



Cisco Catalyst Center 3.2.x

Cisco Catalyst Center
Updated May 5, 2026



© 2026 Cisco Systems, Inc. All rights reserved.

短縮されたシスコの商標

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)

第 1 章 : 新機能および変更された機能に関する情報.....	9
新機能および変更情報.....	10
第 2 章 : システム設定の管理.....	11
システム設定について.....	12
ユーザープロファイルのロールおよび権限.....	12
セキュリティに関する推奨事項.....	13
制限付きシェルについて.....	13
システム 360 の使用.....	15
システム 360 でのサービスの表示.....	18
一般的なノードの操作.....	19
第 3 章 : 証明書の管理.....	21
プロキシの設定.....	22
プロキシ証明書の設定.....	23
SSL インターセプトプロキシ証明書のアップロード.....	24
内部証明書の更新.....	25
証明書および秘密キーのサポート.....	26
証明書チェーンのサポート.....	27
Catalyst Center サーバー証明書の更新.....	28
デバイス証明書を管理する.....	34
デバイス証明書の有効期間の設定.....	35
認証局.....	35
認証局のロールをルートから下位に変更.....	35
ロールオーバー下位 CA 証明書のプロビジョニング.....	38
外部 SCEP ブローカの使用.....	39
内部認証局への切り替え.....	40
Catalyst Center 認証局のエクスポート.....	40
CA 証明書のリセット.....	41
デバイス証明書トラストポイントの設定.....	41
信頼できる証明書の設定.....	42
第 4 章 : Cisco アカウントの管理.....	45
プラグアンドプレイの登録.....	46
PnP イベント通知の作成.....	47
シスコのログイン情報の設定.....	48
シスコのクレデンシャルのクリア.....	49
スマートアカウントの設定.....	49

スマートライセンス.....	51
接続モードの設定.....	52

第 5 章 : デバイス設定の構成.....55

イメージ配信サーバーの設定.....	56
アクセス ポイント イメージ転送.....	57
PnP デバイス認証の有効化.....	57
デバイスの可制御性.....	58
デバイスの可制御性の設定.....	62
ライセンス契約書の受諾.....	63
ネットワークの再同期間隔の設定.....	63
SNMP プロパティの設定.....	64
ICMP ping の有効化.....	65
PnP 導入準備用の AP ロケーションの設定.....	65
デバイスプロンプトの構成.....	65
カスタムプロンプトの作成.....	66
SSH キー変更の自動受け入れの設定.....	67
デバイス構成のバックアップ設定の構成.....	67
アーカイブデバイス構成用の外部サーバーの構成.....	68

第 6 章 : 外部サービスの設定.....71

Cisco AI Network Analytics の設定.....	72
クライアント証明書を更新.....	73
Cisco AI Network Analytics の無効化.....	73
Cisco Spaces の統合の設定.....	74
Catalyst Center と Cisco ISE の統合.....	75
Cisco ISE NAD デュアルスタック プロビジョニング ロジック.....	78
認証サーバーとポリシーサーバーの設定.....	79
整合性検証.....	83
KGV ファイルのアップロード.....	83
Cisco SD-Access の互換性マトリクス.....	86
SD-Access イメージ互換性チェックの無効化.....	88
IP アドレスマネージャの設定.....	88
機械推論ナレッジベースの更新.....	90
Meraki 統合の設定.....	91
Catalyst Center と Microsoft Teams の統合.....	92
Microsoft Teams 統合に関する考慮事項.....	92
既知の制限事項.....	95
AppX MS-Teams 統合の構成.....	95
Cisco Cloud Services を使用した AppX MS-Teams 統合の構成.....	96
クラウドアクセスキー.....	97
Webex 統合の設定.....	98
ThousandEyes 統合の構成.....	99

第 7 章 : システム設定の管理	101
ファイルシステムの正常性のモニタリング	102
Cisco IMC 接続の確立	102
システムイベント通知の登録	103
システムトポロジの表示	114
アプライアンスと外部システムの問題のトラブルシューティング	115
監査ログの表示	130
Syslog サーバーへの監査ログのエクスポート	131
デバッグログの設定	132
高可用性のアクティブ化	134
統合設定の設定	135
設定の可視性と制御の有効化	135
タスクと作業項目の詳細の表示、検索、およびフィルタリング	136
タスクの表示、編集、停止、削除	138
作業項目の表示と破棄	141
Geo マップ設定の構成	145
ログインメッセージの設定	145
第 8 章 : 利用規約の管理	147
製品テレメトリについて	148
第 9 章 : 信頼とプライバシー設定の管理	149
アカウント ロックアウト	150
パスワードの有効期限切れ	150
IP アクセス制御	151
IP アクセス制御の構成	151
IP アクセス制御の無効化	153
データの匿名化	154
第 10 章 : アプリケーションの管理	155
アプリケーションの管理	156
アプリケーションのダウンロードとインストール	156
パッケージのダウンロードとアップグレードのイベント通知	157
アップグレード概要レポートの表示	158
アプリケーションのアンインストール	158
第 11 章 : ユーザーの管理	161
ユーザープロファイルについて	162
ユーザ ロールについて	162
内部ユーザーの作成	162
ユーザーの編集	163

ユーザーの削除.....	163
パスワードポリシー.....	164
パスワード要件.....	164
ユーザーパスワードのリセット.....	165
自身のユーザーパスワードの変更.....	165
管理者権限なしでのユーザーパスワードの変更.....	166
思い出せないパスワードのリセット.....	166
ロールベース アクセス コントロールの設定.....	167
Catalyst Center ユーザーロール権限.....	168
ロールベースアクセス制御統計の表示.....	180
サイトベースのロールベース アクセス コントロールの設定.....	181
ユースケース：内部ユーザーへの複数のアクセスグループの割り当て.....	182
ユースケース：外部ユーザーへの複数のアクセスグループの割り当て.....	183
Catalyst Center 機能に対するSRBACの影響.....	185
外部認証の設定.....	192
二要素認証.....	195
二要素認証の前提条件.....	195
二要素認証のワークフロー.....	195
二要素認証の設定.....	196
二要素認証を使用したログイン.....	199
外部ユーザーの表示.....	199

第 12 章：ライセンスの管理.....201

ライセンスマネージャの概要.....	202
Cisco スマート アカウントとの統合.....	205
ライセンスマネージャの設定.....	206
Cisco ネットワーキング サブスクリプション ライセンス.....	208
ライセンスの使用状況と有効期限の可視化.....	208
ライセンス使用量の履歴傾向の表示.....	209
ライセンス詳細の表示.....	210
ライセンスレベルの変更.....	211
スマートライセンス対応デバイスの自動登録.....	213
スマートライセンス対応デバイスのデイレゾ設定.....	214
世界中のセーフモード対応デバイスのライセンスを設定.....	214
デバイスへの特定ライセンス予約またはパーマネントライセンス予約の適用.....	215
デバイスと Catalyst Center が CSSM に接続されている場合の SLR または PLR の有効化.....	216
デバイスと Catalyst Center が CSSM に接続されていない場合の SLR または PLR の有効化.....	216
CSSM からの認証コードの生成.....	217
デバイスに適用された SLR または PLR のキャンセル.....	217
承認コードのインストールと高セキュリティライセンスの有効化.....	218
高セキュリティライセンスの無効化.....	219
CSSM へのリソース使用状況詳細のアップロード.....	219
オンプレミス CSSM を介したポリシーレポートを使用したスマートライセンス.....	220
ライセンス接続モードの同期.....	221

デバイスのスループットの変更.....	222
バーチャルアカウント間のライセンスの転送.....	222
スマートライセンス対応デバイスでの顧客タグの管理.....	223
ライセンスポリシーの変更.....	223
第 13 章 : バックアップと復元.....	225
バックアップと復元について.....	226
バックアップと復元のイベント通知.....	227
バックアップサーバーの要件.....	228
バックアップサーバーのディレクトリレイアウト.....	229
バックアップストレージ要件.....	229
帯域幅と遅延の要件.....	230
ファイル共有の設定.....	231
Linux ベースの NFS ファイル共有の設定.....	231
Windows ベースの NFS ファイル共有の設定.....	235
NFS サーバーの追加.....	237
バックアップファイルを保存する場所の設定.....	238
リモート SSH サーバーの設定.....	242
バックアップの作成.....	242
データのバックアップスケジュール.....	244
バックアップと復元用の物理ディスクの追加.....	246
バックアップからのデータの復元.....	249
障害が発生した仮想アプライアンスの物理ディスクからのデータの復元.....	251
第 14 章 : ディザスタリカバリの実装.....	257
概要.....	258
主な用語.....	258
データレプリケーションの概要.....	260
ディザスタリカバリの GUI のナビゲーション.....	260
前提条件.....	263
アップグレードされた Catalyst Center アプライアンスでのディザスタリカバリの設定.....	268
ディザスタリカバリ証明書の追加.....	268
監視サイトのインストール.....	270
ディザスタリカバリのセットアップ.....	272
メインサイトの登録に関する考慮事項.....	272
メインサイトの登録.....	273
リカバリサイトの登録.....	279
監視サイトの登録.....	281
ディザスタリカバリシステムのアクティブ化.....	282
ディザスタリカバリシステムの一時停止.....	286
システムの一時的停止.....	286
システムへの再参加.....	288
フェールオーバー : 概要.....	290
手動フェールオーバーの開始.....	290

システムの登録解除.....	293
ディザスタリカバリシステムの考慮事項.....	294
バックアップおよび復元の検討事項.....	294
ノードまたはクラスターの交換に関する考慮事項.....	295
再構成に関する考慮事項.....	295
HA に関する考慮事項.....	295
サイト障害に関する考慮事項.....	295
証明書の置き換えに関する考慮事項.....	296
VLAN モードの考慮事項.....	297
ディザスタリカバリシステムを管理する.....	297
現在の監視サイトを置き換える.....	297
イベントタイムラインのモニタリング.....	298
マネージドサービス複製のモニター.....	301
システムおよびサイトの状態.....	301
ディザスタリカバリイベントの通知.....	305
サポートされるイベント.....	306
ディザスタリカバリシステムのトラブルシューティング.....	307
2 サイト障害シナリオ.....	314
BGP ルートアドバタイズメントに関する問題のトラブルシューティング.....	315

第 15 章 : 複数の Catalyst Center クラスターと単一の Cisco ISE システムの統合.....317

複数の Catalyst Center 展開の概要.....	318
作成者ノードクラスター.....	319
リーダーノードクラスター.....	319
複数の Catalyst Center のポリシー管理.....	320
複数の Catalyst Center のアップグレードに関する推奨事項.....	320
複数の Catalyst Center 展開.....	321
複数の Catalyst Center の有効化.....	321
複数の Catalyst Center の単一の Cisco ISE への統合.....	322
他の Catalyst Center クラスターとリーダーノードとしての Cisco ISE の統合.....	323
仮想ネットワークの削除.....	323
セキュリティグループの削除.....	324
リーダーノードの作成者ロールへの昇格.....	324
リーダーノードの正常な昇格.....	324
リーダーノードの強制的な昇格.....	325

第

1

章

:

- □□□□□□□□

|

ここでは、Catalyst Center リリース 3.2.x の新機能および変更された機能について説明します。

Catalyst Center 3.2.2 での新機能および変更された機能の要約と参照先を次の表に示します。

1 : Catalyst Center 3.2.2

機能	説明
アウトオブバンド AP イメージのダウンロード	ワイヤレスコントローラは、イメージが AP に配布された後、AP にイメージをプッシュします。Catalyst Center では、ワイヤレスコントローラから HTTPS 経由で AP でイメージをダウンロードできます。このアウトオブバンドファイル転送は、AP イメージを効率的にアップグレードするための方式です。 アクセス ポイント イメージ転送 (57ページ) を参照してください。
CA 証明書のリセット	CA のリセット機能を使用すると、更新の問題や期限切れ時に CA を管理できます。有効期間が定義されたサブ CA を作成できます。この機能により、サブ CA の有効期限が切れた場合、または別のサブ CA に切り替える場合、CA を簡単にリセットできます。 CA 証明書のリセット (41ページ) を参照してください。
サイトベース、ロールベースのアクセス制御のサポート	サイトユーザーのカスタムロールを作成でき、フィールド通知、EoX ステータス、セキュリティアドバイザリ、ネットワークバグ識別子、Network Reasoner への読み取り/書き込みアクセスの正確な割り当てができます。 Catalyst Center 機能に対する SRBAC の影響 (185ページ) を参照してください。
オンプレミス Cisco SSM を介したポリシーレポートを使用したスマートライセンス	オンプレミス SSM を介して技術情報の詳細を CSSM にアップロードできます。 「 オンプレミス CSSM を介したポリシーレポートを使用したスマートライセンス (220ページ) 」を参照してください。

第

2

章

$$\vdots$$

- □ □ □ □ □ □ □ □
- □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
- □ □ □ □ □ □ □ □ □ □ □ □ □
- □ □ □ □ 360 □ □ □
- □ □ □ □ 360 □ □ □ □ □ □ □ □ □ □
- □ □ □ □ □ □ □ □ □ □

Catalyst Center のシステム設定に関する情報。

Catalyst Center の使用を開始するには、まずシステム設定を構成する必要があります。これにより、サーバーがネットワーク外で通信できるようになり、セキュア通信が確保され、ユーザーが認証され、その他の重要なタスクがサポートされます。システム設定を構成するには、この章の手順を使用します。

注

- プロキシサーバー設定の変更など、Catalyst Center の構成を変更する場合、すべて Catalyst Center GUI で実行する必要があります。
- Catalyst Center アプライアンスの構成設定への変更は `sudo maglev-config update` コマンドを使用して行う必要があります。Cisco IMC から開いた KVM コンソールで、このコマンドを実行します。

Catalyst Center 2.3.7.7 以降 :

- [maglev] のユーザーパスワードを変更するには、[Linux Password] および [Re-enter Linux Password] フィールドに新しいパスワードを指定します。これらのフィールドを空白のままにすると、現在のパスワードが引き続き使用されます。
- その他の設定は、[maglev] のユーザーパスワードを入力せずに変更できます。
- デフォルトでは、Catalyst Center システムのタイムゾーンは UTC に設定されています。Catalyst Center の GUI はブラウザのタイムゾーンで動作するため、このタイムゾーンを変更しないでください。
- セキュリティ上を強化するため、制限付きシェルまたはセキュアシェルが有効になっています。`_shell` コマンドを使用してルートシェルにアクセスしたり、いずれかの制限付きコマンドを使用したりする必要がある場合は、Cisco TAC に連絡して支援を受けてください。

このセクションでは、ユーザープロファイルのロールと、ロールベース アクセス コントロールの権限について説明します。

Catalyst Center は、ロールベース アクセス コントロール (RBAC) をサポートします。権限は、ユーザーロールによって定義されます。Catalyst Center には次の 3 つの主要なデフォルトユーザーロールがあります。

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- OBSERVER-ROLE

SUPER-ADMIN-ROLE は、包括的なアクセスを許可し、Catalyst Center GUI でのカスタムロールの作成と割り当てをサポートします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE のユーザーロールは、アクセスが制限されます。

特定のネットワークサイトへのアクセスを制限するアクセスグループを作成できます。アクセスグループはロールとサイトの組み合わせです。特定のアクセスグループにいつでもログインできます。

Catalyst Center は、次のデフォルトアクセスグループをサポートしています。

- **NW-ADMIN_Global** : NW-ADMIN ロールへのグローバルアクセス用のアクセスグループ

- **[OBSERVER_Global]** : OBSERVER ロールへのグローバルアクセス用のアクセスグループ
- **SUPER-ADMIN_Global** : SUPER-ADMIN ロールへのグローバルアクセス用のアクセスグループ

Catalyst Center の機能の動作は、アクセスグループで指定されたユーザーロールとサイトによって異なります。詳細については、『[Cisco Catalyst Center Administrator Guide](#)』の「Configure site-based, role-based access control」を参照してください。

Catalyst Center のセキュリティ設定方法に関する情報。

Catalyst Center は、それ自体とモニターおよび管理対象のホスト/ネットワークデバイス用の多数のセキュリティ機能を提供します。セキュリティ機能は、明確に理解して、正しく設定する必要があります。セキュリティに関する次の推奨事項に従ってください。

- Catalyst Center は、プライベート内部ネットワーク内、およびインターネットなどの信頼できないネットワークに対して Catalyst Center を開いていないファイアウォールの背後に導入してください。
- 管理ネットワークとエンタープライズネットワークが個別にある場合は、Catalyst Center の管理インターフェイスとエンタープライズ インターフェイスをそれぞれ管理ネットワークとエンタープライズ ネットワークに接続してください。これにより、Catalyst Center の管理に使用されるサービスと、ネットワークデバイスとの通信および管理に使用されるサービスとの間で確実にネットワーク分離が行われます。
- 3 ノードクラスターセットアップで Catalyst Center を展開する場合は、クラスタインターフェイスが分離されたネットワークに接続されていることを確認してください。
- パッチのアナウンス後できる限り早急に、セキュリティパッチを含む重要なアップグレードで Catalyst Center をアップグレードしてください。詳細については、『[Catalyst Center Upgrade Guide](#)』を参照してください。
- HTTPS プロキシサーバーを使用する Catalyst Center によってアクセスされるリモート URL を制限してください。Catalyst Center は、インターネット経由でアクセスして、ソフトウェアアップデート、ライセンス、デバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザーフィードバックなどを提供したりするように設定されています。これらの目的でインターネット接続を提供することは必須要件です。ただし、HTTPS プロキシサーバーを介して安全な接続を提供します。
- 既知の IP アドレスおよび範囲のみを許可し、未使用のポートへのネットワーク接続をブロックすることにより、ファイアウォールを使用した Catalyst Center への入力および出力管理とエンタープライズ ネットワーク接続を制限してください。
- Catalyst Center の自己署名サーバー証明書を、内部認証局 (CA) によって署名された証明書に置き換えてください。
- 使用しているネットワーク環境で可能な場合は、SFTP 互換モードを無効にします。このモードでは、レガシー ネットワーク デバイスが古い暗号スイートを使用して Catalyst Center に接続できます。
- ブラウザベースのアプライアンス設定ウィザードを無効にします。このウィザードには、自己署名証明書が付属しています。

制限付きシェルについての情報。

セキュリティを強化するため、ルートシェルへのアクセスは無効になっています。Shell コマンドへのアクセスが制限されることで、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできなくなるため、運用上のリスクが軽減されます。

セキュリティ上の理由から、**Shell** コマンドへのアクセスが制限されています。ただし、**root shell** に一時的にアクセスしたい場合は、**Cisco TAC** お問い合わせください。

必要に応じて、次の限定されたリストのコマンドを使用できます。

2 :

コマンド	説明
cat	制限付きモードでファイルを連結して出力します。
clear	端末画面をクリアします。
date	指定されたフォーマットで現在の時刻を表示するか、システム日付を設定します。
debug	コンソールデバッグログを有効にします。
df	ファイルシステム情報。
dmesg	カーネルリングバッファを出力または制御します。
du	ディレクトリにおける一連のファイルのディスク使用状況の概要を再帰的に表示します。
free	メモリの使用状況の概要。
history	シェルコマンド履歴を有効にします。
htop	Interactive Process Viewer 。
ip	ルーティング、ネットワークデバイス、インターフェイス、およびトンネルを出力します。
kubectl	制限付きで Kubernetes クラスタを操作します。
last	最後にログインしたユーザーのリストを表示します。
ls	maglev ホームに chroot された制限付きファイルシステムビュー。
lscpu	CPU アーキテクチャに関する情報を出力します。
magctl	Maglev の展開を管理するためのツール。
maglev-config	Maglev の展開を設定するためのツール。
manufacture_check	製造チェックを実行するツール。
netstat	ネットワーク情報を出力します。
nslookup	インターネット ネーム サーバーをインタラクティブに照会します。
ntpq	標準 NTP クエリプログラム。
ping	ICMP ECHO_REQUEST をネットワークホストに送信します。
ps	システム内のアクティブなプロセスのステータスを確認します。
rca	根本原因分析収集ユーティリティ。
reboot	マシンをリブートします。

コマンド	説明
rm	制限付きモードでファイルを削除します。
route	IP ルーティングテーブルを出力します。
runonce	runonce スクリプトを実行します。
scp	制限付きセキュアコピー。
sftp	安全なファイル転送。
shutdown	マシンをシャットダウンします。
ssh	OpenSSH SSH クライアント。
tail	各ファイルの最後の 10 行を標準出力先に出力します。
top	システムプロセスのソートされたリストを表示します。
tracert	ネットワークホストへのルートパケットトレースを出力します。
uname	システム情報を出力します。
uptime	システムの稼働時間を通知します。
vi	テキストエディタ。
w	ログオンしているユーザーとそのユーザーの操作を表示します。

360

[System 360] タブと、そこで提供されるデータに関する情報。

[System 360] タブには、Catalyst Center に関する一目でわかる情報が表示されます。

1. メインメニューから次を選択します。[System] > [System 360] の順に選択します。
2. [System 360] ダッシュボードで、表示される次のデータメトリックを確認します。

[Cluster]

- **[Hosts] : Catalyst Center** ホストに関する情報を表示します。表示される情報には、ホストの IP アドレスと、ホストで実行されているサービスに関する詳細なデータが含まれます。ホストで実行されているサービスに関する詳細なデータを表示するには、[View Services] リンクをクリックします。

注

ホスト IP アドレスの横には、カラーバッジが付きます。緑色のバッジは、ホストが正常であることを示します。赤色のバッジは、ホストが正常でないことを示します。

側面パネルには、次の情報が表示されます。

- **[Node Status]** : ノードのヘルスステータスが表示されます。

ノードヘルスが正常でない場合は、ステータスにカーソルを合わせると、トラブルシューティングのための追加情報が表示されます。

- **[Services Status]** : サービスのヘルスステータスが表示されます。1 つでもサービスがダウンしていると、ステータスは **[Unhealthy]** になります。

- **[Name]** : サービス名。

- **[Appstack]** : アプリケーションスタック名。

アプリケーションスタックは、疎結合されたサービスの集合です。この環境でのサービスは、要求が増えるとインスタンスを追加し、要求が減るとインスタンスを削除する、水平方向にスケール可能なアプリケーションです。

- **[Health]** : サービスのステータス。

- **[Version]** : サービスのバージョン。

- **[Tools]** : サービスのメトリックとログを表示します。Grafana でサービスモニターリングデータを表示するには、**[Metrics]** リンクをクリックします。Grafana は、オープンソースのメトリック分析および可視化スイートです。サービスモニターリングデータを調べることで、問題をトラブルシューティングすることができます。Grafana の詳細については、<https://grafana.com/> を参照してください。**[Logs]** リンクをクリックすると、Kibana でサービスログが表示されます。Kibana は、オープンソースの分析および可視化プラットフォームです。サービスログを調べることで、問題をトラブルシューティングすることができます。Kibana の詳細については、<https://www.elastic.co/products/kibana> を参照してください。

- **[Actions]** : サービスを再起動するために使用できるオプション。一部の内部サービスおよびシステム固有のサービスでは、**[Actions]** オプションが無効になっています。

- **[High Availability]** : HA が有効でアクティブであるかどうかが表示されます。

クラスターで HA をアクティブ化する方法については、「[高可用性のアクティブ化（134ページ）](#)」を参照してください。

重要

HA では、Catalyst Center で動作する 3 つ以上のホストが必要です。

3 ノード HA は、Catalyst Center で実行されている ESXi ではサポートされていません。

- **[Cluster Tools]** : 次のツールにアクセスできます。

- **[Service Explorer]** : アプリケーションスタックおよび関連付けられたサービスにアクセスします。

- **[Monitoring]** : オープンソースメトリック分析および可視化スイートである Grafana を使用して、Catalyst Center コンポーネントの複数のダッシュボードにアクセスします。**[Monitoring]** ツールを使用して、メモリおよび CPU 使用率などの主要な Catalyst Center メトリックを確認および分析します。Grafana の詳細については、<https://grafana.com/> を参照してください。

 注

マルチホスト **Catalyst Center** 環境では、複数のホストによる **Grafana** データの重複が予想されます。

- **[Log Explorer]** : Kibana を使用して **Catalyst Center** のアクティビティログとシステムログにアクセスします。Kibana は Elasticsearch と連動するように設計されたオープンソースの分析および可視化を実行するプラットフォームです。**[Log Explorer]** ツールを使用して、詳細なアクティビティログおよびシステムログを確認します。Kibana の左側にあるナビゲーションウィンドウで、**[Dashboard]** をクリックします。次に、**[System Overview]** をクリックしてすべてのシステムログを表示します。Kibana の詳細については、<https://www.elastic.co/products/kibana> を参照してください。

 注

デフォルトでは、**Catalyst Center** のすべてのロギングが有効になっています。

システム管理

- **[Software Updates]** : アプリケーションまたはシステムの更新のステータスが表示されます。**[View]** リンクをクリックすると、更新の詳細が表示されます。

 注

更新には、その横にカラーバッジが付きます。緑色のバッジは、更新または更新に関連するアクションが正常に完了したことを示します。黄色のバッジは、使用可能な更新があることを示します。

- **[Backups]** : 最新のバックアップのステータスが表示されます。**[View]** リンクをクリックすると、すべてのバックアップの詳細が表示されます。

さらに、次のスケジュールバックアップのステータスも表示されます（またはスケジュールされているバックアップがないことを示します）。

 注

バックアップには、その横にカラーバッジが付きます。緑色のバッジは、バックアップが正常に完了したことをタイムスタンプとともに示します。黄色のバッジは、次のバックアップがまだスケジュールされていないことを示します。

- **[Application Health]** : 自動化および **Assurance** の健全性が表示されます。

 注

アプリケーションの健全性には、その横にカラーバッジが付きます。緑色のバッジは、正常なアプリケーションであることを示します。赤色のバッジは、アプリケーションが正常でないことを示します。トラブルシューティングするには、[View] リンクをクリックします。

外部接続されたシステム

Catalyst Center によって使用されている外部ネットワークサービスに関する情報が表示されます。

- **[Identity Services Engine (ISE)]** : プライマリおよびセカンダリ Cisco ISE サーバーの IP アドレスとステータスを含む Cisco ISE 設定データを表示します。Cisco ISE と統合するように Catalyst Center を設定するには、[Configure] リンクをクリックします。
- **[IP Address Manager (IPAM)]** : IP アドレスマネージャの設定データと統合ステータスを表示します。IP アドレスマネージャを設定するには、[Configure] リンクをクリックします。

3. **[System Health]** をクリックし、ネットワークに接続されている Catalyst Center アプライアンスと外部システムのトポロジを確認します。

[System Health] ウィンドウの詳細については、「[システムトポロジの表示](#) (114ページ)」を参照してください。

360

[System 360] タブのサービスに関する情報。

[System 360] タブは、Catalyst Center で実行されているアプリケーションスタックとサービスに関する詳細情報を提供します。この情報を使用して、特定のアプリケーションやサービスに関する問題のトラブルシューティングに役立てることができます。たとえば、Assurance に問題がある場合は、NDP アプリケーションスタックとそのコンポーネントサービスのモニタリングデータとログを表示できます。

1. メインメニューから次を選択します。[System] > [System 360] の順に選択します。

2. **[System 360]** ウィンドウで、[Service Explorer] タブをクリックします。

ノードクラスと関連サービスが新しいブラウザウィンドウにツリー型の構造で表示されます。

- ノードにカーソルを合わせると、シリアル番号、製品 ID、インターフェイスなどの詳細が表示されます。
- サービステーブルには、ノードに関連付けられているすべてのサービスが表示されます。マネージドサービスは「(M)」というマークで示されます。
- グローバルフィルタアイコンをクリックすると、サービステーブルのサービスをアプリケーションスタック名、サービス正常性ステータス ([Up]、[Down]、または [In Progress])、またはマネージドサービスかどうかに基づいてフィルタ処理できます。
- **[Global Search]** フィールドにサービス名を入力してサービスを検索できます。サービス名をクリックすると、関連付けられているノードでサービスが表示されます。

3. サービスをクリックすると、[サービス360] ビューが起動します。詳細には次の情報が含まれます。

- **[Metrics]** : リンクをクリックすると **Grafana** のサービスモニタリングデータが表示されます。
- **[Logs]** : リンクをクリックすると **Kibana** のサービスログが表示されます。
- **[Name]** : サービス名。
- **[Appstack]** : アプリケーションスタック名。
- **[Version]** : サービスのバージョン。
- **[Health]** : サービスのステータス。
- **[Required Healthy Instances]** : 正常なインスタンスの数が表示され、マネージドサービスであるかどうかを示されます。
- **[Instances]** : インスタンスをクリックすると詳細が表示されます。

4. テーブルにリストされているサービスを検索するには、**[Search]** フィールドにサービス名を入力します。

5. サービステーブルのサービスをアプリケーションスタック名、サービス正常性ステータス (**[Up]**、**[Down]**、または **[In Progress]**)、またはマネージドサービスかどうかに基づいてフィルタ処理するには、フィルタアイコンをクリックします。

この項では、ディスク返品許可 (RMA) などの一般的なノードの操作について説明します。

RMA

返品許可 (RMA) 手順で、DIMM、CPU、単一 SSD などのハードウェア周辺機器を交換する場合は、**Catalyst Center** のグレースフルシャットダウンを実行することを推奨します。

HA

レイヤ 2 ネットワーク内の直接リンクされたスイッチで、ネットワークサービスを維持するためのフォールバック (HA) メカニズムなしでメンテナンスが実行されている場合は、グレースフルシャットダウンを実行することを推奨します。レイヤ 2 ネットワークの冗長性を実現するには、『[Cisco Catalyst Center Appliance Installation Guide](#)』の「NIC Bonding Overview」を参照してください。

ハードウェアを修復する前に、**Catalyst Center** アプライアンスを停止できます。ソフトウェアの問題を修正した後ウォームリスタートを開始することもできます。『[Cisco Catalyst Center Appliance Installation Guide](#)』の「Power cycle the appliance」セクションを参照してください。

第3

章

:

- □□□□□□
- □□□□□□□
- □□□□□□□□□□□□□□
- □□□□□□□□□□
- □□□□□□□□□□□□□□
- □□□
- □□□□□□□□□□□□□□□□
- □□□□□□□□□□

プロキシサーバーへのアクセスの設定に関する情報。

着信プロキシ

Catalyst Center に、それ自体が管理するネットワークデバイスとの間の中間サーバーとして設定されたプロキシサーバーがある場合は、プロキシ認証局 (CA) を設定して、CA がトラストアンカーとしてネットワークデバイスにプロビジョニングされ、プロキシを介して **Catalyst Center** に接続できるようにする必要があります。

発信プロキシ

Catalyst Center に、インターネットとの間の中間サーバーとして設定されたプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。

セキュリティに関する推奨事項 : HTTPS プロキシを通じて、**Catalyst Center** で必要とされる URL と FQDN だけにセキュアアクセスを許可することを推奨します。

詳細については、最新の『[Cisco Catalyst Center Appliance Installation Guide](#)』の「Required internet URLs and fully qualified domain names」と「Provide secure access to the internet」を参照してください。

注

Catalyst Center は、Windows New Technology LAN Manager (NTLM) 認証を使用するプロキシサーバーをサポートしていません。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**System Configuration**]の順に選択します。
2. [**System Configuration**] ドロップダウンリストから、[**Proxy**] > [**Outgoing Proxy**]を選択します。
3. プロキシサーバーの URL アドレスを入力します。
4. プロキシサーバーのポート番号を入力します。

注

- HTTP の場合、ポート番号は通常 80 です。
- ポート番号の範囲は 0 ~ 65535 です。

5. (オプション) プロキシサーバーが認証を必要とする場合、[**Update**]をクリックして、プロキシサーバーにアクセスするためのユーザー名とパスワードを入力します。
6. [**Validate Settings**] チェックボックスをオンにし、適用時に **Catalyst Center** でプロキシ構成時の設定が検証されるようにします。
7. 選択内容を確認し、[**Save**] をクリックします。

選択内容をキャンセルするには、[**Reset**]をクリックします。既存のプロキシ設定を削除するには、[**Delete**]をクリックします。

プロキシを設定した後、[**Proxy**] ウィンドウに設定を表示できます。

重要

Catalyst Center サービスがプロキシサーバーの設定で更新されるまでに最大 5 分かかることがあります。

ネットワーク構成によっては、プロキシゲートウェイは、**Catalyst Center** と管理するリモートネットワークの間に存在する可能性があります。80 や 443 などの一般的なポートは DMZ のゲートウェイプロキシを通過します。このため、**Catalyst Center** 用に設定されたネットワークデバイスからの SSL セッションは、プロキシゲートウェイで終了することになります。したがって、これらのネットワークデバイスは、プロキシゲートウェイ経由のみで **Catalyst Center** と通信できます。ネットワークデバイスが **Catalyst Center** または、（存在する場合は）プロキシゲートウェイと、安全で信頼できる接続を確立するため、ネットワークデバイスは、関連する CA ルート証明書で、または特定の状況ではサーバー独自の証明書を使って、適切にプロビジョニングされた PKI トラストストアを保有する必要があります。

ネットワーク構成によっては、プロキシゲートウェイは、**Catalyst Center** と管理するリモートネットワーク（さまざまなネットワークデバイスを含む）の間に存在する可能性があります。80 や 443 などの一般的なポートは DMZ のゲートウェイプロキシを通過します。このため、**Catalyst Center** 用に設定されたネットワークデバイスからの SSL セッションは、プロキシゲートウェイで終了することになります。したがって、これらのリモートネットワーク内にあるネットワークデバイスは、プロキシゲートウェイ経由でのみ **Catalyst Center** と通信できます。ネットワークデバイスが **Catalyst Center** または、（存在する場合は）プロキシゲートウェイと安全で信頼できる接続を確立するため、ネットワークデバイスは、関連する CA ルート証明書で、または特定の状況ではサーバー独自の証明書を使って、適切にプロビジョニングされた PKI トラストストアを保有する必要があります。

PnP 検出/サービスによってデバイスのオンボード中にそのようなプロキシが配置されている場合は、ネットワークデバイスが安全に **Catalyst Center** を信頼および認証できるように、プロキシと **Catalyst Center** サーバー証明書は同一である必要があります。

プロキシゲートウェイが **Catalyst Center** と管理対象のリモートネットワークの間に存在するネットワークトポロジでは、次の手順を実行してプロキシゲートウェイ証明書を **Catalyst Center** にインポートします。

- **SUPER-ADMIN-ROLE** 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールについて](#)（162 ページ）を参照してください。
- **Catalyst Center** とそのサービスに到達するプロキシゲートウェイの IP アドレスを使用する必要があります。
- プロキシゲートウェイで現在使用されている証明書ファイルを持っている必要があります。証明書ファイルの内容は、次のいずれかで構成されている必要があります。
 - PEM または DER 形式のプロキシゲートウェイの証明書、および自己署名された証明書。
 - PEM または DER 形式のプロキシゲートウェイの証明書、および有効な既知の CA によって発行された証明書。
 - PEM または DER 形式のプロキシゲートウェイの証明書とそのチェーン。

デバイスとプロキシゲートウェイで使用される証明書は、次の手順に従って、**Catalyst Center** にインポートする必要があります。

1. メインメニューから次を選択します。[System] > [Settings] > [System Configuration]の順に選択します。
2. [System Configuration] ドロップダウンリストから、[Proxy] > [Incoming Proxy] を選択します。
3. [Proxy Certificate] ウィンドウで、（存在する場合は）現在のプロキシゲートウェイ証明書のデータを表示します。

 注

[Expiration Date and Time] は、現地時間で表示されます。証明書有効期限の 2 ヶ月前に、Catalyst Center の GUI にシステム通知が表示されます。

4. プロキシゲートウェイ証明書を追加するには、自己署名証明書または CA 証明書を [Drag and Drop Here] 領域にドラッグアンドドロップします。

 注

PEM または DER ファイル（公開キー暗号化標準のファイル形式）だけが、この領域を使用して Catalyst Center にインポートできます。さらに、この手順には秘密キーは必要ではなく、Catalyst Center にアップロードもされません。

5. [Save] をクリックします。
6. [Proxy Certificate] ウィンドウを更新し、更新されたプロキシゲートウェイ証明書のデータを表示します。[Proxy Certificate] ウィンドウに表示された情報は、新しい証明書名、発行者、および証明機関を反映するように変更する必要があります。
7. プロキシゲートウェイ証明書の機能を有効にするには、[Enable] ボタンをクリックします。

[Enable] ボタンをクリックすると、プロキシゲートウェイからの要求時にコントローラがインポートされたプロキシゲートウェイ証明書を返します。[Enabled] ボタンをクリックしない場合、コントローラは独自の自己署名証明書またはインポートされた CA 証明書をプロキシゲートウェイに返します。

プロキシゲートウェイ証明書の機能が使用されている場合、[Enable] ボタンはグレー表示されます。

SSL

Catalyst Center とソフトウェアアップデートのダウンロード元である Cisco Cloud との間に設定されたプロキシサーバーで SSL 復号が有効になっている場合、正式な認証局から発行された証明書を使用した SSL インターセプトプロキシ証明書をアップロードします。

Catalyst Center とソフトウェアアップデートのダウンロード元である Cisco Cloud との間に設定されたプロキシサーバーで SSL 復号が有効になっている場合、正式な認証局から発行された証明書を使用してプロキシが構成されていることを確認してください。プライベート証明書を使用している場合は、次の手順を実行します。

 注

セキュリティを強化するため、ルートシェルへのアクセスは **Catalyst Center** で無効になっています。制限付きシェルでは、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできないため、運用上のリスクが軽減されます。ただし、このセクションのコマンドを使用するには、**Cisco TAC** に連絡して、ルートシェルに一時的にアクセスする必要があります。

1. プロキシサーバーの証明書（.pem 形式）を **Catalyst Center** サーバーのディレクトリに転送します。
2. **maglev** ユーザーとして **Catalyst Center** サーバーに **SSH** 接続し、次のコマンドを入力します。

```
# /usr/local/bin/update_cacerts.sh -v -a example.pem
```

このコマンドは、次の例のような出力を返します。

```
Reading CA cert from file example.pem
Adding certificate
import_04:F7:6B:24:92:95:5A:20:3E:05:83:40:FA:19:8D:94:B2:B0:69:60.crt
Sending MKS Event..
(Attempt 1) Command to execute kubectl create -f /tmp/event_file.yaml
(Attempt 1) kubectl create -f /tmp/event_file.yaml completed successfully
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,
it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Attempting to restart containerd (Attempt 1)...
containerd restarted successfully.
[Attempt 1/10] Restarting Pod/Service that has a host mounted certificate
dependency.
Please wait for the pods to come back up and resume normal working. This might
take a while
Successfully triggered a restart for the containers needing the certificates.
Deleting tempfiles /tmp/tmp.CMu8bA83SC /tmp/tmp.6STo8fQRNB /tmp/tmp.cjBhl4gw5b
```

3. コマンド出力で、「1 added」の行を探し、追加された数がゼロでないことを確認します。チェーン内の証明書に基づき、この数は 1 か 1 よりも多くなる場合があります。
4. **Catalyst Center** で同じ証明書をアップロードし、接続を確認します。
 - a) **Catalyst Center GUI** にログインします。
 - b) **[System] > [Settings] > [Certificates] > [Trusted Certificates]** に移動し、同じ証明書をアップロードします。
詳細については、[信頼できる証明書の設定](#)（42 ページ）を参照してください。
 - c) クラウド、**Cisco Connected Mobile Experiences (CMX)**、および **Cisco Spaces** の接続を確認します。

内部証明書の有効期限が切れる前に、更新して期限を 1 年間延長することについての情報。

Catalyst Center は、**Kubernetes** によって生成された証明書や、**Kong** および資格情報マネージャサービスが使用する証明書など、多数の証明書を使用します。これらの証明書は 1 年間有効で、クラスタをインストールするとすぐに開始されます。これらの内部証明書は、有効期限が切れる前に **Catalyst Center** によって 1 年間自動的に更新されます。

- 期限切れになる前に内部証明書を更新することを推奨します。
- 今から 100 日間の間に期限切れになるように設定されている内部証明書のみを更新できます。この手順では、それ以降に期限切れになる証明書については何も実行されません。
- このスクリプトでは、サードパーティ/認証局 (CA) 署名付き証明書ではなく、自己署名証明書のみを更新します。サードパーティ/CA 署名付き証明書の場合、スクリプトは **Kubernetes** と資格情報マネージャによって使用される内部証明書を更新します。
- 自己署名証明書の場合、更新プロセスではルート CA が変更されないため、証明書をデバイスにプッシュする必要はありません。
- クラスタという用語は、単一ノードと 3 ノード **Catalyst Center** 設定の両方に適用されます。

1. 各クラスタノードが正常であり、問題が発生していないことを確認します。
2. そのノードで現在使用されている証明書のリストとそれらの有効期限を表示するには、次のコマンドを入力します。

```
sudo maglev-config certs info
```

3. 次のコマンドを入力して、すぐに期限切れになるように設定されている内部証明書を更新します。

```
sudo maglev-config certs refresh
```

4. 他のクラスタノードに対して上記の手順を繰り返します。
5. ユーティリティのヘルプを表示するには、次のように入力します。

```
$ sudo maglev-config certs --help
Usage: maglev-config certs [OPTIONS] COMMAND [ARGS]...

Options:
  --help  Show this message and exit.

Commands:
  info
  refresh
```

Catalyst Center デジタル証明書および秘密キーに関する情報です。

Catalyst Center は、セッション (HTTPS) の認証に使用される認証局管理機能をサポートしています。これらのセッションでは、CA と呼ばれる一般に認められた信頼されたエージェントを使用します。**Catalyst Center** は、認証局管理機能を使用して、内部 CA から X.509 証明書をインポートして保存し、管理します。インポートされた証明書は **Catalyst Center** のアイデンティティ証明書になり、**Catalyst Center** は認証のためにこ

の証明書をクライアントに提示します。クライアントは、ノースバウンド API アプリケーションとネットワークデバイスです。

Catalyst Center GUI を使用して次のファイルを（**PEM** または **PKCS** ファイル形式で）インポートできます。

- **X.509** 証明書
- 秘密キー

注

秘密キーについて、**Catalyst Center** は **RSA** および楕円曲線デジタル署名アルゴリズム（**ECDSA**）キーのインポートをサポートしています。ユーザー自身のキー管理システムで秘密キーを保護してください。秘密キーのモジュラスサイズは最小でも **2048** ビット必要です。

内部 **CA** によって発行された有効な **X.509** 証明書と秘密キーを取得する必要があります。ファイルをインポートする前に、証明書が所有している秘密キーに対応している必要があります。ファイルをインポートすると、**X.509** 証明書と秘密キーに基づくセキュリティ機能が自動的にアクティブ化されます。**Catalyst Center** は証明書を、要求するデバイスまたはアプリケーションに提示します。ノースバウンド API アプリケーションとネットワークデバイスでは、これらのログイン情報を使用して **Catalyst Center** との信頼関係を確立できます。

注

自己署名証明書を **Catalyst Center** にインポートして使用しないでください。内部 **CA** から有効な **X.509** 証明書をインポートしてください。適切なプラグアンドプレイ機能を確認するため、デフォルトの自己署名証明書を内部 **CA** によって署名された証明書に置き換えてください。

Catalyst Center は一度に **1** つのインポート済み **X.509** 証明書および秘密キーだけをサポートします。**2** つ目の証明書および秘密キーをインポートすると、最初の（既存の）インポート済み証明書および秘密キーの値が上書きされます。

Catalyst Center と証明書チェーンのサポートに関する情報です。

Catalyst Center では、**GUI** を介して証明書と秘密キーをインポートできます。**Catalyst Center** にインポートされる証明書（署名された証明書）につながる証明書チェーンに含まれる下位証明書がある場合は、それらの下位証明書とそれらの下位 **CA** のルート証明書と一緒に、インポートされる単一のファイルに追加される必要があります。これらの証明書を追加する場合は、認定の実際のチェーンと同じ順序で追加する必要があります。

次の証明書は、単一の **PEM** ファイルと一緒に貼り付ける必要があります。証明書のサブジェクト名と発行元を調べて、正しい証明書がインポートされ、正しい順序が維持されていることを確認してください。また、チェーンに含まれるすべての証明書と一緒に貼り付けられていることを確認してください。

- **[Signed Catalyst Center certificate]** : 件名フィールドに **CN=<FQDN of Catalyst Center>** が含まれていて、発行元が発行機関の **CN** を持っている。

注

内部認証局（CA）による署名入りの証明書をインストールする場合は、**Catalyst Center** へのアクセスに使用するすべての DNS 名（**Catalyst Center** の FQDN を含む）が証明書の **alt_names** セクションで指定されていることを確認してください。詳細については、『[Catalyst Center Security Best Practices Guide](#)』の「**Generate a Certificate Request Using Open SSL**」を参照してください。

- **[Issuing (subordinate) CA certificate that issues the Catalyst Center certificate]** : サブジェクト名のフィールドには **Catalyst Center** の証明書を発行する（下位）CA の CN が含まれており、発行元が、ルート CA の CN を持っている。
- **[Next issuing (root/subordinate CA) certificate that issues the subordinate CA certificate]** : 件名フィールドがルート CA で、発行元が件名フィールドと同じ値である。それらが同じ値でない場合は、その次の発行元を追加していきます。

Catalyst Center

Catalyst Center は、X.509 証明書と秘密キーの **Catalyst Center** へのインポートとストレージをサポートします。

Catalyst Center では、認証局（CA）からの X.509 証明書と **Catalyst Center** によって生成された秘密キーをインポートして保存できます。これらを使用して、**Catalyst Center**、ノースバウンド API アプリケーション、およびネットワークデバイスの上に安全で信頼できる環境を作成することができます。**[System Certificates]** ウィンドウで証明書と秘密キーをインポートできます。

Catalyst Center サーバー証明書を更新するには、次の手順を実行します。

1. 証明書署名要求（CSR）を生成します。
2. CSR を CA に送信して、署名付き証明書を取得します。
3. 署名付き証明書とそのチェーンを **Catalyst Center** にインポートします。

この手順では、CA の例として **Microsoft Active Directory** 証明書サービスを使用します。別の CA を使用する場合は、それに応じて手順を調整してください。

秘密キーに対応する有効な X.509 証明書を内部 CA から取得する必要があります。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**Certificate**] > [**System Certificates**] の順に選択します。

[System Certificates] ウィンドウを最初に表示したときに現在の証明書として表示されるのは、**Catalyst Center** の自己署名証明書のデータです。自己署名証明書は作成日から 1 年後に期限切れになります。

このウィンドウには、**Catalyst Center** のサーバー証明書に関する情報が表示され、これらの証明書を管理するためのアクションが提供されます。**[System Certificates]** の表には、証明書ごとに次の情報が表示されます。

- **[Issued To]** : 証明書の発行先。
- **[Issued By]** : 証明書に署名し、証明書を発行したエンティティの名前。

- **[Used For]** : 証明書がコントローラとディザスタリカバリのどちら（または両方）に使用されるかを示します。
- **[Certificate Serial Number]** : 証明書シリアル番号の最後の 5 文字を示します。
- **[Days Left]** : 証明書の有効期間の残り日数。
- **[Status]** : 証明書のステータスを表示します。
- **[Valid From/Valid To]** : 証明書が有効な時期。

注

証明書の有効な日時は、現地時間で表示されます。証明書有効期限の 2 か月前に、通知センターにシステム通知が表示されます。表示するには、ウィンドウの右上隅にある通知アイコンをクリックします。

- **[Action]** : 証明書を管理するために使用可能なアクション（表示、コピー、置換など）を示します。

2. **[+ New Certificate Request (CSR)]** をクリックします。

CSR を初めて生成するときは、この **[+ New Certificate Request (CSR)]** リンクが有効になります。

既存の CSR を使用しない場合は、既存の要求を削除してください。

- 表で、削除する要求を見つけます。
 - [Action]** で、縦の省略記号 (⋮) の上にカーソルを置き、その要求の **[Delete]** をクリックします。
 - [Delete CSR(s)]** ダイアログボックスで、コントローラの CSR を削除することを示すために、**[Controller]** チェックボックスをオンにします。その後、**[Delete]** をクリックします。
- [+ New Certificate Request (CSR)]** リンクが有効になります。

3. **[New Certificate Request (CSR)]** スライドインペインで、CSR を作成します。

- [Used For]** で、**[Controller]** チェックボックスをオンにして、コントローラに CSR を使用するようになります。
- 次の必須フィールドに値を入力します。
 - **[Key Algorithm]** : キーの生成に使用されるアルゴリズム (ECDSA または RSA) 。
 - **[Digest]** : CSR の保護および検証に使用されるダイジェストアルゴリズム。
 - **[Key Length]** : 証明書のキーのビットサイズ。
 - **[Common Name]** : サーバーの IP アドレス、ホスト名、または FQDN。
 - **[Key Usage]** : 証明書のキーの目的。使用可能な値の説明については、[『RFC 5280』の「セクション 4.2.1.3」](#) を参照してください。
 - **[Extended Key Usage]** : 証明書のキーの追加の目的。使用可能な値の説明については、[『RFC 5280』の「セクション 4.2.1.12」](#) を参照してください。

New Certificate Request (CSR)

Once you click Generate CSR we will create your CSR, and it will be available for view or download. You will then need to submit it to your provider to generate your certificate. Instructions on that process can be found [here](#).

Used For *

☐ Controller

Best practice is to use characters from the **ASCII printable character set**, and be aware that if certain special characters are keyed into the below textfields, they may not be properly rendered once the system certificate is uploaded and its information is displayed. The ASCII printable characters are those in column two or greater of the Standard Code table located [here](#).

☐ FQDN only ⓘ

Key Algorithm*

ECDSA

Algorithm used to generate the key

Key Length*

256

Key size of CSR

Key Usage*

keyEncipherment
digitalSignature

Country

Extended Key Usage*

serverAuth clientAuth

Organization

Digest*

ECDSA-256

Digest

Common Name*

Example: cisco.com

Region / State

Example: California, London, Beijing

Locality

Example: Paris, London, Moscow

Email

User submitting the CSR request

Organizational Unit

Cancel

Generate new CSR

c. **[Generate new CSR]** をクリックします。

4. CSR のコピーをダウンロードします。

a. **[Issued To]** で、CSR のハイパーリンクテキストをクリックします。

b. **[Certificate Signing Request]** スライドインペインで、**[Download CSR]** をクリックします。

CSR は Base64 ファイルとしてローカルにダウンロードされます。

c. **[Done]** をクリックしてスライドインペインを閉じます。

5. 証明書要求を CA に送信し、CA から発行元 CA チェーンをダウンロードします。

たとえば、**Microsoft Active Directory** 証明書サービスを使用して証明書要求を送信するには、次の手順を実行します。

a. 先ほどダウンロードした CSR をコピーします。

b. 新しいブラウザウィンドウで **[Active Directory Certificate Services]** を開きます。

c. **[Welcome]** ページで、**[Request a certificate]** をクリックします。

d. **[Request a Certificate]** ページで、**[advanced certificate request]** をクリックします。

- e. [Submit a Certificate Request or Renewal Request] ページで、[Saved Request] フィールドに要求を貼り付け、証明書テンプレートを選択して、[Submit] をクリックします。

選択した証明書テンプレートがクライアント認証とサーバー認証の両方に設定されていることを確認します。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

```
SzBJMBsGA1UdEQQUMBKHBArD1muHBKn+BkKHBBEB;
A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAKI
6FEYDSB3wiNm10l50dRNFxz1cbyHAW0D2E12u89W;
hrG8j15lLm9534x1TcH+CF9Y
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Catalyst Center 60 day

Additional Attributes:

Attributes:

Submit >

- f. [Certificate Issued] ページで、証明書のエンコード方法を選択し、[Download certificate chain] をクリックします。

証明書チェーンは CA からダウンロードされます。

6. 証明書発行元から p7b で証明書の完全なチェーン（サーバーおよび CA）が提供されたことを確認します。不明な場合は、次の手順を実行し、チェーンを確認して組み立てます。
 - a) p7b バンドルを DER 形式でダウンロードし、server-cert-chain.p7b として保存します。
 - b) 入力するコマンド

```
openssl pkcs7 -in server-cert-chain.p7b -inform DER -out
server-cert-chain.pem -print_certs
```

7. Catalyst Center GUI の [+ System Certificates] ウィンドウで、CSR の [Action] の下の [Import] をクリックします。
8. [Import Certificate] スライドインペインで、その証明書署名付き認証局チェーンが連結された署名付き証明書を Catalyst Center にインポートします。
 - a. [Used For] で、[Controller] チェックボックスをオンにして、コントローラにこの証明書を使用するようにします。
 - b. [Type] で、次の表を使用して証明書のファイル形式タイプを選択します。

タイプ	説明	操作
PEM Chain	プライバシー強化メールファイル形式。	[PEM Chain] をクリックします。 証明書発行元からルーズファイルで証明書とその発行元 CA チェーンが提供された場合は、次の手順を実行します。 1. PEM (base64) ファイルを収集するか、OpenSSL を使用して DER ファイルを PEM 形式に変換します。 2. 証明書とその発行元 CA を連結し、証明書から下位 CA に続いてルート CA までを <code>dnac-server-cert-chain.pem</code> ファイルに出力します。 <pre>cat certificate.pem subCA.pem rootCA.pem > server-cert-chain.pem</pre>
PKCS	公開キー暗号化標準ファイル形式。	[PKCS] をクリックします。



注

[+ New Certificate Request (CSR)] オプションを選択して証明書を要求した場合、[PKCS] ファイルタイプは無効になります。

- c. タイプに基づいてファイルをアップロードします。

アップロードするファイル

結果

PEM ファイルと、該当する場合は秘密キー

1. PEM ファイルと秘密キーファイルをドラッグアンドドロップします。

 注

- PEM ファイルには、有効な PEM 形式の拡張子（.pem、.cer、または.crt）が必須です。証明書の最大ファイルサイズは 1 MB です。
- 秘密キーには、有効な秘密キー形式の拡張子（.key）が必須です。秘密キーの最大ファイルサイズは 1 MB です。
- [+ New Certificate Request (CSR)] を使用して CSR を作成した場合、インポートする秘密キーはありません。秘密キーは Catalyst Center 内に格納されます。

2. 秘密キーについては、[Encrypted] で、暗号化するかどうかを指定します。

[Yes] を指定した場合、[Password] フィールドに秘密キーのパスワードを入力します。

PKCS ファイル

1. [Bundle Password] フィールドに証明書のパスワードを入力します。
2. PKCS ファイルをドラッグアンドドロップします。

 注

PKCS ファイルには、有効な PKCS 形式の拡張子（.pfx または .p12）が必須です。証明書の最大ファイルサイズは 1 MB です。

アップロードに成功すると、システム証明書が検証されます。

- d. [Submit] をクリックします。



注

Catalyst Center サーバーの **SSL** 証明書が置き換えられると、自動的にログアウトされます。証明書のインポートには約 **2** 分かかることがあるため、再度ログインする前に、少なくとも **2** 分待ってください。

9. **Catalyst Center** に再度ログインしたら、**[System Certificates]** ウィンドウに戻り、更新された証明書データを確認します。

更新された証明書の場合、**[Action]** で縦の省略記号 (⋮) の上にカーソルを置き、**[View]** をクリックして、有効な日付などの証明書に関する情報をスライドインペインで表示します。

管理対象デバイスを認証および識別するためのデバイス証明書の管理に関する情報。

管理対象デバイスがデバイスを認証および識別するために **Catalyst Center** によって発行された証明書を表示および管理できます。

ベストプラクティスとして、デバイスが **Catalyst Center** によって管理されなくなった場合（デバイスが失われた場合や、無効になった場合など）、デバイス証明書を取り消すか削除します。

-
1. メインメニューから次を選択します。**[System] > [Settings] > [Certificate] > [Device Certificates]** の順に選択します。

[Device Certificates] ウィンドウには、発行された証明書のステータスが個別のステータスタブに表示されます。

- **[All]** : 有効な証明書、期限切れの証明書、および期限切れ間近の証明書のリストを表示します。
- **[Expired]** : 期限切れの証明書のリストを表示します。
- **[Expiring]** : 有効期限が近づいている証明書のリストを昇順で表示します。
- **[Revoked]** : 失効した証明書のリストを表示します。

2. 有効な証明書を取り消すには、次の手順を実行します。

- a) **[All]** をクリックします。
- b) **[Action]** 列で、取り消す証明書に対応する **[Revoke]** アイコンをクリックします。
- c) 確認ウィンドウで、**[OK]** をクリックします。

3. 期限切れの証明書を削除するには、次の手順を実行します。

- a) **[All]** をクリックします。
- b) **[Action]** 列で、削除する証明書に対応する **[Delete]** アイコンをクリックします。
- c) 確認ウィンドウで、**[OK]** をクリックします。

4. 証明書の詳細を **CSV** 形式でエクスポートする場合は、**[Export]** をクリックします。
-

デバイス証明書の有効期間の設定に関する情報。**Catalyst Center**によって、ユーザーはプライベート（内部）**Catalyst Center** の **CA** で管理、モニターされているネットワークデバイスの証明書の有効期間を変更できません。

Catalyst Center では、**Catalyst Center** のプライベート（内部）**CA** で管理および監視しているネットワークデバイスの証明書の有効期間を変更できます。**Catalyst Center** での証明書の有効期間のデフォルト値は 365 日です。**Catalyst Center GUI** を使用して証明書の有効期間を変更すると、それ以降に **Catalyst Center** に対して証明書を要求するネットワークデバイスにその有効期間の値が割り当てられます。

注

デバイス証明書のライフタイム値を **CA** 証明書のライフタイム値より大きくすることはできません。さらに、**CA** 証明書の残りの有効期間が設定されたデバイスの証明書の有効期間より短い場合、デバイス証明書の有効期間の値は **CA** 証明書の残りの有効期間と同じになります。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**Certificate**] > [**Device Certificates**] の順に選択します。
2. デバイス証明書と現在のデバイス証明書の有効期間を確認します。
3. [**Device Certificates**] ウィンドウで、[**Modify**] をクリックします。
4. [**Device Certificates Lifetime**] ダイアログボックスに、新しい値を入力します（日数）。
5. [**Save**] をクリックします。

認証局 **CA** はエンティティであり、サーバーとクライアントの間の接続の確立と保護に使用される証明書やキーを管理します。

認証局 **CA** はエンティティであり、サーバーとクライアントの間の接続の確立と保護に使用される証明書やキーを管理します。**Catalyst Center** は、デバイス **CA** として機能するプライベート（内部）**Catalyst Center CA** を提供します。この **Catalyst Center CA** は、ルート **CA** として動作するか、下位 **CA** として設定できます。下位 **CA** として設定すると、元に戻すことはできません。

認証局のロールをルートから下位に変更する方法に関する情報。

デバイス **CA** は **Catalyst Center** のプライベート **CA** であり、サーバーとクライアントの間の接続の確立と保護に使用される証明書やキーを管理します。デバイス **CA** のロールをルート **CA** から下位 **CA** に変更するには、この手順を実行します。

[**Certificate Authority**] ウィンドウの **GUI** を使用して、プライベート（内部）**Catalyst Center CA** のロールをルート **CA** から下位 **CA** に変更できます。この変更を行う際は、以下ようになります。

- **Catalyst Center** を下位 **CA** として機能させる場合は、**Microsoft CA** などのルート **CA** があることを確認し、その証明書を使用することに同意してください。

- 下位 **CA** が完全に設定されていない限り、**Catalyst Center** は内部ルート **CA** としての役割を継続します。
- この手順の記述に従い、**Catalyst Center** の証明書署名要求ファイルを生成し、それが外部ルート **CA** によって手動で署名されていることを確認します。

注

Catalyst Center は、この期間中は内部ルート **CA** として実行し続けます。

- 証明書署名要求が外部ルート **CA** によって署名された後、**GUI** を使用してこの署名ファイルを **Catalyst Center** にインポートし直す必要があります（この手順の記述に従う）。
インポート後、**Catalyst Center** は下位 **CA** として自身を初期化し、下位 **CA** の既存機能をすべて提供します。
- **CA** のロールをルートから下位に切り替えると、古い **CA** は廃止され、新しい下位 **CA** の **PKI** チェーンが引き継がれます。失効リストは **CA** によって公開されます。**CA** が廃止されると、信頼を確立できないため、失効が無意味になります。未使用の証明書を最初に失効させることが組織のポリシーで規定されている場合は、**CA** のロールをルートから下位に切り替える前に、**GUI** の **[Device Certificates]** ウィンドウから証明書を失効させることができます。
デバイスの可制御性（デフォルトで有効）は、下位 **CA** から提供された新しい証明書チェーンでデバイスを自動的に更新します。新しいテレメトリ接続は、この新しい証明書チェーンでのみ認証されます。これは、オーセンティケータ側の信頼できる下位 **CA** と一致します。
- **GUI** に表示される下位 **CA** 証明書の有効期間は、証明書から直接読み取られたものであり、システム時刻を使用して計算されたものではありません。したがって今日、証明書を有効期間 1 年でインストールして来年の同じ時間に **GUI** で見ると、証明書の有効期間は 1 年間と表示されます。
- 下位 **CA** 証明書は、**.pem**、**.crt**、**.cer**、**.der** のいずれかの形式である必要があります。
- 下位 **CA** は上位の **CA** と連携しないため、上位レベルの証明書がある場合は、その失効に注意してください。このため、下位 **CA** からネットワークデバイスに対して、証明書の失効に関する情報が通知されることはありません。下位 **CA** にはこの情報がないため、すべてのネットワークデバイスは下位 **CA** を **CRL Distribution Points (CDP)** 送信元としてのみ使用します。
- プラグアンドプレイ（PnP）の **AP** プロファイルに **EAP-Transport Level Security (EAP-TLS)** 認証を使用する場合は、下位 **CA** を使用できないことに注意してください。ルート **CA** のみを使用できます。

ルート **CA** 証明書のコピーが必要です。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Certificate Authority]** の順に選択します。
2. **[CA Management]** で、既存のルートまたは下位 **CA** 証明書の設定情報（現在の証明書の **CA** モード、証明書発行者、発行先、および有効期間値）を確認します。
3. ルート **CA** から下位 **CA** に変更するには、**[Enable SubCA Mode]** をクリックします。
4. 表示される警告内容を確認します。

次に例を示します。

- ルート **CA** から下位 **CA** に変更するプロセスは元に戻すことができません。

- ルート CA モードで登録された、または証明書が発行されたネットワーク デバイスがないことを確認する必要があります。下位 CA に変更する前に、ルート CA モードで登録されているデバイスを取り消します。
 - 下位 CA の設定プロセスが終了しなければ、ネットワークデバイスをオンラインにできません。
5. [OK] をクリックして続行します。
 6. [Import External Root CA Certificate Chain] フィールドにルート CA 証明書をドラッグアンドドロップして、[Upload] をクリックします。
 ルート CA 証明書が Catalyst Center にアップロードされ、証明書署名要求の生成に使用されます。
 アップロードプロセスが完了すると、「Certificate Uploaded Successfully」というメッセージが表示されます。
 7. [Next] をクリックします。
 Catalyst Center で証明書署名要求が生成されて表示されます。
 8. Catalyst Center で生成された証明書署名要求を GUI で確認し、次のアクションのいずれかを実行します。
 - [Download] リンクをクリックして、証明書署名要求ファイルのローカルコピーをダウンロードします。
 その後、この証明書署名要求ファイルを電子メールに添付して、ルート CA に送信することができます。
 - [Copy to the Clipboard] リンクをクリックして、証明書署名要求ファイルの内容をコピーします。
 その後、この証明書署名要求の内容を電子メールに貼り付けるか、電子メールに添付ファイルとして添付して、ルート CA に送信することができます。
 9. 証明書署名要求ファイルをルート CA に送信します。
 ルート CA から下位 CA ファイルが返されます。このファイルを Catalyst Center にインポートし直す必要があります。
 10. ルート CA から下位 CA ファイルを受信した後、Catalyst Center の GUI に再度アクセスし、[Certificate Authority] ウィンドウに戻ります。
 11. [CA Management] タブをクリックします。
 12. [Change CA mode] ボタンの [Yes] をクリックします。
 [Yes] をクリックすると、GUI に証明書署名要求が表示されます。
 13. [Next] をクリックします。
 [Certificate Authority] ウィンドウに、[Import SubCA Certificate] フィールドが表示されます。
 14. 下位 CA 証明書を [Import SubCA Certificate] フィールドにドラッグアンドドロップして、[Apply] をクリックします。
 下位 CA 証明書が Catalyst Center にアップロードされます。
 アップロードが完了すると、GUI の [CA Management] タブに、下位 CA モードが表示されます。
 15. [CA Management] タブのフィールドを確認します。
 - [Sub CA Certificate] : 現在の下位 CA 証明書を表示します。
 - [External Root CA Certificate] : ルート CA 証明書を表示します。
 - [Sub CA Certificate Lifetime] : 下位 CA 証明書の有効期間を表示します。

- **[Current CA Mode]** : SubCA モードを表示します。

CA

既存下位 CA の有効期間の **70%** が経過した後のロールオーバー CA 証明書のプロビジョニングに関する情報。

Catalyst Center では、既存の下位 CA の有効期間が **70%** 以上経過している場合、ロールオーバー下位 CA として下位証明書を保存できます。

- 下位 CA ロールオーバー プロビジョニングを開始するには、認証局のロールを下位 CA モードに変更しておく必要があります。[認証局のロールをルートから下位に変更 \(35ページ\)](#) を参照してください。
- 現在の下位 CA 証明書の有効期限が **70%** 以上経過していることが必要です。この状態になると、**Catalyst Center** の **[CA Management]** タブの下に **[Renew]** ボタンが表示されます。
- ロールオーバー下位 CA の署名付き証明書のコピーが必要です。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Certificate] > [Certificate Authority]** の順に選択します。

2. **[CA Management]** タブで、CA 証明書の設定情報を確認します。

- **[Subordinate CA Certificate]** : 現在の下位 CA 証明書を表示します。
- **[External Root CA Certificate]** : ルート CA 証明書を表示します。
- **[Subordinate CA Certificate Lifetime]** : 現在の下位 CA 証明書の有効期間を表示します。
- **[Current CA Mode]** : SubCA モードを表示します。

3. **[Renew]** をクリックします。

Catalyst Center は既存の下位 CA を使用して、ロールオーバー下位 CA の証明書署名要求を生成し、表示します。

4. 生成された証明書署名要求を GUI で確認し、次のアクションのいずれかを実行します。

- **[Download]** リンクをクリックして、証明書署名要求ファイルのローカルコピーをダウンロードします。
その後、この証明書署名要求ファイルを電子メールに添付して、ルート CA に送信することができます。
- **[Copy to the Clipboard]** リンクをクリックして、証明書署名要求ファイルの内容をコピーします。
その後、この証明書署名要求の内容を電子メールに貼り付けるか、電子メールに添付ファイルとして添付して、ルート CA に送信することができます。

5. 証明書署名要求ファイルをルート CA に送信します。

次にルート CA がロールオーバー下位 CA ファイルを返送してくると、それを **Catalyst Center** にインポートし直す必要があります。

下位 CA ロールオーバーの証明書署名要求は、RootCA モードから SubCA モードに切り替えた際にインポートした下位 CA に署名したルート CA と同じルート CA によって署名される必要があります。

6. ルート CA からロールオーバー下位 CA ファイルを受信した後、[Certificate Authority] ウィンドウに戻ります。
7. [CA Management] タブをクリックします。
8. 証明書署名要求が表示されている GUI で [Next] をクリックします。
[Certificate Authority] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。
9. 下位ロールオーバー CA 証明書を [Import Sub CA Certificate] フィールドにドラッグアンドドロップし、[Save] をクリックします。
ロールオーバー下位 CA 証明書が Catalyst Center にアップロードされます。
アップロードが終了すると、GUI が変更され、[CA Management] タブの [Renew] ボタンが無効になります。

SCEP

Catalyst Center では、ネットワークデバイスへの証明書の登録とプロビジョニングに Simple Certificate Enrollment Protocol (SCEP) が使用されます。

Catalyst Center では、ネットワークデバイスへの証明書の登録とプロビジョニングに Simple Certificate Enrollment Protocol (SCEP) が使用されます。独自の SCEP ブローカと証明書サービスを使用したり、外部の SCEP ブローカを使用したりできます。外部 SCEP ブローカを設定するには、以下の手順を実行します。

注

SCEP の詳細については、「[Simple Certificate Enrollment Protocol Overview](#)」を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [Certificate] > [Certificate Authority] の順に選択します。
2. [Certificate Authority] ウィンドウで、[Use external SCEP broker] オプションボタンをクリックします。
3. 外部証明書をアップロードするには、次のいずれかのオプションを使用します。
 - ファイルを選択する
 - ドラッグアンドドロップしてアップロードする

注

.pem、.crt、.cer などのファイルタイプのみ使用できます。ファイルサイズは 1 MB を超えることはできません。

4. [Upload] をクリックします。

5. デフォルトでは、**[Manages Device Trustpoint]** が有効になっています。つまり、デバイスで **sdn-network-infra-iwan** トラストポイントが設定されます。**Catalyst Center** 次の手順を完了する必要があります。
 - a) デバイスが **SCEP** 経由で証明書を要求する登録 URL を入力します。
 - b) (任意) 証明書で使用する任意のサブジェクトフィールド (国、地域、州、組織、組織単位など) を入力します。共通名 (**CN**) は、デバイスのプラットフォーム ID とデバイスのシリアル番号を使用して **Catalyst Center** によって自動的に設定されます。
 - c) **[Revocation Check]** フィールドで、ドロップダウンリストをクリックし、適切な失効チェックオプションを選択します。
 - d) (任意) **[Auto Renew]** チェックボックスをオンにして、自動登録の割合を入力します。

[Manages Device Trustpoint] が無効になっている場合、デバイスが有線およびワイヤレスのアシユアランスステレメトリを **Catalyst Center** に送信するようにするため、デバイスに手動で **sdn-network-infra-iwan** トラストポイントを設定し、証明書をインポートする必要があります。「[デバイス証明書トラストポイントの設定](#)」を参照してください。

6. **[Save]** をクリックします。

外部 CA 証明書がアップロードされます。

アップロードされた外部証明書を置き換える場合は、**[Replace Certificate]** をクリックし、必要な詳細を入力します。

外部証明書をアップロードした後に内部 PKI 証明書に切り替えることに関する情報。

外部証明書をアップロードした後、内部証明書に切り替える場合は、次の手順を実行します。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Certificate] > [Certificate Authority]** の順に選択します。
2. **[Certificate Authority]** ウィンドウで、**[Use Catalyst Center]** オプションボタンをクリックします。
3. **[Switching back to Internal Certificate Authority]** アラートで、**[Apply]** をクリックします。

[Settings have been updated] メッセージが表示されます。詳細については、[認証局のルールをルートから下位に変更](#) (35ページ) を参照してください。

Catalyst Center

デバイスを認証するための AAA サーバーまたは Cisco ISE サーバーなどの外部エンティティの設定に必要なデバイス証明書をダウンロードできます。

Catalyst Center では、デバイスを認証するための AAA サーバーまたは Cisco ISE サーバーなどの外部エンティティの設定に必要なデバイス証明書をダウンロードできます。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Certificate] > [Certificate Authority]** の順に選択します。

2. **[Download]** をクリックして、デバイス **CA** をエクスポートし、信頼できる **CA** として外部エンティティに追加します。

CA

CA のリセット機能は、更新に問題がある場合や **CA** の有効期限が切れた場合に、ユーザーが **CA** を管理するのに役立ちます。

更新の問題または期限切れの間に **CA** を管理するには、**CA** のリセット機能を使用します。有効期間が定義されたサブ **CA** を作成できます。この機能により、サブ **CA** の有効期限が切れた場合、または別のサブ **CA** に切り替える場合、**CA** を簡単にリセットできます。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Certificate] > [Certificate Authority]** の順に選択します。
2. **CA** テーブルで、リセットする要求を見つけます。 **[Action]** で、縦の省略記号 (⋮) の上にカーソルを置き、 **[Reset to Default]** をクリックします。
3. **[Warning]** メッセージで **[Yes]** をクリックします。

証明書を **RootCA** にリセットするには、最大 5 分かかる場合があります。数分後に **CA** ページを更新し、更新されたステータスを確認します。

[Manages Device Trustpoint] が無効になっている場合に、デバイスが有線およびワイヤレス **Assurance** テレメトリを **Catalyst Center** に送信するためのデバイス証明書トラストポイントの構成に関する情報。

Catalyst Center で **[Manages Device Trustpoint]** が無効になっている場合、デバイスが有線およびワイヤレス **Assurance** テレメトリを **Catalyst Center** に送信するようにするため、デバイスに手動で **sdn-network-infra-iwan** トラストポイントを設定し、証明書をインポートする必要があります。

この手動設定の手順は、**SCEP** を介して外部 **CA** から登録する必要があります。

1. 次のコマンドを入力します。

```
crypto pki trustpoint sdn-network-infra-iwan
  enrollment url http://<SCEP_enrollment_URL_to_external_CA>
  fqdn <device_FQDN>
  subject-name
  CN=<device_platform_ID>_<device_serial_number>_sdn-network-infra-iwan
  revocation-check <crl, crl none, or none> # to perform revocation check
  with CRL, CRL fallback to no check, or no check
  rsakeypair sdn-network-infra-iwan
  fingerprint <CA_fingerprint> # to verify that the CA at the url connection
  matches the fingerprint given
```

2. (任意、ただし推奨) 証明書を自動的に更新し、証明書の有効期限を回避します。

```
auto-enroll 80 regenerate
```

3. (任意) 登録 URL に到達可能なインターフェイスを指定します。それ以外の場合、http サービスの送信元インターフェイスがデフォルトで設定されます。

