



## Cisco DNA Center リリース 2.1.2 管理者ガイド

初版：2020年8月31日

最終更新：2020年10月19日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

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)

© 2020 Cisco Systems, Inc. All rights reserved.



## 目次

---

第 1 章	新機能および変更された機能に関する情報	1
-------	---------------------	---

---

第 2 章	Cisco DNA Center について	5
	About Cisco DNA Center	5
	ログイン	5
	ネットワーク管理者として初回ログイン	6
	デフォルト ホームページ	7
	グローバル検索の使用	11
	開始位置	13

---

第 3 章	システム設定の構成	15
	システム設定について	16
	システム 360 の使用	16
	システム 360 でのサービスの表示	18
	システムヘルスのモニタリング	19
	Cisco IMC 接続の確立	20
	Cisco IMC 設定の削除	20
	システムイベント通知の登録	21
	システムトポロジの表示	21
	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	22
	外部システムの接続に関する問題のトラブルシューティング	22
	システムトポロジ通知	23
	推奨されるアクション (Suggested Actions)	25
	Cisco DNA Center と Cisco ISE の統合	29

データの匿名化	32
認証サーバとポリシーサーバの設定	32
Cisco AI ネットワーク分析 データ収集の設定	35
Cisco AI ネットワーク分析 データ収集の無効化	37
機械推論ナレッジベースの更新	38
シスコアカウント	39
シスコのクレデンシャルの設定	39
シスコのクレデンシャルのクリア	40
接続モードの設定	40
プラグアンドプレイの登録	41
スマートアカウントの設定	42
スマートライセンス	43
デバイスの可制御性	44
デバイスの可制御性の設定	46
ライセンス契約書の受諾	46
クラウドアクセスキー	47
整合性検証	48
KGV ファイルのアップロード	48
IP アドレスマネージャの設定	51
デバッグログの設定	51
ネットワークの再同期間隔の設定	53
監査ログの表示	54
監査ログに対する Syslog 通知の作成	55
高可用性のアクティブ化	55
統合設定の設定	56
ログインメッセージの設定	56
プロキシの設定	57
セキュリティ Cisco DNA Center	58
最小 TLS バージョンの変更と RC4-SHA の有効化 (安全でない)	58
プロキシ証明書の設定	61
証明書および秘密キーのサポート	62

証明書チェーンのサポート	63
Cisco DNA Center サーバ証明書の更新	64
証明書の管理	66
デバイス証明書の有効期間の設定	66
PKI 証明書のロールをルートから下位に変更	66
ロールオーバー下位 CA 証明書のプロビジョニング	69
証明書の更新	71
トラストプールの設定	72
SFTP サーバの設定	73
SNMP プロパティの設定	73
製品使用状況テレメトリの収集について	74
vManage プロパティの設定	74
アカウントのロックアウト	75
パスワードの有効期限切れ	75

---

 第 4 章

**アプリケーションの管理 77**

アプリケーション管理	77
システムの更新プログラムのダウンロードと更新	78
パッケージと更新のダウンロードとインストール	78
パッケージのアンインストール	80

---

 第 5 章

**ユーザの管理 81**

ユーザ プロファイルについて	81
ユーザ ロールの概要	81
ローカルユーザの作成	82
ローカルユーザの編集	82
ローカルユーザの削除	83
ローカルユーザパスワードのリセット	83
自身のユーザパスワードの変更	84
思い出せないパスワードのリセット	84
ロールベース アクセス コントロールの設定	85

Cisco DNA Center ユーザ ロール権限	86
ロールベース アクセス コントロール統計の表示	91
外部認証の設定	91
Two-Factor Authentication	94
二要素認証の前提条件	94
二要素認証のワークフロー	95
二要素認証の設定	95
RADIUS を使用した二要素認証の有効化	97
TACACS+ を使用した二要素認証の有効化	97
二要素認証を使用したログイン	98
外部ユーザの表示	98

---

**第 6 章**

<b>ライセンスの管理</b>	<b>99</b>
ライセンスマネージャの概要	99
Cisco スマート アカウントとの統合	103
ライセンス マネージャのセット アップ	103
ライセンスの使用状況と有効期限の可視化	105
ライセンス詳細の表示	105
ライセンスレベルの変更	107
ライセンス情報のエクスポート	108
コンプライアンスレポートのエクスポート	108
スマートライセンス対応デバイスの自動登録	109
スマートライセンス対応デバイスのデイゼロ設定	109
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	110
デバイスと Cisco DNA Center が CSSM に接続されている場合の SLR/PLR の有効化	110
デバイスと Cisco DNA Center が CSSM に接続されていない場合の CSV を使用した SLR/PLR の有効化	111
CSSM からの承認コードの生成	112
デバイスに適用された SLR または PLR をキャンセル	112

---

**第 7 章**

<b>バックアップと復元</b>	<b>113</b>
------------------	------------

バックアップと復元について	113
バックアップサーバの要件	114
バックアップストレージ要件	116
NFSサーバの設定例：Ubuntu	116
NFSサーバの設定例：CentOS	117
NFSを許可するファイアウォールルールの設定	118
ファイアウォールルールの設定：Debian/Ubuntu	118
ファイアウォールルールの設定：RedHat/CentOS	119
バックアップサーバの設定	119
今すぐデータをバックアップ	121
データのバックアップスケジュール	122
バックアップからデータを復元	123

## 第 8 章

## ディザスタリカバリの実装 127

概要	127
主な用語	128
ディザスタリカバリの GUI のナビゲーション	130
前提条件	131
アップグレード後のディザスタリカバリの設定	134
シナリオ 1	134
シナリオ 2	134
シナリオ 3	134
監視サイトの設定	135
ディザスタリカバリの設定	137
現在の監視サイトの置換	141
システムの登録解除	142
イベントタイムラインのモニタリング	142
システムおよびサイトの状態	144
フェールオーバー：概要	148
手動フェールオーバーの開始	148
ディザスタリカバリシステムの一時停止	152

システムの一時的停止	152
監視サイトのリリース 2.1.2.x へのアップグレード	154
システムへの再参加	154
バックアップおよび復元の検討事項	157
ディザスタリカバリエントの通知	157
サポートされるイベント	158
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	158
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	166





# 第 1 章

## 新機能および変更された機能に関する情報

次の表に、新機能および変更された機能の要約と参照先を示します。

表 1: Cisco DNA Center リリース 2.1.2 の新機能および機能変更

機能	説明	参照先
システムヘルス	[System Health] ページでは、Cisco DNA 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し、発生する可能性がある問題を監視できます。	<a href="#">システムヘルスのモニタリング (19 ページ)</a>
システムトポロジ	[System Health] ページのシステムトポロジには、ネットワークに接続された Cisco DNA Center アプライアンスと外部システム (Cisco Connected Mobile Experiences (Cisco CMX) や Cisco ISE など) がグラフィック形式で表示されます。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。	<a href="#">システムトポロジの表示 (21 ページ)</a>
ディザスタリカバリ	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する Cisco DNA Center の高可用性 (HA) に基づいて構築されます。HA では、クラスタノードに障害が発生したときに、運用を接続されたクラスタノードに切り替えることで対処します。ディザスタリカバリでは、クラスタに障害が発生したときに、ネットワーク管理作業を接続されたクラスタに移すことで対処します。	<a href="#">ディザスタリカバリの実装 (127 ページ)</a>
ロールベースアクセスコントロール	Cisco DNA 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 権限を持つユーザは、特定の Cisco DNA Center 機能へのユーザ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。	<a href="#">ロールベースアクセスコントロールの設定 (85 ページ)</a>

機能	説明	参照先
監査ロギング	<p>監査ログは、発生したシステムイベント、発生した場所、開始したユーザを記録します。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。</p> <p>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。</p>	<a href="#">監査ログの表示 (54 ページ)</a>
スマートライセンスの有効化	スマートライセンスは、ライセンスのステータスとソフトウェアの使用状況を管理して追跡できる、クラウドベースのソフトウェアライセンス管理ソリューションです。	<a href="#">スマートライセンス</a>
Connection mode	<p>接続モードは、Cisco SSM クラウドにアクセスするためのオプションを提供します。次の接続モードを使用できます。</p> <ul style="list-style-type: none"> <li>• 直接</li> <li>• オンプレミス CSSM</li> <li>• スマートプロキシ</li> </ul>	<a href="#">接続モードの設定</a>
システム設定	<p>次のシステム設定が改善されました。</p> <ul style="list-style-type: none"> <li>• シスコアカウントのクレデンシャル</li> <li>• Connection Mode</li> <li>• PnP Connect</li> <li>• スマート アカウント</li> <li>• スマートライセンスの有効化</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">シスコのクレデンシャルの設定 (39 ページ)</a></li> <li>• <a href="#">プラグアンドプレイの登録 (41 ページ)</a></li> </ul>
テレメトリコレクション	テレメトリ機能でユーザ情報を収集し、Cisco DNA Center アプライアンスのステータスと機能に関する貴重なデータを提供します。	<a href="#">製品使用状況テレメトリの収集について (74 ページ)</a>

機能	説明	参照先
デバイスの可制御性の強化	<p>下記のデバイス設定が、ディスカバリ中または実行時にデバイスの可制御性の一部として有効になります。</p> <ul style="list-style-type: none"> <li>• <b>デバイス検出</b> <ul style="list-style-type: none"> <li>• [SNMP Credentials]</li> <li>• [NETCONF Credentials]</li> </ul> </li> <li>• <b>インベントリへのデバイスの追加</b> <ul style="list-style-type: none"> <li>• Cisco TrustSec (CTS) クレデンシヤル</li> <li>• IPDT の有効化</li> </ul> </li> <li>• <b>デバイスのサイトへの割り当て</b> <ul style="list-style-type: none"> <li>• コントローラ証明書</li> <li>• SNMP トラップサーバ定義</li> <li>• Syslog サーバ定義</li> <li>• NetFlow サーバ定義</li> <li>• Wireless Service Assurance (WSA)</li> </ul> </li> </ul>	<p><a href="#">デバイスの可制御性 (44 ページ)</a></p>
スマートアカウントのクレデンシヤル	<p>権限付与とライセンス管理のためにスマート ライセンス アカウントに接続します。</p>	<p><a href="#">スマートアカウントの設定 (42 ページ)</a></p>
ログインメッセージ	<p>すべてのユーザが Cisco DNA Center アプライアンスにログインしたときに表示されるメッセージを設定できます。</p>	<p><a href="#">ログインメッセージの設定 (56 ページ)</a></p>
機械推論ナレッジベース	<p>既存のネットワーク推論ワークフローで新しい更新があるたびに、[AVAILABLE UPDATE] が [Machine Reasoning Knowledge Base] ウィンドウに表示され、新しい更新の詳細が示されます。</p>	<p><a href="#">機械推論ナレッジベースの更新 (38 ページ)</a></p>
IPAM サーバのハートビートモニタリング	<p>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。</p>	<p><a href="#">システム 360 の使用 (16 ページ)</a></p>
コンプライアンスレポートの出力	<p>準拠していないデバイスをすべて表示するレポートを生成してエクスポートできます。</p>	<p><a href="#">コンプライアンスレポートのエクスポート (108 ページ)</a></p>



- 
- (注) この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。
-



## 第 2 章

# Cisco DNA Center について

---

- [About Cisco DNA Center](#) (5 ページ)
- [ログイン](#) (5 ページ)
- [ネットワーク管理者として初回ログイン](#) (6 ページ)
- [デフォルト ホームページ](#) (7 ページ)
- [グローバル検索の使用](#) (11 ページ)
- [開始位置](#) (13 ページ)

## About Cisco DNA Center

Cisco Digital Network Architecture は、設計、プロビジョニング、ネットワーク環境全体へのポリシーの適用を迅速かつ容易にする一元化された使いやすい管理機能を備えています。Cisco DNA Center GUI はネットワークを隅々まで見ることを可能にし、ネットワークパフォーマンスの最適化およびユーザエクスペリエンスおよびアプリケーションエクスペリエンスの最適化のためにネットワークインサイトを利用します。

## ログイン

ブラウザで Cisco DNA Center のネットワーク IP アドレスを入力してアクセスします。互換性のあるブラウザについては、「[Cisco DNA Center のリリースノート](#)」を参照してください。この IP アドレスで外部ネットワークに接続します。これは、Cisco DNA Center のインストール時に設定されます。Cisco DNA Center のインストールと設定の詳細については、『[Cisco DNA Center Installation Guide](#)』を参照してください。

ログイン状態を維持するには、Cisco DNA Center を継続的に使用する必要があります。長時間非アクティブ状態が続くと、Cisco DNA Center のセッションから自動的にログアウトします。

---

**ステップ 1** 次のフォーマットで、Web ブラウザのアドレスバーにアドレスを入力します。ここで、*server-ip* は Cisco DNA Center をインストールしたサーバの IP アドレス（またはホスト名）です。

`https://server-ip`

例 : <https://192.0.2.1>

ネットワーク構成によっては、ブラウザを更新して Cisco DNA Center サーバのセキュリティ証明書を信頼する必要があります。これを行うと、クライアントと Cisco DNA Center 間の接続のセキュリティが確保されます。

**ステップ 2** システム管理者により割り当てられた、Cisco DNA Center のユーザ名とパスワードを入力します。Cisco DNA Center にホーム ページが表示されます。

使用しているユーザ ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じ権限を持つ他のユーザが先にログインしていない場合、ホームページではなく初回セットアップウィザードが表示されます。詳細は、[ネットワーク管理者として初回ログイン \(6 ページ\)](#) を参照してください。

**ステップ 3** ログアウトするには、[Menu] アイコン (☰) をクリックし、[Sign Out] を選択します。

## ネットワーク管理者として初回ログイン

使用しているユーザ ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じロールを持つ他のユーザが先にログインしていない場合は、[Get Started] ウィザードにリダイレクトされます。

このウィザードを使用すると、Cisco DNA Center から即時値をすぐに取得できます。これは複数の画面で構成され、ネットワーク デバイスの状況の検出とモニタに必要な情報を収集します。さらに、Cisco DNA Center ホームページ ダッシュボードを使用してネットワークの全体的な健全性を視覚化できます。

ウィザードで行うタスクと同じタスクはすべて、その他の Cisco DNA Center の機能で実行できます。ウィザードを使用しても、このような機能を使うことができます。任意の時点でウィザード全体をスキップできます。ウィザードが再び表示されることはありません。ただし、Cisco DNA Center では、同じ権限を持つユーザがこのウィザード手順を完了するまで、このようなユーザのログイン時に同じロールが表示され続けます。ウィザードの完了後は、Cisco DNA Center でウィザードが再度表示されることはありません。

[Get Started] ウィザードをスキップした場合でも、ホームページの右上にある [Get Started] リンクからいつでも再アクセスできます。

### 始める前に

ウィザードを完了するには、以下の情報が必要です。

- SYSLOG サーバと SNMP サーバの IP アドレス
- NetFlow サーバの IP アドレスとポート
- ディスカバリ : 開始する IP アドレス (CDP ディスカバリを選択している場合) または開始と終了の IP アドレス (範囲ディスカバリを選択している場合)
- オプション : 優先される管理 IP アドレス

- デバイス CLI クレデンシャル（イネーブル パスワードなど）
- SNMP v2c クレデンシャル（read コミュニティ ストリングなど）

**ステップ 1 ログイン（5 ページ）** の説明に従って、通常の手順で Cisco DNA Center にログインします（まだログインしていない場合）。

初めてログインした場合は、[Get Started] ウィザードにリダイレクトされます。

**ステップ 2** [Get Started] ウィザードで [Get Started] をクリックしてデバイスの検出を続行するか、または [Exit] をクリックしてホームページに戻ります。

**ステップ 3** デバイス検出のネットワークプロパティを入力し、[Save & Next] をクリックします。

前の画面に戻るには、[Back] をクリックします。

**ステップ 4** [Discovery Type]、[Starting IP Address]、および [CLI Credentials] を指定します。

**ステップ 5** 完了したら [Begin Discovery] をクリックすると Cisco DNA Center にホームページが表示されます。ここに、検出が完了するにつれネットワークの健全性情報が徐々に表示されていきます。

## デフォルト ホームページ

ログインすると、Cisco DNA Center のホームページが表示されます。ホームページには、主要エリアとして、[Summary]アシュアランス、[Network Snapshot]、[Network Configuration]、および[Tools]があります。

[Summary]アシュアランス エリアには次の内容が含まれます。

- [Health]：企業全体の正常性スコア（ネットワークデバイス、有線クライアント、ワイヤレスクライアントなど）が提供されます。[View Details] をクリックすると、[Overall Health] ウィンドウが表示されます。
- [Critical Issues]：P1 と P2 の問題の数が表示されます。[View Details] をクリックすると、[Open Issues] ウィンドウが表示されます。
  - [P1]：ネットワーク運用に幅広い影響を与える前に早急な対応を必要とする重大な問題。
  - [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある主要な問題。
- [Trends and Insights]：ネットワークのパフォーマンスに関するインサイトが提供されます。[View Details] をクリックすると、[Network Insights] ウィンドウが表示されます。

[Network Snapshot] エリアには次のコンポーネントが含まれます。

- [Sites]：ネットワーク上で検出されたサイトの数と、DNS サーバおよび NTP サーバの数が示されます。[Add Sites] をクリックすると、[Add Site] ウィンドウが表示されます。

- **[Network Devices]** : ネットワーク上で検出されたネットワーク デバイスの数と、要求されていないデバイス、プロビジョニングされていないデバイス、および到達不能なデバイスの数が示されます。 **[Find New Devices]** をクリックすると、 **[New Discovery]** ウィンドウが表示されます。
- **[Application policies]** : ネットワーク上で検出されたアプリケーションポリシーの数と、成功およびエラーになった展開の数を表示します。 **[Add New Policy]** をクリックすると、 **[Application Policies]** ウィンドウが表示されます。
- **[Network Profiles]** : ネットワーク上で検出されたプロファイルの数を示します。 **[Manage Profiles]** をクリックすると、 **[Network Profiles]** ウィンドウが表示されます。
- **[Images]** : ネットワーク上で検出されたイメージの数と、タグなしイメージおよび未検証イメージの数が示されます。 **[Import Images/SMUs]** をクリックすると、 **[Image Repository]** ウィンドウが表示されます。
- **[Licensed Devices]** : Cisco DNA Center ライセンスを持つデバイスの数と、スイッチ、ルータ、およびアクセスポイントの数が示されます。 **[Manage Licenses]** をクリックすると、 **[License Management]** ウィンドウが表示されます。

