SENSE キー エラーの数。これは、アドレス指定されている論理ユニットにアクセスできないことを示しています。
MedErrs	このフローのこの LUN で受信した MEDIUM ERROR SCSI SENSE キー エラーの数。これは、メディアの欠陥が原因である可能性がある、回復されないエラー状態のため、コマンドが終了したことを示しています。
HwErrs	このフローのこの LUN で受信した HARDWARE ERROR SCSI SENSE キー エラーの数。これは、ターゲットが回復不能なハードウェア障害を検出したことを示しています。
IllReqErrs	このフローのこの LUN で受信した ILLEGAL REQUEST SCSI SENSE キー エラーの数。
UnitAttErrs	このフローのこの LUN で受信した UNIT ATTENTION SCSI SENSE キー エラーの数。
DatProtErrs	このフローのこの LUN で受信した DATA PROTECT SCSI SENSE キー エラーの数。
BlankErrs	このフローのこの LUN で受信した BLANK CHECK SCSI SENSE キー エラーの数。
CpAbtrErrs	このフローのこの LUN で受信した COPY ABORTED SCSI SENSE キー エラーの数。

フィールド	説明
AbrtCmdErrs	このフローのこの LUN で受信した ABORTED COMMAND SCSI SENSE キー エラーの数。
VolFlowErrs	このフローのこの LUN で受信した VOLUME OVERFLOW SCSI SENSE キー エラーの数。
MiscmpErrs	このフローのこの LUN で受信した VOLUME OVERFLOW SCSI SENSE キー エラーの数。

コンパクト

フィールド	説明
デバイス	これは、フラッシュ デバイスのシーケンス番号で、初期化されたフラッシュデバイスのテーブル内でインデックスを作成するために使用されます。最小値は1である必要があります。最大値は、 <code>ciscoFlashDevicesSupported</code> オブジェクトの値以下である必要があります
パーティション (Partition)	これは、システムによってパーティションを参照するために使用される、フラッシュのパーティション名です。これは、AAAAAAAAAnn の形式の任意の英数字文字列です。ここで A は任意に選べる英字を、n は数字を表しています。数字は常に文字列の末尾部分に置く必要があります。システムは、数値部分のみを使用してパーティション インデックスにマップします。フラッシュの操作では、この名前に基づいてデバイスのパーティションが選択されます。システムには、デフォルト パーティションの概念があります。これは、デバイスの最初のパーティションです。パーティション名が指定されていない場合、システムはデフォルトのパーティションを操作します。したがって、パーティション名は、操作をデフォルトのパーティションで実行する場合、またはデバイスに1つのパーティションしかない (パーティション分割されていない) 場合を除き、必須です。
サイズ	これは、フラッシュ パーティションのサイズです。 <code>ciscoFlashDeviceMinPartitionSize</code> の整数倍である必要があります。パーティションが1つだけである場合、このサイズは <code>ciscoFlashDeviceSize</code> に等しくなります。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。