```
source interface <interface>
```

Catalyst Center は、シスコからの信頼できる証明書バンドルのインポートとストレージをサポートしています。この信頼できる証明書バンドルは、有効なプロフェッショナルのサードパーティベンダーが発行した、または自己署名デジタル証明書の提示に対し、**Catalyst Center** およびそのアプリケーションを認証するためにシスコ ネットワーキング デバイスで使用されます。

Catalyst Center には、事前インストールされているシスコの信頼できる証明書バンドル（シスコが信頼する外部ルートバンドル）が含まれています。**Catalyst Center** は、シスコからの更新された信頼できる証明書バンドルのインポートとストレージもサポートしています。信頼できる証明書バンドルは、**Catalyst Center** およびそのアプリケーションとの信頼関係を確立するために、サポートされるシスコ ネットワーキング デバイスによって使用されます。

注

シスコの信頼できる証明書バンドルは、サポートされているシスコデバイスのみをアンバンドルして使用できる、**ios.p7b** と呼ばれるファイルです。この **ios.p7b** ファイルには、シスコを含む有効な認証局のルート証明書が含まれています。このシスコの信頼できる証明書バンドルは、**Cisco cloud (Cisco InfoSec)** で使用できます。このバンドルは <https://www.cisco.com/security/pki/> にあります。

信頼できる証明書バンドルは、同じ **CA** を使用してすべてのネットワークデバイス証明書と **Catalyst Center** 証明書を管理するための安全で便利な方法を提供します。**Catalyst Center** は信頼できる証明書バンドルを使用して、自身の証明書とプロキシゲートウェイ証明書を検証し、証明書が有効な **CA** 署名付き証明書であるかどうかを判断します。さらに、**PnP** ワークフローの開始時にネットワーク **PnP** 対応デバイスにアップロードできるように、また、その後の **HTTPS** ベースの接続で **Catalyst Center** を信頼できるように、信頼できる証明書バンドルを使用できます。

GUI の **[Trusted Certificates]** ウィンドウを使用して、シスコの信頼できる証明書バンドルをインポートします。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Certificates] > [Trusted Certificates]** の順に選択します。
2. **[Trusted Certificates]** ウィンドウで、**[Update trusted certificates now]** ハイパーリンクをクリックして信頼できる証明書バンドルの新規ダウンロードおよびインストールを開始します。

このハイパーリンクは、**ios.p7b** ファイルの更新バージョンが使用可能で、インターネットアクセスが可能なときにのみ表示されます。

Catalyst Center に新しい信頼できる証明書バンドルがダウンロードおよびインストールされると、Catalyst Center はシスコのデバイスのダウンロードをサポートするよう、この信頼できる証明書バンドルを使用可能にします。

3. 新しい証明書ファイルをインポートする場合は、[Import] をクリックしてローカルシステムから有効な証明書ファイルを選択し、[Import Certificate] ウィンドウで [Import] をクリックします。
 4. [Export] をクリックして、証明書をエクスポートします。
-

第

4 Cisco

章

:

- [□□□□□□□□□□](#)
- [□□□□□□□□□□□□](#)
- [□□□□□□□□□□](#)
- [□□□□□□□□](#)
- [□□□□□□□□](#)

プラグアンドプレイ (PnP) のコントローラとして **Catalyst Center** を登録し、**Cisco PnP Connect** クラウドポータルから **Catalyst Center** の PnP にデバイスインベントリを同期することについての情報

Catalyst Center を、**Cisco Plug and Play (PnP) Connect** のコントローラとして、リダイレクトサービス用に **Cisco** スマートアカウントに登録できます。これにより、**Cisco PnP Connect** クラウドポータルから **Catalyst Center** の PnP に、デバイスインベントリを同期することができます。

SUPER-ADMIN-ROLE またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザーのみがこの手順を実行することができます。

スマートアカウントで、特定の機能の実行を許可するロールがユーザーに割り当てられます。

- スマートアカウント管理者ユーザーは、すべてのバーチャルアカウントにアクセスできます。
- ユーザーは、割り当てられたバーチャルアカウントにのみアクセスできます。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**Cisco Accounts**] > [**PnP Connect**] の順に選択します。

PnP 接続プロファイルのテーブルが表示されます。

2. **Cisco.com** ユーザーを設定済みの場合は、ステップ 3 に進みます。設定していない場合は、次の手順を実行します。

- a) ブラウザでシークレットウィンドウまたはプライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。
- b) 別の **Catalyst Center GUI** インスタンスを開いてログインします。
- c) [**PnP Connect**] ウィンドウの別のインスタンスを開きます。
- d) [**Cisco.com ID**] フィールドで、[**Add**] リンクをクリックします。
- e) [**Information**] ポップアップウィンドウで、次のチェックボックスの一方または両方をオンにして、[**Authenticate**] をクリックします。

- 必須 : [**I am in private or incognito mode**]

- オプション : [**Save Credentials**]

- f) [**Activate your device**] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[**Next**] をクリックします。
- g) [**Log in**] ポップアップウィンドウで、**cisco.com** ユーザーの電子メールアドレスを入力し、[**Next**] をクリックします。
- h) [**Verify with your password**] ポップアップウィンドウで、**cisco.com** ユーザーのパスワードを入力し、[**Verify**] をクリックします。

[**Device Activated**] ポップアップウィンドウが表示されます。

- i) [**Device Activated**] ポップアップウィンドウを閉じます。
- j) [**PnP Connect**] ウィンドウを更新します。
- k) [**Cisco.com ID**] フィールドに、ユーザーに対して入力した電子メールアドレスが表示されていることを確認します。また、[**Change**] リンクが表示されていることを確認します。

3. [**Register**] をクリックして、バーチャルアカウントに登録します。

4. [Register Virtual Account] ウィンドウで、設定したスマートアカウントが [Select Smart Account] ドロップダウンリストに表示されます。[Select Virtual Account] ドロップダウンリストからアカウントを選択できます。
5. 必要な [IP] または [FQDN] オプションボタンをクリックします。
6. コントローラの IP アドレスまたは FQDN（完全修飾ドメイン名）を入力します。
7. プロファイル名を入力します。指定した設定を使用して、選択したバーチャルアカウントのプロファイルが作成されます。
8. [Use as Default Controller Profile] チェックボックスをオンにして、この Catalyst Center コントローラを Cisco PnP Connect クラウドポータルにデフォルトコントローラとして登録します。
9. [登録 (Register)] をクリックします。

PnP

プラグアンドプレイ（PnP）イベントが Catalyst Center で発生する際に通知を受け取るためのイベント通知の作成に関する情報。

イベント通知を作成することで、プラグアンドプレイ（PnP）イベントが Catalyst Center で発生するたびに通知を受け取ります。サポートされているチャンネルを設定し、イベント通知を作成する方法については、『[Cisco Catalyst Center Platform User Guide](#)』の「Work with Event Notifications」[英語]を参照してください。

次の PnP イベントのイベント通知を作成してください。

イベント名	イベント ID	説明
デバイスの追加に失敗しました。	NETWORK-TASK_FAILURE-3-008	デバイスは、単一または一括インポートでは追加されません。単一または一括インポートによってデバイスを追加すると、エラーが発生します。
デバイスの追加に成功しました。	NETWORK-TASK_COMPLETE-4-007	単一または一括インポートによってデバイスが正常に追加されました。
デバイスはエラー状態です。	NETWORK-ERROR_1-002	デバイスはエラー状態になります。
デバイスはプロビジョニング状態です。	NETWORK-INFO_4-003	デバイスはプロビジョニング状態になります。
デバイスがオンボーディング状態でスタックします。	NETWORK-TASK_PROGRESS-2-006	デバイスが 15 分以上オンボーディング状態でスタックしています。
デバイスが請求を待っています。	NETWORK-INFO_2-001	デバイスは未請求の状態になり、プロビジョニングの準備ができています。
スマートアカウントの同期に失敗しました。	NETWORK-TASK_FAILURE-1-005	一部のデバイスでスマートアカウントの同期に失敗しました。
スマートアカウントの同期に成功しました。	NETWORK-TASK_COMPLETE-4-004	一部のデバイスで、スマートアカウントの同期に成功しました。

Catalyst Center のシスコのクレデンシャルの設定についての情報。

次の手順を使用して、**Catalyst Center** でソフトウェアイメージや更新プログラムのダウンロードに使用するログイン情報を設定します。ログイン情報は、シスコの **Web** サイトにログインするために使用するユーザー名とパスワードです。

重要

- シスコは新しい認証インフラストラクチャを導入しました。そのため、**Cisco.com** ユーザーが設定されている **Catalyst Center** リリース **2.3.7.7** からデータをバックアップし、そのデータを **Catalyst Center** リリース **3.1.3** で復元する場合は、そのユーザーを再認証する必要があります。
- Catalyst Center** では、セキュリティ上の理由で、**Cisco.com** ユーザーのログイン情報はローカルに保存されなくなりました。

SUPER-ADMIN-ROLE 権限またはシステム設定への「書き込み」権限のある **CUSTOM-ROLE** を持つユーザーのみがこの手順を実行できます。詳細については、[ユーザ ロールについて](#) (162ページ) を参照してください。

-
- メインメニューから次を選択します。[**System**] > [**Settings**] > [**Cisco Accounts**] > [**Cisco.com Credentials**] の順に選択します。
 - 次の手順で **Cisco.com** ユーザーを設定します。
 - ブラウザでシークレット/プライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。
 - 別の **Catalyst Center** GUI インスタンスを開いてログインします。
 - [**Cisco.com Credentials**] ウィンドウの別のインスタンスを開きます。
 - [**Cisco.com ID**] フィールドで、[**Add**] リンクをクリックします。
 - [**Information**] ポップアップウィンドウで [**I am in private or incognito mode**] チェックボックスをオンにして、[**Proceed**] をクリックします。
 - [**Activate your device**] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[**Next**] をクリックします。
 - [**Log in**] ポップアップウィンドウで、**cisco.com** ユーザーの電子メールアドレスを入力し、[**Next**] をクリックします。
 - [**Verify with your password**] ポップアップウィンドウで、**cisco.com** ユーザーのパスワードを入力し、[**Verify**] をクリックします。

[**Device Activated**] ポップアップウィンドウが表示されます。
 - ユーザーが正常に設定されたことを確認します。
 - [**Device Activated**] ポップアップウィンドウを閉じます。
 - [**Cisco.com Credentials**] ページを更新します。
 - [**Cisco.com ID**] フィールドに、ユーザーに対して入力した電子メールアドレスが表示されていることを確認します。また、[**Change**] リンクと [**Delete**] リンクの両方が表示されていることを確認します。
-

Catalyst Center のシスコのクレデンシャル消去についての情報。シスコのクレデンシャルは、シスコの顧客またはパートナーとして制限付きの場所にアクセスするために、シスコの **Web** サイトのログインに使用するユーザー名とパスワードです。

Catalyst Center に対して現在設定されている **cisco.com** のクレデンシャルを削除するには、次の手順を実行します。

 注

- ソフトウェアのダウンロードやデバイスのプロビジョニングに関連するタスクを実行する際、**cisco.com** のログイン情報が設定されていないと、タスクの開始前にログイン情報を入力するように求められます。入力したログイン情報を保存して **Catalyst Center** 全体で使用するには、表示されたダイアログボックスで **[Save for Later]** チェックボックスをオンにします。それ以外の場合は、これらのタスクを実行するたびにログイン情報を入力する必要があります。
- この手順を完了すると、エンドユーザーライセンス契約 (EULA) の承認が取り消されます。EULA の承認を再入力する方法については、[ライセンス契約書の受諾](#) (63ページ) を参照してください。

SUPER-ADMIN-ROLE 権限またはシステム設定への「書き込み」権限のある **CUSTOM-ROLE** を持つユーザーのみがこの手順を実行できます。詳細については、[ユーザロールについて](#) (162ページ) を参照してください。

-
- メインメニューから次を選択します。[**System**] > [**Settings**] > [**Cisco Accounts**] > [**Cisco.com Credentials**] の順に選択します。
 - [**Delete**] リンクをクリックします。
 - 表示されたダイアログボックスで、[**Delete**] をクリックして操作を確定します。
-

Cisco スマートアカウントのログイン情報の設定に関する情報。このログイン情報は、スマートライセンスアカウントに接続する目的で使用されます。

シスコスマートアカウントのログイン情報は、スマートライセンスアカウントに接続する目的で使用されます。ライセンスマネージャツールは、権限付与とライセンス管理のために、このスマートアカウントの詳細なライセンス情報を使用します。

重要

シスコは新しい認証インフラストラクチャを導入しました。そのため、スマートアカウントのログイン情報が設定された **Catalyst Center** リリース **2.3.7.7** からデータをバックアップし、そのデータを **Catalyst Center** リリース **3.1.3** で復元する場合は、関連付けられたスマートアカウントを再認証する必要があります。

SUPER-ADMIN-ROLE 権限またはシステム設定への「書き込み」権限のある CUSTOM-ROLE を持っていることを確認してください。

1. メインメニューから次を選択します。[System] > [Settings] > [Cisco Accounts] > [Smart Account] の順に選択します。
2. 適切なスマートアカウントユーザーとスマートアカウント名をスマート ライセンス アカウントにリンクします。
 - a) ブラウザでシークレット/プライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。
 - b) 別の Catalyst Center GUI インスタンスを開いてログインします。
 - c) [Smart Account] ウィンドウの別のインスタンスを開きます。
 - d) [Add] リンクをクリックします。
 - e) [Information] ポップアップウィンドウで [I am in private or incognito mode] チェックボックスをオンにして、[Proceed] をクリックします。
 - f) [Activate your device] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[Next] をクリックします。
 - g) [Log in] ポップアップウィンドウで、cisco.com ユーザの電子メールアドレスを入力し、[Next] をクリックします。
 - h) [Verify with your password] ポップアップウィンドウで、cisco.com ユーザーのパスワードを入力し、[Verify] をクリックします。

[Device Activated] ポップアップウィンドウが表示されます。

- i) 追加したスマートアカウントユーザーが [Smart Account Credentials] セクションと [Expired Smart Accounts] セクションの両方に表示されていることを確認します。

スマートアカウントユーザーの状態	結果
両方のセクションに記載されている	[Actions] 列のゴミ箱アイコンをクリックして、[Expired Smart Accounts] セクションからユーザーを削除します。
両方のセクションに記載されていない	ステップ 3 に進みます。

3. 選択したスマートアカウントの名前を変更するには、[Change] をクリックします。Cisco SSM クラウドでスマート ライセンス アカウントへの接続に使用されるスマートアカウントを選択するように促されます。
 - a) ドロップダウンリストから [Smart Account] を選択します。
 - b) [Save] をクリックします。
4. [View all virtual accounts] をクリックし、そのスマートアカウントに関連付けられているすべてのバーチャルアカウントを表示します。

 注

シスコ アカウントは複数のスマートアカウントとバーチャルアカウントをサポートしています。

5. (オプション) スマートライセンス対応デバイスをバーチャルアカウントに自動登録する場合、[Auto register smart license enabled devices] チェックボックスをオンにします。スマートアカウントに関連付けられているバーチャルアカウントのリストが表示されます。
6. 必要なバーチャルアカウントを選択します。スマートライセンス対応デバイスがインベントリに追加されるたびに、選択したバーチャルアカウントに自動的に登録されます。
7. ライセンスを取得したスマートアカウントユーザーとそれに関連する履歴データを削除する場合は、[Delete historical information] をクリックします。
[Delete Historical Data] スライドインペインには、ライセンスを取得したスマートアカウントユーザーが表示されます。また、Catalyst Center に現在存在していない既存のスマートアカウントも表示されますが、それらの履歴データは引き続き利用できます。
8. [Smart Account list] エリアで、削除するスマートアカウントの横にあるチェックボックスをオンにします。
9. [Delete] をクリックします。
10. 次の確認ウィンドウで、[Delete] をクリックします。
11. [Delete the associated license historical information] チェックボックスをオンにして、関連するライセンスの履歴情報を削除します。

使用可能な Catalyst Center ライセンスを表示するためのスマートライセンス用の仮想アカウントの登録に関する情報。

シスコ スマート ライセンシングを使用すると、Cisco SSM に Catalyst Center を登録できます。

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 (software.cisco.com)。

シスコライセンスの詳細については、cisco.com/go/licensingguide を参照してください。

 注

Catalyst Center インスタンスのスマートライセンス登録は、次の接続モードを使用してサポートされています。

- 直接
- オンプレミス Cisco SSM
- スマートプロキシ

- スマートライセンスを有効にするには、Cisco クレデンシャルを設定し（「[シスコのログイン情報の設定](#)（48ページ）」を参照）、Cisco SSM で Catalyst Center ライセンス規則をアップロードする必要があります。
- スマートライセンスを有効にするには、**[System] > [Settings] > [Cisco Accounts] > [Smart Account]** でスマートアカウントを追加する必要があります。詳細については、[スマートアカウントの設定](#)（49ページ）を参照してください。

-
1. メインメニューから次を選択します。**[System] > [Settings] > [Cisco Accounts] > [Smart Licensing]** の順に選択します。
デフォルトでは、**[Smart Account]** の詳細が表示されます。
 2. 登録するバーチャルアカウントを **[Search Virtual Account]** ドロップダウンリストから選択します。
 3. **[Register]** をクリックします。
 4. 登録が正常に完了したら、**[View Available Licenses]** リンクをクリックして、Catalyst Center の使用可能なライセンスを確認します。
-

Catalyst Center と連携するネットワーク内のスマート対応デバイスと Cisco Smart Software Manager (SSM) の間の接続を管理するための接続モードの設定に関する情報。

接続モードは、Catalyst Center と連携するネットワーク内のスマート対応デバイスと Cisco Smart Software Manager (SSM) の間の接続を管理します。異なる接続モードを設定するには、SUPER-ADMIN アクセス権限が必要です。

SSM の SSL 証明書には、SAN フィールド内の関連する IP アドレスが含まれている必要があります。

-
1. メインメニューから次を選択します。**[System] > [Settings] > [Cisco Accounts] > [SSM Connection Mode]** の順に選択します。
以下の接続モードがあります。

- 直接
- オンプレミス **CSSM**
- スマートプロキシ

2. Cisco SSM クラウドへの直接接続を有効にするには、**[Direct]** を選択します。
3. 組織のセキュリティを高める必要がある場合は、**[On-Prem CSSM]** を選択します。オンプレミスオプションでは、Cisco SSM クラウドでライセンスを管理する際に、インターネットで直接接続する代わりに Cisco SSM 機能のサブセットにアクセスできます。

- a) **[On-Prem CSSM]** を有効にする前に、サテライトがネットワークサイトに展開されて稼働していることを確認してください。

サテライトが FQDN で設定されている場合、サテライト FQDN の **Call Home** 設定が IP アドレスの代わりにプッシュされます。

デュアルスタック IPv4/IPv6 展開では、オンプレミス CSSM は FQDN を使用する必要があります。IP アドレスを入力すると、**Catalyst Center** は代わりに FQDN を入力するように求めます。この要件は、新規インストールとシステムアップグレードの両方に適用されます。

- b) **[On-Prem CSSM Host]**、**[Smart Account Name]**、**[Client ID]**、および **[Client Secret]** の詳細を入力します。

[Smart Account] フィールドに、1 つの SSM オンプレミスアカウント名のみを入力します。スペースやアンダースコアは使用できません。

オンプレミス CSSM の設定中にホスト/IP の値を変更できます。これは、既存の設定に必要な FQDN 形式に更新する必要があるアップグレードの場合に特に役立ちます。ホスト/IP を変更すると、デバイスが SSM 接続モード設定と非同期になる可能性があることに注意してください。

クライアント ID とクライアントシークレットを取得する方法については、『[Cisco Smart Software Manager On-Prem User Guide](#)』を参照してください。

- c) **[Test Connection]** をクリックして Cisco SSM 接続を検証します。
- d) **[Save]** をクリックしてから **[Confirm]** をクリックします。
- e) 変更した SSM で再登録が必要なデバイスがある場合は、**[Need to Re-Register Devices]** ダイアログボックスが表示されます。ダイアログボックスで **[OK]** をクリックします。
- f) **[Tools] > [License Manager] > [Devices]** ウィンドウで、再度登録するデバイスを選択し、**[Sync Connection Mode]** をクリックします。

注

このようなデバイスには、「接続モードが同期していない (Connection Mode out of sync)」旨のタグまたはメッセージが表示されます。

- g) **[Resync Devices]** ダイアログボックスで、次の手順を実行します。
 - **[Smart Account]** を入力します。
 - **[Virtual Account]** を入力します。
 - **[Now]** をクリックしてすぐに再同期を開始するか、**[Later]** をクリックして特定の時間に再同期をスケジュールします。
 - **[Resync]** をクリックします。

[Recent Tasks] ウィンドウには、デバイスの再同期ステータスが表示されます。

4. **[Smart Proxy]** を選択し、**Catalyst Center** を介して **Cisco SSM** クラウドにスマート対応デバイスを登録します。このモードでは、デバイスを **Cisco SSM** クラウドに直接接続する必要はありません。**Catalyst Center** は、デバイスからの要求を自身を介して **Cisco SSM** クラウドにプロキシします。

Call Home 設定をデバイスにプロビジョニングするときに、サテライトが **FQDN** で設定されている場合、**IP** アドレスの代わりにサテライトの **FQDN** がプッシュされます。

第

5

章

:

- [配置管理](#)
- [配置管理数据库](#)
- [PnP 配置管理](#)
- [配置管理](#)
- [配置管理数据库](#)
- [SNMP 配置管理](#)
- [ICMP ping 配置](#)
- [PnP 配置管理 AP 配置](#)
- [配置管理](#)
- [SSH 配置管理](#)
- [配置管理数据库](#)
- [配置管理数据库](#)

ソフトウェアイメージを格納および配布するイメージ配布サーバーの設定に関する情報です。

イメージ配信サーバーは、ソフトウェアイメージの保管と配信に役立ちます。ソフトウェアイメージを配信するように最大 **3** つの外部イメージ配信サーバーを設定できます。また、新しく追加されたイメージ配信サーバーに **1** つ以上のプロトコルを設定できます。

サポートされているサーバーの詳細については、[バックアップサーバーの要件](#)（228ページ）の「自動化データバックアップのサーバー要件」を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [Device Settings] > [Image Distribution Servers]。

2. [Image Distribution Servers] ウィンドウで、[Servers] をクリックします。

[Image Distribution Servers] テーブルには、イメージ配信サーバーのホスト、ユーザー名、SFTP、SCP、および接続に関する詳細が表示されます。

3. [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server] スライドインペインが表示されます。

4. イメージ配信サーバーの次の項目を設定します。

- [Host] : イメージ配信サーバーのホスト名または IP アドレスを入力します。
- [Root Location] : ファイル転送用の作業ルートディレクトリ。

注

Cisco AireOS ワイヤレスコントローラの場合、設定されたパスが 16 文字を超えると、イメージの配信は失敗します。

- [Username] : イメージ配信サーバーへのログインに使用されるユーザー名を入力します。ユーザー名には、サーバーの作業ルートディレクトリに対する読み取り/書き込み権限が必要です。
- [Password] : イメージ配信サーバーへのログインに使用されるパスワード。
- [ポート番号] : イメージ配信サーバーが実行されているポート番号を入力します。

5. [Save] をクリックします。

6. 一部のワイヤレスコントローラの旧バージョンのソフトウェアでは、SFTP の暗号方式として弱い暗号方式（SHA1 ベースの暗号など）しかサポートされていないため、Catalyst Center でソフトウェアイメージの管理やワイヤレスアシュアランスの設定を行うには、ワイヤレスコントローラからの SFTP 接続に対して SFTP 互換モードを有効にする必要があります。Catalyst Center の SFTP サーバーでは、弱い暗号方式のサポートを最大 90 日間まで一時的に有効にすることができます。弱い暗号を許可するには、以下を実行します。

- a) SFTP サーバーの IP アドレスの横にある [i] アイコンにカーソルを合わせ、[Click here] をクリックします。
- b) [Compatibility Mode] スライドインペインで [Compatibility Mode] チェックボックスをオンにして期間（1 分～90 日）を入力します。
- c) [Save] をクリックします。

7. オプション: 設定を編集するには、対応するイメージ配信サーバーの横にある **[Edit]** アイコンをクリックし、必要な変更を行って **[Save]** をクリックします。
8. オプション: イメージ配信サーバーを削除するには、イメージ配信サーバーの横にある **[Delete]** アイコンをクリックし、**[Delete]** をクリックします。

ワイヤレスコントローラから AP に HTTPS 経由でイメージを転送します。

ワイヤレスコントローラは、イメージが AP に配布された後、AP にイメージをプッシュします。Catalyst Center では、ワイヤレスコントローラから HTTPS 経由で AP でイメージをダウンロードできます。このアウトオブバンドファイル転送は、AP イメージを効率的にアップグレードするための方式です。

1. メインメニューから次を選択します。 **[System > Settings > Device Settings > Software Image Management]**
2. **[Access Point Image Transfer]** タブをクリックします。
3. **[Image Transfer Settings]** ドロップダウンリストをクリックし、**[Use HTTPS Only]** を選択します。

このオプションにより、ワイヤレスコントローラから AP へのすべてのイメージ転送で HTTPS プロトコルのみが使用されます。ワイヤレスコントローラで HTTPS が有効になっていない場合、イメージ転送に対してのみ有効になり、イメージ転送後に無効になります。

PnP

プラグアンドプレイ (PnP) デバイスの認証の有効化に関する情報。

デバイスで認証を有効にするには、次の手順を実行します。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Device Settings]** の順に選択します。
2. **[Device Settings]** ドロップダウンリストから **[PnP Device Authorization]** を選択します。

注

デフォルトでは、デバイスは自動的に許可されます。

3. **[Device Authorization]** チェックボックスをオンにしてデバイスで許可を有効にします。
4. **[Save]** をクリックします。

SNMP、NETCONF、Syslog などの機能の状態同期を自動的に適用して、**Catalyst Center** がネットワークデバイスを効果的に管理およびモニターできるようにする、システムレベルのプロセスについて説明します。

デバイスの可制御性は、**Catalyst Center** 上のシステムレベルのプロセスであり、次のことを行います。

- 一部のデバイスレイヤ機能の状態同期を適用する
- デバイス管理に必要とされるネットワーク設定を展開するのに役立つ
- デバイスがインベントリに追加されたときや、サイトに割り当てられたときなど、ネットワークに変更が加えられたときに検出を実行する

デバイスにプッシュされる設定を表示するには、**[Provision] > [Inventory]** に移動し、**[Focus]** ドロップダウンリストから **[Provision]** を選択します。**[Provision Status]** 列の **[See Details]** をクリックします。

注

Catalyst Centerによりデバイスが設定または更新されると、トランザクションが監査ログにキャプチャされ、変更の追跡と問題のトラブルシューティングに使用できます。

デバイスの可制御性により、以下のデバイス設定が有効になります。

- **[Device Discovery]** :
 - SNMP クレデンシヤル
 - NETCONF クレデンシヤル
- インベントリへのデバイスの追加
 - Cisco TrustSec (CTS) クレデンシヤル

注

[Global] サイトが **Cisco ISE** で **AAA** として設定されている場合にのみ、**Cisco TrustSec (CTS)** クレデンシヤルがインベントリ中にプッシュされます。それ以外の場合、**Cisco ISE** でそのサイトが **AAA** として設定されていれば、**[Assign to Site]** 時に **CTS** がデバイスにプッシュされます。

- デバイスのサイトへの割り当て
 - 有線エンドポイントデータ収集の有効化
 - コントローラ証明書



Cisco IOS デバイスの場合、PKCS 証明書の有効期限の処理で問題が発生しないように、デバイスの UI コンソールからタイムゾーンを設定することを推奨します。

- SNMP トラップサーバ定義
- Syslog サーバ定義
- アプリケーションの可視性
- Application QoS Policy
- NetFlow サーバ定義
- Wireless Service Assurance (WSA)
- ワイヤレステレメトリ
- DTLS 暗号スイート
- AP 偽装
- IPDT の有効化

デバイスの可制御性はデフォルトで有効になっています。デバイスの可制御性を有効にしたくない場合は、手動で無効にします。詳細については、[デバイスの可制御性の設定](#) (62ページ) を参照してください。

デバイスの可制御性が無効になっている場合、ディスカバリ実行時やデバイスのサイトへの割り当て時に、そのデバイスのクレデンシャルや機能が **Catalyst Center** によって設定されることはありません。

状況に応じて、以下を含むネットワーク設定が、デバイスの可制御性によってデバイスに設定されるかどうかが決まります。

• デバイス検出

- **SNMP** と **NETCONF** のクレデンシャルがまだデバイスに存在しない場合は、この設定が検出プロセス中に適用されます。
- **IOS** デバイスで **NETCONF** を有効にすると、最大 6 つの **DNS** サーバーを設定できます。6 つの **DNS** サーバーすべてが使用されていて、新しいサーバーを追加する必要がある場合にのみ、既存の **DNS** サーバーが削除されます。それ以外の場合、既存の **DNS** サーバーは変更されません。

• インベントリ内のデバイス

- 初期インベントリ収集が正常に終了すると、**IPDT** がデバイスで設定されます。
- 以前のリリースでは、次の **IPDT** コマンドが設定されていました。

```
ip device tracking
ip device tracking probe delay 60
ip device tracking probe use-svi
```

- インターフェイスごとに、次の手順を実行します。

```
interface $physicalInterface
ip device tracking maximum 65535
```

- 現在のリリースでは、新しく検出されたデバイスに対して次の **IPDT** コマンドが設定されます。

```
device-tracking tracking
device-tracking policy IPDT_POLICY
tracking enable
```

- インターフェイスごとに、次の手順を実行します。