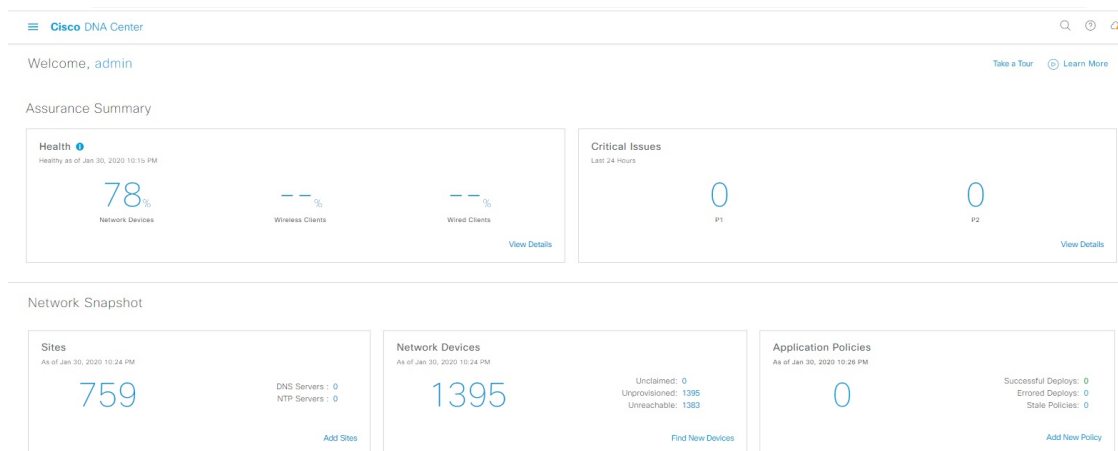
**[Network Configuration]** エリアには次の内容が含まれます。

- **[Design]** : ネットワーク全体のデバイスに適用できるネットワークの構造とフレームワーク（物理トポロジ、ネットワーク設定、デバイス タイプ プロファイルなど）を作成します。
- **[Policy]** : ネットワークの特定の側面（ネットワーク アクセスなど）に対する組織のビジネス目標を反映したポリシーを作成します。 Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワーク デバイスのさまざまなタイプ、メーカー、モデル、オペレーティングシステム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。
- **[Provision]** : デバイスの準備と設定（サイトへのデバイスの追加、インベントリへのデバイスの割り当て、必要な設定とポリシーの展開、ファブリックドメインの作成、ファブリックへのデバイスの追加など）を行います。
- **アシュアランス[Assurance]** : ネットワーク インフラストラクチャ、アプリケーション、およびエンドユーザクライアントのパフォーマンスと正常性について、プロアクティブで予測型の実用的洞察を提供します。
- **[Platform]** : インテント API を使用してネットワークにプログラムでアクセスできます。最適な IT システムと統合してエンドツーエンドのソリューションを作成し、マルチベンダー デバイスのサポートを追加できます。

**[Tools]** : **[Tools]** エリアを使用して、ネットワークを設定および管理します。



図 1 : Cisco DNA Center ホームページ



ホームページのさまざまなビュー :

使用する前に

ネットワーク管理者またはシステム管理者として初めて Cisco DNA Center にログインするとき、またはシステムにデバイスが存在しない場合は、次のダッシュレットが表示されます。[Get Started] をクリックして開始ワークフローを完了し、ネットワーク内の新しいデバイスを検出します。

In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

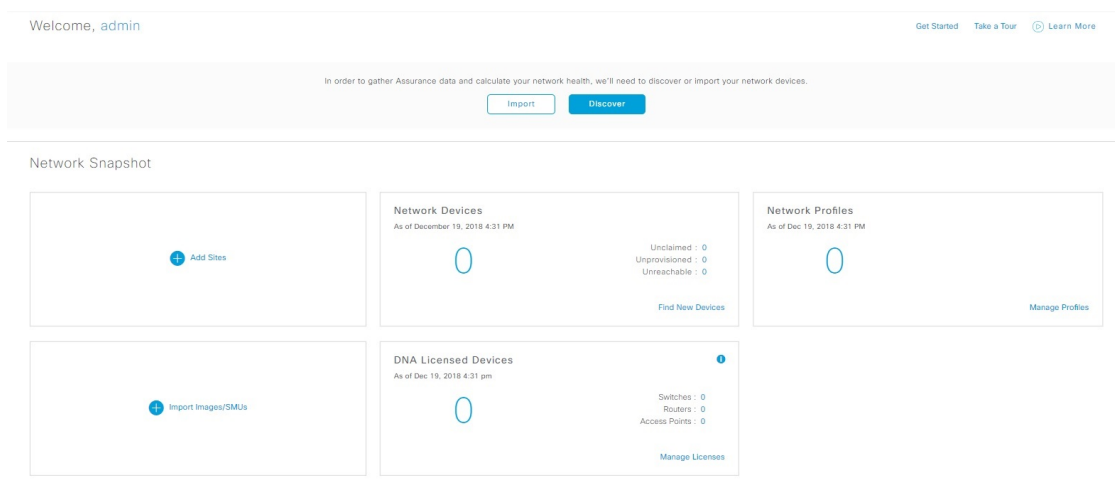
Get Started

初めてオブザーバとして Cisco DNA Center にログインすると、次のメッセージが表示されます。

Ask your Network Administrator to add Network Devices to gather Assurance data.

0 日目のホームページ

開始をスキップした場合、またはシステム内にデバイスが存在しない場合は、次のホームページが表示されます。



検出が進行中の場合は、[Discovery] ウィンドウへのリンクが付いた進捗状況メッセージが表示されます。

We've discovered 10 devices in your network. [View Discovery](#)




システム内にデバイスがある場合は、検出されたデバイスのネットワーク スナップショットが表示されます。

ホームページの左上隅にある [Menu] アイコン (☰) をクリックすると、次のメニューにアクセスできます。

- 設計
- ポリシー
- プロビジョニング
- 保証
- ワークフロー
- ツール
- プラットフォーム
- アクティブな状態
- システム

ホームページの右上隅と右下隅にあるアイコンをクリックして共通のタスクを実行できます。

アイコン	説明
🔍	[Search] : デバイス、ユーザ、ホスト、ハンバーガーメニューのメニュー、およびその他の項目が保存されている Cisco DNA Center データベース内の任意の場所で、それらを検索します。検索機能を使用する際のヒントについては、「 <a href="#">グローバル検索の使用 (11 ページ)</a> 」を参照してください。

アイコン	説明
	<p><b>Help</b></p> <ul style="list-style-type: none"> <li>• [About] : 現在の Cisco DNA Center のソフトウェアバージョンが表示されます。 [Release Notes] をクリックすると、別のブラウザタブでリリースノートが起動します。 [Packages] をクリックすると、システムおよびアプリケーションパッケージのバージョンが表示されます。 [Serial number] をクリックすると、Cisco DNA Center のアプライアンスのシリアル番号が表示されます。</li> <li>• [API Reference] : Cisco DevNet に Cisco DNA Center プラットフォーム API のドキュメントが開きます。</li> <li>• [Developer Resources] : 開発者ツールにアクセスできる Cisco DevNet が開きます。</li> <li>• [Help] : 状況に応じたオンラインヘルプが、ブラウザの別のタブに表示されます。</li> <li>• [Contact Support] : Cisco Technical Assistance Center (TAC) でサポートケースが開きます。</li> <li>• [Make a Wish] : コメントや提案事項が Cisco DNA Center 製品チームに送信されます。</li> </ul>
	[Software Updates] : 利用可能なソフトウェアアップデートのリストが表示されます。[Go to Software Updates] リンクをクリックすると、システムとアプリケーションのアップデートを表示できます。
	[Interactive Help] : ユーザが GUI から特定のタスクを完了できる対話型ヘルプフローのメニューを開きます。

Cisco DNA Center を初めて使用する場合は、[開始位置 \(13 ページ\)](#) で使い方のヒントや提案を参照してください。



(注) デフォルトでは、入力したログイン名がウェルカムテキストに表示されます。名前を変更するには、名前のリンク (例: **admin**) をクリックします。[User Management] ウィンドウに移動し、表示名を編集できます。

## グローバル検索の使用

グローバル検索機能を使用して、Cisco DNA Center の任意の場所で次のカテゴリの項目を検索します。

- **アクティビティ** : Cisco DNA Center のメニュー項目、ワークフロー、および機能を名前で検索します。
- **アプリケーション** : 名前で検索します。
- **アプリケーショングループ** : 名前で検索します。
- **認証テンプレート** : 名前またはタイプで検索します。
- **デバイス** : 収集ステータス、到達可能性ステータス、ロケーション、またはタグで検索します。
- **ファブリック** : ファブリック名で検索します。
- **ホストおよびエンドポイント** : 名前、IP アドレスまたは MAC アドレスで検索します。
- **IP プール** : 名前または IP アドレスでそれらを検索します。
- **ネットワーク デバイス** : 名前、IP アドレス、シリアル番号、ソフトウェアバージョン、プラットフォーム、製品ファミリ、または MAC アドレスで検索します。
- **ネットワークプロファイル** : プロファイル名で検索します。
- **ネットワーク設定**
  - **デバイスログイン情報** : 名前で検索します。
  - **IP アドレスプール** : グループ名またはプールの CIDR で検索します。
  - **サービス プロバイダー プロファイル** : プロファイル名、WAN プロバイダー、またはモデルで検索します。
- **ポリシー** : 名前または説明で検索します。
- **サイト** : 名前で検索します。
- **トラフィックのコピー** : 名前と説明で検索します。
- **移行** : 移行名で検索します。
- **ユーザ** : システム設定およびユーザをユーザ名で検索します。大文字と小文字は区別されません。ユーザ名のサブストリング検索はサポートされていません。
- 新しいバージョンの Cisco DNA Center として別のアイテムがリリースされます。

グローバル検索を開始するには、Cisco DNA Center ページの右上隅にある **Q** アイコンをクリックします。Cisco DNA Center にポップアップグローバル検索ウィンドウが表示されます。[Search] フィールドに項目に関する識別情報を入力します。

ターゲット項目の名前、アドレス、シリアル番号、またはその他の識別情報の全体または一部を入力できます。[Search] フィールドで大文字と小文字は区別されません。任意の文字または文字の組み合わせを入力できます。

検索文字列の入力を開始すると、入力に一致する可能性がある検索ターゲットのリストが Cisco DNA Center に表示されます。複数のカテゴリの項目が検索文字列と一致する場合は、Cisco DNA Center によってカテゴリ別にソートされます。各カテゴリには最大 5 つの項目が含まれます。最初のカテゴリの最初の項目が自動的に選択され、その項目の概要情報が右側の [summary] パネルに表示されます。

必要に応じてリストをスクロールできます。提案された検索ターゲットのいずれかをクリックすると、概要パネルにその項目の情報が表示されます。カテゴリに項目が 5 つ以上ある場合は、カテゴリ名の横にある [View All] をクリックします。検索ターゲットの完全なリストからカテゴリ化されたリストに戻るには、[Go Back] をクリックします。

検索文字列にさらに多くの文字を追加すると、グローバル検索で表示されるリストが自動的に絞り込まれます。

概要パネルには、詳細へのリンクが表示されます。リンクはカテゴリおよび項目ごとに必要に応じて変わります。例：アクティビティの場合、概要パネルには Cisco DNA Center システム以外のメニュー項目およびワークフローへのリンクが表示されます。アプリケーションの場合、[Application 360] ビューが表示されます。ホスト/エンドポイントの場合は [Client 360] ビューと [Topology] ビューへのリンクが表示され、ネットワーク デバイスの場合は [Device 360] ビューと [Topology] ビューへのリンクが表示されます。

完了したら、✖ をクリックしてウィンドウを閉じます。

グローバル検索では、カテゴリごとに一度に 5 つの結果を表示できます。

## 開始位置

Cisco DNA Center の使用を開始するには、まず、サーバがネットワーク外と通信できるように Cisco DNA Center を設定する必要があります。

設定後、現在の環境で Cisco DNA Center の使用を開始する方法を決定します。

- 既存のインフラストラクチャ：既存のインフラストラクチャ（ブラウフィールド導入）があれば、ディスカバリを実行して開始します。ディスカバリを実行すると、すべてのデバイスが [Inventory] ウィンドウに表示されます。ディスカバリの実行の詳細については、[Cisco DNA Center ユーザガイド](#)を参照してください。
- 新規または存在しないインフラストラクチャ：既存のインフラストラクチャがなく、ゼロから開始（新規導入）する場合は、ネットワーク階層を作成します。ネットワーク階層の作成については、[Cisco DNA Center ユーザガイド](#)を参照してください。





## 第 3 章

# システム設定の構成

- システム設定について (16 ページ)
- システム 360 の使用 (16 ページ)
- システム 360 でのサービスの表示 (18 ページ)
- システムヘルスのモニタリング (19 ページ)
- Cisco DNA Center と Cisco ISE の統合 (29 ページ)
- データの匿名化 (32 ページ)
- 認証サーバとポリシーサーバの設定 (32 ページ)
- Cisco AI ネットワーク分析 データ収集の設定 (35 ページ)
- 機械推論ナレッジベースの更新 (38 ページ)
- シスコアカウント (39 ページ)
- デバイスの可制御性 (44 ページ)
- クラウドアクセスキー (47 ページ)
- 整合性検証 (48 ページ)
- IP アドレスマネージャの設定 (51 ページ)
- デバッグログの設定 (51 ページ)
- ネットワークの再同期間隔の設定 (53 ページ)
- 監査ログの表示 (54 ページ)
- 高可用性のアクティブ化 (55 ページ)
- 統合設定の設定 (56 ページ)
- ログインメッセージの設定 (56 ページ)
- プロキシの設定 (57 ページ)
- セキュリティ Cisco DNA Center (58 ページ)
- SFTP サーバの設定 (73 ページ)
- SNMP プロパティの設定 (73 ページ)
- 製品使用状況テレメトリの収集について (74 ページ)
- vManage プロパティの設定 (74 ページ)
- アカウントのロックアウト (75 ページ)
- パスワードの有効期限切れ (75 ページ)

## システム設定について

Cisco DNA Center の使用を開始するには、最初にシステム設定を構成して、サーバがネットワークの外部と通信し、セキュアな通信の確保やユーザの認証といった主要なタスクを実行できるようにする必要があります。システム設定を構成するには、この章で説明されている手順を使用します。



- (注) Cisco DNA Center の設定（プロキシサーバの設定を含む）の変更については、Cisco DNA Center GUI で実行する必要があります。IP アドレス、静的ルート、DNS サーバ、**maglev** ユーザパスワードの変更については、CLI から `sudo maglev-config update` コマンドを使用して実行する必要があります。

## システム 360 の使用

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

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [System 360]** の順に選択します。

**ステップ 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]** : Cisco DNA 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、要求が増えると自身のインスタンスを追加し、要求が減ると自身のインスタンスを解放する、水平方向にスケーラブル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。
- [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。  
**重要** Cisco DNA Center で HA が機能するためには 3 つ以上のホストが必要です。
- [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、Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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、Cisco DNA Center のすべてのロギングが有効になっています。
  - [Workflow] : 成功、失敗、保留中のステータスのマーキングを含む Cisco DNA Center インフラストラクチャタスクの詳細なグラフィカル表示を提供する、ワークフロービジュアルライザにアクセスします。[Workflow] ツールを使用して、Cisco DNA Center タスクにおける障害の場所を特定します。

## 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] : 自動化およびアシュアランス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

Cisco DNA 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 Cisco DNA 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。
- [vManage] : vManage の設定データが表示されます。vManage を設定するには、[Configure] リンクをクリックします。

---

## システム 360 でのサービスの表示

[System 360] タブは、Cisco DNA 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、アシュアランス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。

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [System 360] の順に選択します。
- ステップ 2** [System 360] タブの [Cluster Tools] 領域で、[Service Explorer] をクリックします。  
ノードクラスタ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、ノードクラスタの正常性ステータスが表示されます。正常な状態のノードクラスタは緑色でマークされます。異常があるノードクラスタは赤色でマークされます。
  - 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。
- ステップ 3** サービスをクリックして、サービス 360 ビューを起動します。次の詳細が表示されます。
- [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。
  - [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。
  - [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。
- ステップ 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。
- ステップ 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。

## システムヘルスのモニタリング

[System Health] ページでは、Cisco DNA 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する方法については、以降のトピックを参照してください。

## Cisco IMC 接続の確立

[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。これにより、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。これを行うには、次の手順を実行します。



(注) アプライアンスの Cisco IMC 接続設定を入力できるのは、SUPER-ADMIN-ROLE 権限を持つユーザのみです。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [System Configuration] > [System Health Notifications] 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 [Address] 列に表示されます。Cisco DNA Center

**ステップ 2** Cisco IMC へのログインに必要な情報を設定します。

a) アプライアンスの IP アドレスをクリックします。

[Edit Cisco DNA Center Server Configuration] スライドインペインが開きます。

b) 次の情報を入力し、[Save] をクリックします。

- 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。
- Cisco IMC にログインするために必要なユーザ名とパスワード。

c) 必要に応じて、クラスタの他のアプライアンスについて手順 2a と 2b を繰り返します。

## Cisco IMC 設定の削除

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。



(注) これらの設定を削除できるのは、SUPER-ADMIN-ROLE 権限を持つユーザのみです。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [System Configuration] > [System Health Notifications] の順に選択します。

**ステップ 2** 設定を削除するアプライアンスについて、[Actions] 列の [Delete] アイコン (🗑️) をクリックします。

ダイアログボックスが開き、設定の削除を確認するように求められます。

ステップ3 [OK] をクリックします。

## システムイベント通知の登録

Cisco IMC との接続が確立されると、Cisco DNA 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。これらの未処理のイベントは、ルールエンジンによって処理されてシステムイベント通知に変換されます。これらの通知をサブスクライブする方法については、『[Cisco DNA Center Platform User Guide](#)』の「Work with Events」を参照してください。この手順を完了するときは、必ず **[Platform]** > **[Developer Toolkit]** > **[Events]** テーブルで次のイベントを選択してサブスクライブしてください。

- SYSTEM-CIMC
- SYSTEM-DISASTER-RECOVERY
- SYSTEM-EXTERNAL-CMX
- SYSTEM-EXTERNAL-IPAM
- SYSTEM-EXTERNAL-ISE-AAA-TRUST
- SYSTEM-EXTERNAL-ISE-PAN-ERS
- SYSTEM-EXTERNAL-ISE-PXGRID
- SYSTEM-EXTERNAL-ITSM
- SYSTEM-HARDWARE

## システムトポロジの表示

[System Health] ページのトポロジには、ネットワークに接続された Cisco DNA 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（Cisco ISE）など）がグラフィック形式で表示されます。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。このページにアプライアンスと外部システムのデータを取り込むには、まず以降のトピックで説明するタスクを完了する必要があります。

- [Cisco IMC 接続の確立](#)（20 ページ）
- [システムイベント通知の登録](#)（21 ページ）

このページを表示するには、Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックし、**[System]** > **[System Health]** の順に選択します。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。

## 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

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。コンポーネントに関する問題のトラブルシューティングを開始するには、コンポーネントのトポロジアイコンにカーソルを合わせます。ポップアップウィンドウが開き、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。
- Cisco DNA 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が3つ以上ある場合や Cisco DNA 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。

## 外部システムの接続に関する問題のトラブルシューティング

Cisco DNA 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を ping し、到達できない理由をトラブルシューティングします。

### 始める前に

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。『[Cisco DNA Center Administrator Guide](#)』の「Download and Install Packages and Updates」を参照してください。
- 機械推論機能への書き込み権限を持つロールを作成し、この手順を実行するユーザ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] ウィザードページの[System]行を展開します。詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Configure Role-Based Access Control」を参照してください。

---

**ステップ 1** [System Health] ページの右上部分から、[Tools] > [Network Ping] を選択して [Ping Device] ページを開きます。

このページには、Cisco DNA Center で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。

**ステップ 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] ポップアップウィンドウが開きます。

**ステップ 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。

**ステップ 4** [Run Machine Reasoning] をクリックします。

Cisco DNA 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。

**ステップ 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。

**ステップ 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] ポップアップウィンドウが開き、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。

## システムトポロジ通知

次の表に、[System Health] ページのシステムトポロジに表示される Cisco DNA 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、[Cisco DNA Center Ok] という通知が表示されます。

表 2: Cisco DNA Center アプライアンスの通知

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

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
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 - xxxxx) State is Disabled	—	PowerSupply PSU1 (SerialNumber - xxxxx) 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

表 3: 接続されている外部システムの通知

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	—	There is a critical issue with the integrated CMX server.	CMX server is integrated and servicing.
IP アドレス管理 (IPAM) サーバ	There is a critical issue with the connected third-party IPAM provider	—	<ul style="list-style-type: none"> <li>A third-party IPAM provider is connected.</li> <li>There is no third-party IPAM provider connected.</li> <li>The third-party IPAM provider is currently synchronizing.</li> </ul>
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	Servicenow connection health status is NOT up and running	—	Servicenow connection health status is up and running



## 推奨されるアクション (Suggested Actions)

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。

## 推奨されるアクション (Suggested Actions)

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 (Suggested Actions)
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)。	<ul style="list-style-type: none"> <li>• Cisco DNA Center と Cisco ISE の間のプロキシサーバのプロキシ設定を確認します。</li> <li>• Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。</li> </ul>
		Cisco ISE との接続を確立できない。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• Cisco DNA Center と Cisco ISE の間のプロキシサーバのプロキシ設定を確認します。</li> <li>• Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。</li> </ul>
	ERS : 可用性	ERS API コールへの応答がない。	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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、『<a href="#">Cisco Identity Services Engine Administration Guide</a>』の「Enable External RESTful Services APIs」を参照してください。</li> </ul>
	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。	Cisco DNA Center GUI で信頼を再確立します。詳細については、『 <a href="#">Cisco Identity Services Engine Administration Guide</a> 』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。		

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 (Suggested Actions)
			<ol style="list-style-type: none"> <li>1. Cisco DNA Center で現在設定されている AAA 設定を削除します。</li> <li>2. 適切な AAA 設定を再入力します。詳細については、『<a href="#">Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide</a>』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。</li> <li>3. 信頼を再確立します。詳細については、『<a href="#">Cisco Identity Services Engine Administration Guide</a>』の「Enable PKI in Cisco ISE」を参照してください。</li> </ol>
	信頼：到達可能性	SSH 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 Cisco DNA Center エンドポイント URL に到達できない。	<ul style="list-style-type: none"> <li>• Cisco DNA Center と Cisco ISE の間のプロキシサーバのプロキシ設定を確認します。</li> <li>• Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。</li> </ul>
	信頼：設定	Cisco ISE 証明書チェーンが無効である。	<ul style="list-style-type: none"> <li>• 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、『<a href="#">Cisco Identity Services Engine Administration Guide</a>』の「ISE CA Chain Regeneration」を参照してください。</li> <li>• 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。</li> </ul>
		Cisco ISE 証明書チェーンのアップロード用に設定された Cisco DNA Center エンドポイント URL が禁止されている。	

## 推奨されるアクション (Suggested Actions)

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 (Suggested Actions)
			<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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、『<a href="#">Cisco Identity Services Engine Administration Guide</a>』の「Enable External RESTful Services APIs」を参照してください。</li> </ul>
	信頼：認証	Cisco ISE パスワードの期限が切れている。	<ul style="list-style-type: none"> <li>• Cisco ISE 管理者パスワードを再生成します。詳細については、『<a href="#">Cisco Identity Services Engine Administrator Guide</a>』の「Administrative Access to Cisco ISE」を参照してください。</li> <li>• Cisco ISE の管理者ユーザに対して設定されている GUI と SSH のログイン情報が同じであることを確認します。</li> </ul>
	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。	<ol style="list-style-type: none"> <li>1. Cisco DNA Center で現在設定されている AAA 設定を削除します。</li> <li>2. 適切な AAA 設定を再入力します。詳細については、『<a href="#">Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide</a>』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。</li> <li>3. 信頼を再確立します。詳細については、『<a href="#">Cisco Identity Services Engine Administration Guide</a>』の「Enable PKI in Cisco ISE」を参照してください。</li> </ol>

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 (Suggested Actions)
Cisco Connected Mobile Experiences (CMX) サーバ IP アドレス管理 (IPAM) サーバ IT サービス管理 (ITSM) サーバ	到達可能性	サーバとの接続を確立できない。	該当するサーバがダウンしていないかどうかを確認します。
	認証	サーバにログインできない。	Cisco DNA 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。
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		
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。	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>

## Cisco DNA Center と Cisco ISE の統合

Cisco ISE には、Cisco DNA 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、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、Cisco DNA 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、Cisco DNA Center で Cisco ISE の設定を行う必要があります。Cisco DNA 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 DNA Center 設置ガイド](#)を参照してください。

3. ネットワークでのユーザ認証に Cisco ISE を使用している場合、Cisco ISE を統合するためにアシュアランスを設定します。この統合により、有線クライアントの詳細（ユーザ名やオペレーティングシステムなど）をアシュアランスで確認できるようになります。詳細については、[Cisco DNA Assurance ユーザガイド](#)の「Cisco DNA 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、Cisco DNA Center で信頼性が確立されると、Cisco DNA Center は Cisco ISE と情報を共有します。Cisco ISE を使って AAA サーバとして構成されたサイトに割り当てられた Cisco DNA 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、Cisco DNA Center におけるそれらの Cisco DNA Center デバイスに対するすべての更新（デバイス クレデンシャルなど）も Cisco ISE を変更によって更新します。

Cisco ISE を使って AAA サーバとしてサイトに関連付けられている Cisco DNA Center デバイスが想定どおり Cisco ISE に伝達されない場合、Cisco DNA 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 Cisco DNA 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。Cisco DNA 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、入力検証エラーとして、Cisco ISE 自体による拒否が原因で失敗した場合、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 Cisco DNA Center を更新する際にその変更は反映されません。Cisco DNA 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 サーバを編集します。Cisco DNA Center は新しい証明書を Cisco ISE からダウンロードし、Cisco DNA Center を更新します。

Cisco ISE は既存のデバイス情報を Cisco DNA Center と共有しません。Cisco DNA 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 Cisco DNA Center と同じ名前を付ける必要があります。Cisco DNA 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) Cisco DNA 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 Cisco DNA Center 監査ログにキャプチャされます。Cisco DNA Center と Cisco ISE 間のワークフローに問題がある場合は、Cisco DNA Center GUI で監査ログの情報を確認します。

Cisco DNA Center は、プライマリ管理者 ISE ノードと統合されています。Cisco DNA 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。

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

Cisco ISE サーバに到達不能な場合、Cisco DNA 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。Cisco DNA Center は 15 分間隔でのポーリングを 3 日間継続します。Cisco DNA Center は接続が復活しない場合、ポーリングを停止し、Cisco ISE サーバのステータスを [信頼できない (Untrusted)] に更新します。この場合、Cisco DNA Center と Cisco ISE サーバ間の信頼関係を再確立する必要があります。

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

- Cisco DNA Center と Cisco ISE の統合はプロキシサーバ経由ではサポートされていません。プロキシサーバ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を使用しないように Cisco DNA Center を設定します。設定するにはプロキシサーバの IP アドレスをバイパスします。
- Cisco DNA Center と Cisco ISE の統合は、現在、Cisco DNA Center 仮想 IP アドレス (VIP) 経由ではサポートされていません。Cisco DNA 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 Cisco DNA Center のすべてのインターフェイスの IP アドレスが Cisco DNA Center 証明書に含まれていることを確認します。Cisco DNA 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、Cisco DNA Center 証明書の SAN 拡張に含まれている必要があります。
- Cisco DNA Center は、Cisco ISE CLI (イーサネット ルーティング スイッチ経由) と GUI (SSH 接続経由) の両方にアクセスする必要があります。Cisco DNA Center には一組の Cisco ISE クレデンシャルのみ定義できるため、それらのクレデンシャルは、Cisco ISE GUI および CLI ユーザアカウントの両方で同じであることを確認します。
- Cisco ISE の管理者ユーザ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。詳細については、[『Cisco Firepower Threat Defense Virtual for Microsoft Azure Quick Start Guide』](#) を参照してください。
- Cisco ISE 証明書が変更された場合は、Cisco DNA Center を更新する必要があります。更新するには、AAA サーバ (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、Cisco DNA 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、Cisco DNA 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、Cisco DNA Center を更新する必要があります。Cisco DNA Center は SSH を介して Cisco ISE に接続し、CLI を実行して証明書情報を取得します。
- Cisco DNA 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、Cisco DNA 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] ページで Cisco ISE を AAA サーバとして設定する際に提供されています。シークレットパスワードを変更するには、[Design] > [Network Settings] > [Network] の順に移動し、[Change Shared Secret] リン

クをクリックします。これにより、Cisco ISEは、Cisco DNA 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。

## データの匿名化

Cisco DNA 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 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。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [Anonymize Data] の順に選択します。

[Anonymize Data] ウィンドウが表示されます。

**ステップ 2** [Enable Anonymization] チェックボックスをオンにします。

**ステップ 3** [保存 (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。

## 認証サーバとポリシーサーバの設定

Cisco DNA 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。

### 始める前に

- 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、Cisco DNA Center と Cisco ISE が [Cisco DNA Center 設置ガイド](#) の説明に従って、統合されたことを確認します。
- 他の製品 (Cisco ISE 以外) で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバで Cisco DNA Center を登録します。これには、AAA サーバと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバで Cisco DNA Center の属性名を定義します。
  - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバ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。



1. ネットワークに Cisco ISE バージョン 2.3 以降を導入した。マルチホスト Cisco ISE を導入している場合は、Cisco ISE 管理ノードと統合している。
2. Cisco ISE ノードで SSH が有効になっている。
3. Cisco DNA Center と統合する予定の Cisco ISE ホストで pxGrid サービスが有効になっており、ERS サービスが読み取り/書き込み操作に対して有効になっている。



---

(注) Cisco ISE バージョン 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Cisco DNA Center は現在 2 つを超える pxGrid ノードをサポートしていません。

---

4. Cisco ISE GUI と Cisco ISE シェルのユーザ名とパスワードが同じである。
5. Cisco DNA Center と Cisco ISE の間にプロキシが設定されていない。プロキシサーバが Cisco ISE に設定されている場合、Cisco DNA Center の IP アドレスはそのプロキシサーバをバイパスする必要があります。
6. Cisco DNA Center と Cisco ISE の間にファイアウォールが存在しない。ファイアウォールがある場合は、Cisco DNA Center と Cisco ISE の間の通信を確立します。
7. Cisco DNA Center と Cisco ISE の間の ping が、IP アドレスとホスト名の両方で成功する。
8. Cisco ISE 管理ノード証明書のサブジェクト名または SAN のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている。
9. サードパーティ証明書を使用している場合は、証明書の SAN フィールドにすべての IP アドレスが含まれている。
10. Cisco ISE の pxGrid 承認が自動または手動に設定されており、Cisco DNA Center の pxGrid 接続が有効になっている。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **システム > 設定 > 外部サービスの > 認証およびポリシーサーバ**。

**ステップ 2** [Add] をクリックします。

**ステップ 3** 次の情報を入力して、プライマリ AAA サーバを設定します。

- [Server IP Address] : AAA サーバの IP アドレス。
- [Shared Secret] : デバイス認証のキー。共有秘密情報の長さは、最大 128 文字です。

**ステップ 4** AAA サーバ (Cisco ISE 以外) を設定するには、[Cisco ISE Server] トグルボタンを [Off] 位置のままにして、次の手順に進みます。

Cisco ISE サーバを設定するには、[Cisco ISE Server] トグルボタンを [On] に設定し、次の各フィールドに情報を入力します。

- [Username] : Cisco ISE CLI にログインするために使用する名前。  
(注) このユーザにはスーパーユーザの管理権限が必要です。
- [Password] : Cisco ISE CLI ユーザ名に対応するパスワード。
- [FQDN] : Cisco ISE サーバ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 サーバの FQDN は `ise.cisco.com` である可能性があります。

#### • SSH キー :

SSH キーは Base64 エンコード形式の Diffie-Hellman 暗号キーです。このキーは、Cisco ISE 管理コンソールへの SSH 接続にセキュリティを提供します。Cisco ISE CLI コマンド `show crypto authorized_keys` および `show crypto host_keys` を使用してキーを取得できます。

Cisco ISE。

- [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。
- (注) 必要な情報を入力すると、Cisco ISE は Cisco DNA Center と 2 つのフェーズを経て統合されます。統合が完了するまでに数分かかります。フェーズごとの統合ステータスは、次のように [Authentication And Policy Servers] ページと [System 360] ページに表示されます。

Cisco ISE サーバ登録フェーズ :

- [Authentication and Policy Servers] ページ : 「進行中」
- [System 360] ページ : 「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] ページ : 「アクティブ」
- [System 360] ページ : 「プライマリ使用可能」 および 「PXGRID 使用可能」

設定された ISE サーバ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 ISE 接続を再同期します。

ステップ5 [View Advanced Settings] をクリックして、設定を構成します。

- [Protocol] : [TACACS] と [RADIUS]。[RADIUS] がデフォルトです。両方のプロトコルを選択できません。

注目 ここで Cisco ISE サーバの TACAS 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 サーバを設定するときに、[Design] > [Network Settings] > [Network] で Cisco ISE サーバを TACAS サーバとして設定できません。

- [Authentication Port] : AAA サーバへの認証メッセージのリレーに使用されるポート。デフォルト値は UDP ポート 1812 です。
- [Accounting Port] : AAA サーバ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。デフォルトの UDP ポートは 1813 です。
- [Port] : TACAS によって使用されるポート。デフォルトポートは 49 です。
- [Retries] : 接続の試行が中止される前に、Cisco DNA 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 サーバの応答を待機する時間。デフォルトのタイムアウトは 4 秒です。

ステップ6 [Add] をクリックします。

ステップ7 セカンダリサーバを追加するには、ステップ2～6を繰り返します。

---

## Cisco AI ネットワーク分析 データ収集の設定

Cisco AI ネットワーク分析が、ワイヤレスコントローラおよびサイト階層から Cisco DNA Center にネットワークイベントデータをエクスポートできるようにするには、次の手順を実行します。

### 始める前に

- Cisco DNA Center 用の Cisco DNA 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、Cisco DNA Advantage ソフトウェアライセンスに含まれています。
- AI ネットワーク分析 アプリケーションがダウンロードおよびインストールされていることを確認します。パッケージと更新のダウンロードとインストール (78 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)

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings]

ステップ2 [System Configuration] までスクロールダウンし、**AI ネットワーク分析** を選択します。  
[AI ネットワーク分析 (SIP MWI notification mechanism) ] ウィンドウが表示されます。

## 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.

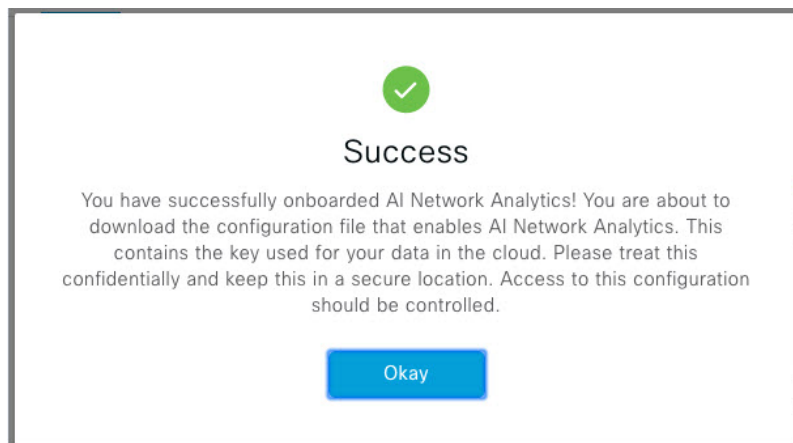
Configure

[Recover from a config file](#) ⓘ

ステップ3 次のいずれかを実行します。

- アプライアンスに以前のバージョンの Cisco AI ネットワーク分析 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。
  1. [Recover from a config file] をクリックします。  
[Restore AI ネットワーク分析] ウィンドウが表示されます。
  2. 表示されたエリアにコンフィギュレーション 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。
  3. [Restore] をクリックします。  
Cisco AI ネットワーク分析 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 ネットワーク分析 を初めて設定する場合は、次の手順を実行します。
  1. [Configure] をクリックします。
  2. [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。
  3. [次へ (Next)] をクリックします。  
[terms and conditions] ウィンドウが表示されます。
  4. [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 ネットワーク分析 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。



ステップ 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、[Cloud Connection] エリアに  が表示されます。

ステップ 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。

---

## Cisco AI ネットワーク分析 データ収集の無効化

Cisco AI ネットワーク分析 データ収集を無効にするには、Cisco AI ネットワーク分析 クラウドサービスへの接続をオフ（無効）にする必要があります。これにより、AI 駆動型の問題、ネットワークヒートマップ、サイトの比較、ピアの比較など、Cisco AI ネットワーク分析 関連のすべての機能が無効になります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings]

ステップ 2 [System Configuration] までスクロールダウンし、AI ネットワーク分析 を選択します。  
[AI ネットワーク分析 (SIP MWI notification mechanism) ] ウィンドウが表示されます。

ステップ 3 [Cloud Connection] エリアで、 が表示されるように、ボタンをクリックしてオフにします。

図 2: データ収集を無効にした [AI Network Analytics] ウィンドウ

## 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.

Cloud Connection ⓘ



Update

Cloud Data Storage  
Europe (Germany)

[Download configuration file](#)

**ステップ 4** [Update] をクリックします。

**ステップ 5** Cisco AI ネットワーク分析 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。

**ステップ 6** (オプション) 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。

## 機械推論ナレッジベースの更新

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にアクセスするために、機械推論ナレッジベースを毎日自動更新するように Cisco DNA Center を設定することもできれば、手動更新を実行することもできます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] の順に選択します。

**ステップ 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の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] 領域が表示され、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 Cisco DNA Center で自動的に毎日更新されます。

**ステップ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、次回の更新の日付と時刻が表示されます。

自動更新は、Cisco DNA 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。

**ステップ4** 機械推論ナレッジベースを Cisco DNA Center で手動で更新するには、次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 Cisco DNA Center にインポートします。次の手順を実行します。

1. [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。

2. 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。
3. [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 Cisco DNA Center にインポートします。

---

## シスコアカウント

### シスコのクレデンシャルの設定

Cisco DNA Center の Cisco のクレデンシャルを設定できます。Cisco 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名とパスワードです。