```
interface $physicalInterface
device-tracking attach-policy IPDT_POLICY
```

• デバイス プロビジョニング

- ユーザーインテントに一致する必要な **DTLS** 設定および **DNS** 設定がデバイスにない場合、**DTLS** 暗号スイートと **DNS** 設定の両方がプッシュされます。
- **Network Assurance** 証明書の設定が **[Assign to Site]** 時にすでに存在する場合、その設定はスキップされ、失敗した試行が再試行されます。
- **WSA** 設定と **PKCS12** 証明書が **[Assign to Site]** 時にすでに有効になっている場合、その設定はスキップされます。



注

以前の設定試行が失敗した場合、デバイスの可制御性ワークフローによって、プロビジョニング時に設定が再試行されます。

• グローバルサイト内のデバイス

- デバイスが正常に追加、インポート、または検出されると、**Catalyst Center** はデフォルトでそのデバイスを **Managed** 状態にし、**Global** サイトに割り当てます。
- **グローバル** サイト用の **SNMP** サーバ、**Syslog** サーバ、および **NetFlow** コレクタ設定が定義済みの場合でも、デバイス上のこれらの設定を変更 **Catalyst Center** しません。

• サイトに移動されたデバイス

- デバイスを **Global** サイトから、**SNMP** サーバー、**Syslog** サーバー、**NetFlow** コレクタ設定が定義済みの新しいサイトに移動させると、**Catalyst Center** が、デバイスのこれらの設定を新しいサイト用に定義された設定に変更します。
- ユーザーインテントに一致する必要な **DTLS** 設定および **DNS** 設定がデバイスにない場合、**DTLS** 暗号スイートと **DNS** 設定の両方がプッシュされます。
- **WSA** 設定は、適用範囲に基づいてデバイスで有効になります。
- **Network Assurance (NA)** 証明書の設定がデバイス上に作成されます。
- デバイスの可制御性によって、**sdn-network-infra-iwan** という **PKCS** トラストポイントが作成され、それを使用して証明書がインストールされます。この名前のトラストポイントが存在する場合は、最新の証明書で置き換えられます。
- ワイヤレス **AP** 参加証明書が存在しない場合は、デバイス上に設定されます。
- **[Force Configuration Push]** 時に、証明書は再プッシュされず、設定されていれば再作成されません。
- 必要な **AP** 偽装設定が存在しない場合は、デバイスにプッシュされます。

- サイトから削除されたデバイス

- デバイスをサイトから削除する場合、**Catalyst Center** はそのデバイスの **SNMP** サーバー、**Syslog** サーバー、および **NetFlow** コレクタ設定を削除しません。

- **Catalyst Center** から削除されたデバイス

- デバイスを **Catalyst Center** から削除し、**[Clean Up Configuration]** チェックボックスをオンにすると、**SNMP** サーバー、**Syslog** サーバー、**DNS** 設定、**PKCS** 設定、**NetFlow** コレクタ設定、テレメトリサブスクリプション、**AP** 偽装設定、**WSA** 設定、**Catalyst Center** によってプッシュされた **NA** 証明書の設定が、そのデバイスから削除されます。
- デバイスの削除時に、**DTLS** 暗号スイート設定とワイヤレス **AP** 参加証明書は削除されません。

- サイト間で移動されたデバイス

- たとえば、サイト **A** からサイト **B** にデバイスを移動すると、**Catalyst Center** はそのデバイスの **SNMP** サーバー、**Syslog** サーバー、**NetFlow** コレクタ設定を、サイト **B** に割り当てられている設定で置き換えます。

- サイトテレメトリの変更の更新

設定タイプ	[Force Configuration Push] が有効になっていない	[Force Configuration Push] が有効になっている
DNS の設定	必須の DNS 設定が利用可能でない場合にプッシュされます。	DNS 設定がすでに存在する場合は再プッシュされません。
WSA の設定	設定が利用可能で有効である場合は再プッシュされません。 前回の試行が失敗した場合は再試行されます。	現在のデバイス設定に関係なく、常に再プッシュされます。
DTLS 設定	必要な DTLS 設定が利用可能でない場合にプッシュされます。 すでに存在する場合は再プッシュされません。	DTLS 設定がすでに存在する場合は再プッシュされません。
ワイヤレス AP 参加証明書の設定	設定されていれば再プッシュおよび再生成されません。	設定されていれば再プッシュおよび再生成されません。
PKCS12 の設定	設定が利用可能で有効である場合は再プッシュされません。 前回の試行が失敗した場合は再試行されます。	現在のデバイス状態に関係なく、常に再プッシュされます。
NA 証明書の設定	設定が利用可能で有効である場合は再プッシュされません。 前回の試行が失敗した場合は再試行されます。	現在のデバイス状態に関係なく、常に再プッシュされます。
テレメトリ サブスクリプションの設定	すでに利用可能であれば再プッシュされません。 前回の試行が失敗した場合は再試行されます。	必要なデバイス設定と既存のデバイス設定に違いがある場合にのみ再プッシュされます。

設定タイプ	[Force Configuration Push] が有効になっていない	[Force Configuration Push] が有効になっている
AP 偽装設定	必須の設定が見つからない場合にプッシュされます。	設定がすでに存在していれば再プッシュされません。

注

デバイスの制御可能性が有効になっている場合に、**Catalyst Center** がユーザー指定の **SNMP** クレデンシャルでデバイスに接続できずにデバイス情報を収集できない場合は、**Catalyst Center** がユーザー指定の **SNMP** クレデンシャルをデバイスにプッシュします。**SNMPv3** の場合、ユーザーは **[Default]** グループの下に作成されます。

Cisco AireOS デバイスの場合、ユーザー指定の **SNMPv3** パスフレーズの長さは **12 ～ 31** 文字である必要があります。

デバイスの可制御性の設定に関する情報。

デバイスの可制御性は、**Catalyst Center** でデバイスを管理するために必要なネットワーク設定を展開します。デバイスの可制御性はデフォルトで有効です。

デバイスの可制御性を手動で無効にするには、次の手順を実行します。

注

デバイスの可制御性を無効にすると、**Catalyst Center** は、**SNMP** クレデンシャル、トラップサーバー、IP デバイストラッキング (IPDT)、**NetFlow**、**Syslog**、**NETCONF** などの重要な設定について、検出されたデバイスを自動的に設定しません。

デバイスの可制御性を無効にした後にデバイスをサイトに割り当てると、**Catalyst Center** はアウトオブバンド設定変更通知と **AP** の管理をサポートしません。これは、**Catalyst Center** がデバイスのトラップの受信者として登録されなくなるためです。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**Device Settings**] > [**Device Controllability**]。
2. [**Enable Device Controllability**] チェックボックスをオフにします。
3. **Catalyst Center** がデバイステレメトリ設定で特定された問題を自動的に修正しないようにするには、[**Enable autocorrect telemetry config**] チェックボックスをオフのままにします。

テレメトリの自動修正が有効になっている場合、**Catalyst Center** は、デバイスと **Catalyst Center** の間のセキュア通信に関連する証明書の問題を自動的に検出して解決します。（この機能は、**NetFlow**、**NBAR**、または **CBAR** テレメトリの設定の問題には対処しません）。**Catalyst Center** は各デバイスの証明書の変更を **15** 分ごとにチェックします。各デバイスへの修正は **24** 時間以内に **1** 回のみ行えます。

デフォルトでは、このチェックボックスは無効になっています。デバイスの可制御性が有効になっている場合にのみ有効にできます。

4. [Save] をクリックします。

ソフトウェアのダウンロードやデバイスのプロビジョニングに関するシスコエンドユーザー ライセンス契約 (EULA) への同意についての情報。

ソフトウェアをダウンロードする前、またはデバイスをプロビジョニングする前に、エンドユーザーライセンス契約 (EULA) に同意する必要があります。

1. メインメニューから次を選択します。[System] > [Settings] > [Device Settings] > [Device EULA Acceptance] の順に選択します。
2. Cisco.com ユーザーを設定済みの場合は、ステップ 3 に進みます。設定していない場合は、次の手順を実行します。
 - a) ブラウザでシークレット/プライベートウィンドウを開きます（以前にキャッシュされたログイン情報の使用を避けるため）。
 - b) 別の Catalyst Center GUI インスタンスを開いてログインします。
 - c) [Device EULA Acceptance] ウィンドウの別のインスタンスを開きます。メインメニューから次を選択します。[System] > [Settings] > [Device Settings] > [Device EULA Acceptance] の順に選択します。
 - d) [Cisco.com ID] フィールドで、[Add] リンクをクリックします。
 - e) [Information] ポップアップウィンドウで [I am in private or incognito mode] チェックボックスをオンにして、[Proceed] をクリックします。
 - f) [Activate your device] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[Next] をクリックします。
 - g) [Log in] ポップアップウィンドウで、cisco.com ユーザーの電子メールアドレスを入力し、[Next] をクリックします。
 - h) [Verify with your password] ポップアップウィンドウで、cisco.com ユーザーのパスワードを入力し、[Verify] をクリックします。

[Device Activated] ポップアップウィンドウが表示されます。

 - i) [Device Activated] ポップアップウィンドウを閉じます。
 - j) [Device EULA Acceptance] ウィンドウを更新します。
 - k) [Cisco.com ID] フィールドに、ユーザーに対して入力した電子メールアドレスが表示されていることを確認します。また、[Change] リンクが表示されていることを確認します。
3. 新しいブラウザタブで [Cisco End User License Agreement Supplemental Product Terms] リンクを開きます。
4. Catalyst Center EULA を開いて内容を確認します。
5. [I have read and accept the Device EULA] チェックボックスをオンにします。
6. [Save] をクリックします。

ネットワークの再同期間隔の設定に関する情報。

[System] > [Settings] > [Network Resync Interval] の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、**[Device Inventory]** を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。**[Network Resync Interval]** を使用してポーリング間隔を設定すると、その値が **[Device Inventory]** ポーリング間隔値よりも優先されます。

- **SUPER-ADMIN-ROLE** 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールについて](#)（162ページ）を参照してください。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

-
1. メインメニューから次を選択します。**[System] > [Settings] > [Device Settings] > [Network Resync Interval]** の順に選択します。
 2. **[Resync Interval]** フィールドに、新しい時間値（分）を入力します。
 3. （オプション）すべてのデバイスに対して設定された既存のポーリング間隔をオーバーライドする場合は、**[Override for all devices]** チェックボックスをオンにします。
 4. **[Save]** をクリックします。
-

SNMP

再試行とタイムアウトを含む、**SNMP** プロパティの設定に関する情報。

SNMP の再試行とタイムアウトの値を設定することができます。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールについて](#)（162ページ）を参照してください。

-
1. メインメニューから次を選択します。**[System] > [Settings] > [Device Settings] > [SNMP]** の順に選択します。
 2. 次のフィールドを設定します。
 - **[Retries]** : 許容されるデバイス接続の最大試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
 - **[Timeout]** : タイムアウトになるまでにデバイスとの接続の確立を試みる際に、**Catalyst Center** が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。
 3. **[Save]** をクリックします。
 4. （オプション）デフォルトの設定に戻すには、**[Reset]** をクリックしてから **[Save]** をクリックします。
-

ICMP ping

Internet Control Message Protocol (ICMP) ping の有効化に関する情報。Catalyst Center は、ICMP を使用して、FlexConnect モードで到達不能なアクセスポイントに ping を送信します。

Internet Control Message Protocol (ICMP) ping が有効になっていて、FlexConnect モードで到達不能なアクセスポイントがある場合、Catalyst Center は ICMP を使用して 5 分ごとにそれらのアクセスポイントに ping を実行し、到達可能性を強化します。

ICMP ping を有効にするには、次の手順を実行します。

1. メインメニューから次を選択します。[System] > [Settings] > [Device Settings] > [ICMP Ping] の順に選択します。
2. [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにします。
3. [Save] をクリックします。

PnP AP

PnP の導入準備中に、[Configure AP Location] チェックボックスを使用して、割り当てられたサイトを AP の場所に設定できます。

Catalyst Center では、PnP 導入準備の AP の場所として、PnP 要求中に割り当てられたサイトを使用できます。[Configure AP Location] チェックボックスをオンにすると、Catalyst Center は割り当てられたサイトを PnP 導入準備用の AP の場所として設定します。チェックボックスをオフにした場合は [Configure Access Points] ワークフローを使用して、PnP 導入準備用の AP の場所を設定します。詳細については、『[Catalyst Center User Guide](#)』の「AP Configuration in Catalyst Center」を参照してください。

注

これらの設定は、Day-N 運用中には適用されません。Day-N 運用の AP の場所を設定するには、[Configure Access Points] ワークフローを使用します。

1. メインメニューから次を選択します。[System] > [Settings] > [Device Settings] > [PnP AP Location] の順に選択します。
2. [Configure AP Location] チェックボックスをオンにします。
3. [Save] をクリックします。

カスタムプロンプトを使用するためのデバイスの設定に関する情報。

Catalyst Center ではユーザー名とパスワードのカスタムプロンプトを作成できます。カスタムプロンプトを使用してデバイスに関する情報を収集するように、ネットワーク内のデバイスを構成できます。

ユーザー名とパスワードに関するカスタムプロンプトの作成についての情報。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**Device Settings**] > [**Device Prompts**] の順に選択します。
[**Device Prompts**] ウィンドウが開きます。
2. [**Create Custom Prompt**] をクリックします。
[**Create Custom Prompt**] スライドインペインが開きます。
3. ユーザー名のカスタムプロンプトを作成するには、次の手順を実行します。
 - a. [**Prompt Type**] ドロップダウンリストから、[**username**] を選択します。
 - b. [**Prompt Text**] フィールドに、正規表現 (Regex) でテキストを入力します。
 - c. [**Save**] をクリックします。
4. パスワードのカスタムプロンプトを作成するには、次の手順を実行します。
 - a. [**Prompt Type**] ドロップダウンリストから、[**password**] を選択します。
 - b. [**Prompt Text**] フィールドに、正規表現 (Regex) でテキストを入力します。
 - c. [**Save**] をクリックします。

 注

[**Device Prompts**] ウィンドウにカスタムプロンプトが表示されます。ユーザー名とパスワードのカスタムプロンプトを 8 つまで作成できます。

5. カスタムプロンプトを必要な順序でドラッグアンドドロップします。

 注

Catalyst Center は、カスタムプロンプトの順序を維持し、プロンプトをコンマ区切り値としてデバイスに渡します。最上位のカスタムプロンプトの優先度が高くなります。

6. 編集アイコンをクリックして、カスタムプロンプトを編集します。
7. カスタムプロンプトを削除するには、削除アイコンをクリックします。

 注

ユーザー名のプロンプトとパスワードのプロンプトには、一意の正規表現が必要です。同じまたは類似の正規表現を作成すると、デバイスで認証の問題が発生します。

SSH

Catalyst Center が SSH キーの変更を自動的に受け入れるかどうかを設定します。

[SSH key configuration] ウィンドウでは、Catalyst Center が SSH キーの変更を自動的に受け入れるかどうかを設定できます。

重要

このオプションが有効になっている場合は、SSH キー検証に失敗したすべてのデバイスを手動で再同期する必要があります。

-
1. メインメニューから次を選択します。[System] > [Device Settings] > [SSH key trust]。
 2. 行われた SSH キーの変更の自動受け入れを有効または無効にするには、[Accept all changes] トグルボタンをクリックします。
-

デバイスの実行構成のバックアップ設定の構成に関する情報。

Catalyst Center は、デバイスの実行構成の定期的なバックアップを実行します。バックアップの日時と、デバイスごとに保存できる構成ドリフトの合計数を選択できます。

 注

- **[Daily Backup]** : Catalyst Center は、毎日午後 11:00 (UTC タイムゾーン) に実行するようにスケジュールされた自動設定バックアップを実行します。このプロセス中、Catalyst Center は、最後にデバイス構成の収集が行われた時点のタイムスタンプと、デバイス構成がアーカイブされた時点のタイムスタンプを比較します。この差が 30 分を超える場合は、デバイス構成のアーカイブが実行されます。
日次バックアップは、週次バックアップがスケジュールされている日には実行されません。
- **[Weekly Backup]** : Catalyst Center は、毎週日曜日の午後 11:30 (UTC タイムゾーン) に実行するようにスケジュールされた自動設定バックアップを実行します。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Configuration Archive]** を選択します。
2. **[Configuration Archive]** ウィンドウで、**[Internal]** タブをクリックします。
3. **[Number of config drift per device]** ドロップダウンリストをクリックし、デバイスごとに保存する構成ドリフトの数を選択します。

デバイスごとに 7 ~ 50 の構成ドリフトを保存できます。保存される構成ドリフトの合計には、デバイスのすべてのラベル付き構成が含まれます。

 注

デフォルトでは、デバイスごとに保存される構成ドリフトの数は 15 です。

4. バックアップの日時を選択します。
選択したバックアップの日時は、ネットワークに展開された Catalyst Center クラスタのタイムゾーンに基づきます。
5. **[Save]** をクリックします。
バックアップは、スケジュールした後にアクティビティセンターで表示できます。
6. **[External]** タブをクリックして、デバイス構成をアーカイブするための外部サーバーを構成します。詳細については、[アーカイブデバイス構成用の外部サーバーの構成](#) (68ページ) を参照してください。

デバイスの実行コンフィギュレーションをアーカイブするための外部サーバーを構成することについての情報。

デバイスの実行コンフィギュレーションをアーカイブするための外部 SFTP サーバーを構成できます。

外部サーバーで SSH、SFTP、SCP が有効になっていることを確認します。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Configuration Archive]** を選択します。
2. **[Configuration Archive]** ウィンドウで、**[External]** タブをクリックします。
3. **[Add]** をクリックして、**[External Repository]** を追加します。

 注

追加できる SFTP サーバーは 1 つだけです。

4. **[Add New External Repository]** スライドインペインで、次の詳細を入力します。
 - a) **[Host]** : ホストの IP アドレスを入力します。
 - b) **[Root Location]** : ルートフォルダの場所を入力します。

 注

- ルートの場所のパスが相対パスではなく絶対パスであることを確認します。
- 外部サーバーのルートの場所は空である必要があります。

- c) **[Server Protocol]** : SFTP サーバーのユーザー名、パスワード、ポート番号を入力します。
 - d) **[Backup Format]** を選択します。

- **[RAW]** : 実行コンフィギュレーションがすべて公開されます。すべての機密設定とプライベート設定は、バックアップデータでマスク解除されます。パスワードを入力して、バックアップファイルをロックします。

 注

ファイルのパスワードは **Catalyst Center** に保存されません。SFTP サーバー上のファイルにアクセスするには、パスワードを覚えておく必要があります。

- **[Sanitized (Masked)]** : 実行コンフィギュレーションの機密設定とプライベート設定の詳細がマスクされます。

パスワードは、**RAW** バックアップ形式を選択した場合にのみ適用されます。

- e) バックアップサイクルをスケジュールします。

バックアップの日付、時刻、タイムゾーン、およびバックアップの繰り返し間隔を入力します。

5. **[Save]** をクリックします。

6. SFTP サーバーの詳細を編集するには、[Action] 列の編集ボタンをクリックします。
 7. SFTP サーバーを削除するには、[Action] 列の下にある削除ボタンをクリックします。
-

第

6

章

:

- Cisco AI Network Analytics
- Cisco Spaces
- Catalyst Center Cisco ISE
-
-
- Cisco SD-Access
- IP
-
- Meraki
- Catalyst Center Microsoft Teams
-
-
- Webex
- ThousandEyes

Cisco AI Network Analytics

Cisco AI Network Analyticsの設定に関する情報。Cisco AI Network Analyticsで、ネットワークデバイスから Cisco AI Cloud にネットワークイベントデータをエクスポートできます。

この手順で、Cisco AI Analytics 機能を有効にして、ネットワークデバイスとインベントリ、サイト階層、トロポジデータからネットワークイベントのデータを Cisco AI Cloud にエクスポートします。

- Catalyst Center の Advantage ソフトウェアライセンスを保有していることを確認してください。AI ネットワーク分析 アプリケーションは、Advantage ソフトウェアライセンスに含まれています。
- AI Network Analytics アプリケーションの最新バージョンがインストールされていることを確認してください。アプリケーションのダウンロードとインストール (156ページ) を参照してください。
- ネットワークまたはHTTPプロキシが、次のクラウドホストへのアウトバウンドHTTPS (TCP 443) アクセスを許可するように設定されていることを確認します。
 - [api.use1.prd.kairos.ciscolabs.com] (米国東部地域)
 - [api.euc1.prd.kairos.ciscolabs.com] (EU 中央地域)

1. メインメニューから次を選択します。[System] > [Settings]の順に選択します。
2. [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
AI ネットワーク分析 ウィンドウが開きます。

AI Network Analytics

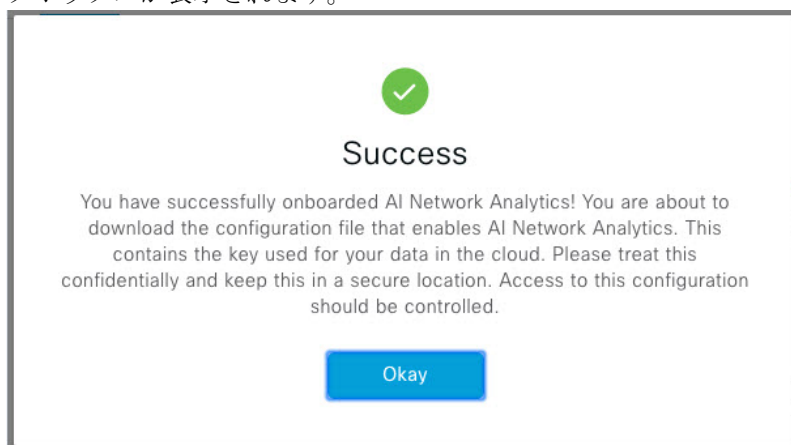
Using AI and Machine Learning, AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Configure

Recover from a config file ⓘ

3. 次のいずれか 1 つのタスクを実行します。
 - アプライアンスに以前のバージョンの Cisco AI Network Analytics がインストールされている場合は、次の手順を実行します。
 - a. [Recover from a config file] をクリックします。
[Restore] AI ネットワーク分析ウィンドウが開きます。
 - b. 表示されたエリアに構成ファイルをドラッグアンドドロップするか、ファイルシステムからファイルを選択します。
 - c. [Restore] をクリックします。
Cisco AI Network Analytics の復元には数分かかる場合があります、その後、[Success] ダイアログボックスが表示されます。
 - Cisco AI Network Analytics を初めて構成する場合は、次の手順を実行します。

- a. [Configure] をクリックします。
- b. [Where should we securely store your data?] 領域で、データを保存する場所を選択します。[Europe (Germany)] または [US East (North Virginia)] を選択できます。
[Testing cloud connectivity...] タブで示されているように、システムはクラウド接続のテストを開始します。クラウド接続のテストが完了すると、[Testing cloud connectivity...] タブが [Cloud connection verified] に変わります。
- c. [Next] をクリックします。
[Terms and Conditions] ウィンドウが表示されます。
- d. [Accept Cisco Universal Cloud Agreement] チェックボックスをオンにして契約条件に同意してから、[Enable] をクリックします。
Cisco AI Network Analytics が有効になるまでに数分かかる場合があります、その後、[Success] ダイアログボックスが表示されます。



4. [Success] ダイアログボックスで [Okay] をクリックします。
AI ネットワーク分析 ウィンドウが表示され、[Enable AI Network Analytics] トグルボタンが表示されます。
☒
5. (推奨) AI ネットワーク分析 ウィンドウで、[Download Configuration] ファイルをクリックします。

クライアント証明書は、クラウド接続が失われないように、有効期限が切れる前に更新する必要があります。

AI エージェントは、X.509 クライアント証明書を使用して AI クラウドへの認証を実行します。証明書は、AI クラウドへのテナントのオンボーディング時に AI クラウド CA によって作成および署名され、3 年間有効です（2021 年 8 月に 1 年に短縮）。有効期限が切れる前に、クラウド接続が失われないようにクライアント証明書を更新する必要があります。証明書の自動更新メカニズムが導入されています。このメカニズムでは、更新後に証明書を手動でバックアップする必要があります。新しい Catalyst Center を復元または移行する場合は、バックアップが必要です。

更新後、すべての AI 分析ウィンドウ（ピア比較、ヒートマップ、ネットワーク比較、トレンドおよびインサイト）に通知が表示され、新しい AI ネットワーク分析構成をバックアップするように指示されます。

Cisco AI Network Analytics

ネットワークイベントデータの収集を無効にするには、Cisco AI Network Analytics を無効にします。

Cisco AI Network Analytics のデータ収集を無効にするには、次の手順で AI Network Analytics の機能を無効にする必要があります。

1. メインメニューから次を選択します。[System] > [Settings]の順に選択します。
2. [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
各機能のチェックマーク (☒) は、その機能が有効になっていることを示します。チェックボックスがオフの場合 (☐)、機能は無効になっています。
3. [AI Network Analytics] 領域で、[Enable AI Network Analytics] トグルボタンをクリックしてオフにします (☐)。
4. [Update] をクリックします。
5. Cisco AI Network Analytics クラウドからネットワークデータを削除するには、Cisco Technical Response Center (TAC) に連絡してサポートリクエストをオープンします。
6. 以前の設定が間違っていて配置されている場合は、[Download configuration file] をクリックします。

Cisco Spaces

この手順を使用して、Catalyst Center と Cisco Spaces を統合します。この統合により、物理スペースの管理、ネットワーク インフラストラクチャ データの使用、運用効率の向上、およびスペースの使用状況のモニターが可能になります。

この手順を使用して、Catalyst Center と Cisco Spaces を統合します。この統合により、物理スペースの管理、ネットワーク インフラストラクチャ データの使用、運用効率の向上、およびスペースの使用状況のモニターが可能になります。

Cisco Spaces 統合を設定するには、次の手順を実行します。

1. メインメニューから [System > Settings] を選択します。
2. [Cisco Spaces/CMX Servers] をクリックします。
3. cisco.com でアカウントのログイン情報をアクティブにするには、次のタスクのいずれかを実行します。
 - ログイン情報がシステムにすでに保存されている場合は、このアクティベーションを続行できます。ログイン情報は必要に応じて変更できます。
 - ログイン情報がシステムでまだ設定されていない場合は、[Add] をクリックして cisco.com アカウントにログインし、デバイスをアクティブ化します。
 - このアクティベーションにのみログイン情報を使用する場合は、[Save Credentials] をオフのままにします。
 - 今後の使用のためにログインを保存する場合は、[Save Credentials] を選択します。
4. cisco.com のログイン情報を入力し、[Activate] をクリックします。
 - a. ログイン情報にリンクされている Cisco Spaces アカウントがすでにある場合は、それらが一覧に表示されます。続行するには、いずれかを選択してください。
 - Cisco Spaces アカウントがない場合は、新しいアカウントを作成するように求めるプロンプトが表示されます。

1. アカウント名を入力します。
2. Cisco Spaces のリージョンを選択します。
3. **[Create New Spaces account]** をクリックして、セットアップを完了します。

 注

ウェルカムメールを受信してアクティブ化されていない Cisco Spaces アカウントや、期限切れの Cisco Spaces アカウントは選択できません。

b. Cisco Spaces を **[Global]** サイト階層と統合するには、次のタスクのいずれかを実行します。

- 自動的に統合するには、**[Add Cisco Spaces integration to all sites]** を選択します。
- 特定の **[Site(s)]** を手動で選択して統合を有効にする場合は、**[Add Cisco Spaces integration to all sites]** の選択を解除します。

 注

(オプション) **[Add Cisco Spaces integration to all sites]** が選択解除されている場合は、**[Site(s)]** を選択して Cisco Spaces のアクティベーションを有効にしてから、**[Continue]** をクリックします。

選択したら、**[Continue]** をクリックします。

5. 最後の利用規約を確認し、**[Agree and Proceed]** をクリックして、Cisco Spaces のアクティベーションを開始します。
6. 新しい Cisco Spaces アカウントが作成された場合は、電子メールに移動し、Cisco Spaces からの招待を受け入れて、アカウントを完全にアクティブ化します。電子メールに記載された指示に従って利用規約に同意し、新しいアカウントに初めてログインします。

 注

詳細については、『[Cisco Spaces Configuration Guide](#)』の「Integrate Cisco Spaces with Catalyst Center」を参照してください。

Catalyst Center Cisco ISE

Catalyst Center と Cisco ISE のインテグレーションに関する情報。Cisco ISE には Catalyst Center で異なる使用例があります。Cisco ISE は、ユーザー、デバイス、およびクライアント認証用の AAA サーバーとして使用する、またはアクセス制御を適用するためのアクセス コントロール ポリシーとともに使用することができます。

ます。アクセス コントロール ポリシーを使用していない場合、または **Cisco ISE** をデバイス認証用の AAA サーバーとして使用していない場合は、**Cisco ISE** のインストールおよび設定は不要です。

Cisco ISE には、**Catalyst Center** に関して次の 3 つの使用例があります。

1. **Cisco ISE** はユーザー、デバイス、クライアント認証用の AAA（「トリプル A」と発音）サーバーとして使用できます。アクセス コントロール ポリシーを使用していない場合、または **Cisco ISE** をデバイス認証用の AAA サーバーとして使用していない場合は、**Cisco ISE** のインストールおよび設定は不要です。
2. アクセス コントロール ポリシーは **Cisco ISE** を使用してアクセス制御を適用します。アクセス コントロール ポリシーを作成および使用する前に、**Catalyst Center** と **Cisco ISE** を統合します。このプロセスでは、特定のサービスを用いて **Cisco ISE** をインストールして設定し、**Catalyst Center** で **Cisco ISE** の設定を行う必要があります。**Catalyst Center** を用いた **Cisco ISE** のインストールと設定の詳細については、[Cisco Catalyst Center Installation Guide](#)を参照してください。
3. ネットワークでのユーザー認証に **Cisco ISE** を使用している場合、**Cisco ISE** を統合するために **Assurance** を設定します。この統合により、有線クライアントの詳細（ユーザー名やオペレーティングシステムなど）を **Assurance** で確認できるようになります。詳細については、『[Cisco Catalyst Assurance User Guide](#)』の「**Catalyst Center** の **Cisco ISE** 設定について」を参照してください。

Cisco ISE が正常に登録され、**Catalyst Center** で信頼性が確立されると、**Catalyst Center** は **Cisco ISE** と情報を共有します。**Cisco ISE** を使って AAA サーバーとして構成されたサイトに割り当てられた **Catalyst Center** デバイスのインベントリデータは **Cisco ISE** に伝達されます。さらに、**Catalyst Center** でこれらのデバイスに対して次の設定を更新すると、この変更によって **Cisco ISE** も更新されます。

- デバイスのホスト名
- **[Design] > [Network Settings] > [Servers]** に表示される AAA サーバーの設定。
- デバイスのクレデンシャル
- デバイスの Loopback0 の IP アドレス
- デバイスの管理 IP アドレス
- デバイスに関連付けられているネットワーク デバイス グループ (NDG) タグ

Cisco ISE を使って AAA サーバーとしてサイトに関連付けられている **Catalyst Center** デバイスが想定どおり **Cisco ISE** に伝達されない場合、**Catalyst Center** は一定期間待機した後、自動的に再試行します。この後続の試行は、**Cisco ISE** への最初の **Catalyst Center** デバイス プッシュが、ネットワークの問題、**Cisco ISE** のダウンタイム、またはその他の自動訂正可能なエラーが原因で失敗した場合に行われます。**Catalyst Center** は、デバイスの追加または **Cisco ISE** へのデータの更新を再試行することで、**Cisco ISE** との最終的な一貫性の確立を試みます。ただし、**Cisco ISE** へのデバイスまたはデバイスデータの伝達が、**Cisco ISE** 自体による拒否が原因で入力検証エラーとして失敗した場合、再試行は行われません。

Cisco ISE について RADIUS の共有秘密を変更しても、**Cisco ISE** が **Catalyst Center** を更新する際にその変更は反映されません。**Catalyst Center** の共有秘密を **Cisco ISE** と一致するように更新するには、新しいパスワードで AAA サーバーを編集します。**Catalyst Center** は新しい証明書を **Cisco ISE** からダウンロードし、**Catalyst Center** を更新します。

Cisco ISE は既存のデバイス情報を **Catalyst Center** と共有しません。**Catalyst Center** が **Cisco ISE** 内のデバイスに関する情報を認識するには、そのデバイスに **Catalyst Center** と同じ名前を付ける必要があります。**Catalyst Center** と **Cisco ISE** は、デバイスのホスト名変数を通じて、この統合用に固有のデバイスを識別します。

 注

Catalyst Center インベントリ デバイスを Cisco ISE に伝達し、変更を更新するプロセスはすべて Catalyst Center 監査ログにキャプチャされます。Catalyst Center と Cisco ISE 間のワークフローに問題がある場合は、Catalyst Center GUI で監査ログの情報を確認します。

Catalyst Center は、プライマリ管理者 ISE ノードと統合されています。Catalyst Center から Cisco ISE にアクセスする場合は、このノードと接続します。

Catalyst Center は 15 分ごとに Cisco ISE をポーリングします。Cisco ISE サーバーがダウンした場合、Catalyst Center に Cisco ISE サーバーが赤色（到達不能）で表示されます。

Cisco ISE サーバーに到達不能な場合、Catalyst Center はポーリングを 15 秒に増やし、その後 30 秒、1 分、2 分、4 分といった具合に、最大ポーリング時間の 15 分になるまで倍増していきます。Catalyst Center は 15 分間隔でのポーリングを 3 日間継続します。Catalyst Center は接続が復活しない場合、ポーリングを停止し、Cisco ISE サーバーのステータスを [Untrusted] に更新します。この場合、Catalyst Center と Cisco ISE サーバー間の信頼関係を再確立する必要があります。

NDG: というプレフィックスが付いたネットワーク デバイス グループ (NDG) タグは、Cisco ISE に反映されます。

Cisco ISE と統合されたデバイスを削除すると、削除されたデバイスは Cisco ISE の新しい NDG グループに移動します。

次の追加要件と推奨事項を確認して、Catalyst Center と Cisco ISE の統合を確認してください。

- Catalyst Center と Cisco ISE の統合はプロキシサーバー経由ではサポートされていません。プロキシサーバーを使用して設定されている Cisco ISE がネットワークにある場合、そのプロキシサーバーを使用しないように Catalyst Center を設定します。設定するにはプロキシサーバーの IP アドレスをバイパスします。
- Catalyst Center と Cisco ISE の統合は、現在、Catalyst Center 仮想 IP アドレス (VIP) 経由ではサポートされていません。Catalyst Center にエンタープライズ CA 発行の証明書を使用している場合は、サブジェクトの別名 (SAN) 拡張内にある Catalyst Center のすべてのインターフェイスの IP アドレスが Catalyst Center 証明書に含まれていることを確認します。Catalyst Center が 3 ノードクラスタの場合、3 ノードの全インターフェイスの IP アドレスが、Catalyst Center 証明書の SAN 拡張に含まれている必要があります。
- Cisco ISE での管理者レベルのアクセス権が必要です。
- Cisco ISE の管理者ユーザーのパスワードの有効期限を無効にします。または、期限が切れる前に、パスワードを忘れずに更新します。
- Cisco ISE 証明書が変更された場合は、Catalyst Center を更新する必要があります。更新するには、AAA サーバー (Cisco ISE) を編集し、パスワードを再入力して保存します。これにより、Catalyst Center は新しい管理証明書の証明書チェーンを Cisco ISE からダウンロードし、Catalyst Center を更新します。Cisco ISE を HA モードで使用し、管理者証明書がプライマリまたはセカンダリ管理ノードで変更された場合は、Catalyst Center を更新する必要があります。
- Catalyst Center は、pxGrid 経由で接続するように、自身の証明書、および Cisco ISE の証明書を設定します。pxGrid に対する別の証明書を使用して、別の pxGrid クライアント (Firepower など) に接続することもできます。これらの接続が、Catalyst Center および Cisco ISE の pxGrid 接続と干渉することはありません。
- RADIUS のシークレットパスワードは変更できます。シークレットパスワードは、[System] > [Settings] > [External Services] > [Authentication and Policy Servers] で Cisco ISE を AAA サーバーとして設定する際に指定しています。シークレットパスワードを変更するには、[Design] > [Network Settings] > [Network] の順に選択し、[Change Shared Secret] リンクをクリックします。これにより、Cisco ISE は、

Catalyst Center によって管理されているネットワークデバイスに接続するとき、新しいシークレットパスワードを使用するようになります。

- 分散 Cisco ISE クラスタでは、各ノードは PAN（管理）、MnT（監視とトラブルシューティング）、PSN（ポリシーサービス）などの特定の機能のみを実行します。PAN ノードでは管理証明書のみを使用し、PSN ノードでは EAP 認証証明書のみを使用することができます。ただし、この構成により pxGrid の Catalyst Center と Cisco ISE の統合が妨げられます。したがって、Cisco ISE プライマリ PAN ノードで EAP 認証証明書の使用を有効にすることをお勧めします。
- アップグレード後に Catalyst Center が PSN を認識するようにするには、次の手順を実行する必要があります。
 1. PSN に関連付けられている PAN を再度追加します。『[Cisco Identity Services Engine Administrator Guide](#)』の「Configure a Primary Policy Administration Node」を参照してください。
 2. Cisco ISE を Catalyst Center と再統合します。『[Cisco Catalyst Center Installation Guide](#)』の「Integrate Cisco ISE with Catalyst Center」を参照してください。
- Catalyst Center は、CRL 配布ポイント（CDP）および Online Certificate Status Protocol（OCSP）による証明書失効チェックをサポートしています。統合中に、Catalyst Center はポート 9060 で Cisco ISE 管理証明書を受信し、その Cisco ISE 管理証明書内の CDP および OCSP URL に基づいてその有効性を検証します。CDP（CRL のリストを含む）と OCSP の両方が設定されている場合、Catalyst Center は OCSP を使用して証明書の失効ステータスを確認し、OCSP URL にアクセスできない場合は CDP にフォールバックします。CDP に複数の CRL がある場合、Catalyst Center は最初の CRL に到達できない場合は、次の CRL に接続します。ただし、JDK PKI Oracle のバグにより、すべての CRL エントリはチェックされません。
プロキシは証明書の検証ではサポートされていません。Catalyst Center はプロキシなしで CRL および OCSP サーバーに接続します。
 - 証明書の OCSP および CRL エントリはオプションです。
 - LDAP は、証明書検証用のプロトコルとしてサポートされていません。CDP または AIA 拡張に LDAP URL を含めないでください。
 - Catalyst Center から CDP および OCSP のすべての URL に到達できる必要があります。到達不能な URL が原因で、統合の失敗など、統合エクスペリエンスの低下が生じる可能性があります。
- Cisco ISE の証明書のサブジェクト名と発行者は ASN.1 PrintableString 文字に準拠する必要があります。スペースと次の文字のみを使用できます。A～Z、a～z、0～9、'()' +、-./:=?

Cisco ISE NAD

デバイスが Cisco ISE によって管理されるサイトに割り当てられる場合、または既存のデバイスが更新される場合、システムはデバイスの IP 設定と Loopback0 設定に基づいて NAD 管理アドレスを決定します。

デバイスが Cisco ISE によって管理されるサイトに割り当てられる場合、または既存のデバイスが更新される場合、システムはデバイスの IP 設定と Loopback0 設定に基づいてネットワークアクセスデバイス（NAD）管理アドレスを割り当てます。

デュアルスタック Catalyst Center 環境では、IPv4 と IPv6 の両方をサポートするように Cisco ISE サーバーを設定します。

次の表に、NAD 管理アドレスに適用される永続性ロジックを示します。

デバイス設定	Loopback0 アドレス	結果の NAD 管理アドレス
IPv6 デバイス	IPv4 Loopback0	IPv6 管理アドレス
IPv6 デバイス	IPv6 Loopback0	IPv6 Loopback0 アドレス
IPv4 デバイス	IPv6 Loopback0	IPv4 管理アドレス

デバイス設定	Loopback0 アドレス	結果の NAD 管理アドレス
IPv4 デバイス	IPv4 Loopback0	IPv4 Loopback0 アドレス
IPv6/IPv4 デバイス	なし	対応する管理アドレス
IPv6 デバイス	複数の IPv6 Loopback0	最後の IPv6 Loopback0 アドレス
IPv6 デバイス	リンクローカル IPv6 アドレスおよびグローバル IPv6 アドレスの両方	グローバル IPv6 ループバック IP アドレス

AAA サーバーおよびポリシーサーバーの構成に関する情報。Catalyst Center では、ユーザー認証とアクセス制御に AAA サーバーとポリシーサーバーを使用します。

Catalyst Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Catalyst Center および Cisco ISE が統合されていることを確認します。

他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、次のタスクを実行します。

- AAA サーバーで Catalyst Center を登録します。これには、AAA サーバーと Catalyst Center の共有秘密を定義することが含まれます。
- AAA サーバーで Catalyst Center の属性名を定義します。
- Catalyst Center マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。

Cisco ISE を設定する前に、以下の点を確認してください。

- Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『[Cisco Catalyst Center Compatibility Matrix](#)』[英語]を参照してください。Cisco ISE のインストールについては、『[Cisco Identity Services Engine インストールおよびアップグレードガイド](#)』[英語]を参照してください。
- スタンドアロン Cisco ISE 展開環境がある場合は、Catalyst Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。
- 分散型 Cisco ISE 展開がある場合：

Catalyst Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

 注

PAN 経由で ERS を使用することを推奨します。ただしバックアップの場合は、ポリシーサービスノード (PSN) で ERS を有効化できます。

分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。これを行うこともできますが、PAN 上で pxGrid サービスを有効化する必要はありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。

TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する Protected Access Credential (PSN) は、**[Work Centers] > [Trustsec] > [Trustsec Servers] > [Trustsec AAA Servers]** でも定義する必要があります。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。

- ポート 443、5222、8910、9060 で Catalyst Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Catalyst Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できません。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名 (SAN) のいずれかに Cisco ISE の IP アドレスまたは完全修飾ドメイン名 (FQDN) が含まれている必要があります。
- Catalyst Center システム証明書の SAN フィールドに、Catalyst Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

1. メインメニューから次を選択します。[System] > [Settings] > [External Services] > [Authentication and Policy Servers]。
2. [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。
3. プライマリ AAA サーバーを設定するには、次の情報を入力します。
 - [Server IP Address] : AAA サーバの IP アドレス。
 - [Shared Secret] : デバイス認証のキー。共有秘密は 4 ～ 100 文字で指定する必要があります。スペース、疑問符 (?)、小なり山カッコ (<) を含めることはできません。

 注

既存の Cisco ISE クラスタの一部である PSN をプライマリ AAA サーバーに設定しないでください。

4. Cisco ISE サーバーを設定するには、次の詳細情報を入力します。
 - [Server IP Address] : Cisco ISE サーバーの IP アドレス。
 - [Shared Secret] : デバイス認証のキー。共有秘密は 4 ～ 100 文字で指定する必要があります。スペース、疑問符 (?)、小なり山カッコ (<) を含めることはできません。

- **[Username]** : Cisco ISE に HTTPS 経由でログインするために使用するユーザー名。
- **[Password]** : Cisco ISE HTTPS ユーザー名のパスワード。

 注

ユーザー名とパスワードは、ネットワーク管理者に属する ISE 管理者アカウントである必要があります。

- **[FQDN]** : Cisco ISE サーバーの完全修飾ドメイン名 (FQDN) 。

 注

- Cisco ISE (**[Administration]** > **[Deployment]** > **[Deployment Nodes]** > **[List]**) で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
- 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名 (CN) または Subject Alternative Name (SAN) と一致する必要があります。

FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

hostname.domainname.com

たとえば、Cisco ISE サーバーの FQDN は **ise.cisco.com** である可能性があります。

- **[Virtual IP Address (es)]** : Cisco ISE ポリシーサービスノード (PSN) が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

5. **[Advanced Settings]** をクリックして、設定を構成します。

- **[Connect to pxGrid]** : pxGrid 接続を有効にするには、このチェックボックスをオンにします。

Catalyst Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Catalyst Center システムを認証するために Cisco ISE に送信)、**[Use Catalyst Center Certificate for pxGrid]** チェックボックスをオンにします。動作環境で使用するすべての証明書を同じ認証局 (CA) で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Catalyst Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Catalyst Center 証明書が、Cisco ISE で使用中の CA と同じ CA によって生成されていること (そうでない場合、pxGrid 認証は失敗します)。
- **[Certificate Extended Key Use (EKU)]** フィールドに「クライアント認証」が含まれていること。
- **[Enable Multiple Catalyst Center operation]** : 複数の Catalyst Center クラスタを単一の Cisco ISE システムに統合するには、このチェックボックスをオンにします。
- **[Protocol]** : **[RADIUS]** (デフォルト) と **[TACACS]**。両方のプロトコルを選択できます。

⚠ 重要

ここで Cisco ISE サーバーの TACACS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design] > [Network Settings] > [Servers]**で Cisco ISE サーバーを TACACS サーバーとして設定できません。

- **[Authentication Port]** : AAA サーバーへの認証メッセージのリレーに使用される UDP ポート。認証で使われるデフォルトの UDP ポートは **1812** です。
- **[Accounting Port]** : AAA サーバーへの重要なイベントのリレーに使用される UDP ポート。デフォルト値は UDP ポート **1812** です。
- **[Port]** : TACACS サーバーとの通信に使用される TCP ポート。TACACS で使用されるデフォルトの TCP ポートは **49** です。
- **[Retries]** : 接続の試行が中止される前に、Catalyst Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は **3** 回です。
- **[Timeout]** : 接続の試行が中止される前に、デバイスが AAA サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは **4** 秒です。

📄 注

必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Catalyst Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、**[Authentication and Policy Servers]** ウィンドウと **[System 360]** ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ :

- **[Authentication and Policy Servers]** ウィンドウ : 「進行中」
- **[System 360]** ウィンドウ : 「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ :

- **[Authentication and Policy Servers]** ウィンドウ : 「アクティブ」
- **[System 360]** ウィンドウ : 「プライマリ使用可能」および「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により **[FAILED]** と表示されている場合は、**[Retry]** をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

6. **[Add]** をクリックします。
7. セカンダリサーバーを追加するには、前述の手順を繰り返します。
8. デバイスの Cisco ISE 統合ステータスを表示するには、次の手順を実行します。
 - a. メインメニューから次を選択します。 **[Provision] > [Inventory]** の順に選択します。
[Inventory] ウィンドウにデバイス情報が表示されます。
 - b. **[Focus]** ドロップダウンメニューから **[Provision]** を選択します。
 - c. **[Devices]** テーブルの **[Provisioning Status]** 列に、デバイスのプロビジョニングステータスに関する情報 (**[Success]**、**[Failed]**、**[Not Provisioned]**) が表示されます。

[See Details] をクリックすると、追加情報を含むスライドインペインが開きます。

- d. 表示されるスライドインペインで、[See Details] をクリックします。
- e. [ISE Device Integration] タイルまでスクロールダウンして、デバイスの統合ステータスに関する詳細情報を表示します。

Catalyst Center の整合性検証に関する情報。

完全性検証 (IV) では、セキュリティリスクのあるデバイスデータに対する、デバイス侵害の可能性を示す予期しない変更または無効な値を監視します (該当する場合)。これは、各デバイスのソフトウェア、ハードウェア、プラットフォーム、構成時の設定を、シスコのすべてのサポート対象デバイスの設定に対する **Known Good Values (KGV)** の認証済みセットと比較することで行われます。この目的は、シスコデバイスに対する不正な変更の検出時間を大幅に短縮することで、侵害の影響を最小限に抑えることにあります。

注

IV では、**Catalyst Center** にアップロードされたソフトウェアイメージの完全性検証チェックを実行します。整合性検証チェックを実行するために、IV サービスは、**Known Good Value (KGV)** ファイルをアップロードする必要があります。

KGV

Catalyst Center への KGV ファイルのアップロードに関する情報。

セキュリティの整合性を提供するために、真正かつ有効なソフトウェアを実行しているものとしてシスコデバイスを検証する必要があります。現在、シスコデバイスには、真正なシスコソフトウェアを実行しているかどうかを判別するための参照ポイントがありません。IV では、収集されたイメージ整合性データをシスコソフトウェアの **KGV** と比較するためのシステムを使用します。

シスコは、その多くの製品の **KGV** が含まれる **KGV** データファイルを生成および発行しています。この **KGV** ファイルは標準の **JSON** 形式であり、シスコによって署名され、他のファイルとともに単一の **KGV** ファイルにバンドルされ、シスコの **Web** サイトから入手できます。KGV ファイルは、次の場所に掲載されています。

https://cscrd.cloudapps.cisco.com/cscrd/security/center/files/trust/Cisco_KnownGoodValues.tar

KGV ファイルは IV にインポートされ、ネットワークデバイスから取得した整合性の測定を検証するために使用されます。

 注

デバイス整合性の測定値は IV に提供され、IV 内で完全に使用されます。IV と **cisco.com** の間の接続は必要ありません。KGV ファイルを保護された環境にエアギャップ転送し、IV にロードできます。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#)（162ページ）を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [External Services] > [Integrity Verification] の順に選択します。
2. 現在の KGV ファイル情報を確認します。
 - [File Name] : KGV tar ファイルの名前。
 - [Imported By] : KGV ファイルをインポートした Catalyst Center ユーザー。自動的にダウンロードされる場合、値は [System] です。
 - [Imported Time] : KGV ファイルがインポートされた時刻。
 - [Imported Mode] : ローカルまたはリモートのインポートモード。
 - [Records] : 処理されたレコード。
 - [File Hash] : KGV ファイルのファイルハッシュ。
 - [Published] : KGV ファイルの発行日。
3. KGV ファイルをインポートするには、次のいずれかの手順を実行します。
 - KGV ファイルをローカルにインポートするには、[Import New from Local] をクリックします。
 - KGV ファイルを **cisco.com** からインポートするには、[Import Latest from Cisco] をクリックします。

 注

[Import Latest from Cisco] オプションでは、ファイアウォール設定は必要ありません。ただし、ファイアウォールがすでに設定されている場合は、<https://cscrdm.cloudapps.cisco.com> への接続のみを開く必要があります。

4. [Import Latest from Cisco] をクリックした場合は、**cisco.com** への接続が行われ、最新の KGV ファイルが自動的に Catalyst Center にインポートされます。

 注

セキュアな接続は、**Catalyst Center** とそのプロキシ（初回セットアップ時に設定された場合）に追加された証明書を使用して行われます。

5. **[Import New from Local]** をクリックした場合は、**[Import KGV]** ウィンドウが表示されます。
6. 次の手順のいずれかを実行してローカルにインポートします。
 - ローカル KGV ファイルを **[Import KGV]** フィールドにドラッグアンドドロップします。
 - **[Click here to select a KGV file from your computer]** をクリックして、ご使用のコンピュータ上のフォルダから KGV ファイルを選択します。
 - **[Latest KGV file]** リンクをクリックし、最新の KGV ファイルをダウンロードしてから、そのファイルを **[Import KGV]** フィールドにドラッグアンドドロップします。
7. **[Import]** をクリックします。
 KGV ファイルが **Catalyst Center** にインポートされます。
8. インポートが完了したら、GUI で現在の KGV ファイル情報を検証し、ファイルが更新されたことを確認します。

IV は、**Catalyst Center** が展開されてから 7 日後に最新の KGV ファイルを **cisco.com** からシステムに自動的にダウンロードします。自動ダウンロードは 7 日ごとに継続されます。KGV ファイルをローカルシステムに手動でダウンロードして、**Catalyst Center** にインポートすることもできます。たとえば、金曜日に新しい KGV ファイルが使用可能になり、自動ダウンロードが 7 日ごと（月曜日）に行われる場合は、手動でダウンロードできます。

表示される KGV 自動ダウンロード情報には、以下が含まれます。

- **[Frequency]** : 自動ダウンロードの頻度。
- **[Last Attempt]** : KGV スケジューラが最後にトリガーされた時間。
- **[Status]** : KGV スケジューラの最後の試行のステータス。
- **[Message]** : ステータスメッセージ。

 注

最新の KGV ファイルをインポートするときにエラーが見つかった場合は、エラーメッセージが表示されます。このエラーメッセージは複数の言語に翻訳されるようになりました。

最新の KGV ファイルをインポートしたら、**[Design] > [Image Repository]** を選択して、インポートされたイメージの整合性を表示します。

 注

すでにインポートされたイメージが **[Unable to verify]** ステータス（物理または仮想）である場合は、**KGV** ファイルをインポートした効果を **[Image Repository]** ウィンドウで確認できます。さらに、将来のイメージインポートでも、新しくアップロードした **KGV** を検証のために参照します（該当する場合）。

KGV

Catalyst Center の **IV** の **KGV** バンドルの更新に関する情報。

Catalyst Center では、すべての失効またはスタック状態の **IV** ワークフローをキャンセルまたはクリアして、新しいワークフローを開始できます。この機能は、有効になるまでに時間がかかるため、性質上非同期です。

IV KGV ファイルダウンロードワークフローでは、**cisco.com** から直接最新の **KGV** のダウンロードをトリガーするか、新しい **KGV** を手動でアップロードします。さらに、スケジューラが毎日実行され、**cisco.com** から最新の **KGV** バンドルがダウンロードまたは更新されます。

KGV ファイルのダウンロード中または別のフェーズ中に、スケジューラ **IV** ワークフローまたはユーザートリガー **IV** ワークフローがスタック状態になった場合、新しい要求を送信できません。一度に **1** つの **IV KGV** ワークフローのみが許可されます。サービスリクエストを発生させてサービスを再起動する以外に、新しいリクエストを送信するオプションはありません。この問題を解決するために、**Catalyst Center** では、新しい **API** を導入しました。この **API** により、古いまたは停滞した **IV** ワークフローをキャンセルし、そのワークフローに関連付けられているタスクエントリをクリアし、さらにロックメカニズムをリセットできます。この処理により、新しい **IV** ワークフロー要求の同時リクエストを防止します。

 注

このキャンセル機能：

- **KGV** ファイルのインポート時に **[Import Latest From Cisco]** を選択した場合にのみ適用されます。
- 他のシナリオでは機能せず、古いワークフローでのみ機能します。

Cisco SD-Access

最新の **SD-Access** 互換性マトリックス情報をインポートまたはダウンロードする方法を説明します。

Catalyst Center は、運用上の **SD-Access** ファブリックノードのハードウェアおよびソフトウェアの属性を、[Cisco SD-Access 互換性マトリックス](#) の情報と定期的に比較します。

検出された互換性の問題は集約され、各ファブリックサイトの **SD-Access** 準拠状態に表示されます。ファブリックサイトの集約された適合性状態は **[Provision > SD-Access > Fabric Sites]** ウィンドウから確認できます。

最新の **SD-Access** 互換性マトリックス情報をインポートまたはダウンロードするには、次の手順を実行します。

1. メインメニューから次を選択します。[**System > Settings > SD-Access Compatibility Matrix**]。

[**SD-Access Compatibility Matrix**] ウィンドウには、最後にインポートされた互換性マトリックスの情報が表示されます。

 注

Catalyst Center は、毎日 1 回実行するようにスケジュールされている SD-Access 互換性マトリックス情報の自動ダウンロードを実行します。

自動ダウンロードの日時は、[**SD-Access Compatibility Matrix**] ウィンドウにも表示されます。

2. SD-Access 互換性マトリックスファイルを手動でインポートするには、[**Import Latest From Cisco**] ハイパーリンクをクリックします。

 注

最新バージョンのファイルがすでに存在している場合は、[**SD-Access Compatibility Matrix**] ウィンドウの上部にバナーが表示されます。

3. エアギャップ展開では、シスコから SD-Access 互換性マトリックスファイルをインポートすることはできないため、Catalyst Center では次のアップロードプロセスを提供します。

- a. デバイスロールおよび Catalyst Center パッケージバージョンの [Cisco SD-Access 互換性マトリックス](#) から SD-Access 互換性マトリックスファイルをダウンロードします。

 注

ダウンロードした JSON ファイルに変更を加えないでください。

- b. [**Import New From Local**] ハイパーリンクをクリックし、次のいずれかを実行します。

- [**Choose a file**] をクリックしてファイルをインポートします。
- JSON ファイルをドラッグアンドドロップエリアにドラッグアンドドロップします。

 注

ファイルサイズは 10 MB を超えることはできません。

SD-Access

SD-Access イメージ互換性チェックを無効にする方法を学びます。

Catalyst Center 2.3.7.5 以降のリリースでは、SD-Access イメージ互換性チェックを無効にするオプションがあります。

注

適切なネットワーク運用を確保するため、SD-Access イメージ互換性チェックを常に有効にしてください。

SD-Access イメージ互換性チェックを無効にするには、次の手順を実行します。

1. メインメニューから次を選択します。[**System > Settings > SD-Access Compatibility Matrix**]。
2. [**SD-Access Compatibility Matrix**] ウィンドウで、[**SD-Access Image Compatibility Checks**] トグルボタンをクリックしてオフにします。

IP

外部 IP アドレスマネージャの設定に関する情報。

Catalyst Center を外部 IP アドレスマネージャ (IPAM) と通信するように設定できます。Catalyst Center を使用して、IP アドレスプールの作成、予約、または削除を行うと、Catalyst Center はその情報を外部 IPAM に伝達します。

外部 IPAM 統合の要件：

- IPAM 関数への書き込み権限を持つロールを作成し、Catalyst Center との統合に使用するユーザーアカウントに割り当てます。
- ポイントツーポイントアドレッシングの LAN 自動化による IP プール作成を有効にするには、ロールに次のものが含まれている必要があります。
 - Infoblox の場合：[**Network Views**] の書き込み権限。
 - BlueCat の場合：[**Configurations**] へのフルアクセス権限。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**External Services**] > [**IP Address Manager**] の順に選択します。
2. [**Server Name**] フィールドに、IPAM サーバーの名前を入力します。
3. [**Server URL**] フィールドに、IPAM サーバーの URL または IP アドレスを入力します。

証明書がこのサーバーに対して信頼されていないことを示す警告アイコンとメッセージが表示されます。信頼証明書を **IPAM** から直接インポートするには、次の手順を実行します。

a) 警告アイコンをクリックします。

[Certificate Warning] ダイアログボックスが表示されます。

b) 証明書の発行者、シリアル番号、および有効期限を確認します。

c) 情報が正しい場合は、チェックボックスをオンにして **Catalyst Center** による IP アドレスへのアクセスを許可し、信頼できない証明書を信頼できる証明書に追加します。

d) [Allowed] をクリックします。

4. [Username] および [Password] フィールドに、**IPAM** ログイン情報を入力します。

5. [Provider] ドロップダウンリストからプロバイダーを選択します。

- [BlueCat] をプロバイダーとして選択した場合は、自分のユーザーに、**BlueCat** アドレスマネージャの API アクセスが許可されていることを確認します。1 人または複数のユーザーの API アクセスを設定する方法に関する詳細については、**BlueCat** のドキュメンテーションを参照してください。

Catalyst Center を連邦情報処理標準 (FIPS) モードの **BlueCat** と統合するには、**BlueCat 9.3.0** を使用します。

6. [View] ドロップダウンリストから、デフォルトの **IPAM** ネットワークビューを選択します。専用ビューが 1 つ設定されている場合、[default] のみがドロップダウンリストに表示されます。ネットワークビューが **IPAM** で作成され、IP アドレスプールのコンテナとして使用されます。

7. **Catalyst Center** の IP アドレスプールを **IPAM** と同期する場合は、[Sync global pools from IP Address Pools to the selected view from IPAM server] チェックボックスをオンにします。IP プールを同期しない場合は、このチェックボックスをオフのままにします。

注

IPAM のビューが **Catalyst Center** の IP アドレスプールとすでに同期されていることがわかっている場合にのみ、同期をスキップしてください。たとえば、次のような場合です。

- **IPAM** がバックアップと復元によって新しいサーバーインスタンスにアップグレードされた場合
- 誤って削除した **IPAM** を読み込む場合

ビューが **Catalyst Center** の IP アドレスプールと同期していない場合、**IPAM** を追加や更新する際に同期をスキップすると、今後のプール操作でエラーが発生する可能性があります。

8. [Save] をクリックします。

証明書が正常に追加されたことを確認するには、[System] > [Settings] > [Trust & Privacy] > [Trusted Certificates] に移動します。

 注

信頼できる証明書では、証明書はサードパーティの信頼できる証明書として参照されます。

[System] > **[System 360]**に移動し、外部IPアドレスマネージャ設定が正常に完了したことを確認します。

機械推論ナレッジベースの更新に関する情報機械推論ナレッジベースは、機械推論エンジン（MRE）が使用するナレッジパック（ワークフロー）のリポジトリです。

機械推論ナレッジパックは、機械推論エンジン（MRE）がセキュリティの問題を特定し、根本原因の自動分析を改善するために使用する、段階的なワークフローです。これらのナレッジパックは、より多くの情報を受信しながら継続的に更新されます。機械推論ナレッジベースは、これらのナレッジパック（ワークフロー）のリポジトリです。最新のナレッジパックは、機械推論ナレッジベースが毎日自動で更新されるよう **Catalyst Center** を設定するか、手動で更新することで入手できます。

1. メインメニューから次を選択します。 **[System]** > **[Settings]**の順に選択します。
2. **[External Services]** まで下にスクロールし、**[Machine Reasoning Knowledge Base]** を選択します。
[Machine Reasoning Knowledge Base] ウィンドウには、次の情報が表示されます。
 - **[INSTALLED]** : インストールされている機械推論ナレッジベースパッケージのバージョンとインストール日が表示されます。

機械推論ナレッジベースに新しいアップデートがある場合は、**[Machine Reasoning Knowledge Base]** ウィンドウに **[AVAILABLE UPDATE]** が表示され、アップデートの **[Version]** と **[Details]** が示されます。

 - **[AUTO UPDATE]** : 機械推論ナレッジベースが **Catalyst Center** で自動的に毎日更新されます。
 - **[CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER, SECURITY ADVISORY, FIELD NOTICES AND EOX]** : 自動構成を実行できる **CX Cloud** と **Catalyst Center** を統合します。この統合により、**Catalyst Center** のセキュリティ アドバイザリ ツールから直接デバイスの脆弱性を検出する機能が更に強化されました。
3. （推奨） **[AUTO UPDATE]** チェックボックスをオンにして、機械推論ナレッジベースを自動的に更新します。
[Next Attempt] 領域に、次の更新の日付と時刻が表示されます。
 自動更新は、**Catalyst Center** がクラウドの機械推論エンジンに正常に接続されている場合にのみ実行できます。
4. 機械推論ナレッジベースを **Catalyst Center** で手動で更新するには、次のタスクのいずれかを実行します。
 - **[AVAILABLE UPDATES]** の下にある **[Update]** をクリックします。**[Success]** ポップアップウィンドウが表示され、更新のステータスが表示されます。
 - 機械推論ナレッジベースをローカルマシンに手動でダウンロードして **Catalyst Center** にインポートします。次の手順を実行します。
 - a. **[Download]** をクリックします。
[Opening mre_workflow_signed] ダイアログボックスが表示されます。

- b. ダウンロードしたファイルを開くか、ローカルマシンの目的の場所に保存して、**[OK]**をクリックします。
 - c. **[Import]**をクリックして、ダウンロードした機械推論ナレッジベースをローカルマシンから **Catalyst Center** にインポートします。
 5. **[CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY]** チェックボックスをオンにして、ネットワークバグ ID およびセキュリティアドバイザリとの **Cisco CX Cloud** の連携を有効にします。
 6. **[Security Advisories Settings]** エリアで、**[RECURRING SCAN]** トグルボタンをクリックして、毎週の定期的なスキャンを有効または無効にします。
 7. **[CISCO CX CLOUD]** トグルボタンをクリックして、**Cisco CX Cloud** を有効または無効にします。
-

Meraki

この手順を使用して **Catalyst Center** と **Meraki** ダッシュボードを統合し、ネットワーク展開を一元的にモニターします。

この手順を使用して **Catalyst Center** と **Meraki** ダッシュボードを統合し、ネットワーク展開を一元的にモニターします。

Meraki ダッシュボードでの統合の設定に関する詳細については、『[Meraki and Catalyst Center Global Overview](#)』の「**Add Catalyst Center to Dashboard**」を参照してください。

1. **Meraki** ダッシュボードから、**Catalyst Center** を新しい組織として追加します。
 - a) **[Global Overview]** ページの **Organizations** で、**[Add organizations]** をクリックし、**[Add Catalyst Center as an organization]** を選択します。
 - b) **[Add Organization]** ダイアログボックスで、次の詳細情報を入力します。
 - **[Cloud hosting region]** : クラウドホスティング地域を選択します。
 - **[Organization name for the Catalyst Center]** : 組織名を入力します。
 - **[Catalyst Center IP address or FQDN]** : **Catalyst Center** の IP アドレスまたは FQDN を入力します。
 - **[Catalyst Center Member ID]** : **Catalyst Center** メンバー ID を入力します。

ヒント

Catalyst Center メンバー ID を表示するには次の手順を実行します。

1. **Catalyst Center** のウィンドウの右上にあるヘルプアイコンをクリックし、**[About]** を選択します。
2. **[Member ID]** をクリックします。

- c) **[Add Organization]** をクリックします。

[Connect Catalyst Center] ダイアログボックスに、作成に成功したことを示すメッセージが表示され、Meraki ダッシュボードを Catalyst Center に接続する方法が示されます。

2. Catalyst Center から、Catalyst Center を Cisco Catalyst クラウドに登録します。
 - a) メインメニューから次を選択します。[System > Settings > External Services > Cisco Catalyst Cloud] の順に選択します。
 - b) [Cisco Catalyst Cloud] ページで、[Register] をクリックします。
 - c) [Activate your device] ポップアップウィンドウで、[Next] をクリックして続行します。



注

[Activation code] フィールドは事前に入力されています。

- d) [Sign in] ポップアップウィンドウで、Cisco アカウントにサインインします。
Catalyst Center が登録され、[Cisco Catalyst Cloud] ページに登録情報が表示されます。
3. [Cisco Catalyst Cloud] ページの [アプリケーション] で、[Meraki Dashboard] タイルを見つけ、[Activate] をクリックして Catalyst Center を Meraki ダッシュボードに接続します。
システムは、[Meraki Dashboard] タイルの右上隅に「Activated」と記載された緑色のチェックマークを表示し、接続が成功したことを示します。
4. Meraki ダッシュボードから、統合された Catalyst Center データを表示するには、[Global Overview] ページを更新します。

Catalyst Center Microsoft Teams

Catalyst Center と Microsoft Teams の統合について説明するトピックを紹介します。

Catalyst Center は、Microsoft Teams との統合をサポートしています。このセクションの内容

- Catalyst Center を Microsoft Teams と統合する場合に必要な情報について説明します。
- 既知の制限事項について説明します。
- これらの 2 つの製品の統合について説明します。

Microsoft Teams

このセクションでトピックを紹介します。

Catalyst Center と Microsoft Teams の統合については、次の点に注意してください。

- Cisco Catalyst クラウドポータルは、Microsoft テナントから次の情報を取得し、クラウドでローカルに保存します。
 - Microsoft Teams 通話レコードデータ
 - ユーザー プロファイル データ (ID、電子メール アドレス、名、姓、表示名、オフィス ロケーションなど)

- **Catalyst** クラウドポータルでは、削除する前に 1 時間データが保存されます。
- **Catalyst Center** のプライバシーポリシーを表示するには、[Catalyst Center プライバシーデータシート](#)を参照してください。
- クラウドデータベースの情報にアクセスできるのは、**Cisco Cloud Ops** チームのみです。
- **Catalyst** クラウドポータルは、**AWS EBS** を使用して暗号化されたファイルシステムに **Microsoft Teams** データを保存します。アクセストークンなどの機密データが暗号化されてデータベースに保存されます。
- **Catalyst** クラウドポータルでは、データを取得するために、**Microsoft** から次の API 権限が必要です。
 - User.ReadBasic.All
 - CallRecords.Read.All
 - User.Read
- オンプレミス **Catalyst Center** インスタンスは、データを取得するために **Catalyst** クラウドポータルを 5 分ごとにポーリングします。
- **Catalyst Center** が **Microsoft Teams** と統合されている場合、**Catalyst** クラウドポータルは次の FQDN を使用します。
 - dna.cisco.com
 - dnaservices.cisco.com
 - *.ciscoconnectdna.com
 - neoffers.cisco.com
 - neoffers-de.cisco.com
 - app-experience-connect.cisco.com
 - app-experience-connect-de.cisco.com
- **Catalyst** クラウドポータルサービスは静的 IP アドレスを使用しません。トラフィックを制御する必要がある場合は、代わりにドメイン名を使用します。
- 統合には **Catalyst** クラウドポータルへの接続が必要になるため、エアギャップ **Catalyst Center** 展開を **Microsoft Teams** と統合することはできません。
- **Catalyst Center** バージョン 2.3.7.5 以前の場合は、米国西部または EU 中央地域を使用して、**Catalyst** クラウドポータルでオンプレミス **Catalyst Center** インスタンスを登録します。**Catalyst Center** 2.3.7.6 以降の場合、米国西部地域を使用してのみ登録できます。
- 接続すると、**Catalyst Cloud** ポータルと **Microsoft Teams** は次の API を使用します。
 - 認証 : {org tenant id}/adminconsent および {org tenant id}/oauth2/v2.0/token
 - サブスクリプション : v1.0/subscriptions
 - コールレコードを取得しています : v1.0/communications/callRecords/{call record id}?\$expand=sessions(\$expand=segments) および v1.0/users/{user id}
- **Microsoft Teams** アカウントで多要素認証 (MFA) が使用されている場合、同意フローでアカウントの詳細を入力するときに MFA が使用されます。

- Catalyst Center 2.3.7.6 以降では、OAuth2 標準のデバイス認証フローが使用されます。以前の Catalyst Center バージョンでは、ワンタイムパスワード (OTP) 認証が使用されていました。このバージョンでは、ユーザーは Catalyst Cloud ポータルでパスワードを生成し、そのパスワードを使用して、Catalyst Center と Catalyst Cloud ポータルの統合を完了しました。
- Catalyst Cloud ポータルの権限を付与すると、Microsoft Teams は標準的な OAuth アクセスおよび更新トークンを発行します。Catalyst Cloud ポータルは、更新トークンを使用して毎時アクセストークンを更新します。ユーザーのログイン情報は Catalyst Cloud ポータルには送信されません。
- 次のロールで設定された Microsoft Teams ユーザーのみが、統合を開始できます。
 - グローバル管理者
 - 特権ロール管理者
 - アプリケーション設定が有効になっている場合に権限を付与する権限を持つカスタムロール

注

詳細については、次の[記事](#)を参照してください。

- 統合プロセス中に、次の手順を実行して、Microsoft Teams を認証するために必要な同意を提供します。
 1. **[Authenticate your application]** ページで、**[Click here to start the consent flow]** リンクをクリックします。
 2. 表示されるダイアログボックスで、Microsoft Teams のパスワードを入力し、**[Sign in]** をクリックします。
 3. **[Permissions requested]** ダイアログボックスで、最初の 2 つのチェックボックスを選択し、**[Accept]** をクリックします。
 4. 次のいずれかを実行します。
 - 前の FAQ エントリで説明した 3 つのロールのいずれかで設定している場合（管理者権限があることを意味します）、最初に **[I am an Admin]** をクリックします。次に、**[Permissions requested]** ダイアログボックスで、3 つすべてのチェックボックスをクリックします。最後に、**[Accept]** をクリックします。
 - 管理者権限がない場合は、まず **[Copy URL]** をクリックします。次に、管理者権限を持つユーザーにこの URL を送信します。最後に、そのユーザーに URL を開いてもらい、必要な同意を与えます。
- Microsoft に登録されている Catalyst クラウドポータルの OAuth アプリケーションのアプリケーション ID は、904c49f0-22c5-4a6f-a96c-613c2c319fc8 です。アプリケーションの名前は Cisco Catalyst Center Applications Experience です。
- Microsoft Teams が物理 Catalyst Center アプライアンスと統合された場合に発生する可能性のある制限事項や制限事項に違いはありません。
- 1 つの Catalyst Center インスタンスを 1 つの Microsoft Teams テナントにマッピングできます。Catalyst Center インスタンスを適切な Microsoft Teams アカウントと統合します。

- 単一の **Catalyst** クラウドポータルアカウントに複数の **Catalyst Center** インスタンスを登録できます。
Catalyst クラウドポータルは、登録された **Microsoft Teams** アカウントからデータを収集します。登録済み **Catalyst Center** の各インスタンスは、管理対象クライアントからデータを取得します。
- ネットワークに **Catalyst 9000** シリーズスイッチのみがある場合、**Microsoft Teams** のスコアとメトリックのみを使用できます。**Catalyst 9000** シリーズスイッチは、定性的なメトリック（パケット損失、遅延、ジッターなど）を提供しないため、ネットワーク アプリケーション パフォーマンス管理（APM）メトリックは使用できません。

Catalyst Center と **Microsoft Teams** の統合に関する既知の制限事項について説明します。

Catalyst Center を **Microsoft Teams** と統合した後に、次の制限事項が発生する可能性があります。

- 正常性データは、10 分未満の会議では使用できない場合があります。
- 通話が終了すると、**Microsoft Teams** から **Catalyst** クラウドポータルに通知が送信されるまでに数時間かかることがあります。
- オンプレミスバージョンの **Catalyst Center** では、通話レコードデータが 14 日間保存されます。

AppX MS-Teams

Catalyst Center との **Microsoft Teams** 統合の構成に関する情報。**Catalyst Center** に通話品質メトリック情報が表示されます。

アクティブ化すると、**Catalyst Center** のアプリケーション 360 ダッシュボードとクライアント 360 ダッシュボードに通話品質メトリック情報が表示されます。

管理者権限を付与された **Microsoft Teams** アカウントが必要です。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**External Services**] > [**Cisco Catalyst - Cloud**] の順に選択します。
2. [**Region**] ドロップダウンリストから **Catalyst Cloud US** リージョンを選択します。統合を機能させるには、同じリージョン（**Catalyst Cloud US**）で **Microsoft Teams** を有効にする必要があります。
3. 🔍 アイコンをクリックし、名前で検索して、[**AppX MS-Teams**] を見つけます。
4. [**Activate**] をクリックします。
[**Cisco Catalyst - Cloud**] ウィンドウにリダイレクトされます。
5. [**Cisco Catalyst - Cloud**] ウィンドウで、次の手順を実行します。
 - a) cisco.com ログイン情報を使用して **Cisco Catalyst - Cloud** にログインします。
cisco.com ログイン情報がない場合は、作成することができます。
 - b) [**Activate application on your product**] ウィンドウで、同意フローリンクをクリックして、次のタスクを実行します。
 - [**Sign in to your account**] ウィンドウで、**Microsoft** 管理者のユーザー名とパスワードを入力し、[**Sign In**] をクリックします。

- [承認 (Accept)] をクリックします。
- c) [Activate application on your product] ウィンドウで、**Catalyst Center** を選択し、[Next] をクリックします。
新しい **Catalyst Center** を登録するには、こちらのリンクをクリックして、次の手順を実行します。
 - [Host name/IP] フィールドに、**Catalyst Center** の IP アドレスを入力します。
 - [Product Name] フィールドに、**Catalyst Center** の名前を入力します。
 - [Type] フィールドに、**Catalyst Center** のタイプを入力します。
 - [Register] をクリックします。
- d) **Cisco Catalyst - Cloud** が **Catalyst Center** と自動的に同期します。その後、[Choose the Scope for your Cisco Catalyst Center] ウィンドウにリダイレクトされます。[Next] をクリックします。
- e) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
- f) [Activate] をクリックします。
Catalyst Center に再びリダイレクトされます。

注

製品を非アクティブ化するか、**AppX MS-Teams** アプリケーションから接続解除する場合は、[Cisco Cloud Services](#) を使用した **AppX MS-Teams 統合の構成** (96ページ) を参照してください。

Cisco Cloud Services AppX MS-Teams

Cisco Cloud Services を介してデバイスでの **MS-Teams** 統合のステータスをアクティブ化、非アクティブ化、またはチェックする方法を学びます。

次の手順を使用して、**Cisco Cloud** サービスを介したデバイスでの **MS-Teams** 統合のステータスをアクティブ化、非アクティブ化、またはチェックします。

管理者権限を付与された **Microsoft Teams** アカウントが必要です。

1. **cisco.com** ログイン情報を使用して [Cisco Cloud サービス](#) にログインします。
cisco.com ログイン情報がない場合は、[作成することができます](#)。
2. メインメニューから次を選択します。 **アプリケーションと製品**。
3. [Region] ドロップダウンリストから **Catalyst Cloud US** リージョンを選択します。統合を機能させるには、同じリージョン (**Catalyst Cloud US**) で **Microsoft Teams** を有効にする必要があります。
4.  アイコンをクリックし、名前で検索して、[AppX MS-Teams] を見つけます。
5. [AppX MS-Teams] タイルで、[Activate] をクリックします。詳細については、[AppX MS-Teams 統合の構成](#) (95ページ) を参照してください。
6. 製品がアクティブ化されたら、[Exit] をクリックします。
7. [Applications] ウィンドウにリダイレクトされます。
8. [AppX MS-Team] タイルをクリックして、[App 360] ウィンドウに詳細を表示します。

9. (オプション) [App 360] ウィンドウから製品をアクティブ化するには、次の手順を実行します。

- a) [Product Activations] テーブルで、[Add] をクリックします。
- b) アクティブ化する製品を選択し、[Next] をクリックします。

 注

一度に複数の製品を選択することはできません。

- c) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。それ以外の場合は、[Activate] をクリックします。

10. (オプション) 製品を非アクティブ化するには、次の手順を実行します。

- a) [AppX MS-Teams] タイルをクリックします。
- b) [Product Activations] テーブルで、非アクティブ化する製品の横にあるチェックボックスをオンにします。
- c) [More Action] ドロップダウンリストから、[Deactivate] を選択します。
- d) 確認ウィンドウで、[Deactivate] をクリックします。

11. (オプション) AppX MS-Teams アプリケーションから製品の接続を解除するには、次の手順を実行します。

- a) [AppX MS-Teams] タイルをクリックして、[App 360] ウィンドウに詳細を表示します。
- b) 上部のメニューバーで、[View all details] をクリックします。
[Details] スライドインペインが表示されます。
- c) [Disconnect now] をクリックします。

Catalyst Center でのクラウドアクセスキーの追加に関する情報。Catalyst Center は複数のクラウドアクセスキーをサポートしています。

Catalyst Center に Cloud Device Provisioning Application パッケージをインストールしたら、クラウドアクセスキーを登録できます。システムでは、複数のクラウドアクセスキーがサポートされています。各キーは、そのクラウドアクセスキーを使用して検出された AWS インフラストラクチャのコンストラクトまたはリソースをすべて含む個別のクラウドプロファイルとして使用されます。クラウドアクセスキーを追加すると、AWS VPC インベントリ収集が自動的にトリガーされます。そのクラウドアクセスキーの VPC インベントリ収集で検出されたリソースが AWS インフラストラクチャで構築され、CSR およびワイヤレスコントローラのクラウドプロビジョニングで表示して使用できます。

- Amazon Web Services (AWS) コンソールからアクセスキー ID と秘密鍵を取得します。
- AWS マーケットプレイスで CSR またはワイヤレスコントローラ製品に登録し、ターゲットリージョンのイメージ ID を確認します。
- AWS での HA フェールオーバー時に CSR で使用するキーペアを特定します。そのリージョンの CSR をプロビジョニングする際は、このキーペアの名前を Catalyst Center のリストから選択します。
- AWS での HA フェールオーバー時に CSR で使用する IAM ロールを特定します。CSR をプロビジョニングする際は、この IAM ロールを Catalyst Center のリストから選択します。

- Catalyst Center と AWS の間の HTTPS REST API を介した通信に使用するプロキシを設定します。[プロキシの設定](#)（22ページ）を参照してください。
- eNFV アプリの Cloud Connect 拡張機能は、Cloud Device Provisioning Application パッケージを別途展開することで有効になります。このパッケージは、デフォルトでは Catalyst Center の標準インストールに含まれていません。カタログサーバーからパッケージをダウンロードしてインストールする必要があります。詳細については、[アプリケーションのダウンロードとインストール](#)（156ページ）を参照してください。

-
1. メインメニューから次を選択します。[System] > [Settings] > [Cloud Access Keys] の順に選択します。
 2. [Add] をクリックします。
 3. [Access Key Name] を入力し、[Cloud Platform] をドロップダウンリストから選択します。AWS コンソールから取得した [Access Key ID] と [Secret Key] を入力します。
 4. [Save and Discover] をクリックします。
-

- クラウドアクセスキーを追加すると、AWS VPC インベントリ収集が自動的にトリガーされます。クラウドプラットフォームとの同期には数分かかります。インベントリ収集は、デフォルトの間隔で実行するようにスケジュールされています。
- クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。

Webex

クライアント 360 向けの Webex 統合の設定に関する情報。

Catalyst Center はクライアント 360 の Webex 会議セッション情報を提供します。

-
1. メインメニューから次を選択します。[System] > [Settings] > [External Services] > [Webex Integration] の順に選択します。
 2. [Authenticate to Webex] をクリックします。
 3. [Cisco Webex] ポップアップウィンドウで、電子メールアドレスを入力し、[Sign In] をクリックします。
 4. パスワードを入力し、[Sign In] をクリックします。
Webex 認証が正常に完了します。
 5. [Default Email Domain for Webex Meetings Sign-In] で、Webex ユーザーの電子メールアドレスを入力し、[Save] をクリックします。
Webex ドメインは組織全体に適用され、ドメインを使用するすべてのユーザーが会議を主催したり会議に参加したりできます。
 6. オプション: [Authentication Token] で、[Delete] をクリックして Webex 認証を削除します。
-

ThousandEyes

認証トークンを使用した ThousandEyes 統合の構成に関する情報。統合後、Catalyst Center はアプリケーションヘルス ダッシュボードに ThousandEyes エージェントのテストデータを提供します。

外部 ThousandEyes API エージェントと通信するように Catalyst Center を構成して、認証トークンを使用して ThousandEyes の統合を有効にできます。統合後、Catalyst Center はアプリケーションヘルス ダッシュボードに ThousandEyes エージェントのテストデータを提供します。

-
1. メインメニューから次を選択します。[System] > [Settings] > [External Services] > [ThousandEyes Integration] の順に選択します。
 2. ThousandEyes アカウントを Catalyst Center に接続するには、次の手順を実行します。
 - a. [Start set up] をクリックします。デバイス認証コードが表示されます。
 - b. [Login] をクリックし、[Cisco ThousandEyes authentication] ポップアップウィンドウにデバイス認証コードを入力して、[Verify] をクリックします。
 - c. [ThousandEyes login] ウィンドウで、ThousandEyes のログイン情報を入力し、[Login] をクリックします。
 3. ThousandEyes との接続を解除するには、[Disconnect] をクリックします。
-

第

7

章

$$:$$

- □□□□□□□□□□□□□□
- □□□□□□
- □□□□□□□□
- □□□□□□□□□□
- □□□□□□
- □□□□□□□□□□
- Geo □□□□□□□□
- □□□□□□□□□□

Catalyst Center の物理コンポーネントにおける正常性のモニタリングに関する情報。

[System Health] ページでは、Catalyst Center アプライアンスの物理コンポーネントの正常性をモニターし、発生する可能性がある問題を監視できます。この機能を有効にして実稼働環境で使用方法については、以降のトピックを参照してください。

Cisco IMC

Cisco Integrated Management Controller (IMC) 接続を確立する方法に関する情報。

[System Health] ページを有効にするには、Cisco Integrated Management Controller (Cisco IMC) との接続を確立する必要があります。この接続により、物理アプライアンスのハードウェアの正常性情報が収集されます。この手順を完了してください。

Super-ADMIN-ROLE 権限を持つユーザーまたは [システム設定] への「書き込み」権限を持つ CUSTOM-ROLE を持つユーザーは、アプライアンスの Cisco IMC 接続設定を設定できます。

1. メインメニューから次を選択します。[System] > [Settings] > [System Configuration] > [System Health] の順に選択します。

クラスタの各アプライアンスの IP アドレスが [Catalyst Center Address] 列に表示されます。

[Settings](#) / System Configuration

System Health

Cisco IMC Configuration Validation Catalog

Define your Cisco Integrated Management Controller (Cisco IMC) and provide required credentials. These settings are used to communicate with Cisco IMC and allow it to monitor the health of the Catalyst Center hardware.

Catalyst Center Address	Cisco IMC Address
172.20.86.106	NA

2. Cisco IMC へのログインに必要な情報を入力してください。

- a) アプライアンスの IP アドレスをクリックします。

[Edit Catalyst Center Server Configuration] スライドインペインが表示されます。

Edit Catalyst Center Server Configuration

Cisco IMC address must correspond with the Catalyst Center IP address it is managing. The two systems must be able to communicate over the network.

Catalyst Center Address
172.20.86.106

Cisco IMC Address*

Cisco IMC Username*

Cisco IMC Password*

- b) アプライアンスの **Cisco IMC** ポートに対して設定された IP アドレスを入力します。
- c) **Cisco IMC** ユーザー名とパスワードを入力し、**[Save]** をクリックします。
- d) 必要に応じて、クラスターの他のアプライアンスについてこの手順を繰り返します。

Cisco IMC

このタスクでは、**Cisco IMC** 接続設定を削除する方法について説明します。

特定のアプライアンスに対して以前に設定された **Cisco IMC** 接続設定を削除するには、次の手順を実行します。

Super-ADMIN-ROLE 権限を持つユーザーまたはシステム設定への「書き込み」権限を持つ **CUSTOM-ROLE** を持つユーザーは、これらの設定を削除できます。

1. メインメニューから次を選択します。 **[System] > [Settings] > [System Configuration] > [System Health]** の順に選択します。
2. 設定を削除するアプライアンスについて、 **[Actions]** 列で対応する削除アイコン (🗑️) をクリックします。
3. 確認ウィンドウで、 **[OK]** をクリックします。

システムイベント通知に関する情報。

Cisco IMC との接続が確立されると、**Catalyst Center** は **Cisco IMC** からイベント情報を収集し、その情報を未処理のシステムイベントとして保存します。ルールエンジンによって、これらの未処理イベントは処理され、システムヘルストポロジに表示されるシステムイベント通知に変換されます。使用可能な形式のい

れかでこれらの通知を受信するには、[Cisco Catalyst Center Platform User Guide](#) の「イベント通知の操作」トピックで説明されている手順を実行します。この手順を完了するときは、次のイベントを選択してサブスクライブしてください。

3 : Catalyst Center

イベント名	イベント ID	ドメイン	サブドメイン	説明
System Backup v2	SYSTEM-BACKUP-v2	システム	システムバックアップ	バックアップ操作が失敗すると通知が送信されます。
System Restore v2	SYSTEM-RESTORE-v2	システム	システムの復元	このイベントは、復元操作中に障害が発生すると生成されます。
System Software Upgrade v2	SYSTEM-SOFTWARE-UPGRADE-v2	システム	システム ソフトウェア アップグレード	ソフトウェア アップグレード操作が失敗すると通知が送信されます。
Disaster Recovery health status v2	SYSTEM-DISASTER-RECOVERY-v2	システム	ディザスタリカバリ	ディザスタリカバリシステムの状態が変わると通知が送信されます。
CMX connectivity failure v2	SYSTEM-EXTERNAL-CMX-v2	外部との統合	CMX 接続	CMX との接続がない場合に通知が送信されます。
External IPAM provider connectivity failure v2	SYSTEM-EXTERNAL-IPAM-v2	外部との統合	IPAM の統合	外部 IPAM プロバイダーとの接続がない場合に通知が送信されます。
ISE AAA trust establishment failure v2	SYSTEM-EXTERNAL-ISE-AAA-TROST-v2	外部との統合	Cisco ISE AAA 信頼確立	ISE AAA 信頼関係の確立が失敗すると、通知が送信されます。
ISE PAN ERS connectivity failure v2	SYSTEM-EXTERNAL-ISE-PAN-ERS-v2	外部との統合	Cisco ISE PAN ERS 接続	Cisco ISE プライマリおよびセカンダリ PAN ERS との接続がない場合に、通知が送信されます。

イベント名	イベント ID	ドメイン	サブドメイン	説明
ISE PxGrid health state change notification v2	SYSTEM-EXTERNAL-ISE-PXGRID-v2	外部との統合	Cisco pxGrid	Cisco ISE PxGrid 接続の正常性状態が変わると、通知が送信されます。
External ITSM provider connectivity failure v2	SYSTEM-EXTERNAL-ITSM-v2	外部との統合	ITSM の統合	外部 ITSM プロバイダーとの接続がない場合に通知が送信されます。
Certificate Status Notification v2	SYSTEM-CERTIFICATE-v2	システム	システム証明書	システム証明書、組み込み証明書、プロキシ証明書、ディザスタリカバリ証明書、またはサードパーティの信頼できる証明書が期限切れになった場合、失効した場合、または 90 日以内に期限切れになる場合に通知が送信されます。
Cisco IMC Certificate Status Notification v2	CISCO-IMC-CERTIFICATE-v2	アプライアンス	Cisco IMC 証明書	Cisco IMC 証明書の有効期限が切れた、失効した、または 90 日以内に期限切れになる場合に通知が送信されます。
Cisco IMC Connectivity status v2	CISCO-IMCv2	アプライアンス	Cisco IMC	Cisco IMC の接続ステータスが変更されるたびに通知が送信されます。
System Appliance Configuration Status Notification v2	CISCO-IMC-CONFIGURATION-v2	アプライアンス	Cisco IMC 設定	Cisco IMC ハードウェア設定がシスコの標準に準拠していない場合に通知が送信されます。

イベント名	イベント ID	ドメイン	サブドメイン	説明
System Hardware health status v2	CISCO-IMC-HARDWARE-v2	アプライ アンス	Cisco IMC ハー ドウェアの正常 性ステータス	いずれかのハー ドウェア コン ポーネントの正 常性ステータス が変わると、通 知が送信されま す。サポートさ れているハー ドウェア コン ポーネントは次 のとおりです。 • CPU • メモリ • ディスク • NIC • ファン • 電源モ ジュール • RAID コント ローラ

イベント名	イベント ID	ドメイン	サブドメイン	説明
System managed services v2	SYSTEM-MANAGED-SERVICES-v2	システム	システム マネージド サービス	プラットフォーム提供マネージドサービスのステータスが変更されると、通知が送信されます。
注 マネージドサービスの場合、プローブ間隔 (Catalyst Center が古いイベントをデータベースから削除するのにかかる時間) は 60 分 です。マネージドサービスがダウンして再びアクティブになった場合、サービスが復元されたことをシステムの正常性 GUI に反映するには、この時間がかかります。				
System Performance: Filesystem Utilization v2	SYSTEM-PERFORMANCE-v2 :	システム	システムパフォーマンス : ファイルシステム使用率	ファイルシステム (パーティション) の使用率がキャパシティに達すると通知が送信されます。
System Scale Limits v2	SYSTEM-SCALE-LIMITS-v2 :	システム	システムスケール制限	拡張機能の制限を超過すると、通知が送信されます。

イベント名	イベント ID	ドメイン	サブドメイン	説明
Application Health v2	SYSTEM-APPLICATION-HEALTH-v2	システム	アプリケーション健全性	モニタリング用に登録されたアプリケーションの正常性状態が変化したときに、通知が送信されます。
Cisco Trusted Certificate Update Notifications v2	CISCO-TRUSTED-CERTIFICATE-BUNDLE-v2	システム	シスコの信頼できる証明書	新しいシスコの信頼できる証明書バンドルが利用可能になると、通知が送信されます。
Internet URL Accessible Notifications v2	INTERNET-URL-ACCESS-v2	システム	Internet Access	Catalyst Center が 必要な URL アクセス (124 ページ) にリストされている URL のいずれかに到達できない場合に通知が送信されます。

システムヘルスイベント通知に関する情報。

次の表に、**Catalyst Center** がシステム正常性通知メッセージを生成するときに提供される主要な情報を示します。

サブドメイン	タグ	インスタンス	状態	メッセージ
ドメイン : システム				
CPU	CPU	<node-hostname>:CPU-1	OK	Catalyst Center CPU-1 is working as expected on <node-hostname>
			NotOk	Catalyst Center CPU-1 has failed on <node-hostname>
			Disabled	Catalyst Center CPU-1 is disabled on <node-hostname>
メモリ	Memory	<node-hostname>:DIMM_A1	OK	Catalyst Center RAM DIMM_A1 is working as expected on <node-hostname>
			NotOk	Catalyst Center RAM DIMM_A1 has failed on <node-hostname>

サブドメイン	タグ	インスタンス	状態	メッセージ
ディスク	Disk	<node-hostname>:Disk 1	OK	Catalyst Center Disk 2 is working as expected on <node-hostname>
			NotOk	Catalyst Center Disk 2 has failed on <node-hostname>
RAID コントローラ	RAIDController	<node-hostname>:Controller-1	OK	Catalyst Center RAID VD-2 is working as expected on <node-hostname>
			NotOk	Catalyst Center RAID VD-2 has degraded on <node-hostname>
			Disabled	Catalyst Center RAID VD-2 is offline on <node-hostname>
ネットワークインターフェイス	NIC	<node-hostname>:nic-1	OK	Catalyst Center network interfaces are working as expected
			NotOk	Catalyst Center: <x> network interfaces are missing for <node-hostname>: nic-1
PSU_FAN	PSU	<node-hostname>:psu-1	OK	Catalyst Center power supply (PSU-1) is powered on and thermal condition is normal for <node-hostname>
			NotOk	Catalyst Center power supply (PSU-2) is powered off and thermal condition is critical for <node-hostname>

サブドメイン	タグ	インスタンス	状態	メッセージ
ディザスタリカバリ	DisasterRecovery	<disaster-recovery-hostname>	OK	- Disaster recovery cluster is up - Disaster recovery failover succeeded to <site-name>
			Degraded	- Disaster recovery failover triggered from <site-name> to site-name - Disaster recovery failed while failing over to <site-name> - Disaster recovery standby cluster on <site-name> is down; cannot failover - Disaster recovery witness is down; cannot failover - Disaster recovery replication halted; recovery point objective will be impacted - Disaster recovery pause failed - Disaster recovery route advertisement failed - Disaster recovery IPSec communication failed
			NotOk	- Disaster recovery configuration failed - Disaster recovery failed to rejoin the standby system
プラットフォームサービス	ManagedServices	<hostname>:<name>	OK	Managed Service <service-name> is Running
			NOTOK	Managed Service <service-name> is Interrupted

サブドメイン	タグ	インスタンス	状態	メッセージ
スケール 制限	wired_concurrent_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of concurrent wired clients exceeded 26250 (105% of limit)
			DEGRADED	The number of concurrent wired clients exceeded 21250 (85% of limit)
			CAUTION	The number of concurrent wired clients exceeded 18750 (75% of limit)
	wireless_concurrent_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of concurrent wireless clients exceeded 18750 (75% of limit)
			DEGRADED	The number of concurrent wireless clients exceeded 21250 (85% of limit)
			CAUTION	The number of concurrent wireless clients exceeded 18750 (75% of limit)
	wired_devices	<hostname>:<name>	OK	OK
			NOTOK	The number of wired devices exceeded 1050 (105% of limit)
			DEGRADED	The number of wired devices exceeded 850 (85% of limit)
			CAUTION	The number of wired Devices exceeded 750 (75% of limit)
	wireless_devices	<hostname>:<name>	OK	OK
			NOTOK	The number of wireless devices exceeded 3800 (105% of limit)
			DEGRADED	The number of wireless devices exceeded 3400 (85% of limit)
			CAUTION	The number of wireless devices exceeded 3000 (75% of limit)
	interfaces	<hostname>:<name>	OK	OK
			NOTOK	The number of interfaces exceeded 1140000000 (95% of limit)
			DEGRADED	The number of interfaces exceeded 1020000000 (85% of limit)
			CAUTION	The number of interfaces exceeded 900000000 (75% of limit)
	ippools	<hostname>:<name>	OK	OK

サブドメイン	タグ	インスタンス	状態	メッセージ
	netflows	<hostname>:<name>	NOTOK	The number of IP pools exceeded 47500 (95% of limit)
			DEGRADED	The number of IP pools exceeded 42500 (85% of limit)
			CAUTION	The number of IP pools exceeded 37500 (75% of limit)
			OK	OK
	physical_ports	<hostname>:<name>	NOTOK	The number of Netflows exceeded 37500 (75% of limit)
			DEGRADED	The number of Netflows exceeded xxx (x% of limit)
			CAUTION	The number of Netflows exceeded yyy (y% of limit)
			OK	OK
	policy	<hostname>:<name>	NOTOK	The number of physical ports exceeded 50400 (95% of limit)
			DEGRADED	The number of physical ports exceeded 40800 (85% of limit)
			CAUTION	The number of physical ports exceeded 36000 (75% of limit)
			OK	OK
	security_group	<hostname>:<name>	NOTOK	The number of policies exceeded 23750 (95% of limit)
			DEGRADED	The number of policies exceeded 21250 (85% of limit)
			CAUTION	The number of policies exceeded 18750 (75% of limit)
			OK	OK
	sites	<hostname>:<name>	NOTOK	The number of security groups exceeded 3800 (95% of limit)
			DEGRADED	The number of security groups exceeded 3400 (85% of limit)
			CAUTION	The number of security groups exceeded 3000 (75% of limit)
			OK	OK
		<hostname>:<name>	NOTOK	The number of sites exceeded 475 (95% of limit)
			DEGRADED	The number of sites exceeded 425 (85% of limit)
			CAUTION	

サブドメイン	タグ	インスタンス	状態	メッセージ
	transient_clients	<hostname>:<name>		The number of sites exceeded 375 (75% of limit)
			OK	OK
			NOTOK	The number of transient clients exceeded 71250 (95% of limit)
			DEGRADED	The number of transient clients exceeded 63750 (85% of limit)
	MongoDB	<hostname>:<name>	CAUTION	The number of transient clients exceeded 56250 (75% of limit)
			CRITICAL	The disk usage exceeded 16.58 GB (80% of limit)
	postgres	<hostname>:<name>	CRITICAL	The disk usage exceeded 65.53 GB (80% of limit)
	ソフトウェアアップグレード	<hostname>:<name>	OK	Successfully finished downloading package <package-name> with version <package-version>
			NOTOK	Catalog package download failed for <package-name>
	バックアップ	<hostname>:<name>	OK	The backup completed successfully.
			NOTOK	Failed to backup
復元	Restore	<hostname>:<name>	OK	The restore operation completed successfully.
			NOTOK	The configuration restore operation failed.
ドメイン：接続性				
ISE	ISE_ERS	<Cisco-ISE-hostname>	Success	ISE AAA trust establishment succeeded for ISE server <ISE-server-details>
			Failed	ISE AAA trust establishment failed for ISE server <ISE-server-details>
ドメイン：統合				
IPAM	IPAM	<IPAM-hostname>	OK	IPAM connection to Catalyst Center established. IPAM <IPAM-IP-address>.
			Critical	IPAM connection to Catalyst Center offline. IPAM <IPAM-IP-address>.

サブドメイン	タグ	インスタンス	状態	メッセージ
ISE	ISE_AAA	<Cisco-ISE-hostname>	Up	ISE AAA trust establishment succeeded for ISE server. ISE <ISE-IP-address>
			Down	ISE AAA trust establishment failed for ISE server. ISE <ISE-IP-address>
CMX	CMX	<CMX-hostname>	serviceAvailable	CMX connection to Catalyst Center offline. CMX <CMX-IP-address>.
			serviceNotAvailable	CMX connection to Catalyst Center offline. CMX <CMX-IP-address>.
ITSM	ITSM	<ITSM-hostname>	Up	ITSM connection to Catalyst Center offline. ITSM <ITSM-IP-address>.
			Down	ITSM connection to Catalyst Center offline. ITSM <ITSM-IP-address>.

Catalyst Center アプライアンスのシステム正常性スケール番号に関する情報。

システム正常性は **Catalyst Center** アプライアンスをモニターします。ネットワークコンポーネントが特定のしきい値を超えるたびに通知を生成します。通知の優先順位は、しきい値の測定パーセンテージによって異なります。

システムの正常性は、次のしきい値で通知を生成します。

- しきい値の **75 %** を超えると、情報（P3）通知が生成されます。
- しきい値の **85%** を超えると、警告（P2）通知が生成されます。
- しきい値の **95%** を超えると、クリティカル（P1）通知が生成されます。

注

- 使用可能な **Catalyst Center** アプライアンスのリストについては、「[Release Notes for Cisco Catalyst Center](#)」のトピックを参照してください。
- すべてのアプライアンス（タイプに関係なく）について **1,000,000** 件の通知が監査ログに保持され、**1** 年間保存されます。
- 現在のアプライアンスの規模の数を確認するには、[Cisco Catalyst Center](#) のデータシートを参照してください。
- システム正常性は、**3** つの **44** コア アプライアンスで構成される **Catalyst Center** クラスタではサポートされていません。

[System Health] ウィンドウには、**Catalyst Center** アプライアンスと接続された外部システムのグラフィカルトポロジが表示されます。このシステムトポロジを使用して、ネットワークコンポーネントのステータ

スのモニタリング、問題の特定、証明書の有効期限の追跡、ハードウェアコンプライアンスの確認、およびディザスタリカバリ情報の表示を行います。

[System Health] ウィンドウのトポロジには、ネットワークに接続された **Catalyst Center** アプライアンスと外部システム（**Cisco Connected Mobile Experiences (Cisco CMX)** や **Cisco Identity Services Engine** など）をグラフィック形式で表示できます（**Cisco ISE**）。このページから、ネットワーク上の問題があるコンポーネントや注意が必要なコンポーネントをすばやく特定できます。

このページでアプライアンスおよび外部システムのデータを表示するには、次のトピックで説明されているタスクを完了します。

- [Cisco IMC 接続の確立](#)（102ページ）
- [システムイベント通知の登録](#)（103ページ）

このページを表示するには、メニューアイコンをクリックして次を選択します。[**System > System 360**] の順に選択し、[**System Health**] タブをクリックします。トポロジのデータは **30** 秒間隔でポーリングされます。新しいデータを受信すると、そのデータがトポロジに自動的に反映されます。

注

- **Catalyst Center** は **IPv6** をサポートしています。IPv6 が有効になっているクラスタを表示すると、トポロジには、そのクラスタのエンタープライズ仮想 IP アドレスに関する次の情報も表示されます。

- [Pre] フィールド：16 ビットのプレフィックス
- [GID] フィールド：32 ビットのグローバル ID
- [Subnet] フィールド：16 ビットのサブネット値

クラスタのエンタープライズ仮想 IP アドレスの残りは、クラスタのトポロジアイコンのラベル付けに使用されます。

- **IPv6** 対応のクラスタは、やはり **IPv6** 対応の外部システムにのみ、接続してデータを取得することができます。
- 接続されているアプライアンスまたは外部システムに、有効期限が設定されている証明書がインストールされている場合は常に、トポロジで次のことが実行されます。
 - 証明書が **90** 日以内に期限切れになるように設定されている場合、トポロジに警告が表示されます。
 - 証明書が **30** 日以内に期限切れになるように設定されている場合は、トポロジにエラーが表示されて問題への注意が喚起されます。
- システムヘルスはハードウェア コンプライアンス チェックを定期的に行い、接続されているアプライアンスまたは外部システムが最小構成要件を満たしていない場合は常に、そのことを示します。たとえば、接続されている仮想ドライブに関して**ライトスルー**キャッシュ書き込みポリシーが設定されていない場合、システムヘルスはトポロジを更新して、そのことを示します。
- 実稼働環境でディザスタリカバリが正常に機能している場合、システムヘルスは、メインサイトとリカバリサイトの両方のアプライアンスに関するハードウェア情報を提供します。以前は、メインサイトのアプライアンスに関してのみ、ハードウェア情報が提供されていました。

アプライアンスと外部システムの問題のトラブルシューティングに関する情報。

システム正常性のトポロジの画面では、注意が必要なネットワークコンポーネントがある場合、軽微な問題については ▲ アイコン、重大な問題については ✖ アイコンで示されます。コンポーネントで発生した問題をトラブルシューティングするには、そのトポロジアイコンの上にカーソルを合わせます。ポップアップウィンドウに次の情報が表示されます。

- 問題が検出された日時を示すタイムスタンプ。
- **Catalyst Center** アプライアンスにインストールされている **Cisco IMC** ファームウェアのバージョン（アプライアンスのポップアップウィンドウの場合）。
- 問題の簡単な概要。
- 問題の現在の状態またはシビラティ（重大度）。
- 問題に関連するドメイン、サブドメイン、および IP アドレスまたはロケーション。

接続された外部システムに問題がある関連サーバーが 3 つ以上ある場合や **Catalyst Center** アプライアンスに問題があるハードウェアコンポーネントが 3 つ以上ある場合、それらの外部システムまたはアプライアンスのポップアップウィンドウを開くと、**[More Details]** リンクが表示されます。リンクをクリックするとスライドインペインが開き、該当するサーバーまたはコンポーネントのリストが表示されます。それらの各項目の **[>]** をクリックしてエントリを展開することで、特定の項目の情報を確認できます。

注

サポートバンドル機能を使用して、詳細な根本原因分析（RCA）データにアクセスできます。この機能の詳細については、『[Cisco Catalyst Center User Guide](#)』の「**Generate the Root Cause Analysis File from Catalyst Center**」の章を参照してください。

外部システムの接続における問題のトラブルシューティングに関する情報。

Catalyst Center が現在外部システムと通信できない場合は、次の手順を実行してそのシステムに ping し、接続の問題をトラブルシューティングします。

この手順を完了する前に、次の操作を実行します。

- 機械推論パッケージをインストールします。[アプリケーションのダウンロードとインストール](#)（156ページ）を参照してください。
- 機会推論機能への書き込み権限を持つロールを作成します。この手順を完了するユーザーにそのロールを割り当てます。**[Create a User Role]** ウィザードでこのパラメータにアクセスするには、**[Define the Access]** ページの **[System]** 行を展開します。詳細については、[ロールベース アクセス コントロールの設定](#)（167ページ）を参照してください。

1. **[System Health]** ウィンドウの右上部分から、**[Tools] > [Network Ping]** を選択して **[Ping Device]** ウィンドウを開きます。

ウィンドウには、**Catalyst Center** が現在管理しているすべてのデバイスが一覧表示されます。

2. 到達可能性ステータスが **[Reachable]** であるデバイスのオプションボタンをクリックし、**[Troubleshoot]** リンクをクリックします。

[Reasoner Inputs] ウィンドウが開きます。

3. **[Target IP Address]** フィールドに、到達できない外部システムの IP アドレスを入力します。

4. **[Run Machine Reasoning]** をクリックします。

Catalyst Center で外部システムを ping すると、ダイアログボックスが表示されます。

5. **[View Details]** をクリックして、ping が成功したかどうかを確認します。

6. ping が失敗した場合は、**[View Relevant Activities]** リンクをクリックして **[Activity Details]** スライドインペインを開き、**[View Details]** アイコンをクリックします。

[Device Command Output] ウィンドウが開き、外部システムに到達できない原因として考えられる内容が一覧表示されます。

Catalyst Center アプライアンスハードウェアおよび接続された外部システムの両方をテストする **検証ツール** に関する情報。

検証ツールは、**Catalyst Center** アプライアンスハードウェアおよび接続された外部システムの両方をテストします。検証ツールは、ネットワークに重大な影響を与える前に対処する必要がある問題を特定します。検証プロセスでは、次のような多数のチェックが行われます。

- ciscoconnectdna.com への接続機能（システムおよびパッケージの更新をダウンロードするため）。
- 期限切れの証明書の有無。
- アプライアンスハードウェアとバックエンドサービスの現在の状態。
- スケール番号のしきい値を超えたネットワークコンポーネント。

ツールへアクセスするには、次の手順を実行します。

1. メインメニューから次を選択します。 **[System > System 360]** を選択してから、**[System Health]** タブをクリックします。

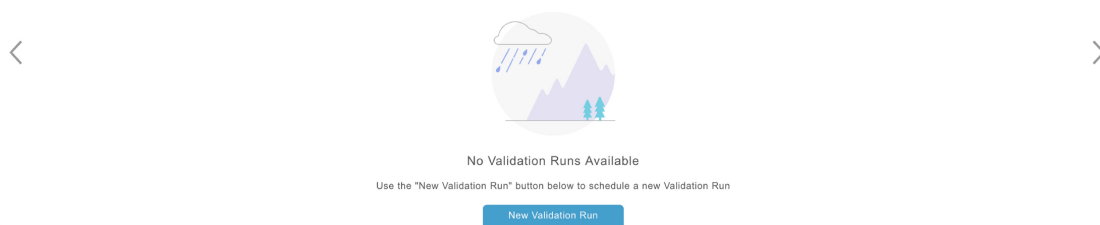
2. **[Tools]** ドロップダウンメニューから、**[Validation Tool]** を選択します。

[Validation Tool]

[Validation Tool] ウィンドウのナビゲーションに関する情報。

[Validation Tool] ウィンドウの内容は、**Catalyst Center**以前に完了した検証処理に関する情報があるかどうかによって異なります。情報がない場合、ウィンドウは次のようになります。

System Health > Validation Tool



Catalyst Center に検証処理に関する情報がある場合、ウィンドウは次のようになります。

System Health > Validation Tool

Validation Runs (7) As of: Jun 25, 2021 2:17 PM  ⑥

①

②  Add ④  Delete 0 Selected

☐	Name	Description	Selected Set(s)	Status	Start Time	Duration	Actions
☐	vr7		upgrade	Success	Jun 25, 2021 1:57 PM	104 ms	View Status ⑤
☐	vr6		upgrade	Success	Jun 25, 2021 1:30 PM	104 ms	View Status
☐	vr5		upgrade	Failed	Jun 25, 2021 12:42 PM	115 ms	View Status
③ ☐	vr4		upgrade	Success	Jun 25, 2021 5:00 AM	135 ms	View Status
☐	vr3		upgrade	Failed	Jun 25, 2021 3:51 AM	274 ms	View Status
☐	vr2		upgrade	Failed	Jun 25, 2021 3:43 AM	1 second(s)	View Status
☐	vr1		upgrade	Partial Success	Jun 25, 2021 2:57 AM	5 second(s)	View Status

1 - 7 

次の表に、**[Validation Tool]** ページを構成するコンポーネントと、検証処理に関する情報が利用可能な場合の機能を示します。

引き出し線

説明

- ① **[Search Table]** フィールド：このページにリストされている検証処理をフィルタリングするための検索文字列を入力します。
- ② **[Add]** ボタン：クリックして **[New Validation Run]** スライドインペインを開き、新しい処理のために必要な設定を入力します。詳細については、[検証処理の開始](#)（119ページ）を参照してください。
- ③ **[Validation Runs]** テーブル：以前に完了した検証処理がリストされます。このテーブルには、処理ごとの名前、適用可能な検証セット、完了ステータスなどの情報が表示されます。

注

- デフォルトでは、処理は開始時刻順に並べられ、最新の処理が最初にリストされます。
- 現在進行中のすべての処理に対しては、期間はゼロと表示されます。

- ④ **[Delete]** ボタン：検証処理のチェックボックスをオンにした状態でこのボタンをクリックすると、処理が削除されます。次に **[Warning]** ダイアログボックスで **[OK]** をクリックして、削除を確定します。

注

進行中の処理は削除できません。

- ⑤ **[View Status]** リンク：特定の処理の詳細を表示します。詳細については、[検証処理の詳細の表示](#)（119ページ）を参照してください。

引き出し線	説明
6	[Refresh] ボタン：クリックすると、このページに表示されている情報が更新されます。

検証の実行を開始する方法について説明します。

検証処理を開始するには、以下の手順を実行します。

注

一度に実行できる検証は 1 つだけです。検証実行がすでに進行中の場合は、完了してから別の処理を開始します。

1. **[Validation Runs]** テーブルが表示されるかどうかに応じて、**[Validation Tool]** ウィンドウで次のいずれかを実行します。

- テーブルが表示されない場合は、以前の検証処理が削除されているか、検証処理がまだ完了していないことを意味します。**[New Validation Run]** をクリックします。
- **[Validation Runs]** テーブルが表示されたら、**[Add]** をクリックします。

[New Validation Run] スライドインペインが開きます。

2. **[Name]** フィールドに、検証処理の名前を入力します。

英数字のみを含む一意の名前を入力します。特殊文字は使用しないでください。

3. オプション: **[Description]** フィールドに、これから開始する検証処理に関する簡単な説明を入力します。説明は最大 250 文字まで入力できます。

4. **[Validation Set(s) Selection]** エリアで、実行する検証セットのチェックボックスをオンにします。検証セットを最大化して、実行するチェックを表示できます。

5. **[Run]** をクリックします。

検証処理の詳細の表示に関する情報。

[Validation Run Details] スライドインペイン から、選択した処理中に行われたチェック、完了ステータス、期間、およびその他の関連情報を表示できます。

The screenshot shows the 'Validation Tool' interface. On the left, a table lists validation runs with columns 'Name' and 'Description'. The run 'TEST_5185' is selected. On the right, the 'Validation Run Details' panel shows the run's name, description, and status ('Partial Success'). Below this, a 'Result' section shows a table of validation results for the 'UPGRADE VALIDATION SET'.

Validation	Status	Duration	Message
Validating maglev parent catalog server settings [VERSION 1.0.90]	Success	12 ms	ParentCatalogServer https://www.wrong.com:443 configured
Validating maglev parent catalog server repository settings [VERSION 1.0.90]	Warning	9 ms	ParentCatalogServerRepository NOT configured

ここから、次のタスクを実行することもできます。

- 表示する情報をフィルタリングするには、[Search Table] フィールドに検索文字列を入力します。
- このペインの内容を PDF ファイルとしてダウンロードするには、[Export] をクリックします。
- このペインの内容をコピーするには、[Copy] をクリックします。

検証セットの更新方法に関する情報。

検証セットは、**Catalyst Center** をアップグレードするたびに更新する必要があります。検証セットを手動で更新する必要がある場合は、次の手順を実行します。

1. メインメニューから次を選択します。[System] > [Settings] > [System Configuration] > [System Health] の順に選択します。

[Settings](#) / System Configuration

System Health

Cisco IMC Configuration **Validation Catalog**

Update Catalyst Center with most recent Validation Catalog

[Download Latest](#) | [Import](#)

Validation Set Versions

Appliance Infrastructure Status	3.2.0
Appliance Scale	3.2.0
Assurance Health	3.2.0
Cisco ISE Health and Cisco DNA	2.2.0
Center Role	
Upgrade Readiness Status	9.2.0

2. [Validation Catalog] タブをクリックします。
3. [Download Latest] をクリックして、使用可能な最新の検証セットのローカルコピーをダウンロードします。
4. 検証セットを **Catalyst Center** にインポートします。
 - a) [Import] をクリックし、[Import Validation Set] ダイアログボックスを開きます。

Import Validation Set



Choose a file or drag and drop to upload.

Accepted files: .tar.gz
Accepted sizes: up to 10MB

Cancel
Import

b) 次のいずれか 1 つのタスクを実行します。

- **[Choose a file]** リンクをクリックして、インポートする **.tar** ファイルに移動します。
- 適切な **.tar** ファイルをデスクトップから強調表示された領域にドラッグアンドドロップします。

c) **[Import]** をクリックします。

[System Health] ページのシステムトポロジ通知に関する情報。

次の表に、**[System Health]** ページのシステムトポロジに表示される **Catalyst Center** アプライアンスおよび接続された外部システムについてのさまざまな通知を示します。通知は対応するシビラティ（重大度）に応じてグループ化されています。

- 重大度 1（エラー）：無効化された **RAID** コントローラや故障した電源などの重大なエラーを示します。
- 重大度 2（警告）： **Cisco ISE** サーバーとの信頼を確立できないなどの問題を示します。
- 重大度 3（成功）：サーバーやハードウェアコンポーネントが想定どおりに動作していることを示します。

 注

アプライアンスのすべてのハードウェアコンポーネントが問題なく動作している場合は、各コンポーネントの個別の通知は表示されません。代わりに、[OK] 通知が表示されます。

4 : Catalyst Center

コンポーネント	重大度 1 の通知	重大度 2 の通知	重大度 3 の通知
CPU	Processor CPU1 (SerialNumber - xxxxxx) State is Disabled	Processor CPU1 (SerialNumber - xxxxxx) Health is NotOk and State is Enabled	Processor CPU1 (SerialNumber - xxxxxx) Health is Ok and State is Enabled
ディスク	Driver - PD1 State is Disabled	Driver - PD1 Health is Critical and State is Enabled	Driver - PD1 Health is Ok and State is Enabled
MemoryV1	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is NotOk	–	Memory Summary (TOTALSYSTEMMEMORYGIB - 256) Health is Ok
MemoryV2	Storage DIMM1 (SerialNumber - xxxxx) Status is NotOperable	–	Storage DIMM1 (SerialNumber - xxxxx) Status is Operable
NIC	NIC Adapter Card MLOM State is Disabled	NIC Adapter Card MLOM State is Enabled and port0 is Down	NIC Adapter Card MLOM State is Enabled and port0 is Up
電源モジュール	PowerSupply PSU1 (SerialNumber - xxxx) State is Disabled	–	PowerSupply PSU1 (SerialNumber - xxxx) State is Enabled
RAID	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) State is Disabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) Health is NotOK and State is Enabled	Cisco 12G SAS Modular Raid Controller (SerialNumber - xxxxx) Health is OK and State is Enabled

5 :

コンポーネント	重大度 1 の通知	重大度 2 の通知	重大度 3 の通知
Cisco Connected Mobile Experiences (CMX) サーバー	–	There is a critical issue with the integrated CMX server.	CMX server is integrated and servicing.

コンポーネント	重大度 1 の通知	重大度 2 の通知	重大度 3 の通知
IP アドレス管理 (IPAM) サーバー	There is a critical issue with the connected third-party IPAM provider	–	• A third-party IPAM provider is connected. • There is no third-party IPAM provider connected. • The third-party IPAM provider is currently synchronizing.
Cisco ISE-外部 RESTful サービス (ERS)	–	ISE PAN ERS connection: ISE ERS API call unauthorized	ISE PAN ERS connection: ERS reachability with ISE - Success
Cisco ISE-信頼性	–	ISE AAA Trust Establishment: Trust Establishment Error	ISE AAA Trust Establishment: Successfully established trust and discovered PSNs from PAN
IT サービス管理 (ITSM) サーバー	ServiceNow connection health status is not up and running	–	ServiceNow connection health status is up and running

システムヘルスのディスク使用率の通知に関する情報。

システムヘルスは、システム内のすべてのノードのディスク使用率をモニターします。任意のノードのディスク使用率がネットワーク運用に影響を与える可能性のあるレベルに達すると、システムヘルスから自動的に通知が送信されます。

ディスク使用率が **75%** を超えると、警告通知が送信されます。

ディスク使用率が **85%** を超えると、重大な通知が送信されます。

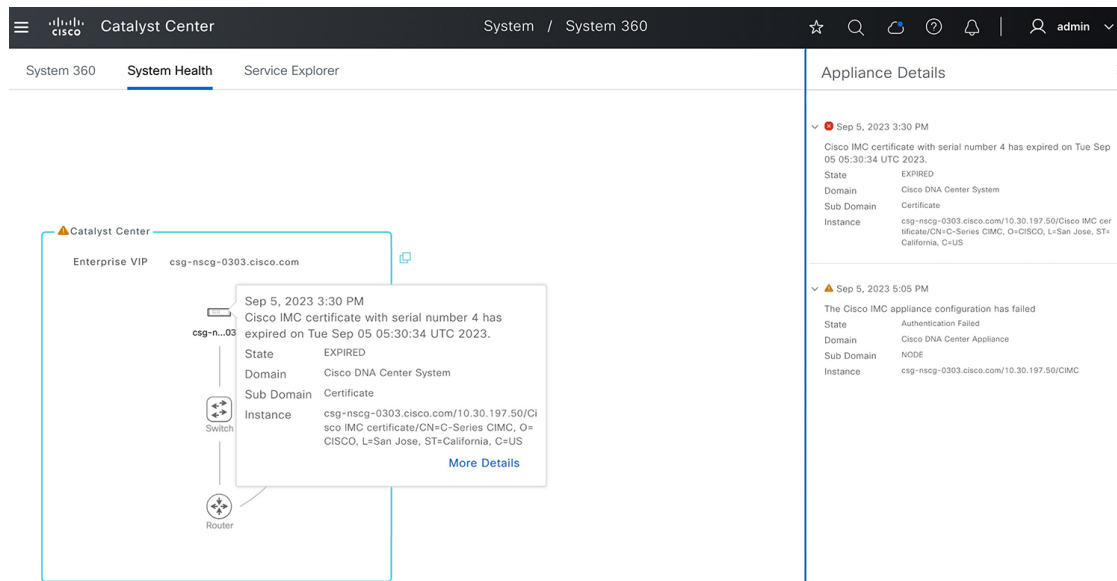
これらの通知を設定およびサブスクライブするには、『[Catalyst CenterPlatform User Guide](#)』の「Work with Event Notifications」トピックに説明されている手順を実行してください。この手順を完了するときは、**[System Performance: Filesystem Utilization]** イベントを選択してサブスクライブしてください。

注

- バックアップファイルを復元または **Catalyst Center** をアップグレードすると、システムヘルスによってディスク使用率の監視が再開され、1 時間ごとに更新が収集されます。
- 3 ノードの HA デプロイメントでは、3 つのクラスターノードで構成されているすべてのパーティションが監視されます。生成される通知は、関連するパーティションに固有です。
- ディザスタリカバリが有効になっている展開では、システムヘルスはアクティブサイトとスタンバイサイトの両方でノードごとにディスク使用率を監視します。

システムの正常性トポロジウィンドウに証明書イベント通知が表示される方法について説明します。

Catalyst Center では、失効した証明書、期限切れの証明書、または近い将来に期限切れになる証明書を毎日チェックします。これらのイベントのいずれかが発生するたびに通知を受信する場合は、**SYSTEM-CERTIFICATE-v2** および **CISCO-IMC-CERTIFICATE-v2** イベントに登録します（[システムイベント通知の登録](#)（103ページ）を参照）。選択した形式で受信する通知に加えて、Catalyst Center は証明書イベントを示すように **[System Health]** ウィンドウのトポロジも更新します。これらの通知を表示するには、アプライアンスの上にカーソルを合わせます。使用可能な場合は、**[More Details]** リンクをクリックして、**[Appliance Details]** スライドインペインで通知を表示することもできます。



Catalyst Center では、Cisco PKI Web サイトからのシスコの信頼できる証明書バンドル（**ios.p7b**）のストレージおよび更新をサポートしています。このバンドルは Catalyst Center とともに事前インストールされており、サポートされているシスコのネットワークデバイスが、有効なサードパーティベンダーデバイス証明書が提示された際に、コントローラとそのアプリケーション（ネットワークプラグアンドプレイなど）を認証できるようになります。Catalyst Center は、証明書バンドルのサードパーティ証明書のステータスを個別に確認します。シスコ署名付き証明書の場合、新しいバージョンのバンドルがダウンロード可能かどうかはシステムによってチェックされます。サードパーティの証明書または信頼できる証明書バンドルの更新が必要な場合に通知を受信するには、**CISCO-TRUSTED-CERTIFICATE-BUNDLE-v2** イベントに登録します。

URL

到達可能性を確保するために Catalyst Center がチェックを行う URL を示します。

Catalyst Center は、次の URL に到達可能かどうかを確認します。

- <http://validation.identrust.com/crl/hydrantidcao1.crl>
- <http://commercial.ocsp.identrust.com>
- <https://www.ciscoconnectdna.com>
- <https://cdn.ciscoconnectdna.com>
- <https://registry.ciscoconnectdna.com>
- <https://registry-cdn.ciscoconnectdna.com>

これらの URL のいずれかに到達できない場合（特にリストされている最初の 2 つは、システム証明書の失効ステータスを確認するために使用されるため）、ネットワーク運用に影響を与える可能性があります。この発生時に通知を受信するには、**INTERNET-URL-ACCESS-v2** イベントに登録します。

システムの正常性をモニタリングする際に発生する可能性のある問題と推奨されるアクションに関する情報。

次の表に、システムの正常性のモニタリング時によく発生する一般的な問題と、それらの問題を修復するための推奨される処置を示します。

コンポーネント	サブコンポーネント	問題	推奨されるアクション
Cisco ISE	外部 RESTful サービス (ERS) -到達可能性	タイムアウトが発生する (Cisco ISE ERS API の負荷がしきい値を超えたことが原因と考えられる)。	• Catalyst Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Catalyst Center から Cisco ISE に到達できるかどうかを確認します。
		Cisco ISE との接続を確立できない。	• ファイアウォールが設定されているかどうかを確認します。 • Catalyst Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Catalyst Center から Cisco ISE に到達できるかどうかを確認します。
	ERS-可用性	ERS API コールへの応答がない。	• インストールされている Cisco ISE のバージョンを確認します。 • Cisco ISE で ERS が有効になっているかどうかを確認します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable External RESTful Services APIs」を参照してください。
	ERS-認証	Cisco ISE ERS API コールが許可されない。	AAA 設定のログイン情報と Cisco ISE のログイン情報が同じであるかどうかを確認します。
	ERS-設定	Cisco ISE の証明書が変更されている。	Catalyst Center GUI で信頼を再確立します。詳細については、『 Cisco Identity Services Engine Administration Guide 』の「Enable PKI in Cisco ISE」を参照してください。
ERS-未分類または一般的なエラー		未定義の診断エラーが発生する。	1. Catalyst Center で現在設定されている AAA 設定を削除します。 2. 適切な AAA 設定を再入力します。詳細については、『Cisco Catalyst Center Second Generation Appliance Installation Guide』の「Integrate Cisco ISE with Catalyst Center」を参照してください。 3. 信頼を再確立します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable PKI in Cisco ISE」を参照してください。

コンポーネント	サブコンポーネント	問題	推奨されるアクション
	信頼-到達可能性	HTTPS 接続を確立できない。	AAA 設定のログイン情報と Cisco ISE のログイン情報が同じであるかどうかを確認します。
		Cisco ISE 証明書チェーンのアップロード用に設定された Catalyst Center エンドポイント URL に到達できない。	• Catalyst Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Catalyst Center から Cisco ISE に到達できるかどうかを確認します。
	信頼-設定	Cisco ISE 証明書チェーンが無効である。	• 必要に応じて、Cisco ISE 内部ルート CA チェーンを再生成します。詳細については、『Cisco Identity Services Engine Administration Guide』の「ISE CA Chain Regeneration」を参照してください。 • 内部 CA 証明書チェーンが Cisco ISE から削除されていないことを確認します。
		Cisco ISE 証明書チェーンのアップロード用に設定された Catalyst Center エンドポイント URL が禁止されている。	• URL を起動し、エンドポイントの /aaa/Cisco ISE/certificate ディレクトリにアクセスできるかどうかを確認します。 • Cisco ISE で [Use CSRF Check for Enhanced Security] オプションが有効になっているかどうかを確認します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable External RESTful Services APIs」を参照してください。
	信頼-認証	Cisco ISE パスワードの期限が切れている。	• Cisco ISE 管理者パスワードを再生成します。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Administrative Access to Cisco ISE」を参照してください。 • Cisco ISE GUI にログインできることを確認します。
	信頼-未分類または一般的なエラー	未定義の診断エラーが発生する。	

コンポーネント	サブコンポーネント	問題	推奨されるアクション
			1. Catalyst Center で現在設定されている AAA 設定を削除します。 2. 適切な AAA 設定を再入力します。詳細については、『Cisco Catalyst Center Second Generation Appliance Installation Guide』の「Integrate Cisco ISE with Catalyst Center」を参照してください。 3. 信頼を再確立します。詳細については、『Cisco Identity Services Engine Administration Guide』の「Enable PKI in Cisco ISE」を参照してください。
Cisco Connected Mobile Experiences (CMX) サーバー	到達可能性 認証	サーバーとの接続を確立できない。 サーバーにログインできない。	該当するサーバーがダウンしていないかどうかを確認します。 Catalyst Center で正しいログイン情報が設定されていることを確認します。
IP アドレス管理 (IPAM) サーバー			
IT サービス管理 (ITSM) サーバー			

コンポーネント	サブコンポーネント	問題	推奨されるアクション
ハードウェア	ディスク	指定したハードウェアコンポーネントに問題がある。	問題のあるコンポーネントを交換します。
	ファン		
	電源モジュール		
	メモリ モジュール		
	CPU		
	ネットワークカード		
	RAID コントローラ		
	ネットワーキング	インターフェイスがない。	1. Cisco IMC に接続します。 2. PID が UCSC-C220-M4 または UCSC-C220-M4S の場合は、次の手順を実行します。 a. メインメニューから、[Compute] > [BIOS] > [Configure BIOS] を選択します。 b. [Advanced] タブをクリックします。 c. [LOM and PCIe Slots Configuration] を展開します。 d. 無効な mLOM を有効にして、ホストを再起動します。 3. その他すべての PID について、問題のあるコンポーネントを交換します。
システム構成	ハードウェア構成	Catalyst Center <IP_address> 仮想ドライブの書き込みキャッシュポリシーとしてライトバックを指定することはできません。書き込みポリシーはライトスルーである必要があります。	1. Cisco IMC に接続します。 2. メインメニューから、[Storage] > [Raid Controller] を選択します。 3. [Virtual Drive] タブをクリックします。 4. 仮想ドライブを選択し、[Edit] を右クリックします。書き込みポリシーがライトスルーでない場合は、仮想ドライブを更新します。書き込みポリシーはライトスルーである必要があります。

コンポーネント	サブコンポーネント	問題	推奨されるアクション
システム リソース	ストレージ	指定したマウントディレクトリに空きがない。	- 現在のディレクトリから不要なデータを削除して記憶域を解放します。 - 記憶域が多い新しいマウントディレクトリを指定します。

監査ログの表示に関する情報。監査ログは、**Catalyst Center**で実行中のアプリケーション、デバイスの **Public Key Infrastructure (PKI)** 通知、およびシステムイベントに関する情報を収集します。

監査ログは、**Catalyst Center**で実行されているさまざまなアプリケーションに関する情報を取得します。さらに、監査ログは、デバイス **Public Key Infrastructure (PKI)** 通知についての情報も取得します。これらの監査ログの情報は、アプリケーションまたはデバイス **CA** 証明書に関連する問題（ある場合）のトラブルシューティングを支援するために使用できます。

監査ログは、発生したシステムイベント、発生した場所、開始したユーザーを記録するシステムでもあります。監査ログを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。

1. メインメニューから次を選択します。[Activities] > [Audit Logs] の順に選択します。

[Audit Logs] ウィンドウが開きます。このウィンドウで、ネットワーク内の現在のポリシーに関するログを表示できます。これらのポリシーは、**Catalyst Center** にインストールされているアプリケーションによってネットワークデバイスに適用されます。

2. タイムラインスライダをクリックして、ウィンドウに表示するデータの時間範囲を次のとおり指定します。
 - a. [Time Range] 領域で、[Last 2 Weeks]、[Last 7 Days]、[Last 24 Hours]、または [Last 3 Hours] の時間範囲を選択します。
 - b. カスタム範囲を指定するには、[By date] をクリックし、開始日時と終了日時を指定します。
 - c. [Apply] をクリックします。

3. 対応する子監査ログを表示するには、監査ログの横にある矢印をクリックします。

各監査ログは、いくつかの子監査ログの親になることができます。矢印をクリックすると、一連の追加の子監査ログを表示できます。

 注

監査ログは、**Catalyst Center** によって実行されたタスクに関するデータをキャプチャします。子監査ログは、**Catalyst Center** によって実行されたタスクのサブタスクです。

4. (任意) 左側のペインに表示された監査ログのリストで特定の監査ログメッセージをクリックします。右側のペインで **[Event ID] > [Copy Event ID to Clipboard]** をクリックします。コピーされた ID を API で使用すると、イベント ID に基づく監査ログメッセージを取得できます。

監査ログの右側のペインに各ポリシーの **[Description]**、**[User]**、**[Interface]**、**[Destination]** が表示されます。

 注

監査ログには、ペイロード情報を含む POST、DELETE、PUT などのノースバウンド操作の詳細と、デバイスにプッシュされた設定などのサウスバウンド操作の詳細が表示されます。**Cisco DevNet** の API の詳細については、『[Catalyst Center Platform Intent APIs](#)』を参照してください。

5. (任意) **[Filter]** をクリックして、**[UserID]**、**[Log ID]**、または **[Description]** でログをフィルタリングします。
6. 鉛筆アイコンをクリックして監査ログイベントを登録します。
syslog サーバーのリストが表示されます。
7. 接続する syslog サーバーのチェックボックスをオンにし、**[Save]** をクリックします。

 注

監査ログイベントの登録を解除するには、syslog サーバーのチェックボックスをオフにして **[Save]** をクリックします。

8. 右側のペインで、**[Search]** フィールドを使用して、ログメッセージ内の特定のテキストを検索します。
9. メインメニューから次を選択します。**[Activities] > [Tasks]** で、OS の更新やデバイスの交換などの予定、進行中、完了および失敗したタスクと、既存、レビュー保留、および失敗した操作項目を確認します。

Syslog

安全で簡単なログモニタリングのため、**Catalyst Center** から syslog サーバーに監査ログをエクスポートすることについての情報。

監査ログの syslog を有効にすると、次のような利点があります。

- ロギングの一元化：ログを一元的に収集して保存し、モニタリングを容易にします。
- セキュリティモニタリング：不正または不審なアクティビティを迅速に検出します。

- 規則遵守：監査や調査用の改ざん防止記録を維持します。

複数の **syslog** サーバーに接続することで、監査ログを **Catalyst Center** から複数の **syslog** サーバーにエクスポートできます。

[System] > [Settings] > [External Services] > [Destinations] > [Syslog] 領域で **syslog** サーバーを設定します。

-
1. メインメニューから次を選択します。 **[Activities] > [Audit Logs]** の順に選択します。
 2. ウィンドウの上部にある鉛筆アイコンをクリックします。
 3. 接続する **syslog** サーバーを選択し、 **[Save]** をクリックします。
 4. オプション: **syslog** サーバーから切断するには、選択を解除して **[Save]** をクリックします。
-

サービスのデバッグログの設定に関する情報。

サービスの問題のトラブルシューティングに役立てるために、**Catalyst Center** サービスのログレベルを変更できます。

ログレベルによって、ログファイルでキャプチャされるデータ量が違います。各ログレベルは累積的です。つまり、各レベルには、指定されたレベル以上のレベルで生成されたデータがあれば、すべて含まれます。たとえば、ログレベルを **[Info]** に設定すると、**[Warn]** および **[Error]** ログもキャプチャされます。より多くのデータをキャプチャして、問題のトラブルシューティングに役立つようにログレベルを調整することをお勧めします。たとえば、ログレベルを調整することで、より多くのデータをキャプチャし、根本原因分析または **RCA** サポートファイルで確認できるようになります。

サービスのデフォルトのログレベルには情報提供 (**[Info]**) が含まれています。情報提供からのログレベルを、さまざまなログレベル (**[Debug]** または **[Trace]**) に変更して、より詳細な情報をキャプチャできます。

 注意

開示される可能性がある情報のタイプによっては、**[Debug]** レベル以上で収集されたログでアクセスを制限する必要があります。

 注

ログファイルが作成されると **Catalyst Center** ホストの一元的な場所に保存され、GUI で表示されます。この場所から、**Catalyst Center** は、GUI (**[System]** > **[System 360]** > **[Log Explorer]**) でログを照会して表示できます。ログは、過去2日間のクエリにのみ使用できます。2日以上経過したログは、この場所から自動的に消去されます。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#) (162ページ) を参照してください。

1. メインメニューから次を選択します。 **[System]** > **[Settings]** > **[System Configuration]** > **[Debugging Logs]** の順に選択します。

[Debugging Logs] ウィンドウが表示されます。

2. **[Service]** ドロップダウンリストからサービスを選択し、そのログレベルを調節します。

[Service] ドロップダウンリストには、現在 **Catalyst Center** に設定され、実行中のサービスが表示されます。

3. **[Logger Name]** を入力します。

これは、ロギングフレームワークにメッセージを出力するソフトウェアコンポーネントを制御するために追加された高度な機能です。この機能を使用する際は、十分注意してください。この機能を誤用すると、テクニカルサポートのために必要な情報が失われる可能性があります。ログメッセージは、ここで指定されたロガー（パッケージ）に対してのみ書き込まれます。デフォルトでは、ロガー名には **com.cisco** で始まるパッケージが含まれています。追加のパッケージ名はカンマ区切り値として入力できます。明示的に指示されていない限り、デフォルト値は削除しないでください。*を使用すると、すべてのパッケージがログに記録されます。

4. **[Logging Level]** ドロップダウンリストで、サービスの新しいログレベルを選択します。

Catalyst Center では次のログレベルがサポートされています（詳細は以下、降順）。

- **[Trace]** : トレースメッセージ
- **[Debug]** : デバッグメッセージ
- **[Info]** : 正常だが重要な状態メッセージ
- **[Warn]** : 警告状態メッセージ
- **[Error]** : エラー状態メッセージ

5. [Time Out] フィールドで、ログレベルの期間を選択します。

ログレベルの期間を 15 分単位で設定します（～無制限）。期間を無制限に指定する場合、トラブルシューティング作業が完了するたびに、デフォルトのログレベルをリセットする必要があります。

6. 選択内容を確認し、[Save] をクリックします。

Catalyst Center での高可用性（HA）のアクティブ化に関する情報。HA により、障害によるダウンタイムの量が削減され、ネットワークの復元力が向上します。

Catalyst Center クラスタで高可用性（HA）をアクティブにするには、次の手順を実行します。

 注

3 ノード HA は、Catalyst Center で実行されている ESXi ではサポートされていません。

『[Cisco Catalyst Center High Availability Guide](#)』の以下のトピックを確認し、実稼働環境が記載されている要件を満たしていることを確認します。

- 「ハイアベイラビリティ要件」
- 「サポートされるアプライアンス」

1. メインメニューから次を選択します。[System] > [Settings] > [System Configuration] > [High Availability] の順に選択します。
2. ページにクラスター内の 3 つの Catalyst Center アプライアンスが表示されていることを確認します。



3. [Activate High Availability] をクリックします。
4. HA が有効になっていることを確認します。
 - [Status] フィールドには、[Active] と表示されます。
 - [High Availability] ページの右上隅にある、[Activities] リンクをクリックします。結果のテーブルで、HA アクティブ化イベントのステータスが [SUCCESS] と表示されていることを確認します。

統合設定の設定に関する情報。ファイアウォールなどのルールが、**Catalyst Center**、および **Catalyst Center** プラットフォームと通信する必要があるサードパーティ製アプリケーションの間に存在する場合は、**[Integration Settings]** を設定する必要があります。

ファイアウォールなどのルールが、**Catalyst Center** と **Catalyst Center** プラットフォーム と通信する必要があるサードパーティ製アプリケーションの間に存在する場合は、**[Integration Settings]** を設定する必要があります。**Catalyst Center** の IP アドレスが、インターネットや外部ネットワークに接続する別の IP アドレスに内部的にマッピングされる場合には、このような事例が発生します。

重要

Catalyst Center のバックアップおよび復元後、**[Integration Settings]** ページにアクセスし、（必要に応じて）次の手順を使用して **[Callback URL Host Name]** または **[IP Address]** を更新する必要があります。

Catalyst Center プラットフォーム をインストールしておきます。

1. メインメニューから次を選択します。 **[System] > [設定] > [Integration Settings]** の順に選択します。
2. サードパーティ製アプリケーションが **Catalyst Center** プラットフォームと通信するときに接続する必要がある **[Callback URL Host Name]** または **[IP Address]** を入力します。

注

[Callback URL Host Name] または **[IP Address]** は、**Catalyst Center** に内部的にマッピングされている外部向けホスト名または IP アドレスです。3 ノードクラスセットアップの VIP アドレスを設定します。

3. **[Apply]** をクリックします。

設定の可視性と制御機能により、デバイス構成のプレビューを適用し、ネットワークに展開する前に **ITSM** の承認を要求できます。この機能により、デバイスの保護を強化できます。

[Visibility and Control of Configurations] 機能は、計画したネットワーク構成をデバイスに展開する前にセキュリティを強化するソリューションを提供します。優れた可視化機能により、デバイス構成を展開する前にプレビューできます（CLI および **NETCONF** コマンドを使用）。可視化機能はデフォルトで有効になっています。可視化機能が有効になっている場合は、確認するまでデバイス設定を展開できません。強化された制御により、計画されたネットワーク設定を **IT サービス管理 (ITSM)** に送信して承認できます。制御が有効になっている場合は、**IT** 管理者が承認するまで設定を展開できません。

 注

プロビジョニング ワークフローで **[Visibility and Control of Configurations]** がサポートされている場合は、タスク展開のスケジュール時に次のバナーメッセージが表示されます。

このワークフローでは、ネットワーク管理者などのユーザーがネットワークデバイスにワークフローを展開する前に、設定をプレビューできます。ワークフロー設定を構成するには、**[System] > [Settings] > [Visibility and Control of Configurations]** に移動します。

[ITSM Approval] を有効にできるように、**Catalyst Center** で **ITSM** が有効になっており、かつ設定されていることを確認します。ITSM を有効にし、設定する方法については、『[Catalyst Center ITSM Integration Guide](#)』の「[Configure the Catalyst Center Automation Events for ITSM \(ServiceNow\) Bundle](#)」[英語] を参照してください。

1. メインメニューから次を選択します。 **[System] > [Settings] > [System Configuration] > [Visibility and Control of Configurations]** の順に選択します。
2. **[Configuration Preview]** トグルボタンをクリックして、可視性を有効または無効にします。
可視性を有効にした場合、デバイス設定を展開する前にプレビューする必要があります。
可視性を無効にした場合、デバイス設定を展開する前にプレビューを強制されなくなります。可視性が無効になっている場合は、プレビューの要否にかかわらず設定をスケジュールして展開できます。
3. オプション: **[ITSM Approval]** トグルボタンをクリックして制御を有効または無効にします。
制御を有効にした場合、計画したネットワーク構成を展開する前に、**ITSM** 管理者に送信して承認を受ける必要があります。
制御を無効にした場合、計画したネットワーク構成を展開する前の **ITSM** の承認が不要になります。制御が無効になっている場合、**ITSM** の承認なしで設定を展開できます。

[Tasks] ウィンドウで、タスクと作業項目の詳細を表示、検索、およびフィルタリングできます。

[Tasks] ウィンドウで、タスクと作業項目の詳細を表示、検索、およびフィルタリングできます。

1. メインメニューから次を選択します。 **[Activities] > [Tasks]** の順に選択します。
デフォルトでは、**[Tasks]** ウィンドウには実行予定、進行中、失敗、および成功したすべてのタスクに加えて、既存の作業項目やレビュー保留中、失敗した作業項目が表示されます。失敗したすべてのタスクには、エラーログを迅速に分析するためのヒントを提供するトレース ID があります。左側の **[SUMMARY]** ペインには、表示されるタスクと作業項目のリストを絞り込むためのフィルタリングオプションが表示されます。矢印アイコンをクリックすると、**[SUMMARY]** ペインを展開したり折りたたんだりできます。
2. 次の表を使用して、**[Tasks]** ウィンドウでタスクと作業項目の詳細を表示、検索、およびフィルタ処理できます。

アクション	手順
特定のタスクと作業項目の詳細をフィルタ処理します。	a. [SUMMARY] ペインの [Type] で、[Task] をクリックしてタスクのみをフィルタリングするか、[Work Item] をクリックして作業項目のみをフィルタリングします。 b. [Status] > [Review Status] > [Last Updated] > [Categories] > [Recurring] で使用可能なフィルタオプションを使用して、タスクと作業項目の詳細をフィルタリングします。 フィルタリングが適用された結果が [Tasks] ウィンドウに表示されます。  ヒント [Categories] で [Show all] をクリックして [Search] フィールドを使用すると、特定のカテゴリを検索できます。
適用されたフィルタを削除します。	a. [SUMMARY] ペインの [FILTERED BY] で、適用したフィルタの横にある [x] をクリックします。 フィルタを削除した結果が [Tasks] ウィンドウに表示されます。 b. チェックボックスをオフにして、[Status]、[Review Status]、および [Categories] フィルタを削除することもできます。
タイトルまたはユーザー名でタスクと作業項目を検索します。	デフォルトでは、[Search] フィールドは、説明によってタスクと作業項目を検索します。タスクまたは作業項目の検索時にフィルタが適用されている場合は、適用されたフィルタで検索が実行されます。たとえば、[In Progress] フィルタを適用して、名前に「provision」が含まれるすべてのタスクと作業項目を検索した場合、このキーワードを含む進行中のタスクと作業項目のみが検索されます。 a. [Search by description] フィールドに、タスクまたは作業項目の説明を入力します。 [Tasks] ウィンドウには、入力した説明に基づいてフィルタリングされたタスクと作業項目のリストが表示されます。 b. ユーザー名で検索するには、[Search] フィールドで次の手順を実行します。 1. フィルタアイコンをクリックします。 2. [username] をクリックします。 3. [Search by username] フィールドにユーザー名を入力します。 4. [Apply] をクリックします。

アクション	手順
タスクと作業項目のリストをソートします。	デフォルトでは、タスクと作業項目は最終更新日時順に表示されます。タスクと作業項目は、開始時刻または更新時刻でソートできます。 a. [Search] フィールドの右側でソートドロップダウンリストにカーソルを合わせ、ソートオプションを選択します。 [Tasks] ウィンドウには、選択したソートオプションに基づいてソートされたタスクと作業項目のリストが表示されます。

タスクは、ユーザーまたはシステムがスケジュール設定した操作であり、繰り返される可能性があります。**[Tasks]** ウィンドウでは、進行中、完了、失敗したタスクや、レビューが保留中、完了、失敗した作業項目を表示できます。

Catalyst Center では、実行予定のタスク、実行中のタスク、失敗したタスク、および完了したタスクを表示できます。

タスクは、ユーザーまたはシステムがスケジュール設定した操作であり、繰り返される可能性があります。タスクがある場合、これは、スケジュールどおりに展開するために完了する必要がある対応する作業項目がないことを意味します。

タスクで使用可能な情報はカテゴリによって異なり、さまざまなカテゴリが存在します。一般的なタスクのカテゴリには、プロビジョニング、設定アーカイブ、インベントリ、セキュリティアドバイザリなどがあります。すべてのタスクには、タスクの開始者、そのカテゴリ、完了ステータス、成功ステータス、開始日、最終更新日、および終了日が詳細として表示されます。

1. メインメニューから次を選択します。[Activities] > [Tasks]の順に選択します。

デフォルトでは、**[Tasks]** ウィンドウには実行予定、進行中、失敗、および成功したすべてのタスクに加えて、既存の作業項目やレビュー保留中、失敗した作業項目が表示されます。

注

タスクでタイムゾーンが異なる複数のデバイスに対してサイト設定を有効にした場合、**[Starts]** フィールドには、ローカルタイムゾーンに基づく最も早いタイムゾーンでのデバイスの開始時刻が表示されます。たとえば、太平洋標準時ゾーンにおいて、**2024 年 5 月 8 日午後 12 時**に展開予定の**2**つのデバイスがあるとして。一方のデバイスはカリフォルニア州サンノゼにあり、もう一方のデバイスはインドのベンガルールにあります。ローカルタイムゾーンは最も早いタイムゾーンのデバイスと一致するため、**[Starts]** フィールドには**2024 年 5 月 8 日 12:00 PM**と表示されます。インドのベンガルールにいる場合、ローカル時刻は最も早いタイムゾーンでデバイスより**12 時間 30 分**進んでいるため、このフィールドには**2024 年 5 月 9 日 12:30 AM**と表示されます。

2. [Tasks] ウィンドウでタスクを表示、編集、または削除するには、次の表を使用します。

アクション	手順
タスクを表示します。	a. タスク名をクリックすると、スライドインペインが開いて詳細情報が表示されます。 タスクの詳細は、表示されたタスクの種類によって異なります。 b. スライドインペインでは、表示された詳細に応じて、次の操作を実行できます。 • [Device Details] または [Provision Details] をクリックすると、デバイスとプロビジョニングの詳細が表示されます。 • [View Details] または [See Details] をクリックすると、進行中のタスク、完了したタスク、および失敗したタスクの詳細が表示されます。 • [Search Table] を使用してタスクを検索します。 • 表の右上隅にあるフィルタアイコンを使用して、タスクをフィルタ処理します。 • 失敗したタスクのエラーレポートをダウンロードするには、[Download Error Report] をクリックします。 tar ファイルが作成され、ローカルマシンに保存されます。

ヒント

サポートケースを作成する際に、含めるその他の詳細に加えて、ダウンロードしたエラーレポートを添付できます。

定期タスクのスケジュールを編集します。

アクション	手順
	a. タスクを見つけて [Edit] をクリックします。 b. [Edit Schedule] スライドインペインで [Start Date] と [Start Time] を定義します。 c. [Recurrence] トグルボタンを使用して、繰り返し間隔をクリックします。 d. [Run at Interval] フィールドに値を入力します。 e. (オプション) このタスクの終了日時をスケジュールするには、次の手順を実行します。 1. [Set Schedule End] チェックボックスをオンにします。 2. 特定の日付にタスクを終了するには、[End Date] をクリックして日付を選択します。 3. ある回数の発生後にタスクを終了するには、[End After] をクリックし、[Occurrences] フィールドに数値を入力します。 f. [Preview] をクリックして、表が変更されていることを確認します。 g. 表にリストされている各デバイスの [Site Time] (デバイスのタイムゾーン) と [Local Time] (ユーザーのタイムゾーン) に、意図したスケジュール時刻が反映されていることを確認します。 h. 準備ができれば、[Save] をクリックします。
タスクを停止します。	a. タスク名をクリックすると、スライドインペインが開いて詳細情報が表示されます。 b. [Stop] をクリックします。
	 注 プロビジョニングワークフローがこの機能をサポートしていない場合、[Stop] は無効になります。 c. [Stop] ダイアログボックスで [Yes] をクリックしてタスクの停止を確定します。 タスクは、進行中の場合にのみ停止できます。システムがデバイスの設定を開始すると、タスクは停止できません。プロビジョニングが保留中になっているデバイスのみが停止します。
タスクを削除します。	a. タスクを見つけて [Delete] をクリックします。

構成の可視化と制御機能を有効にした場合、任意のワークフローで **[Generate configuration preview]** を選択すると、作業項目が作成されます。構成が確認され、展開の準備ができると、その作業項目がタスクになります。**[Tasks]** ウィンドウで作業項目を表示できます。

構成の可視化と制御機能を有効にした場合、任意のワークフローで **[Generate configuration preview]** を選択すると、作業項目が作成されます。構成が確認され、展開の準備ができると、その作業項目がタスクになります。

構成の可視性と制御を有効にするには、「[設定の可視性と制御の有効化（135ページ）](#)」を参照してください。

-
1. メインメニューから次を選択します。**[Activities]** > **[Tasks]**の順に選択します。

デフォルトでは、**[Tasks]** ウィンドウには実行予定、進行中、失敗、および成功したすべてのタスクに加えて、既存の作業項目やレビュー保留中、失敗した作業項目が表示されます。

2. 次の表を使用して、**[Tasks]** ウィンドウで作業項目を表示および破棄します。

アクション**手順**

作業項目を表示します。

アクション

手順

- a. [SUMMARY] ペインの [Type] で [Work Item] をクリックします。
[Tasks] ウィンドウは作業項目のみをフィルタ処理して表示します。
- b. 作業項目名をクリックすると、スライドインペインが開いて詳細情報が表示されます。
最初にリストされているデバイスの構成プレビューが表示されます。
- c. スライドインペインでは、次の操作を実行できます。
 - 左側のペインでデバイスを選択して、デバイスの構成をプレビューします。
 - **[View by Configuration Source]** ドロップダウンリストを使用して、構成プレビューウィンドウのデータをフィルタ処理します。
 - ビュースイッチャ ( ) をクリックして、計画された構成と実行中の構成の比較ビューを並べて表示するか、計画された構成のみを表示します。

 注

並列比較ビューは YANG 構成の表示には対応していません。

- 並列比較ビューでは、一方の構成で 1 つのコマンドをクリックすると、もう一方の構成で対応するコマンドが強調表示されます。

 注

次の制限事項に注意してください。

- システムでは、サブレベルのコマンドではなく、第 1 レベルのコマンドに対する並列強調表示のみがサポートされています。
 - 構成間で強調表示を並べて表示するには、すべてのコマンドが完全に一致している必要があります。
 - 一方の構成で No で始まるコマンドをクリックすると、もう一方の構成で一致をチェックするときに No の部分が無視されます。
- **[Search Configuration]** フィールドを使用して、表示された構成中の値を検索します。
 - 選択したデバイスのワークフローの進行状況を表示するには、右側のペインの右上隅にある **[Back to workflow progress]** をクリックします。[Configuration Preview] ペインに戻るには、[Go

アクション

手順

to generated config] をクリックします。

 注

[Back to workflow progress] および [Go to generate config] は、ワークフローでワークフローの進行状況ビューがサポートされている場合にのみ使用できます。

作業項目の破棄

- a. 作業項目を見つけて、[Discard] をクリックします。

作業項目名をクリックしてスライドインペインを開き、[Discard] をクリックすることもできます。

- b. [Discard] ダイアログボックスで、次のいずれかを実行します。

- 作業項目を破棄して現在のアクティビティに戻る場合は、[Discard] をクリックします。

 注

作業項目を破棄した場合、後から復元できません。

- 生成された任意の構成を保持し、他のすべてのリソースを破棄する場合は、[Retain generated configs (if any)] チェックボックスをオンにして [Accept] をクリックします。

生成された構成を保持し、他のすべてのリソースを破棄すると、すべての構成をプレビューし、生成されていない構成を破棄することを選択したため、[Exit and Preview Later] の代わりに [Exit] が作業項目に表示されます。

 ヒント

構成のプレビューが失敗した場合は、生成された構成を保持し、他のすべてのリソースを破棄して、ユーザーまたは IT 管理者が問題を詳細に調査できるようにすることを検討してください。

プレビューしたデバイス構成を展開するか、ITSM 承認のために計画されたネットワーク構成を送信するには、『[Cisco Catalyst Center User Guide](#)』の「[Visibility and Control of Configurations Workflow](#)」、「[Visibility and Control of Wireless Device Configurations](#)」、または「[Visibility and Control of Fabric Configurations](#)」を参照してください。

Geo

このトピックでは、**Catalyst Center** で **Geo** マップ設定を構成する方法について説明します。

Catalyst Center で **Geo** マップ設定を構成できます。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**System Configuration**] > [**Geo Map Settings**] の順に選択します。
 2. 利用可能な管理境界をひとつ選択します。この境界はさまざまな地域的、文化的、または政治的グループに属する対象者によって異なる特性で定義される地理的特徴を示します。
 - 中国 (CN)
 - インド (IN)
 - 日本 (JP)
 - 米国 (US) (デフォルト)
 3. [**Save**] をクリックします。
-

ユーザーが **Catalyst Center** にログインするときに表示されるログインメッセージの設定に関する情報。

Catalyst Center にログインしたすべてのユーザーに表示されるメッセージを設定できます。

SUPER-ADMIN-ROLE またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザーのみがこの手順を実行することができます。

1. メインメニューから次を選択します。[**System**] > [**Settings**] > [**System Configuration**] > [**Login Message**] の順に選択します。
2. [**Login Message**] テキストボックスにメッセージを入力します。
3. [**Save**] をクリックします。

このメッセージは、**Catalyst Center** ログインページの [**Log In**] ボタンの下に表示されます。

後でこのメッセージを削除する場合は、次の手順を実行します。

- a. [**Login Message Settings**] ページに戻ります。

b. [Clear] をクリックし、[Save] をクリックします。

第

8

章

:

- □□□□□□□□

|

シスコは、お客様の製品エクスペリエンスを向上させるために、お客様のシステム情報を収集します。

Catalyst Center Offer Disclosure は、データの取り扱い方法、セキュリティ管理、および AI 機能について、**Catalyst Center** に固有の詳細情報を提供します。これは、お客様のシステム情報とお客様のコンテンツの取り扱いに関するシスコの全般的アプローチの概要を述べる一般開示事項、およびシスコの個人データの管理方法をより詳細に説明するシスコ オンライン プライバシー ステートメントを補完するものです。この 2 つの文書は、データ処理の概要とオファー固有の詳細を説明することによって透明性を提供し、シスコがオファー全体で情報をどのように保護および処理しているかを理解していただくのに役立ちます。

メインメニューから次を選択します。、**[System] > [Settings] > [Terms and Conditions]** の順に選択します。**[Product Telemetry]** ウィンドウから、ライセンス契約、プライバシーポリシー、プライバシーデータシートを確認できます。

第9

章

:

- [□□□□ □□□□□](#)
- [□□□□□□□□□□□](#)
- [IP □□□□□](#)
- [□□□□□□](#)

アカウントロックアウトポリシーを設定して、ユーザーによるログインの試行、アカウントのロックアウト期間、ログインのエントリ回数を管理することについての情報。

アカウントロックアウトポリシーを設定して、ユーザーによるログインの試行、アカウントのロックアウト期間、ログインの再試行回数を管理できます。

デフォルトでは、アカウントロックアウトは、ユーザー名と送信元 IP アドレスの両方に対して失敗した試行を追跡するデュアルレイヤセキュリティを使用します。トリガーされると、両方の要素が同時にロックされます。IP アドレスはすべての認証試行からブロックされ、ユーザー名はすべての IP アドレスでロックされます。

アカウントロックアウトは、外部認証ユーザーではなく、ローカルユーザーにのみ影響します。

1. メインメニューから次を選択します。[System] > [Settings] > [Trust & Privacy] > [Account Lockout] の順に選択します。
2. [Enforce Account Lockout] トグルボタンをクリックして、チェックマークが表示された状態にします。
3. [Enforce Account Lockout] の次のパラメータの値を入力します。
 - Maximum Login Retries
 - Lockout Effective Periods (minutes)
 - Reset Login Retries after (minutes)

注

[Info] にカーソルを合わせると、各パラメータの詳細が表示されます。

4. [Idle Session Timeout] の値（セッションが期限切れになり、ユーザーがログインページにリダイレクトされるまでの時間）を選択します。デフォルトは 1 時間です。
5. [Save] をクリックします。

セッションをアイドル状態のままにすると、セッションタイムアウトの 5 分前に [Session Timeout] ダイアログボックスが表示されます。

続行するには、次のいずれかのタスクを実行します。

 - セッションを続行する場合は、[Stay signed in] をクリックします。
 - すぐにセッションを終了するには、[Sign out] をクリックします。

パスワード有効期限ポリシーの設定に関する情報。

パスワード有効期限ポリシーを設定して、以下を管理できます。

- パスワードの有効期限の通知間隔
- パスワードが期限切れになる前にユーザーに通知が表示される日数
- 猶予期間

1. メインメニューから次を選択します。[System] > [Settings] > [Trust & Privacy] > [Password Expiry] の順に選択します。
2. [Enforce Password Expiry] トグルボタンをクリックして、チェックマークが表示された状態にします。
3. 次の [Enforce Password Expiry] パラメータの値を入力します。
 - パスワード期限（日）
 - パスワードの期限の警告（日）
 - 猶予期間（日）

注

[Info] にカーソルを合わせると、各パラメータの詳細が表示されます。

4. [Save] をクリックして、パスワード有効期限設定を保存します。

IP

ホストまたはネットワークの IP アドレスに基づいて **Catalyst Center** へのアクセスを制御する IP アクセス制御に関する情報。

IP アクセス制御により、ホストまたはネットワークの IP アドレスに基づいて **Catalyst Center** へのアクセスを制御できます。この機能では、**Catalyst Center GUI** へのアクセスのみを制御できます。この機能で、企業全体のネットワークアクセスを制御することはできません。

Catalyst Center には、次を含む IP アクセス制御のオプションが用意されています。

- **Catalyst Center** へのアクセスをすべての IP アドレスに許可します（デフォルト）。
- 選択した IP アドレスのみに **Catalyst Center** へのアクセスを許可します。

IP

選択した IP アドレスのみに **Catalyst Center** へのアクセスを許可するように IP アクセス制御を構成することについての情報。

IP アクセス制御を構成し、選択した IP アドレスのみに **Catalyst Center** へのアクセスを許可するには、次の手順を実行します。

1. [IP アクセス制御の有効化](#)（152ページ）
2. [IP アドレスリストへの IP アドレスの追加](#)（152ページ）

3. (任意) [IP アクセスリストからの IP アドレスの削除](#) (153ページ)

IP

Catalyst Center へのアクセスに選択した IP アドレスのみに対する IP アクセス制御の有効化に関する情報。

- SUPER-ADMIN-ROLE 権限を取得しておきます。
- Catalyst Center サービスサブネット、クラスタサービスサブネット、およびクラスタ インターフェイス サブネットを許可サブネットのリストに追加します。

1. メインメニューから次を選択します。[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。
2. [リストされている IP アドレスのみに接続を許可する (Allow only listed IP addresses to connect)] オプション ボタンをクリックします。
3. [Add IP List] をクリックします。
4. [Add IP] スライドインペインの [IP Address] フィールドに、IP アドレスを入力します。

注

IP アドレスを IP アクセスリストに追加しないと、Catalyst Center にアクセスできなくなる可能性があります。

5. [Subnet Mask] フィールドにサブネット マスクを入力します。
サブネットマスクの有効範囲は 0 ～ 32 です。
6. [Save] をクリックします。

IP IP

IP アクセスリストへの IP アドレスの追加に関する情報。

IP アクセスリストに IP アドレスを追加するには、次の手順を実行します。

IP アクセス制御が有効になっていることを確認してください。詳細については、[IP アクセス制御の有効化](#) (152ページ) を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。
2. [Add] をクリックします。

3. **[Add IP]** スライドインペインの **[IP Address]** フィールドに、ホストまたはネットワークの IP アドレスを入力します。
4. **[Subnet Mask]** フィールドにサブネット マスクを入力します。
サブネットマスクの有効範囲は **0 ~ 32** です。

5. **[Save]** をクリックします。

IP IP

IP アクセスリストから IP アドレスを削除して **Catalyst Center** へのアクセスを無効にする方法についての情報。

IP アクセスリストから IP アドレスを削除して **Catalyst Center** へのアクセスを無効にするには、以下の手順を実行します。

IP アクセスコントロールを有効にして、IP アドレスを IP アクセスリストに追加したことを確認します。詳細については、[IP アクセス制御の有効化](#)（152ページ）および[IP アクセスリストへの IP アドレスの追加](#)（152ページ）を参照してください。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Trust & Privacy] > [IP Access Control]** の順に選択します。
2. **[Action]** 列で、対応する IP アドレスの **[Action]** アイコンをクリックします。
3. **[Delete]** をクリックします。

IP

すべての IP アドレスが **Catalyst Center** にアクセスできるように、IP アクセス制御を無効化することについての情報。

IP アクセス制御を無効化し、すべての IP アドレスに **Catalyst Center** へのアクセスを許可するには、次の手順を実行します。

SUPER-ADMIN-ROLE 権限を取得しておきます。

-
1. メインメニューから次を選択します。[System] > [Settings] > [Trust & Privacy] > [IP Access Control] の順に選択します。
 2. [Allow all IP addresses to connect] オプションボタンをクリックします。
-

Catalyst Center では、個人を特定できるデータを匿名化できます。匿名化を有効にすると、デバイス検索時に、MAC アドレス、IP アドレスなどの匿名以外の情報しか指定できなくなります。

Catalyst Center では、有線エンドポイントとワイヤレスエンドポイントのデータを匿名化できます。ユーザー ID やデバイスのホスト名など、有線エンドポイントとワイヤレスエンドポイントの個人を特定できる情報をスクランブル化できます。

[Discovery] を実行する前に、匿名化が有効になっていることを確認します。[Discovery] を実行した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

-
1. メインメニューから次を選択します。[System] > [Settings] > [Trust & Privacy] > [Anonymize Data] の順に選択します。
 2. [Anonymize Data] ウィンドウで、[Enable Anonymization] チェックボックスをオンにします。
 3. [Save] をクリックします。
匿名化を有効にすると、デバイス検索時に、MAC アドレス、IP アドレスなどの匿名以外の情報しか指定できなくなります。
-

第10

章

- :
- -
 -
 -

Catalyst Center でのアプリケーションの管理に関する情報。

Catalyst Center のアプリケーション管理に関する情報。**Catalyst Center** はその多くの機能を、**Catalyst Center** のコアインフラストラクチャとは別にパッケージ化された個別のアプリケーションとして扱います。このため、ユーザーは設定に応じて、必要なアプリケーションをインストールして実行し、使用していないアプリケーションをアンインストールできます。

Catalyst Center はその多くの機能を、コアインフラストラクチャとは別にパッケージ化された個別のアプリケーションとして扱います。このため、ユーザーは設定に応じて、必要なアプリケーションをインストールして実行し、使用していないアプリケーションをアンインストールできます。

[Software Management] ウィンドウに表示されるアプリケーションパッケージの数とタイプは、**Catalyst Center** のリリースおよび **Catalyst Center** のライセンスレベルによって異なります。使用可能なアプリケーションパッケージはすべて、現在インストールされているかどうかに関係なく表示されます。

一部のアプリケーションは基本的なアプリケーションであり、ほぼすべての **Catalyst Center** の導入で必要になります。パッケージの説明については、**[View Installed Applications]** リンクをクリックし、その名前の上にカーソルを置きます。

各 **Catalyst Center** アプリケーションパッケージは、サービスバンドル、メタデータファイル、およびスクリプトで構成されています。

注

- パッケージ管理アクティビティでは **CLI** コマンドを使用しないでください。**Catalyst Center** のパッケージのインストールまたはアップグレードタスクで問題が発生した場合は、**Cisco TAC** に連絡してサポートを受けてください。
- **[Software Maintenance]** ウィンドウから、入手可能な最新の **Catalyst Center** リリースにアップグレードできます。アップグレード手順については、『[Cisco Catalyst Center Upgrade Guide](#)』を参照してください。

Catalyst Center でのアプリケーションのダウンロードとインストールに関する情報。

Catalyst Center 個々のアプリケーションはコアインフラストラクチャから独立して扱われます。具体的には、アプリケーションの個別のパッケージをインストールして、**Catalyst Center** 上で実行できます。

アプリケーションパッケージのインストールとデプロイには時間がかかる場合があるため、ネットワークのメンテナンス期間中にスケジュールしてください。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#)（162ページ）を参照してください。

1. メインメニューから次を選択します。 **[System] > [Software Management]** の順に選択します。
重要

この時点で、**Catalyst Center**によって接続性チェックが実行されます。接続に問題がある場合、[Software Management] ウィンドウに、現在利用可能なアプリケーションは表示されません。

2. ウィンドウの下部で、インストールするアプリケーションを選択します。

次のいずれかを行うことができます。

- すべてのアプリケーションを選択する：[Select All] をクリックします。
- 個々のアプリケーションを選択する：チェックボックスをオンにします。



任意のアプリケーションカードで [View Details] をクリックして、使用可能なアプリケーションの詳細を表示します。

3. [Install] をクリックします。



インストール中に依存関係がチェックされ、自動的にインストールされます。

ウィンドウの上部に、進行中のバナーメッセージが表示されます。

リアルタイムの進行中の詳細を表示するには、[View Release Activities] をクリックします。関連するアクティビティでは、[Actions] 列の省略記号 (...) にカーソルを合わせ、[View Status] を選択します。

4. [View Installed Applications] をクリックし、選択したアプリケーションがインストールされていることを確認します。

パッケージのダウンロードとアップグレードのイベント通知に関する情報。

パッケージのダウンロードまたはアップグレードイベントが発生するたびに通知を受信できます。これらの通知を設定および登録するには、『[Cisco Catalyst Center Platform User Guide](#)』の「[Work with event notifications](#)」トピックに説明されている手順を実行してください。この手順を完了したら **SYSTEM-SOFTWARE-UPGRADE-v2** イベントを選択し、サブスクライブしていることを確認します。

次の場合に通知が生成され、送信されます。

- パッケージのアップグレードのダウンロードに失敗しました。これは通常、**Catalyst Center** アプライアンスに必要なディスク容量がないか、破損したパッケージをダウンロードしようとしているために発生します。
- パッケージのアップグレードのインストールに失敗しました（パッケージに関連付けられているサービスが現在ダウンしているためと考えられます）。
- パッケージのアップグレードのダウンロードまたはインストールが成功しました。

 注

通知は、以前にこの操作を完了するために行った試行が失敗した場合にのみ送信されます。

アップグレード概要レポートスライドインペインを開く方法と、そこから提供される情報について説明します。

[Upgrade Summary Report] スライドインペイン から、**Catalyst Center** およびそのアプリケーションの最新のアップグレードの結果を表示できます。このレポートにより、次のことが可能になります。

- アプライアンスにインストールされている以前の **Catalyst Center** バージョンを特定します。
- アップグレードがいつ行われたかを確認します。
- **[Post-check]** タブで、アップグレード後チェック **Catalyst Center** が正常に完了したかどうかを確認します。特定のチェックで問題が発生した場合は、**[Issues]** 列にある情報 **[i]** アイコンをクリックして問題の説明を確認します。
- **[Packages]** タブには、アップグレードされたアプリケーションパッケージとその現在のバージョン番号が表示されます。

このレポートを開くには、次の手順を実行します。

1. **[System] > [Software Management]** メインメニューから次を選択します。
2. **[Upgrade Summary Report]** リンクをクリックします。

Catalyst Center でのアプリケーションのアンインストールに関する情報。

Catalyst Center 個々のアプリケーションはコアインフラストラクチャから独立して扱われます。具体的には、**Catalyst Center** からアプリケーションの個々のパッケージをアンインストールすることができます。

アンインストールできるのはシステムに必須でないアプリケーションのパッケージのみです。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#)（162ページ）を参照してください。

1. メインメニューから次を選択します。 **[System] > [Software Management]** の順に選択します。

2. **[View Installed Applications]** をクリックして、**Catalyst Center** にインストールされているすべてのアプリケーションを表示します。
3. 削除するパッケージに対して、そのパッケージの **[Uninstall]** チェックボックスをオンにします。

 注

- 同時に複数のパッケージをアンインストールすることはできません。
- アンインストールできるのは、オプションパッケージのみです。

4. **[Uninstall]** をクリックして、アプリケーションのアンインストールを確認します。

ウィンドウの上部に、進行中のバナーメッセージが表示されます。リアルタイムの進行中の詳細を表示するには、**[Software Management]** ウィンドウで **[View Release Activities]** をクリックします。関連するアクティビティでは、**[Actions]** 列の省略記号 () にカーソルを合わせ、**[View Status]** を選択します。

5. **[View Installed Applications]** をクリックし、アプリケーションがアンインストールされたことを確認します。
-

11

章

$$\vdots$$

- [illegible]

Catalyst Center でのユーザーの管理に関する情報。

Catalyst Center のユーザープロフィール情報。

ユーザープロフィールで、ユーザーのログイン、パスワード、メールアドレス、およびロール（権限）を定義します。

ユーザーの内部プロフィールと外部プロフィールの両方を設定できます。内部ユーザープロフィールは **Catalyst Center** に配置され、外部ユーザープロフィールは外部 **AAA** サーバーに配置されます。

Catalyst Center をインストールすると、**SUPER-ADMIN-ROLE** 権限を持つデフォルトのユーザープロフィールが作成されます。

Catalyst Center で使用可能なユーザーロールを一覧表示します。

各ユーザーは、次のユーザーロールを割り当てられます。ユーザーが実行できる機能はこれによって決まります。

- **管理者（SUPER-ADMIN-ROLE）**：このロールを持つユーザーは、**Catalyst Center** のすべての機能へのフルアクセスが可能です。管理者は、**SUPER-ADMIN-ROLE** を含むさまざまなロールを持つ他のユーザープロフィールを作成できます。
- **ネットワーク管理者（NETWORK-ADMIN-ROLE）**：このロールを持つユーザーは、**Catalyst Center** のすべてのネットワーク関連機能へのフルアクセスが可能です。ただし、バックアップと復元など、システム関連の機能へのアクセス権はありません。
- **オブザーバ（OBSERVER-ROLE）**：このロールを持つユーザーは、**Catalyst Center** の機能への表示専用アクセスが可能です。オブザーバロールを持つユーザーは、**Catalyst Center** やそれが管理するデバイスを設定または制御する機能にはアクセスできません。
- **Customized Role**：**SUPER-ADMIN-ROLE** 権限を持つユーザーは、特定の **Catalyst Center** 機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

Catalyst Center での内部ユーザーの作成とユーザーロールの割り当てに関する情報。

ユーザーを作成してロールを割り当てることができます。

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、[ユーザーロールについて](#)（162ページ）を参照してください。

-
1. メインメニューから次を選択します。[**System**] > [**Users & Roles**] > [**User Management**] の順に選択します。
 2. [**Add**] をクリックします。
 3. 新しいユーザーの姓、名、電子メールアドレス、およびユーザー名を入力します。
電子メールアドレスは、**Apache EmailValidator** クラスで定義された要件に準拠している必要があります。

4. **[Role List]** で、**SUPER-ADMIN-ROLE**、**NETWORK-ADMIN-ROLE**、または **OBSERVER-ROLE** のいずれかのロールを選択します。
 5. パスワードを入力し、確認します。
 6. **[Save]** をクリックします。
-

Catalyst Center におけるユーザーのプロパティの編集に関する情報。

一部のユーザープロパティは編集できますが、ユーザー名は編集できません。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#)（162ページ）を参照してください。

-
1. メインメニューから次を選択します。 **[System] > [Users & Roles] > [User Management]** の順に選択します。
 2. 編集するユーザーの横にあるオプションボタンをクリックします。
 3. **[Edit]** をクリックします。
 4. 必要に応じて、姓、名または電子メールアドレスを編集します。
 5. **[Role List]** で、必要に応じて新しいロール（**[SUPER-ADMIN-ROLE]**、**[NETWORK-ADMIN-ROLE]**、または **[OBSERVER-ROLE]**）を選択します。
 6. **[Save]** をクリックします。
-

Catalyst Center でのユーザーの削除に関する情報。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#)（162ページ）を参照してください。

-
1. メインメニューから次を選択します。 **[System] > [Users & Roles] > [User Management]** の順に選択します。
 2. 削除するユーザーの横にあるオプションボタンをクリックします。
 3. **[Delete]** をクリックします。
 4. 確認のプロンプトで、**[Continue]** をクリックします。
-

Catalyst Center のパスワードポリシーについて説明します。

Catalyst Center をデプロイしたら、以下のパスワードポリシーの要件を確認します。

Catalyst Center

このセクションでは、新規のデプロイ用のパスワードポリシーについて説明します。

- **maglev** ユーザーおよび管理者スーパーユーザーのデフォルトパスワードは、**P@ssword9** です。
初めて **Catalyst Center GUI** にログインすると、管理者スーパーユーザーのパスワードを変更するように求められます。
- ユーザーのパスワードを変更するか、新しいユーザーを設定する場合は、そのユーザーのパスワードが新しい要件に準拠していることを確認します。

Catalyst Center

このセクションでは、システムアップグレード時のパスワードの動作について説明します。

- 以前のバージョンの **Catalyst Center** で設定されたロールベースアクセスコントロール (RBAC) ユーザーは、引き続き現在のパスワードを使用して **Catalyst Center 2.3.7.9** 以降にログインできます。
たとえば、アプライアンスをバージョン **2.3.7.6** から **2.3.7.11** にアップグレードしたとします。アプライアンスからデータをバックアップしました。その後、**Catalyst Center 2.3.7.11** がインストールされている別のアプライアンスにバックアップファイルを復元しました。既存の RBAC ユーザーは、現在のパスワードを使用してログインできます。
- ユーザーのパスワードを変更するか、新しい RBAC ユーザーを設定する場合は、そのユーザーのパスワードが新しい要件に準拠していることを確認します。

新しいパスワードが満たす必要がある基準については、「[パスワード要件 \(164ページ\)](#)」を参照してください。

Catalyst Center のパスワード要件について説明します。

Catalyst Center 2.3.7.11 以降で設定したユーザーパスワードは、次の要件を満たしている必要があります。

- 9 文字以上である必要があること。
- 次のうち少なくとも 3 つのカテゴリの文字を含むこと。
 - 大文字の A ~ Z
 - 小文字の a ~ z
 - 数字 (0 ~ 9)
 - 特殊文字 (例 : !, \$, # など)
- 英語の QWERTY キーボード上で連続する文字を 4 文字以上含まないこと。
たとえば、59Asdfpj! は、a、s、d、および f の文字が連続して含まれているため、有効なパスワードではありません。
- 関連するユーザー名にある連続する文字を 2 文字以上含まないこと。

- 任意の言語の完全な単語を含まないこと。
- 個人情報に基づくフレーズを含まないこと。

 注

24 個の異なるパスワードを使用した後にのみ、以前のパスワードを再利用できます。

ユーザーパスワードのリセットに関する情報。

別のユーザーのパスワードをリセットできます。

セキュリティ上の理由から、パスワードは管理者を含め、どのユーザーに対しても表示されません。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザロールについて](#)（162ページ）を参照してください。

-
1. メインメニューから次を選択します。[**System**] > [**Users & Roles**] > [**User Management**] の順に選択します。
 2. パスワードをリセットするユーザーの横にあるオプションボタンをクリックします。
 3. [**More Actions**] ドロップダウンリストから、[**Reset Password**] をクリックします。
 4. パスワードを入力し、確認します。
 5. [**Save**] をクリックします。
-

自身のユーザーパスワードの変更にに関する情報。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、「[ユーザーロールについて](#)」を参照してください。

-
1. メインメニューから次を選択します。[**System**] > [**Users & Roles**] > [**Change Password**] の順にクリックします。
 2. 必要なフィールドに情報を入力します。
 3. [**Update**] をクリックします。
-

管理者権限なしでのユーザーパスワードの変更にに関する情報。

次の手順では、管理者権限なしでパスワードを変更する方法について説明します。

1. 右上隅で、表示されたユーザー名をクリックし、**[My Profile and Settings] > [My Account]** の順に選択します。
2. **[Password]** フィールドで、**[Update Password]** をクリックします。
3. **[Update Password]** ダイアログボックスに新しいパスワードを入力し、新しいパスワードを確認します。
4. **[Update]** をクリックします。

思い出せないパスワードのリセットに関する情報。

パスワードを忘れた場合は、**CLI** を使用してパスワードをリセットできます。

注

セキュリティを強化するため、ルートシェルへのアクセスは **Catalyst Center** で無効になっています。Shell コマンドへのアクセスが制限されることで、ユーザーは基礎となるオペレーティングシステムとファイアシステムにアクセスできなくなります。これにより、運用上のリスクが軽減されます。このセクションのコマンドを実行するには、**Cisco TAC** に連絡して一時的なルートシェルアクセスを要求してください。

1. システムでそのユーザーが作成されているかどうかを確認するには、次のコマンドを入力します。