- (注) 次の手順を使用して、Cisco DNA Center 用に設定された Cisco のクレデンシャルは、ソフトウェアイメージや更新プログラムをダウンロードするために使用されます。Cisco のクレデンシャルはまた、セキュリティのために、このプロセスによって暗号化されます。

#### 始める前に

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、[ユーザロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ 1** [System]Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして > [Settings] > [Cisco Accounts] > [Cisco.com Credentials] を選択します。

**ステップ 2** シスコユーザ名およびパスワードを入力してください。

**ステップ 3** [Save] をクリックします。

cisco.com クレデンシャルがソフトウェアとサービスに対して設定されます。

## シスコのクレデンシャルのクリア

Cisco DNA Center に対して現在設定されている cisco.com のログイン情報を削除するには、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 Cisco DNA 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 \(46 ページ\)](#) を参照してください。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Cisco Accounts] > [Cisco.com Credentials] の順に選択します。

**ステップ 2** [Clear] をクリックします。

**ステップ 3** 表示されたダイアログボックスで、[Continue] をクリックして操作を確定します。

## 接続モードの設定

接続モードは、Cisco DNA 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。



**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Cisco Accounts] > [SSM Connection Mode] の順に選択します。

次の接続モードを使用できます。

- 直接
- オンプレミス CSSM
- スマートプロキシ

**ステップ 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。

**ステップ 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。

- [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。
- [On-Prem CSSM Host]、[Smart Account Name]、[Client Id]、および [Client Secret] の詳細を入力します。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。
- [Test Connection] をクリックして CSSM 接続を検証します。
- [Save] をクリックしてから [Confirm] をクリックします。

**注意** ネットワーク内に CSSM ですでに登録されているスマート対応デバイスがある場合、それらのデバイスは CSSM から登録解除されます。登録を解除すると、デバイスは評価ライセンスモードになり、ネットワークパフォーマンスの低下や停止が発生することがあります。したがって、この操作はメンテナンス期間中に実行することを推奨します。

**ステップ 4** [Smart Proxy] を選択し、Cisco DNA 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。Cisco DNA 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。

## プラグアンドプレイの登録

Cisco DNA 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 Cisco DNA 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。

始める前に

**SUPER-ADMIN-ROLE** またはシステム管理権限を持つ **CUSTOM-ROLE** のユーザ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に割り当てられます。

- スマートアカウント管理者ユーザは、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。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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。

**ステップ 2** [Register] をクリックして、バーチャルアカウントを登録します。

**ステップ 3** [バーチャルアカウントの登録 (Register Virtual Account)] ウィンドウで、設定したスマートアカウントが [スマートアカウントの選択 (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バーチャルアカウントを選択できます。

**ステップ 4** 必要なコントローラのオプションボタンをクリックします。

**ステップ 5** IP アドレスまたは FQDN (完全修飾ドメイン名) を入力します。

**ステップ 6** 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。

**ステップ 7** [保存 (Save)] をクリックします。

## スマートアカウントの設定

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。

### 始める前に

スーパー管理者ロール (SUPER-ADMIN-ROLE) 権限を取得しておきます

**ステップ 1** [System]Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして > [Settings] > [Cisco Accounts] > [Smart Account]。

**ステップ 2** [Add] ボタンをクリックします。スマートアカウントのログイン情報を入力するように求められます。

- スマートアカウントのユーザー名およびパスワードを入力します。
- [Save] をクリックします。スマートアカウントが設定されます。

**ステップ 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。

- ドロップダウンリストから [スマートアカウント (Smart Account)] を選択します。
- [Save] をクリックします。

**ステップ 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。

**ステップ 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。

**ステップ 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。

## スマートライセンス

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンスモデルです。また、これは安全です。ユーザがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。製品アクティベーションキー (PAK) は不要です。
- **管理の統合**：My Cisco Entitlements (MCE) は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります ([software.cisco.com](https://software.cisco.com))。

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

### 始める前に

- 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 (「[シスコのクレデンシャルの設定 \(39 ページ\)](#)」を参照)、Cisco SSM で Cisco DNA 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は、[System] > [Settings] > [Cisco Accounts] > [SSM Connection Mode] が [On-Prem CSSM] の場合はサポートされません。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Cisco Accounts] > [Smart Licensing] の順に選択します。

デフォルトでは、[Smart User] と [Smart Domain] の詳細が表示されます。

**ステップ 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。

**ステップ 3** [登録 (Register)] をクリックします。

**ステップ 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、Cisco DNA Center の使用可能なライセンスを確認します。

## デバイスの可制御性

デバイスの可制御性とは、Cisco DNA Center におけるいくつかのデバイス層機能の同期状態を徹底するシステムレベルのプロセスです。この目的は、Cisco DNA Center がデバイスを管理するのに必要なネットワーク設定の導入を支援することです。ディスカバリを実行したり、インベントリにデバイスを追加したり、デバイスをサイトに割り当てたりすると、ネットワークデバイスに変更が加えられます。

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) Cisco DNA 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。

下記のデバイス設定がデバイスの可制御性の一部として有効になります。

- デバイス検出
  - [SNMP Credentials]
  - [NETCONF Credentials]
- インベントリへのデバイスの追加
  - Cisco TrustSec (CTS) クレデンシャル



(注) [Global] サイトが Cisco ISE で AAA として設定されている場合のみ、Cisco TrustSec (CTS) クレデンシャルがインベントリ中にプッシュされます。それ以外の場合は、CTS が Cisco ISE で AAA として設定されている場合に「サイトへの割り当て」中に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
  - コントローラ証明書
  - SNMP トラップサーバ定義
  - Syslog サーバ定義
  - NetFlow サーバ定義

- Wireless Service Assurance (WSA)
- IPDT の有効化

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有効にたくない場合は、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 \(46 ページ\)](#) を参照してください。

デバイスの可制御性が無効の場合、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、上述のクレデンシャルや機能が Cisco DNA Center で設定されることはありません。ただし、テレメトリ設定と関連する設定は、デバイスのプロビジョニング時、または **[Provision] > [Inventory] > [Actions]** から **[Update Telemetry Settings]** アクションが実行される時にプッシュされます。サイトでのネットワーク設定の作成時にデバイスの可制御性が有効になっていると、関連付けられたデバイスは、それに応じて設定されます。

次のような状況により、デバイスの可制御性によってデバイスにネットワーク設定が適用されるかどうかが決まります。

- **デバイス検出** : SNMP と NETCONF 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。
- **インベントリ内のデバイス (Device in Inventory)** : 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
```

- **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、Cisco DNA Center はデフォルトでデバイスを **[Managed]** 状態にして **[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 Cisco DNA Center しません。
- **サイトに移動されたデバイス (Device Moved to Site)** : デバイスを **[グローバル (Global)]** サイトから、SNMP サーバ、Syslog サーバ、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、Cisco DNA Center ではデバイスのこれらの設定が新しいサイト用に定義された設定に変更されます。

- **サイトから削除されたデバイス (Device Removed from Site)** : デバイスをサイトから削除する場合、Cisco DNA Center ではデバイスの SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が削除されません。
- **削除されるデバイス Cisco DNA Center** : デバイスを Cisco DNA Center から削除し、[Configuration Clean-up] チェックボックスがオンにすると、SNMP サーバ、Syslog サーバ、および NetFlow コレクタ設定はデバイスから削除されます。
- **別のサイトに移動したデバイス (Device Moved from Site to Site)** : たとえばサイト A からサイト B にデバイスを移動させると、Cisco DNA Center ではデバイスの SNMP サーバ、Syslog サーバ、NetFlow コレクタ設定が、サイト B に割り当てられた設定に置き換えられます。
- **サイトテレメトリの変更の更新** : デバイスの可制御性の範囲内にある設定に対する変更は、デバイスの可制御性が有効になっていない場合でも、デバイスのプロビジョニング中、またはテレメトリ設定の更新アクションの実行時にネットワークデバイスに適用されます。

## デバイスの可制御性の設定

デバイスの可制御性は、Cisco DNA 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の展開を支援します。



- (注) デバイスの可制御性を無効にすると、[Device Controllability] ページに記載されているログイン情報または機能は、ディスカバリ時または実行時にデバイスに設定されません。

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。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[System] > [Settings] > [Device Settings] > [Device Controllability] を選択します。

**ステップ 2** [Enable Device Controllability] チェックボックスをオフにします。

**ステップ 3** [保存 (Save)] をクリックします。

## ライセンス契約書の受諾

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。



(注) cisco.com のログイン情報をまだ設定していない場合は、先に進む前に、[Device EULA Acceptance] ウィンドウで設定するように求められます。

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Device Settings] > [Device EULA Acceptance] の順に選択します。
- ステップ 2** [Cisco End User License Agreement] リンクをクリックし、EULA を読みます。
- ステップ 3** [I have read and accept the Device EULA] チェックボックスをオンにします。
- ステップ 4** [保存 (Save)] をクリックします。

## クラウドアクセスキー

Cisco DNA 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 WLC のクラウドプロビジョニングで表示して使用できます。

### 始める前に

- 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 WLC 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 Cisco DNA 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 Cisco DNA Center のリストから選択します。
- Cisco DNA 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 \(57 ページ\)](#) 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 Cisco DNA 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、[パッケージと更新のダウンロードとインストール（78 ページ）](#)を参照してください。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Cloud Access Keys] の順に選択します。
- ステップ 2** [Add] をクリックします。
- ステップ 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。
- ステップ 4** [Save and Discover] をクリックします。
- 

#### 次のタスク

- 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。

## 整合性検証

整合性検証 (IV) では、主要な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) このリリースでは、IV で Cisco DNA Center にアップロードされたソフトウェアイメージの整合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 ファイルのアップロード

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://tools.cisco.com/cscrd/security/center/files/trust/Cisco\\_KnownGoodValues.tar](https://tools.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。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [External Services] > [Integrity Verification] の順に選択します。

**ステップ 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 Cisco DNA Center ユーザ。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。

**ステップ 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://tools.cisco.com> への接続のみを開く必要があります。

**ステップ 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 Cisco DNA Center にインポートされます。

(注) <https://tools.cisco.com> へのセキュアな接続は、Cisco DNA 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。

**ステップ 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。

**ステップ 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。

**ステップ 7** [Import] をクリックします。

KGV ファイルが Cisco DNA Center にインポートされます。

**ステップ 8** インポートが完了したら、UI 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、Cisco DNA 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、Cisco DNA 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。

次の KGV 自動ダウンロード情報が表示されます。

- [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。

---

### 次のタスク

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検証不能ステータス（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）。
-

## IP アドレスマネージャの設定

Cisco DNA Center を外部 IP アドレスマネージャと通信するように設定できます。Cisco DNA 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、Cisco DNA Center はその情報を外部 IP アドレスマネージャに伝達します。

### 始める前に

- 外部 IP アドレスマネージャがすでに設定され、動作している必要があります。
- トラストプールに IPAM 証明書を手動でインポートします。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Settings] > [External Services] > [IP Address Manager]** の順に選択します。

**ステップ 2** [IP Address Manager] セクションで、以下のフィールドに必須情報を入力します。

- [Server Name] : サーバの名前。
- [Server URL] : サーバの IP アドレス。
- [Username] : サーバのアクセスに必要なユーザ名。
- [Password] : サーバのアクセスに必要なパスワード。
- [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。

(注) [BlueCat] をプロバイダーとして選択した場合は、自分のユーザに、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** のマニュアルを参照してください。

- [View] : ドロップダウンリストから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。

**ステップ 3** [Apply] をクリックして設定を適用し、保存します。

### 次のタスク

[System 360] タブをクリックし、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。

## デバッグログの設定

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、Cisco DNA 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 Cisco DNA Center ホストの一元的な場所に保存されます。この場所から、Cisco DNA Center は、GUI でログを照会して表示できます。ログファイルの合計圧縮サイズは 2 GB です。ログファイルが 2 GB を超える場合、古いログファイルは新しいファイルで上書きされます。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [System Configuration] > [Debugging Logs] の順に選択します。

[Debugging Logs] ウィンドウには、次のフィールドが表示されます。

- Services
- Logger Name
- Logging Level
- Timeout

**ステップ 2** [Services] 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。

[Services] ドロップダウンリストには、現在 Cisco DNA Center に設定され、実行しているサービスが表示されます。

**ステップ 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。

**ステップ 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。

Cisco DNA 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

**ステップ 5** [Timeout] 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。

**ステップ 6** 選択内容を確認し、[Apply] をクリックします

（選択内容をキャンセルするには [Cancel] をクリックします）。

## ネットワークの再同期間隔の設定

[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。

### 始める前に

- 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 ロールの概要（81 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。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Device Settings] > [Network Resync Interval] の順に選択します。
- ステップ 2** [Resync Interval] フィールドに、新しい時間値 (分) を入力します。
- ステップ 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。
- ステップ 4** [保存 (Save)] をクリックします。
- 

## 監査ログの表示

監査ログは、Cisco DNA 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 PKI 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。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [アクティビティ (Activity)] > [監査ログ (Audit Logs)]。

[監査ログ (Audit Logs)] 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、Cisco DNA 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。

- ステップ 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。
- [時間範囲 (Time Range)] エリアで、[過去 2 週間 (Last 2 Weeks)]、[過去 7 日間 (Last 7 Days)]、[過去 24 時間 (Last 24 Hours)]、または [過去 3 時間 (Last 3 Hours)] の時間範囲を選択します。
  - カスタム範囲を指定するには、[日付 (By date)] をクリックし、開始日時と終了日時を指定します。
  - [Apply] をクリックします。

- ステップ 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、Cisco DNA 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、Cisco DNA Center によって実行されたタスクのサブタスクです。

- ステップ 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 [イベント ID (Event ID)] > [イベント ID をクリップボードにコピー (Copy Event ID to

**Clipboard**)] をクリックします。コピーされた ID を活用すると、API を使用してイベント ID に基づいて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 **[説明 (Description)]**、**[ユーザ (User)]**、**[インターフェイス (Interface)]**、**[宛先 (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、『[CISCO DNA Center PlatformIntent APIs](#)』を参照してください。

- ステップ 5** (オプション) **[フィルター (Filter)]** をクリックして、ユーザ ID またはイベント ID でログをフィルタリングします。
- ステップ 6** 右側のペインで、**[検索 (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。
- ステップ 7** Cisco DNA Center GUI で **[Menu]** アイコン (☰) をクリックして **[Activity] > [Scheduled Tasks]** で、OS の更新やデバイスの交換などの予定 (upcoming)、進行中 (in progress)、完了 (completed) および失敗 (failed) 管理タスクを表示します。

## 監査ログに対する Syslog 通知の作成

監査ログの syslog 通知を作成できます。たとえば、Postman などのサードパーティ製ソフトウェア開発 API ツールを使用して、監査ログ通知を syslog サーバに送信する POST メソッドを作成します。次に例を示します。

```
POST <cluster-ip>/dna/intent/api/v1/subscription'
```

Cisco DNA Center から syslog サーバへの監査ログ通知を実行およびテストできます。Cisco DNA Center GUI で **[Menu]** アイコン (☰) をクリックして **[Platform] > [Developer Toolkit] > [APIs]** の順に選択します。

## 高可用性のアクティブ化

Cisco DNA 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。

- ステップ 1** Cisco DNA Center GUI で、**[Menu]** アイコン (☰) をクリックし、**[System] > [Settings] > [System Configuration] > [High Availability]** の順に選択します。
- ステップ 2** **[Activate High Availability]** をクリックします。
- HA の詳細については、『[Cisco DNA Center High Availability Guide](#)』を参照してください。

## 統合設定の設定

ファイアウォールなどのルールが、Cisco DNA Center と Cisco DNA 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。Cisco DNA 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。

### 始める前に

前のセクションの説明に従って Cisco DNA Center プラットフォーム をインストールしておきます。

**ステップ 1** サードパーティ製アプリケーションが Cisco DNA 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、Cisco DNA 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 ノードクラスタセットアップの VIP アドレスを設定します。

**ステップ 2** [Apply] ボタンをクリックします。

## ログインメッセージの設定

ユーザが Cisco DNA Center にログインしたときにすべてのユーザに表示されるメッセージを設定できます。

### 始める前に

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

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [System Configuration] > [Login Message] の順に選択します。

**ステップ 2** [Login Message] テキストボックスにテキストメッセージを入力します。

**ステップ 3** [保存 (Save)] をクリックします。

このメッセージが Cisco DNA Center にログインしたときに表示されます。

**ステップ 4** ログインメッセージを削除する場合は、[Login Message] 画面で [Clear] をクリックします。



ステップ5 [Save] をクリックして設定を更新します。

## プロキシの設定

Cisco DNA Center と管理対象のネットワークデバイスやソフトウェアアップデートをダウンロードする Cisco cloud との間に中継装置としてプロキシサーバが構成されている場合は、プロキシサーバへのアクセスを設定する必要があります。Cisco DNA Center GUI の [Proxy Config] ウィンドウを使用して、アクセスを設定します。



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

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [System Configuration] > [Proxy Config] の順に選択します。

**ステップ2** プロキシサーバの URL アドレスを入力します。

**ステップ3** プロキシサーバのポート番号を入力します。

HTTP の場合、ポート番号は通常 80 です。

**ステップ4** (オプション) プロキシサーバが認証を必要とする場合、プロキシサーバにアクセスするためのユーザ名とパスワードを入力します。

**ステップ5** [Validate Settings] チェックボックスをオンにし、適用時に Cisco DNA Center でプロキシ構成時の設定が検証されるようにします。

**ステップ6** 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。

次の点に注意してください。

- プロキシを設定した後、[Proxy Config] ウィンドウに設定を表示できます。
- Cisco DNA 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で SSL 復号が有効になっている場合、または Cisco DNA Center と管理対象のデバイスとの間にプロキシが設定されている場合は、手順 7 に進みます。
- Cisco DNA 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で SSL 復号が有効になっていない場合は、この手順までで終了です。

ステップ7 プロキシ証明書を Cisco DNA Center にインポートします。

「[プロキシ証明書の設定 \(61 ページ\)](#)」を参照してください。

## セキュリティ Cisco DNA Center

Cisco DNA Center は、それ自体とモニタ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。次のセキュリティに関する推奨事項に従うことを強く推奨します。

- Cisco DNA 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 Cisco DNA 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、Cisco DNA 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、Cisco DNA 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 ノードクラスタセットアップで Cisco DNA 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。
- Cisco DNA Center の自己署名サーバ証明書を、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。
- 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 Cisco DNA Center をアップグレードしてください。詳細については、『[Cisco DNA Center Upgrade Guide](#)』を参照してください。
- HTTPS プロキシサーバを使用する Cisco DNA 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。Cisco DNA 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 Cisco DNA 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。

## 最小 TLS バージョンの変更と RC4-SHA の有効化 (安全でない)

外部ネットワークからのノースバウンド REST API 要求 (ノースバウンド REST API ベースのアプリケーション、ブラウザ、および HTTPS を使用して Cisco DNA Center に接続しているネッ

トワークデバイスなど) は、Transport Layer Security (TLS) プロトコルを使用して保護されません。

デフォルトでは、Cisco DNA Center は TLSv1.1 と TLSv1.2 をサポートしますが、RC4 暗号には既知の弱点があるため、SSL/TLS 接続の RC4 暗号はサポートしません。ネットワークデバイスでサポートされている場合は、最小 TLS バージョンを TLSv1.2 にアップグレードすることを推奨します。

Cisco DNA Center 制御下のネットワークデバイスが既存の最小 TLS バージョン (TLSv1.1) または暗号をサポートできない場合、Cisco DNA Center には最小 TLS バージョンをダウングレードし、RC4-SHA を有効にする設定オプションが用意されています。ただし、セキュリティ上の理由から、Cisco DNA Center TLS のバージョンをダウングレードしたり RC4-SHA 暗号を有効にしたりすることは推奨されません。

Cisco DNA Center で TLS のバージョンの変更や RC4-SHA の有効化が必要な場合は、アプライアンスにログインし、CLI を使用して行います。



(注) CLI コマンドは、リリースごとに変更される可能性があります。次の CLI の例では、すべての Cisco DNA Center リリースに適用されない可能性のあるコマンド構文を使用しています。

#### 始める前に

この手順を実行するためには、maglev SSH アクセス権限が必要です。



**重要** このセキュリティ機能は、Cisco DNA Center にポート 443 を適用します。この手順の実行により、Cisco DNA Center インフラストラクチャへのポートのトラフィックが数秒間無効になることがあります。したがって、TLS の設定は頻繁に行わないようにし、オフピーク時間またはメンテナンス期間中にのみ行う必要があります。

**ステップ 1** SSH クライアントを使用して、設定ウィザードで指定した IP アドレスで Cisco DNA Center アプライアンスにログインします。

SSH クライアントで入力する IP アドレスは、ネットワーク アダプタ用に設定した IP アドレスです。この IP アドレスは、アプライアンスを外部ネットワークに接続します。

**ステップ 2** 要求された場合は、SSH アクセス用にユーザ名とパスワードを入力します。

**ステップ 3** 次のコマンドを入力して、クラスタで現在有効になっている TLS バージョンを確認します。

#### 例

```
Input
$ magctl service tls_version --tls-min-version show
Output
TLS minimum version is 1.1
```

**ステップ 4** クラスタの TLS バージョンを変更する場合は、次のコマンドを入力します。たとえば、Cisco DNA Center 制御下のネットワークデバイスが既存の TLS バージョンをサポートできない場合は、現在の TLS バージョンを下位バージョンに変更する必要があることがあります。

**例：TLS バージョン 1.1 から 1.0 への変更**

```
Input
$ magctl service tls_version --tls-min-version 1.0
Output
Enabling TLSv1.0 is recommended only for legacy devices
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.0 for api-gateway
deployment.extensions/kong patched
```

**例：TLS バージョン 1.1 から 1.2 への変更 (RC4-SHA を有効にしていない場合のみ可能)**

```
Input
$ magctl service tls_version --tls-min-version 1.2
Output
Enabling TLSv1.2 will disable TLSv1.1 and below
Do you want to continue? [y/N]: y
WARNING: Enabling TLSv1.2 for api-gateway
deployment.extensions/kong patched
```

(注) RC4-SHA 暗号が有効になっている場合、TLS バージョン 1.2 を最小バージョンとして設定することはサポートされていません。

**ステップ 5** クラスタで RC4-SHA を有効にするには、次のコマンドを入力します (セキュアでないため、必要な場合だけにしてください)。

TLS バージョン 1.2 が最小バージョンである場合、RC4-SHA 暗号を有効にすることはサポートされていません。

**例：TLS バージョン 1.2 が有効になっていない**

```
Input
$ magctl service ciphers --ciphers-rc4=enable kong
Output
Enabling RC4-SHA cipher will have security risk
Do you want to continue? [y/N]: y
WARNING: Enabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

**ステップ 6** プロンプトで次のコマンドを入力して、TLS および RC4-SHA が設定されていることを確認します。

**例**

```
Input
$ magctl service display kong
Output
containers:
- env:
  - name: TLS_V1
    value: "1.1"
  - name: RC4_CIPHERS
    value: "true"
```

RC4 および TLS の最小バージョンが設定されている場合は、**magctl service display kong** コマンドの env: にリストされます。これらの値が設定されていない場合は、env: に表示されません。

**ステップ 7** 以前に有効にした RC4-SHA 暗号を無効にする場合は、クラスタで次のコマンドを入力します。

```
Input
$ magctl service ciphers --ciphers-rc4=disable kong
Output
WARNING: Disabling RC4-SHA Cipher for kong
deployment.extensions/kong patched
```

**ステップ 8** Cisco DNA Center アプライアンスからログアウトします。

## プロキシ証明書の設定

ネットワーク構成によっては、プロキシゲートウェイは、Cisco DNA 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、Cisco DNA 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 Cisco DNA Center と通信できます。ネットワークデバイスが Cisco DNA 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 Cisco DNA Center を信頼および認証できるように、プロキシと Cisco DNA Center サーバ証明書を同一にすることを推奨します。

プロキシゲートウェイが Cisco DNA 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 Cisco DNA Center にインポートします。

### 始める前に

- 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 ロールの概要 \(81 ページ\)](#) を参照してください。
- Cisco DNA 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、Cisco DNA Center にインポートする必要があります。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [Proxy Certificate] の順に選択します。
- ステップ 2** [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、グリニッジ標準時（GMT）値で表示されます。証明書有効期限日時 の 2 ヶ月前に、Cisco DNA Center の GUI にシステム通知が表示されます。
- ステップ 3** 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 Cisco DNA 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、Cisco DNA Center にアップロードもされません。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** [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。
- ステップ 6** 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。

---

## 証明書および秘密キーのサポート

Cisco DNA Center は、セッション（HTTPS）の認証に使用される PKI 証明書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。Cisco DNA Center は、PKI 証明書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 Cisco DNA Center のアイデンティティ証明書になり、Cisco DNA 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。

Cisco DNA 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 (Private key)



(注) 秘密キーについては、Cisco DNA Center で RSA キーのインポートをサポートしています。DSA、DH、ECDH、および ECDSA キータイプはサポートされていないため、インポートしないでください。また、独自のキー管理システムで秘密キーを保護する必要があります。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。

インポートする前に、内部 CA で発行された有効な X.509 証明書と秘密キーを取得する必要があります。証明書は所有する秘密キーに対応している必要があります。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。Cisco DNA 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 Cisco DNA Center との信頼関係を確立できます。



(注) 自己署名証明書を使用したり、Cisco DNA Center にインポートしたりすることは推奨されません。内部 CA から有効な X.509 証明書をインポートすることをお勧めします。さらに、PnP 機能を正常に動作させるには、自己署名証明書 (デフォルトで Cisco DNA Center にインストールされている) を、内部 CA によって署名された証明書で置き換える必要があります。

Cisco DNA 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。

## 証明書チェーンのサポート

Cisco DNA 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。Cisco DNA 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する必要があります。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 Cisco DNA Center certificate] : 件名フィールドに CN=<FQDN of Cisco DNA 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) サードパーティ証明書をインストールする場合は、Cisco DNA Center へのアクセスに使用するすべての IP アドレス（物理ポートと VIP の両方）と DNS 名が証明書の **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、『[Cisco DNA 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 Cisco DNA Center certificate] : 件名フィールドに Cisco DNA Center の証明書を発行する（下位）CA の CN が含まれていて、発行元がルート CA の CN である。
- [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。

## Cisco DNA Center サーバ証明書の更新

Cisco DNA Center は、X.509 証明書と秘密キーの Cisco DNA Center へのインポートとストレージをサポートします。インポートをすると、証明書と秘密キーを使用して、Cisco DNA 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 デバイスの間に安全で信頼できる環境を作成することができます。

GUI の [Certificate] ウィンドウを使用して、証明書と秘密キーをインポートできます。

### 始める前に

内部 CA から発行された有効な X.509 証明書を取得する必要があります。証明書は所有する秘密キーに対応している必要があります。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [System Certificate] の順に選択します。

**ステップ 2** [System Certificate] ウィンドウで、現在の証明書データを確認します。

この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、Cisco DNA Center の自己署名証明書のデータです。自己署名証明書の有効期限は、数年先に設定されています。

(注) [Expiration Date and Time] は、グリニッジ標準時 (GMT) 値で表示されます。証明書有効期限の 2 ヶ月前に、Cisco DNA Center の GUI にシステム通知が表示されます。

[Certificate] ウィンドウに表示されるその他のフィールドは次のとおりです。

- [Current Certificate Name] : 現在の証明書の名前
- [Issuer] : 証明書に署名し、証明書を発行したエンティティの名前
- [認証局 (Certificate Authority) ] : 自己署名または CA の名前



- [Expires] : 証明書の有効期限

**ステップ 3** 現在の証明書を置換するには、[Replace Certificate] をクリックします。

次の新しいフィールドが表示されます。

- [Certificate] : 証明書データを入力するフィールド
- [Private Key] : 秘密キーデータを入力するフィールド

**ステップ 4** [Certificate] ドロップダウンリストから、Cisco DNA 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 エンハンスド 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

**ステップ 5** [PEM] を選択した場合、次のタスクを実行します。

- [Certificate] フィールドで、[Drag and Drop] 領域にファイルをドラッグアンドドロップして、[PEM] ファイル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、.cert、.crt) が必須です。証明書の最大ファイルサイズは 10 KB です。

- [Private Key] フィールドで、[Drag and Drop] 領域にファイルをドラッグアンドドロップして、秘密キーをインポートします。

- 秘密キーの [Encrypted] ドロップダウンリストから、暗号化オプションを選択します。

- 暗号化を選択した場合、[Password] フィールドに秘密キーのパスフレーズを入力します。

(注) 秘密キーには、有効な秘密キー形式の拡張子 (.pem または .key) が必須です。

**ステップ 6** [PKCS] を選択した場合、次のタスクを実行します。

- [Certificate] フィールドで、[Drag and Drop] 領域にファイルをドラッグアンドドロップして、[PKCS] ファイル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、.p12) が必須です。証明書の最大ファイルサイズは 10 KB です。

- [Certificate] フィールドについては、[Password] フィールドで証明書用のパスフレーズを入力します。

(注) PKCS の場合は、インポートした証明書もパスフレーズを必要とします。

- [秘密キー (Private Key) ] フィールドについては、秘密キーの暗号化オプションを選択します。

- [Private Key] フィールドで、暗号化を選択した場合は、[Passphrase] フィールドに秘密キーのパスフレーズを入力します。

ステップ7 [Upload/Activate] をクリックします。

ステップ8 [Certificate] 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。

[Certificate] ウィンドウに表示される情報が更新され、新しい証明書名、発行者、および認証局が反映されます。

## 証明書の管理

### デバイス証明書の有効期間の設定

Cisco DNA Center では、Cisco DNA 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。Cisco DNA Center での証明書の有効期間のデフォルト値は 365 日です。Cisco DNA 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 Cisco DNA 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。

GUI の [PKI Certificate Management] ウィンドウを使用してデバイス証明書の有効期間を変更できます。

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [PKI Certificate] の順に選択します。

ステップ2 [Device Certificate] タブをクリックします。

ステップ3 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。

ステップ4 [Device Certificate Lifetime] フィールドに、新しい値（日数）を入力します。

ステップ5 [保存 (Save)] をクリックします。

ステップ6 (オプション) [PKI Certificate Management] ウィンドウを更新して、新しいデバイス証明書の有効期間の値を確認します。

### PKI 証明書のロールをルートから下位に変更

デバイス PKI CA は Cisco DNA Center のプライベート CA であり、サーバ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 PKICA のロールをルート CA から下位 CA に変更するには、次の手順を実行します。

Cisco DNA Center のプライベート CA をルート CA から下位 CA に変更するときは、次のことに注意してください。

- Cisco DNA Center が下位 CA の役割を果たすようにする場合、すでにルート CA（たとえば Microsoft CA）があり、Cisco DNA Center を下位 CA として認めているものと見なされます。
- 下位 CA が完全に設定されていない限り、Cisco DNA Center は内部ルート CA としての役割を継続します。
- Cisco DNA Center 用の証明書署名要求ファイルを生成し（次の手順の記述に従う）、手動で外部ルート CA に署名させる必要があります。



(注) Cisco DNA 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 Cisco DNA Center にインポートし直す必要があります（次の手順の記述に従う）。  
インポート後、Cisco DNA 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。
- 内部ルート CA から管理対象デバイスで使用する下位 CA へのスイッチオーバーは自動ではサポートされません。したがって、内部ルート CA でまだデバイスが設定されていないことが前提となります。デバイスが設定されている場合、下位 CA に切り替える前に、ネットワーク管理者が既存のデバイス ID 証明書を手動で取り消す必要があります。
- GUI に表示されている下位 CA 証明書有効期間は、証明書から読み取られたもので、システム時刻を使っ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 7 月に GUI で見ると、証明書の有効期間はそのときでも 1 年間と表示されます。
- 下位 CA 証明書として PEM または DER 形式のみを使用できます。
- 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もありません。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 Cisco Discovery Protocol (CDP) 送信元としてのみ使用します。

[PKI Certificate Management] ウィンドウの GUI を使用して、Cisco DNA Center のプライベート（内部）CA のロールをルート CA から 下位 CA に変更できます。

### 始める前に

ルート CA 証明書のコピーが必要です。

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [PKI Certificate] の順に選択します。

**ステップ 2** [CA Management] タブをクリックします。

**ステップ 3** GUI で既存のルートまたは下位 CA 証明書の設定情報を確認します。

- [Root CA Certificate] : 現在のルート CA 証明書 (外部または内部) を表示します。
- [Root CA Certificate Lifetime] : 現在のルート CA 証明書の最新の有効期間を表示します (日数)。
- [Current CA Mode] : 現在の CA モードを表示します (ルート CA または下位 CA)。
- [Sub CA mode] : ルート CA から下位 CA に変更できます。

**ステップ 4** [CA Management] タブで、[Sub CA Mode] チェックボックスをオンにします。

**ステップ 5** [Next] をクリックします。

**ステップ 6** 表示される警告内容を確認します。

- 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。ネットワークデバイスを誤ってルート CA モードで登録した場合は、ルート CA から下位 CA に変更する前に、取り消しをする必要があります。
- 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。

**ステップ 7** [OK] をクリックして続行します。

[PKI Certificate Management] ウィンドウに、[Import External Root CA Certificate] フィールドが表示されません。

**ステップ 8** [Import External Root CA Certificate] 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 Cisco DNA 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せん。

**ステップ 9** [Next] をクリックします。

Cisco DNA Center で証明書署名要求が生成されて表示されます。

**ステップ 10** Cisco DNA 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。

- ステップ 11** 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 Cisco DNA Center にインポートし直す必要があります。
- ステップ 12** ルート CA から下位 CA ファイルを受信した後、Cisco DNA Center の GUI に再度アクセスし、[PKI Certificate Management] ウィンドウに戻ります。
- ステップ 13** [CA Management] タブをクリックします。
- ステップ 14** [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。
- ステップ 15** [Next] をクリックします。
- [PKI Certificate Management] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。
- ステップ 16** [Import Sub CA Certificate] フィールドに下位 CA 証明書をドラッグ 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 Cisco DNA 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。
- ステップ 17** [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 (日数)。
  - [Current CA Mode] : SubCA モードを表示します。

## ロールオーバー下位 CA 証明書のプロビジョニング

Cisco DNA 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に、ユーザがロールオーバー下位 CA として下位証明書を適用することができます。

### 始める前に

- 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、PKI 証明書の権限を下位 CA モードに変更しておく必要があります。[PKI 証明書のロールをルートから下位に変更 \(66 ページ\)](#) 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、Cisco DNA Center の [CA Management] タブの下に [Renew] ボタンが表示されません。
- ロールオーバー下位 CA の署名付き PKI 証明書のコピーが必要です。

- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (≡) をクリックして [System] > [Settings] > [Trust & Privacy] > [PKI Certificate] の順に選択します。
- ステップ 2** [CA Management] タブをクリックします。
- ステップ 3** 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 (日数) を表示します。
  - [Current CA Mode] : SubCA モードを表示します。
- ステップ 4** [Renew] をクリックします。
- Cisco DNA 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。
- ステップ 5** 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。
- ステップ 6** 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 Cisco DNA 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。
- ステップ 7** 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、[PKI Certificate Management] ウィンドウに戻ります。
- ステップ 8** [CA Management] タブをクリックします。
- ステップ 9** 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。
- [PKI Certificate Management] ウィンドウに、[Import Sub CA Certificate] フィールドが表示されます。
- ステップ 10** 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、[Apply] をクリックします。
- ロールオーバー下位 CA 証明書が Cisco DNA 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。

## 証明書の更新

Cisco DNA 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年間有効です。証明書はクラスタをインストールするとすぐに開始され、期限切れに設定される前に Cisco DNA Center によって1年自動的に更新されます。

- 期限切れになる前に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 Cisco DNA Center 設定の両方に適用されます。

**ステップ 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。

**ステップ 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
```

**ステップ 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証明書を更新します。

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

**ステップ 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。

**ステップ 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
```

## トラストプールの設定

Cisco DNA Center には、事前インストールされているシスコ トラストプール 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。Cisco DNA Center は、シスコからの更新されたトラストプール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。トラストプールバンドルは、Cisco DNA 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 トラストプールバンドルは、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 Cisco trustpool バンドルは、シスコクラウド（Cisco InfoSec）で使用できます。リンクは <https://www.cisco.com/security/pki/> にあります。

このトラストプールバンドルは、同じ CA を使用してすべてのネットワークデバイスの証明書および Cisco DNA Center の証明書を管理する、安全で便利な方法を提供します。トラストプールバンドルは Cisco DNA Center によって使用され、自身の証明書およびプロキシゲートウェイ証明書（存在する場合）を検証し、それが有効な CA 署名付き証明書かを判断します。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 Cisco DNA Center を信頼できるように、トラストプールバンドルを使用できます。

GUI の [Trustpool] ウィンドウを使用して、シスコ トラストプール バンドルをインポートします。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [Trustpool] の順に選択します。
- ステップ 2** [Trustpool] ウィンドウで、[Update] ボタンをクリックしてトラストプール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。
- [Update] ボタンは、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どときにのみアクティブになります。
- Cisco DNA Center に新しいトラストプールバンドルがダウンロードおよびインストールされると、Cisco DNA 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、このトラストプールバンドルを使用可能にします。
- ステップ 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。
- ステップ 4** [Export] をクリックして、証明書の詳細を CSV 形式でエクスポートします。
-



## SFTP サーバの設定

SFTP サーバを内部ファイルサーバのバックアップとして使用できます。Cisco DNA Center のローカル SFTP サーバは、セキュアな暗号方式をサポートしています。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Device Settings] > [SFTP] の順に選択します。

**ステップ 2** SFTP の設定を行います。

- [Host] : SFTP サーバのホスト名または IP アドレス。
- [Username] : SFTP サーバにログインするために使用する名前。ユーザには、サーバ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] : SFTP サーバにログインするために使用するパスワード。
- [Port Number] : SFTP サーバが稼働しているポート番号。
- [Root Location] : ファイル転送用の作業ルートディレクトリ。