```
magctl user display <username>
```

このコマンドは、パスワードをリセットするために使用できるテナント名を返します。出力は次のようになります。

```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```

2. パスワードをリセットするには、次のコマンドとテナント名を入力します。

```
magctl user password update <username> <tenant-name>
```

新しいパスワードを入力するように求められます。

3. 新しいパスワードを入力します。

確認のために新しいパスワードを再入力するよう求められます。

4. 新しいパスワードを入力します。

パスワードがリセットされ、新しいパスワードを使用して **Catalyst Center** にログインできます。

特定の **Catalyst Center** 機能へのユーザーアクセスを許可または制限するカスタムロールを定義する、ロールベースのアクセス制御の設定に関する情報。

Catalyst Center は、ロールベース アクセス コントロール (RBAC) をサポートしています。これにより、**SUPER-ADMIN-ROLE** 権限を持つユーザーは、特定の **Catalyst Center** 機能とサイトへのユーザーアクセスを許可または制限するカスタムロールを定義できます。

カスタムロールを定義し、定義したロールにユーザーを割り当てます。

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。

1. カスタムロールを定義します。

- a) メインメニューから次を選択します。[**System**] > [**Users & Roles**] > [**Role Based Access Control**] の順に選択します。
- b) [**Create a New Role**] をクリックします。
- c) タスクの概要ウィンドウが開いたら、[**Let's do it**] をクリックして、ワークフローに直接移動します。
- d) [**Create a New Role**] ウィンドウでロール名を入力します。次に、[**Next**] をクリックします。
- e) [**Define the Access**] ウィンドウで目的の機能に対応する [>] アイコンをクリックして、関連付けられている機能を表示します。
- f) それぞれの機能の権限レベルを必要に応じて [**Deny**]、[**Read**]、または [**Write**] に設定します。[**Next**] をクリックします。

機能の権限レベルを [**Deny**] に設定すると、このロールを割り当てられたユーザーは該当する機能を GUI で表示できなくなります。

依存機能については、推奨される権限レベルの設定を上書きすると、依存機能の権限レベル違反を示す警告メッセージが [**Summary**] ウィンドウに表示されます。

- g) 構成設定を確認します。変更するには、[**Edit**] をクリックします。
- h) [**Create Role**] をクリックします。

2. 作成したカスタムロールにユーザーを割り当てるには、[**Users & Roles**] > [**User Management**] に移動します。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。
 - a. [**User Management**] ウィンドウで、カスタムロールを割り当てるユーザーに対応するオプションボタンをクリックし、次に [**Edit**] をクリックします。
 - b. [**Update Internal User**] スライドインペインで、[**Roles**] ドロップダウンリストをクリックし、カスタムロールを選択します。
 - c. [**Save**] をクリックします。
- 新規ユーザーにカスタムロールを割り当てるには、次の手順を実行します。
 - a. [**User Management**] ウィンドウで、[**Add**] をクリックします。

- b. **[Create Internal User]** スライドインペインで、姓、名、およびユーザー名を入力します。
 - c. **[Role]** ドロップダウンリストからカスタムロールを選択します。
 - d. 新しいパスワードを入力し、確認のために再度入力します。
 - e. **[Save]** をクリックします。
3. 管理者がアクセス権限を更新している間にログインしていた場合は、**Catalyst Center** からログアウトします。その後、再度ログインして新しい権限を適用します。

Catalyst Center

Catalyst Center でのユーザーロール権限を一覧表示します。

6 : Catalyst Center

機能	説明	依存機能の推奨権限設定
アシュアランス	ネットワークのあらゆる側面を完全に可視化して一貫したサービスレベルを維持できます。	–
モニタリング	問題のトラブルシューティングと修復、プロアクティブなネットワークモニタリング、および AI ネットワーク分析 から得られるインサイトにより、ネットワークの正常性のモニタリングと管理を行います。 このロールでは次のことが可能です。 - 問題の解決、クローズ、無視。 - 機械推論エンジン（MRE）のワークフローの実行。 - トレンドとインサイトの分析。 - パストレース、センサーダッシュボード、不正管理などの問題のトラブルシューティング。 - 不正および Cisco Advanced Wireless Intrusion Prevention System（aWIPS）のワークフローの実行。これらのワークフローには、AP 許可リスト、ベンダー許可リスト、aWIPS プロファイルの作成、aWIPS プロファイルの割り当てなどが含まれます。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Read] • [Utilities] > [Machine Reasoner] : [Read] • [Utilities] > [Reports] : [Read] • [Utilities] > [App Hosting] : [Read] • [Utilities] > [Command Runner] : [Read]
設定	問題の設定と管理を行います。ネットワーク、クライアント、およびアプリケーションの正常性のしきい値を更新します。	• [Assurance] > [Monitoring] : [Read] • [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Utilities] > [App Hosting] : [Read]

機能	説明	依存機能の推奨権限設定
トラブルシューティング	センサーテストの作成と管理を行います。クライアントのトラブルシューティングのためのオンデマンドのフォレンジック パケットキャプチャ（インテリジェントキャプチャ）をスケジュールします。	• [Assurance] > [Monitoring] : [Read] • [Assurance] > [Troubleshooting] : [Write] • [Network Provision] > [Device Provision] : [Write] • [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Read] • [Utilities] > [Machine Reasoner] : [Read] • [Utilities] > [App Hosting] : [Read] • [Utilities] > [Command Runner] : [Read]

機能	説明	依存機能の推奨権限設定
拡張機能	アクセス可能なインテントベースのワークフロー、データ交換、通知、およびサードパーティ製アプリケーションの統合に使用できるオープンなプラットフォーム。  注 この権限を [Read] や [Write] に設定している場合、サイト範囲内にある（非グローバル）アクセスグループに割り当てることはできません。	
イベントサブスクリプション	ネットワークおよびシステムイベントのほぼリアルタイムの通知を登録します。修正措置を開始します。  注 ITSM が設定の可視性と制御と統合されている場合は、この権限を [Write] に設定する必要があります。	• [System] > [System Settings] : [Read]
ITSM	ITSM 統合用の事前設定済みバンドルを設定してアクティブ化します。  注 この権限を [Read] や [Write] に設定している場合、サイト範囲内にある（非グローバル）アクセスグループに割り当てることはできません。	• [Extensions] > [Intent API] : [Write]
インテント API	REST API を介して製品にアクセスします。	
ネットワーク設計	ネットワークプロファイルと設定を構成します。テンプレートを管理します。ソフトウェアイメージリポジトリを更新します。サイトおよびネットワークデバイスを管理するためのワイヤレスマップを設定します。	
プロファイルと設定	AAA、NTP、DHCP などのサイト全体のネットワーク設定を管理します。テレメトリとプロファイルを管理します。	• [Network Management] > [Hierarchy] : [Read]

機能	説明	依存機能の推奨権限設定
ワイヤレスマップ	ワイヤレスネットワークを可視化して、ワイヤレスマップを設定します。	• [Network Management] > [Hierarchy] : [Write] • [Network Management] > [Inventory] : [Write] • [Network Design] > [Profiles and Settings] : [Write] • [Assurance] > [Monitoring] : [Read]
ネットワーク管理	ネットワークを検出して構築します。	–
検出	ネットワーク上の新しいデバイスを検出します。	• [Network Management] > [Hierarchy] : [Write] • [Network Management] > [Inventory] : [Write] • [Network Design] > [Profiles and Settings] : [Read]
階層	地理的な場所に基づいてエリア、ビルディング、フロアのネットワーク階層を作成します。このロールには、CMXサーバーの設定も含まれます。	–
インベントリ	ネットワーク上のデバイスを追加、更新、または削除します。デバイス属性を管理し、ネットワークトポロジと設定を表示および管理します。	• [Network Management] > [Hierarchy] : [Read] • [Network Design] > [Profiles and Settings] : [Read]
ライセンス	ソフトウェア資産やネットワーク資産のライセンス使用状況とコンプライアンスに関する情報を管理します。	• [Assurance] > [Monitoring] : [Read]
ネットワーク全体の設定	ネットワーク全体の設定を構成して、ネットワークとデバイスをモニタリングします。	–
 注 この権限セットを [Read] や [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。		
ネットワーク運用	ネットワークデバイスを管理およびメンテナンスします。	–

機能	説明	依存機能の推奨権限設定
コンプライアンス	デバイスのコンプライアンスとアウトオブバンドの変更をモニタリングします。 Cisco Field Notice を管理し、 EoX ステータスを表示します。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Network-wide Settings] : [Read] • [Security] > [Security Advisory] : [Read] • [Network Operations] > [SWIM] : [Read]
LAN の自動化	LAN 自動化によるネットワークのプロビジョニング。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Network-wide Settings] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Read]
プラグアンドプレイ	新しいデバイスを自動的にオンボードしてサイトに割り当て、サイト固有の設定に基づいて設定します。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Network-wide Settings] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Read]
RMA	ネットワーク内の故障したデバイスを交換します。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [License] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Operations] > [Plug and Play] : [Write] • [Network Operations] > [SWIM] : [Write]
SWIM	ソフトウェアイメージを管理します。物理および仮想のネットワークエンティティを更新します。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read]
ネットワーク プロビジョニング	ネットワークデバイスの設定、アップグレード、プロビジョニング、および管理を行います。	–

機能	説明	依存機能の推奨権限設定
デバイスプロビジョニング	サイト固有の設定とネットワークに対して設定されたポリシーを使用してデバイスをプロビジョニングします。このロールには、アプリケーションポリシー、アプリケーションの可視性、クラウド、サイト間VPN、ネットワーク/アプリケーションテレメトリ、セキュリティサービスの挿入、Stealthwatch、および Cisco Umbrella プロビジョニングが含まれます。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Read] • [Network Design] > [Template] : [Write] • [Network Operations] > [Plug and Play] : [Write] • [Network Operations] > [Compliance] : [Read] • [Utilities] > [Command Runner] : [Write] • [System] > [System Settings] : [Read]

機能	説明	依存機能の推奨権限設定
ネットワーク全体の設定	仮想ネットワーク、エクストラネットポリシー、およびその他のネットワーク全体の設定を管理します。	
	 注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
SD-Access	SD-Access ファブリックを設定、管理、およびモニタリングします。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Management] > [Discovery] : [Read] • [Network Management] > [Network-wide Settings] : [Read] • [Network Provision] > [Device Provision] : [Write] • [Network Design] > [Template] : [Write] • [Network Operations] > [Plug and Play] : [Write] • [Network Operations] > [Network-wide Config] : [Read] • [Policy] > [Group-based Policy] : [Read] • [Network Operations] > [LAN Automation] : [Read] • [Network Operations] > [SWIM] : [Read] • [Network Operations] > [Compliance] : [Read] • [Network Design] > [Profiles and Settings] : [Read] • [Utilities] > [Event Viewer] : [Read]

機能	説明	依存機能の推奨権限設定
ポリシー	組織のビジネスインテントを反映するポリシーを設定して管理します。	
	 注 この権限セットを [Read] や [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
アプリケーションポリシー	QoS ポリシーを管理して、ネットワークリソースを効率的に使用します。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Read] • [Network Operations] > [Compliance] : [Read] • [Utilities] > [Command Runner] : [Write] • [System] > [System Settings] : [Read]

機能	説明	依存機能の推奨権限設定
グループベースポリシー	ネットワークのセグメンテーションとアクセス制御を適用するグループベースポリシーを管理します。	
	 注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
IP ベースのアクセス制御	ネットワークのセグメンテーションを適用する IP ベースのアクセス制御リストを管理します。	
	 注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
セキュリティ	ネットワークへのセキュアなアクセスを管理および制御します。	
監査ログ	UI または API を介して、システム、ネットワークデバイス、および設定に加えられた変更のログを表示します。	
不正および aWIPS	ネットワークの不正および aWIPS 脅威をモニタリングします。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Provision] > [Device Provision] : [Write] • [Assurance] > [Monitoring] : [Read] • [Assurance] > [Troubleshooting] : [Read] • [Network Design] > [Profiles and Settings] : [Write] • [Security] > [Audit Log] : [Write] • [System] > [System Settings] : [Read] • [Utilities] > [Reports] : [Write]

機能	説明	依存機能の推奨権限設定
セキュリティアドバイザリ	ネットワークをスキャンして、シスコのセキュリティアドバイザリを検索します。公開されているセキュリティアドバイザリでネットワークに影響する可能性がある情報を確認できます。  注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read]
Stealthwatch	暗号化されたトラフィックに含まれる脅威も検出して軽減できるようにするために、ネットワーク要素から Cisco Stealthwatch にデータを送信するように設定します。  注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	• [Network Management] > [Hierarchy] : [Read] • [Network Management] > [Inventory] : [Read] • [Network Design] > [Profiles and Settings] : [Write] • [Network Provision] > [Device Provision] : [Write] • [System] > [System Settings] : [Read] • [System] > [System Administration] : [Read]
Umbrella	サイバーセキュリティの脅威に対する最前線の防御策として、ネットワーク要素で Cisco Umbrella を使用するように設定します。  注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
システム	設定管理、ネットワーク接続、ソフトウェアアップグレードなどの一元管理を実行します。	

機能	説明	依存機能の推奨権限設定
システム管理	HA、ディザスタリカバリ、バックアップおよび復元など、コアシステムの管理機能を管理します。	• [System] > [System Settings] : [Write]
	 注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
システム設定	コアシステムの接続設定を管理します。このロールには、整合性検証、統合設定、デバッグログ、テレメトリ収集、システムの EULA、IPAM、データプラットフォーム、シスコのクレデンシャル、スマートアカウント、スマートライセンス、SSM 接続モード、デバイスの EULAが含まれます。 このロールには、証明書管理に関連する権限も含まれています。 このロールを使用すると、マシン推論ナレッジベースを自動更新する設定が有効になります。	
	 注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
ユーティリティ	ネットワークの管理に役立つ共通のユーティリティを使用します。	
アプリケーションホスティング	デバイスで実行される仮想化されたコンテナベースのアプリケーションを展開、管理、およびモニタリングします。	

機能	説明	依存機能の推奨権限設定
Bonjour	ネットワーク全体でポリシーベースのサービス検出を有効にするために、Wide-Area Bonjour サービスを使用します。  注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
コマンドランナー	デバイスの実行コンフィギュレーションを表示します。	• [Network Management] > [Inventory] : [Read]
イベントビューア	トラブルシューティングのためにデバイスおよびクライアントイベントを表示します。	

機能	説明	依存機能の推奨権限設定
機械推論	シスコが既知の不具合やバグを検出するためにネットワークをスキャンし、ワークフローを使用してネットワーク上のさまざまな問題をトラブルシューティングします。  注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	• [Network Management] > [Inventory] : [Read] • [Network Management] > [Hierarchy] : [Read]
リモートデバイスのサポート	シスコのサポート担当者が管理対象ネットワークデバイスをリモートでトラブルシューティングできるようにします。  注 この権限セットを [Write] に設定している場合、サイト範囲内（非グローバル）アクセスグループに割り当てることはできません。	
レポート	事前定義されたレポートテンプレートを使用して、ネットワークのあらゆる分野についてのレポートを生成します。	

ロールベース アクセス コントロール統計の表示に関する情報。

各ユーザーロールに属しているユーザーの数を示す統計を表示できます。ドリルダウンして、選択したロールを持つユーザーのリストを表示することもできます。

1. メインメニューから次を選択します。 **[System] > [Users & Roles] > [Role Based Access Control]** の順に選択します。
デフォルトのすべてのユーザーロールとカスタムロールが表示されます。
2. 各ユーザーロールに対応する番号をクリックすると、そのロールを持つユーザーのリストが表示されます。

特定のネットワークサイトにユーザーアクセスを制限するアクセスグループを定義する方法について説明します。

Catalyst Center は、サイトベースのロールベースアクセスコントロール (SRBAC) をサポートします。SRBAC を使用すると、特定のネットワークサイトへのアクセスを制限するアクセスグループを作成できます。アクセスグループはロールとサイトの組み合わせです。サイトはグローバルサイトまたは特定のサイトのいずれかです。いつでも 1 つの特定のアクセスグループにログインできます。

Catalyst Center は、次のデフォルトアクセスグループをサポートしています。

- [NW-ADMIN_Global] : NW-ADMIN ロールへのグローバルアクセス用のアクセスグループ
- [OBSERVER_Global] : OBSERVER ロールへのグローバルアクセス用のアクセスグループ
- [SUPER-ADMIN_Global] : SUPER-ADMIN ロールへのグローバルアクセス用のアクセスグループ

この手順を使用して、アクセスグループを定義し、そのアクセスグループにユーザーを割り当てます。ユーザーに複数のアクセスグループを割り当てることもできます。

1. アクセスグループを定義します。

- メインメニューから次を選択します。[**System > Users & Roles > Access Group**]
- [**Create Access Group**] をクリックして、新しいアクセスグループを作成します。
- [**Create Your Access Group**] ウィンドウで、次の情報を入力します。

- [**Name**] : アクセスグループの一意の名前を入力します。
- [**Role**] : 利用可能リストからロールを選択します。
- [**Scope**] : サイト階層を選択します。

注

外部ユーザーは、グローバル範囲を持つデフォルトのアクセスグループにマッピングされます。このオプションは、外部ユーザーには適用されません。

- [**Next**] をクリックし、[**Summary**] ウィンドウでアクセスグループの構成を確認します。
- [**Create Access Group**] をクリックします。

成功メッセージで、[**Back to Access Group**] リンクをクリックして、[**Access Group**] ウィンドウに新しく作成されたアクセスグループを表示します。

- アクセスグループを編集するには、アクセスグループを選択して、[**Edit Access Group**] をクリックします。

アクセスグループのスライドインペインで、ロールまたはサイト階層を編集し、[**Save**] をクリックします。

2. 作成したアクセスグループにユーザーを割り当てるには、[**Users & Roles > User Management**] に移動します。

- 既存のユーザーにアクセスグループを割り当てるには、次の手順を実行します。

- a. **[User Management]** ウィンドウで、アクセスグループを割り当てるユーザーに対応するオプションボタンをクリックし、次に **[Edit]** をクリックします。
 - b. **[Update Internal User]** スライドインペインで、**[Access Group]** ドロップダウンリストをクリックし、アクセスグループを選択します。
 - c. **[Save]** をクリックします。
- アクセスグループを新しいユーザーに割り当てるには、次の手順を実行します。
 - a. **[User Management]** ウィンドウで、**[Add]** をクリックします。
 - b. **[Create Internal User]** スライドインペインで、姓、名、およびユーザー名を入力します。
 - c. **[Access Group]** ドロップダウンリストで、アクセスグループを選択します。
 - d. 新しいパスワードを入力し、確認のために再度入力します。
 - e. **[Save]** をクリックします。

3 つの異なるアクセスグループを作成し、それらを新しい内部ユーザーに割り当てる方法を示します。

このサンプルユースケースでは、3 つの異なるアクセスグループを作成し、それらを新しい内部ユーザー *User1* に割り当てる方法を示します。

ユーザー名		アクセスグループ	
User1		AG1、AG2、AG3	

アクセスグループ	ロール	範囲	説明
AG1	Custom-role1	グローバル	ロール Custom-role1 へのグローバルアクセスを許可します。
AG2	Custom-role2	IN-BGL	バンガロールサイトのロール Custom-role2 へのアクセスを許可します。
AG3	Custom-role3	US-SJ	サンノゼサイトのロール Custom-role3 へのアクセスを許可します。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

1. カスタムロール *Custom-role1*、*Custom-role2*、*Custom-role3* を定義します。
 - a) メインメニューから次を選択します。 **[System] > [Users & Roles] > [Role Based Access Control]** の順に選択します。
 - b) **[Create a New Role]** をクリックします。

- c) タスクの概要ウィンドウが開いたら、**[Let's do it]** をクリックして、ワークフローに直接移動します。
- d) **[Create a New Role]** ウィンドウでロール名を入力し、**[Next]** をクリックします。
- e) **[Define the Access]** ウィンドウで目的の機能に対応する **[>]** アイコンをクリックして、関連付けられている機能を表示します。
- f) それぞれの機能の権限レベルを必要に応じて **[Deny]**、**[Read]**、または **[Write]** に設定します。**[Next]** をクリックします。

機能の権限レベルを **[Deny]** に設定すると、このロールを割り当てられたユーザーは該当する機能を GUI で表示できなくなります。

依存機能については、推奨される権限レベル設定を上書きすると、違反を示す警告メッセージが **[Summary]** ウィンドウに表示されます。

- g) 構成設定を確認します。変更するには、**[Edit]** をクリックします。
- h) **[Create Role]** をクリックします。

2. アクセスグループ AG1、AG2、および AG3 を定義します。

- a) メインメニューから次を選択します。 **[System > Users & Roles > Access Group]**。
- b) **[Create Access Group]** をクリックして、新しいアクセスグループを作成します。
- c) **[Create Your Access Group]** ウィンドウで、次の情報を入力します。

- **[Name]** : アクセスグループの一意の名前を入力します。
- **[Role]** : 利用可能リストからロールを選択します。
- **[Scope]** : サイト階層を選択します。

- d) **[Next]** をクリックし、**[Summary]** ウィンドウでアクセスグループの構成を確認します。
- e) **[Create Access Group]** をクリックします。

成功メッセージで、**[Back to Access Group]** リンクをクリックして、**[Access Group]** ウィンドウに新しく作成されたアクセスグループを表示します。

- f) アクセスグループを編集するには、アクセスグループを選択して、**[Edit Access Group]** をクリックします。

アクセスグループのスライドインペインで、ロールまたはサイト階層を編集し、**[Save]** をクリックします。

3. アクセスグループ AG1、AG2、AG3 を新しいユーザー User1 に割り当てます。

- a) **[Users & Roles > User Management]** に移動します。
- b) **[User Management]** ウィンドウで、**[Add]** をクリックします。
- c) **[Create Internal User]** スライドインペインで、姓、名、およびユーザー名を入力します。
- d) **[Access Group]** ドロップダウンリストから、アクセスグループを選択します。
- e) 新しいパスワードを入力し、確認のために再度入力します。
- f) **[Save]** をクリックします。

3 つのアクセスグループを作成し、外部ユーザーに割り当てる方法を示します。

このサンプルユースケースでは、3 つのアクセスグループを作成し、Cisco ISE で作成された外部ユーザー *User-ise* に割り当てる方法を示します。

ユーザー名		アクセスグループ	
User-ise		AG4、AG5、AG6	

アクセスグループ	ロール	範囲	説明
AG4	Custom-role4	グローバル	ロール Custom-role4 へのグローバルアクセスを許可します。
AG5	Custom-role5	IN-BGL	ロール Custom-role5 へのバンガロールサイトのアクセスを許可します。
AG6	Custom-role6	US-SJ	ロール Custom-role6 へのサンノゼサイトのアクセスを許可します。

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

1. カスタムロール *custom-role4*、*custom-role5*、および *custom-role6* を定義します。

- メインメニューから次を選択します。[**System**] > [**Users & Roles**] > [**Role Based Access Control**] の順に選択します。
- [**Create a New Role**] をクリックします。
- タスクの概要ウィンドウが開いたら、[**Let's do it**] をクリックして、ワークフローに直接移動します。
- [**Create a New Role**] ウィンドウでロール名を入力し、[**Next**] をクリックします。
- [**Define the Access**] ウィンドウで目的の機能に対応する [>] アイコンをクリックして、関連付けられている機能を表示します。
- 目的の機能の権限レベルを [**Deny**]、[**Read**]、または [**Write**] に設定し、[**Next**] をクリックします。
 機能の権限レベルを [**Deny**] に設定すると、このロールを割り当てられたユーザーは該当する機能を GUI で表示できなくなります。
 依存機能については、推奨される権限レベルを上書きすると、警告メッセージが [**Summary**] ウィンドウに表示されます。
- 構成設定を確認します。変更するには、[**Edit**] をクリックします。
- [**Create Role**] をクリックします。