**ステップ 3** 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、Cisco DNA 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。Cisco DNA Center の SFTP サーバでは、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。弱い暗号方式を許可するには、[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。

**ステップ 4** [保存 (Save)] をクリックします。

**ステップ 5** [SFTP] ウィンドウで新しい SFTP 設定を確認します。

## SNMP プロパティの設定

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。

始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Device Settings] > [SNMP] の順に選択します。

**ステップ 2** 次のフィールドを設定します。

- **再試行回数 (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、Cisco DNA 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。

ステップ 3 [保存 (Save)] をクリックします。

ステップ 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。

## 製品使用状況テレメトリの収集について

Cisco DNA Center は、製品使用状況テレメトリを収集し、Cisco DNA Center アプライアンスのステータスと機能に関するデータを提供します。それらのデータとインサイトにより、シスコは運用および製品の使用状況に関する問題にプロアクティブに対処できます。製品使用状況テレメトリデータは Cisco DNA Center アプライアンスでローカルに収集され、Cisco Connected DNA に送信されます。シスコに送信されるすべてのデータは、暗号化チャネルを介して送信されます。暗号化チャネルは、クラウドベースのソフトウェアのアップデートなど、他の目的にも使用されます。



(注) 製品使用状況テレメトリの収集を無効にすることはできません。

[System] > [Settings] の順に選択してから、[Terms and Conditions] > [Telemetry Collection] の順に選択します。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Telemetry Collection] ページから、ライセンス契約、プライバシーデータ、シスコのプライバシーポリシーを確認できます。

製品使用状況テレメトリの収集はデフォルトで有効になります。次の場合は Cisco Technical Assistance Center (TAC) に連絡することを推奨します。

- テレメトリの設定の変更
- テレメトリに関するその他の問い合わせや要望

## vManage プロパティの設定

Cisco DNA Center は、統合 vManage 設定を使用してシスコの vEdge 展開をサポートします。vEdge トポロジをプロビジョニングする前に、[Settings] ページで vManage の詳細を保存できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [External Services] > [vManage] の順に選択します。

ステップ2 vManage プロパティを設定します。

- [Host Name/IP Address] : vManage の IP アドレス。
- [Username] : vManage にログインするために使用される名前。
- [Password] : vManage にログインするために使用されるパスワード。
- [Port Number] : vManage にログインするために使用されるポート。
- [vBond Host Name/IP Address] : vBond の IP アドレス。vManage を使用して NFV を管理する場合に必要です。
- [Organization Name] : 組織の名前。vManage を使用して NFV を管理する場合に必要です。

ステップ3 vManage 証明書をアップロードするには、[Select a file from your computer] をクリックします。

ステップ4 [保存 (Save) ] をクリックします。

---

## アカウントのロックアウト

アカウント ロックアウト ポリシーを設定して、ユーザ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。

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [Account Lockout] の順に選択します。

ステップ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。

ステップ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] にマウスカーソルを置くと、各パラメータの詳細が表示されます。

ステップ4 [Save] をクリックして、アカウントロックアウトを設定します。

---

## パスワードの有効期限切れ

パスワード有効期限ポリシーを設定して、パスワードの有効期間、パスワードが期限切れになる前にユーザに通知される日数、および猶予期間を管理できます。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Trust & Privacy] > [Password Expiry] の順に選択します。

**ステップ 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。

**ステップ 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] にマウスカーソルを置くと、各パラメータの詳細が表示されます。

**ステップ 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。

---



## 第 4 章

# アプリケーションの管理

- アプリケーション管理 (77 ページ)
- システムの更新プログラムのダウンロードと更新 (78 ページ)
- パッケージと更新のダウンロードとインストール (78 ページ)
- パッケージのアンインストール (80 ページ)

## アプリケーション管理

Cisco DNA 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 Updates] 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、Cisco DNA Center のバージョンおよび Cisco DNA 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なので、ほぼすべての Cisco DNA Center の導入で必要になります。パッケージおよびそのパッケージが必須かどうかに関する説明を表示するには、[Updates] タブでそのパッケージの名前にマウスカーソルを置きます。

各 Cisco DNA 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。



### 重要

アプリケーション管理手順はすべて、Cisco DNA Center GUI から実行します。これらの手順の多くは、シェルにログイン後 CLI を使用して実行することもできますが、この方法はおすすめしません。特に、CLI を使用してパッケージを導入またはアップグレードする場合、**maglev package status** コマンドの結果に、すべてのパッケージが NOT\_DEPLOYED、DEPLOYED、または DEPLOYMENT\_ERROR と表示されている場合を除き、**deploy** または **upgrade** コマンドが入力されていないことを確認する必要があります。その他の状態はすべて、対応するアクティビティが進行中であることを示しています。また、パラレル導入やアップグレードはサポートされていません。

# システムの更新プログラムのダウンロードと更新

アプリケーション管理手順（システムアップデートのダウンロードとインストールを含む）は、[Software Updates] ウィンドウで実行できます。

## 始める前に

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 ロールの概要（81 ページ）](#)」を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Software Updates]。または、クラウドアイコンをクリックし、[Go to Software Updates] リンクをクリックします。

**ステップ 2** [Software Updates] ウィンドウで、次のタブを確認します。

- [Updates] : システムとアプリケーションの更新を示します。[System Update] では、インストールされているシステムのバージョンと、Cisco Cloud からダウンロードされ、利用可能なシステムの更新が表示されます。[Application Updates] は、Cisco Cloud からダウンロードしてインストールできる使用可能なアプリケーション、アプリケーションのサイズ、適切なアクション（ダウンロード、インストール、または更新）を示します。パッケージにカーソルを合わせると、使用可能なバージョンと基本的な説明が表示されます。
- [Installed Apps] : 現在インストールされているアプリケーションパッケージが表示されます。

**重要** [Software Updates] ウィンドウを起動すると、接続のチェックが実行され、ステータスが表示されます。接続の問題がある場合、[Software Updates] ウィンドウには新しい更新が表示されません。

**ステップ 3** システムアップデートが [Software Update] ウィンドウに表示される場合は、[Update] をクリックして Cisco DNA Center を更新します。

更新プロセス中、システムがリブートします。Cisco DNA Center GUI は、システムのリブート中は使用できません。

# パッケージと更新のダウンロードとインストール

Cisco DNA 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せん。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、Cisco DNA Center 上で実行できます。

アプリケーションのパッケージは、インストールと展開に時間がかかる場合があります。そのため、ネットワークのメンテナンス期間中にパッケージをインストールしてください。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Software Updates]**。または、クラウドアイコンをクリックし、[Go to Software Updates] リンクをクリックします。

**ステップ 2** [Software Updates] ウィンドウで、次のタブを確認します。

- **[Updates]** : システムとアプリケーションの更新を示します。[System Update] では、インストールされているシステムのバージョンと、Cisco Cloud からダウンロードされ、利用可能なシステムの更新が表示されます。[Application Updates] は、Cisco Cloud からダウンロードしてインストールできる使用可能なアプリケーション、アプリケーションのサイズ、適切なアクション (ダウンロード、インストール、または更新) を示します。パッケージにカーソルを合わせると、使用可能なバージョンと基本的な説明が表示されます。
- **[Installed Apps]** : 現在インストールされているアプリケーションパッケージが表示されます。

**重要** [Software Updates] ウィンドウを起動すると、接続のチェックが実行され、ステータスが表示されます。接続の問題がある場合、[Software Updates] ウィンドウには新しい更新が表示されません。

**ステップ 3** 次のいずれかの操作を実行して、アプリケーションをダウンロードします。

- すべてのアプリケーションを 1 度にダウンロードするには、[Application Updates] フィールドの上部にある [Download All] をクリックします。
- 特定のアプリケーショングループをダウンロードするには、グループの横にある [Download All] をクリックします。

**ステップ 4** 次のいずれかの操作を実行して、アプリケーションを更新します。

- すべてのアプリケーションを 1 度に更新するには、[Application Updates] フィールドの上部にある [Update All] をクリックします。
- 特定のアプリケーショングループを更新するには、グループの横にある [Update All] をクリックします。

**ステップ 5** [Installed Apps] タブで各アプリケーションのバージョンを調べ、それぞれが更新されていることを確認します。

アプリケーションのバージョンは、このタブで更新されます。

(注) 以前の Cisco DNA Center 構成に含まれていない新しいアプリケーションパッケージが存在する場合があります。このため、この手順ではそれらはインストールされていません (たとえば、このページに一覧表示されているテストサポートパッケージ)。

## パッケージのアンインストール

Cisco DNA 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、Cisco DNA 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。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

- 
- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Software Updates]。または、クラウドアイコンをクリックし、[Go to Software Updates] リンクをクリックします。
  - ステップ 2 インストール済みのアプリケーションを表示するには、[Installed Apps] タブをクリックします。
  - ステップ 3 削除するパッケージの [Uninstall] をクリックします。

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。

パッケージがアンインストールされると、[Installed Apps] タブから削除されます。

---





## 第 5 章

# ユーザの管理

---

- ユーザ プロファイルについて (81 ページ)
- ユーザ ロールの概要 (81 ページ)
- ローカルユーザの作成 (82 ページ)
- ローカルユーザの編集 (82 ページ)
- ローカルユーザの削除 (83 ページ)
- ローカルユーザパスワードのリセット (83 ページ)
- 自身のユーザパスワードの変更 (84 ページ)
- 思い出せないパスワードのリセット (84 ページ)
- ロールベース アクセス コントロールの設定 (85 ページ)
- ロールベース アクセス コントロール統計の表示 (91 ページ)
- 外部認証の設定 (91 ページ)
- Two-Factor Authentication (94 ページ)
- 外部ユーザの表示 (98 ページ)

## ユーザ プロファイルについて

ユーザプロファイルで、ユーザのログイン、パスワード、およびロール（権限）を定義します。

ユーザの内部プロファイルと外部プロファイルの両方を設定できます。内部ユーザプロファイルは Cisco DNA Center に配置され、外部ユーザプロファイルは外部 AAA サーバに配置されます。

Cisco DNA 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プロファイルが作成されます。

## ユーザ ロールの概要

実行できる機能を指定する次のユーザロールがユーザに割り当てられます。

- **管理者 (SUPER-ADMIN-ROLE)** : このロールを持つユーザは、Cisco DNA 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プロファイルを作成できます。
- **ネットワーク管理者 (NETWORK-ADMIN-ROLE)** : このロールを持つユーザは、Cisco DNA 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は、Cisco DNA 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は、Cisco DNA 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。

## ローカルユーザの作成

ユーザを作成し、このユーザにロールを割り当てることができます。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Users & Roles] > [User Management] の順に選択します。
  - ステップ 2** [Add] をクリックします。
  - ステップ 3** 新しいユーザの姓、名、ユーザ名を入力します。
  - ステップ 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。
  - ステップ 5** ロールのパスワードを入力し、確認のためにもう一度入力します。
  - ステップ 6** [保存 (Save) ] をクリックします。
- 

## ローカルユーザの編集

ユーザロールを変更できます (ユーザ名は変更できません)。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

- 
- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Users & Roles] > [User Management]** の順に選択します。
  - ステップ 2 編集するユーザの横にあるオプションボタンをクリックします。
  - ステップ 3 [Edit] をクリックします。
  - ステップ 4 [Role List] で、新しいロール ([SUPER-ADMIN-ROLE]、[NETWORK-ADMIN-ROLE]、または [OBSERVER-ROLE]) を選択します。
  - ステップ 5 [保存 (Save)] をクリックします。
- 

## ローカルユーザの削除

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

- 
- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Users & Roles] > [User Management]** の順に選択します。
  - ステップ 2 削除するユーザの横にあるオプションボタンをクリックします。
  - ステップ 3 [削除 (Delete)] をクリックします。
  - ステップ 4 確認のプロンプトで、[Continue] をクリックします。
- 

## ローカルユーザパスワードのリセット

別のユーザ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、どのユーザに対しても（管理者権限を持つユーザに対してさえも）、表示されません。

### 始める前に

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 ロールの概要 \(81 ページ\)](#) を参照してください。

- 
- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Users & Roles] > [User Management]** の順に選択します。
  - ステップ 2 パスワードをリセットするユーザの横にあるオプションボタンをクリックします。

ステップ3 [Reset Password] をクリックします。

ステップ4 パスワードを入力し、確認します。新しいパスワードは次の要件を満たす必要があります。

- 最低 8 文字。
- 次のうち少なくとも 3 つのカテゴリの文字を含むこと。
  - 小文字の英字
  - 大文字の英字
  - 番号 (Number)
  - 特殊文字

ステップ5 [保存 (Save) ] をクリックします。

---

## 自身のユーザパスワードの変更

---

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Users & Roles] > [Change Password] の順にクリックします。

ステップ2 必要なフィールドに情報を入力します。

ステップ3 [更新 (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

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。

---

ステップ1 システムでそのユーザ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)
```

ステップ2 パスワードをリセットするには、次のコマンドに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。

ステップ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。

**ステップ 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 Cisco DNA Center にログインできます。

## ロールベース アクセス コントロールの設定

Cisco DNA 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 権限を持つユーザは、特定の Cisco DNA Center 機能へのユーザ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を割り当てるには、次の手順を実行します。

### 始める前に

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。

**ステップ 1** カスタムロールを定義します。

- a) Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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。  
[Create a Role] ウィンドウが表示されます。これが RBAC の最初のイテレーションである場合、新しいロールを作成した後に、ユーザを新しいロールに割り当てるように求められます。
- c) [Let's Do it] をクリックします。

今後この画面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。

[Create a New Role] ウィンドウが表示されます。

- d) ロール名を入力し、[Next] をクリックします。  
[Define the Access] ウィンドウにオプションのリストが表示されます。デフォルトでは、Cisco DNA Center のすべての機能に対してオブザーバロールが設定されています。
- e) 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。  
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は該当する機能を GUI で表示できなくなります。
- g) [次へ (Next)] をクリックします。  
[Summary] ウィンドウが表示されます。
- h) サマリーを確認します。情報が正しい場合は、[Create Role] をクリックします。誤りがある場合は、[Edit] をクリックして適切な変更を行います。  
[Done, Role-Name] ウィンドウが表示されます。

**ステップ 2** 作成したカスタムロールにユーザを割り当てるには、[Add Users] をクリックします。

[User Management] > [Internal Users] ウィンドウが表示されます。このウィンドウでは、カスタムロールを既存のユーザまたは新規ユーザに割り当てることができます。

- 既存のユーザ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。
  1. [Internal Users] ウィンドウで、カスタムロールを割り当てるユーザの横にあ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。  
[Update Internal User] スライドインペインが表示されます。
  2. [Role List] ドロップダウンリストから、カスタムロールを選択し、[Save] をクリックします。
- カスタムロールを新規ユーザに割り当てるには、次の手順を実行します。
  1. [Add] をクリックします。  
[Create Internal User] スライドインペインが表示されます。
  2. 表示されるフィールドに氏名とユーザ名を入力します。
  3. [Role List] ドロップダウンリストから、新規ユーザに割り当てるカスタムロールを選択します。
  4. 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。
  5. [保存 (Save)] をクリックします。

**ステップ 3** 既存のユーザがログイン中に、管理者がそのユーザのアクセス権限を変更した場合、新しい権限設定を有効にするには、ユーザが Cisco DNA Center からログアウトして、ログインし直す必要があります。

## Cisco DNA Center ユーザ ロール権限

表 4: Cisco DNA Center ユーザ ロール権限

機能	説明
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。

機能	説明
モニタリングおよびトラブルシューティング	<p>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。</p> <p>このロールでは次のことが可能です。</p> <ul style="list-style-type: none"> <li>• 問題の解決、クローズ、無視。</li> <li>• 機械推論エンジン（MRE）のワークフローの実行。</li> <li>• トレンドとインサイトの分析。</li> <li>• 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。</li> </ul>
モニタリングの設定（Monitoring Settings）	<p>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。</p> <p>注：[Monitoring and Troubleshooting] に対する読み取り権限が最低限必要です。</p>
トラブルシューティング ツール	<p>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。</p> <p>注：[Monitoring and Troubleshooting] に対する読み取り権限が最低限必要です。</p>
ネットワーク設計	<p>ネットワーク階層の設定、ソフトウェアイメージリポジトリの更新、サイトやネットワークデバイスの管理に使用するネットワークプロファイルと設定の構成を行います。</p>
詳細ネットワーク設定（Advanced Network Settings）	<ul style="list-style-type: none"> <li>• グローバルデバイスログイン情報、認証サーバとポリシーサーバ、証明書、トラストプール、クラウドアクセスキー、Stealthwatch、Umbrella、データ匿名化などのネットワーク設定を更新します。</li> <li>• デバイスインベントリとそのクレデンシャルをエクスポートします。</li> </ul> <p>（注） このタスクを完了するには、[Network Settings] に対する読み取り権限が必要です。</p>
イメージリポジトリ	<p>ソフトウェアイメージを管理し、物理および仮想ネットワークエンティティのアップグレードと更新を促進します。</p>
ネットワーク階層	<p>サイト、ビルディング、フロア、およびエリアのネットワーク階層を地理的な場所に基づいて定義および作成します。このロールを持つユーザは、[System Settings] で CMX サーバを追加することもできます。</p>

機能	説明
ネットワーク プロファイル (Network Profiles)	ルーティング、エンタープライズNFV、スイッチング、およびワイヤレスのネットワークプロファイルを作成し、プロファイルをサイトに割り当てます。このロールには、テンプレートエディタ、タギング、モデル設定エディタ、および認証テンプレートが含まれます。  注：SSIDを作成するには、[Network Settings] に対する書き込み権限が必要です。
ネットワーク設定	AAA、NTP、DHCP、DNS、Syslog、SNMP、テレメトリなど、サイト全体の共通のネットワーク設定。このロールを持つユーザは、[System Settings] で SFTP サーバの追加とネットワーク再同期間隔の変更が可能です。  注：ワイヤレスプロファイルを作成するには、[Network Profiles] に対する書き込み権限が必要です。
仮想ネットワーク	仮想ネットワーク (VN) を管理します。トラフィックの分離やVN間通信の制御のために、物理ネットワークを複数の論理ネットワークにセグメント化します。
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、スケジュール、および管理を行います。
コンプライアンス	コンプライアンス プロビジョニングを管理します。
イメージの更新	デバイスのソフトウェアイメージを、完全なアップグレードライフサイクルの後にアップグレードします。
インベントリ管理	ネットワーク上のデバイスの検出、追加、置換、削除、およびデバイス属性と設定プロパティの管理を行います。  注：デバイスを置換するには、[Network Provision] > [PnP] に対する書き込み権限が必要です。
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一元管理します。
ネットワークテレメトリ	デバイスからのアプリケーションテレメトリの収集を有効または無効にします。割り当てられたサイトに関連付けられているテレメトリ設定を構成します。Wireless Service Assurance やコントローラ証明書など他の設定を構成します。  注：ネットワークテレメトリを有効または無効にするには、[Provision] に対する書き込み権限が必要です。
PnP	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、サイト固有のコンテキスト設定に基づいて設定します。



機能	説明
Provision	<p>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、ファブリック、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、Stealthwatch、および Umbrella プロビジョニングが含まれます。</p> <p>注：ネットワークプロファイルが関連付けられたサイトのデバイスをプロビジョニングするには、[Network Profiles] に対する読み取り権限が最低限必要です。</p>
スケジューラ	他のバックエンドサービスと統合されたスケジューラを使用して、ポリシーの展開、ネットワークデバイスのプロビジョニング、アップグレードなどのタスクをスケジュールできます。
ネットワーク サービス	ネットワークのサービスをプロビジョニングします。
アプリケーション ホスティング	ネットワーク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、およびモニタします。
Bonjour	ポリシーベースのサービス検出を有効にするために、ネットワーク全体で Wide-Area Bonjour サービスを有効にします。
Stealthwatch	<p>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。</p> <p>Stealthwatch をプロビジョニングするには、次のコンポーネントに対する書き込み権限が必要です。</p> <ul style="list-style-type: none"> <li>• [Network Design] &gt; [Network Settings]</li> <li>• [Network Provision] &gt; [Provision]</li> <li>• [Network Provision] &gt; [Scheduler]</li> <li>• [Network Services] &gt; [Stealthwatch]</li> </ul>
Umbrella	<p>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。</p> <p>Umbrella をプロビジョニングするには、次のコンポーネントに対する書き込み権限が必要です。</p> <ul style="list-style-type: none"> <li>• [Network Design] &gt; [Network Settings]</li> <li>• [Network Provision] &gt; [Provision]</li> <li>• [Network Provision] &gt; [Scheduler]</li> <li>• [Network Services] &gt; [Stealthwatch]</li> </ul> <p>また、[Advanced Network Settings] に対する読み取り権限も必要です。</p>

機能	説明
プラットフォーム	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。
API	Cisco DNA Center に REST API を使用してアクセスできます。
バンドル	生産性の向上のために、ITSM との統合用に事前設定されたバンドルを設定およびアクティブ化します。
イベント	ネットワークやシステムの関心があるイベントに登録することで、それらのイベントについての通知をほぼリアルタイムで受け取り、修正処置を開始できます。 電子メールおよび Syslog ログの設定は、 <b>[System Settings] &gt; [Destinations]</b> で設定できます。
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側面についてのレポートを生成できます。 ウェブフックは、 <b>[System Settings] &gt; [Destinations]</b> で設定できます。
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。
グループベース ポリシー	シスコのセキュリティグループタグに基づいて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。このロールには、エンドポイント分析が含まれます。
IP ベースのアクセス制御	IP アドレスに基づいて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。
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セキュリティアドバイザリを検索します。シスコが公開し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および把握できます。
システム	Cisco DNA Center の構成管理、ネットワーク接続、ソフトウェアアップグレードなどを一元管理します。
機械推論	セキュリティの脆弱性を迅速に特定して問題の自動分析を改善するために、機械推論ナレッジベースの自動更新を設定します。
システム管理	システムのコア機能と接続の設定を管理します。ユーザロールを管理し、外部認証を設定します。  このロールには、シスコのクレデンシャル、整合性検証、プロキシ設定、デバイスの EULA、HA、統合設定、ディザスタリカバリ、デバッグログ、テレメトリコレクション、システムの EULA、IPAM、vManage サーバ、バックアップと復元、およびデータプラットフォームが含まれます。
ユーティリティ	広く使用されているトラブルシューティングツールやサービスなど、生産性に役立つ情報がまとめられています。

機能	説明
監査ログ	UI または API インターフェイスを通じてネットワークデバイスや Cisco DNA Center に加えられた変更の詳細なログ。
ネットワーク推論機能	ネットワーク分野の専門家の知識に基づく、ネットワークの問題についての自動化された論理的なトラブルシューティングを開始します。
検索	サイト、ネットワークデバイス、クライアント、アプリケーション、ポリシー、設定、タグ、メニュー項目など、Cisco DNA Center のさまざまなオブジェクトを検索します。

## ロールベース アクセス コントロール 統計の表示

各ユーザロールに属しているユーザ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のリストを表示することもできます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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ロールとカスタムロールが表示されます。

**ステップ 2** 各ユーザ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のリストが表示されます。

## 外部認証の設定

外部ユーザの認証と許可に外部サーバを使用している場合、Cisco DNA Center で外部認証を有効にする必要があります。

始める前に

- 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 ロールの概要 \(81 ページ\)](#) を参照してください。
- 少なくとも 1 つの認証サーバを設定する必要があります。



(注) Cisco DNA Center のこのリリースでは、外部認証のフォールバック動作が変更されました。2.1.x 以前のリリースでは、外部認証が有効になっている場合、Cisco DNA Center は AAA サーバに到達できないか、AAA サーバが不明なユーザ名を拒否すると、ローカルユーザにフォールバックしていました。現在のリリースでは、AAA サーバに到達できない場合や AAA サーバが不明なユーザ名を拒否した場合に Cisco DNA Center がローカルユーザにフォールバックすることはありません。

外部認証フォールバックを有効にするには、Cisco DNA 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
```

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Users & Roles] > [External Authentication] の順に選択します。

**ステップ 2** Cisco DNA 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。

**ステップ 3** (任意) AAA 属性を設定します。

AAA サーバの Cisco DNA Center ユーザプロファイルを、[Cisco-AVPair] で AAA 属性として設定する限り、ほとんどの場合、デフォルト AAA 属性設定 (Cisco-AVPair) で十分です。Cisco DNA Center でデフォルトの設定を変更する必要があるのは、AAA サーバの Cisco DNA Center ユーザプロファイルで別の値が設定されている場合だけです。たとえば、AAA 属性を「Cisco-AVPair=Role=SUPER-ADMIN-ROLE」と手動で定義してもかまいません。

- a) [AAA Attribute] フィールドでは、[Cisco AVPair] をデフォルト値のままにしておくか、新しい AAA 属性値を入力します。
- b) [更新 (Update) ] をクリックします。

**ステップ 4** (任意) AAA サーバを設定します。

これらの設定は、現在のプライマリ AAA サーバとセカンダリ AAA サーバを交換したり、異なる AAA サーバを定義したりする場合にのみ行います。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [External Services] > [Authentication and Policy Servers] の順に選択して [Authentication and Policy Servers] ウィンドウを開きます。

- 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 サーバの IP アドレスを選択します。
- c) (任意) Cisco ISE サーバ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「Configure and Manage Policies」を参照してください。

表 5: Cisco ISEサーバの設定

名前	説明
共有秘密鍵 (Shared Secret)	デバイスの認証キー。共有秘密情報の長さは、最大 128 文字です。
Username	Cisco ISE CLI にログインするために使用する名前。
[Password]	Cisco ISE CLI ユーザ名のパスワード。
FQDN	Cisco ISE サーバ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 つの部分で構成されています。  <i>hostname.domainname.com</i>  たとえば Cisco ISE サーバの 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 Cisco DNA 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。
SSH キー (SSH Key)	Cisco ISE と接続し、認証するために使用される Diffie-Hellman-Group14-SHA1 SSH キー。
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) (任意) 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。

表 6: AAA サーバ詳細設定

名前	説明
Protocol	TACACS または RADIUS。
Authentication Port	AAA サーバへの認証メッセージのリレーに使用されるポート。  <ul style="list-style-type: none"> <li>• RADIUS の場合、デフォルトは UDP ポート 1812 です。</li> <li>• TACACS の場合、ポートは 49 であり、変更できません。</li> </ul>
Accounting Port	AAA サーバ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。  <ul style="list-style-type: none"> <li>• RADIUS の場合、デフォルトの UDP ポートは 1813 です。</li> <li>• TACACS の場合、ポートは 49 であり、変更できません。</li> </ul>

名前	説明
Retries	Cisco DNA Center が Cisco ISE との接続を試行できる回数。
Timeout	Cisco DNA 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) [更新 (Update) ] をクリックします。

## Two-Factor Authentication

二要素認証 (2FA) は、ユーザ名とパスワードに加えて識別子手法を使用することで、ユーザ認証のセキュリティを強化するものです。識別子手法は、一般に、実際の対象ユーザだけが所持し (スマホアプリやキーフォブなど)、元のログイン方法と意図的に異なるものを使用します。

Cisco DNA Center の二要素認証の実装では、トークンクライアント (適切な PIN が入力された後に使い捨てトークンコードを生成)、トークンサーバ (トークンコードを検証)、およびユーザのアクセスを管理する認証サーバを使用できます。認証処理には、RADIUS または TACACS+ プロトコルが使用されます。

このセクションでは、次の内容について説明します。

- 二要素認証を実装するために満たす必要がある要件。
- 必要な設定。
- 二要素認証を使用した Cisco DNA Center のログイン手順。

## 二要素認証の前提条件

Cisco DNA 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 Cisco DNA Center ユーザの RBAC ロール認可を伝達する属性値ペアを返すことのできる認証サーバ。この例では、Cisco Identity Services Engine (Cisco ISE) 2.3 パッチ 1 を使用しています。
- 認証サーバと統合する二要素トークンサーバ。この例では、RSA Authentication Manager 7.2 を使用しています。
- 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。

## 二要素認証のワークフロー

以下に、二要素認証が設定されている Cisco DNA Center アプライアンスにユーザがログインしたときの動作の概要を示します。

1. RSA SecurID トークンクライアントでは、ユーザは PIN を入力してトークンコードを取得します。
2. Cisco DNA Center ログインページでは、ユーザ名とトークンコードを入力します。
3. Cisco DNA 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、ユーザが正常に認証されたことを Cisco ISE に通知します。
6. Cisco ISE は認証されたユーザと設定済みの認可プロファイルを照合し、**role=NETWORK-ADMIN-ROLE** 属性値ペアを返します。
7. Cisco DNA Center ユーザのロールベース 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。

## 二要素認証の設定

Cisco DNA 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。

**ステップ 1** RSA Authentication Manager を Cisco ISE と統合します。

- a) RSA Authentication Manager で、2 つのユーザ、すなわち **cdnac\_admin** (管理者ユーザロール用) 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、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) 手順 1a で作成した `cdnac_admin` ユーザと `cdnac_observer` ユーザの 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。

**ステップ 2** 2つの許可プロファイルを作成します。1つは Admin ユーザロール用、もう1つは オブザーバユーザロール用です。

- 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] フィールド：プロファイルの名前を入力します。
- [Access Type] フィールド：[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。

**ステップ 3** Cisco DNA 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, Release 2.3](#)』の「Configure Authentication Policies」のトピックを参照してください。



**ステップ 4** 2つの許可ポリシーを作成します。1つは Admin ユーザロール用、もう1つは オブザーバユーザロール用です。

『[Cisco Identity Services Engine Administrator Guide, Release 2.3](#)』の「Configure Authorization Policies」のトピックを参照してください。

**ステップ 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 を使用した二要素認証の有効化

RADIUS 用に設定された Cisco ISE サーバ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。

**ステップ 1** Cisco ISE と Cisco DNA Center を連動させます。

『[Cisco DNA Center Installation Guide](#)』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。

**ステップ 2** 認証に Cisco ISE サーバを使用するよう Cisco DNA 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 Cisco DNA 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+ を使用した二要素認証の有効化

TACACS+ が設定された Cisco ISE サーバ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。

**ステップ 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。

**ステップ 2** [TACACS Authentication Settings] をクリックしてその内容を表示し、以前に追加した Cisco DNA 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。

**ステップ 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。

**ステップ 4** cdnac\_admin および cdnac\_observer ユーザロールの TACACS+ プロファイルを作成します。

- a) [Add] をクリックします。
- b) 次のタスクを実行します。

- 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。
  - cdnac\_admin ユーザロールの場合は、**Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE** と入力します。
  - cdnac\_observer ユーザロールの場合は、**Cisco-AVPair=ROLE=OBSERVER-ROLE** と入力します。

c) [保存 (Save) ] をクリックします。

ステップ 5 Cisco ISE と Cisco DNA Center を連動させます。

『[Cisco DNA Center Installation Guide](#)』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。

ステップ 6 認証に Cisco ISE サーバを使用するよう Cisco DNA 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 Cisco DNA 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ログイン

二要素認証を使用して Cisco DNA Center にログインするには、次の手順を実行します。

ステップ 1 Cisco DNA Center のログインページで、適切なユーザ名を入力します。

ステップ 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。

ステップ 3 このトークンをコピーして、Cisco DNA Center のログインページの [Password] フィールドに貼り付けます。

ステップ 4 [Log In] をクリックします。

---

## 外部ユーザの表示

RADIUS/TACACS を介して初めてログインした外部ユーザのリストを表示できます。表示される情報には、ユーザ名とロールが含まれます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Users & Roles] > [External Authentication] の順に選択します。

ステップ 2 ウィンドウの下部までスクロールします。[External Users] 領域に外部ユーザのリストが表示されます。



## 第 6 章

# ライセンスの管理

この章は、次の内容で構成されています。

- [ライセンスマネージャの概要 \(99 ページ\)](#)
- [Cisco スマート アカウントとの統合 \(103 ページ\)](#)
- [ライセンス マネージャのセット アップ \(103 ページ\)](#)
- [ライセンスの使用状況と有効期限の可視化 \(105 ページ\)](#)
- [ライセンス詳細の表示 \(105 ページ\)](#)
- [ライセンスレベルの変更 \(107 ページ\)](#)
- [ライセンス情報のエクスポート \(108 ページ\)](#)
- [コンプライアンスレポートのエクスポート \(108 ページ\)](#)
- [スマートライセンス対応デバイスの自動登録 \(109 ページ\)](#)
- [スマートライセンス対応デバイスのデゼロ設定 \(109 ページ\)](#)
- [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 \(110 ページ\)](#)
- [デバイスに適用された SLR または PLR をキャンセル \(112 ページ\)](#)

## ライセンスマネージャの概要

Cisco DNA 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。Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools]>[License Manager] の順に選択します。[License Manager] ページには、次の情報のタブが含まれています。

- [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] : すべてのルータのライセンスの購入情報と使用情報が表示されます。
- [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、ライセンスの購入情報と使用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。

- [All License] : すべてのシスコデバイスの全種類のライセンスに関する包括的な詳細情報が表示されます。

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。次の表では、各コントロールについて説明します。すべてのタブにすべてのコントロールが表示されるわけではありません。

表 7: ライセンス管理のコントロール

制御	説明
<b>Filter</b>	[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 <b>x</b> アイコンをクリックします。
<b>Change Cisco DNA License</b>	1 つ以上のライセンスを選択し、[Actions] > [Change Cisco DNA License] の順にクリックして、選択した Cisco DNA Center ライセンスのレベルを Essential または Advantage に変更します。このコントロールを使用して Cisco DNA Center ライセンスを削除することもできます。詳細については、 <a href="#">ライセンスレベルの変更 (107 ページ)</a> を参照してください。
<b>Change Virtual Account</b>	1 つ以上のライセンスを選択し、[Actions] > [Change Virtual Account] の順にクリックして、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対応デバイスを 1 つ以上選択し、[Actions] > [Manage Smart License] > [Register] の順にクリックして、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対応デバイスを 1 つ以上選択し、[Actions] > [Manage Smart License] > [Deregister] の順にクリックして、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) およびパーマネントライセンス予約 (PLR) を適用するデバイスを選択し、[Actions] > [Manage License Reservation] > [Enable License Reservation] の順にクリックします。
[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。 特定ライセンス予約 (SLR) を更新するデバイスを選択し、[Actions] > [Manage License Reservation] > [Update License Reservation] の順にクリックします。
[Manage License Reservation] > [Cancel/Return License Reservation]	デバイスを選択し、[Actions] > [Manage License Reservation] > [Cancel/Return License Reservation] の順にクリックして、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。

制御	説明
[ <b>Manage License Reservation</b> ] > [ <b>Factory License Reservation</b> ]	デバイスを選択し、[ <b>Actions</b> ] > [ <b>Manage License Reservation</b> ] > [ <b>Factory License Reservation</b> ] の順にクリックして、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。
<b>Recent Tasks</b>	[ <b>Recent Tasks</b> ] をクリックして、最近実行された 50 件すべての Cisco DNA Center タスクを表示します。リストの上部にあるドロップダウンを使用してリストを絞り込み、[ <b>Success</b> ] または [ <b>Failure</b> ] したタスク、またはまだ [ <b>In Progress</b> ] のタスクのみ表示します。
[ <b>更新 (Refresh)</b> ]	このコントロールをクリックして、ウィンドウを更新します。
[ <b>Export</b> ]	クリックして、表示されているライセンスのリストを CSV ファイルとしてエクスポートします。詳細については、 <a href="#">ライセンス情報のエクスポート (108 ページ)</a> を参照してください。
[ <b>検索 (Find)</b> ]	[ <b>Find</b> ] 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。
[ <b>エントリーを表示 (Show entries)</b> ]	テーブルの各ページに表示するエントリー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表示設定では非表示になっています。デフォルトの設定は、列ヘッダーの右端にある [More] アイコン (  ) をクリックすることでカスタマイズできます。

表 8: ライセンスの使用状況情報

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カブルスイッチ)。このリンクをクリックすると、ライセンスの詳細ウィンドウが開きます。詳細については、 <a href="#">ライセンス詳細の表示 (105 ページ)</a> を参照してください。
Device Type: Total Devices	Cisco DNA 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 Licenses	この製品シリーズのデバイスの購入済み Cisco DNA Center サブスクリプションライセンスの総数。

カラム	説明
Purchased Licenses: Network/Legacy	この製品シリーズのデバイスの購入済みネットワーク（またはレガシー）永久ライセンスの総数。
Used Licenses	この製品シリーズのデバイスに適用された Cisco DNA Center サブスクリプションライセンスの総数。
Used Licenses: Network/Legacy	この製品シリーズのデバイスのネットワーク永久ライセンスの総数。
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。

表 9: すべてのライセンス情報

カラム	説明
デバイス名 (Device Name)	デバイスの名前。このリンクをクリックすると、ライセンスの詳細ウィンドウが開きます。詳細については、 <a href="#">ライセンス詳細の表示 (105 ページ)</a> を参照してください。
デバイス ファミリ	Cisco DNA Center で定義されているデバイスのカテゴリ（スイッチやハブなど）。
IP Address	デバイスの IP アドレス。
デバイス シリーズ	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ابل スイッチ）。
Cisco DNA License	Cisco DNA Center のライセンスレベル。
Cisco DNA License Expiry	Cisco DNA Center ライセンスが期限切れになる日付。
License Mode	Cisco DNA Center のライセンスモード。
Network License	ネットワークライセンスの種類。
バーチャル アカウント	この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。
サイト	デバイスが設置されている Cisco DNA Center サイト。
登録ステータス	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 アドレス	ライセンスデバイスの MAC アドレス。
期間	Cisco DNA 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。

カラム	説明
Days to Expiry	Cisco DNA Center ライセンス期間が期限切れになるまでの残りの日数。
ソフトウェア バージョン	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 スマート アカウントとの統合

Cisco DNA Center は、簡素化された柔軟性のある自動ソフトウェア、組織全体のデバイス ライセンスの購入、展開、および管理を提供する Cisco スマート アカウント、オンラインのシスコ サービスをサポートしています。複数のシスコ スマート アカウントを追加できます。