2. アクセスグループ *AG4*、*AG5*、および *AG6* を定義します。

- メインメニューから次を選択します。[**System** > **Users & Roles** > **Access Group**]
- [**Create Access Group**] をクリックして、新しいアクセスグループを作成します。
- [**Create Your Access Group**] ウィンドウで、次の情報を入力します。
 - [**Name**] : アクセスグループの一意の名前を入力します。
 - [**Role**] : 利用可能リストからロールを選択します。
 - [**Scope**] : サイト階層を選択します。
- [**Next**] をクリックし、[**Summary**] ウィンドウでアクセスグループの構成を確認します。
- [**Create Access Group**] をクリックします。

成功メッセージで、**[Back to Access Group]** リンクをクリックして、**[Access Group]** ウィンドウに新しく作成されたアクセスグループを表示します。

- f) アクセスグループを編集するには、アクセスグループを選択して、**[Edit Access Group]** をクリックします。

アクセスグループのスライドインペインで、ロールまたはサイト階層を編集し、**[Save]** をクリックします。

3. Cisco ISE サーバーでアクセスグループ **AG4**、**AG5**、および **AG6** を定義し、そのアクセスグループを外部ユーザー **User-ise** に割り当てます。

詳細については、[外部認証の設定](#)（192ページ）を参照してください。

Catalyst Center SRBAC

SRBACに基づく Catalyst Center 機能の動作

Catalyst Center の機能の動作は、アクセスグループで指定されたユーザーロールとサイトによって異なります。

次の表では、SRBACが Catalyst Center 機能に与える影響を示します。

7 : SRBAC Catalyst Center

機能	SRBAC の影響
検出	[Discovery job] • サイトユーザーがディスカバリ ジョブを作成すると、そのユーザーのアクセスグループと親サイト階層アクセスグループのユーザーのみにそのジョブを表示できます。 • 親サイト階層ユーザーは、子サイト階層ユーザーによって最初に作成されたディスカバリ ジョブを再実行できます。 • 検出されたデバイスは、検出を開始したユーザーがアクセス可能なデバイスに限定されます。

注

アクセスグループサイト階層が異なるため、2 人のユーザーが実行するとディスカバリ ジョブの結果が異なる場合があります。

[Global credentials]

- サイト管理者によって作成されたログイン情報には、すべてのサイトユーザーが読み取り専用モードでアクセスできます。
- ログイン情報を編集または削除できるのは、書き込みアクセス権を持つ作成者、または同じ階層内のスーパーユーザーに限られます。

機能	SRBAC の影響
設備一覧	デバイスの追加 ● サイトユーザーによって追加されたデバイスは、サイトユーザーのアクセスグループとその親サイト階層アクセスグループのユーザーにのみ表示されます。 ● 親サイト階層アクセスグループを持つユーザーによって追加されたデバイスは、子サイト階層アクセスグループのユーザーに表示されません。 ● 子サイト階層ユーザーがすでに存在するデバイスを再追加またはインポートしようとする、そのデバイスが存在することを示すエラーが表示されます。ただし、子サイト階層ユーザーは引き続きインベントリ内のデバイスを表示できません。 [EoX Status] ● [Network Operations > Compliance] への書き込み権限を持つサイトユーザーがスキャンを開始できます。 ● サイトユーザーが EoX スキャンをスケジュールすると、そのサイトに関連するデバイスがスキャンされます。[Inventory] ページには、そのサイトに関連するデバイスの EoX ステータスのみが表示されます。 ● サイトユーザーの場合、Catalyst Center ホームページの EoX ステータスタイルには、ユーザーに関連付けられているサイトのスキャンの概要が表示されます。
トポロジ	[Shared custom view layouts] ● 下位レベルのアクセスグループのユーザーがカスタムビューを作成すると、上位レベルのアクセスグループのユーザーはそれらのビューにアクセスできます。ただし、下位レベルのアクセスグループのユーザーは、上位レベルのアクセスグループのユーザーによって作成されたビューにアクセスできません。 ● ユーザーは、自分のアクセスグループに関連付けられているデバイスとサイト階層のみを表示できます。

機能	SRBAC の影響	
プラグ アンド プレイ	[Method of adding device] プラグアンドプレイ接続の検出 プラグアンドプレイを使用したデバイスの手動追加 Cisco スマートアカウントからのデバイスの追加 [Claim device to a site] • プラグアンドプレイでデバイスがサイトに対して要求されると、その特定のサイト階層とその親サイト階層のアクセスグループユーザーに表示されます。 • デバイスのプラグアンドプレイ履歴は、デバイスの以前のアクセスグループに関係なく、サイトアクセスグループのすべてのユーザーに表示されます。 • デバイスに関連付けられているすべての関連プラグアンドプレイワークフローは、デバイスが要求された特定のサイト階層に割り当てられます。 プラグアンドプレイを介してデバイスがオンボーディングされ、インベントリに追加された後、デバイスが別のサイトに割り当てられている場合、プラグアンドプレイのデバイスレコードは新しいサイトの siteHierarchyId で更新され、新しいサイトのアクセスグループユーザーに表示されます。	[Visibility rules] 最初はすべてのユーザーに表示されます。 サイトに要求した後、検出されたデバイスはアクセスグループユーザーと親サイト階層アクセスグループユーザーにのみ表示されます。 アクセスグループユーザーと親サイト階層アクセスグループユーザーにのみ表示されます。 デバイスを追加したアクセスグループユーザーと親サイト階層アクセスグループユーザーにのみ表示されます。
RMA とネットワークの更新	• アクセスグループに関連付けられているユーザーは、交換または更新のために、現在のアクセスグループまたは下位レベルのアクセスグループに属しているデバイスをマークまたは解除できます。 • ファブリックデバイスを障害としてマークするには、ユーザーがそのすべてのネイバーデバイスにアクセスする必要があります。 • ユーザーがデバイスを交換または更新対象としてマークすると、現在または上位レベルのアクセスグループのユーザーが交換用ワークフローをトリガーできます。 • アクセスグループに関連付けられているユーザーは、ワークフローをスケジュールできます。上位レベルのアクセスグループのユーザーは、ワークフローを変更またはキャンセルできます。	

機能	SRBAC の影響
タギング	サイトユーザーによって作成されたタグは、他のすべてのサイトユーザーに表示されます。ただし、名前の変更やダイナミックルールの変更などのタグの編集は、タグを作成したアクセスグループのユーザーのみが実行できます。
ライセンス	読み取り/書き込みアクセスがある場合、サイトスコープ（非グローバル）アクセスグループに「ライセンス」および「システム設定」権限セットを割り当てることはできません。サイトスコープユーザーは、ライセンスまたはシステム設定ページを表示できません。
ネットワーク設定	● サイトプロファイルは、作成元のアクセスグループでのみ編集または削除できます。ただし、システム内の任意のサイトを任意のプロファイルに割り当てることができます。 ● AAA および ISE サーバーの設定はグローバルリソースです。グローバルサイトアクセスグループを持つユーザーのみが、これらの設定を作成、編集、または削除できます。 ● SSID や RF プロファイルなどのすべてのワイヤレス設定はグローバルであり、グローバルサイトアクセスグループを持つユーザーのみが作成できます。さらに、特定のサイトにアクセスできるユーザーは、そのサイトの設定を上書きできます。 ● 特定のサイトのアクセスグループを持つユーザーは、その特定のサイトの設定を上書きできます。
ワイヤレスコントローラのプロビジョニング	[Managed AP Location] ● サイトユーザーは、アクセスグループに関連付けられているサイトに基いて、管理対象 AP の場所を選択できます。 ● Catalyst Center では、ワイヤレスコントローラの場所と管理対象 AP の場所の両方のアクセス可能性を検証します。 ● 複数の管理対象 AP ロケーションを持つワイヤレスコントローラをプロビジョニングするには、ユーザーはすべての管理対象 AP ロケーションの親サイトにアクセスする必要があります。 たとえば、ネットワーク階層に Area1（親サイト）と Sub-area1 および Sub-area2（子サイト）が含まれている場合、Sub-area1 および Sub-area2 で AP を管理しているワイヤレスコントローラをプロビジョニングするには、ユーザーが Area1 にアクセスする必要があります。 サイトユーザーが Sub-area1 または Sub-area2 のみにアクセスできる場合、プロビジョニングは失敗します。

機能	SRBAC の影響
AP のプロビジョニング	• アクセスグループのユーザーは、アクセスグループに関連付けられたサイトに AP をプロビジョニングできます。 • AP のプロビジョニングは、関連付けられたコントローラの物理および管理対象 AP の場所へのユーザーアクセスに基づいて許可されます。 • ユーザーは、AP に関連付けられたコントローラとその管理対象の場所にアクセスする必要があります。 • ユーザーは、AP のセカンダリコントローラとその管理対象場所にアクセスする必要があります。
証明書	証明書は特定のサイトまたはアクセスグループに関連付けられます。アクセスグループユーザーは、アクセスグループに関連付けられているサイトに割り当てられたデバイスの証明書のみを表示できます。

機能	SRBAC の影響
不正および aWIPS	● グローバルサイトにアクセスするユーザーは、[Rogue Overview] ダッシュボードで不正および aWIPS 機能を有効または無効にできます。 ● [Overview] ダッシュボードの [Threats] テーブルには、現在ログインしているユーザーが所有しているサイトにある AP によって強力に検出された不正のみが表示されます。テーブル内の検出対象 AP サイトは、ユーザーが所有するサイトのいずれかである必要があります。 ● ワイヤレス不正封じ込め操作は、ユーザーがその不正に対して最も強力なワイヤレスコントローラにアクセスできる場合にのみ許可されます。 有線不正封じ込め操作は、不正が検出されたスイッチにユーザーがアクセスできる場合にのみ許可されます。 ● グローバルサイトにアクセスできるアクセスグループのユーザーは、許可リストから MAC アドレスを作成または削除できます。 ● ユーザーは、他のユーザーによって作成されたすべてのプロフィールを表示できます。ただし、ユーザーがサイトを編集、削除、または割り当てることは、プロフィールの一部であるすべてのサイトをユーザーが所有している場合にのみ可能です。ユーザーがプロフィールの一部であるすべてのサイトを所有していない場合、プロフィール名をクリックすると、読み取り専用の詳細が表示されます。

aWIPS プロファイルの設定

- 任意の管理者がプロフィールを作成できますが、自分が所有するサイトの下にあるデバイスにのみマッピングできます。
- マッピングされたプロフィールの編集または削除は、ユーザーがそのプロフィールにマッピングされているすべてのワイヤレスコントローラにアクセスできる場合にのみ許可されます。ユーザーがいずれかのデバイスにプロフィールをマッピングし、後でデバイスがユーザーにアクセス権がない別のサイトに移動した場合、ユーザーはそのプロフィールを編集または削除できません。
- プロファイル割り当て画面では、現在のユーザーがアクセス可能なデバイスのみが表示されます。

機能	SRBAC の影響
SD-Access	REP サイトユーザーによって作成された REP リングは、次の場所に表示されます。 • サイトユーザーのアクセスグループに含まれるユーザー。 • 親サイトの階層アクセスグループに含まれるユーザー。 • サイト階層内のすべてのリングメンバーの最も近い共通の親であるアクセスグループ内のユーザー。 PRP • LAN-A ファブリックサイトと LAN-B ファブリックサイトの両方にアクセスできるユーザーは、PRP を設定および表示できます。 • LAN-A サイトにのみアクセスできるユーザーには、アクセスが制限されていることを示すバナーメッセージが表示されます。 MRP • すべてのリングメンバーにアクセスできるユーザーは、完全な MRP リングの詳細を表示できます。 • 部分的なリングメンバーにアクセスできるユーザーには、部分的なデータと、アクセスが制限されていることを示すバナーメッセージが表示されます。
フィールド 通知	• [Network Operations > Compliance] への書き込み権限を持つサイトユーザーがスキャンを開始できます。 • サイトユーザーがスキャンを開始すると、そのサイトに関連付けられているデバイスのみがスキャンされます。結果はサイト固有です。 • サイトユーザーの場合、Catalyst Center ホームページの [Field Notices] タイルには、そのユーザーに関連付けられている特定のサイトのスキャンサマリーが表示されます。
セキュリティ アドバイザリ	• [Security > Security Advisories] への書き込み権限を持つサイトユーザーがスキャンを開始できます。 • サイトユーザーがスキャンを開始すると、そのサイトに関連付けられているデバイスのみがスキャンされます。結果はサイト固有です。 • サイトユーザーは、他のサイトからのデータにさらされることなく、自分の場所に関連するセキュリティアドバイザリに対処できます。

機能	SRBAC の影響
ネットワークバグ ID	• [Network Reasoner] への書き込み権限を持つサイトユーザーがスキャンを開始できます。 • サイトユーザーがスキャンを開始すると、そのサイトに関連付けられているデバイスのみがスキャンされます。結果はサイト固有です。 • サマリーには、サイトユーザーによって管理されているデバイスに影響するバグのみが表示されます。
ネットワーク推論機能	• サイトユーザーは、割り当てられたサイトとロールに関連するワークフローにのみアクセスできます。 • サイトユーザーは、自分のサイトに割り当てられたデバイスとリソースのみを表示して操作できます。たとえば、CPU 使用率などのワークフローをトリガーする場合、サイトに割り当てられたデバイスのみが分析に使用できます。

外部ユーザーの認証と許可に外部サーバーを使用している場合の外部認証の設定に関する情報。

外部ユーザーの認証と許可に外部サーバーを使用するには、**Catalyst Center** で外部認証を有効にします。

- **SUPER-ADMIN-ROLE** 権限を持つユーザーのみがこの手順を実行することができます。詳細については、[ユーザ ロールについて](#) (162ページ) を参照してください。
- 少なくとも 1 つの認証サーバーを設定する必要があります。
- **SRBAC** の場合、**Cisco ISE** サーバーでアクセスグループを定義する必要があります。

Catalyst Center でロールを設定するのと同じように **Cisco ISE** サーバーを設定します。たとえば、`<AAA attribute name>=rds=<comma separated list of rd names>` のようになります。最初の **rd** は、デフォルトのアクセスグループのプロファイルとして処理できます。

 注

Catalyst Center が物理アプライアンスにデプロイされている場合は、このメモを確認してください。

外部認証が有効化されている場合：

- AAA サーバーに到達できない場合や AAA サーバーが不明なユーザー名を拒否した場合に、Catalyst Center がローカルユーザーにフォールバックすることはありません。
- ローカルフォールバックは、SUPER-ADMIN-ROLE 権限を持つユーザーに対してデフォルトで有効になっていて、無効にすることはできません。

外部認証フォールバックを再度有効にするには、Catalyst Center インスタンスに SSH 接続し、次の CLI コマンドを入力します。

```
magctl rbac external_auth_fallback enable
```

1. メインメニューから次を選択します。[System] > [Users & Roles] > [External Authentication] の順に選択します。
2. Catalyst Center で外部認証を有効にするには、[Enable External User] チェックボックスをオンにします。
3. オプション: AAA 属性を設定します。

TACACS 認証では、次の AAA 属性がサポートされています。

Catalyst Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

RADIUS 認証では、次の AAA 属性がサポートされています。

Catalyst Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

- a) [AAA Attribute] フィールドに、表で説明されているユースケースに適した属性を入力します。[AAA Attribute] フィールドのデフォルト値は Null です。
- b) [Update] をクリックします。

4. オプション: AAA サーバーを設定します。

これらの設定は、現在のプライマリ AAA サーバーとセカンダリ AAA サーバーを交換したり、異なる AAA サーバーを定義したりする場合にのみ行います。

メインメニューから次を選択します。[System] > [Settings] > [External Services] > [Authentication and Policy Servers]

- a) [Primary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。
- b) [Secondary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。
- c) オプション: Cisco ISE サーバーを使用している場合は、必要に応じて設定を更新できます。

Cisco ISE ポリシーの詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』の「Segmentation」を参照してください。

8 : Cisco ISE

名前	説明
Shared Secret	デバイス認証に使用されるキーです。共有秘密の長さは、最大 100 文字です。 AAA アドレスを更新する前に、共有秘密を指定します。
Username	Cisco ISE CLI にログインするために使用する名前。
Password	Cisco ISE CLI ユーザー名のパスワード。
FQDN	Cisco ISE サーバーの完全修飾ドメイン名 (FQDN)。FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。 <i>hostname.domainname.com</i> たとえば Cisco ISE サーバーの FQDN は、 ise.cisco.com である可能性があります。
Subscriber Name	一意のテキスト文字列 (acme など)。これは Catalyst Center から Cisco ISE への統合中に、Cisco ISE に新しい pxGrid クライアントを設定するために使用されます。
Virtual IP Address	Cisco ISE ポリシーサービスノード (PSN) が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

- d) オプション: 詳細設定を更新するには、[View Advanced Settings] をクリックして、必要に応じて設定を更新します。

9 : AAA

名前	説明
Protocol	TACACS または RADIUS。
Authentication Port	AAA サーバーへの認証メッセージのリレーに使用されるポート。 • RADIUS の場合、デフォルトは UDP ポート 1812 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Accounting Port	AAA サーバーへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。 • RADIUS の場合、デフォルトの UDP ポートは 1813 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Retries	Catalyst Center が Cisco ISE との接続を試行できる回数。

名前	説明
Timeout	Catalyst Center が Cisco ISE からの応答を待機する時間の長さ。タイムアウトの最大値は 60 秒です。

e) [Update] をクリックします。

二要素認証では、ユーザーの識別に、ユーザー名とパスワードに加えて ID 方式を使用します。

二要素認証（2FA）は、ユーザー名とパスワードに加えて識別子手法を要求することで、ユーザー認証のセキュリティを強化するものです。この識別子手法は通常、対象ユーザーだけが所持し（スマホアプリやキーフォブなど）、元のログイン方法とは別に保存されます。

二要素認証の **Catalyst Center** の実装では、トークンクライアント、トークンサーバー、および認証サーバーが使用されます。正しい PIN が入力されると、トークンクライアントは使い捨てのトークンコードを生成します。トークンサーバーはトークンコードを検証します。認証サーバーはユーザーアクセスを管理します。認証処理には、RADIUS または TACACS+ プロトコルが使用されます。

二要素認証の前提条件を一覧表示します。

Catalyst Center で使用する二要素認証を設定するには、次の前提条件を満たしている必要があります。

- 認証された **Catalyst Center** ユーザーの RBAC ロール認可を伝達する属性値ペアを返すことができる認証サーバー。たとえば、**Cisco Identity Services Engine (Cisco ISE) 2.3 パッチ 1** が使用されます。
- 認証サーバーと統合する二要素トークンサーバー。たとえば、**RSA Authentication Manager 7.2** などです。
- ソフトウェアトークンを生成するクライアントのマシン上のトークンカードアプリケーション。この例では、**RSA SecurID** ソフトウェアトークンを使用しています。

二要素認証のプロセスについて説明します。

このセクションでは、二要素認証が設定されている **Catalyst Center** アプライアンスにユーザーがログインしたときに発生するイベントのシーケンスについて説明します。

1. **RSA SecurID** トークンクライアントでは、ユーザーは PIN を入力してトークンコードを取得します。
2. **Catalyst Center** ログインページでは、ユーザー名とトークンコードを入力します。
3. **Catalyst Center** では、**Cisco ISE** へのログイン要求の送信に、RADIUS または TACACS+ プロトコルを使用します。
4. **Cisco ISE RSA Authentication Manager** サーバーに要求を送信します。
5. **RSA Authentication Manager** でトークンコードを検証し、ユーザーが正常に認証されたかどうかを **Cisco ISE** に通知します。
6. ユーザーが認証されている場合、**Cisco ISE** は認証されたユーザーと設定済みの許可プロファイルを照合します。その後、**role=NETWORK-ADMIN-ROLE** 属性値ペアを返します。

7. Catalyst Center ユーザーのロールベース アクセス コントロール (RBAC) ロールに関連付けられている機能およびページへのアクセス権を付与します。

Catalyst Center の二要素認証を設定する手順。

Catalyst Center アプライアンスで二要素認証を設定するには、次の手順を実行します。

1. RSA Authentication Manager を Cisco ISE と統合します。

- a) RSA Authentication Manager で、2つのユーザー、すなわち **cdnac_admin** (管理者ユーザーロール用) と **cdnac_observer** (オブザーバロール用) を作成します。

詳細については、RSA Self-Service Console Help の「Add a User to the Internal Database」のトピックを参照してください。このトピックにアクセスするには、次の手順を実行します。

1. [RSA Self-Service Console Help](#) を開きます。
2. [Search help] フィールドで、「Add a User To the Internal Database」と入力して、[Search help] をクリックします。

- b) 新しい認証エージェントを作成します。

詳細については、[RSA Self-Service Console Help](#) の「Add an Authentication Agent」のトピックを参照してください。

- c) 認証マネージャエージェント設定ファイル (sdconf.rec) を生成します。

1. RSA セキュリティコンソールで、[Access] > [Authentication Agents] > [Generate Configuration File] の順に選択します。

[Configure Agent Timeout And Retries] タブが開きます。

2. [Maximum Retries] と [Maximum Time Between Each Retry] フィールドについては、デフォルト値を使用します。

3. [Generate Configuration File] をクリックします。

[Download Configuration File] タブが開きます。

4. [Download Now] リンクをクリックします。

5. 画面に指示が表示されたら、[Save to Disk] をクリックして、zip ファイルのローカルコピーを保存します。

6. ファイルを解凍します。このバージョンの sdconf.rec ファイルを使用して、エージェントに現在インストールされているバージョンを上書きします。

- d) 前の手順で作成した **cdnac_admin** ユーザーと **cdnac_observer** ユーザーの PIN を生成します。

詳細については、[RSA Self-Service Console Help](#) の「Create My On-Demand Authentication PIN」のトピックを参照してください。

- e) Cisco ISE を開始するには、[Administration] > [Identity Management] > [External Identity Sources] > [RSA SecurID] の順に選択して、[Add] を選択します。

- f) [RSA SecurID Identity Sources] ページで、[Browse] をクリックし、ダウンロードした sdconf.rec ファイルを選択して、[Open] をクリックします。

- g) [Reauthenticate on Change PIN] チェックボックスをオンにして、[Submit] をクリックします。

2. 2つの許可プロファイルを作成します。1つはAdminユーザーロール用、もう1つはオブザーバユーザーロール用です。

a) Cisco ISE で、[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] を選択します。

b) 両方のプロファイルについて、次の情報を入力します。

- [Name] : プロファイル名を入力します。
- [Access Type] : [ACCESS_ACCEPT] を選択します。
- [Advanced Attributes Settings] 領域 : 最初のドロップダウンリストから [Cisco:cisco-av-pair] を選択します。

Admin ユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=NETWORK-ADMIN-ROLE] を選択します。

オブザーバユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=OBSERVER-ROLE] を選択します。

3. Catalyst Center アプライアンスの認証ポリシーを作成します。

『[Cisco Identity Services Engine Administrator Guide](#)』の「Configure Authentication Policies」のトピックを参照してください。

4. 2つの許可ポリシーを作成します。1つはAdminユーザーロール用、もう1つはオブザーバユーザーロール用です。

『[Cisco Identity Services Engine Administrator Guide](#)』の「Configure Authorization Policies」のトピックを参照してください。

5. RSA Authentication Manager セキュリティコンソールで、ソフトウェアトークンが両方のユーザーに割り当てられていることを確認します。

詳細については、[RSA Self-Service Console Help](#) の「View a Token」のトピックを参照してください。

注

トークンを割り当てる必要がある場合は、「Assign a Software Token to a User」のトピックで説明されている手順を実行します。

RADIUS

Cisco ISE サーバーが RADIUS 用に設定されている場合の二要素認証の有効化に関する情報。

RADIUS 用に設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

1. Cisco ISE と Catalyst Center を連動させます。

『[Catalyst Center Installation Guide](#)』の「Integrate Cisco ISE with Catalyst Center」を参照してください。

2. 認証に Cisco ISE サーバーを使用するよう Catalyst Center を設定します。

「[外部認証の設定](#)」を参照してください。

重要

Cisco ISE と Catalyst Center の両方に同じ共有秘密を指定していることを確認します。

TACACS+

TACACS+ 用に設定された Cisco ISE サーバーを使用した二要素認証の有効化に関する情報。

TACACS+ が設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

-
1. Cisco ISE で、**[Administration] > [Network Resources] > [Network Devices]** の順に選択すると、**[Network Devices]** ウィンドウが開きます。
 2. **[TACACS Authentication Settings]** をクリックして、その内容を表示します。以前に追加した Catalyst Center デバイスに対して共有秘密がすでに設定されていることを確認します。
 3. **[Work Centers] > [Device Administration] > [Policy Elements]** を選択すると、**[TACACS Profiles]** ウィンドウが開きます。
 4. **example_admin** および **example_observer** ユーザーロールの TACACS+ プロファイルを作成します。
 - a) **[Add]** をクリックします。
 - b) 次のタスクを完了します。
 - プロファイル名を入力します。
 - **[Raw View]** タブをクリックした後、**[Profile Attributes]** テキストボックスに次のテキストを入力します。
 - **example_admin** ユーザーロールの場合は、**Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE** と入力します。
 - **example_observer** ユーザーロールの場合は、**Cisco-AVPair=ROLE=OBSERVER-ROLE** と入力します。
 - c) **[Save]** をクリックします。
 5. Cisco ISE と Catalyst Center を連動させます。

『[Catalyst Center Installation Guide](#)』の「[Integrate Cisco ISE with Catalyst Center](#)」を参照してください。
 6. 認証に Cisco ISE サーバーを使用するよう Catalyst Center を設定します。

「[外部認証の設定](#)」を参照してください。

重要

Cisco ISE と Catalyst Center の両方に同じ共有秘密を指定していることを確認します。

二要素認証を使用した **Catalyst Center** へのログイン方法についての説明。

二要素認証を使用して **Catalyst Center** にログインするには、次の手順を実行します。

-
1. **Catalyst Center** のログインページで、適切なユーザー名を入力します。
 2. **RSA SecurID** トークンクライアントを開き、以前設定した **PIN** を入力して使い捨てトークンを生成します。
 3. このトークンをコピーします。コピーしたトークンを **Catalyst Center** のログインページの **[Password]** フィールドに貼り付けます。
 4. **[Log In]** をクリックします。
-

RADIUS または **TACACS** を使用して初めてログインした外部ユーザーを表示する方法についての情報。

RADIUS/TACACS を使用して初めてログインした外部ユーザーのリストを表示できます。表示される情報には、ユーザー名とロールが含まれます。

-
1. メインメニューから次を選択します。 **[System] > [Users & Roles] > [External Authentication]** の順に選択します。
 2. ウィンドウの下部までスクロールします。 **[External Users]** エリアに、外部のユーザーが一覧表示されます。

Cisco ISE ユーザーの場合、**Cisco ISE** には **RADIUS** 受け入れパケットの電子メールアドレスが含まれません。その結果、電子メールアドレスにドメインが表示されません。

章

- □□□□□□□□□□□□
- Cisco □□□□ □□□□□□□□
- □□□□□□□□□□
- Cisco □□□□□□□□ □□□□□□□□
□ □□□□□
- □□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□
- □□□□□□□□□□
- □□□□□□□□□□
- □□□□□□□□□□□□□□□□□□
□
- □□□□□□□□□□□□□□□□□□
□□□
- □□□□□□□□□□□□□□□□□□
□□□□□□
- □□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□
- □□□□□□□□□□ SLR □□□ PLR
□□□□□□
- □□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□
- CSSM □□□□□□□□□□□□□□□□□□
□□□
- □□□□□□ CSSM □□□□□□□□□□
□□□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□□□
□
- □□□□□□□□□□□□□□□□□□□□
□□□□□□
- □□□□□□□□□□□□□□

Catalyst Center でのライセンスの管理に関する情報。

Catalyst Center ライセンスマネージャに関する情報。

Catalyst Center ライセンスマネージャ機能は、スマートアカウントライセンスを含む、シスコ製品のすべてのライセンスの可視化と管理に役立ちます。

ライセンスマネージャにアクセスするには、メニューアイコンをクリックして次を選択します。**[Tools] > [License Manager]**の順に選択します。**[License Manager]** ウィンドウには、次の情報のタブが含まれています。

- **[Overview]** :

[Overview] タブには、選択したスマートアカウントと仮想アカウントに基づいて詳細が表示されます。

- **[Switch]** : すべてのスイッチのライセンスの購入情報と使用情報が表示されます。
- **[Router]** : 非統合ライセンスデバイスの使用数を示します。
- **[Wireless]** : すべてのワイヤレスコントローラとアクセスポイントについて、購入済みで使用中のライセンス情報が表示されます。
- **[ISE]** : Cisco Identity Services Engine (ISE) によって管理されているデバイスのライセンスの購入情報と使用情報が表示されます。

- **[Licenses]** : **[License Summary]** には、すべてのシスコデバイスにわたるすべてのタイプのライセンスについて、Cisco Smart Software Management (CSSM) から購入したライセンスの総数、期限切れ間近のライセンスの数、コンプライアンス違反の詳細が、CSSM から受信したとおり表示されます。

- **[Devices]** : **[Devices]** テーブルには、ライセンスタイプ、ライセンスの有効期限、ライセンスモード、仮想アカウント、関連サイト、および Catalyst Center による管理対象の各デバイスのスマートアカウント/バーチャルアカウントの登録ステータスが表示されます。

- **[Reporting]** : **[Smart License Compliance]** カードを使用すると、**[Smart License Compliance]** ワークフローを開始できます。

- **[Sync Status]** : リソース使用率測定 (RUM) 同期ステータスを表示します。

ライセンスを管理するには、各タブに一覧表示されているテーブルの上部にあるコントロールを使用できます。次の表は各コントロールについて説明したものです。

注

すべてのタブですべてのコントロールを使用できるわけではありません。

10 :

制御	説明
Filter	[Filter] をクリックして 1 つ以上のフィルタ値を指定し、 [Apply] をクリックします。複数のフィルタを適用することができます。フィルタを削除するには、対応するフィルタ値の横にある x アイコンをクリックします。

制御	説明
Change Cisco License	1 つ以上のライセンスを選択し、 [Actions] > [Change Cisco License] の順に選択して、選択したライセンスのレベルを Essentials または Advantage に変更します。このコントロールを使用してライセンスを削除することもできます。詳細については、 ライセンスレベルの変更 （211ページ）を参照してください。
Change Virtual Account	1 つ以上のライセンスを選択し、 [Actions] > [Change Virtual Account] の順に選択して、ライセンスの管理に使用されるバーチャルアカウントを指定します。
[Manage Smart License] > [Register]	スマートライセンスが有効になっているデバイスを 1 つ以上選択し、 [Actions] > [Manage Smart License] > [Register] の順に選択して、スマートライセンスが有効になっているデバイスを登録します。
[Manage Smart License] > [Deregister]	スマートライセンスが有効になっているデバイスを 1 つ以上選択し、 [Actions] > [Manage Smart License] > [Deregister] の順に選択して、スマートライセンスが有効になっているデバイスを登録解除します。
[Manage License Reservation] > [Enable License Reservation]	特定ライセンス予約（SLR）または永久ライセンス予約（PLR）を適用するデバイスを選択し、 [Actions] > [Manage License Reservation] > [Enable License Reservation] の順に選択します。
[Manage License Reservation] > [Update License Reservation]	デバイスが SLR 登録済みの状態である必要があります。 ワイヤレスデバイスまたはスイッチに適用されている SLR を、ワイヤレス コントローラ パッケージで更新できます。 SLR を更新するデバイスを選択し、[Actions] > [Manage License Reservation] > [Update License Reservation] の順に選択します。
[Manage License Reservation] > [Cancel/Return License Reservation]	デバイスを選択し、 [Actions] > [Manage License Reservation] > [Cancel/Return License Reservation] の順に選択して、デバイスに適用された SLR または PLR を取り消すか、返却します。
[Manage License Reservation] > [Factory License Reservation]	デバイスを選択し、 [Actions] > [Manage License Reservation] > [Factory License Reservation] の順に選択して、工場出荷時にデバイスにインストールされている SLR を有効にします。
Recent Tasks	[Recent Tasks] をクリックして、最近実行された 50 件すべての Catalyst Center タスクを表示します。ドロップダウンを使用してステータスが [Success] 、 [Failure] 、または [In Progress] のタスクのみを表示します。
License Usage	[License Usage] をクリックすると、すべてのタイプのライセンスについて、ライセンス使用率が表示されます。
Refresh	[Refresh] をクリックすると、現在のデータを使用してウィンドウがリロードされます。
Find	[Find] フィールドに検索用語を入力し、いずれかの列にその用語が含まれている、リスト内のライセンスをすべて検索します。検索文字列の任意の場所で、ワイルドカードとしてアスタリスク（*）を使用します。
[Show Records]	テーブルの各ページに表示するレコードの総数を選択します。

ライセンステーブルには、各デバイスに表示される情報が表示されます。すべての列はソートに対応しています。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

注

すべてのタブですべての列が使用されるわけではありません。また一部の列は、デフォルトの列ビュー設定で非表示になります。非表示の列を表示するには、歯車アイコンをクリックし、**[Edit Table Columns]**で、テーブルに表示する列を選択します。

11 :

カラム	説明
Device Type: Device Series	デバイスの製品シリーズの名前（例：Catalyst 3850 シリーズイーサネットスタックブルスイッチ）。詳細については、 ライセンス詳細の表示 （210ページ）を参照してください。
Device Type: Total Devices	Catalyst Center によってアクティブに管理されている、この製品シリーズのデバイスの総数。
Purchased Cisco Licenses	この製品シリーズのデバイスの購入済み Catalyst Center サブスクリプションライセンスの総数。
Purchased Licenses: Network/Legacy/OS	この製品シリーズのデバイスの購入済み永久ライセンスの総数。 • Network • Legacy • OS
Used Licenses	この製品シリーズのデバイスに適用された Catalyst Center サブスクリプションライセンスの総数。
Used Licenses: Network/Legacy/OS	この製品シリーズのデバイスの永久ライセンスの総数。 • Network • Legacy • OS
Feature Licenses (applicable only for Routers)	セキュリティ、AVC などの特定機能のために購入したライセンスの数。

12 :

カラム	説明
Device Name	デバイスの名前。詳細については、 ライセンス詳細の表示 （210ページ）を参照してください。
Device Family	スイッチやハブなど、Catalyst Center で定義されているデバイスのカテゴリ。

カラム	説明
IP Address	デバイスの IP アドレス。
Device Series	表示されているデバイスが属しているシスコ製品シリーズの正式名称 (例: Cisco Catalyst 3850 シリーズ イーサネット スタックブル スイッチ)。
Cisco License	Catalyst Center のライセンスレベル。
Cisco License Expiry	Catalyst Center ライセンスの有効期限。
License Mode	Catalyst Center のライセンスモード。
Device License	デバイスライセンスの種類。
Virtual Account	デバイスのライセンスを管理しているシスコバーチャルアカウントの名前。 バーチャルアカウントとサイト階層は別個のエンティティであり、相互接続されていません。 バーチャルアカウント名に /、\、= のいずれかの文字が含まれている場合、ライセンス操作が失敗する可能性があります。Cisco SSM ポータル (software.cisco.com) を使用してバーチャル アカウント名からこれらの文字を削除し、[License Manager Overview] ウィンドウから更新を実行することを推奨します。
Site	デバイスが設置されている Catalyst Center サイト。
Registration Status	デバイスの登録ステータス。
Authorization Status	デバイスの認証ステータス。
Reservation Status	デバイスの予約ステータス。
Last Updated Time	テーブル内のこのエントリが最後に更新された時刻。
MAC Address	ライセンスデバイスの MAC アドレス。
Term	Catalyst Center サブスクリプション ライセンスが有効である合計期間。
Days to Expiry	Catalyst Center ライセンス期間が期限切れになるまでの残りの日数。
Software Version	デバイスで現在実行されているネットワーク オペレーティング システムのバージョン。

Cisco

Catalyst Center は Cisco スマート アカウントと統合して、ライセンス管理を簡素化します。

スマートアカウントは、組織全体でシスコソフトウェアライセンスを管理するための、一元化された統合型のシンプルなソリューションを提供します。スマートアカウントは、すべてのシスコソフトウェア アセットを保持するコンテナとして機能するため、お客様は必要に応じてこれらのアセットを表示、保存、管理、および移動できます。スマートアカウントにより、ソフトウェア利用資格と使用状況が完全に可視化されるため、ソフトウェア管理の最適化が可能になります。スマートアカウントは、ライセンスのプール、ポータビリティをサポートしており、規則遵守レポートを提供します。

バーチャルアカウントは、スマートアカウント内でカスタマイズして利用できるサブアカウントで、シスコのライセンスをさらに整理し最適化するために使用されます。これらは、ビジネスユニット、製品タイプ、または地理的な場所を反映するように構造化でき、アセットのより適切な計画と利用が可能になります。

スマートアカウントが複数ある場合は、1つのアカウントがデフォルトに設定されます。ライセンスマネージャが登録やライセンスレベルの変更などの可視化およびライセンス操作に使用するデフォルトアカウントは、変更することができます。

各デバイスは、一度に1つのスマートアカウントとのみ同期できます。複数のスマートアカウントがある場合は、同期用にアカウントを選択する必要があります。選択したスマートアカウントは必要に応じて変更できます。ただし、デバイスに現在関連付けられているスマートアカウントを削除すると、同期プロセスは失敗します。

デフォルトのスマートアカウントを変更した後、CSSMからデータを取得し、[License Manager Overview] ウィンドウと [All License] ウィンドウに表示するまでに数分かかります。

Cisco スマート アカウントをすでに保有している場合、**Catalyst Center** を使用して次のことができます。

- ライセンスの使用量と有効期限日を追跡する
- ユーザーが介入せずに、新しいライセンスを適用および有効化する
- **Essentials** から **Advantage**（あるいはその逆）に各デバイスのライセンスレベルを上げ、新しい機能ライセンスのレベルでデバイスをリブートする
- 未使用ライセンスを特定して再適用する。

これらの操作は、**Catalyst Center** を離れることなく自動的に実行できます。

Catalyst Center ライセンスマネージャを使用する前に、**Cisco** スマートアカウントへのアクセスを設定する必要があります。

Catalyst Center ライセンスマネージャツールを使用する前に、**Cisco** スマートアカウントへのアクセスを設定する必要があります。

- この手順を実行するには、**SUPER-ADMIN-ROLE** 権限または適切な **RBAC** 範囲があることを確認します。
- スマート アカウントの **Cisco** ユーザー ID とパスワードを収集します。
- スマートアカウントが複数ある場合、**Catalyst Center** で使用するスマートアカウントを選択し、そのアカウントのユーザー ID とパスワードを収集します。
- **Catalyst Center** のデバイスにライセンスを適用するには、デバイスがインベントリに存在し、サイトが割り当てられ、必要なドメインに接続されていることを確認します。

- **id.cisco.com**

- **apx.cisco.com**

Catalyst Center 2.3.7.6 以降のリリースでは廃止されました。

- **apix.cisco.com**

- **commerce.cisco.com**

- **smartreceiver.cisco.com**

- 任意のファイアウォールまたはプロキシで、『[Cisco Catalyst Center Installation Guide](#)』に記載されているすべての使用できるポート、FQDN、および URL が許可されていることを確認します。

1. Catalyst Center システム管理者のユーザー名とパスワードを使用してログインします。
2. メインメニューから次を選択します。[System] > [Settings] > [Cisco.com Credentials] の順に選択します。
3. [Cisco.com Credentials] に、cisco.com アカountのユーザー名とパスワードを入力します。
4. [Information] ポップアップウィンドウで [I am inprivate or incognito mode] チェックボックスをオンにして、[Proceed] をクリックします。
5. メインメニューから次を選択します。[System] > [Settings] > [Smart Account] の順に選択します。
6. [Smart Account] で [Add] をクリックし、スマートアカウントのユーザー名とパスワードを入力します。
7. [Information] ポップアップウィンドウで [InPrivateまたはシークレットモードを使用しています (I am inprivate or incognito mode)] チェックボックスをオンにして、[Proceed] をクリックします。
8. [Save] をクリックします。
9. スマートアカウントが複数ある場合は、[Add] をクリックして追加のアカウントを入力します。
10. スマートアカウントが複数ある場合は、デフォルトに設定するアカウントを 1 つ選択します。ライセンスマネージャは、可視化およびライセンス操作にデフォルトのアカウントを使用します。デフォルトのスマートアカウントを変更するには、次の手順を実行します。
 - a) 選択したスマートアカウントの横にある [Change] をクリックします。
 - b) アクティブなスマートアカウントを変更し、デフォルトに設定するスマートアカウントを選択します。
 - c) [Apply] をクリックします。
デフォルトのアカウントを変更した後、CSSM からデータを取得し、[License Manager Overview] ウィンドウと [All License] ウィンドウに表示するまでに数分かかります。
11. スマートアカウントを編集するには、[Actions] 列にある三点リーダーをクリックし、[Edit] を選択します。
12. スマートアカウントを削除するには、[Actions] 列にある三点リーダーをクリックし、[Delete] を選択します。
13. 仮想または下位のスマートアカウント名とパスワードを使用してスマートアカウントにアクセスするには、[Link Your Smart Account] で次のいずれかを選択します。
 - [Use Cisco.com user ID] : Cisco.com とスマートアカウントのログイン情報が同じ場合。
 - [Use different credentials] : Cisco.com とスマートアカウントのログイン情報が異なる場合は、スマートアカウントのログイン情報を入力します。
14. [View all virtual accounts] をクリックし、すべての仮想スマート ライセンス アカountを表示します。

Catalyst Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカountに登録します。Cisco Plug and Play Connect クラウドポータルから、デバイスインベントリを Catalyst Center プラグアンドプレイに同期できます。詳細については、『[Cisco Catalyst Center User Guide](#)』の「Register or Edit a Virtual Account Profile」[英語] を参照してください。

Cisco

Cisco Networking Subscription (CNS) ライセンスの License Manager サポートの概要について説明します。

Wi-Fi 7 AP のリリースでは、Catalyst Center ライセンスマネージャは Cisco Networking Subscription (CNS) ライセンスをサポートします。AP のライセンスステータス、準拠、および非準拠の理由に対する可視性があります。ワイヤレスコントローラを CSSM と同期すると、Wi-Fi 7 AP は準拠し、CNS Essentials または Advantage サブスクリプションを表示します。

ライセンスマネージャ レポートには、すべてのデバイスが含まれます。準拠デバイスと非準拠デバイスでフィルタ処理できます。Catalyst Center 上のバナーは、必要なサブスクリプションに登録されていない AP を示し、ライセンスマネージャに戻って修正します。

CNS ライセンスに準拠するには、次の手順を実行する必要があります。

- スマートアカウントを設定します。
- [Cisco Smart Software Management] 接続モードを選択します。
Wi-Fi 7 を含む次世代デバイスの登録は、Cisco Smart Software Manager オンプレミス接続モードではサポートされていません。
- デバイスのアシュアランステレメトリを有効にします。
- デバイスをサイトに割り当てます。
- NTP を有効にします。

ライセンスの使用状況と有効期限の表示に関する情報。

Catalyst Center では、購入済みのライセンスのグラフィカル表示、使用中のライセンス数（デバイスに割り当てられている数）、およびその期間を表示できます。

1. メインメニューから次を選択します。[Tools] > [License Manager] の順に選択します。
2. [Overview] タブの Catalyst Center には、アクティブなスマートアカウントの名前が表示されます。[Virtual Account] ドロップダウンリストから、ライセンスの詳細を表示するバーチャルアカウントを選択します。
3. デバイスカテゴリボタンをクリックして、対応するライセンス使用状況の詳細（[Switches]、[Routers]、[WLC]、または [ISE]）。

ライセンスの使用状況の円グラフには、購入済みのライセンスの総数と選択したデバイスカテゴリで現在使用中のライセンスの数が表示されます。また、グラフには各合計内での Essentials ライセンスと Advantage ライセンスの割合も示されます。

購入したライセンスの数は、Cisco Smart Software Manager (CSSM) から取得されます。使用されているライセンスの数は、Catalyst Center によって管理されているデバイスから取得されます。

ライセンスの使用状況のテーブルには、使用されているライセンスと利用可能なライセンスの小計が、製品ファミリー名別にアルファベット順でリストされます。

4. 特定の製品ファミリーの詳細を表示するには、[Device Series] 列で目的の製品ファミリーの名前をクリックします。

Catalyst Center に、選択した製品ファミリーに関する詳細が表示されます。

5. ライセンス期間のグラフィカル表示を確認するには、**[Cisco License Timeline]** セクションまでスクロールダウンします。各製品ファミリのタイムライングラフでは、設定したスマートアカウントのライセンスの期限日が視覚的に表示されます。



注

このセクションは、**[ISE]** デバイスカテゴリでは使用できません。

ライセンス使用量の履歴傾向の表示に関する情報。

Catalyst Center では、**CSSM** で購入および使用されたすべてのライセンスの履歴傾向を、日次、週次、および月次で表示できます。**CSSM** には、最大 1 年間の履歴情報が保存されます。

この手順を使用して、ライセンス使用量の履歴傾向を表示します。

CSSM のスマートアカウントに **Catalyst Center** を登録します。詳細については、[Cisco スマートアカウントとの統合](#) (205ページ) を参照してください。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Licenses]** の順に選択します。

- **[License Summary]** エリアには、**CSSM** から購入した **Catalyst Center** サブスクリプションライセンスの総数が表示されます。
- **[Smart Account]** エリアには、スマートアカウントに関する詳細が表示されます。
- 次のエリアでは、サブスクリプションライセンスの合計数、期限切れのサブスクリプションライセンス、非準拠のサブスクリプションライセンスが表示されます。
 - **[CNS ESSENTIALS]**
 - **[CNS ADVANTAGE]**
 - **[Cisco DNA ESSENTIALS]**
 - **[Cisco DNA ADVANTAGE]**
 - **[NETWORK ESSENTIALS]**
 - **[Network Advantage]**
 - **[OS Essentials]**
 - **[OS Advantage]**
- **[License]** ウィンドウのテーブルに、検出されたデバイスとそのライセンスが表示されます。**[Focus]** ドロップダウンリストから必要なビューを選択できます。
 - バーチャルアカウントビュー

- ライセンスビュー
- デバイスシリーズビュー
- デバイスタイプビュー
- ライセンスタイプビュー

2. 選択したライセンスの履歴情報を表示するには、そのデバイスの行にあるライセンスリンクをクリックします。

ライセンス詳細 スライドインペイン に、選択したデバイスの完全なライセンスの詳細とライセンスの履歴が表示されます。

注

ライセンス詳細 スライドインペイン のタイトルが、選択したデバイスのタイトルと一致します。

3. ライセンス詳細 スライドインペイン で、**[Frequency]** ドロップダウンリストから履歴情報の頻度を選択します。

利用可能なオプションは下記のとおりです。

- **[Daily]** : 最初の日におけるライセンスデータのスナップショットを表示します。
- **[Weekly]** : 月曜日のライセンスデータのスナップショットを表示します。
- **[Monthly]** : その月の 1 日におけるライセンスデータのスナップショットを表示します。

頻度の選択に応じて、**[Purchased]**、**[In Use]**、および **[Balance]** のライセンスのライセンスデータを示すグラフが表示されます。

[License History] テーブルは、頻度の選択に応じて、**[Date]**、**[Purchased]**、**[In Use]**、および **[Balance]** に基づいてライセンス履歴情報をフィルタ処理します。

注

CSSM は前日のデータのみを提供するため、ライセンス履歴情報は常に 1 日前のデータです。Catalyst Center は、CSSM からライセンスの履歴情報を毎日定期的に取得します。

Catalyst Center でのライセンス詳細の表示に関する情報。

Catalyst Center でライセンスの詳細を見つけて表示するには、いくつかの方法があります。たとえば、**[License Manager]** ウィンドウの **[Switches]**、**[Routers]**、**[Wireless]**、**[ISE]**、または **[Devices]** タブでライセンスの使用状況や期間のグラフをクリックできます。各グラフには、製品ファミリ内のライセンスに関する集約された情報が表示されます。

単一のデバイスのすべてのライセンスの詳細を表示するには、ライセンスマネージャの **[Devices]** テーブルを使用します。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Devices]** の順に選択します。

[License Manager] ウィンドウには、検出されたすべてのデバイスと、それらのライセンスの一覧を示すテーブルが表示されます。テーブルには、デバイスの種類やライセンスの期限日など、基本的なデバイスおよびライセンスの詳細が含まれています。

2. 必要なライセンス詳細のデバイスを見つけるには、テーブルをスクロールします。デバイスが見つからない場合に使用できるオプションを以下に示します。

- **[Filter]** :  をクリックして、該当するフィールドにフィルタ条件を入力します。（たとえば、**[Device Name]** フィールドにデバイス名の全体または一部を入力）。フィルタ条件を複数のフィールドに入力することができます。**[Apply]** をクリックすると、テーブルにはフィルタ条件に一致する情報を表示する行のみが表示されます。

特定のサイトに属するデバイスを表示する場合は、左側のペインでそのサイトまで移動してクリックします。フィルタ処理されて該当するデバイスが表示されます。サイト階層を示すサイトマーカーがページの上部に表示されます。

- **[Find]** : **[Find]** フィールドをクリックし、テーブルの列のいずれかに検索するテキストを入力します。**Enter** を押すと、テーブルは **[Find]** フィールドの入力に一致するテキストが含まれる最初の行にスクロールします。
- **[Customize]** : 歯車アイコンをクリックし、**[Edit Table Columns]** で、テーブルに表示する列を選択します。たとえば、**[Device Series]** を選択解除するか、**[Days to Expiry]** を選択します。**[Apply]** をクリックすると、テーブルに選択した列のみが表示されます。

3. 必要なデバイスが見つかったら、該当するデバイスの行の **[Device Name]** リンクをクリックします。

Catalyst Center に **[License Details]** スライドインペインが表示され、選択したデバイスのすべてのライセンス詳細情報とライセンス履歴が示されます。**[Actions]** には、デバイスまたはそのライセンスで実行できるアクションが表示されます。

完了したら  をクリックし、**[License Details]** スライドインペイン を閉じます。

デバイスライセンスの機能レベルの変更に関する情報。

次のライセンスタイプについて、デバイスのライセンスレベルを **Essentials** または **Advantage** にアップグレードまたはダウングレードできます。

- DNA
- CNS
- OS

注

- デバイスのライセンスタイプは変更できません。対応するライセンスタイプのライセンスレベルのみを変更できます。
- ネットワークライセンスの変換は、**Cisco Catalyst 9000** デバイスファミリの製品でのみ使用できます。この変換は、**Catalyst Center** のライセンスレベルが変更されると暗黙的に処理されます。
- デバイスのライセンスレベルは、ルータ、スイッチ、ワイヤレスコントローラなど、一度に 1 つのファミリーから変更できます。
- UL でサポートされているデバイスを使用している場合は、デバイスライセンスのみを使用できます。
- デバイスが **OS Advantage** ライセンスのみをサポートしている場合、そのデバイスのライセンスは変更できません。

Catalyst Center サブスクリプションライセンスでライセンスレベルを更新できます。デバイスのライセンスレベルを変更すると、**Catalyst Center** は、スマートアカウントを使用して、自動的にライセンスをダウンロードして適用します。

ライセンスレベルを変更した後、デバイスを再起動すると変更が有効になります。**Cisco Catalyst 3560-CX** シリーズスイッチや **Cisco AireOS** ワイヤレスコントローラ などのデバイスの場合、再起動は必要ありません。

1. メインメニューから次を選択します。[Tools] > [License Manager] > [Devices] の順に選択します。
[License Manager] ウィンドウには、検出されたデバイスと、各デバイスのライセンスの一覧を示すテーブルが表示されます。
2. [Find] を使用するか、テーブルをスクロールして、ライセンスレベルを変更するデバイスを検索します。デバイスの検索で問題が発生したり、複数のデバイスを選択したりする場合は、「[ライセンス詳細の表示](#) (210 ページ)」を参照してテーブルを変更し、必要なデバイスだけを表示します。
3. ライセンスレベルを変更するデバイスの横にあるチェックボックスをオンにします。
4. [Actions] > [Change License] > [Change Cisco License] を選択します。
5. 複数のデバイスファミリ（スイッチやワイヤレスコントローラなど）からデバイスを選択した場合は、次の手順を実行します。
 - a) ライセンスレベルを変更するデバイスファミリ（[Routers]、[Switch]、または [Wireless]）の横にあるオプションボタンをクリックします
 - b) [Continue] をクリックします。
6. 必要なライセンスレベルを選択します。
 - a) デバイスに必要なライセンスレベルをクリックします。
現在のライセンスレベルに基づいて、**Catalyst Center** には使用可能なライセンスレベル（[Essentials] または [Advantage]）のみが表示されます。
デバイスからライセンスを削除するには、[Remove] をクリックします。

 注

デバイスから **CNS** ライセンスを削除することはできません。**CNS** ライセンスを削除すると、デバイスはデフォルトで **CNS Advantage** ライセンスを使用します。

b) 以下から必要なライセンスタイプをクリックします。

- すべて
- DNA
- CNS
- OS

c) [Continue] をクリックします。

7. ライセンスレベルが更新されたときにデバイスを再起動するには、[Reboot device on update] チェックボックスをオンにします。
8. オプション: [Task Name] フィールドで、タスク名を更新します。
9. デバイスのライセンスレベルを更新するスケジュールを選択します。
 - [Now] : ライセンスレベルをただちに更新し、デバイスを再起動します。
 - [Later] : ライセンスレベルを更新してデバイスを再起動する日付と時刻をスケジュールします。
10. [Confirm] をクリックします。
11. [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。
[Recent Tasks] ウィンドウでライセンスレベル変更タスクのステータスを確認できます。

スマートライセンス (SL) が有効なデバイスの自動登録の有効化に関する情報。

スマートライセンス (SL) が有効なデバイスの自動登録を有効化することができます。自動登録を有効化すると、**Catalyst Center** に追加される **SL** が有効なデバイス（ただしスマートライセンスポリシーで [SLP] が有効なデバイスは除く）は、選択したバーチャルアカウントに自動登録されます。

 注

自動登録はスマートプロキシモードではサポートされていません。

1. **Catalyst Center** システム管理者のユーザー名とパスワードを使用してログインします。
2. メインメニューから次を選択します。[System] > [Settings] > [Cisco Accounts] > [Smart Account] の順に選択します。

3. **[License]** をクリックします。
4. **[Auto register smart license enabled device]** チェックボックスをオンにします。
5. 仮想アカウントを選択します。
6. **[Apply]** をクリックします。

スマートライセンス対応デバイスのデイズロ設定に関する情報。

自動登録が有効化される前に **Catalyst Center** に追加されたデバイスは、自動登録されません。登録されていないスマートライセンス対応デバイスを表示するには、**[All Licenses]** ウィンドウを開きます。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Devices]** の順に選択します。
[License Manager] ウィンドウには、自動登録されていない SL 対応デバイスの数と、検出されたデバイスとそのライセンスの一覧が表示されたテーブルのバナーメッセージが、自動登録を設定するリンクとともに表示されます。
 また、**[Registration Status]** 列を選択して、未登録のデバイスをフィルタリングすることもできます。
2. 登録する SL 対応デバイスを選択し、**[Actions] > [Manage Smart License] > [Register]** の順に選択します。
3. 仮想アカウントを選択して **[Continue]** をクリックします。
4. デバイスを登録するには、次のいずれかを実行します。
 - すぐにデバイスを登録する場合は、**[Now]** を選択し、**[Confirm]** をクリックします。
 - 後でデバイスを登録する場合は、**[Later]** を選択し、日時を指定します。スケジュールのパラメータの指定が終わったら、**[Confirm]** をクリックします。

世界中のセーフモード対応デバイスの場合、ライセンスを設定するまで無線機能は制限されます。

世界中のセーフモード (**WWSM**) 対応デバイスは、デイズロおよびライセンス要件を満たしていない場合、**WWSM** になります。**WWSM** を無効化するには、デバイスで **CNS** ライセンスを有効にする必要があります。

WWSM 対応デバイスでライセンスを設定し、**WWSM** を無効にするには、この手順を使用します。

スマートアカウントのデバイスで **CNS** ライセンスが使用できることを確認します。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Reporting]** の順に選択します。
2. **[Smart License Compliance]** をクリックします。

または、最初の2つの手順の代わりに、メニューアイコンをクリックして次を選択します。を選択し、**[Workflows > Smart License Compliance]** の順に選択します。

3. [Smart License Compliance] ウィンドウで、**[Let's Do It]** をクリックします。

今後タスクの概要をスキップするには、**[Don't show this to me again]** チェックボックスをオンにします。

4. [Select Smart Account] ウィンドウで、次の手順を実行します。

- a) オプション: **[Workflow Name]** フィールドで、タスク名を更新します。
- b) **[Smart Account]** ドロップダウンリストで、CNS ライセンスを含むスマートアカウントを選択します。
- c) **[Virtual Account]** ドロップダウンリストで、バーチャルアカウントを選択します。
- d) **[Next]** をクリックします。

5. [Choose Sites and Devices] ウィンドウで、次の手順を実行します。

- a) オプション: 左側のペインで、必要なサイトを選択します。
- b) ライセンスレベルを設定するデバイスの横にあるチェックボックスをオンにします。

[Search] フィールドを使用して、名前でデバイスを検索できます。

フィルタアイコン (▼) をクリックすると、列ヘッダーに基づいてテーブル内のデバイスをフィルタ処理できます。

- c) **[Next]** をクリックします。

6. [Modify Policy] ウィンドウで、次の手順を実行します。

- a) CSSM ポリシーを確認します。

(オプション) レポート間隔を変更するには、**[Modify]** をクリックし、**[Change Reporting Interval]** ダイアログボックスで次の手順を実行します。

1. **[Reporting Interval in Days]** フィールドには、デバイスがリソース使用状況を CSSM にレポートするレポート間隔を入力します。

2. **[Save]** をクリックします。

- b) **[Next]** をクリックします。

7. [Sync Data with Cisco] ウィンドウで **[Submit]** をクリックします。

8. [Summary] ウィンドウで **[Finish]** をクリックします。

特定ライセンス予約 (SLR) またはパーマネントライセンス予約 (PLR) の有効化についての情報。Catalyst Center のお客様は、ライセンスマネージャで API ベースのワークフローを使用して CSSM から安全にライセンスを予約できます。

スマートライセンスでは、スマートデバイスのインスタンスによって Cisco Smart Software Management (CSSM) と定期的に同期して、ライセンスステータスの最新化とコンプライアンスの報告が行われるようにする必要があります。一部のお客様は、インターネットアクセスが制限された高度に保護されたネットワーク内にあるデバイスを使用しています。このようなタイプのネットワークでは、デバイスは定期的に CSSM と同期してコンプライアンス違反を表示することができません。このようなお客様の環境をサポートするため、特定ライセンス予約 (SLR) およびパーマネントライセンス予約 (PLR) が導入されました。Catalyst Center のお客様は、ライセンスマネージャで API ベースのワークフローを使用して CSSM から安全にライセンスを予約できます。Catalyst Center では、ステージング環境で CSSM に一度接続すれば、デバイスから SLR モードまたは PLR モードでシスコに接続する必要はありません。CSSM への接続やステージングが実行できない場合は、CSSM で利用できる手動 SLR/PLR ワークフローが使用できます。

SLR によってお客様は、製品インスタンスにノードロック ライセンス ファイル (SLR 承認コード) をインストールできます。このライセンスファイルによって、個別の (特定の) ライセンス (権限付与タグ) が有効化されます。

PLR によってお客様は、製品にすべてのライセンス済み機能を有効化する承認コードをインストールできます。

SLR と PLR の両方に、スマートアカウントのレベルでの事前承認が必要です。サポートが必要な場合は、licensing@cisco.com にご連絡ください。

デバイスと Catalyst Center の両方が CSSM に接続されている場合に SLR または PLR を有効にする方法については、[デバイスと Catalyst Center が CSSM に接続されている場合の SLR または PLR の有効化 \(216 ページ\)](#) を参照してください。

デバイスと Catalyst Center が CSSM に接続されていない場合に SLR または PLR を有効にする方法については、[デバイスと Catalyst Center が CSSM に接続されていない場合の SLR または PLR の有効化 \(216 ページ\)](#) を参照してください。

Catalyst Center CSSM SLR PLR

デバイスと Catalyst Center が CSSM に接続されている場合の特定ライセンス予約 (SLR) またはパーマネントライセンス予約 (PLR) の有効化についての情報。

-
1. メインメニューから次を選択します。[Tools] > [License Manager] > [Devices] の順に選択します。
 2. SLR または PLR を適用するデバイスを選択して、[Actions] > [Manage License Reservation] > [Enable License Reservation] の順にクリックします。
 3. [Specific License Reservation (SLR)] または [Permanent License Reservation (PLR)] を選択し、[Continue] をクリックして選択したデバイスの要求コードを取得します。
 4. 選択したデバイスの要求コードが生成されたら、[Continue] をクリックします。
 5. ライセンスを予約するバーチャルアカウントを選択し、[Continue] をクリックして選択したデバイスの承認コードを生成します。
 6. 承認コードが生成されたら、次のいずれかを実行します。
 - SLR をすぐに適用する場合は、デバイスを選択して、[Continue] をクリックします。
 - 後で SLR を適用する場合は、[Apply Later] をクリックします。
 7. [Confirm] をクリックして、SLR/PLR を選択したデバイスに適用します。
- [All Licenses] ウィンドウの [Reservation Status] に、更新された最新のデバイスのステータスを表示できるようになりました。
-

Catalyst Center CSSM SLR PLR

デバイスと Catalyst Center が CSSM に接続されていない場合の特定ライセンス予約 (SLR) またはパーマネントライセンス予約 (PLR) の有効化についての情報。

CSSM に接続されていないデバイスの SLR または PLR を有効にするには、次の手順を実行します。

-
1. メインメニューから次を選択します。[Tools] > [License Manager] > [Devices] の順に選択します。

2. SLR または PLR を適用するデバイスを選択して、**[Actions] > [Manage License Reservation] > [Enable License Reservation]** の順にクリックします。
3. **[Specific License Reservation (SLR)]** または **[Permanent License Reservation (PLR)]** を選択し、**[Continue]** をクリックして選択したデバイスの要求コードを取得します。

Telnet を介してデバイスに接続し、要求コードを取得することもできます。

4. 選択したデバイスの要求コードが生成されたら、**[Export]** をクリックします。これにより、**requestcodes.csv** ファイルがダウンロードされます。このファイルには、IP アドレス、デバイスのシリアル番号、および要求コードが含まれています。
5. 任意の場所にファイルを保存します。
6. CSSM から各デバイスの承認コードを取得し、CSV ファイル内で更新します。「[CSSM からの承認コードの生成](#)」を参照してください。
7. **[Upload CSV]** リンクをクリックします。
8. **[Select a file from your computer]** リンクをクリックして、保存した CSV ファイルを選択します。
9. **[Continue]** をクリックします。
10. ライセンスを予約するバーチャルアカウントを選択し、**[Continue]** をクリックします。選択したデバイスに SLR または PLR が適用されます。

[All Licenses] ウィンドウの **[Reservation Status]** に、更新された最新のデバイスのステータスを表示できるようになりました。

CSSM

CSSM からの認証コードの生成に関する情報。

CSSM にログインするには、スマートアカウントのクレデンシャルが必要です。

1. **CSSM** にログインします。
2. **[Inventory] > [Licenses] > [License Reservation]** を選択します。**[Smart License Reservation]** ウィザードが表示されます。
[Licenses] タブの **[License Reservation]** ボタンは、自分のスマートアカウントで特定ライセンス予約 (SLR) を有効にした場合にのみ表示されます。
3. **[Step 1: Enter Request Code]** タブで、**[Reservation Request Code]** フィールドに要求コードを入力して、**[Next]** をクリックします。
4. **[Step 2: Select Licenses]** タブで、**[Reserve a specific license]** チェックボックスをオンにします。
5. **[Quantity to Reserve]** フィールドに、予約するライセンスの数を入力し、**[Next]** をクリックします。
6. **[Step 3: Review and Confirm]** タブで **[Generate Authorization Code]** をクリックします。
7. **[Step 4: Authorize Code]** タブで認証コードを取得します。

SLR PLR

デバイスに適用される特定ライセンス予約 (SLR) またはパーマネントライセンス予約 (PLR) のキャンセルに関する情報。

デバイスに適用されている SLR または PLR をキャンセルまたは返すことができます。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Licenses]** の順に選択します。
2. デバイスをクリックし、 **[Actions] > [Manage License Reservation] > [Cancel/Return License Reservation]** の順に選択します。
3. **[Cancel]** をクリックしてライセンスを返却します。

[All Licenses] ウィンドウの **[Reservation Status]** に、更新された最新のデバイスのステータスを表示できるようになりました。

承認コードのインストールと、高セキュリティライセンスの有効化についての情報。デバイスのスループットを **250 Mbps** 超に増やすには、シスコから承認コードを取得する必要があります。承認コードをインストールし、高セキュリティライセンス (HSEC) を有効にすることができます。

シスコでは、デフォルトで **250 Mbps** のスループットを提供しています。デバイスのスループットを **250 Mbps** 超に増やすには、シスコから承認コードを取得する必要があります。必要に応じて、単一のワークフローまたは個別のワークフローで承認コードをインストールし、高セキュリティ (HSEC) ライセンスを有効にできます。

デバイスで Cisco IOS XE リリース 17.3.2 以降が実行されていることを確認します。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Reporting]** の順に選択します。
または、 **[Workflows] > [Smart License Compliance]** を使用できます。
2. **[Smart License Compliance]** カードをクリックします。
3. **[Smart License Compliance]** ウィンドウで、 **[Let's Do It]** をクリックします。
今後このウィンドウをスキップするには、 **[Don't show this to me again]** チェックボックスをオンにします。
4. **[Select Smart Account]** ウィンドウで、ドロップダウンリストから **[Smart Account]** と **[Virtual Account]** を選択します。
5. **[Next]** をクリックします。
6. **[Choose Sites and Devices]** ウィンドウで、承認コードをインストールするデバイスを選択し、 **[Next]** をクリックします。
7. **[Policy Settings]** ウィンドウで、CSSM ポリシーを確認し、 **[Next]** をクリックします。
8. **[Choose Device Features]** ウィンドウで、次の手順を実行します。
 - a) デバイスを選択します。
 - b) **[Auth Codes]** ドロップダウンリストから、 **[Install]** を選択します。
 - c) **[HSEC]** ドロップダウンリストから、 **[Enable]** を選択します。
 - d) **[Next]** をクリックします。
9. **[Review Device Features]** ウィンドウで、 **[Next]** をクリックします。

10. [Installing Device Features] ウィンドウで、承認コードと HSEC インストールステータスを確認し、[Next] をクリックします。
 11. [Sync Data with Cisco] ウィンドウで [Next] をクリックします。
 12. [Summary] ウィンドウで承認コードと HSEC インストールステータスを確認したら、[Finish] をクリックします。
-

高セキュリティライセンスの無効化に関する情報。

無駄な利用を防ぐために、デバイスで HSEC ライセンスを無効化できます。

-
1. メインメニューから次を選択します。[Tools] > [License Manager] > [Reporting] の順に選択します。
 2. [Smart License Compliance] カードをクリックします。
 3. [Smart License Compliance] ウィンドウで、[Let's Do It] をクリックします。
今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。
 4. [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。
 5. [Next] をクリックします。
 6. [Choose Sites and Devices] ウィンドウで、HSEC ライセンスを無効にするデバイスを選択し、[Next] をクリックします。
 7. [Policy Settings] ウィンドウで、[Next] をクリックします。
 8. [Choose Device Features] ウィンドウで、次のアクションを実行します。
 - a) デバイスを選択します。
 - b) [HSEC] ドロップダウンリストから、[Disable] を選択します。
 - c) [Next] をクリックします。
 9. [Review Device Features] ウィンドウで、[Next] をクリックします。
 10. [Installing Device Features] ウィンドウで、HSEC 無効化操作のステータスを確認し、[Next] をクリックします。
 11. [Sync Data with Cisco] ウィンドウで [Next] をクリックします。
 12. [Summary] ウィンドウで [Finish] をクリックします。
-

CSSM

CSSM へのリソース使用状況詳細のアップロードに関する情報。

リソース使用状況の詳細を CSSM に即座にアップロードしたり、アップロードをスケジュールすることができます。

リソース使用状況の詳細を CSSM にアップロードするために、NETCONF を有効にしたり、サイトにデバイスを追加したりする必要はありません。

Network Essentials ライセンスを持つ非 IoT デバイスを追加します。進行中のタスクがないことを確認します。少なくとも 1 つの AP がワイヤレスコントローラに関連付けられていることを確認します。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Reporting]** の順に選択します。
2. **[Smart License Compliance]** カードをクリックします。
3. **[Smart License Compliance]** ウィンドウで、**[Let's Do It]** をクリックします。
今後このウィンドウをスキップするには、**[Don't show this to me again]** チェックボックスをオンにします。
4. **[Select Smart Account]** ウィンドウで、ドロップダウンリストから **[Smart Account]** と **[Virtual Account]** を選択します。
5. **[Next]** をクリックします。
6. **[Choose Sites and Devices]** ウィンドウで、リソース使用率の詳細を取得するデバイスを選択し、**[Next]** をクリックします。
7. リソース使用率の詳細を即座にアップロードするには、**[Modify Policy]** ウィンドウで **[Next]** をクリックします。定期レポートの頻度を変更するには、次の手順を実行します。
 - a) **[Policy Settings]** で、**[Reporting Interval]** フィールドに対応する **[Modify]** をクリックします。
 - b) **[Change Reporting Interval]** ウィンドウで、値を入力します。
レポート間隔（日数）は、**Catalyst Center** から **CSSM** へのリソース使用率の詳細の定期的なアップロードの頻度を示します。アップロードの頻度は増やすことができますが、最小レポート頻度未満に減らすことはできません。
 - c) **[Save]** をクリックします。
8. **[Sync Data with Cisco]** ウィンドウで **[Next]** をクリックします。
9. **[Summary]** ウィンドウで **[Finish]** をクリックします。
CSSM との同期が成功すると、デバイスで確認応答を受信します。

ライセンス使用状況レポートが失敗したデバイスの数は、別の **[Smart License Compliance]** カードに **[Retry]** オプションとともに表示されます。**[Smart License Compliance]** カードをクリックし、手順をやり直して、失敗したデバイスから **CSSM** にライセンス使用状況レポートを送信します。

CSSM

オンプレミス SSM を介して技術情報の詳細を **CSSM** へアップロードします。

オンプレミス SSM を介して技術情報の詳細を **CSSM** にアップロードできます。

Before you begin

オンプレミス SSM 接続モードを有効にする必要があります。詳細については、[接続モードの設定](#)（52ページ）を参照してください。

1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Reporting]** の順に選択します。
2. **[Smart License Compliance]** カードをクリックします。
3. **[Smart License Compliance]** ウィンドウで、**[Let's Do It]** をクリックします。
今後このウィンドウをスキップするには、**[Don't show this to me again]** チェックボックスをオンにします。

4. **[Select Smart Account]** ウィンドウで、ドロップダウンリストから **[Smart Account]** と **[Virtual Account]** を選択します。
 5. **[Next]** をクリックします。
 6. **[Choose Sites and Devices]** ウィンドウで、リソース使用率の詳細を取得するデバイスを選択し、**[Next]** をクリックします。
 7. リソース使用率の詳細を即座にアップロードするには、**[Modify Policy]** ウィンドウで **[Next]** をクリックします。スケジュールレポートの頻度を変更する場合は、提供されたオプションを使用します。
 - a) **[Policy Settings]** で、**[Reporting Interval]** フィールドに対応する **[Modify]** をクリックします。
 - b) **[Change Reporting Interval]** ウィンドウで、値を入力します。
 レポート間隔（日数）は、オンプレミス SSM から Cisco Cloud SSM へのリソース使用率の詳細の定期的なアップロードの頻度を示します。アップロードの頻度は増やすことができますが、最小レポート頻度（24時間）未満に減らすことはできません。
 - c) **[Save]** をクリックします。
 8. **[Sync Data with Cisco]** ウィンドウで **[Next]** をクリックします。
 9. **[Summary]** ウィンドウで **[Finish]** をクリックします。
 CSSM との同期が成功すると、デバイスで確認応答を受信します。
-

接続モードを **Smart Call Home** から **Smart Transport** に変更します。

Catalyst Center 2.3.7.6 以降、スマートライセンスの **Smart Call Home (SCH)** サポートはサポート終了になります。Smart Licensing で SCH を使用している場合は、スマートトランスポートに移行します。

次のシナリオのいずれかが発生すると、**[Tools] > [License Manager] > [Devices]** のデバイス名列に **[Connection Mode Out of Sync]** タグが付けられます。

- **[System] > [Settings] > [SSM Connection mode]** で SSM 接続モードを変更するとき
 - Catalyst Center セットアップで FQDN を変更するとき
 - SSM 接続モードを変更したとき、または企業 VIP IP アドレスが変更されたとき
 - デバイスで手動で設定されたスマートトランスポートが、Catalyst Center セットアップの SSM 接続モードと一致しない場合
 - Catalyst Center を以前のリリースから 2.3.7.6 以降のリリースにアップグレードした後
-

1. メインメニューから次を選択します。**[Tools] > [License Manager] > [Devices]** の順に選択します。
 スマートライセンス対応デバイスに対して **[Connection mode out of sync]** 警告メッセージが表示された場合は、警告メッセージをクリックして、接続モードが非同期の詳細を表示します。
2. **[License Manager window]** で、**[Sync Connection Mode]** をクリックします。
 SCH からスマートトランスポートへの接続モードの遷移は、次のシーケンスで行われます。
 - a. SCH の登録解除
 - b. スマートトランスポート URL をデバイスにプッシュ

c. スマート ライセンスの登録の完了

オンプレミス CSSM を使用したデュアルスタック IPv4/IPv6 環境では、IPv6 デバイスに対して [Sync Connection Mode] のアクションがブロックされます。同期を有効にするには、[SSM Connection Mode] ウィンドウでオンプレミス CSSM ホストアドレスを IP アドレスから FQDN に変更する必要があります。

3. オプション: メインメニューから次を選択します。[Activities > Tasks] で [Sync Connection Mode] タスクのステータスを表示します。
4. オプション: メインメニューから次を選択します。[Activities > Audit Logs] でデバイスへの設定の変更を表示します。

スマートライセンス対応ルータのスループットの変更に関する情報。

スマートライセンス対応ルータのスループットを変更できます。

1. メインメニューから次を選択します。[Tools] > [License Manager] > [Reporting] の順に選択します。
2. 変更するデバイスを選択します。
3. [More Actions] をクリックし、[Change Throughput] を選択します。
4. [Choose Throughput] ウィンドウでスループット値を選択し、[Next] をクリックします。
5. [Apply Throughput] ウィンドウで [Next] をクリックします。
6. [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。
[Recent Tasks] ウィンドウで [Change Throughput] タスクのステータスを確認できます。

バーチャルアカウント間のライセンスの転送に関する情報。

バーチャルアカウント間でライセンスを転送できます。

1. メインメニューから次を選択します。[Tools] > [License Manager] > [Licenses] の順に選択します。
2. 転送するライセンスを選択し、[Transfer Licenses] をクリックします。
3. [Transfer Licenses] ウィンドウで、バーチャルアカウントを選択します。
4. 選択した各ライセンスの [Transfer License Count] を入力し、[Transfer] をクリックします。
5. [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。
[Recent Tasks] ウィンドウで [License Transfer] タスクのステータスを確認できます。

スマートライセンス対応デバイスに対する顧客タグの管理についての情報。スマートライセンス対応デバイスには、最大 4 つの顧客タグを追加できます。顧客タグを更新および削除することもできます。

スマートライセンス対応デバイスに最大 4 つの顧客タグを追加して、製品インスタンスのテレメトリデータの識別を容易にすることができます。顧客タグを更新および削除することもできます。

-
1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Reporting]** の順に選択します。
 2. 顧客タグを追加するデバイスを選択します。
 3. **[More Actions]** をクリックし、**[Manage Free Form Fields]** を選択して、顧客タグを追加、更新、または削除します。
 4. 顧客タグを追加または更新するには、**[Free Form Fields]** ウィンドウで次の手順を実行します。
 - a) 顧客タグを入力します。
 - b) **[Save]** をクリックします。
 5. 顧客タグを削除するには、**[Free Form Fields]** ウィンドウで次の手順を実行します。
 - a) 削除する顧客タグの削除アイコンをクリックします。
 - b) **[Save]** をクリックします。
 - c) **[Warning]** ウィンドウで **[Continue]** をクリックします。
 6. **[Recent Tasks]** リンクをクリックして、**[Recent Tasks]** ウィンドウを起動します。
[Recent Tasks] ウィンドウで **[Manage Customer Tags]** タスクのステータスを確認できます。
-

ライセンスポリシーの変更に関する情報。ネットワークデバイスが **CSSM** に機能の使用状況を報告するレポート間隔を変更できます。

ネットワークデバイスが **CSSM** に機能の使用状況を報告するレポート間隔を変更できます。

-
1. メインメニューから次を選択します。 **[Tools] > [License Manager] > [Reporting]** の順に選択します。
 2. **[Smart License]** テーブルで、**[Modify Policy]** をクリックします。
[Modify Policy] ウィンドウに、ポリシー設定と **CSSM** ポリシーの詳細が表示されます。
 3. **[Policy Settings]** で、**[Modify]** をクリックします。
 4. **[Change Reporting Interval]** ウィンドウで、レポート間隔の値を入力します。
 5. **[Save]** をクリックします。
-

第
13

章

:

- [バックアップファイルの作成](#)
- [バックアップファイルの復元](#)
- [バックアップファイルの削除](#)
- [バックアップファイルの検索](#)
- [バックアップファイルのリストアップ](#)
- [NFS バックアップ](#)
- [バックアップファイルの圧縮](#)
- [バックアップ SSH](#)
- [バックアップのスケジュール](#)
- [バックアップのログ](#)
- [バックアップの監視](#)
- [バックアップのレポート](#)
- [バックアップのバックアップ](#)

復元するバックアップファイルを作成するためのバックアップ機能と復元機能についての情報。

Catalyst Center のバックアップと復元に関する情報。

バックアップおよび復元機能を使用すると、ネットワーク設定に必要な場合に、バックアップファイルを作成し、別のアプライアンスに復元できます。

- 自動化データのみ、または自動化データと **Assurance** データの両方をバックアップできます。

重要

Catalyst Center の自動化と **Assurance** データをバックアップする際、**NetFlow** データはバックアップされません。

- 自動化データは、**Catalyst Center** データベース、クレデンシャル、ファイルシステム、およびファイルで構成されています。自動バックアップは、すべてのデータのバックアップです。
- **Assurance** データは、ネットワークアシュアランスと分析データで構成されています。**Assurance** データの最初のバックアップは、すべてのデータのバックアップです。その後は増分バックアップです。

重要

- バックアップファイルは変更または削除しないでください。変更すると、バックアップファイルを **Catalyst Center** に復元できない場合があります。
- バックアップは、送信元クラスターと同じ **FIPS** モード設定を持つ **Catalyst Center** クラスターでのみ復元できます。**FIPS** モード設定が異なるクラスターを含むバックアップおよび復元操作は失敗します (**Catalyst Center** はバックアップに互換性なしのラベルを付けるため)。
- **Catalyst Center** はバックアップファイルを作成して、リモートサーバーにポストします。各バックアップは、ディレクトリ名として **UUID** を使用して一意に格納されます。リモートサーバーの要件の詳細については、[バックアップサーバーの要件](#) (228ページ) を参照してください。
- 一度に 1 つのバックアップのみ実行できます。一度に複数のバックアップを実行することはできません。
- バックアップの実行中は、ファイルサービスにアップロードされたファイルを削除することはできず、ファイルに加えた変更はバックアッププロセスによってキャプチャされないことがあります。
- 推奨事項：
 - データベースとファイルの現在のバージョンを維持するために毎日バックアップを実行する。
 - 設定を変更した後にバックアップを実行します。たとえば、デバイスで新しいポリシーを変更または作成するときなどです。
 - バックアップは影響の少ない時間帯かメンテナンス時間にのみ実行する。
- 週の特定期の時刻に週単位のバックアップをスケジュールできます。

- **Catalyst Center** を使用してリモートサーバーからバックアップファイルを復元できます。
- バックアップファイルを復元すると、**Catalyst Center** によって既存のデータベースとファイルが削除され、バックアップデータベースとファイルで置き換えられます。復元を実行している間、**Catalyst Center** は使用できません。
- **Catalyst Center** は、バージョンをまたがるバックアップと復元をサポートしています。つまり、2つの以前のバージョンの **Catalyst Center** のいずれかからバックアップを作成し、それを最新バージョンの **Catalyst Center** に復元できます。たとえば、**Catalyst Center 3.1.3-75710** バージョンまたは **Catalyst Center 3.1.5-75246** バージョンのバックアップは **Catalyst Center 3.1.6-75205** バージョンに復元できます。**Catalyst Center** のそれ以降のリリースにも同じことが当てはまります。詳細については、「[Release Notes for Cisco Catalyst Center](#)」を参照してください。
- 「[Cisco Catalyst Center Data Migration](#)」記事で、次のトピックを参照してください。
 - 移行シナリオ 2、3、5、および 8 の手順では、異なる IP アドレスを持つ **Catalyst Center** アプライアンスにバックアップを復元する方法について説明します。この状況は、**Catalyst Center** の IP アドレスが変更されていて、古いシステムから復元する必要がある場合に生じる可能性があります。

重要

Catalyst Center のバックアップと復元後：

- **[Integration Settings]** ウィンドウにアクセスし、（必要に応じて）**[Callback URL Host Name]** または **[IP Address]** を更新する必要があります。詳細については、「[Configure integration settings](#)」を参照してください。
- **Catalyst Center** メンバー ID が変更されると、**Cisco Spaces** との統合が中断されます。これは、たとえば、別のハードウェアアプライアンスで復元するとき、またはハードウェアアプライアンスから仮想アプライアンスに移行するときに発生します。詳細については、『[Cisco Spaces Configuration Guide](#)』の「[Integrate Cisco Spaces with Catalyst Center](#)」を参照してください。
- 「変換およびアプライアンスのアップグレードに関する考慮事項」トピックでは、バックアップファイルを復元してより上位の **Catalyst Center** アプライアンスにアップグレードする場合に注意すべきその他の点について説明します。

バックアップと復元のイベント通知に関する情報。

バックアップまたは復元イベントが発生するたびに通知を受信できます。これらの通知を設定および登録するには、『[Cisco Catalyst Center Platform User Guide](#)』の「[Work with event notifications](#)」トピックに説明されている手順を実行してください。この手順を完了したら、**SYSTEM-BACKUP-v2** イベントと **SYSTEM-RESTORE-v2** イベントを選択し、サブスクライブしていることを確認します。

通知は、次の表に示すイベントのいずれかが発生するたびに生成および送信されます。

動作	イベント
バックアップ	システムのバックアップファイルを作成するプロセスが開始された。 システムのバックアップファイルを作成できなかった。このイベントは通常、次の理由で発生します。 - 必要なディスク領域がリモートストレージにありません。 - システムのサーバーのステータスを取得できません。これは、バックアップ操作のための事前チェックです。 - システムでバックアップファイルを作成中に、接続の問題や遅延が発生しました。
復元	バックアップファイルを復元するプロセスが開始された。 バックアップファイルの復元に失敗した。このイベントは通常、次の理由で発生します。 - バックアップファイルが破損しています。 - システムでバックアップファイルを作成中に、接続の問題や遅延が発生しました。

バックアップサーバーの要件に関する情報。

バックアップサーバーは、サポートされている次のいずれかのオペレーティングシステムを実行している必要があります。

- Red Hat Enterprise 8 以降
- Ubuntu 16.04（または Mint など）以降

Assurance

Assuranceデータのバックアップをサポートする場合、サーバーは **Linux** または **Windows** ベースの **NFS** サーバー、または次の要件を満たす **NetApp**、**Isilon** などのストレージベンダーが提供する **NFS** にすることができます。

- **NFS v4** および **NFS v3** をサポートしている（このサポートを確認するには、サーバーから **nfsstat -s** を入力します）。
- **NFS** エクスポートディレクトリに対する読み取り/書き込み権限がある。
- **Catalyst Center** と **NFS** サーバー間のネットワーク接続が安定している。
- **Catalyst Center** と **NFS** サーバー間のネットワーク速度が十分速い。

NFS 搭載ディレクトリを **Catalyst Center** バックアップサーバーとして使用することはできません。カスケードされた **NFS** マウントは遅延の層が増えるため、サポートされません。

サポートされているバックアップサーバーのタイプは、**Catalyst Center** の展開モデルによって異なります（コンテナ化されたバックアップサーバーは、いずれのデプロイメントタイプでもサポートされていません）。

Catalyst Center 展開	サポートされるバックアップサーバーのタイプ
ベアメタルまたは仮想アプライアンス	物理、VM ベース
クラウドベース（AWS、Azure など）	オンプレミス、クラウドベース

Catalyst Center

ネットワークに複数の **Catalyst Center** クラスタが含まれている場合、次の設定例は、**NFS** サーバーのバックアップディレクトリ構造に名前を付ける方法を示しています。

リソース	設定例
Catalyst Center クラスタ	<i>cluster1</i> <i>cluster2</i>
自動化と Assurance のバックアップをホストするバックアップサーバー	例示したディレクトリは <code>/data/</code> で、両方のタイプのバックアップをホストする十分なスペースがあります。
NFS エクスポート設定	<code>/etc/exports</code> ファイルの内容： <pre> /data/cluster1 *(rw,sync,no_subtree_check,all_squash) /data/cluster2 *(rw,sync,no_subtree_check,all_squash) </pre>

バックアップサーバーのディレクトリレイアウトに関する情報。

バックアップを簡素化するために、バックアップサーバーに次のディレクトリレイアウトを使用することをお勧めします。

Catalyst Center

`cluster1` : `/data/automation/cluster1`

Catalyst Center

- `cluster1` : `/data/automation/cluster1`
- `cluster2` : `/data/automation/cluster2`

バックアップストレージ要件に関する情報。バックアップには、**Assurance** データと自動化データの必要な保存期間をカバーするのに十分な外部ストレージを割り当てる必要があります。

Catalyst Center は、外部 **NFS** の場所に **Assurance** と自動化データのバックアップコピーを保存します。バックアップには、必要な保存期間をカバーするのに十分な外部ストレージを割り当てる必要があります。次のストレージを推奨します。

マシンプロファイル	マシン プロファイル エイリアス	シスコ製品番号	NFS ストレージ (14 日単位で増分)	自動化データストレージ (NFS サーバー上で日次でフル)
medium	medium	第 2 世代アプライアンス : • DN2-HW-APL • DN2-HW-APL-U (プロモーション)	1.7 TB	50 GB
		第 3 世代アプライアンス : DN3-HW-APL		
t2_large	large	第 2 世代アプライアンス : • DN2-HW-APL-L • DN2-HW-APL-L-U (プロモーション)	3 TB	100 GB
		第 3 世代アプライアンス : DN3-HW-APL-L		
t2_2xlarge	extra large	第 2 世代アプライアンス : • DN2-HW-APL-XL • DN2-HW-APL-XL-U (プロモーション)	8.4 TB	300 GB
		第 3 世代アプライアンス : DN3-HW-APL-XL		

サーバーをバックアップするための帯域幅と遅延の要件について説明します。

Catalyst Center サーバーをバックアップするために、特定の帯域幅と遅延が必要です。これらの表を使用して、各アプライアンスプロファイルのバックアップの転送にかかる時間を推定します（バックアップの生成にかかった時間を除く）。推定値には、すべてのデータの最初のバックアップ時間が表示されます。以降の増分バックアップは時間が短縮されます。

「NFS マウント書き込み」速度を確認するには、**Catalyst Center** シェルに `magctl disk check -d /data/nfs -c 4096` と入力します。3 ノードの HA クラスタがある場合は、**Catalyst Center** で NFS を設定した後、各ノードでコマンドを入力します。

アプライアンスプロファイル	データベースサイズ	NFS マウントの書き込み速度	帯域幅	転送時間
Medium	50 GB	100 ~ 125 MB/秒	1 Gbps	7 分
Medium	50 GB	1000 ~ 1250 MB/秒	10 Gbps	1 分

アプライアンスプロファイル	データベースサイズ	NFS マウントの書き込み速度	帯域幅	転送時間
Large	100 GB	100 ～ 125 MB/秒	1 Gbps	13 分
Large	100 GB	1000 ～ 1250 MB/秒	10 Gbps	2 分
Extra large	300 GB	100 ～ 125 MB/秒	1 Gbps	42 分
Extra large	300 GB	1000 ～ 1250 MB/秒	10 Gbps	4 分

アプライアンスプロファイル	すべてのデータのバックアップサイズ	NFS マウントの書き込み速度	帯域幅	転送時間
Medium	1.75 TB	100 ～ 125 MB/秒	1 Gbps	4 時間
Medium	1.75 TB	1000 ～ 1250 MB/秒	10 Gbps	25 minutes
Large	3.1 TB	100 ～ 125 MB/秒	1 Gbps	7 時間
Large	3.1 TB	1000 ～ 1250 MB/秒	10 Gbps	43 分
Extra large	8.69 TB	100 ～ 125 MB/秒	1 Gbps	20 時間
Extra large	8.69 TB	1000 ～ 1250 MB/秒	10 Gbps	2 時間

Linux および Windows ベースの NFS をセットアップする方法について説明します。

ファイル共有を使用する必要があるユースケースはいくつかあります。以下に例を示します。

- バックアップや復元操作の完了
- リモートでの **Catalyst Center** のインストール
- **RCA** ログバンドルを保存するためのリポジトリの作成

このセクションのトピックでは、Linux ベースと Windows ベースの両方の NFS をセットアップする方法について説明します。

Linux NFS

このトピックでは、Ubuntu および Red Hat Linux ディストリビューションで NFS ファイル共有を設定する方法について説明します。

このセクションでは、Ubuntu および Red Hat Linux ディストリビューションで NFS ファイル共有を設定する方法について説明します。

 注

VMware VM を設定する場合は、10G サポートと低オーバーヘッドを提供する [vmxnet] ドライバを使用することを推奨します。

Ubuntu

Ubuntu ディストリビューションでのファイル共有の設定方法を学習します。

Ubuntu ディストリビューションでファイル共有を設定するには、以下で詳しく説明されている手順を実行します。

1. NFS パッケージをインストールします。 **apt-get install -y nfs-kernel-server**
2. NFS サービスを有効にして起動します。

```
systemctl enable nfs-server
systemctl start nfs-server
```

3. NFS サービスが有効になっていて、開始されていることを確認します（これはデフォルトで実行されます）。 **systemctl status nfs-kernel-server**

結果の出力は次の例のようになります。

```
nfs-server.service - NFS server and services
Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset:
       enabled)
Active: active (exited) since Sun 2020-03-22 15:35:12 UTC; 18min ago
Main PID: 19253 (code=exited, status=0/SUCCESS)
Tasks: 0 (limit: 4915)
CGroup: /system.slice/nfs-server.service
Mar 22 15:35:12 k8smaster systemd[1]: Starting NFS server and services...
Mar 22 15:35:12 k8smaster systemd[1]: Started NFS server and services.
```

4. 次のタスクを完了して、NFS エクスポートを設定します。

- a. NFS ファイル共有ディレクトリを設定します。

```
sudo mkdir -p /srv/nfs
sudo chmod 755 -R /srv/nfs/
sudo chown -R nobody:nobody /srv/nfs/
```

- b. **/etc/exports** ファイルに NFS ファイル共有エントリを追加します。

- ファイルを開きます。 **sudo vim /etc/exports**
- 次の行を追加します。 **/srv/nfs *(rw,sync,no_subtree_check,all_squash)**

- c. NFS ファイル共有をエクスポートします。 **sudo exportfs -rv**

次のメッセージが表示されます。 exporting */srv/nfs

- d. NFS エクスポートを確認します。

NFS ファイル共有の可用性を確認するには、別の Linux マシンから **showmount -e NFS-server-IP-address** コマンドを入力します。結果の出力は次の例のようになります。

```
Export list for NFS-server-IP-address:
/srv/nfs *
```

5. NFS を許可するファイアウォールルールを設定します。

- a. ファイアウォールが有効になっているかどうかを確認します（ステータスは active です）。**sudo ufw status**

デフォルトの Ubuntu/Debian ディストリビューションでは、ファイアウォールが無効になっています。必要に応じて、この手順を完了する前にファイアウォールを有効にしてください。

- b. mountd 用の静的ポートを設定します。

- **/etc/default/nfs-kernel-server** ファイルを開きます。
- **RPCMOUNTDOPTS="--manage-gids** 行を見つけます。
- この行の末尾にスペースと **--port 32767** を追加します。

- c. 次の行を **/etc/services** ファイルに追加して、mountd ポートを追加します。

```
mountd 32767/tcp
mountd 32767/udp
```

- d. NFS サービスを再起動します。**sudo systemctl restart nfs-kernel-server nfs-mountd portmap**

- e. NFS を許可するファイアウォールルールを追加します。

```
sudo ufw allow portmapper
sudo ufw allow nfs
sudo ufw allow mountd
```

Red Hat CentOS

Red Hat または CentOS ディストリビューションでのファイル共有の設定方法について学びます。

Red Hat または CentOS ディストリビューションでファイル共有を設定するには、以下で詳しく説明されている手順を実行します。

-
1. NFS パッケージをインストールします。**yum install -y nfs-utils**
 2. NFS サービスを有効にして起動します。

```
systemctl enable nfs-server
systemctl start nfs-server
```

3. サービスのステータスを確認します。**systemctl status nfs-server**

結果の出力は次の例のようになります。

```
nfs-server.service - NFS server and services
Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; vendor
preset: disabled)
Active: active (exited) since Sun 2020-03-22 12:14:30 EDT; 2s ago
Process: 10418 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then
systemctl reload gssproxy ; fi (code=exited, status=0/SUCCESS)
Process: 10404 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
Process: 10402 ExecStartPre=/usr/sbin/exportfs -r (code=exited,
status=0/SUCCESS)
Main PID: 10418 (code=exited, status=0/SUCCESS)
Mar 22 12:14:30 cene8.ecrt.local systemd[1]: Starting NFS server and
services...
Mar 22 12:14:30 cene8.ecrt.local systemd[1]: Started NFS server and services.
```

4. 次のタスクを完了して、NFS エクスポートを設定します。

a. NFS ファイル共有ディレクトリを設定します。

```
sudo mkdir -p /srv/nfs
sudo chmod 755 -R /srv/nfs/
sudo chown -R nobody:nobody /srv/nfs/
```

b. /etc/exports ファイルに NFS ファイル共有エントリを追加します。

- ファイルを開きます。 **sudo vim /etc/exports**
- 次の行を追加します。 **/srv/nfs *(rw,sync,no_subtree_check,all_squash)**

c. NFS ファイル共有をエクスポートします。 **sudo exportfs -rv**

次のメッセージが表示されます。 **exporting */srv/nfs**

d. NFS エクスポートを確認します。

NFS ファイル共有の可用性を確認するには、別の Linux マシンから **showmount -e NFS-server-IP-address** コマンドを入力します。結果の出力は次の例のようになります。

```
Export list for NFS-server-IP-address:
/srv/nfs *
```

e. mountd ポートが **nfs.conf** ファイルで設定されているかどうかを確認します。 **grep -A2 mountd /etc/nfs.conf**

結果の出力が次のようになっている場合は、**mountd** ポートを設定する必要があります。

```
# [mountd]
# debug=0
# manage-gids=n
```

この場合、**nfs.conf** ファイルに次の行を追加します。

```
[mountd]
manage-gids = 1
port = 20048
```

f. NFS サービスを再起動します。 **sudo systemctl restart nfs-server rpcbind nfs-mountd**

Red Hat/CentOS バージョン 7 以降では、デフォルトでファイアウォール (**firewalld** サービスによって管理) が有効になっています (以前のバージョンでは **iptables** を使用)。サーバー上で NFS が実行

されている場合、ファイル共有アクセスが阻止されます。外部クライアントから、**showmount -e NFS-server-IP-address** コマンドを入力します。結果の出力は次の例のようになります。

```
clnt_create: RPC: Port mapper failure - Unable to receive: errno 113 (No route to host)
```

5. NFS を許可するファイアウォールルールを追加します。

```
firewall-cmd --permanent --add-service={nfs, rpc-bind, mountd}
firewall-cmd --reload
```

6. NFS 用に SELinux を設定します。



Red Hat および CentOS ディストリビューションでは、SELinux がデフォルトで有効になっています。

- a. NFS の読み取り/書き込み boolean オプションを有効にします。

実行する操作	結果...
読み取り専用の NFS エクスポートを有効にする	setsebool -P nfs_export_all_ro 1 コマンドを入力します。
読み取り/書き込み NFS エクスポートを有効にする	次のコマンドを入力します。 • setsebool nfsd_anon_write on • setsebool -P nfs_export_all_rw 0

- b. boolean が設定されていることを確認します。

```
getsebool -a |grep nfs_expo
nfs_export_all_ro --> on
nfs_export_all_rw --> off
```

- c. NFS ディレクトリに SELinux コンテキストを設定します。

```
semanage fcontext -a -t public_content_rw_t "/srv/nfs(/.*)?"
restorecon -Rv /srv/nfs/
```

Windows NFS

Windows ベースの NFS ファイル共有の設定方法について説明します。

Catalyst Center デプロイ用の Windows ベースの NFS ファイル共有を設定するには、次の手順を実行します。

1. サーバーマネージャを開始します。

2. NFS サービスをインストールします。

- a) **[Manage] > [Add Roles and Features]**を選択して、**[Add Roles and Features]** ウィザードを開始します。
- b) **[Next]** を 3 回クリックして、**[Before You Begin]**、**[Installation Type]**、**[Server Selection]** ウィザード画面をスキップします。
- c) **[Server Roles]** ウィザード画面で、**[Server for NFS]** チェックボックスをオンにして、**[Next]** をクリックします。
- d) **[Features]** ウィザード画面で、**[Services for Network File System Management]** チェックボックスをオンにして、**[Next]** をクリックします。
- e) **[Confirmation]** ウィザード画面で、選択したオプションが表示されていることを確認します。
- f) **[Install]** をクリックします。

3. [New Share] ウィザードを開始します。

- a) サーバーマネージャのナビゲーションウィンドウで、**[File and Storage Services]** をクリックします。
[File and Storage Services] ページが開きます。
- b) このページのナビゲーションウィンドウで、**[Shares]** をクリックします。
- c) **[Tasks]** をクリックしてから、**[New Share]** を選択します。
[New Share] ウィザードが表示されます。

4. [New Share] ウィザードを完了します。

- a) **[Select the profile for this share]** ウィザード画面で、**[NFS Share - Advanced]** プロファイルをクリックし、**[Next]** をクリックします。
- b) **[Select the server and path for this share]** ウィザード画面で、ファイル共有を配置する場所を指定し、**[Next]** をクリックします。

問題	結果
共有を [Shares] ディレクトリ内のフォルダ内の専用ディスクまたはパーティションに配置する場合	1. [Select by volume] オプションボタンをクリックします。 2. 使用するディスクまたはパーティションをクリックします。
共有が配置される場所に移動する場合	1. [Type a custom path] オプションボタンをクリックします。 2. テキストフィールドをクリックして、[Select Folder] ダイアログボックスを開きます。 3. 共有を配置するフォルダに移動します。 4. [Select Folder] をクリックします。

- c) **[Specify share name]** ウィザード画面で、共有の名前を入力し、**[Next]** をクリックします。
- d) **[Specify authentication methods]** ウィザード画面で、次のオプションを選択し、**[Next]** をクリックします。
 - **[No server authentication (AUTH/SYS)]**
 - **[Enable unmapped user access]**
 - **[Allow unmapped user access by UID/GID]**
- e) **[Specify the share permissions]** ウィザード画面で、**[Add]** をクリックします。
- f) **[Add Permissions]** ダイアログボックスで、次のタスクを完了し、**[Next]** をクリックします。

1. **[Add]** をクリックします。
 2. この共有にアクセスできるホスト、クライアントグループ、またはネットグループを設定します。
 3. **[Share permissions]** ドロップダウンリストで、**[Read/Write]** を選択します。
 4. **[Allow root access (not recommended)]** チェックボックスをオフのままにします。
- g) **[Permissions]** ウィザード画面で、次のタスクを完了し、**[Next]** をクリックします。
1. **[Customize permissions]** をクリックして、**[Advanced Security Settings for share-name]** ダイアログボックスを開きます。
 2. **[Add]** をクリックして、**[Permission Entry for share-name]** ダイアログボックスを開きます。
 3. **[Select a principal]** リンクをクリックして、**[Select User, Computer, Service Account, or Group]** ダイアログボックスを開きます。
 4. 最後のテキストボックスに、**[Everyone]** を入力してから、**[Check Names]** をクリックします。**[Everyone]** が表示されたら、**[OK]** をクリックします。
 5. **[Basic permissions]** エリアで、使用可能なオプション (**[Full control]** を含む) をすべて選択してから、**[OK]** をクリックします。
 6. **[Anonymous LOGON]** ユーザーに対して、前の 2 つの手順を繰り返します。
- h) **[Next]** を 2 回クリックして、**[Management Properties]** および **[Quota]** ウィザード画面をスキップします。
- i) **[Confirmation]** ウィザード画面で、**[Create]** をクリックします。
5. Windows NFS サーバーを保護します。
- a) サーバーマネージャのメインメニューで、**[Tools] > [Windows Firewall with Advanced Security]** の順に選択します。
 - b) **[Inbound Rules]** テーブルには、2 つの **[Server for NFS]** サービス (NFS-TCP-in と NFS-UDP-in) があります。両方のサービスで次のタスクを完了します。
 1. サービスをダブルクリックして、**[Properties]** ダイアログボックスを開きます。
 2. **[Scope]** タブをクリックします。
 3. **[Remote IP address]** セクションでは、Catalyst Center 用に設定された IP アドレス (Windows NFS サーバーとインターフェイスで接続する NIC の VIP を含む) を入力して、ホストアクセスを制限します。
 4. **[OK]** をクリックします。

NFS

Catalyst Center では、バックアップ用に複数のネットワーク ファイル システム (NFS) サーバーを追加できます。

バックアップ操作に使用できる NFS サーバーを追加するには、次の手順を実行します。

1. メインメニューから次を選択します。 **[System] > [Settings] > [Backup Configuration]** の順に選択します。

2. [Add NFS] をクリックします。
3. [Add NFS] スライドインペインで、次の手順を実行します。
 - a) それぞれのフィールドに [Server Host] と [Source Path] を入力します。
 - b) ドロップダウンリストから [NFS Version] を選択します。
 - c) [Port] はデフォルトで追加されます。このフィールドは空のままにもできます。
 - d) (オプション) [Port Mapper] 番号を入力します。
 - e) [Save] をクリックします。
4. [View NFS List] をクリックして、使用可能な NFS サーバーを表示します。
[NFS スライドインペイン] には、NFS サーバーのリストが詳細とともに表示されます。
5. [NFS スライドインペイン] で [Actions] の下にある省略記号をクリックして、NFS サーバーを削除します。



進行中のバックアップジョブがない場合にのみ、NFS サーバーを削除できます。

バックアップ用に追加した NFS サーバーを設定します。詳細については、[バックアップファイルを保存する場所の設定](#) (238ページ) を参照してください。

自動化と Assurance データのバックアップを設定する方法を説明します。

Catalyst Center では、自動化と Assurance データのバックアップを設定できます。

バックアップファイルの保存場所を設定するには、次の手順を実行します。

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。
- データバックアップサーバーが [バックアップサーバーの要件](#) (228ページ) で説明されている要件を満たしている。

1. メインメニューから次を選択します。[System] > [Backup and Restore] の順に選択します。
次のウィンドウを表示できます。

System / Backup & Restore



Backup & Restore

Backup and restore capabilities have not been configured.

[Configure Settings](#)

2. **[Configure Settings]** をクリックします。

または **[System] > [Settings] > [System Configuration] > [Backup Configuration]** の順に選択します。

3. **[Physical Disk]** または **[NFS]** サーバーオプションを選択します。

System / Settings

[Settings](#) / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed in the Administrator Guide. [Backup Server Requirements](#)

☒ Physical Disk ☐ Network File System (NFS)

Mount Path*

mks-managed-c123r1frjb-err837q0hc



Encryption Passphrase*

Confirm Passphrase*

Backup Retention (in number of backups)*

14

[More Information](#)

Reset

Submit

- [Physical Disk]** : Catalyst Center は、Assurance のバックアップコピーと自動化データを保存するため、外部ディスクを仮想マシンにマウントするオプションを提供します。物理ディスクを設定するには、**[Physical Disk]** オプションボタンをクリックし、次の設定を定義します。

 注

物理ディスクオプションは、単一ノード仮想マシンでのみサポートされます。

フィールド	説明
Mount Path	外部ディスクの場所。
Encryption Passphrase	バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用するパスフレーズ。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。 このパスフレーズは必須で、バックアップファイルを復元するときに入力求められます。このパスフレーズがなければ、バックアップファイルは復元されません。 パスフレーズを設定した後にパスフレーズを変更する場合は、[Update Passphrase] をクリックします。
Backup Retention	データを保持するバックアップ数。 指定したバックアップ数より古いデータは削除されます。

5. **[NFS] : Catalyst Center** はバックアップファイルを作成して、リモート **NFS** サーバーにポストします。リモートサーバーの要件の詳細については、[バックアップサーバーの要件](#) (228ページ) を参照してください。**NFS** バックアップサーバーを設定するには、**[NFS]** オプションボタンをクリックして次の設定を定義します。

フィールド	説明
Mount Path	リモートサーバーの場所。
Encryption Passphrase	バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用するパスフレーズ。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。 このパスフレーズは必須で、バックアップファイルを復元するときに入力求められます。このパスフレーズがなければ、バックアップファイルは復元されません。 パスフレーズを設定した後にパスフレーズを変更する場合は、[Update Passphrase] をクリックします。
Backup Retention	データを保持するバックアップ数。 指定したバックアップ数より古いデータは削除されます。

6. **[Submit]** をクリックします。

要求が送信されると、**[System] > [Backup & Restore]** で、設定された物理ディスクまたは **NFS** サーバーを表示できます。

SSH

自動化専用バックアップ用にリモート SSH サーバーを追加します。

次の手順を使用して、自動化専用バックアップ用にリモートサーバーを設定します。

注

リモート バック アップサーバーのサポートは、自動化専用バックアップで利用できます。

1. メインメニューから次を選択します。[**System**] > [**System Configuration**] > [**Backup Configuration**] の順に選択します。
2. [**Backup Configuration**] ページで、[SSH (Remote Server)] を選択し、[Add SSH] をクリックします。
3. [**Add SSH**] スライドインペインで、リモート SSH サーバーの詳細を入力し、[Save] をクリックします。
 - a) [SSH IP Address] フィールドにサーバーの IP アドレスを入力します。
 - b) [SSH Port] フィールドに、SSH ポート番号を入力します。
 - c) [Username] フィールドに、サーバーのユーザー名を入力します。
 - d) [Password] フィールドに、サーバーのパスワードを入力します。
 - e) [Server Path] フィールドに、バックアップディレクトリパスを入力します。
4. [**Backup Configuration**] ページで、[View SSH List] をクリックして、サーバーが正常に追加されたことを確認します。

[SSH List] スライドインペインには、追加されたサーバーとその詳細が表示されます。
5. [**Backup Configuration**] ページで、次の手順にしたがって、バックアップストレージのサーバーパスを設定します。
 - a) [Refresh] をクリックします。
 - b) [Server Path] ドロップダウンリストからサーバーパスを選択します。
 - c) [Submit] をクリックします。

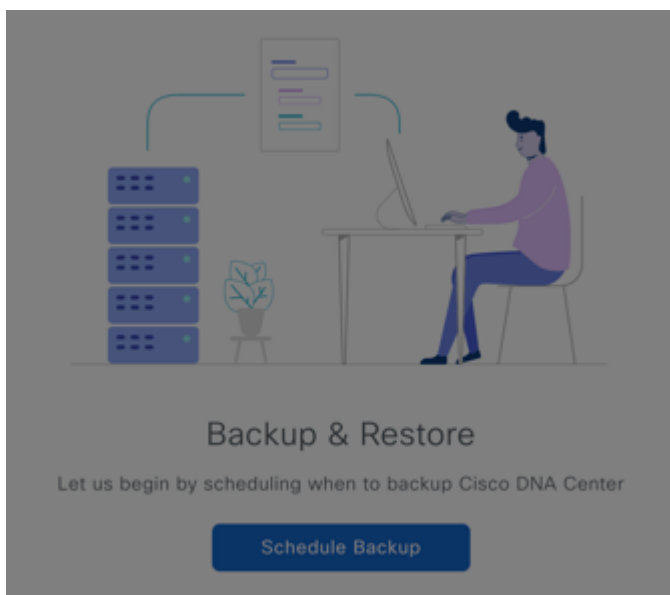
リモート SSH サーバーが設定され、自動化専用バックアップに使用できるようになります。

バックアップのためのアプライアンスの準備に必要な手順を説明します。

アプライアンスのバックアップを作成するには、次の手順を使用します。

バックアップの場所を設定する必要があります。詳細については、[バックアップファイルを保存する場所の設定](#) (238ページ) を参照してください。

1. メインメニューから次を選択します。 **[System] > [Backup & Restore]** の順に選択します。
2. **[Schedule Backup]** をクリックします。



[Schedule Backup] スライドインペインが開きます。

Schedule Backup
×

Backup Name*

Schedule Type

☒ Backup now

☐ Schedule backup daily

☐ Schedule backup weekly

Scope

☐ Cisco Catalyst Center (All data) ⓘ

☐ Cisco Catalyst Center (Without assurance data) ⓘ

[Schedule Backup] スライドインペインで、次の手順を実行します。

- a. バックアップの一意的な名前を入力します。
- b. **[Schedule Type]** エリアで次のオプションのいずれかを選択します。
 - **[Backup Now]** : すぐにバックアップを作成します。
 - **[Schedule Backup Daily]** : 日次ベースのバックアップをスケジュールします。
 - **[Schedule Backup Weekly]** : 週次ベースのバックアップをスケジュールします。
- c. **[Scope]** エリアで次のオプションのいずれかを選択します。

- **[Cisco Catalyst Center (All Data)]** : 自動化と Assurance データのバックアップを作成するには、このオプションを選択します。
- **[Cisco Catalyst Center (Without Assurance Data)]** : 自動化データのバックアップのみを作成するには、このオプションを選択します。

d. **[Save]** をクリックします。

3. **Catalyst Center** がバックアッププロセスを開始します。バックアップのエントリが **[Backup & Restore]** ウィンドウに追加されます。

Backup & Restore ⓘ

[View Activities](#) [View Settings](#)

NUMBER OF BACKUPS

0 0 1
Success Failed In progress

DISK USAGE ⓘ

1.5 TB 200 MB ⓘ
Available Used

Q Search Table

[+ Schedule Backup](#) [Delete All](#)

Status **All** In Progress Success Failed

Backup Name	File Size	Version	Status	Scope	Is Compatible ⓘ	Created Date ▾
EFT-Backup		1.3.2 ⓘ	Creating 20.45%	Cisco Catalyst Center (All data)		Wed Mar 13, 2024 01:40 PM

バックアップが完了すると、ステータスが **[Creating]** から **[Success]** に変わります。

Backup & Restore ⓘ

[View Activities](#) [View Settings](#)

NUMBER OF BACKUPS

1 0 0
Success Failed In progress

DISK USAGE ⓘ

1.5 TB 200 MB ⓘ
Available Used

Q Search Table

[+ Schedule Backup](#) [Delete All](#)

Status **All** In Progress Success Failed

Backup Name	File Size	Version	Status	Scope	Is Compatible ⓘ	Created Date ▾
EFT-Backup	196.7 MB	1.3.2 ⓘ	Success	Cisco Catalyst Center (All data)	✓ ⓘ	Wed Mar 13, 2024 01:40 PM

定期的なバックアップをスケジュールし、実行する曜日と時間を定義する方法を説明します。

次の要件が満たされていることを確認します。

- **SUPER-ADMIN-ROLE** 権限を持つユーザのみがこの手順を実行することができます。
- データバックアップサーバーが **バックアップサーバーの要件** (228ページ) で説明されている要件を満たしている。

- バックアップサーバーが **Catalyst Center** で設定されている。詳細については、[バックアップファイルを保存する場所の設定](#)（238ページ）を参照してください。

1. メインメニューから次を選択します。[**System**] > [**Backup & Restore**] の順に選択します。
[**Backup & Restore**] ウィンドウが表示されます。
2. [**Schedule Backup**] をクリックします。

注

進行中のバックアップジョブがない場合にのみ、新しいバックアップをスケジュールできます。

Backup & Restore

[View Activities](#) [View Settings](#)

NUMBER OF BACKUPS

1 0 0
Success Failed In progress

DISK USAGE

1.5 TB 200 MB
Available Used

Search Table

[Schedule Backup](#) [Delete All](#)

Status [All](#) [In Progress](#) [Success](#) [Failed](#)

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date
EFT-Backup	196.7 MB	1.3.2	Success	Cisco Catalyst Center (All data)	Yes	Wed Mar 13, 2024 01:40 PM

3. [**Schedule Backup**] スライドインペインで、次の手順を実行します。
 - a. [**Backup Name**] フィールドで、バックアップの一意の名前を入力します。
 - b. スケジュールオプションを選択します。
 - [**Schedule Backup Daily**] : 日次バックアップジョブをスケジュールするには、バックアップを実行する時刻を選択します。
 - [**Schedule Backup Weekly**] : 週次バックアップジョブをスケジュールするには、バックアップを実行する曜日と時刻を選択します。
 - c. バックアップの範囲を定義します。
 - [**Cisco Catalyst Center (All data)**] : このオプションを使用すると、システム管理者は自動化、Assurance、システム固有のセットのバックアップを作成できます。
 - [**Cisco Catalyst Center (without Assurance data)**] : このオプションを使用すると、管理者は自動化およびシステム固有のセットのバックアップを作成できます。
 - d. [**Save**] をクリックします。

[**Backup & Restore**] ウィンドウには、バックアップがスケジュールされている日時を示すバナーメッセージが表示されます。

4. オプション: [**View Upcoming Backups**] をクリックすると、今後のスケジュールを変更できます。スライドインペインの [**Upcoming Schedules**] でスケジュールされた日時にバックアップを実行しない場合は、トグルボタンをクリックして特定のスケジュールを無効にします。

5. オプション: スケジュールを編集するには、[Edit Schedule] をクリックします。
6. オプション: スケジュールを削除するには、[Delete Schedule] をクリックします。
7. バックアップが開始されると、[Backup & Restore] ウィンドウにバックアップが表示されます。バックアップ名をクリックすると、実行された手順のリストが表示されます。

または、[Backup & Restore] ウィンドウの左上にある [View Activities] をクリックしてから、[Execution ID] をクリックすることもできます。[Create Backup Details] スライドインペインが開き、実行された手順のリストが表示されます。

8. [Backup & Restore] ウィンドウで [In Progress]、[Success]、または [Failure] タブをクリックすると、バックアップのリストをステータスが [In Progress]、[Success]、または [Failure] のタスクのみをフィルタリングして表示できます。

バックアッププロセス中は、Catalyst Center によりバックアップデータベースおよびファイルが作成されます。バックアップファイルは指定された場所に保存されます。バックアップファイルは単一のセットに限らず、一意の名前で識別される複数のバックアップファイルを作成できます。プロセスが完了すると、バックアップジョブのステータスが [In Progress] から [Success] に変わります。

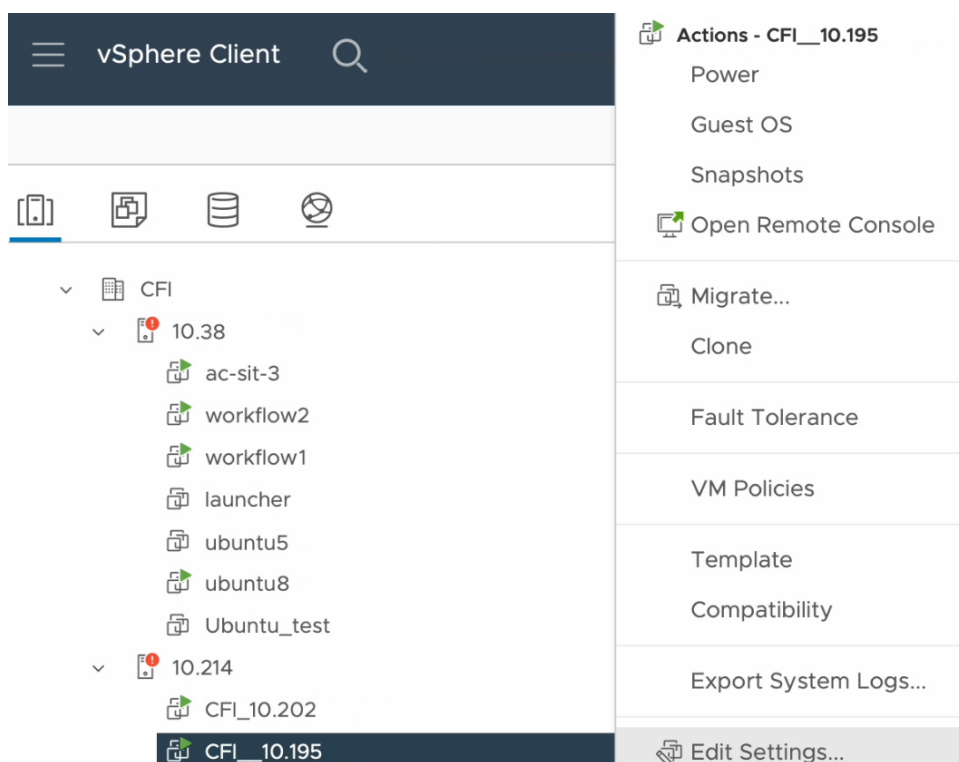
注

バックアッププロセスが失敗しても、アプライアンスまたはそのデータベースへの影響はありません。バックアップの失敗の最も一般的な原因は、ディスク領域の不足です。バックアッププロセスが失敗した場合は、リモートサーバーに十分なディスク容量があるかどうかを確認し、別のバックアップを試行します。

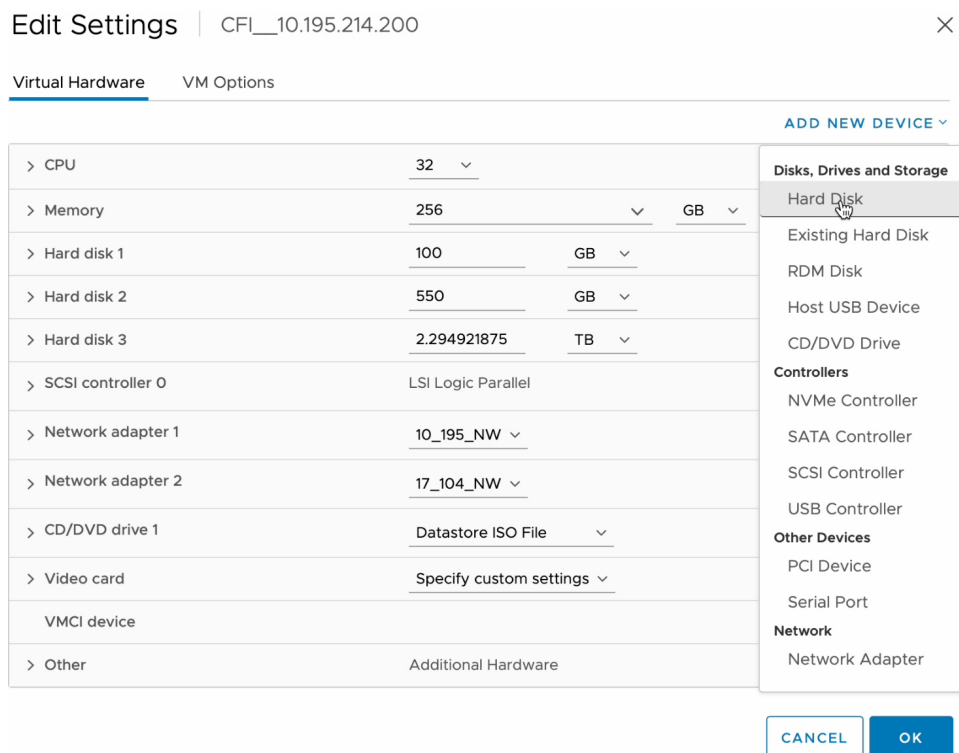
バックアップ復元用の物理ディスクを追加する方法を詳しく説明します。

Catalyst Center on ESXi 専用のバックアップと復元操作に使用できる物理ディスクを追加するには、次の手順を実行します。

1. **sudo shutdown** コマンドを使用してコンソールセッションからシャットダウンして、Catalyst Center on ESXi 仮想アプライアンスの電源をオフにします。
2. VMware vSphere にログインし、電源がオフになっていることを確認します。
3. vSphere クライアントの左側のペインで、ESXi ホストを右クリックし、[Edit Settings] を選択します。



4. [Edit Settings] ダイアログボックスで [Add New Device] をクリックし、[Hard Disk] を選択します。



5. [New Hard disk] フィールドに、目的のストレージサイズを入力します。

Edit Settings
CFI_10.195.214.200

Virtual Hardware
VM Options

ADD NEW DEVICE

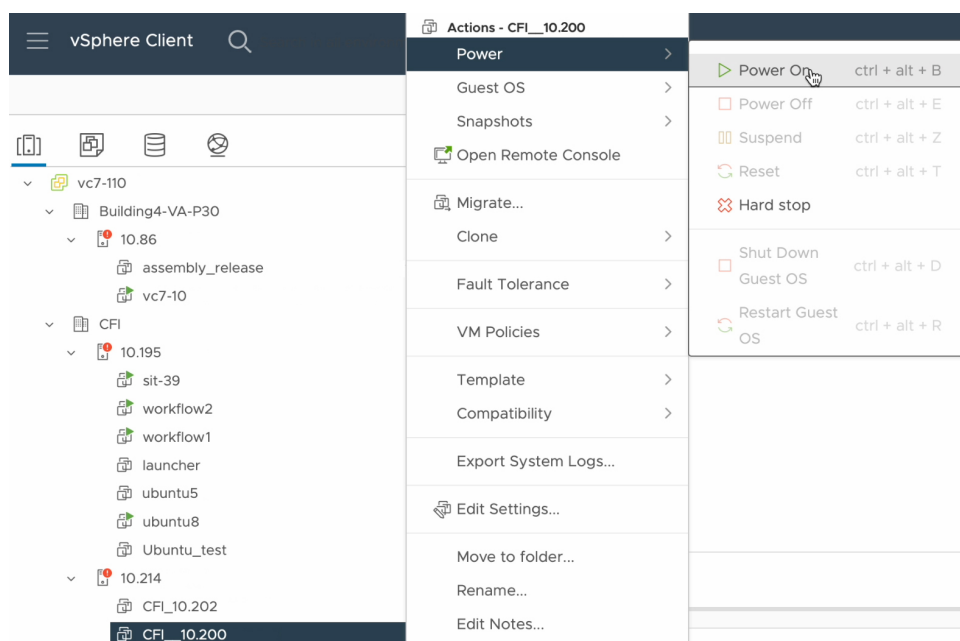
> CPU	32		
> Memory	256		GB
> Hard disk 1	100	GB	
> Hard disk 2	550	GB	
> Hard disk 3	2.294921875	TB	
> New Hard disk *	125	GB	
> SCSI controller 0	LSI Logic Parallel		
> Network adapter 1	10_195_NW		☒ Connect...
> Network adapter 2	17_104_NW		☒ Connect...
> CD/DVD drive 1	Datastore ISO File		☒ Connect...
> Video card	Specify custom settings		
VMCI device			
> Other	Additional Hardware		

CANCEL
OK

注

バックアップに推奨されるストレージ容量の詳細については、「[バックアップストレージ要件](#)（229 ページ）」を参照してください。

6. [OK] をクリックします。
7. アプライアンスの仮想マシンの電源をオンにします。



追加した物理ディスクをバックアップ用に設定できます。物理ディスクの設定方法については、「[バックアップファイルを保存する場所の設定 \(238ページ\)](#)」を参照してください。

NFS サーバーからバックアップデータを復元する方法について説明します。

NFS サーバーからバックアップデータを復元するには、この手順を使用します。

⚠ 注意

Catalyst Center の復元プロセスでは、データベースとファイルのみ復元します。復元プロセスでは、ネットワークの状態や、最後のバックアップ以降に加えられた変更は復元されません。これには、新しいネットワークポリシーやパスワード、証明書、トラストプールバンドル、または更新されたこれらのものが含まれます。

次の要件が満たされていることを確認します。

- **SUPER-ADMIN-ROLE** 権限を持つユーザのみがこの手順を実行することができます。
- データを復元する元となるバックアップがあること。

データを復元する場合、**Catalyst Center** はメンテナンスモードに入り、復元プロセスが終わるまで使用できません。**Catalyst Center** を使用不可にできるときにデータを復元してください。

1. メインメニューから次を選択します。 **[System] > [Backup & Restore]** の順に選択します。
作成したバックアップは、**[Backup & Restore]** ウィンドウに表示されます。
2. **[Backup Name]** 列で、復元するバックアップを特定します。
3. **[Actions]** 列で、省略記号をクリックし、**[Restore]** を選択します。

Backup & Restore

[View Activities](#) [View Settings](#) As of: Mar 27, 2024 1:28 PM

NUMBER OF BACKUPS DISK USAGE

Success	Failed	In progress	1.5 TB Available	200 MB Used
1	0	0		

[Schedule Backup](#) [Delete All](#)

Status: **All** | In Progress | Success | Failed

Backup Name	File Size	Version	Status	Scope	Is Compatible	Created Date	Duration	Created By	Actions
EFT-Backup	196.7 MB	1.3.2	Success	Cisco Catalyst Center (All data)		Wed Mar 13, 2024 01:40 PM	13m 40s	admin1	Restore Delete

4. **[Restore Backup]** ダイアログボックスで、バックアップ場所の設定時に使用した暗号化パスフレーズを入力し、**[Restore]** をクリックします。

×

Restore Backup

Encryption Passphrase*

.....

SHOW

Cancel

Restore

アプライアンスがメンテナンスモードになり、復元プロセスを開始します。



Maintenance in progress...

[Show more](#)

Loading...

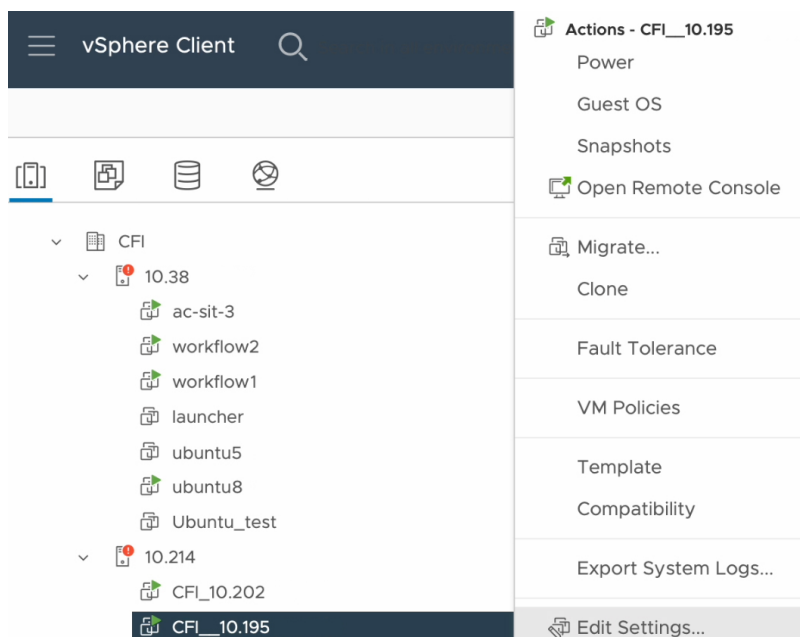
復元操作が完了すると、[Backup & Restore] ウィンドウのテーブルのステータスが [Success] に変更されます。

5. 復元操作が完了したら、[Log In] をクリックして **Catalyst Center** に再度ログインします。
6. 管理者ユーザーのユーザー名とパスワードを入力して、[Login] をクリックします。

物理ディスクを使用した復元操作を行うため、障害のある仮想アプライアンスを準備するのに必要な手順を説明します。

故障または障害が発生した仮想アプライアンスの物理ディスクからデータを復元するには、次の手順を実行します。

1. 新しい仮想アプライアンスで、障害のある仮想アプライアンス用に設定したストレージディスクを使用するように **Catalyst Center** を設定するには、次の手順を実行します。
 - a. アプライアンスの仮想マシンの電源をオフにします。
 - b. **vSphere Client** を開き、左ペインの **Catalyst Center** 仮想マシンを右クリックして [Edit Settings] を選択します。



- c. [Edit Settings] ダイアログボックスで [Add New Device] をクリックし、[Existing Hard Disk] を選択します。

Edit Settings | CFI_10.195

Virtual Hardware VM Options

ADD NEW DEVICE ▾

> CPU	32 ▾	
> Memory	256 ▾	GB ▾
> Hard disk 1	100 ▾	GB ▾
> Hard disk 2	550 ▾	GB ▾
> Hard disk 3	2.294921875 ▾	TB ▾
> SCSI controller 0	LSI Logic Parallel	
> Network adapter 1	10_195_NW ▾	
> Network adapter 2	17_104_NW ▾	
> CD/DVD drive 1	Datastore ISO File ▾	
> Video card	Specify custom settings ▾	
VMCI device		
> Other	Additional Hardware	

Disks, Drives and Storage

- Hard Disk
- Existing Hard Disk
- RDM Disk
- Host USB Device
- CD/DVD Drive

Controllers

- NVMe Controller
- SATA Controller
- SCSI Controller
- USB Controller

Other Devices

- PCI Device
- Serial Port

Network

- Network Adapter

CANCEL OK

- d. [Select File] ダイアログボックスで ESXi ホストをクリックし、作成したストレージディスク (.vmdk) をクリックして [OK] を選択します。

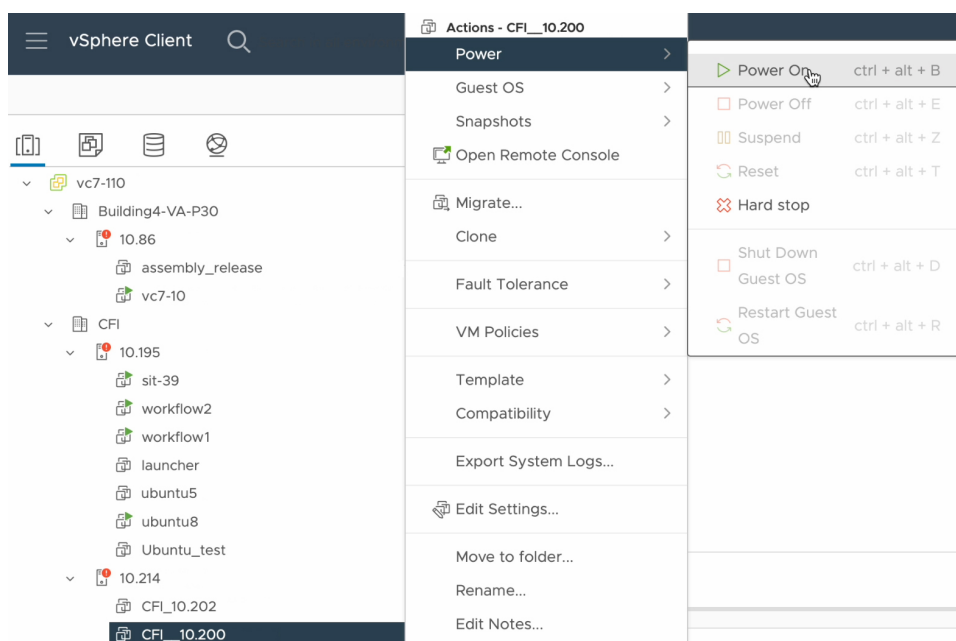
Select File

Datstores	Contents	Information
- ds_214.38 .sdd.sf - CFI_10 CFI_195 - CFI_214 - vmimages	- CFI_195.200.vmdk - CFI_195.200_1.vmdk - CFI_195.200_2.vmdk CFI_195.200_3.vmdk	Name: CFI_195.200_3.vmdk Size: 125 GB Modified: 05/25/2023, 4:42:06 PM Encrypted: No

File Type: Compatible Virtual Disks (*.vmdk, *.dsk, *.raw) ▾

CANCEL OK

- e. アプライアンスの仮想マシンの電源をオンにします。



すべてのサーバーが再起動するには約 45 分かかります。

注

仮想マシンが復旧したら、**magctl appstack status** コマンドを実行してサービスが実行されていることを確認します。

2. バックアップの保管場所を設定するには、次の手順を実行します。

- a) Catalyst Center メニューから、**[System] > [Settings] > [System Configuration] > [Backup Configuration]** の順に選択します。
- b) **[Physical Disk]** ラジオボタンをクリックします。
- c) **[Mount Path]** ドロップダウンリストから物理ディスクを選択します。

System / Settings

[Settings](#) / System Configuration

Backup Configuration

Physical Disk Cisco DNA Center Virtual Appliance provides an option to mount an external disk to the Virtual Machine for Assurance and Automation backups. Note: Physical Disk option is only supported for single node Virtual Machines.

Network File System (NFS) Cisco DNA Center creates the backup files and posts them to a remote server. Each backup is uniquely stored using the UUID as the directory name. For information about the remote server requirements, see Backup Server Requirements listed in the Administrator Guide. [Backup Server Requirements](#)

☒ Physical Disk ☐ Network File System (NFS)

Mount Path*

mks-managed-c123r1frjb-err837q0hc



Encryption Passphrase*

Confirm Passphrase*

Backup Retention (in number of backups)*

14

[More Information](#)

Reset

Submit

- d) バックアップのセキュリティが重要なコンポーネント（証明書やログイン情報など）の暗号化に使用するパスフレーズを入力します。

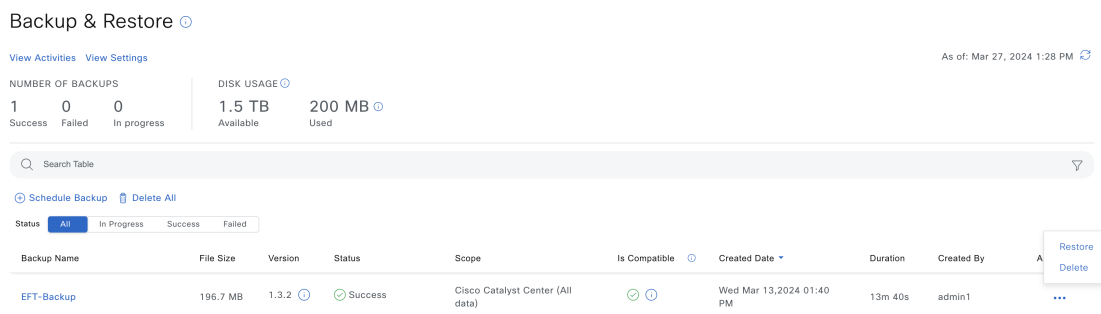
重要

このパスフレーズを忘れないようにしてください。後続の手順でパスフレーズを入力する必要があり、パスフレーズを忘れた場合は作成対象のバックアップを復元することはできません。

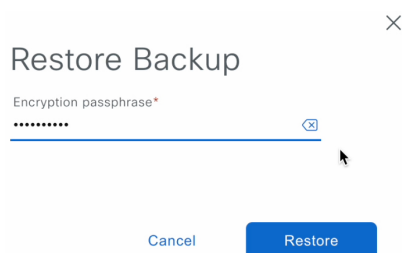
- e) バックアップファイルが削除されるまでの保持期間を設定します。
f) [Submit] をクリックします。

3. バックアップを復元するには、次の手順を実行します。

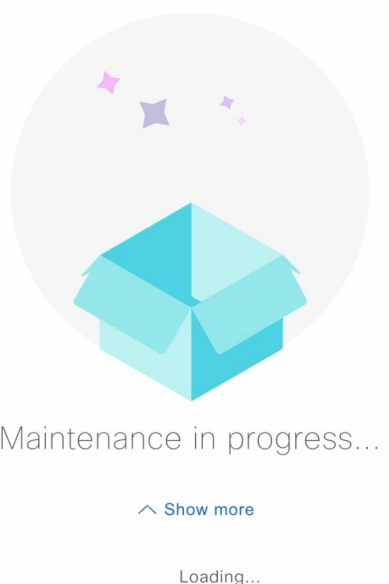
- Catalyst Center メニューから **[System] > [Backup & Restore]** を選択します。
- [Backup & Restore]** ウィンドウでバックアップを見つけ、**[Actions]** 列の下にある省略記号をクリックして **[Restore]** を選択します。



- 前の手順で入力したものと同一暗号化パスフレーズを入力し、**[Restore]** をクリックします。



アプライアンスがメンテナンスモードになり、復元プロセスを開始します。



復元操作が完了すると、**[Backup & Restore]** ウィンドウのステータスが **[Success]** に変更されます。

- 復元操作が完了したら、**[Log In]** をクリックして Catalyst Center に再度ログインします。
- 管理者ユーザーのユーザー名とパスワードを入力して、**[Login]** をクリックします。

第14

章

- :
- □□
 - □□□□
 - □□□□□□□□□□
 - □□□□□□□□□□□□
 - □□□□□□□□□□□□□□
 - □□□□□□□□
 - □□□□□□□□□□
 - □□□□□□□□
 - □□□□□□□□□□□□□□
 - □□□□□□□□□□□□□□
 - □□□□□□□□□□□□□□
 - □□□□□□□□□□□□□□
□□□□□□

ネットワークのダウンタイムから保護するためのディザスタリカバリの導入に関する情報。

Catalyst Center のディザスタリカバリに関する情報。

ディザスタリカバリは、ネットワークのダウンタイムに対する保護策として追加の冗長性レイヤを提供します。クラスタに障害が発生すると、ネットワーク管理作業を接続されたクラスタ（転送先サイト）に移すことで対処します。**Catalyst Center** でのディザスタリカバリの導入は、メインサイト、リカバリサイト、および監視サイトの 3 つのコンポーネントで構成されます。

メインサイトとリカバリサイトは、常にアクティブまたはスタンバイのいずれかの役割を担います。アクティブサイトでネットワークが管理され、アクティブサイトで更新されたデータおよびマネージドサービスの最新のコピーがスタンバイサイトで維持されます。アクティブサイトがダウンすると、**Catalyst Center** で自動的にフェールオーバーが開始され、スタンバイサイトを新しいアクティブサイトにするための必要なタスクが実行されます。

次のトピックでは、運用環境でディザスタリカバリをセットアップして使用方法について説明します。

Catalyst Center でのディザスタリカバリの導入を理解するための主な用語に関する情報。

Catalyst Center でのディザスタリカバリの導入について理解する上で重要な用語を示します。

- **メインサイト**：ディザスタリカバリシステムを設定するときに設定する 1 つ目のサイト。デフォルトでは、ネットワークを管理するアクティブサイトとして動作します。システムでサイトを設定する方法については、[ディザスタリカバリのセットアップ](#)（272 ページ）を参照してください。
- **リカバリサイト**：ディザスタリカバリシステムを設定するときに設定する 2 つ目のサイト。デフォルトでは、システムのスタンバイサイトとして機能します。
- **監視サイト**：ディザスタリカバリシステムを設定するときに設定する 3 つ目のサイト。このサイトは、仮想マシンまたは別のサーバーにあり、データやマネージドサービスの複製には関与しません。このサイトには、現在アクティブなサイトにディザスタリカバリタスクを実行するために必要なクォーラムを割り当てる役割があります。この状況はスプリットブレインイベントと呼ばれ、2 メンバのシステムでサイトが相互に通信できない場合に発生する可能性があります。その場合、両方のサイトがそれぞれアクティブになろうとし、アクティブサイトが 2 つになります。**Catalyst Center** では、アクティブサイトが常に 1 つだけになるように、監視サイトを使用してアクティブサイトとスタンバイサイトを調停します。監視サイトの要件については、[前提条件](#)（263 ページ）を参照してください。
- **登録**：ディザスタリカバリシステムにサイトを追加するには、最初にメインサイトの **VIP** などの情報を提供してシステムに登録する必要があります。リカバリサイトまたは監視サイトを登録する際は、メインサイトの登録時に生成されるトークンも提供する必要があります。詳細については、[ディザスタリカバリのセットアップ](#)（272 ページ）を参照してください。
- **アクティブ設定**：サイトをアクティブサイトとして確立するプロセス。該当するマネージドサービスのポートの公開などのタスクが含まれます。
- **アクティブサイト**：現在ネットワークを管理しているサイト。このサイトのデータは **Catalyst Center** によってスタンバイサイトに継続的に複製されます。
- **スタンバイ設定**：サイトをスタンバイサイトとして確立するプロセス。アクティブサイトのデータの複製の設定やスタンバイサイトのネットワークを管理するサービスの無効化などのタスクが含まれます。
- **スタンバイ準備完了**：分離されたサイトがスタンバイサイトになるための前提条件を満たすと、**Catalyst Center** によってこの状態に移行されます。このサイトをシステムのスタンバイサイトとして確立するには、**[Action]** 領域で **[Rejoin]** をクリックします。
- **スタンバイサイト**：アクティブサイトのデータおよびマネージドサービスの最新のコピーを保持するサイト。アクティブサイトがダウンすると、フェールオーバーが開始され、スタンバイサイトにアクティブサイトの役割が引き継がれます。

注

システムのスタンバイサイトを現在表示していることを示すメッセージが表示されます。アクティブサイトからすべてのディザスタリカバリタスクを開始する必要があります。

- フェールオーバー：Catalyst Center では 2 種類のフェールオーバーがサポートされます。
 - システムトリガー：アクティブサイトがダウンするとすぐに、Catalyst Center でこれを検出し、スタンバイサイトを新しいアクティブサイトとして確立するための必要なタスクが自動的に実行されます。これらのタスクは、イベントタイムラインでモニターできます。
 - 手動：手動でフェールオーバーを開始して現在のスタンバイサイトを新しいアクティブサイトとして指定できます。詳細については、手動フェールオーバーの開始（290ページ）を参照してください。

重要

- フェールオーバー後はアシュアランスが再起動され、新しいアクティブサイトで新規のデータセットが処理されます。アシュアランスデータの履歴は前のアクティブサイトから移行されません。
- フェールオーバー後、Catalyst Center インベントリサービスはデバイスの完全な同期をトリガーします。これには、管理対象のデバイスの数に応じて、数分から数時間かかる場合があります。Catalyst Center の通常スケジュールされたデバイス同期が実行されている場合と同様に、フェールオーバーによってトリガーされたデバイス同期が完了するまで、新しくアクティブ化されたクラスタでデバイスをプロビジョニングすることはできません。
- 分離：フェールオーバーの際に前のアクティブサイトがディザスタリカバリシステムから切り離されます。Catalyst Center のサービスが一時停止され、仮想 IP アドレス（VIP）のアドバタイズが停止します。その状態で、スタンバイサイトを新しいアクティブサイトとして確立するための必要なタスクが Catalyst Center で実行されます。
- 一時停止：システムを構成するサイトを切り離してデータとサービスの複製を停止するために、一時的にディザスタリカバリシステムを停止します。詳細については、ディザスタリカバリシステムの一時停止（286ページ）を参照してください。
- 再参加：フェールオーバーの発生後にスタンバイ準備完了または一時停止状態のサイトをディザスタリカバリシステムに新しいスタンバイサイトとして追加するには、[Disaster Recovery] > [Monitoring] タブの [Action] 領域で [Rejoin] ボタンをクリックします。また、現在一時停止しているディザスタリカバリシステムを再起動する場合もこのボタンをクリックします。
- DR のアクティブ化：システムのアクティブサイトとスタンバイサイトを作成するユーザー始動型の操作。この操作では、クラスタ内通信を設定し、サイトがディザスタリカバリの前提条件を満たしていることを確認し、2 つのサイト間でデータを複製します。
- 登録解除：ディザスタリカバリシステム用に設定した 3 つのサイトを削除するには、[Action] 領域で [Deregister] ボタンをクリックします。前に入力したサイト設定を変更するには、この操作を実行する必要があります。
- 再試行：前に失敗したアクションを再度実行するには、[Action] 領域で [Retry] ボタンをクリックします。
- VIP プロモーション：このオプションを有効にすると、Catalyst Center の展開用に設定されたエンタープライズインターフェイス VIP が、システムのディザスタリカバリ VIP として使用できるように昇格され

ます。詳細については、[メインサイトの登録に関する考慮事項](#)（272ページ）の「VIPの昇格」セクションを参照してください。

Catalyst Center でのデータ複製プロセスに関する情報。

データ レプリケーションプロセスは、ディザスタリカバリシステムのメインサイトとリカバリサイトの間でデータを同期します。データレプリケーションプロセスの期間は、いくつかの要因によって異なります。この要因には、複製するデータの量、ネットワークの有効な帯域幅、メインサイトとリカバリサイト間の遅延などが挙げられます。**Catalyst Center** の展開でディザスタリカバリがアクティブになっている場合、データレプリケーションは、現在アクティブなサイト（ネットワークを管理している）での操作やアプリケーションの使用に影響を与えません。

重要

フェールオーバー後、障害が発生したサイトからのアシュアランスデータは複製されません。新しいアクティブサイトになるサイトでは、新しいセットのアシュアランスデータが収集されます。

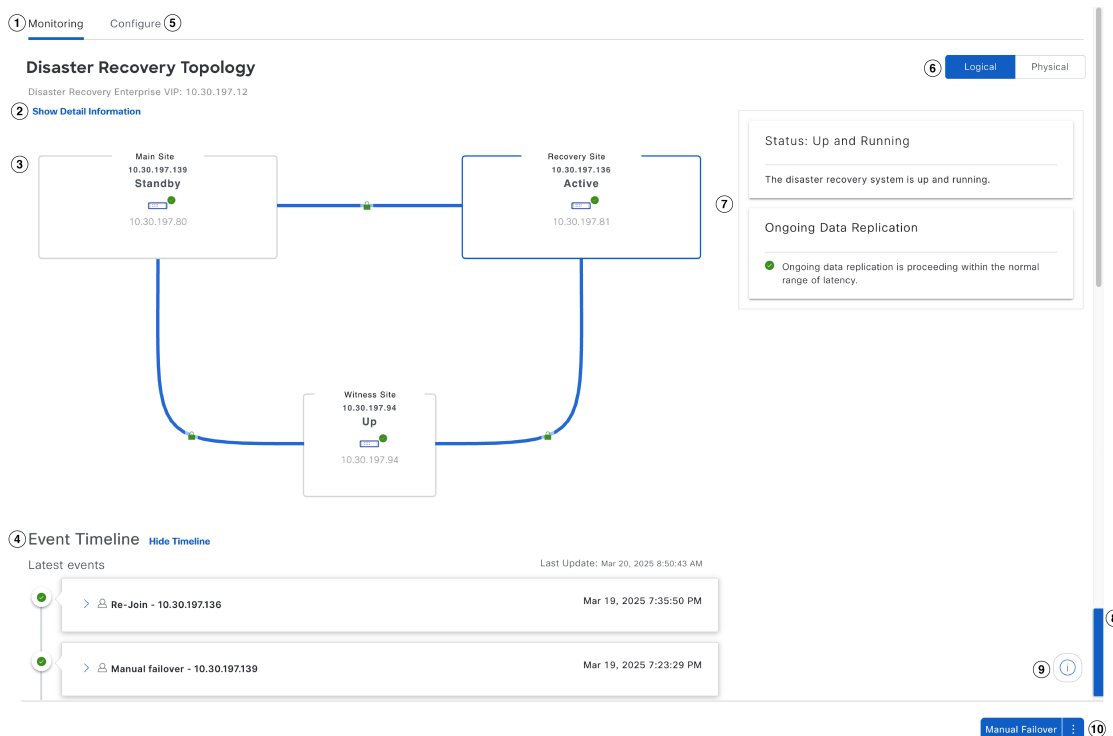
次のシナリオのどれが該当するかに応じて、データの完全レプリケーションまたは増分レプリケーションが実行されます。

- **初期アクティブ化後**：ディザスタリカバリシステムの初期構成とアクティブ化の後で、リカバリサイトにデータがありません。このシナリオでは、メインサイトとリカバリサイトの間でデータの完全なレプリケーションが行われます。
- **フェールオーバー後**：現在アクティブなサイトで障害が発生すると、ディザスタリカバリシステムがフェールオーバーをトリガーします。このシナリオでは、障害が発生したサイトがシステムに再参加した後に、メインサイトとリカバリサイト間でデータの完全なレプリケーションが発生します。
- **通常の操作時**：これは通常の状況でシステムに適用されるシナリオです。日常の運用中に、現在のアクティブサイトで発生した変更は、現在のスタンバイサイトと継続的に同期されます。

GUI

Catalyst Center のディザスタリカバリ GUI のナビゲーションに関する情報。

次の表に、**Catalyst Center** のディザスタリカバリの GUI を構成するコンポーネントとその機能を示します。



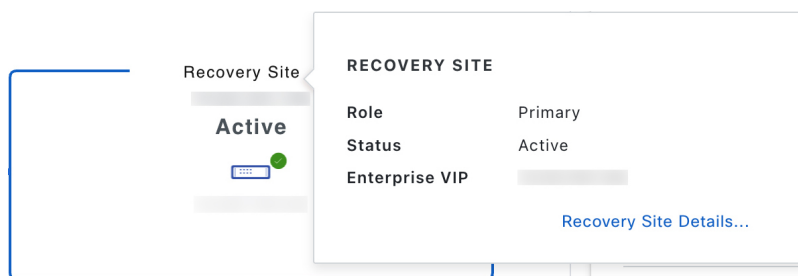
引き出し線	説明
1	[Monitoring] タブ : クリックして次のアクションを実行します。 - システムを構成するサイトのトポロジを表示します。 - システムの現在のステータスを確認します。 - ディザスタリカバリタスクを実行します。 - 現在までに完了しているタスクのリストを表示します。
2	[Show Detail Information] リンク : クリックして、[Disaster Recovery System] スライドインペインを開きます。詳細については、ディザスタリカバリシステムのステータスの表示 (262ページ) を参照してください。
3	[Topology] : サイトとそのメンバーの現在のステータスを示すシステムの論理トポロジまたは物理トポロジが表示されます。 - 論理トポロジと物理トポロジの両方で、青色のボックスは、現在システムのアクティブサイトとして機能しているサイトを示します。 - 論理トポロジでは、青色の線は 2 つのサイトを接続する IPSec トンネルが動作していることを示し、赤色の線はトンネルがダウンしていることを示します。 - サイトの状態については、システムおよびサイトの状態 (301ページ) を参照してください。
4	[Event Timeline] : システムのディザスタリカバリタスクについて、進行中のタスクと完了したタスクがすべて表示されます。詳細については、イベントタイムラインのモニタリング (298ページ) を参照してください。

引き出し線	説明
5	[Configure] タブ：ディザスタリカバリシステムのサイト間の接続を確立するために必要な設定を入力する場合にクリックします。詳細については、 ディザスタリカバリのセットアップ (272ページ) を参照してください。
6	[Logical] タブと [Physical] タブ：適切なタブをクリックして、システムの論理トポロジと物理トポロジを切り替えます。
7	• [Status] 領域：システムの現在のステータスを示します。システムの状態については、システムおよびサイトの状態 (301ページ) を参照してください。 • [Ongoing Data Replication] エリア：システム内のサイト間での GlusterFS、MongoDB、および Postgres データのレプリケーションステータスを示します。詳細については、「マネージドサービス複製のモニター (301ページ)」を参照してください。
8	[Interactive Help] ボタン：クリックすると、スライドインペインが開き、 Catalyst Center の特定のタスクを完了するための画面上のガイダンスを示すウォークスルーへのリンクが表示されます。
9	[Legend] ：トポロジのアイコンの意味を示します。凡例を表示するには、 [Disaster Recovery] ウィンドウの右下隅にある  をクリックします。
10	[Action] エリア：現在開始できるディザスタリカバリタスクが表示されます。使用可能なタスクは、システムのステータスやサイト設定によって異なります。

ディザスタリカバリシステムのステータスの表示に関する情報。

トポロジでは、ディザスタリカバリシステムの現在のステータスが視覚的に表示されます。この情報をテーブルに表示するには、ディザスタリカバリシステム **[Disaster Recovery System]** スライドインペインを使用します。このペインを開くには、次のいずれかのタスクを完了します。

- **[Show Detail Information]** リンクをクリックします。次に、スライドインペインでステータスを確認するサイトを展開します。
- トポロジで、サイトのエンタープライズ仮想 IP アドレスまたは特定のノードのアイコンにカーソルを合わせます。開いたダイアログボックスで、右下隅にあるリンクをクリックします。



スライドインペインが開き、関連するサイト情報が表示されます。

Disaster Recovery System



System Status Up and Running
 Disaster Recovery Enterprise VIP

> Main Site

▼ Recovery Site

Role Primary
 Status Active
 Enterprise VIP

IPSEC STATUS

Tunnel Recovery-Main Up
 Tunnel Recovery-Witness Up

NODE

Status Up
 Enterprise IP
 Cluster IP
 Management IP

実稼働環境でディザスタリカバリを有効にする前に、前提条件を満たしていることを確認してください。

監視の前提条件

重要

- 最新の **Catalyst Center** バージョンにアップグレードする場合は、アップグレード後にディザスタリカバリが適切に機能するように、いくつかの手順を実行する必要があります。[アップグレードされた Catalyst Center アプライアンスでのディザスタリカバリの設定](#) (268ページ) を参照してください。
- ディザスタリカバリは **IPv6** をサポートしていません。

一般的な前提条件

- Catalyst Center** は、次の 2 つのディザスタリカバリ設定をサポートしています。
 - 1+1+1 セットアップ** : 1 つ目の **Catalyst Center** アプライアンスはメインサイトとして機能し、2 つ目のアプライアンスはリカバリサイトとして機能し、3 つ目のシステム（仮想マシン上に常駐）は監視サイトとして機能します。次のアプライアンスとバージョンがこのセットアップをサポートしています。
 - DN2-HW-APL（44 コア第 2 世代アプライアンス） : **Catalyst Center 2.2.2.x** 以降
 - DN3-HW-APL（32 コア第 3 世代アプライアンス） : **Catalyst Center 2.3.7.6** 以降
 - DN2-HW-APL-L（56 コア第 2 世代アプライアンス） : **Catalyst Center 2.2.1.x** 以降

- DN3-HW-APL-L (56 コア第 3 世代アプライアンス) : Catalyst Center 2.3.7.6 以降
 - DN2-HW-APL-XL (112 コア第 2 世代アプライアンス) : Catalyst Center 2.2.1.x 以降
 - DN3-HW-APL-XL (80 コア第 3 世代アプライアンス) : Catalyst Center 2.3.7.6 以降
- **3+3+1 セットアップ** : 1 つ目の 3 ノード Catalyst Center クラスタはメインサイトとして機能し、2 つ目の 3 ノードクラスタはリカバリサイトとして機能し、3 つ目のシステム (仮想マシン上に常駐) は監視サイトとして機能します。次のアプライアンスとバージョンがこのセットアップをサポートしています。
- DN2-HW-APL (44 コア第 2 世代アプライアンス) : Catalyst Center 2.2.2.x 以降
 - DN3-HW-APL (32 コア第 3 世代アプライアンス) : Catalyst Center 2.3.7.6 以降
 - DN2-HW-APL-L (56 コア第 2 世代アプライアンス) : Catalyst Center 2.1.2.x 以降
 - DN3-HW-APL-L (56 コア第 3 世代アプライアンス) : Catalyst Center 2.3.7.6 以降
 - DN2-HW-APL-XL (112 コア第 2 世代アプライアンス) : Catalyst Center 2.1.2.x 以降
 - DN3-HW-APL-XL (80 コア第 3 世代アプライアンス) : Catalyst Center 2.3.7.6 以降
- Catalyst Center アプライアンスでエンタープライズポートのインターフェイスに **VIP** を設定しておきます。ディザスタリカバリではサイト内通信にエンタープライズ ネットワークを使用するため、この設定が必要になります。『[Catalyst Center Appliance Installation guide](#)』では、以下のトピックを参照してください。
- エンタープライズポートの詳細については、「[Interface Cable Connections](#)」のトピックを参照してください。
 - エンタープライズポートの設定の詳細については、「[Configure the Primary Node Using the Maglev Wizard](#)」または「[Configure the Primary Node Using the Advanced Install Configuration Wizard](#)」のトピックを参照してください。
- ディザスタリカバリタスクを実行できるように、ネットワーク管理者ユーザーを割り当てておきます。この機能には、この特権レベルのユーザーしかアクセスできません。
- 次の両サイトを接続するリンクが **1 Gbps** で、**RTT 遅延が 350 ミリ秒以下**であることを確認しておきます。
- メインサイトとリカバリサイト
 - メインサイトと監視サイト
 - リカバリサイトと監視サイト

注

監視サイトとの接続には **1 Gbps** のリンクが推奨されますが、監視サイトが使用する実際の帯域幅は **50 Mbps**です。リンク速度がこれよりも速い限り、問題は発生しません。

- メインサイトとリカバリサイトの両方にインストールされるディザスタリカバリ **IPSec** 証明書は、同じルート **CA** によって署名されている必要があります。そうでない場合、サイトの登録および再参加は失敗します。

 注

Catalyst Center は、登録プロセス中にこの証明書を監視サイトに自動的にコピーします。

メインサイトとリカバリサイトが使用するすべての IP アドレス（特にエンタープライズポートの仮想 IP アドレス）と完全修飾ドメイン名（**FQDN**）がこの証明書に含まれていることを確認してください。また、証明書の **[keyUsage]** パラメータに **[digitalSignature]** が指定されていることを確認します。サードパーティ証明書を生成する方法については、『Catalyst CenterSecurity Best Practices Guide』の「[Generate a Certificate Request Using SSL](#)」を参照してください。

- 『Catalyst CenterSecurity Best Practices Guide』の「Disaster Recovery Ports」トピックに記載されているすべてのポートを開いておきます。
- FQDN のみの証明書を使用している場合は、メインサイトとリカバリサイトの両方、およびディザスタリカバリの VIP で同じ **cluster_hostname**（つまり、Catalyst Center 構成ウィザードで設定した Catalyst Center の FQDN）を使用していることを確認します。
- ネットワークがファイアウォールの背後にある場合は、ファイアウォールで **ICMP** を有効にします。Catalyst Center は、ディザスタリカバリシステムのメインサイト、リカバリサイト、および監視サイト間の接続を追跡するため、**ICMP ping** を定期的送信します。

メインサイトとリカバリサイトの前提条件

- メインサイトとリカバリサイトの両方が同じ数のノードで構成されている必要があります。Catalyst Center では、この要件を満たさないディザスタリカバリシステムを登録してアクティブにすることはできません。
- メインサイトとリカバリサイトの両方について、同じハードウェアプロファイルを持つ Catalyst Center アプライアンスで構成する必要があります。たとえば、サイトは、第 2 世代の 112 コア アプライアンスと第 3 世代の 80 コア アプライアンスで構成できます。次の表に、ディザスタリカバリをサポートするアプライアンスとそれぞれのシスコ製品番号を示します。

13： Catalyst Center

マシンプロファイル	マシンプロファイルエイリアス	シスコの部品番号	コア数
medium	medium	第 1 世代 - DN1-HW-APL - DN1-HW-APL-U（プロモーション） 第 2 世代 - DN2-HW-APL - DN2-HW-APL-U（プロモーション） 第 3 世代：DN3-HW-APL	44 32

マシンプロファイル	マシンプロファイルエイリアス	シスコの部品番号	コア数
t2_large	large	第 2 世代 • DN2-HW-APL-L • DN2-HW-APL-L-U (プロモーション) 第 3 世代 : DN3-HW-APL-L	72
t2_2xlarge	extra large	第 2 世代 • DN2-HW-APL-XL • DN2-HW-APL-XL-U (プロモーション) 第 3 世代 : DN3-HW-APL-XL	112 80

また、メインサイトとリカバリサイトが同じバージョンの **Catalyst Center** を実行していることを確認してください。

- **Catalyst Center 2.3.7.9** 以降では、**HA** が有効になっている混合 3 ノードクラスターのサポートが追加されています。有効な混合クラスターは、次の要件を満たしています。
 - 第 2 世代と第 3 世代の **Catalyst Center** アプライアンスで構成されている。第 1 世代のアプライアンスはサポートされていない。
 - その 3 つのアプライアンスに同じマシンプロファイルが設定されている。たとえば、2 つの第 2 世代大規模アプライアンスと 1 つの第 3 世代大規模アプライアンスを含むクラスターは、有効な混合クラスターです。
- メインサイトとリカバリサイトの両方で、高可用性 (**HA**) を設定して有効にしておきます。これが設定されていないと、これらのサイトの登録は失敗します。詳細については、最新の『[Catalyst Center High Availability Guide](#)』を参照してください。

重要

これは、3 ノードセットアップにのみ適用されます。

- メインサイトとリカバリサイトの連邦情報処理標準 (**FIPS**) モード設定が同じであることを確認します。**FIPS** モードが一方のサイトで有効になっていて、もう一方のサイトで無効になっている場合、検証エラーが原因でディザスタリカバリシステムの登録が失敗します。**FIPS** モードの詳細については、[\[IP addressing mode used for the services\]](#) 画面の説明を参照してください (『[Catalyst Center Appliance Installation guide's](#)』の「[Configure the Primary Node Using the Maglev Wizard](#)」トピックにあります)。
- ボーダー ゲートウェイ プロトコル (**BGP**) を使用してシステムの仮想 IP アドレスルートをアドバタイズする場合は、メインサイトとリカバリサイトの各ネイバールータでシステムのエンタープライズ仮想 IP アドレスを設定する必要があります。入力する必要がある設定は、次の例のようになります。

内部 **BGP (iBGP)** の設定例

```
router bgp 64555
  bgp router-id 10.30.197.57
  neighbor 172.25.119.175 remote-as 64555
```

```
neighbor 172.25.119.175 update-source 10.30.197.57
neighbor 172.25.119.175 next-hop-self
```

引数の説明

- 64555 は、ネイバルルータのローカルおよびリモート **AS** 番号です。
- 10.30.197.57 はネイバルルータの **IP** アドレスです。
- 172.25.119.175 は、システムのエンタープライズ仮想 **IP** アドレスです。

外部 BGP (eBGP) の設定例

```
router bgp 62121
  bgp router-id 10.30.197.57
  neighbor 172.25.119.175 remote-as 64555
  neighbor 172.25.119.175 update-source 10.30.197.57
  neighbor 172.25.119.175 next-hop-self
  neighbor 172.25.119.175 ebgp-multihop 255
```

引数の説明

- 62121 は、ネイバルルータのローカル **AS** 番号です。
 - 64555 は、ネイバルルータのリモート **AS** 番号です。
 - 10.30.197.57 はネイバルルータの **IP** アドレスです。
 - 172.25.119.175 は、システムのエンタープライズ仮想 **IP** アドレスです。
- **BGP** ルートアドバタイズメントを有効にする場合（前の項目を参照）、パフォーマンスを向上させるために **Catalyst Center** へのルートをフィルタリングすることを推奨します。フィルタリングを行うには、次の設定を入力します。

```
neighbor system's-Enterprise-virtual-IP-address route-map DENY_ALL out
!
ip prefix-list DENY_ALL seq 5 deny 0.0.0.0/0 le 32
!
route-map DENY_ALL permit 10
match ip address prefix-list DENY_ALL
```

監視サイトの前提条件

- 監視サイトをホストする仮想マシンが、最低でも **2.1 GHz** コアと **2** つの仮想 **CPU**、**4 GB** の **RAM**、および **15 GB** のハードディスク領域を搭載した **VMware ESXi** ハイパーバイザバージョン **7.0** 以降を実行していることを確認しておきます。
- 監視サイトの **VM** のホスト名が **20** 文字以内であることを確認します。監視サイトのホスト名がこの制限を超えると、監視サイトとディザスタリカバリシステムの設定に失敗する可能性があります。
- パブリッククラウドでの監視サイトの展開はサポートされていません。
- 監視サイトをメインサイトおよびリカバリサイトとは別の場所に用意し、それらの両方のサイトから到達可能であることを確認しておきます。
- 監視サイトからアクセス可能な **NTP** サーバーを設定しておきます。この **NTP** サーバーをメインサイトとリカバリサイトで使用される **NTP** サーバーと同期する必要があります。
- 監視サイトは、実際の帯域幅の約 **50 Mbps** を使用します。この帯域幅は、主に監視サイトとプライマリサイトまたはスタンバイサイト間の接続（**WAN**、**LAN**、専用回線など）のモニタリングに使用されます。

証明書的前提条件

- メインサイトとリカバリサイトの両方にインストールされるディザスタリカバリ IPsec 証明書は、同じルート CA によって署名されている必要があります。そうでない場合、サイトの登録および再参加は失敗します。

注

Catalyst Center は、登録プロセス中にこの証明書を監視サイトに自動的にコピーします。

メインサイトとリカバリサイトが使用するすべての IP アドレス（特にエンタープライズポートの仮想 IP アドレス）と完全修飾ドメイン名（FQDN）がこの証明書に含まれていることを確認してください。また、証明書の [keyUsage] パラメータに [digitalSignature] が指定されていることを確認します。サードパーティ証明書を生成する方法については、『*Catalyst Center Security Best Practices Guide*』の「[Generate a Certificate Request Using Open SSL](#)」を参照してください。

- メインサイトとリカバリサイトにインストールされた証明書で、各証明書に指定されている最初のワイルドカード以外の DNS 名が一致していることを確認します。Catalyst Center で同じ証明書を使用する場合は、証明書の最初のワイルドカード以外の DNS 名も一致していることを確認します。
- FQDN のみの証明書を使用している場合は、メインサイトとリカバリサイトの両方、およびディザスタリカバリの VIP で同じ **cluster_hostname**（つまり、Catalyst Center 構成ウィザードで設定した Catalyst Center の FQDN）を使用していることを確認します。

Catalyst Center

Catalyst Center アップグレード後のディザスタリカバリの設定に関する情報。

システムを最新の Catalyst Center バージョンにアップグレードした後にディザスタリカバリを正常に設定するには、次の手順を実行します。

1. [監視サイトのインストール](#)（270ページ）。
2. [ディザスタリカバリのセットアップ](#)（272ページ）。

Catalyst Center は、X.509 証明書と秘密キーの Catalyst Center へのインポートとストレージをサポートします。ディザスタリカバリ証明書は、クラスター内通信に使用されます。

Catalyst Center は、X.509 証明書と秘密キーの Catalyst Center へのインポートとストレージをサポートします。ディザスタリカバリ証明書は、クラスター間の通信に使用されます。

内部 CA によって発行された有効な X.509 証明書を取得する必要があります。証明書が所有する秘密キーと一致していることを確認してください。

 注

- Catalyst Center で使用するのと同じ証明書をディザスタリカバリシステムで使用する場合は、この手順をスキップできます。証明書を設定する場合は、☐ および **[DR]** チェックボックスを選択します（[Catalyst Center サーバー証明書の更新（28ページ）](#) を参照）。
- ディザスタリカバリ証明書の要件の詳細については、『[Security Best Practices Guide](#)』を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [Certificate] > [System Certificates] の順に選択します。
2. [+ New Certificate Request (CSR)] をクリックします。
3. Catalyst Center にインポートする証明書のファイル形式タイプを選択します。
 - **[PEM]** : プライバシー強化メール ファイル形式。
 - **[PKCS]** : 公開キー暗号化標準ファイル形式。
4. **[PEM]** を選択した場合、次のタスクを実行します。
 - a) 強調表示されている領域に **PEM** ファイルをドラッグアンドドロップして、証明書をインポートします。

 注

PEM ファイルには、有効な PEM 形式の拡張子（.pem）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

- b) **[Private Key]** 領域で、強調表示されている領域に秘密キーをドラッグアンドドロップしてインポートします。

 注

秘密キーには、有効な秘密キー形式の拡張子（.key）が必須です。秘密キーの最大ファイルサイズは 10 MB です。

アップロードに成功すると、秘密キーが検証されます。

- c) 適切なオプションボタンをクリックして、秘密キーを暗号化するかどうかを指定します。
 - d) 秘密キーを暗号化する場合、**[Password]** フィールドに秘密キーのパスワードを入力します。
5. **[PKCS]** を選択した場合、次のタスクを実行します。

- a) 強調表示されている領域に **PKCS** ファイルをドラッグアンドドロップして、証明書をインポートします。



注

PKCS ファイルには、有効な **PKCS** 形式の拡張子（.pfx または .p12）が必須です。証明書の最大ファイルサイズは **10 MB** です。

アップロードに成功すると、システム証明書が検証されます。

- b) [Password] フィールドに、証明書のパスワードを入力します（**PKCS** の要件）。
- c) 適切なオプションボタンをクリックして、秘密キーを暗号化するかを指定します。
- d) 秘密キーを暗号化する場合、[Password] フィールドに秘密キーのパスワードを入力します。

6. [Save] をクリックします。

Catalyst Center サーバーの **SSL** 証明書が置き換えられると、自動的にログアウトされます。もう一度ログインし直してください。

Catalyst Center のディザスタリカバリシステムの監視サイトとして機能する仮想マシンのセットアップに関する情報。

ディザスタリカバリシステムの監視サイトとして機能する仮想マシンを設定するには、次の手順を実行します。

1. 監視サイトで実行している **Catalyst Center** のバージョンに固有の **OVF** パッケージをダウンロードします。

- a) <https://software.cisco.com/download/home/286316341/type> を開きます。



注

この URL にアクセスするには、**Cisco.com** のアカウントが必要です。アカウントの作成方法については、次のページを参照してください。 <https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html>

- b) [Select a Software Type] 領域で、**Catalyst Center** のソフトウェアリンクをクリックします。
- [Software Download] ページが更新され、**Catalyst Center** の最新リリースで使用可能なソフトウェアのリストが表示されます。
- c) 次のいずれかを実行します。
- 必要な **OVF** パッケージ（*.ova）がすでに表示されている場合は、その [Download] アイコンをクリックします。

- **[Search]** フィールドに関連するバージョン番号を入力し、ナビゲーションペインでそのリンクをクリックして、該当するバージョンの **OVF** パッケージに対応する **[Download]** アイコンをクリックします。
2. このパッケージを、VMware vSphere 7.0 以降を実行しているローカルマシンにコピーします。
 3. vSphere クライアントで、**[File] > [Deploy OVF Template]** を選択します。
 4. **[Deploy OVF Template]** ウィザードを完了します。
 - a) **[Source]** 画面に表示される指示に従います。
 1. **[参照 (Browse)]** をクリックします。
 2. 監視サイトの **OVF** パッケージ (**.ova**) まで移動します。
 3. **[Open]** をクリックします。
 4. **[Deploy from a file or URL]** フィールドで、パッケージのパスが表示されていることを確認し、**[Next]** をクリックします。
[OVF Template Details] 画面が開きます。
 - b) **Next >** をクリックします。
 - c) **[Name and Location]** 画面で、次の手順を実行します。
 - **[Name]** フィールドに、パッケージに対して設定する名前を入力します。
 - **[Inventory Location]** フィールドで、パッケージを配置するフォルダを選択します。
 - **Next >** をクリックします。**[Host/Cluster]** 画面が開きます。
 - d) 展開したテンプレートを実行するホストまたはクラスタをクリックし、**[Next >]** をクリックします。
[Storage] 画面が開きます。
 - e) 仮想マシンファイルを配置するストレージドライブをクリックし、**[Next >]** をクリックします。
[Disk Format] 画面が開きます。
 - f) **[Thick Provision]** オプションボタンをクリックし、**[Next]** をクリックします。
 - g) **[Network Mapping]** 画面の指示に従って、**[Next]** をクリックします。
 1. **[Destination Networks]** 列にリストされている IP アドレスをクリックします。
 2. 表示されたドロップダウンリストで、展開したテンプレートで使用するネットワークを選択します。**[Ready to Complete]** 画面が開き、入力したすべての設定が表示されます。
 - h) **[Power on after deployment]** チェックボックスをオンにし、**[Finish]** をクリックします。
 - i) **[Deployment Completed Successfully]** ダイアログボックスが開いたら、**[Close]** をクリックします。
 5. 監視サイトのネットワーク設定を入力します。
 - a) 次のいずれかを実行して、作成した仮想マシンのコンソールを開きます。
 - vSphere クライアントのリストから仮想マシンを右クリックし、**[Open Console]** を選択します。
 - vSphere クライアントのメニューで **[Open Console]** アイコンをクリックします。**[Witness User Configuration]** ウィンドウが開きます。
 - b) 管理者ユーザー (*maglev*) のパスワードを入力して確認用にもう一度入力し、**N**を押して次に進みます。

c) 次の設定を入力し、[N] を押して次に進みます。

- IP アドレス
- 仮想マシンの IP アドレスに関連付けられているネットマスク
- デフォルトゲートウェイの IP アドレス
- (オプション) 優先 DNS サーバーの IP アドレス

d) NTP サーバーのアドレスまたはホスト名を 1 つ以上入力し（複数の場合はカンマで区切る）、S を押して設定を送信します。監視サイトの設定が開始されます。

1 つ以上の NTP アドレスまたはホスト名が必要です。

e) 監視サイトに設定した IP アドレスに SSH ポート 2222 を使用してログインし、設定が完了したことを確認します。

注

後で、監視サイトの VM で **maglev** ユーザー用に設定されたパスワードを変更する必要がある場合は、標準の **Linux passwd** ユーティリティを使用します。これを行う前にディザスタリカバリシステムを一時停止する必要はありません。また、パスワードを変更しても、ディザスタリカバリ操作に機能上の影響はありません。

ディザスタリカバリのセットアッププロセスの概要を簡単に説明します。

Catalyst Center 展開でのディザスタリカバリの設定は、2 段階のプロセスです。最初の段階は、ディザスタリカバリシステムを構成するサイトを登録することです。2 番目の段階は、システムをアクティブにして、ディザスタリカバリを有効にすることです。完了する必要がある手順の説明、およびこのプロセス中に発生する可能性のあるエラーとその対処方法については、このセクションのトピックを参照してください。

VIP 昇格とルートアドバタイズメントについて説明します。また、ディザスタリカバリシステムでこれら 2 つの機能を使用するかどうかを判断するのに役立つ情報も提供します。

ディザスタリカバリシステムのメインサイトを登録する前に、次の機能の使用方法を決定する必要があります。

[VIP Promotion]

Catalyst Center 展開用に設定されたエンタープライズ インターフェイス VIP をシステムのディザスタリカバリ VIP として使用するかどうかを決定する必要があります。VIP 昇格は、次の項目がすべて当てはまる場合にのみ適切です。

- 既存の **Catalyst Center** インスタンスがネットワークを管理しており、すべてのデバイスがインスタンスのエンタープライズ VIP で構成されているブラウнフィールド展開があります。このインスタンスは、ディザスタリカバリシステムのメインサイトとして機能します。

- 既存のエンタープライズインターフェイスVIPアドレスは、メインサイトとリカバリサイトが存在する2つのデータセンター間で一方から他方に変更できます。これは通常、複数のデータセンターを包含する拡張 L2 ネットワークの場合に適用されます。
- 新しいディザスタリカバリシステムのエンタープライズインターフェイスVIPの場合、既存のデバイスを再設定する必要はありません。

VIP昇格を使用する場合は、手順 2b で [Yes] オプションボタンをクリックし、[メインサイトの登録](#) (273ページ) で手順 2b から 2e を完了します。

ルート アドバタイズメント オプション

次に、展開で使用するルートアドバタイズメントオプションを決定する必要があります。ディザスタリカバリの主な目的の1つは、フェールオーバーが発生した後も、デバイスの再プロビジョニングを必要とせずに継続的なネットワーク運用を可能にすることです。これは、ディザスタリカバリシステムの現在のアクティブサイトで自動的に設定されるフローティングVIPを指定することによって実現されます。フェールオーバーが発生するたびに、このVIP（この章ではディザスタリカバリVIPとして言及）は、以前のアクティブサイトからクリアされ、新しいアクティブサイトで設定されます。その結果、現在どのサイトがアクティブかに関係なく、ネットワークのデバイスはCatalyst Centerと通信し続けることができます。[メインサイトの登録](#) (273ページ) の手順 2g を完了するときに選択できる3つのルートアドバタイズメントオプションがあります。

- **[Border Gateway Protocol (BGP)]** : このオプションは、ほとんどのディザスタリカバリシステムで推奨されており、デフォルトで選択されています。BGPルートアドバタイズメントにより、システムの現在アクティブなサイトに確実にアクセスすることができます。これはフェールオーバーの発生後に重要になります。

重要

- このオプションを使用する場合は、まず「メインサイトとリカバリサイトの前提条件」セクション ([前提条件](#) (263ページ) トピックにあります) 末尾の2つの箇条書きで説明されている手順を完了します。
- ピアルータはBGPを使用する必要があります。ピアルータの外では、OSPF、EIGPなどの任意のIGPプロトコルを使用できます。
- **[Disaster recovery VIPs without route advertisement]** : ルートがBGPを使用してアドバタイズされないシステムの仮想IPアドレスを設定する場合は、このオプションを選択します。このオプションは、メインサイトとリカバリサイトの両方が、システムのグローバル仮想IPアドレスが存在するサブネットにアクセスできるデータセンターに適しています。
- **[No disaster recovery VIPs]** : このオプションを選択すると、サイトに設定された仮想IPアドレスが、そのサイトに属するデバイスで自動的に設定されます。フェールオーバーが発生するたびに、これらの仮想IPアドレスがデバイスで再設定されます。

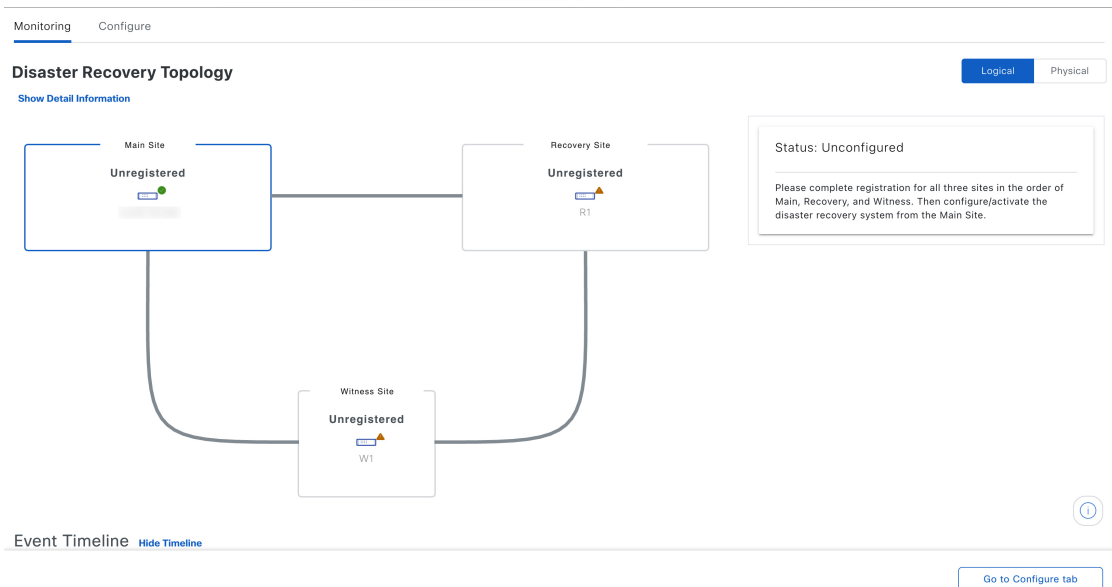
ディザスタリカバリ システムのメインクラスタサイトを登録する方法を学習します。

システムのメインサイトを登録するには、次の手順を実行します。

- [メインサイトの登録に関する考慮事項](#) (272ページ) を確認済みであることを確かめてください。
- ディザスタリカバリシステムのメインサイトとリカバリサイトが存在する Catalyst Center アプライアンスやクラスタの場合は、次の手順を実行します。

- 同じバックアップスケジュールとプロキシサーバーを設定します。システムをアクティブ化する前にこの処理を行わないと、フェールオーバーが発生してリカバリサイトがアクティブサイトになった後に、これら 2 つの設定を再度指定する必要が生じます。
- 各サイトが異なる NFS デバイスを指す NFS バックアップ設定を構成します。

1. メインメニューから次を選択します。[System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。



デフォルトでは、[Monitoring] タブが選択されています。

2. メインサイトを登録します。
 - a) [Configure] タブをクリックします。

[Main Site] オプションボタンはすでに選択されている必要があります。

b) **[Promote the enterprise and/or management VIPs of the cluster to the disaster recovery VIPs]**

エリアで、次のオプションボタンのいずれかをクリックします。

- クラスタをメインサイトとして設定し、このクラスタに接続されているデバイスに仮想 IP アドレスの変更を自動的に伝達するには、**[Yes]** をクリックします。これは、クラスタに現在設定されている仮想 IP アドレスを昇格させ、それらをディザスタリカバリシステムのグローバル仮想 IP アドレスとして割り当てることによって実現します。多数のデバイスが接続されているクラスタでディザスタリカバリを有効にする場合は、このオプションを選択することをお勧めします。このオプションを選択しない場合、新しいディザスタリカバリ仮想 IP アドレスと通信するようにこれらのデバイスを再設定する必要があります。このオプションを選択した場合、次の手順を実行します。
- 1. **[New main site enterprise VIP]** フィールドに、サイトのエンタープライズ ネットワークの新しい仮想 IP アドレスを入力します。これにより、昇格するアドレスが置き換えられます。このアドレスがまだ使用されていない一意のアドレスであり、以前の仮想 IP アドレスと同じサブネットにあることを確認します。
- 2. (オプション) **[Promote the cluster management VIP, <IP-address>, to the disaster recovery management VIP]** チェックボックスをオンにします。
- 3. (オプション) **[New main site management VIP]** フィールドに、サイトの管理ネットワークの新しい仮想 IP アドレスを入力します。これにより、昇格するアドレスが置き換えられます。このアドレスがまだ使用されていない一意のアドレスであり、以前の仮想 IP アドレスと同じサブネットにあることを確認します。
- 仮想 IP アドレスの変更を接続デバイスに伝達せず、クラスタをメインサイトとして設定するには、**[No]** をクリックします。まだどのデバイスにも接続されていない、または少数のデバイスにのみ接続されている新しいクラスタには、このオプションをお勧めします。このオプションを選択する場合は、ステップ 2f に進みます。

c) **[Action]** 領域で、**[Promote]** をクリックします。

[Disaster Recovery VIP Promotion] ダイアログが開きます。

d) **[Continue]** をクリックします。

Catalyst Center は、入力した仮想 IP アドレスを検証します。

e) **[VIP Promotion Status]** 領域に検証ステータスが表示されます。

- 入力したアドレスのいずれかが無効である場合（アドレスが置換するアドレスと同じサブネットに存在しない可能性があります）、必要な修正を行い、ステップ 2c を繰り返します。
- 入力したアドレスが正常に検証されると、ディザスタリカバリシステム用に設定されるすべての仮想 IP アドレスが **[VIP Promotion Status]** 領域に表示されます。次のステップに進みます。

f) **[Site VIP/IP addresses]** エリアに次の情報を入力します。

- **[Main Site VIP]** : アクティブサイトのクラスタノードとエンタープライズ ネットワークの間のトラフィックを管理する仮想 IP アドレス。Catalyst Center では、このフィールドはシステムの情報に基づいて入力されます。
- **[Recovery Site VIP]** : リカバリサイトのクラスタノードとエンタープライズ ネットワークの間のトラフィックを管理するエンタープライズ仮想 IP アドレス。
- **[Witness Site IP]** : 監視サイトの仮想マシンとエンタープライズ ネットワークの間のトラフィックを管理する IP アドレス。

重要

入力したアドレスが現在到達可能であることを確認します。到達できない場合、システムのサイトの登録は失敗します。

注

手順 2f および 2j の間の任意の時点で、[Reset] をクリックして、入力したすべての設定をクリアできます。その後、メインサイトを登録する前に、手順 2f を繰り返して正しい設定を入力する必要があります。

g) [Route advertisement] 領域で、次のいずれかのオプションボタンをクリックします。

- **[Border Gateway Protocol (BGP)]** : これは推奨オプションです。
- **ルートアドバタイズメントなしのディザスタリカバリ VIP**
- **[No disaster recovery VIPs]** : このオプションボタンをクリックする場合は、手順 2k に進んでください。

h) 前の手順で最初の 2 つのオプションボタンのいずれかをクリックした場合は、[Enterprise VIP for Disaster Recovery] フィールドに値を入力します。

このフローティング仮想 IP アドレスを設定しておく、ネットワークのアクティブサイトとして現在動作しているサイトに自動的に切り替えて運用されます。このアドレスは、ディザスタリカバリシステムとエンタープライズネットワークの間のトラフィックを管理します。

注

- **[Border Gateway Protocol (BGP)]** オプションボタンをクリックし、管理仮想 IP アドレスを設定しない場合は、手順 2j に進みます。
- **[Disaster recovery VIPs without route advertisement]** をクリックし、管理仮想 IP アドレスを設定しない場合は、手順 2k に進みます。

i) オプション: [Management VIP for Disaster Recovery] フィールドに値を入力します。

このフローティング仮想 IP アドレスを設定しておく、ネットワークのアクティブサイトとして現在動作しているサイトに自動的に切り替えて運用されます。このアドレスは、ディザスタリカバリシステムと管理ネットワークの間のトラフィックを管理します。

j) [Border Gateway Protocol (BGP)] オプションボタンをクリックした場合は、ルートアドバタイズメントを有効にするために必要な情報を入力します。

- **[Border Gateway Protocol Type]** 領域で、BGP ピアが相互に外部 ([Exterior BGP (eBGP)]) セッションを確立するか、内部 ([Interior BGP (iBGP)]) セッションを確立するかを指定します。
- **[Main Site Router Settings for Enterprise Network]** 領域および **[Recovery Site Router Settings for Enterprise Network]** 領域に、ディザスタリカバリシステムのメインサイトとリカバリサイトに設定されているエンタープライズ仮想 IP アドレスのアドバタイズのために **Catalyst Center** が使用するリモートルータの IP アドレスを入力します。また、ルータのリモートおよびローカル AS 番号も入力します。

以下の点に注意してください。

- 追加のリモートルータを設定する場合は、**[Add]** (+) アイコンをクリックします。サイトごとに最大 **2** 台のルータを設定できます。
- **AS** 番号を入力する場合は、**1** ～ **4,294,967,295** の範囲内の **32** ビットの符号なし数であることを確認します。
- **[iBGP]** オプションを選択すると、**Catalyst Center** はローカル **AS** 番号をリモート **AS** 番号として入力した値に自動的に設定します。
- 前の手順で管理仮想 IP アドレスを設定した場合は、**[Main Site Router Settings for Management Network]** 領域および **[Recovery Site Router Settings for Management Network]** 領域も表示されます。**Catalyst Center** でこの仮想 IP アドレスのアドバタイズに使用されるリモートルータに関する適切な情報を入力します。

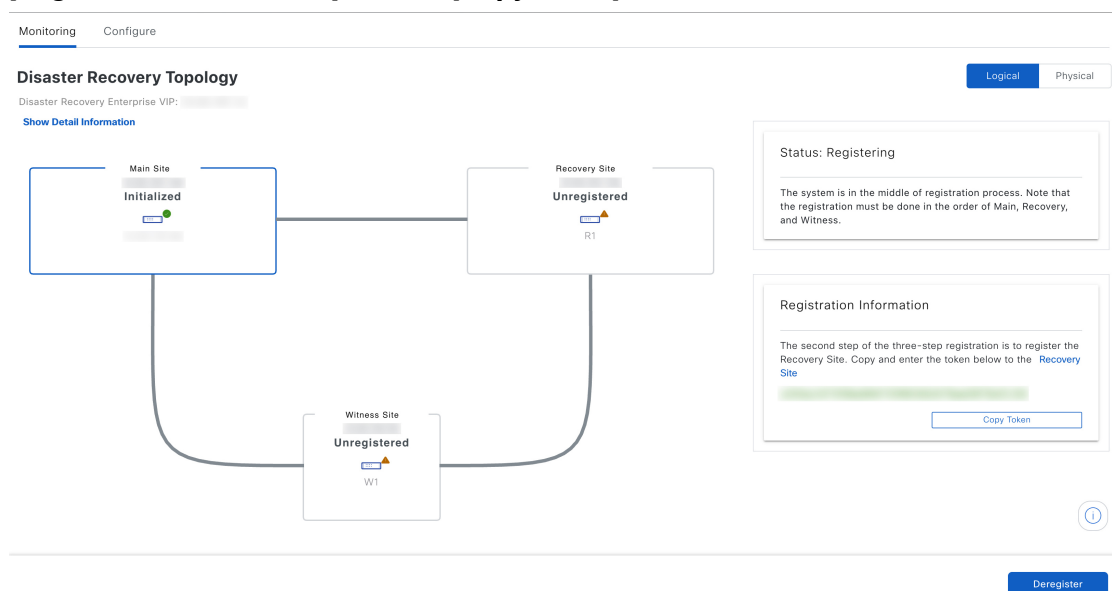
k) **[Action]** 領域で、**[Register]** をクリックします。

[Disaster Recovery Registration] ダイアログが開きます。

l) **[Continue]** をクリックします。

リカバリサイトおよび監視サイトをメインサイトに登録するために必要なトークンが生成されます。

3. **[Registration Information]** 領域で、**[Copy Token]** をクリックします。



このトピックには、メインサイトの登録中に発生する可能性のある問題の一般的な検証エラーと解決策が一覧表示されています。

システムのメインサイトを登録するときにエラーが発生する場合があります。このトピックでは、該当するエラーとその対処方法について説明します。

検証タイプ	実行された検証	エラーの解決
VIP の到達可能性	リカバリサイトのポート 443 で TCP ソケットを開くことができるかどうかを確認します。 監視サイトのポート 2222 で TCP ソケットを開くことができるかどうかを確認します。	リカバリサイトの VIP がリカバリサイトの Catalyst Center インスタンス用に設定されたエンタープライズ VIP と一致しており、メインサイトから到達可能であることを確認してください。 監視サイトの IP アドレスが正しく設定されており、メインサイトから到達可能であることを確認します。
エンタープライズおよび管理インターフェイス VIP の到達可能性	次の要素を検索して、エンタープライズ インターフェイス経由でディザスタリカバリシステムの VIP に到達できるかどうかを確認します。 - ディザスタリカバリシステムの VIP 用にエンタープライズ インターフェイスで定義された静的ルート - エンタープライズ インターフェイスで設定されたデフォルトゲートウェイ これらの要素のいずれも存在しない場合、検証は失敗します。 次の要素を検索して、管理インターフェイス経由でディザスタリカバリシステムの VIP に到達できるかどうかを確認します。 - ディザスタリカバリシステムの VIP 用に管理インターフェイスで定義された静的ルート - 管理インターフェイスで設定されたデフォルトゲートウェイ これらの要素のいずれも存在しない場合、検証は失敗します。	ディザスタリカバリシステムのエンタープライズ VIP 用のエンタープライズ インターフェイスで静的ルートを定義するか、エンタープライズ インターフェイスでデフォルトゲートウェイを定義します。 ディザスタリカバリシステムの管理 VIP 用の管理インターフェイスで静的ルートを定義するか、管理インターフェイスでデフォルトゲートウェイを定義します。

検証タイプ	実行された検証	エラーの解決
証明書アップロード	サードパーティの証明書がアップロードされているかどうかを確認します。アップロードされている場合、Catalyst Center は、証明書が自己署名されていないことも確認します。 [System Certificates] ページ ([System > Settings > Certificates > System Certificates]) で、次のいずれかが当てはまることを確認します。 • [Use System Certificate for Disaster Recovery as well] オプションが選択されている。 • ディザスタリカバリ固有の証明書がアップロードされている。 どちらの場合も、[SAN] フィールドの最初のエントリとして、ワールドカード以外の DNS 名が指定されている必要があります。	

上記に記載されていないエラーの場合、その原因は **[Status]** 領域で識別されます。必要な修正を行い、**[Action]** 領域から次のオプションのいずれかを選択して続行します。

- **[Retry]** : エラーの原因が修正された場合、またはエラーが断続的な問題（登録プロセス中の関連サービスの再起動など）によって発生した場合は、このオプションを試行して登録を続行します。
- **[Deregister]** : 設定を変更したり、登録をやり直したりする場合は、このオプションを使用して、詳細とオプションを最初から入力できるようにします。

リカバリクラスターサイトを登録してデータレプリケーションを有効にする方法を学習します。

リカバリサイトを登録するための手順は以下のとおりです。

注

手順 4 に先立つ任意の時点で、**[Reset]** をクリックして、入力したすべての設定をクリアできます。クリアした場合、リカバリサイトを登録する前に、この手順を最初から繰り返して正しい設定を入力する必要があります。

前提条件 (263ページ) トピックを表示し、「メインサイトとリカバリサイトの前提条件」セクションで説明されている要件が満たされていることを確認します。

1. **[Registration Information]** 領域で **[Recovery Site]** リンクを右クリックして、新しいブラウザタブで結果ページを開きます。
2. 必要に応じて、適切なユーザー名とパスワードを入力してリカバリサイトにログインします。

[Disaster Recovery] ページに、**[Recovery Site]** オプションボタンがすでに選択された状態で **[Configure]** タブが開きます。

3. 次の情報を入力します。
 - **[Main Site VIP]** : アクティブサイトのクラスタノードとエンタープライズ ネットワークの間のトラフィックを管理する仮想 IP アドレス。
 - **[Recovery Site VIP]** : リカバリサイトのクラスタノードとエンタープライズ ネットワークの間のトラフィックを管理する仮想 IP アドレス。 **Catalyst Center** では、このフィールドはシステムの情報に基づいて入力されます。

注

メインサイトとリカバリサイト間で **IPSec** トンネルが設定されると、**VIP** をホストするノード上のエンタープライズ トラフィックは、エンタープライズ **VIP** (UDP/TCP/ICMP) を介して送信されます。

- メインサイトの登録中に作成した登録トークン。
 - アクティブサイトのネットワーク管理者ユーザーに対して設定されたユーザー名とパスワード。
4. **[Action]** 領域で、**[Register]** をクリックします。
[Disaster Recovery Registration] ダイアログが開きます。
 5. **[Continue]** をクリックします。

メインサイトとリカバリサイトの接続が確立されると、トポロジでステータスが更新されます。

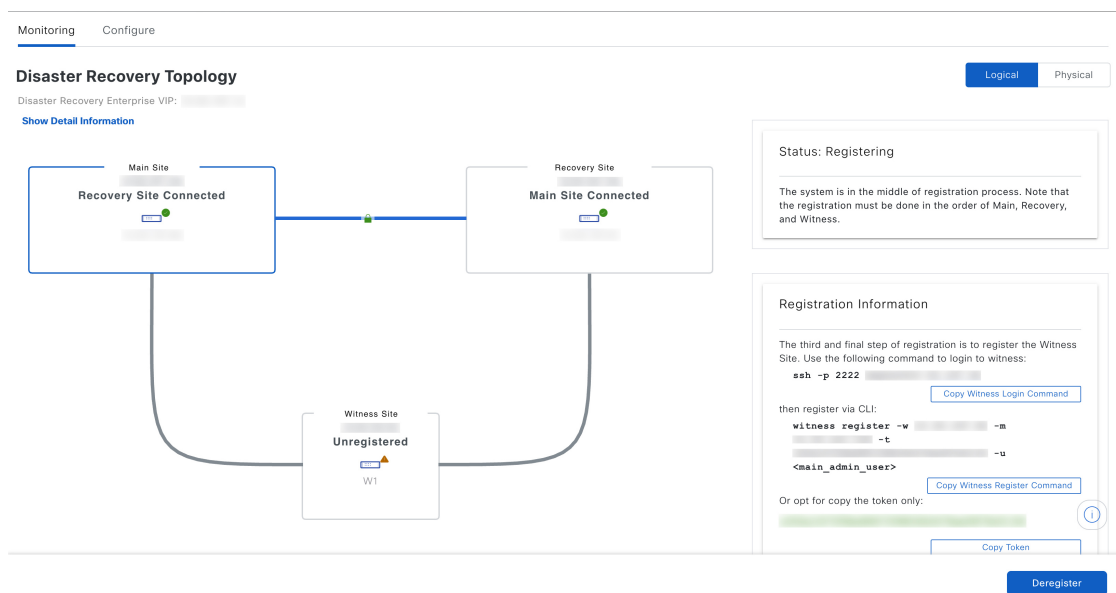
適切なサイト接続を確保するために、監視サイトを登録する方法について説明します。

監視サイトを登録するための手順は以下のとおりです。

ディザスタリカバリシステムの監視サイトを登録する前に、次の条件が満たされていることを確認してください。

- メインサイトとリカバリサイトの両方から監視サイトに到達可能である。
- メインサイトとリカバリサイトに設定された VIP に監視サイトから到達可能である。

1. メインサイトのブラウザタブに戻ります。



2. **[Registration Information]** エリアで、**[Copy Witness Login Command]** をクリックします。
3. 監視サイトへの SSH コンソールを開き、コピーしたコマンドを貼り付けてログインします。
4. 要求された場合は、デフォルトのユーザー (maglev) のパスワードを入力します。
5. **[Registration Information]** エリアに戻り、**[Copy Witness Register Command]** をクリックします。
6. SSH コンソールで、コピーしたコマンドを貼り付けます。
7. <main_admin_user> をネットワーク管理者ユーザーのユーザー名に置換してコマンドを実行します。
8. 要求された場合は、ネットワーク管理者ユーザーのパスワードを入力します。

このトピックでは、監視サイト登録プロセス中に発生する可能性のある一般的なエラーに関する障害対応ガイドランスを示します。

このトピックでは、監視サイトの登録時に発生する可能性のあるエラーとその対処方法について説明します。

エラータイプ	実行された検証	解像度
IP 検証	メインサイトの登録時に入力された監視サイトの IP アドレスが、監視サイトの登録時に入力された IP アドレスと一致することを検証します。	メインサイトと監視サイトを登録する際に、同じ監視サイトの IP アドレスを入力してください。
バージョン検証	監視サイトの OVA パッケージが、システムのメインサイトとリカバリサイトにインストールされている Catalyst Center バージョンに対して正しいバージョンであることを検証します。各 Catalyst Center バージョンは、1 つの OVA バージョンのみをサポートします。	エラーメッセージに表示されている監視サイトの OVA パッケージバージョンを展開します。

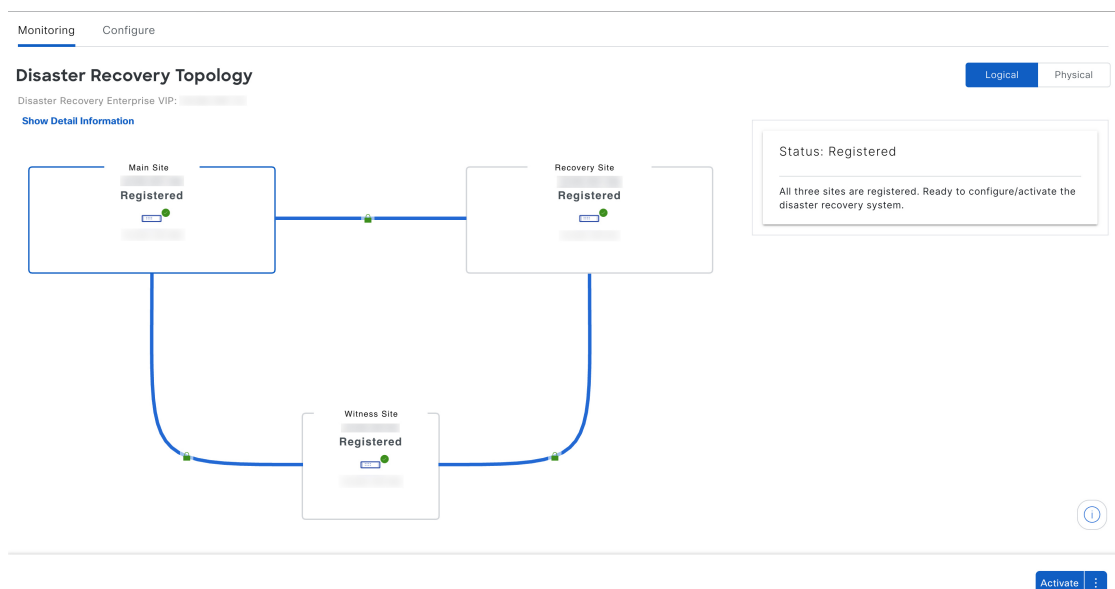
検証チェックを伴わないエラーの場合、その原因は **[Status]** 領域で識別できます。必要な修正を行い、次のいずれかのタスクを実行して続行します。

- 監視サイトにログインしてから、**witness reset** コマンドを実行します。
- 登録の設定を変更するか、プロセスを最初からやり直すには、**[Action]** 領域の **[Deregister]** をクリックします。

システムサイトを登録した後に、ディザスタリカバリ システムをアクティブ化する方法について説明します。

システムのサイトを登録したら、次の手順を実行して、**Catalyst Center** 展開でできるようにシステムをアクティブ化します。

1. メインサイト、リカバリサイト、および監視サイトが正常に登録されていることを確認します。
 - a) メインサイトのブラウザタブに戻り、**[Monitoring]** をクリックしてディザスタリカバリの **[Monitoring]** タブを表示します。



- b) [Logical Topology] 領域で、3つのサイトが表示され、ステータスが [Registered] であることを確認します。
- c) [Event Timeline] 領域で、各サイトの登録がイベントとしてリストされ、各タスクが正常に完了したことを確認します。

Event Timeline [Hide Timeline](#)

Latest events

Last Update: Mar 20, 2025 2:33:52 PM

✓

▼

Witness site registration - [redacted]

Status Message:

Successfully registered [redacted] as witness site.

Mar 19, 2025 6:26:09 PM

✓

▼

Recovery site registration - [redacted]

Status Message:

Successfully registered [redacted] as recovery site.

Mar 19, 2025 2:47:38 PM

✓

▼

Main site registration - [redacted]

Status Message:

Successfully registered [redacted] as main site.

Mar 19, 2025 2:37:39 PM

2. [Actions] 領域で [Activate] をクリックします。

リカバリサイトに現在存在するすべてのデータが消去されることを示すダイアログが開きます。

3. ディザスタリカバリシステムの設定とメインサイトのデータのリカバリサイトへの複製を開始するには、[Continue] をクリックします。

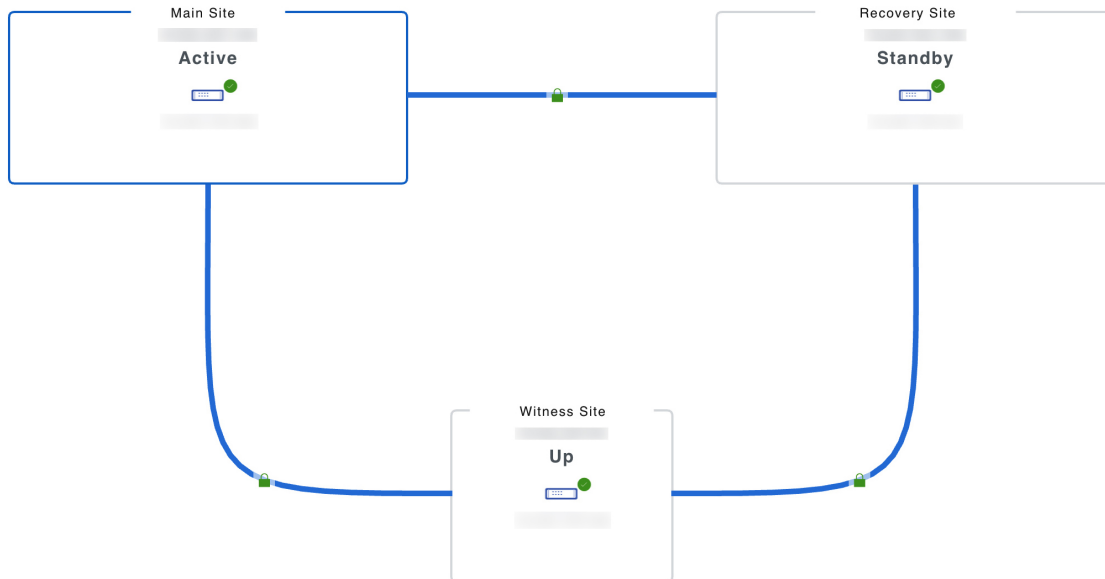
Cisco Catalyst Center | Updated May 5, 2026

 注

アクティブ化プロセスは、完了までに時間がかかる場合があります。進捗状況をモニターするには、イベントのタイムラインを表示します。

4. Catalyst Center で必要なタスクが完了したら、システムが動作していることを確認します。

a. トポロジを表示し、それぞれのサイトのステータスが次のように表示されていることを確認します。



b. イベントのタイムラインを表示し、[Activate Disaster Recovery System] タスクが正常に完了したことを確認します。

Event Timeline

Hide Timeline

Latest events

Last Update: Mar 19, 2025 6:44:07 PM

✓

▼

Activate Disaster Recovery System -

Mar 19, 2025 6:41:48 PM

Start Time:

Mar 19, 2025 6:31:20 PM

Status Message:

Successfully setup disaster recovery

End Time:

Mar 19, 2025 6:41:48 PM

✓

>

Configure active -

Mar 19, 2025 6:38:32 PM

✓

>

Configure standby -

Mar 19, 2025 6:41:35 PM

✓

>

Witness site registration -

Mar 19, 2025 6:26:09 PM

✓

>

Recovery site registration -

Mar 19, 2025 2:47:38 PM

✓

>

Main site registration -

Mar 19, 2025 2:37:39 PM

c. メインサイトから ping を実行して、サイトに到達できることを確認します。

アクティブ化または再参加操作の開始後にディザスタリカバリシステムが行う検証について説明します。

[Activate] および [Rejoin] 操作の開始後にディザスタリカバリシステムが行う検証を、次の表に示します。

検証	説明
パッケージの一致	メインサイトとリカバリサイトに同じパッケージバージョンがインストールされているかどうかを確認します。
主要なサービスの正常性	ディザスタリカバリ操作に不可欠なマネージドサービスおよびその他の主要なサービスの正常性を確認します。
IPsec のステータスと送信	ディザスタリカバリシステムのすべてのサイトで IPsec トンネルが稼働しているかどうかを確認します。
Consul 接続	consul（メインサイト、リカバリサイト、および監視サイトで共有される分散データベース）がすべてのサイトと通信できるかどうかを決定します。

ディザスタリカバリシステムの一時的停止に関する情報。長期間にわたってシステムを停止する場合は、ディザスタリカバリシステムを一時的に停止して、アクティブサイトからスタンバイサイトへのデータの複製を一時的に無効にすることができます。

メインサイトとリカバリサイトを一時停止することで、ディザスタリカバリシステムが実質的に停止します。サイト間の接続が解除され、各サイトがスタンドアロンクラスタとして機能するようになります。長期間にわたってシステムを停止する場合は、システムを一時的に停止して、アクティブサイトからスタンバイサイトへのデータの複製を一時的に無効にする必要があります。また、ディザスタリカバリシステムを一時的に停止して、次のいずれかを実行します。

- クラスタのアップグレードや追加パッケージのインストールなどの管理タスクを完了します。
- システムまたはディザスタリカバリ証明書を置き換えます。
- メイン、リカバリ、または監視サイトクラスタでメンテナンスを実行します。
- 計画的なネットワーク停止または停電に備えます。

ディザスタリカバリシステムを一時的に停止する手順。

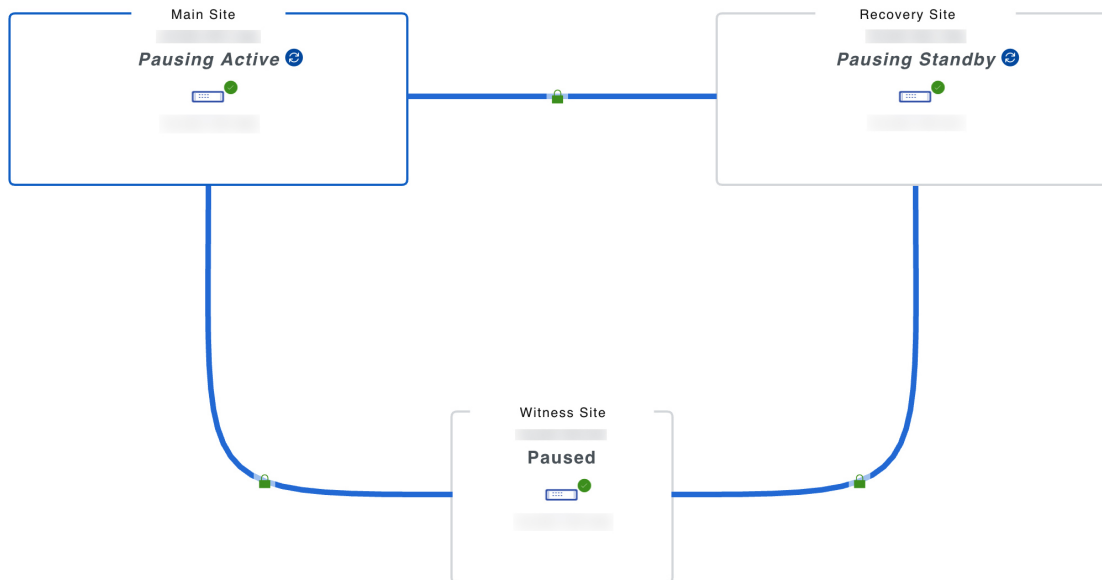
システムコンポーネントのメンテナンスを実施する前などにディザスタリカバリシステムを一時的に停止するには、次の手順を実行します。

1. メインメニューから次を選択します。[System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

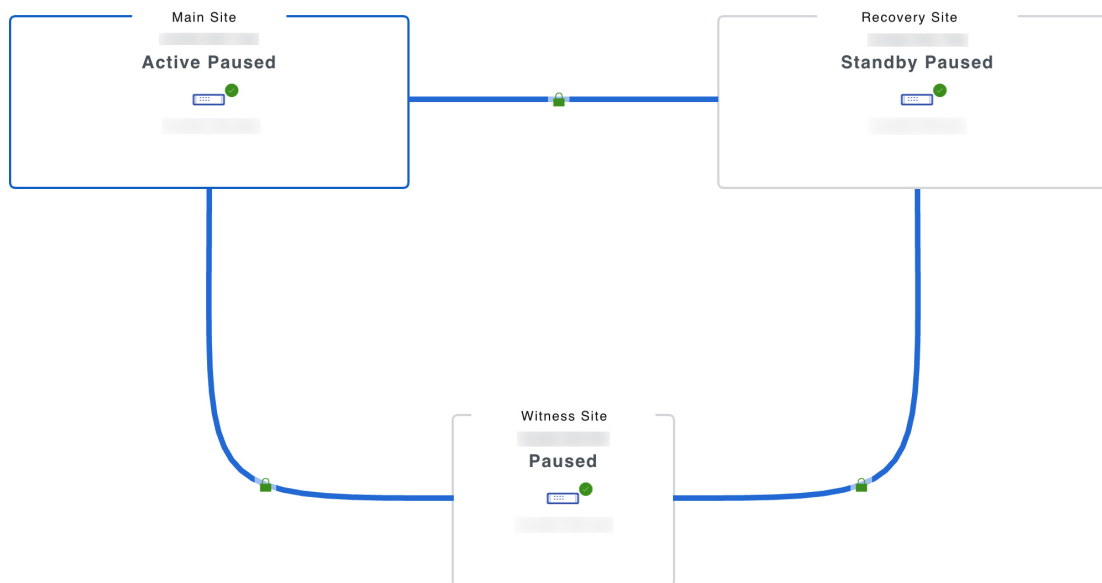
デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。

2. [Action] 領域で、 で [Pause] をクリックします。
3. 表示されたダイアログで、[Continue] をクリックして次に進みます。

ページの右下隅に、システムを一時的に停止するプロセスが開始されたことを示すメッセージが表示されます。システムを一時的に停止するために、Catalyst Center でデータとサービスの複製が無効化されます。また、リカバリサイト側の停止していたサービスが再開されます。このプロセスの実行中は、トポロジにおいて、メインサイトとリカバリサイトのステータスが [Pausing] に設定されます。



Catalyst Center で必要なタスクが完了すると、トポロジに表示されたメインサイト、リカバリサイト、および監視サイトのステータスが更新されて **[Paused]** に設定されます。



4. ディザスタリカバリシステムが一時停止していることを確認します。
 - a. **[Status]** 領域で、システムのステータスが **[Paused]** と表示されていることを確認します。
 - b. イベントのタイムラインで、**[Pause Disaster Recovery System]** タスクが正常に完了したことを確認します。

Event Timeline [Hide Timeline](#)

Latest events

Last Update: Mar 19, 2025 6:56:43 PM

▼ **Pause Disaster Recovery System -** Mar 19, 2025 6:55:38 PM

Start Time:
Mar 19, 2025 6:47:53 PM

Status Message:
Successfully prepared clusters for pause Disaster Recovery System.

End Time:
Mar 19, 2025 6:55:38 PM

▶ **Active cluster standalone -** Mar 19, 2025 6:50:52 PM

▶ **Standby cluster standalone -** Mar 19, 2025 6:55:25 PM

現在一時停止中のディザスタリカバリシステムに再参加するための手順。

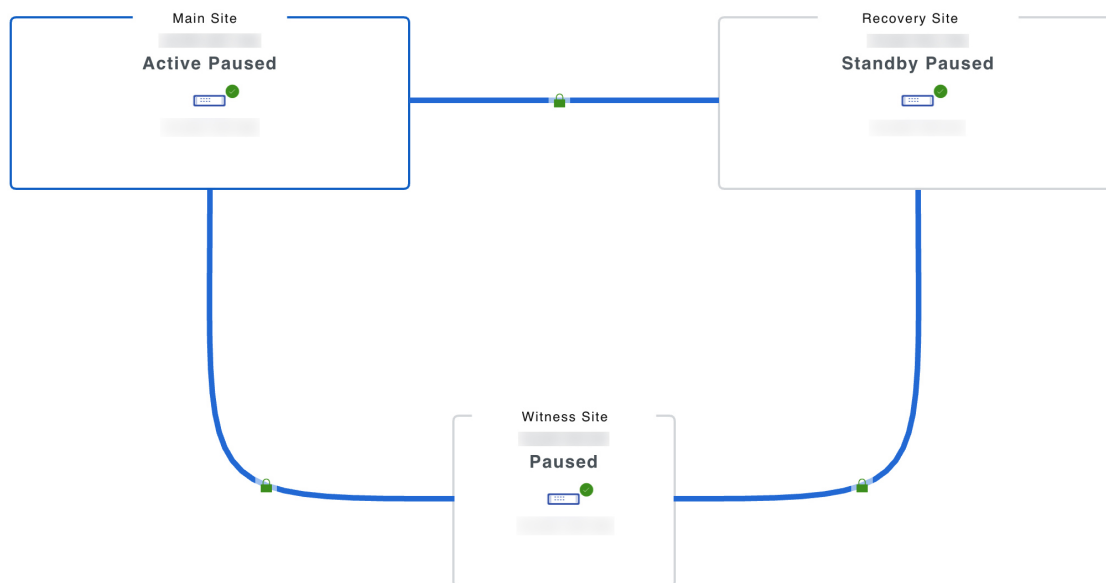
現在一時停止中またはフェールオーバーしているディザスタリカバリシステムを再起動するには、次の手順を実行します。

重要

この操作を実行する前に、現在のアクティブサイトに想定するすべてのデータ（特に最近の変更）があることを確認してください。この操作により、スタンバイサイトのデータベースがリセットされます。

1. メインメニューから次を選択します。[System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。



2. [Action] 領域で、[Rejoin] をクリックします。

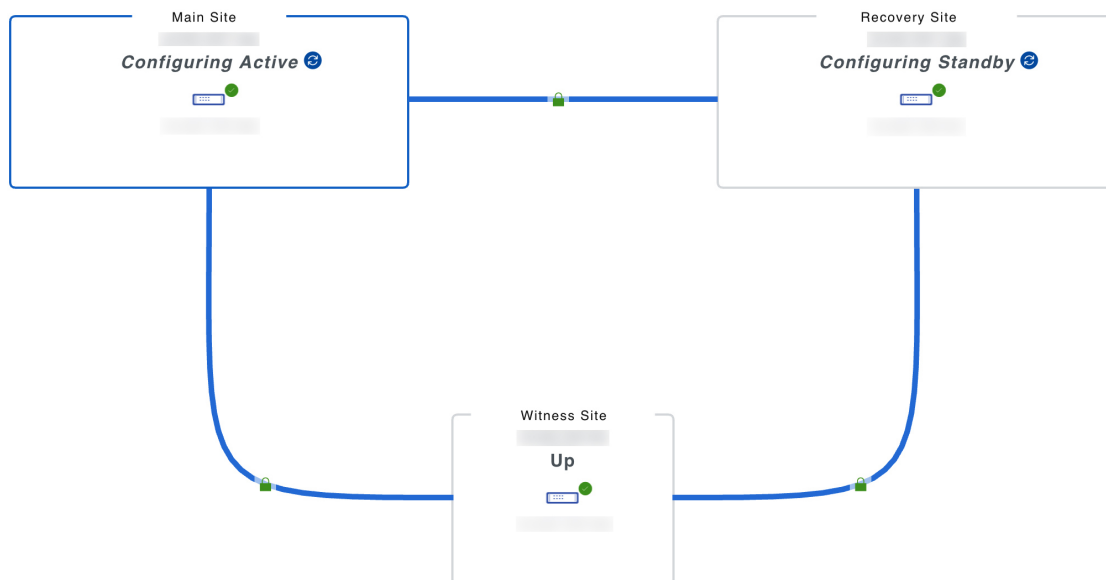
スタンバイサイトのすべてのデータが消去されることを示すダイアログが表示されます。

3. [Continue] をクリックして進みます。

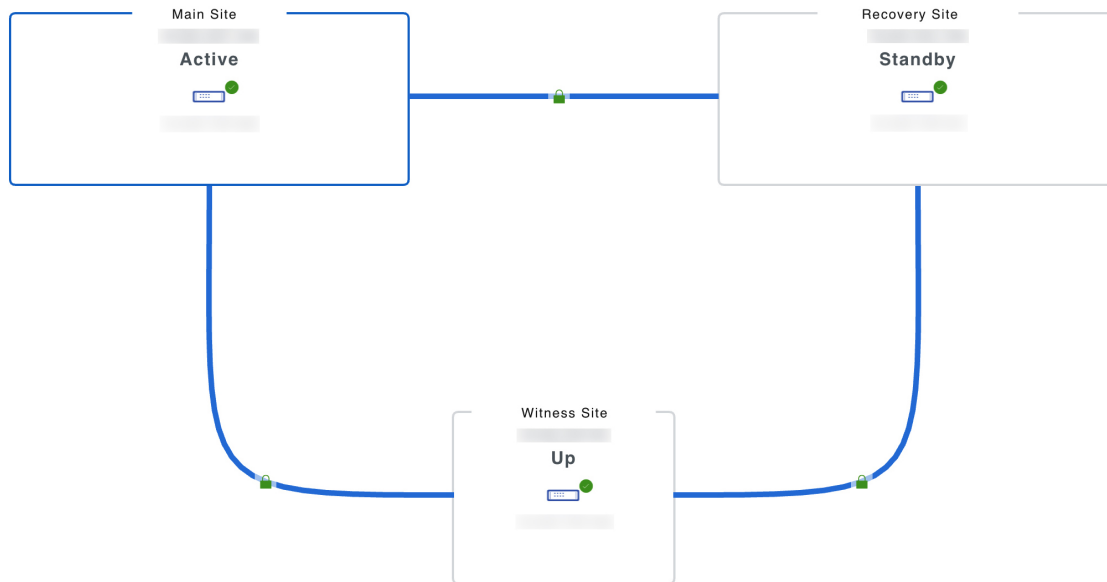
ページの右下隅に、メインサイト、リカバリサイト、および監視サイトを再接続するプロセスが開始されたことを示すメッセージが表示されます。このプロセスの実行中は、トポロジにおいて、メインサイトとリカバリサイトのステータスが **[Configuring]** に設定されます。

注

パッシブクラスタ上の **Postgres** データベースも、アクティブな **Catalyst Center** クラスターのスタンバイサイトとして再初期化されます。この移行中に、**[System Health]** ページで、**postgres** の異常が一時的にレポートされることがあります。再参加の完了後に、**postgres** に異常のラベルが付けられない限り、これは無視できます。



Catalyst Center で必要なタスクが完了すると、トポロジに表示されたメインサイト、リカバリサイト、および監視サイトのステータスが更新されます。



4. **[Status]** エリアに表示されたステータスが **[Up and Running]** になっていることを確認して、ディザスタリカバリシステムが稼働状態に戻ったことを確認します。

ディザスタリカバリシステムのスタンバイサイトが新しいアクティブサイトになる場合のフェールオーバーの概要。

フェールオーバーが実行されると、ディザスタリカバリシステムのスタンバイサイトがそれまでのアクティブサイトの役割を引き継ぎ、新しいアクティブサイトになります。**Catalyst Center** では、次の 2 種類のフェールオーバーをサポートしています。

- システムトリガー：ハードウェアの不具合やネットワークの停止などの問題によってシステムのアクティブサイトがオフラインになると実行されます。**Catalyst Center** では、アクティブサイトがエンタープライズ ネットワークの他の要素（およびスタンバイサイトと監視サイト）と 7 分間通信できなかったことを認識すると、スタンバイサイトがその役割を引き受けるのに必要なタスクを完了するため、中断することなくネットワーク動作を継続できます。
- 手動：ネットワーク管理者であるユーザーがシステムのアクティブサイトとスタンバイサイトの現在の役割を入れ替えるように **Catalyst Center** に指示することで実行されます。通常は、サイトのアプライアンスにインストールされている **Catalyst Center** ソフトウェアの更新前やサイトの定期メンテナンスの実行前に行います。

いずれかの種類のフェールオーバーの実行後、前のアクティブサイトがオンラインに戻ると、ディザスタリカバリシステムは自動的に **[Standby Ready]** 状態に移行します。このサイトを新しいスタンバイサイトとして確立するには、**[Monitoring]** タブの **[Action]** 領域で **[Rejoin]** をクリックします。

現在のアクティブサイトで問題が発生し、スタンバイサイトを新しいアクティブサイトとして指定する場合の手動フェールオーバーの開始に関する情報。

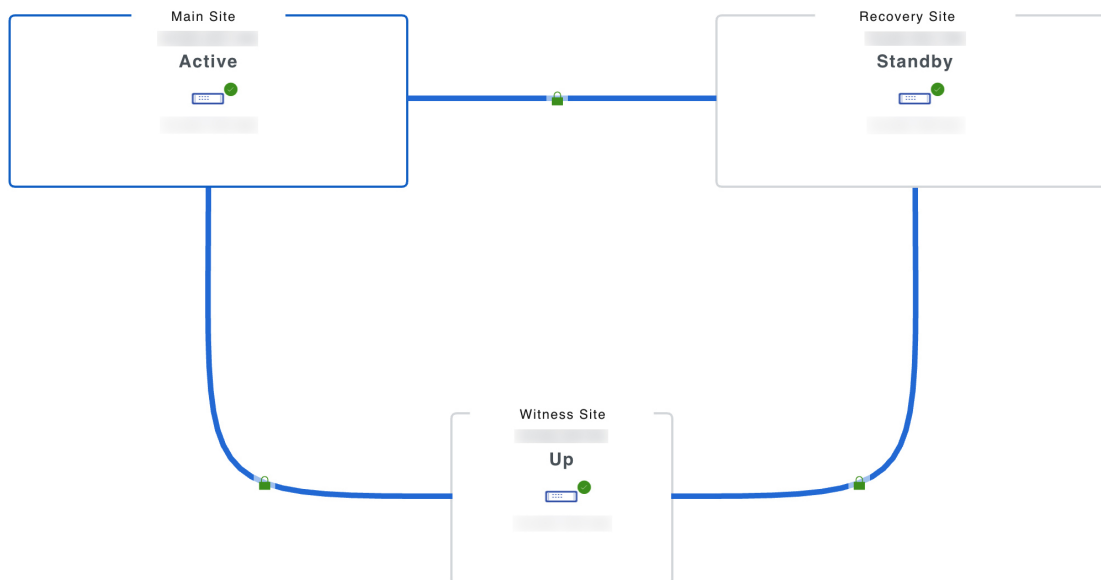
手動でフェールオーバーを開始する場合は、**Catalyst Center** でディザスタリカバリシステムのメインサイトとリカバリサイトに現在割り当てられているロールを入れ替えます。手動フェールオーバーは、現在のアクティブサイトで問題が発生していることが判明し、スタンバイサイトを新しいアクティブサイトとしてプロアクティブに指定する場合に便利です。手動フェールオーバーを開始するには、次の手順を実行します。

注

手動フェールオーバーは、監視サイトから開始することはできません。これは、現在アクティブなサイトからのみ実行できます。

1. メインメニューから次を選択します。[System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。次の例では、ユーザーは現在のアクティブサイトにログインしています。



2. [Action] 領域で、[Manual Failover] をクリックします。

スタンバイサイトのロールを [Active] に切り替えることを示す [Disaster Recovery Manual Failover] ダイアログが表示されます。

3. [Continue] をクリックして進みます。

ページの右下隅に、フェールオーバープロセスが開始されたことを示すメッセージが表示されます。これまでアクティブサイトとして機能していたサイトは、システムから切り離されます。

この時点で、メインサイトとリカバリサイトの接続が解除され、データの複製は行われなくなります。前のアクティブサイトに問題がある場合は、この間にそれらの問題を解決します。

前のアクティブサイトをディザスタリカバリシステムに再度追加するまで、次のフェールオーバー（システムによるフェールオーバーとユーザーによるフェールオーバーの両方）を開始することはできません。

4. メインサイトとリカバリサイトを再接続し、ディザスタリカバリシステムを再設定します。
 - a. Catalyst Center ウィンドウが更新されたら、**[Go To Recovery Cluster]** をクリックします。



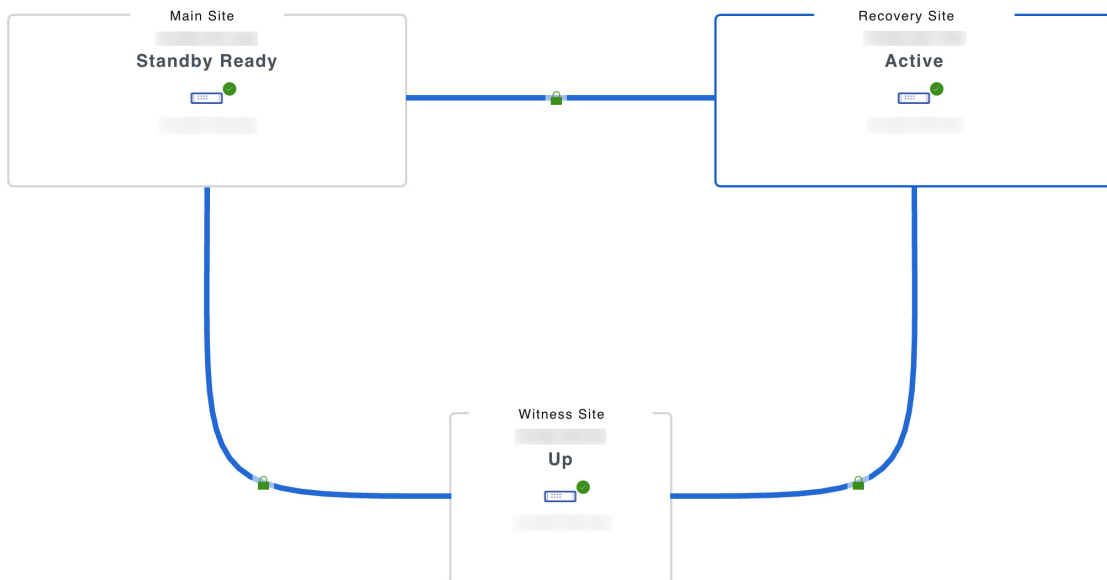
Go to the recovery cluster () to perform Catalyst Center operations.

If the other cluster is also down and cannot be restored, you may choose the Standalone action to remove this cluster from the disaster recovery system and make it a standalone Catalyst Center cluster.

Go To Recovery Cluster

- b. リカバリサイトにログインします。

これまでアクティブサイトとして機能していたサイトは、システムから切り離されて **[Standby Ready]** 状態になります。

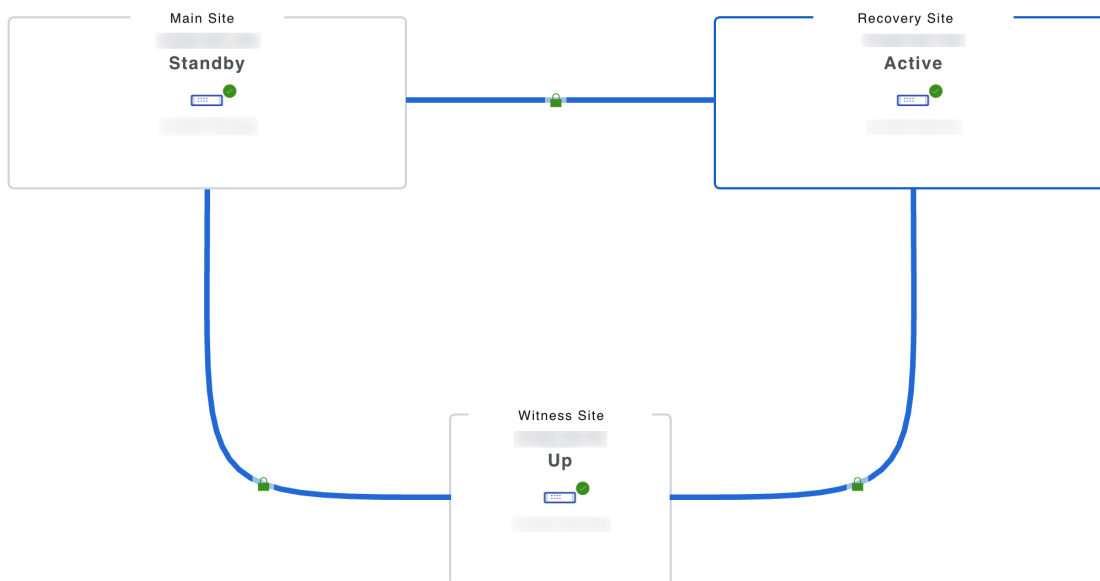


- c. **[Action]** 領域で、**[Rejoin]** をクリックします。

スタンバイサイトのデータが消去されることを示すダイアログが表示されます。

5. **[Continue]** をクリックして次に進み、データの複製を再開します。

Catalyst Center で関連するワークフローが完了すれば、手動フェールオーバーは完了です。現在アクティブサイトとして機能していたメインサイトがスタンバイサイトになります。



6. ディザスタリカバリシステムが稼働状態に戻ったことを確認します。
 - a. [Monitoring] タブの右上に表示されたステータスが [Up and Running] になっていることを確認します。
 - b. イベントのタイムラインで、[Rejoin] タスクが正常に完了したことを確認します。

Event Timeline

Hide Timeline

Latest events

Last Update: Mar 19, 2025 7:38:04 PM

✓

▼

Re-Join - [REDACTED]

Mar 19, 2025 7:35:50 PM

Start Time:

Mar 19, 2025 7:28:36 PM

Status Message:

Successfully setup disaster recovery

End Time:

Mar 19, 2025 7:35:50 PM

✓

>

Configure active - [REDACTED]

Mar 19, 2025 7:32:48 PM

✓

>

Configure standby - [REDACTED]

Mar 19, 2025 7:35:40 PM

ディザスタリカバリシステムの登録解除に関する情報。サイトに入力した設定を更新するには、登録解除が必要になる場合があります。

ディザスタリカバリシステムがアクティブ化された後、特定のサイトについて入力した設定の更新が必要になることがあります。この状況が発生した場合は、次の手順を実行します。

 注

システムを登録解除すると、システム内のすべてのサイトに関する現在の設定がクリアされます。

1. [Action] 領域で、[Pause] をクリックしてシステムの運用を一時停止します。
詳細については、[システムの一時停止](#)（286ページ）を参照してください。
2. [Action] 領域で、[Deregister] をクリックします。
Catalyst Center で以前にシステムのサイトについて設定した内容がすべて削除されます。
3. 適切な設定を入力してサイトを再登録し、システムを再度アクティブ化するには、[ディザスタリカバリのセットアップ](#)（272ページ）で説明されているタスクを実行します。

ディザスタリカバリシステムを管理する際の考慮事項についての情報。

このセクションでは、ディザスタリカバリシステムを管理する際の注意事項について説明します。

ディザスタリカバリシステムのバックアップと復元に関する考慮事項についての情報。

- バックアップは、システムのアクティブサイトからのみスケジュールできます。
- バックアップファイルの復元は、ディザスタリカバリが有効になっている状態では実行できません。まずシステムを一時停止する必要があります。詳細については、[システムの一時停止](#)（286ページ）を参照してください。
- バックアップファイルの復元は、システムを一時停止する前にアクティブだったサイトでのみ実行してください。バックアップファイルを復元した後、システムのサイトに再参加する必要があります。これにより、ディザスタリカバリが再開され、アクティブサイトのデータのスタンバイサイトへの複製が開始されます。詳細については、[システムへの再参加](#)（288ページ）を参照してください。
- バックアップファイルの復元は、システム内の他のノードと同じバージョンの **Catalyst Center** がインストールされているクラスタノードでのみ実行できます。
- フェールオーバーが発生すると、展開のバックアップと復元の設定およびスケジュールは、新しいアクティブサイトに複製されません。再度構成する必要があります。
- 展開に適用する場合は、**Catalyst Center** への着信 TLS 接続の TLS バージョンをアップグレードすることをお勧めします。『[Catalyst Center Security Best Practices Guide](#)』の「[Change the Minimum TLS Version and Enable RC4-SHA \(Not Secure\)](#)」トピックを参照してください。メインサイトをすでにアップグレードしている場合は、リカバリサイトもアップグレードすることをお勧めします（理想的には、ディザスタリカバリシステムをアクティブ化する前、またはフェールオーバーが発生した後）。

ノードまたはクラスタの交換に関する考慮事項についての情報。

ディザスタリカバリシステムの構成を壊さずに、次のいずれかの交換を実行することはできません。

- **1+1+1** セットアップでノードの **1** つを置き換える。
- **3+3+1** セットアップで **1** つのサイトのすべてのノードを置き換える。

この必要がある場合は、[システムの登録解除](#)（293ページ）で説明されている手順を完了して、システムを再起動してください。

ディザスタリカバリシステムの再構成に関する考慮事項についての情報。

- リカバリサイトにあるアプライアンスに存在するデータは、次のシナリオで削除されます。
 - ディザスタリカバリシステムを初めてセットアップし、システムをアクティブ化するとき。
 - リカバリサイトが現在アクティブなサイトである場合に、システムを一時停止し、登録を解除してから、リカバリサイトとして再登録するとき。
- 既存のディザスタリカバリシステムを再構成するときは、どのサイトが現在アクティブなサイトであるかを確認し、それをシステムのメインサイトとして登録してください。または、リカバリサイトのデータ（現在アクティブな場合）のバックアップを作成し、システムの再構成の前にこのデータをシステムのメインサイトに復元することもできます。
- 次の変更は、システムを再構成せずに行うことはできません。
 - ディザスタリカバリシステムのエンタープライズおよび管理インターフェイスに設定された IP アドレスと静的/デフォルトルートの変更。
 - 監視サイトの IP アドレスを変更しています。
 - サイトの **cluster_hostname** 設定の更新。
 - システムの BGP 設定を変更しています。

[システムの登録解除](#)（293ページ）で説明されている手順を実行して、新しい IP アドレスとルートを設定します。**cluster_hostname** 値を更新した場合は、更新後に同じ手順を実行します。

HA

ディザスタリカバリシステムの HA に関する考慮事項についての情報。

ディザスタリカバリシステムの構成を壊さずに、メインサイトとリカバリサイトを単一ノードクラスタから HA クラスタに変換することはできません。必要な場合は、次の手順を実行します。

1. [システムの登録解除](#)（293ページ）。
2. 両方のサイトを HA クラスタに変換します。
3. 再登録し、ディザスタリカバリを再アクティブ化します（[ディザスタリカバリのセットアップ](#)（272ページ）を参照）。

ディザスタリカバリシステムのサイト障害に関する考慮事項についての情報。

デフォルトでは、ディザスタリカバリシステムは 7 分間待機してから、サイトに障害が発生したことを認識し、次のいずれかのアクションを実行します。

- アクティブサイトがダウンすると、フェールオーバープロセスが開始されます。
- スタンバイサイトまたは監視サイトのいずれかがダウンすると、システムはそのサイトをダウンとしてマークし、[Action] 領域からタスクを開始する機能を無効にします。

7 分が経過する前にタスクを開始しようとする、完了できない理由を示すメッセージが [Details] 領域に表示されます。

ディザスタリカバリシステムで使用されている証明書の期限が切れたらどうなりますか。

[Status] エリアは、ディザスタリカバリシステム用に設定された証明書の有効期限が切れたときに表示されます。証明書が 90 日以内に期限切れになる場合は、次の警告メッセージが表示されます。

Status: Up and Running

The disaster recovery system is up and running. It will perform replication as needed.

CERTIFICATE STATUS

⚠ **The Disaster Recovery Certificates will expire in 89 days.** One day before the expiration, the disaster recovery system will automatically pause and discontinue replicating data. To avoid any interruption in service, please follow the steps below for the certificate renewal.

証明書の有効期限が 30 日以下の場合は、代わりに次のエラーメッセージが表示されます。

Status: Up and Running

The disaster recovery system is up and running. It will perform replication as needed.

CERTIFICATE STATUS

✖ **The Disaster Recovery Certificates will expire in 29 days.** One day before the expiration, the disaster recovery system will automatically pause and discontinue replicating data. To avoid any interruption in service, please follow the steps below for the certificate renewal.

証明書が 1 日後に期限切れになるように設定されていて、ディザスタリカバリシステムが動作している場合、Catalyst Center はシステムを自動的に一時停止します。

Status: Paused

The disaster recovery system is now paused. Main and Recovery Sites are two standalone clusters. There is no replication between these two sites. Click 'Re-Join' to form the disaster recovery system again and resume replication.

CERTIFICATE STATUS

✖ **The Disaster Recovery Certificates will expire in 1 day.** The disaster recovery system has paused and the data replication stopped. To avoid any interruption in service, please follow the steps below for the certificate renewal.

新しい証明書を設定してシステムの動作を復元するには、次のタスクを実行する必要があります。

1. [ディザスタリカバリシステムの一時停止](#) (Catalyst Center が既に行っていない場合)。
2. 「[ディザスタリカバリ証明書の追加](#) (268ページ)」トピックで説明されている手順を実行して、システムの証明書を置き換えます。
3. [システムに再参加して再起動](#)してください。

VLAN

Catalyst Center に対して VLAN モードが有効になっている場合、ディザスタリカバリがサポートされないことを示します。

- VLAN モードの説明は、『[Cisco Catalyst Center Installation Guide](#)』の「Configure the Primary Node Using the Maglev Wizard」トピックのステップ 7 および 8 を参照してください。
- VLAN モード：
 - Maglev 設定ウィザードを使用して Catalyst Center アプライアンスを設定する場合にのみ有効にできます。
 - ブラウザベースの構成ウィザードを使用して有効にすることはできません。
 - アプライアンスを再イメージ化せずに無効にすることはできません。
- 次の項目は、VLAN モードが有効になっている Catalyst Center 展開ではサポートされていません。
 - ACI ファブリック内の Catalyst Center
 - ディザスタリカバリ

一般的なディザスタリカバリ管理タスクを実行する方法について説明します。

このセクションでは、展開のディザスタリカバリシステムの管理中に実行する必要があるさまざまなタスクを完了する方法について説明します。

現在の監視サイトの置換に関する情報。

ディザスタリカバリシステムの現在の監視サイトを新しいサイトに置き換えるには、この手順を実行します。

-
1. 現在の監視サイトにログインします。
 - a) 監視サイトの SSH コンソールを開き、**ssh -p 2222 maglev@witness-site's-IP-address** コマンドを実行します。
 - b) デフォルトのユーザー (maglev) のパスワードを入力します。

 注

次の手順に進む前に、監視サイトのIPアドレスをメモしておきます。監視サイトを置き換えた後、同じアドレスを設定する必要があります。設定しない場合、監視サイトは期待どおりには機能しません。

2. **witness reset** コマンドを実行します。
3. 現在の監視サイトの仮想マシンを削除します。
4. **監視サイトのインストール** (270ページ) の説明に従って、新しい監視サイトの仮想マシンをインストールします。
5. 新しい監視サイトにログインします。
 - a) 監視サイトの SSH コンソールを開き、**ssh -p 2222 maglev@witness-site's-IP-address** コマンドを実行します。
 - b) デフォルトのユーザー (maglev) のパスワードを入力します。
6. **witness reconnect -w witness-site's-IP-address -m system's-virtual-IP-address -u admin-username** コマンドを実行します。

以下の点に注意してください。

- メインサイトの現在のディザスタリカバリステータスに関係なく、監視サイトを再接続するときは、メインサイトのエンタープライズ VIP を使用します。
- このコマンドの実行後に監視サイトが動作していることを確認するには、次の手順を実行します。
 - a. ディザスタリカバリポロジから、[Show Detail Information] リンクをクリックして、[Disaster Recovery System] スライドインペインを開きます。
 - b. [Witness Site] セクションで、監視サイトと設定済みの IPSec リンクのステータスが [Up] であることを確認します。
- このコマンドで使用可能なすべてのオプションを表示するには、**witness reconnect --help** コマンドを実行します。

イベントタイムラインのモニタリングに関する情報。

イベントのタイムラインから、現在実行されているディザスタリカバリタスクの進捗状況を追跡し、それらのタスクが完了したときに確認できます。タイムラインを表示するには次の手順を実行します。

1. メインメニューから次を選択します。[System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。
デフォルトでは、[Monitoring] タブが選択されています。
2. ページの下部までスクロールします。

システムに対する進行中のタスクと完了したタスクが、最新のタスク (完了時のタイムスタンプに基づく) から順番に降順で表示されます。Catalyst Center では、それぞれのタスクについて、システム (☒) またはユーザー (👤) のどちらによって開始されたかが示されます。

Event Timeline [Hide Timeline](#)

Latest events

Last Update: Mar 19, 2025 7:41:10 PM

The image shows a vertical timeline on the left with two green circular markers. To the right, two event cards are listed. The first card is titled 'Re-Join - [redacted]' with a timestamp of 'Mar 19, 2025 7:35:50 PM'. The second card is titled 'Manual failover - [redacted]' with a timestamp of 'Mar 19, 2025 7:23:29 PM'. Each card has a right-pointing chevron icon.

たとえば、システムの一時停止後の復元についてモニターするとします。この場合、復元プロセスの各タスクが開始されたときと完了したときに、**Catalyst Center** でイベントのタイムラインが更新されます。特定のタスクにおける処理の概要を表示するには、[>] をクリックします。

Event Timeline [Hide Timeline](#)

Latest events

Last Update: Mar 19, 2025 7:41:47 PM

The image shows a vertical timeline on the left with two green circular markers. The first marker is expanded, showing a detailed event card for 'Re-Join - [redacted]' with a timestamp of 'Mar 19, 2025 7:35:50 PM'. This card includes the following details:

- Start Time:** Mar 19, 2025 7:28:36 PM
- Status Message:** Successfully setup disaster recovery
- End Time:** Mar 19, 2025 7:35:50 PM

 Below this main card, two sub-tasks are listed:

- 'Configure active - [redacted]' with a timestamp of 'Mar 19, 2025 7:32:48 PM'.
- 'Configure standby - [redacted]' with a timestamp of 'Mar 19, 2025 7:35:40 PM'.

 Each sub-task card also has a right-pointing chevron icon.

Catalyst Center は、完了した関連するサブタスクを示します。

Event Timeline [Hide Timeline](#)

Latest events

Last Update: Mar 19, 2025 7:44:07 PM

✓ **Re-Join - [redacted]** Mar 19, 2025 7:35:50 PM

Start Time:
Mar 19, 2025 7:28:36 PM

Status Message:
Successfully setup disaster recovery

End Time:
Mar 19, 2025 7:35:50 PM

✓ **Configure active - [redacted]** Mar 19, 2025 7:32:48 PM

Start Time:
Mar 19, 2025 7:28:49 PM

Status Message:
Successfully configured active system

End Time:
Mar 19, 2025 7:32:48 PM

✓ > Starting BGP VIP advertisement for Disaster Recovery System. - [redacted] Mar 19, 2025 7:32:42 PM

✓ > Starting BGP session. - [redacted] Mar 19, 2025 7:32:37 PM

✓ > Configuring global VIPs for Disaster Recovery System. - [redacted] Mar 19, 2025 7:31:52 PM

タスクと同様に、[>] をクリックして特定のサブタスクの概要情報を表示できます。

Event Timeline [Hide Timeline](#)

Latest events

Last Update: Mar 19, 2025 7:44:45 PM

✓ **Re-Join - [redacted]** Mar 19, 2025 7:35:50 PM

Start Time:
Mar 19, 2025 7:28:36 PM

Status Message:
Successfully setup disaster recovery

End Time:
Mar 19, 2025 7:35:50 PM

✓ **Configure active - [redacted]** Mar 19, 2025 7:32:48 PM

Start Time:
Mar 19, 2025 7:28:49 PM

Status Message:
Successfully configured active system

End Time:
Mar 19, 2025 7:32:48 PM

✓ **Starting BGP VIP advertisement for Disaster Recovery System. - [redacted]** Mar 19, 2025 7:32:42 PM

Start Time:
Mar 19, 2025 7:32:40 PM

Status Message:
Start BGP VIP advertisement for Disaster Recovery System workflow completed successfully.

End Time:
Mar 19, 2025 7:32:42 PM

✓ > Starting BGP session. - [redacted] Mar 19, 2025 7:32:37 PM

イベントタイムラインのモニタリング中に発生する可能性のある問題とその解決方法については、[ディザスタリカバリシステムのトラブルシューティング](#) (307ページ) を参照してください。

複製時にモニターされるマネージドサービスと、考えられる 4 つのステータスメッセージについて説明します。

ディザスタリカバリシステムをアクティブにすると、Catalyst Center は GlusterFS、MongoDB、および PostgreSQL サービスのデータレプリケーションステータスのモニタリングを開始します。これらのサービスの複製が行われるたびに、**[Status]** エリアに次のいずれかのメッセージが表示されます。

- 複製が正常に完了しています。

ONGOING DATA REPLICATION

✓ Ongoing data replication is proceeding within the normal range of latency.

- 複製は完了していますが、現在、システムのメインサイトとリカバリサイトの間でデータ同期のタイムラグがあり、20 分以上になっています。

ONGOING DATA REPLICATION

⚠ Ongoing data replication is slowing down. You may want to be on the lookout for the status of network and/or system.

- 複製は完了していますが、システムのメインサイトとリカバリサイトの間でデータ同期のタイムラグが 30 分以上あります。

ONGOING DATA REPLICATION

✗ Ongoing data replication is slowing down significantly. **Please check the system and network. Contact Cisco support if the issue persists.**

- 複製が停止しました。

ONGOING DATA REPLICATION

✗ Ongoing data replication has stopped. It is critical to keep the data of the secondary site in-sync with the primary site. **Please check the system and network. Contact Cisco support immediately to prevent data loss.**

これらのメッセージでは、マネージドサービスの複製にタブを維持し、ネットワークまたはシステムの問題がシステムのサイト間でのこれらのサービスのデータの同期に影響を与える場合を示します。

ディザスタリカバリシステムの現在の状態に関する情報。

ディザスタリカバリ GUI の **[Status]** 領域には、システムの現在の状態が表示されます。次の表で、システムトポロジに表示される個々のサイトの状態を説明します。

14 :

状態	説明
Unregistered	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Initializing	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために、他のサイトが必要とするデータを送信する準備をしています。
Initialized	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトに送信するデータを正常に準備しました。

状態	説明
Failed to Initialize	登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトが必要とするデータを送信する準備をしているときに、サイトでエラーが発生しました。
Connecting Recovery	メインサイトは、リカバリサイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Connecting Witness	メインサイトは、監視サイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Recovery Site Connected	メインサイトは、リカバリサイトとのセキュア通信を正常に確立しました。
Failed to Connect Recovery	リカバリサイトとの安全なチャネルを確立しているときに、メインサイトでエラーが発生しました。
Failed to Connect Witness	監視サイトとの安全なチャネルを確立しているときに、メインサイトでエラーが発生しました。
Registered	アクティブサイトは、他の 2 つのサイトとのセキュア通信を正常に確立しました。
Deregistering	システムから現在のディザスタリカバリ構成を削除します。
Deregister Failed	システムから現在のディザスタリカバリ構成を削除しているときにエラーが発生しました。
Validating	ディザスタリカバリ構成を開始する前に、システムの状態を検証しています。
Validated	ディザスタリカバリ構成を開始する前に、システムの状態を正常に検証しました。
Validation Failed	ディザスタリカバリ構成を開始する前のシステムの状態を検証中にエラーが発生しました。
Configuring Active	このサイトをアクティブサイトとして確立するためのワークフローを実行しています。
Failed to Configure	このサイトでディザスタリカバリを有効にするワークフローの実行中にエラーが発生しました。
Syncing Config Data	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しています。
Config Data Synced	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを正常に同期しました。
Active Sync Failed	保留中のアクティブサイトが、ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しているときにエラーが発生しました。
Waiting Standby Configuration	このサイトをアクティブサイトとして確立するためのワークフローが正常に完了しました。スタンバイサイトのワークフローが完了するのを待っています。
Active	サイトは、アクティブサイトとしてネットワークを正常に管理しています。

状態	説明
Failed to Configure	サイトは、ディザスタリカバリクラスタのアクティブサイトとして自身を有効にするワークフローの一部を実行できませんでした。
Isolating	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができていないため、自身を隔離するワークフローを実行しています。
Isolated	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができていないため、自身を隔離するワークフローを正常に実行しました。
Failed to Isolate	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができていないため、自身を隔離するワークフローを実行中にエラーが発生しました。
Configuring Active	（システムトリガーまたは手動フェールオーバーの一部として）以前のスタンバイサイトをアクティブサイトとして構成しています。
Failed during Failover	（フェールオーバーまたは 2 つのシステムの障害からのリカバリの一部として）このサイトをアクティブサイトとして確立するワークフローの実行中にエラーが発生しました。
Pausing Active	（管理操作または計画的な停止に備えるために）アクティブサイトでディザスタリカバリ操作を無効にするワークフローを実行しています。
Active Paused	アクティブサイトでディザスタリカバリ操作を無効にしました。
Failed to Pause Active	アクティブサイトでディザスタリカバリ操作を無効にしているときにエラーが発生しました。
Active Stand Alone	他の 2 つのサイトとの接続を失った以前のアクティブサイトを、すべてのディザスタリカバリ構成を削除することにより、独立したシステムとして確立するワークフローを実行しています。
Down	アクティブサイトは、他の 2 つのサイトとの接続を失いました。

15 :

状態	説明
Unregistered	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Initializing	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために、他のサイトが必要とするデータを送信する準備をしています。
Initialized	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトに送信するデータを正常に準備しました。
Failed to Initialize	登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトが必要とするデータを送信する準備をしているときに、サイトでエラーが発生しました。
Connecting Main	リカバリサイトは、メインサイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。

状態	説明
Connecting Witness	リカバリサイトは、監視サイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Main Site Connected	リカバリサイトは、メインサイトとのセキュア通信を正常に確立しました。
Failed to Connect Main	メインサイトとの安全なチャネルを確立しているときに、リカバリサイトでエラーが発生しました。
Failed to Connect Witness	監視サイトとの安全なチャネルを確立しているときに、リカバリサイトでエラーが発生しました。
Registered	スタンバイサイトは、他の 2 つのサイトとのセキュア通信を正常に確立しました。
Deregistering	システムから現在のディザスタリカバリ構成を削除します。
Deregister Failed	システムから現在のディザスタリカバリ構成を削除しているときにエラーが発生しました。
Validating	ディザスタリカバリ構成を開始する前に、システムの状態を検証しています。
Validated	ディザスタリカバリ構成を開始する前に、システムの状態を正常に検証しました。
Validation Failed	ディザスタリカバリ構成を開始する前のシステムの状態を検証中にエラーが発生しました。
Configuring Standby	このサイトをスタンバイサイトとして確立するためのワークフローを実行しています。
Failed to Configure	このサイトでディザスタリカバリを有効にするワークフローの実行中にエラーが発生しました。
Syncing Config Data	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しています。
Config Data Synced	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを正常に同期しました。
Standby Sync Failed	保留中のスタンバイサイトが、ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しているときにエラーが発生しました。
Waiting Active Configuration	このサイトをスタンバイサイトとして確立するためのワークフローが正常に完了しました。アクティブサイトのワークフローが完了するのを待っています。
Standby	サイトは、ディザスタリカバリクラスタのスタンバイサイトとして正常に構成されています。
Failed to Configure	サイトは、ディザスタリカバリクラスタのスタンバイサイトとして自身を有効にするワークフローの一部を実行できませんでした。
Isolating	他の 2 つのサイトとの接続が失われたため、サイトは自身を隔離するワークフローを実行しています。

状態	説明
Isolated	他の 2 つのサイトとの接続が失われたため、サイトは自身を隔離するワークフローを正常に実行しました。
Failed to Isolate	他の 2 つのサイトとの接続が失われたため、サイトが自身を隔離するワークフローを実行中にエラーが発生しました。
Configuring Standby	(手動フェールオーバーの一部として) 以前のアクティブサイトをスタンバイ準備サイトとして構成しています。
Standby Ready	以前のアクティブシステムは、(フェールオーバーの結果として) スタンバイシステムとして構成する準備ができています。
Pausing Standby	(管理操作または計画的な停止に備えるために) スタンバイサイトでディザスタリカバリ操作を無効にするワークフローを実行しています。
Standby Paused	スタンバイサイトでディザスタリカバリ操作を無効にしました。
Failed to Pause Standby	スタンバイサイトでディザスタリカバリ操作を無効にしているときにエラーが発生しました。
Standby Stand Alone	他の 2 つのサイトとの接続を失った以前のスタンバイサイトを、すべてのディザスタリカバリ構成を削除することにより、独立したシステムとして確立するワークフローを実行しています。
Down	サイトは、他の 2 つのサイトとの接続を失いました。

16 :

状態	説明
Unregistered	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Registered	このサイトが監視サイトとして指定され、検証チェックが正常に完了しました。
Up	監視サイトの設定が正常に完了しました。
Down	サイトは、他の 2 つのサイトとの接続を失いました。

ディザスタリカバリイベントの通知に関する情報

ディザスタリカバリイベントが発生するたびに通知を送信するように **Catalyst Center** を設定できます。これらの通知を設定およびサブスクライブする方法については、『[Cisco Catalyst Center Platform User Guide](#)』の「[Work with Event Notifications](#)」を参照してください。この手順を完了したら、**[Platform > Developer Toolkit > Events]** テーブルで **SYSTEM-DISASTER-RECOVERY-v2** イベントを選択し、サブスクライブしていることを確認します。

重要

ディザスタリカバリは、ベストエフォートベースで IPsec アップ/ダウン通知をサポートします。ネットワークの中断により、分散ストアへの書き込みが妨げられる場合、一部のアップ/ダウン通知がドロップされることがあります。ネットワーク通信が復元されると、イベント通知が再開されます。

サブスクリプション後、**Catalyst Center** は、システムの証明書の有効期限が切れたために IPsec セッションがダウンしていることを示す通知を送信します。証明書を更新するには、次の手順を実行します。

1. システムの一時停止 (286ページ)。
2. メインサイトとリカバリサイトの両方で、現在のシステム証明書を置き換えます。メインメニューから次を選択します。[**System > Settings > Certificates > System Certificates**] の順に選択します。
3. システムへの再参加 (288ページ)。

Catalyst Center が通知を生成するディザスタリカバリイベントを一覧表示します。

次の表に、ディザスタリカバリイベントを示します。**Catalyst Center** では、イベントが発生すると通知を生成します。

システムのヘルスステータス	イベント	通知
OK	ディザスタリカバリシステムが動作中です。	Activate DR (Disaster Recovery Setup Successful)
OK	メインサイトまたはリカバリサイトへのフェールオーバーが正常に完了しました。	Failover Successful
OK	メインサイトの登録が正常に完了しました。	Successfully Registered Main Site
OK	リカバリサイトの登録が正常に完了しました。	Successfully Registered Recovery Site
OK	監視サイトの登録が正常に完了しました。	Successfully Registered Witness Site
OK	ディザスタリカバリシステムが正常に一時停止しました。	DR Pause Success
OK	スタンバイサイトが動作しています。	Standby Site Up
OK	監視サイトが動作しています。	Witness Site Up
OK	ディザスタリカバリシステムが正常に登録解除されました。	Unregister Success
Degraded	メインサイトまたはリカバリサイトへのフェールオーバーが失敗しました。	Failover Failed
Degraded	スタンバイサイトが現在ダウンしているため、自動フェールオーバーは使用できません。	Standby Cluster Down

システムのヘルスステータス	イベント	通知
Degraded	監視サイトが現在ダウンしているため、自動フェールオーバーは使用できません。	Witness Cluster Down
Degraded	ディザスタリカバリシステムを一時停止できません。	Pause Failure
Degraded	BGP ルートアドバタイズメントが失敗しました。	BGP Failure
Degraded	システムのサイト間を接続する IPsec トンネルが動作中です。	IPsec Up
Degraded	システムのサイト間を接続する IPsec トンネルが現在ダウンしています。	IPsec Down
NotOk	ディザスタリカバリシステムの設定に失敗しました。	Activate DR Failure
NotOk	現在 [Standby Ready] 状態にあるサイトは、ディザスタリカバリシステムに再参加できません。	Activate DR Failure
NotOk	ディザスタリカバリシステムの登録解除に失敗しました。	Unregistration Failed
NotOk	メインサイトの登録に失敗しました。	Main Registration Failed
NotOk	リカバリサイトの登録に失敗しました。	Recovery Registration Failed
NotOk	監視サイトの登録に失敗しました。	Witness Registration Failed

ディザスタリカバリシステムのトラブルシューティングに関する情報。

次の表に、ディザスタリカバリシステムで発生する可能性がある問題とその対処方法を示します。

 注

ディザスタリカバリ操作が失敗またはタイムアウトした場合は、**[Retry]** をクリックして操作を繰り返します。問題が解消されず、その解決策が次の表に記載されていない場合は、**Cisco TAC** にお問い合わせください。

17:

エラーコード	メッセージ	ソリューション
SODR10007	Token does not match.	リカバリサイトの登録時に提供されたトークンが、メインサイトの登録時に生成されたトークンと一致しません。メインサイトの [Disaster Recovery] > [Configuration] タブで、 [Copy Token] をクリックして正しいトークンをコピーします。
SODR10048	Packages (<i>package names</i>) are mandatory and not installed on the main site.	システムを登録する前に、リストされているパッケージをインストールします。
SODR10056	Invalid credentials.	リカバリサイトおよび監視サイトの登録時に、メインサイトの正しいクレデンシャルを入力したことを確認します。
SODR10062	(<i>)</i> site is trying to (<i>)</i> with invalid IP address. Expected is (<i>)</i> ; actual is (<i>)</i> .	リカバリサイトおよび監視サイトの登録時に提供されたメインサイトの IP アドレスが、メインサイトの登録時に提供された IP アドレスと異なります。
SODR10067	Unable to connect to (<i>recovery or witness site</i>).	メインサイトが稼働していることを確認します。
SODR10072	All the nodes are not up for (<i>main or recovery site</i>).	サイトの 3 台のノードすべてが稼働しているかどうかを確認します。
SODR10076	High availability should be enabled on (<i>main or recovery</i>) site cluster.	次の手順を実行して、高可用性 (HA) を有効にします。 HA を有効にする必要があるサイトにログインします。 - メインメニューから次を選択します。 [System] > [Settings] > [System Configuration] > [High Availability] の順に選択します。 [Activate High Availability] をクリックします。
SODR10100	(<i>Main or recovery</i>) site has no third party certificate.	Catalyst Center で現在使用しているデフォルトの証明書をサードパーティ証明書に置き換えます。詳細については、 Catalyst Center サーバー証明書の更新 (28 ページ) を参照してください。

エラーコード	メッセージ	ソリューション
SODR10113	Save cluster metadata failed.	適切なリカバリ手順の実行については、 Cisco TAC にお問い合わせください。
SODR10118	Appliance mismatch between main () and recovery ().	メインサイトとリカバリサイトで異なるアプライアンスが使用されています。ディザスタリカバリを正常に登録するには、両方のサイトで同じ 56 または 112 コアアプライアンスを使用する必要があります。
SODR10121	Failed to advertise BGP. Reason: ().	詳細については、「 BGP ルートアドバタイズメントに関する問題のトラブルシューティング (315 ページ) 」を参照してください。
SODR10122	Failed to stop BGP advertisement. Reason: ().	詳細については、「 BGP ルートアドバタイズメントに関する問題のトラブルシューティング (315 ページ) 」を参照してください。
SODR10123	Failed to establish secure connection between main () and () ().	この問題に対する解決策はありません。 Cisco TAC に連絡して、サポートを受けてください。
SODR10124	Cannot ping VIP: (main, recovery, or witness site's VIP or IP address).	次のアクションを実行します。 - 指定したアドレスが正しいことを確認します。 - アドレスが他のアドレスから到達可能であるかどうかを確認します。
SODR10129	Unable to reach main site. ()	メインサイトに設定されたエンタープライズ仮想 IP アドレスが、リカバリサイトと監視サイトから到達可能であるかどうかを確認します。
SODR10132	Unable to check IP addresses are on the same interface. Retry the operation. ()	試行した操作をやり直します。
SODR10133	The disaster recovery enterprise VIP () and the IP addresses () are not configured or reachable via the same interface. Check the gateway or static routes configuration.	ディザスタリカバリシステムのサイト間の通信は、エンタープライズネットワークを介して行われます。メインサイトとリカバリサイトのエンタープライズ仮想 IP アドレス、および監視サイトの IP アドレスは、エンタープライズインターフェイスを介して到達できるようにする必要があります。 このエラーは、少なくとも 1 つのサイトが、企業インターフェイス以外のインターフェイスを使用して IP アドレスまたは仮想 IP アドレスを設定していることを意味します。

エラーコード	メッセージ	ソリューション
SODR10134	The disaster recovery management VIP (<i>VIP address</i>) and the IPs (<i>IP addresses</i>) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration.	管理インターフェイスに、ディザスタリカバリシステムの管理仮想IPアドレスを設定します。このエラーは、仮想IPアドレスが現在、管理クラスタの仮想IPアドレスを持たないインターフェイスで設定されていることを示します。管理インターフェイスで設定されている管理仮想IPアドレスに /32 静的ルートを追加します。
SODR10136	Certificates required to establish IPsec session not found.	[System Certificate] ページ ([System > Settings > Certificates > System Certificates] の順に選択) からサードパーティ証明書を再度アップロードして、登録を再試行します。問題が解決しない場合は、Cisco TAC にお問い合わせください。
SODR10138	Self-signed certificate is not allowed. Upload a third-party certificate and retry.	-

エラーコード	メッセージ	ソリューション
SODR10139	Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate.	メインサイトとリカバリサイトにインストールされているサードパーティ証明書に、ディザスタリカバリシステム用に指定された別の DNS 名があります。お使いのシステムの DNS 名を指定するサードパーティ証明書を生成し、この証明書を両方のサイトにアップロードします。  注 DNS 名にワイルドカードが使用されていないことを確認します。
SODR10140	Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.	メインサイトとリカバリサイトにインストールされているサードパーティ証明書で、ディザスタリカバリシステムの DNS 名が指定されていません。Catalyst Center では、この名前を使用して、システムのサイト間を接続する IPsec トンネルを設定します。お使いのシステムの DNS 名を指定するサードパーティ証明書を生成し、この証明書を両方のサイトにアップロードします。  注 DNS 名にワイルドカードが使用されていないことを確認します。
-	-	ネットワークのパーティショニングまたは別の条件により、システムで使用する 3 つのサイトすべてが接続されていない場合は、Catalyst Center でサイトのステータスを [Isolated] に設定します。適切なリカバリ手順の実行については、Cisco TAC にお問い合わせください。

エラーコード	メッセージ	ソリューション
-	External postgres services does not exists to check service endpoints.	次のアクションを実行します。 1. エラーが発生したサイトにログインします。 2. 次のコマンドを実行します。 • Kubectrl get sep -A • kubectrl get svc -A grep external 3. 結果の出力で、external-postgresを検索します。 4. 存在する場合は、kubectrl delete sep external-postgres -n fusion コマンドを実行します。 5. 以前に失敗した操作を再試行します。
-	Success with errors.	フェールオーバーの開始後またはディザスタリカバリシステムの一時停止後にこのメッセージが表示される場合は、1つ以上のサービスで軽微なエラーが発生したにもかかわらず操作が正常に完了したことを示しています。先に進み、[Rejoin] をクリックすることで、システムを再起動できます。これらのエラーは、その操作によって解決されます。
-	Failed.	このメッセージは、1つ以上のサービスで重大なエラーが発生したためにディザスタリカバリ操作が失敗したことを示しています。この障害をトラブルシューティングするために、イベントタイムラインを表示し、関連するエラーにドリルダウンすることをお勧めします。このメッセージが表示されたら、[Retry] をクリックして操作を再実行します。
-	Cannot ping VIP: (VIP address).	システムに設定されているエンタープライズ VIP アドレスが到達可能であることを確認します。
-	VIP drop-down list is empty.	システムの VIP アドレスとクラスタ内リンクが正しく設定されていることを確認します。
-	Cannot perform (disaster recovery operation) due to ongoing workflow: BACKUP. Please try again at a later time.	スケジュールされたバックアップの実行中にディザスタリカバリ操作がトリガーされました。バックアップの完了後に操作を再試行してください。

エラーコード	メッセージ	ソリューション
-	The GUI indicates that the standby site is still down after it has come back online.	スタンバイサイトがダウンしたときに、そのサイトを Catalyst Center の最初の試行でディザスタリカバリシステムから分離できなかった場合、2回目の試行が自動的に開始されないことがあります。この場合、そのサイトが稼働状態に戻っても、GUIではダウンしているものとして表示されます。スタンバイサイトがメンテナンスモードのままであるため、システムを再起動することもできません。 スタンバイサイトを復元するには、次の手順を実行します。 1. SSH クライアントで、スタンバイサイトにログインします。 2. maglev maintenance disable コマンドを実行して、サイトをメンテナンスモードから復旧させます。 3. Catalyst Center にログインします。 4. メインメニューから次を選択します。 [System] > [Disaster Recovery] の順に選択します。 デフォルトでは、[Monitoring] タブが選択されています。 5. ディザスタリカバリシステムを再起動するために、[Action] 領域で [Rejoin] をクリックします。
-	Multiple services exists for MongoDB to check node-port label.	デバッグ用に、MongoDB ノードポートがサービスとして公開されます。このポートを特定して非表示にするには、次のコマンドを実行します。 • kubectl get svc --all-namespaces grep mongodb • magctl service unexpose mongodb <port-number>
-	Multiple services exist for Postgres to check node-port label.	デバッグ用に、Postgres ノードポートがサービスとして公開されます。このポートを特定して非表示にするには、次のコマンドを実行します。 • kubectl get svc --all-namespaces grep postgres • magctl service unexpose postgres <port-number>

2

2 サイト障害シナリオを表示します。

2 サイト障害は、ディザスタリカバリシステムにある 3 つのサイトのうち少なくとも 2 つが同時にダウンした場合、またはサイトがパーティション化された場合に発生します。障害が発生したサイトを復元できるようにしてください。可能な場合は、ディザスタリカバリで自動的に再アクティブ化されますが、手動での再参加が必要です。システムが回復不能な場合、**Catalyst Center** がさまざまな障害シナリオにどのように対応するか、および実行する必要があるユーザーアクションについては、次の表を参照してください。

障害シナリオ	システムおよびユーザーの応答
シナリオ 1: 複数のサイトがダウンし、ほぼ同時にオンラインに戻ります。	1. システムは、アクティブサイトとスタンバイサイトを分離します。 2. システムはアクティブサイトを復元し、スタンバイサイトは [Standby Ready] 状態に入ります。 3. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムライン」を参照してください。 4. [Action] エリアで [Rejoin] をクリックして、ディザスタリカバリシステムを再アクティブ化します。
シナリオ 2: アクティブサイト、スタンバイサイト、および監視サイトがダウンします。アクティブサイトとスタンバイサイトはオンラインに戻りますが、監視サイトはオフラインのままです。	1. システムは、アクティブサイトとスタンバイサイトを分離します。 2. システムはアクティブサイトを復元し、スタンバイサイトは [Standby Ready] 状態に入ります。 3. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムライン」を参照してください。 4. 現在の監視サイトを置き換える (297 ページ)。 5. [Action] 領域で、[Rejoin] をクリックします。

障害シナリオ	システムおよびユーザーの応答
シナリオ 3 : アクティブサイト、スタンバイサイト、および監視サイトがダウンします。アクティブサイトと監視サイトはオンラインに戻りますが、スタンバイサイトはオフラインのままです。	1. システムはアクティブサイトを分離してから復元します。 2. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムライン」を参照してください。 3. 以前のアクティブサイトがオンラインに戻り、再アクティブ化された後。 スタンバイサイトのノードを交換する必要があると判断した場合は、代わりに次の手順を実行します。 a. 監視サイトにログインして witness reset コマンドを実行します。 b. アクティブサイトにログインし、[Standalone] をクリックしてから、[Continue] をクリックします。 c. スタンバイサイトのノードを交換します。 d. ディザスタリカバリのセットアップ (272ページ)。
シナリオ 4 : アクティブサイト、スタンバイサイト、および監視サイトがダウンします。スタンバイサイトと監視サイトはオンラインに戻り、アクティブサイトはオフラインのままです。	1. システムはスタンバイサイトを分離し、新しいアクティブサイトとして確立します。 2. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムライン」を参照してください。 3. 以前のアクティブサイトがオンラインに戻り、[Standby Ready] 状態になった後、[Action] エリアで [Rejoin] に従います。 以前のアクティブサイトでノードを交換する必要があると判断した場合は、代わりに次の手順を実行します。 a. 監視サイトにログインして witness reset コマンドを実行します。 b. アクティブサイトにログインし、[Standalone] をクリックしてから、[Continue] をクリックします。 c. 以前のアクティブサイトのノードを置き換えます。 d. ディザスタリカバリのセットアップ (272ページ)。

BGP

BGP ルートアドバタイズメントに関する問題のトラブルシューティングについての情報。

BGP ルートアドバタイズメント エラーを受信した場合は、次の手順を実行して原因をトラブルシュートします。

1. Catalyst Center クラスターで BGP セッションのステータスを検証します。

- a) イベントタイムラインで、**[Starting BGP advertisement]** タスクが正常に完了したことを確認します **[Activate Disaster Recovery System > View Details > Configure active > View Details]** の順に選択）。

タスクが失敗した場合は、次を実行してから手順 1b に進みます。

1. エラーメッセージに示されているネイバルルータが稼働しているかどうかを確認する。

2. ネイバルルータと **Catalyst Center** の接続があることを確認する。復元されない場合は、接続を復元します。その後、新しいディザスタリカバリシステムをアクティブにするか、一時停止された既存のシステムを再起動します。

- b) **Catalyst Center GUI** で、ディザスタリカバリシステムの論理トポロジを表示し、ネイバルルータが現在アクティブかどうかを確認します。

ダウンしている場合は、ルータの観点から、**Catalyst Center** クラスターが BGP ネイバーとして設定されているかどうかを確認します。そうでない場合は、クラスターをネイバーとして設定します。その後、新しいディザスタリカバリシステムをアクティブにするか、一時停止された既存のシステムを再起動します。

- c) **bgpd** および **bgpmanager** のログファイルを表示するには、次のコマンドを実行します。

- **sudo vim /var/log/quagga/bgpd.log**
- **magctl service logs -rf bgpmanager | lq**

ログファイルを表示するときは、エラーメッセージがないか確認します。メッセージがない場合は、BGP セッションが正しく機能していることを示します。

- d) **Catalyst Center** とそのネイバルルータ間の BGP セッションのステータスを確認します：**echo admin-password | sudo VTYSH_PAGER=more -S -i vtysh -c 'show ip bgp summary'** コマンド

コマンド出力で、ネイバルルータの IP アドレスを検索します。同じ行の末尾に、ルータの接続状態が **[0]** とリストされていることを確認します。この場合、BGP セッションがアクティブであり、適切に機能していることを示します。

2. エラーメッセージに示されているネイバルルータから、BGP セッションのステータスを検証します。

- a) **show ip bgp summary** コマンドを実行します。

- b) コマンド出力で、**Catalyst Center** クラスターの仮想 IP アドレスを検索します。同じ行の末尾に、クラスターの接続状態が **[0]** とリストされていることを確認します。この場合、BGP セッションがアクティブであり、適切に機能していることを示します。

- c) **show ip route** コマンドを実行します。

- d) コマンドの出力を表示し、**Catalyst Center** がディザスタリカバリシステムのエンタープライズ仮想 IP アドレスがアドバタイズされているかどうかを確認します。

たとえば、システムのエンタープライズ仮想 IP アドレスが **10.30.50.101** であるとしします。これが出力に表示される最初の IP アドレスである場合は、**Catalyst Center** がアドバタイズしていることを確認します。

15 Catalyst Center Cisco ISE

$$\vdots$$

- Catalyst Center
- Catalyst Center
- Catalyst Center
- Catalyst Center
- Catalyst Center Cisco ISE
- Catalyst Center Cisco ISE
- Catalyst Center
- Catalyst Center
- Catalyst Center
- Catalyst Center
- Catalyst Center

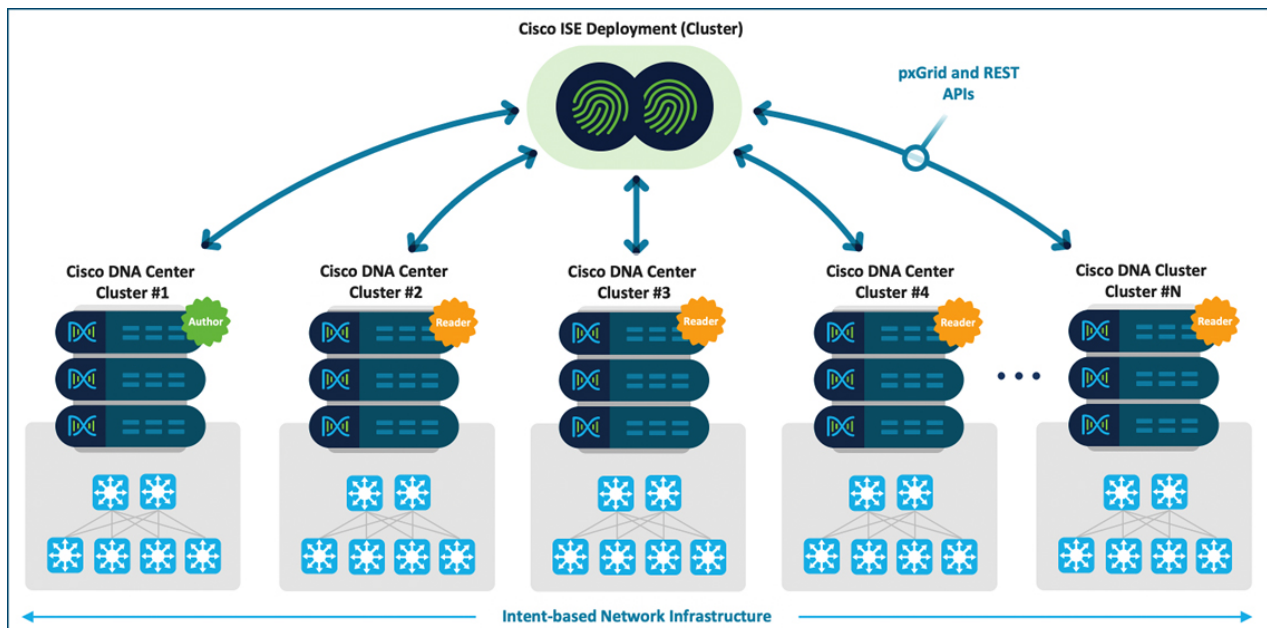
Catalyst Center

これは、複数の Catalyst Center 展開の概要です。

複数の Catalyst Center クラスターを単一の Cisco ISE システムと統合する場合、各 Catalyst Center クラスターは独立しています。クラスター間で情報が共有されることはありません。このシナリオでは、Cisco Software-Defined Access (SD-Access) が Catalyst Center に展開されると、一連の仮想ネットワーク (VN) と他のすべての SD-Access は各クラスターに対してローカルになります。

Catalyst Center では、単一の Cisco ISE システムと統合された複数の Catalyst Center クラスター間で SD-Access およびグループベースポリシー (GBP) 要素を調整するメカニズムを提供します。一貫した VN のセットによって複数の Catalyst Center クラスター間で SD-Access をグローバルに管理するため、複数の Catalyst Center 機能は Cisco ISE との既存のセキュアな接続を活用して、VN、セキュリティグループタグ (SGT)、アクセス契約、およびグループベースのアクセス制御 (GBAC) ポリシーを 1 つのクラスターから別のクラスターに提供します。Cisco ISE は、あるクラスター (作成者ノードと呼ばれる) から学習した情報を取得し、他のクラスター (リーダーノードと呼ばれる) に提供します。

Multiple Catalyst Center 機能は、Cisco ISE リリース 3.2 以降と統合すると使用できます。



注

- 複数の Catalyst Center の操作は、デフォルトで無効になっています。この機能を使用するには、**[Enable Multiple Catalyst Center operation]** ([**Advanced Settings**] 内) を選択して Catalyst Center を Cisco ISE と統合します。この機能は、初期設定時あるいは後から (Cisco ISE が統合された後) 有効にできます。この機能を有効にした後は、Cisco ISE 統合を削除するだけで機能を無効にできます。
- Cisco ISE の以前のリリースを使用している場合はアカウントチームに連絡し、限定提供プログラムに含めるための要求を Cisco SDA の設計審議会に送信する必要があります。複数の Catalyst Center 限定提供パッケージが利用可能になると、この機能の限定提供 (LA) バージョンにアクセスできます。詳細については、『[Multiple Cisco DNA Center to Single Cisco ISE Prescriptive Deployment Guide](#)』を参照してください。

複数の Catalyst Center 機能では、クラスターに固有のロールが指定されています。

- 作成者ノードクラスター
- リーダーノードクラスター

このトピックでは、複数の Catalyst Center の展開での作成者ノードクラスターについて説明します。

作成者ノードのロールは、Cisco ISE 展開と統合する最初のクラスター（**[Multiple] Catalyst Center** オプションが有効になっている）、または **[Multiple] Catalyst Center** オプションを有効にする最初のクラスターに割り当てられます。作成者ノードクラスターは、グループベースのポリシー（GBP）と Cisco SD-Access グローバルデータの管理ポイントです。作成者ノードクラスターは、VN、SGT、アクセス契約、および GBAC ポリシーを管理します。作成者ノードクラスターでのみ、VN および GBP コンポーネントを作成、変更、または削除できます。

作成者ノードクラスターは、Cisco ISE がこの情報を使用し、Cisco ISE pxGrid を介してリーダーノードロールの他のすべての Cisco Catalyst Center クラスターに公開できるよう、ERS（REST）API を介して Cisco ISE に VN および GBP 情報をプッシュします。

作成者ノードには 1 つのクラスターのみ指定できます。これは、GBP とユーザー定義のグローバル SDA データ（仮想ネットワークやエクストラネットポリシーなど）を管理できる唯一のノードです。

作成者ノードで SGT または VN が動作している場合、それらを削除することはできません。

このトピックでは、複数の Catalyst Center 展開でのリーダーノードクラスターについて説明します。

複数の Catalyst Center 機能が有効になっている他のすべての Catalyst Center クラスターには、リーダーノードクラスターのロールが割り当てられます。リーダーノードクラスターには、VN と SGT の読み取り専用ビューがあります。

リーダーノードクラスターは、作成者ノードクラスターで定義されているものと同じ VN、SGT、アクセス契約、および GBAC ポリシーを使用して保持しますが、リーダーノードクラスターにはアクセス契約またはポリシーは表示されません。

VN は、作成者ノードクラスターでのみ作成できます。VN を作成すると、ファブリック プロビジョニング操作で使用するために、リーダーノードクラスターに伝播します。リーダーノードクラスターは、仮想ネットワーク識別子（VNID）、ルートターゲット（RT）、そのクラスターにローカルなルート識別子（RD）などの関連ネットワーク属性を設定します。

VN および GBP 機能を除き、各リーダーノードクラスターは独立したクラスターとして独自のネットワークインフラストラクチャを管理します。

複数の Catalyst Center 機能を使用すると、単一の Cisco ISE に統合された複数の Cisco Catalyst Center クラスター全体でグローバルポリシーを管理できます。この機能で、複数の Cisco Catalyst Center クラスターで仮想ネットワークとファブリックを管理するという基本的な制限が変更されることはありません。VN は、複数の Catalyst Center クラスター間で同じ名前を持つことができます。これにより、複数のクラスター間で一貫したセキュリティグループと VN ネットワークの関連付けをサポートできます。ただし、個々のクラスターレベルでは、VN に関連付ける実際のネットワーク属性（VRF、ルートターゲット、ルート識別子など）はクラスター間で同一ではありません。これは、独立した Catalyst Center クラスターを操作する場合と同じです。

最大 4 つの Catalyst Center クラスターをリーダーノードクラスターとして追加できます。Catalyst Center ノードをリーダーとして追加する前に、Catalyst Center のリーダーノードクラスターで管理者が作成したすべての Cisco SD-Access グローバルデータを削除して、Cisco ISE と統合する必要があります。これにはデフォルト以外の VN（「DEFAULT_VN」および「INFRA_VN」以外のあらゆる VN、エクストラネットポリシーなど）が含まれます。デフォルト以外の GBP のポリシーデータ（SGT、アクセス契約、GBP）がある場合、ユーザー

はデフォルト以外のすべての GBP データを自動的にクリーンアップ（削除）するか、Cisco ISE にまだ存在しない GBP データをマージするかを選択できます。

注

- 単一の Cisco ISE 展開に統合できるのは 5 つの Catalyst Center クラスターのみです。これには 1 つの作成者ノードクラスターと最大 4 つのリーダーノードクラスターが含まれます。
- リーダーノードで使用されている場合でも、作成者ノードの SGT または VN を削除できます。その場合は、古い SGT または VN をリーダーノードで手動で削除する必要があります（参照を削除した後）。

Catalyst Center

このトピックでは、複数の Catalyst Center のポリシー管理について説明します。

Catalyst Center を Cisco ISE と統合し、GBP 同期を実行した後、ポリシー情報は Catalyst Center と Cisco ISE の間で同期されます。ポリシー作成権限は Catalyst Center 内にあります。SGT、セキュリティグループ ACL (SGACL)、および出力ポリシーの管理用の Cisco ISE ウィンドウは読み取り専用になります。

グループベースのポリシー（セキュリティグループ、アクセス契約、および GBAC ポリシー）は、Catalyst Center ではなく Cisco ISE で管理できます。

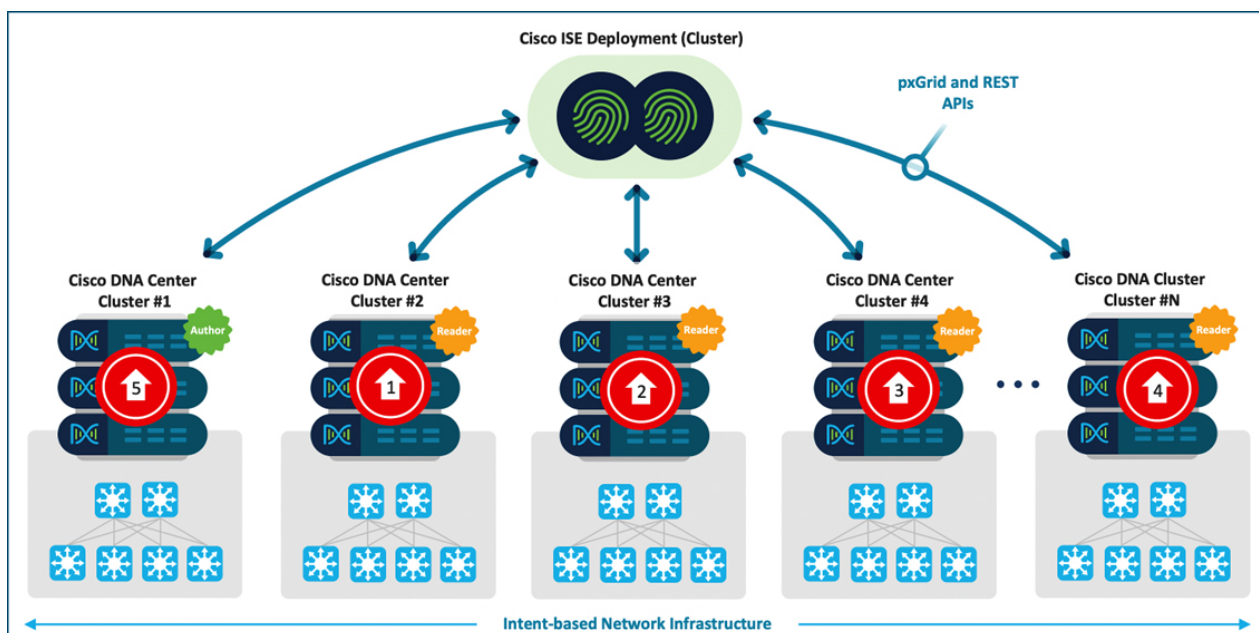
Catalyst Center GUI でメニューアイコンをクリックして、**[Policy] > [Group-Based Access Control] > [Policies] > [GBAC Configuration] > [Manage Group-Based Access Control in Cisco ISE]** の順に選択します。

Catalyst Center

このトピックでは、複数の Catalyst Center 展開のアップグレードに関する推奨事項について説明します。

複数の Catalyst Center 環境では、クラスターのアップグレードプロセス時を除き、すべての作成者ノードクラスターとリーダーノードクラスターで同じ Catalyst Center ソフトウェアバージョンを実行することをお勧めします。最初にすべてのリーダーノードクラスターをアップグレードしてから、作成者ノードクラスターをアップグレードすることで、ソフトウェアバージョン間の機能の不一致や非互換性を回避できます。アップグレードサイクルの途中でリーダーノードクラスターを作成者ノードロールに昇格させないでください。リーダーノードクラスターを昇格させる前に、すべての Catalyst Center クラスターをアップグレードして同じソフトウェアバージョンを実行する必要があります。

1: Catalyst Center



注

複数の Catalyst Center 機能の基本機能では、参加しているすべての作成者ノードクラスターとリーダーノードクラスターで同じソフトウェアバージョンを使用する必要はありません。ただし、一致しないコードバージョンを使用すると、クラスタ間で修正、機能、および特徴に違いが生じる可能性があります。すべての作成者ノードクラスターとリーダーノードクラスターで同じ Catalyst Center ソフトウェアバージョンを使用することをお勧めします。

Catalyst Center

このトピックでは、複数の Catalyst Center 展開シナリオについて説明します。

複数の Catalyst Center を展開するには 2 つのオプションがあります。

- 現在 Cisco ISE と統合されていない複数の Catalyst Center クラスタの新規展開。
- Cisco ISE と統合されている既存の Catalyst Center クラスタと、Cisco ISE と統合されていない新しい Catalyst Center クラスタ。

Catalyst Center

このタスクでは、複数の Catalyst Center の機能を有効にするワークフローについて説明します。

複数の Catalyst Center クラスタの機能はデフォルトでは無効になっています。Cisco ISE との統合中または統合後に有効にできます。複数の Catalyst Center の機能を有効にした後は、Cisco ISE の統合を完全に削除することによってのみ無効にできます。

 注

複数の Catalyst Center の操作には、pxGrid 機能が必要です。複数の Catalyst Center を有効にした後、pxGrid を無効にすることはできません。

1. Catalyst Center GUI でメニューアイコンをクリックして、**[System] > [Settings] > [Authentication and Policy Servers]** の順に選択します。
2. **[Cisco ISE]** を追加します。
3. 必要な Cisco ISE の情報を入力します。詳細については、「[Catalyst Center と Cisco ISE の統合](#)（75ページ）」を参照してください。
4. **[System] > [Settings] > [Authentication and Policy Servers] > [Add] > [ISE] > [Advanced Settings]** を選択します。

[Advanced Settings] スイッチには、**[Multiple Catalyst Center]** 操作を有効にするスイッチなどのさまざまな詳細オプションが表示されます。
5. **[Multiple Catalyst Center Operation]** オプションを有効にします。
6. （オプション）既存の Cisco ISE 統合を編集する場合は、Cisco ISE の管理者パスワードを再入力します。
7. **[Add]** をクリックします。

Catalyst Center Cisco ISE

このタスクでは、複数の Catalyst Center デバイスを単一の Cisco ISE に統合するワークフローについて説明します。

Catalyst Center と Cisco ISE を初めて統合する場合は前提条件があります。詳細については、[Catalyst Center と Cisco ISE の統合](#)（75ページ）を参照してください。

Catalyst Center がすでに Cisco ISE と統合されている場合は、**[Multiple] Catalyst Center** 操作を有効にした後、次の手順を実行して Catalyst Center と Cisco ISE を再統合します。これにより、Catalyst Center は作成者またはリーダーノードクラスターのロールをネゴシエートできます。ネゴシエートは複数の Catalyst Center 機能が有効化された Cisco ISE に最初に参加するノードか、あるいは後続のノードに基づいて行われます。

1. Catalyst Center GUI でメニューアイコンをクリックして、**[System] > [Settings] > [Authentication and Policy Servers]** の順に選択します。
2. **[Actions]** 列で、省略記号アイコン（）の上にカーソルを置き、**[Edit]** を選択します。
3. **[System] > [Settings] > [Authentication and Policy Servers] > [Add] > [ISE] > [Advanced Settings]** を選択します。
4. **[Multiple Catalyst Center Operation]** オプションを有効にします。
5. 再度 Cisco ISE の管理者パスワードを入力します。

6. **[Add]** をクリックします。Catalyst Center は Cisco ISE と作成者ノードロールをネゴシエートします。
 - 設定された Cisco ISE サーバーのステータスがパスワードの変更により **[FAILED]** になっている場合は、**[Retry]** をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。
 - スライドインペイン で統合ステータスを確認します。**[Authentication and Policy Server]** ウィンドウで、統合の **[Status]** が **[Active]** と表示されていることを確認します。
7. 作成者ノードとしてネゴシエートされたクラスタのロールを確認するには、**[システム (System)] > [設定 (Settings)] > [システム設定 (System Configuration)] > [複数の Catalyst Center の設定 (Multiple Catalyst Center Settings)]** の順に選択します。

Catalyst Center

Cisco ISE

このタスクでは、他の Catalyst Center クラスタをリーダーノードの形式で Cisco ISE と統合する方法について説明します。

複数の Catalyst Center が有効になっている同じ Cisco ISE と後続の Catalyst Center クラスタを統合するには、Catalyst Center クラスタにデフォルト以外の VN (「DEFAULT_VN」および「INFRA_VN」以外の VN) を含めることはできません。

[Policy > Virtual Network] で、統合するクラスタにデフォルトの VN のみが含まれていることを確認します。

1. Catalyst Center GUI でメニューアイコンをクリックして、**[System] > [Settings] > [Authentication and Policy Servers]** の順に選択します。
2. **[Add]** をクリックし、**[ISE]** を選択します。
3. 必要な Cisco ISE の情報を入力します。[Catalyst Center と Cisco ISE の統合 \(75ページ\)](#) を参照してください。
4. **[System] > [Settings] > [Authentication and Policy Servers] > [Add] > [ISE] > [Advanced Settings]** を選択します。
5. **[Multiple Catalyst Center Operation]** オプションを有効にします。
6. **[Add]** をクリックします。
7. (オプション) クラスタを Cisco ISE と初めて統合する場合は、スライドインペイン で **[Accept]** をクリックし、Catalyst Center が Cisco ISE によってプッシュされた証明書を受け入れられるようにします。スライドインペインを閉じます。
8. **[Authentication And Policy Servers]** ウィンドウで、統合のステータスが **[Active]** であることを確認します。
9. 作成者ノードとリーダーノードを確認するには、**[System > Settings > System Configuration > Multiple Cisco] Catalyst Center [Settings]** の順に選択します。

このトピックでは、複数の Catalyst Center 展開で仮想ネットワークを削除する方法について説明します。

作成者ノードクラスターは、リーダーノードクラスターでの仮想ネットワーク (VN) の使用状況を認識していません。作成者ノードクラスターで VN を削除する前に、すべてのリーダーノードクラスターで VN へのすべての参照を削除する必要があります。作成者ノードクラスターで VN を削除すると、作成者ノードと、その VN への参照がないリーダーノードクラスターで VN が削除されます。ただし、リーダーノードの 1 つがその VN を使用している場合、そのような VN のステータスは **[Out of sync with Author]** として表示されます。リーダーノードクラスター上の VN のすべての参照 (ホストのオンボーディングセクションの VN の追加や静的ポート割り当てなど) を削除してから、リーダーノードクラスター上の該当の VN の削除に進む必要があります。

このトピックでは、複数の Catalyst Center の展開でセキュリティグループを削除する方法について説明します。

作成者ノードクラスターは、リーダーノードクラスターでのセキュリティグループの使用状況を認識していません。作成者ノードクラスターでセキュリティグループを削除する前に、すべてのリーダーノードクラスターでセキュリティグループへのすべての参照を削除する必要があります。作成者ノードクラスターでセキュリティグループを削除すると、そのセキュリティグループは、作成者ノードクラスター、Cisco ISE、およびリーダーノードクラスター (参照がない場合) から削除されます。リーダーノードクラスターの 1 つがそのセキュリティグループを使用している場合、そのセキュリティグループのステータスには **[Out of sync with Author]** と表示されます。リーダーノードクラスターのセキュリティグループのすべての参照を削除してから、そのリーダーノードクラスター上のセキュリティグループを削除してください。

このトピックでは、必要に応じてリーダーノードを作成者ロールに昇格させる方法について説明します。

複数の Catalyst Center ソリューションアーキテクチャには複数の Catalyst Center クラスターがあり、1 つのクラスターのみをポリシー作成者にすることができます。管理者はリーダーノードクラスターを昇格させて、作成者ノードクラスターのロールを引き継ぐ必要がある場合があります。この昇格は、次の場合にのみ実行する必要があります。

- 作成者ノードクラスターをサービス停止状態にするか、長期間使用できないようにします。
- 作成者ノードクラスターが永続的に使用できないか、長期間にわたって応答せず、その間にポリシーの変更が必要な場合。

リーダーノードから作成者ノードへのこの昇格は、次の 2 つの方法で実行できます。

1. リーダーノードの作成者ロールへのグレースフル昇格。
2. リーダーノードの作成者ロールへの強制昇格。

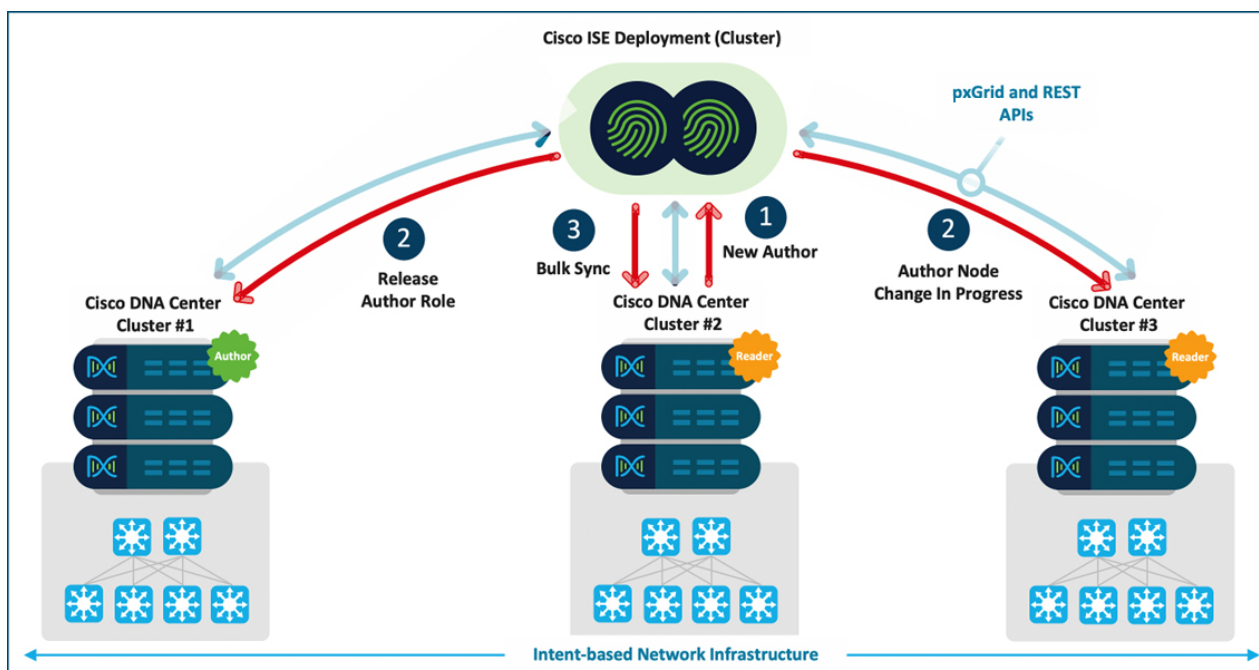
このタスクでは、リーダーノードを作成者ロールにグレースフルに昇格させる方法について説明します。

複数の Catalyst Center の展開で必要に応じて、リーダー Catalyst Center クラスターを作成者ロールに手動で昇格できます。すべてのリーダーノードクラスターには、**[Promote to Author]** ボタンがあります。現在の作成者ノードクラスターがまだ動作している間に、リーダーノードクラスターを作成者ノードに昇格させることができます。ただし、既存の作成者ノードクラスターがグループベースのポリシー作成アクティビティを実行している最中 (たとえば、Cisco ISE とのポリシーの同期中) は、昇格操作を開始しないでください。作成者ノードクラスターがビジー状態の場合、作成者ノードが現在の処理を完了するまで、昇格操作は段階的に実施されます。

注

- リーダーノードクラスターが作成者ロールにグレースフル昇格されると、リーダーノードクラスターは Cisco ISE に対して（リーダーから作成者への）ロール変更要求を開始します。
- Cisco ISE がロール変更要求を受信すると、現在の作成者ノードにポリシー作成者のロールを解放するように要求します。（同期が進行中でない場合）現在の作成者ノードはポリシー作成者のロールを解放し、リーダーノードクラスターのロールを引き継ぎます。
- 昇格用に選択された現在のリーダーノードは、作成者ノードのロールを引き継ぎます。作成者とリーダーのロールが変更されると、Cisco ISE は設定の更新を通じて、新しい作成者ノードの情報を他のリーダーノードクラスターに通知します。

2 :



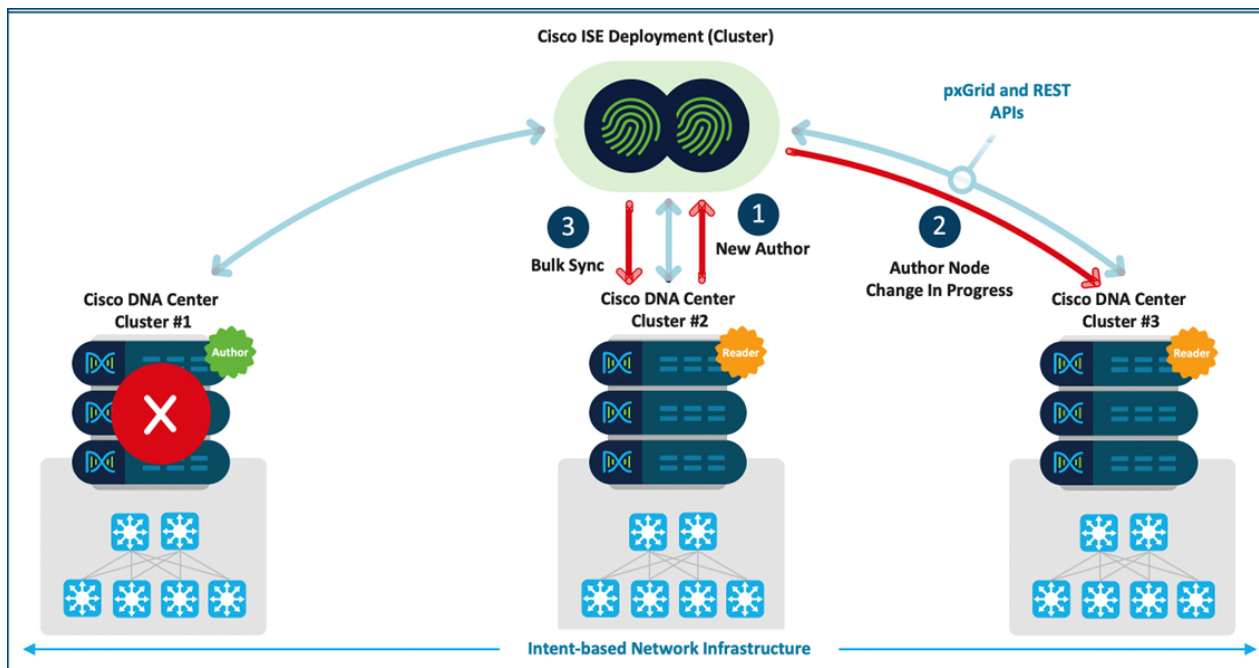
1. リーダーノードクラスターで **[System > Settings > System Configuration > Multiple Cisco] Catalyst Center [Settings]** の順に選択し、作成者ノードとリーダーノードを確認します。
2. **[Promote to Author]** ボタンをクリックします。
3. **[Continue]** をクリックして、ノードを作成者ロールに昇格させます。
昇格には数分かかる場合があります。

このトピックでは、リーダーノードの作成者ロールへの強制昇格について説明します。

強制昇格は、次のような状況で現在のリーダーノードクラスタを作成者ノードロールに昇格させることを目的とした手動プロセスです。

- 現在の作成者ノードクラスターがサービス停止中である。
- 現在の作成者ノードクラスターが応答していない。
- リーダーノードから作成者ロールへのグレースフル昇格に 5 分以上かかっている。

3:



既存の作成者ノードクラスターが **GBP** の作成アクティビティでサービス中である間は、強制昇格オプションを使用しないでください。データが失われ、作成者ノードクラスターが **Cisco ISE** と同期しなくなる可能性があります。強制昇格は、サービスをすぐに復元する必要があり、データを失うリスクを許容する場合にのみ推奨されます。強制昇格後、昇格したリーダーノードクラスターは、その展開における新しい作成者ノードクラスターになります。以前の作成者ノードクラスターが使用可能になると、リーダーロールに移行し、**Cisco ISE** から最新の設定データをダウンロードします。

リーダーノードクラスターの昇格が開始されると、リーダーノードクラスターは **Cisco ISE** に対して（リーダーから作成者への）ロールの変更要求を開始します。**Cisco ISE** がロール変更要求を受信すると、現在の作成者ノードにポリシー作成者のロールを解放するように要求します。現在の作成者ノードが応答せず、管理者が **[Force Promotion]** を選択した場合、リーダーノードクラスター **ACA** は、**Cisco ISE** で直ちにリーダーノードクラスターを作成者ロールに、またはその逆に、強制的に変更する要求を開始します。この設定の更新メッセージは、すべてのノードに送信されます。

リーダーノードクラスターを作成者ノードクラスターに強制昇格させる手順は、「リーダーノードの作成者ロールへのグレースフル昇格」で説明されている手順とまったく同じです。最後に、**[Force Promotion]** を開始するための追加の手順があります。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。