複数のシスコ スマート アカウントがある場合、1 つのアカウントがデフォルトとして指定され、ライセンスマネージャで可視化およびライセンス操作（登録、ライセンスレベルの変更など）に使用します。

デフォルトのシスコ 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] および [All License] ウィンドウに表示するまでに数分かかります。

デフォルトアカウントを除くすべてのシスコ スマート アカウントを削除できます。

Cisco スマート アカウントをすでに保有している場合、Cisco DNA 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を追跡する
- 人が介入せずに、新しいライセンスを適用および有効にする
- 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、新たに変更された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、Cisco DNA Center を離れることなく自動的に実行できます。

## ライセンス マネージャのセット アップ

Cisco DNA 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。

### 始める前に

- この手順を実行するには、SUPER-ADMIN-ROLE 権限と、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 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：Cisco DNA 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 ID とパスワードを収集します。
- スマートアカウントを有効にするには、Cisco DNA Center が tools.cisco.com に到達できる必要があります。
- Cisco DNA 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、デバイスにサイトが割り当てられている必要があります。また、tools.cisco.com に到達できる必要があります。
- すべてのファイアウォールまたはプロキシで、『Cisco DNA Center 設置ガイド』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。

- 
- ステップ 1** Cisco DNA Center システム管理者のユーザ名とパスワードを使用してログインします。
- ステップ 2** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Cisco.com Credentials] の順に選択します。
- ステップ 3** [Cisco.com Credentials] に、cisco.com アカウントのユーザ名とパスワードを入力します。
- ステップ 4** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Smart Account] の順に選択します。
- ステップ 5** [Smart Account] で [Add] をクリックし、スマートアカウントのユーザ名とパスワードを入力します。
- ステップ 6** [保存 (Save) ] をクリックします。
- ステップ 7** 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。
- ステップ 8** スマートアカウントが複数ある場合は、デフォルトのアカウントを 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。
- ステップ 9** 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。
- ステップ 10** デフォルト以外の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。
- ステップ 11** 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、[スマートアカウントのリンク (Link Your Smart Account) ] 配下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。



**ステップ 12** [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 アカウントを表示します。

### 次のタスク

Cisco DNA 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 アカウントに登録します。これにより、Cisco Plug and Play Connect クラウドポータルから Cisco DNA Center のネットワーク プラグアンドプレイに、デバイスインベントリを同期することができます。詳細については、『Cisco DNA Center User Guide』の「Register or Edit a Virtual Account」を参照してください。

## ライセンスの使用状況と有効期限の可視化

Cisco DNA 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。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools] > [License Manager] の順に選択します。

**ステップ 2** ライセンスの使用状況を確認するデバイスカテゴリのタイプを選択します。タイプは [Switches]、[Routers]、[Wireless]、[ISE] または [All Licenses] のいずれかです。

ウィンドウの上部の [License Usage] 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。

グラフの下の [License Usage] テーブルには、使用されているライセンスと未使用の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。

**ステップ 3** 特定の製品ファミリーの詳細な比較を表示するには、テーブル内の [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。

Cisco DNA Center に、選択した製品ファミリーの詳細を示すウィンドウが表示されます。

**ステップ 4** ライセンス期間のグラフィカル表示を確認するには、ウィンドウの [License Timeline] セクションまでスクロールダウンします。各製品ファミリーのタイムライングラフは、その製品ファミリーに対して設定したスマートアカウントのライセンスが期限切れになるまでのビジュアル表示です。

## ライセンス詳細の表示

Cisco DNA Center でライセンス詳細を検索して表示するには、さまざまな方法があります。たとえば、[License Manager] ウィンドウの [Switches]、[Routers]、[Wireless]、[ISE]、または [All Licenses] タブに表示された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。これに


より、各製品ファミリのライセンスについての集約された情報を示すポップアップがそれぞれ表示されます。

1つのデバイスに関する最も包括的なライセンスの詳細を取得する最もシンプルな方法は、[License Manager]の[All Licenses]テーブルを使用することです。これについては次の手順で説明します。


**ステップ1** Cisco DNA Center GUIで[Menu]アイコン(☰)をクリックして[Tools]>[License Manager]>[All Licenses]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。テーブルの情報には、デバイスの種類やライセンスの有効期限など、基本的なデバイスおよびライセンスの情報のみが含まれます。

**ステップ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。必要なデバイスを見つけられない場合、次の操作を行います。


- [Filter] :  をクリックし、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すべてまたは一部を入力します）。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] :  をクリックし、テーブルに表示する列を選択します。たとえば、[Device Model]を選択解除、または[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。

**ステップ3** 必要なデバイスが見つかったら、そのデバイスの行の[Device Name]リンクをクリックします。

Cisco DNA Centerで[License Details]スライドインウィンドウが表示され、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表示されます。[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]ウィンドウを閉じます。

## ライセンスレベルの変更

デバイスライセンスの機能レベルを、アップグレードまたはダウングレードすることができます。これは、Cisco DNA Center (サブスクリプション) ライセンスで行うことができます。機能レベルの選択内容は、基本的な Essentials レベルか包括的な Advantage レベルのいずれかです (ネットワークライセンス変換は、Cisco Catalyst 9000 デバイスファミリの製品でのみ使用可能です。Cisco DNA Center ライセンスレベルが変更になると、ネットワークライセンス変換が暗黙のうちに処理されることに注意してください)。

デバイスのライセンスレベルを変更するたびに、Cisco DNA Center は、スマートアカウントを使用して、内部で自動的にライセンスをダウンロードして適用します。

ライセンスレベルの変更を適用するとデバイスのリポートが必要になるため、License Manager からユーザに、ライセンスレベルの変更が完了後すぐにデバイスをリポートするかどうかの確認があります。ライセンスの変更時にリポートしないように選択することもできますが、その場合は後でリポートをスケジュールする必要があります。リポートしなければ、ライセンスレベルの変更は適用されません。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[Tools] > [License Manager] > [All Licenses]** 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。

**ステップ 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 \(105 ページ\)](#) のヒントに従ってテーブルを変更し、必要なデバイスだけを表示します。

**ステップ 3** ライセンスレベルを変更する各デバイスの横にあるチェックボックスをオンにし、**[Actions] > [Change Cisco DNA License]** の順に選択します。

Cisco DNA Center は、変更するライセンスタイプにふさわしい [Change License Level] ウィンドウを表示します。

**ステップ 4** これらのデバイスに必要なライセンスレベル ([Essentials] または [Advantage]) をクリックします。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。

**ステップ 5** [Next] をクリックします。Cisco DNA Center が、変更をすぐに適用するか、後で適用をするかを確認します。また、ライセンスステータスの更新後すぐにデバイスをリポートするかどうかを選択する必要があります。

続行するには、次の操作を行います。

- 変更する準備ができていない場合は、[Back] をクリックしてライセンスレベルの選択を変更するか、 をクリックし、ウィンドウを閉じて変更をキャンセルします。
- すぐに変更する準備ができていない場合は、[Now] をクリックし、次に [Confirm] をクリックします。変更が適用されるとすぐに、このライセンスを使用するデバイスがリポートされます。

- 後で変更を適用する場合は、[Later] をクリックして、スケジュール済みのタスクの名前を入力し、変更を適用する日時を指定します。デバイスが設置されているサイトのタイムゾーンのスケジュールに従って変更を行う場合は、[Site Settings] をクリックします。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。

---

## ライセンス情報のエクスポート

ライセンス情報を Cisco DNA Center から迅速にエクスポートし、PDF または Microsoft Excel ファイルにバックアップできます。これらのライセンス バックアップ ファイルの目的は、組織のアカウントिंगとレポートのニーズを支援することです。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools] > [License Manager] の順に選択します。
  - ステップ 2** [All Licenses] をクリックします。Cisco DNA Center に、現在割り当てられているすべてのライセンスのリストが表示されます。
  - ステップ 3** [Export] をクリックします。Cisco DNA Center に、[Export Licenses] ウィンドウが表示されます。
  - ステップ 4** エクスポート先のファイル形式を選択します。
  - ステップ 5** (オプション) エクスポートに含めるか、またはエクスポートから除外するライセンス情報の各タイプの横にあるチェックボックスをオンにします。以降のエクスポートのデフォルトとして選択内容を保存する場合は、下部にあるチェックボックスをオンにします。
  - ステップ 6** [Export] をクリックして、エクスポートしたライセンスファイルの場所とファイル名を指定します。
  - ステップ 7** [OK] をクリックしてエクスポートを完了します。

---

## コンプライアンスレポートのエクスポート

準拠していないデバイスをすべて表示するレポートを生成してエクスポートできます。

- 
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools] > [License Manager] の順に選択します。
  - ステップ 2** [All Licenses] をクリックします。Cisco DNA Center に、現在割り当てられているすべてのライセンスのリストが表示されます。
  - ステップ 3** [Export Compliance Report] をクリックします。Cisco DNA Center に、[Export Non Compliant Devices] ウィンドウが表示されます。
  - ステップ 4** エクスポートするファイル形式を選択します。

- ステップ5** (オプション) エクスポートに含めるか、またはエクスポートから除外するライセンス情報の各タイプの横にあるチェックボックスをオンにします。以降のエクスポートのデフォルトとして選択内容を保存する場合は、下部にあるチェックボックスをオンにします。
- ステップ6** [Export] をクリックして、コンプライアンス違反レポートをダウンロードします。  
レポートには、各デバイスのコンプライアンス違反の理由を表示できます。

---

## スマートライセンス対応デバイスの自動登録

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、Cisco DNA Center に追加される SL が有効なデバイスは、選択したバーチャルアカウントに自動登録されます。

- 
- ステップ1** Cisco DNA Center システム管理者のユーザ名とパスワードを使用してログインします。
- ステップ2** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [Cisco Accounts] > [Cisco.com Credentials] の順に選択します。
- ステップ3** [License] をクリックします。
- ステップ4** [Auto register smart license enabled device] チェックボックスをオンにします。
- ステップ5** 仮想アカウントを選択します。
- ステップ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ゼロ設定

自動登録を有効にする前に Cisco DNA 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は、[All License] ページで確認できます。

- 
- ステップ1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools] > [License Manager] > [All License] 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] 列を使用して、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。
- ステップ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。
- ステップ3** 仮想アカウントを選択して [Continue] をクリックします。
- ステップ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。

## 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

スマートライセンスには、ライセンスのステータスの最新化とコンプライアンスの報告のために、Cisco Smart Software Management (CSSM) と定期的に同期するスマートデバイスのインスタンスが必要です。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。Cisco DNA 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 からライセンスを安全に保有できます。Cisco DNA Center では、ステージング環境での CSSM への一時的な接続が必要となります。次に、デバイスは SLR 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 Cisco DNA Center が CSSM に接続されている場合の SLR/PLR の有効化

### 始める前に

SLR/PLR を生成するデバイスと Cisco DNA Center の両方が CSSM に接続されていることを確認します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools] > [Licenses] > [All Licenses] の順に選択します。

- ステップ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。
- ステップ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。
- ステップ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。
- ステップ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。
- ステップ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。
- ステップ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] ページの [Reservation Status] の下に、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。

## デバイスと Cisco DNA Center が CSSM に接続されていない場合の CSV を使用した SLR/PLR の有効化

CSSM に接続されていないデバイスの SLR/PLR を有効にするには、次の手順を実行します。

- ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools]>[Licenses]>[All Licenses] の順に選択します。
- ステップ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。
- ステップ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。
- ステップ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。
- ステップ5 任意の場所にファイルを保存します。
- ステップ6 CSSM から各デバイスの認可コードを取得し、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。
- ステップ7 [Upload CSV] リンクをクリックします。
- ステップ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。
- ステップ9 [Continue] をクリックします。

**ステップ 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。SLR/PLR は、選択したデバイスに適用されます。

[All Licenses] ページの [Reservation Status] の下に、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 からの承認コードの生成

### 始める前に

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。

---

**ステップ 1** CSSM にログインします。

**ステップ 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。

**ステップ 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。

**ステップ 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。

**ステップ 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。

**ステップ 6** [Step 3: Review and Confirm] タブで [Generate Authorization Code] をクリックします。

**ステップ 7** [Step 4: Authorize Code] タブで承認コードを取得します。

---

## デバイスに適用された SLR または PLR をキャンセル

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。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [Tools] > [Licenses] > [All Licenses] の順に選択します。

**ステップ 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。

**ステップ 3** [Cancel] をクリックしてライセンスを返却します。

[All Licenses] ページの [Reservation Status] の下に、更新された最新のデバイスのステータスが表示されます。





## 第 7 章

# バックアップと復元

- [バックアップと復元について](#) (113 ページ)
- [バックアップサーバの要件](#) (114 ページ)
- [バックアップストレージ要件](#) (116 ページ)
- [NFS サーバの設定例：Ubuntu](#) (116 ページ)
- [NFS サーバの設定例：CentOS](#) (117 ページ)
- [NFS を許可するファイアウォールルールの設定](#) (118 ページ)
- [バックアップサーバの設定](#) (119 ページ)
- [今すぐデータをバックアップ](#) (121 ページ)
- [データのバックアップスケジュール](#) (122 ページ)
- [バックアップからデータを復元](#) (123 ページ)

## バックアップと復元について

バックアップおよび復元機能を使用して、別のアプライアンスに復元するためのバックアップファイルを作成できます（ネットワーク構成に必要な場合）。

### バックアップ

自動化データのみ、または自動化データとアシュアランスデータの両方をバックアップできます。

自動化データは、Cisco DNA 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。自動化バックアップは完全バックアップです。

アシュアランスデータは、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。アシュアランスデータの最初のバックアップは完全バックアップで、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しないでください。変更すると、バックアップファイルを Cisco DNA Center に復元できない場合があります。

Cisco DNA Center はバックアップファイルを作成して、リモートサーバにポストします。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。リモートサーバの要件の詳細については、[バックアップサーバの要件 \(114ページ\)](#) 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。

次の点を推奨します。

- 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。
- 設定に変更を加えた後はバックアップを実行する（デバイスで新しいポリシーを作成または変更した場合など）。
- 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。

## Restore

Cisco DNA Center を使用してリモートサーバ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、Cisco DNA 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、Cisco DNA Center は使用できません。

Cisco DNA Center のあるバージョンのバックアップを作成し、Cisco DNA Center の別のバージョンにそのバックアップを復元することはできません。バックアップは、バックアップが行われたアプライアンスおよびアプリケーションと同じ Cisco DNA Center ソフトウェアバージョン、アプリケーション、およびアプリケーションバージョンを実行しているアプライアンスにのみ復元できます。Cisco DNA Center の現在のアプリケーションとバージョンを表示するには、**[System] > [Software Updates]** を選択します。

バックアップは、別の IP アドレスを持つ Cisco DNA Center アプライアンスに復元することができます。この状況は、Cisco DNA 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。

# バックアップサーバの要件

バックアップサーバは、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。

- RedHat Enterprise（または CentOS）7 以上
- Ubuntu 16.04（または Mint など）以上

### 自動化データバックアップのサーバ要件

自動化データのバックアップをサポートするには、サーバが次の要件を満たしている必要があります。

- SSH (ポート 22) /リモート同期 (rsync) を使用している。Cisco DNA Center は、バックアップ実行時の FTP (ポート 21) の使用をサポートしていません。
- Linux rsync ユーティリティをインストールしている。
- バックアップユーザがバックアップのインストール先フォルダを所有しているか、ユーザグループの読み取り/書き込み権限がある。たとえば、バックアップユーザが「バックアップ」でユーザのグループが「スタッフ」の場合に、バックアップディレクトリに必要な権限を次のサンプル出力に示します。

- 例 1: バックアップディレクトリは「バックアップ」ユーザが所有している。

```
$ ls -l /srv/  
drwxr-xr-x 4 backup root 4096 Apr 10 15:57 acme
```

- 例 2: 「バックアップ」ユーザのグループに必要な権限が設定されている。

```
$ ls -l /srv/  
drwxrwxr-x. 7 root staff 4096 Jul 24 2017 acme
```

- SFTP サブシステムを有効にしている。次の行はアンコメントされていて、SSHD 設定に含まれている必要があります。

```
Subsystem sftp /usr/libexec/openssh/sftp-server
```

前述の行をアンコメントにする必要があるファイルは、通常は /etc/ssh/sshd\_config にあります。

### アシュアランスバックアップのサーバ要件

アシュアランスのデータバックアップをサポートするには、サーバが次の要件を満たす Linux ベースの NFS サーバである必要があります。

- 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。
- Cisco DNA Center と NFS サーバ間のネットワーク接続が安定している。
- Cisco DNA Center と NFS サーバ間のネットワーク速度が十分速い。



(注) NFS 搭載ディレクトリを Cisco DNA Center のバックアップサーバディレクトリ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。

## バックアップストレージ要件

Cisco DNA Center は、外部 NFS デバイスに アシユアランス データのバックアップコピーを保存し、外部リモート同期 (rsync) のターゲットの場所に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。

アプライアンス	NFS ストレージ (14 日単位で増分)	rsync ストレージ (日次のフル)
DN2-HW-APL	1.7 TB	50 GB
DN2-HW-APL-L	3 TB	100 GB
DN2-HW-APL-XL	8.4 TB	300 GB

補足事項：

- 上記の表は、各アプライアンスのアクセスポイントとネットワークデバイスの最大数をサポートする、フル装備のアプライアンス構成を前提としています。
- 一意のデータのみが NFS にバックアップされます。したがって、単一ノードと 3 ノードの HA 構成では、ほぼ同じサイズのバックアップが作成されます。
- NFS ストレージは、アシユアランス のデータバックアップに使用できる唯一の宛先タイプです。
- NFS バックアップは、最初の完全バックアップ後に増分されます。上記の表では、アシユアランスのデータバックアップを最初に実行した日に完全バックアップが生成されると想定しています。その後は毎日、増分バックアップが生成されます。
- rsync ストレージは、自動化データバックアップに使用できる唯一の宛先タイプです。
- rsync バックアップの量は、1 日 1 回のバックアップで見積もられます。バックアップを保持する日数を追加する場合は、必要なストレージ容量 x 追加する日数で算出します。たとえば、DN2-HW-APL アプライアンスがあり、1 日 1 回生成される自動化データバックアップのコピーを 5 つ保存する場合、必要なストレージの合計は 5 x 50 GB = 250 GB です。

## NFS サーバの設定例：Ubuntu

アシユアランス データベース (NDP) のバックアップをリモート共有するには、NFS 共有であることが必要です。NFS サーバを設定する必要がある場合は、次の手順 (Ubuntu ディストリビューション) を例として使用してください。

ステップ 1 `sudo apt-get update` コマンドを実行し、NFS サーバの Advanced Packaging Tool (APT) にアクセスして更新します。

たとえば、次のようにコマンドを入力します。

```
§ sudo apt-get update
```

**ステップ 2** `sudo apt-get install` コマンドを入力し、NFS の Advanced Packaging Tool をインストールします。

たとえば、次のようにコマンドを入力します。

```
§ sudo apt-get install -y nfs-kernel-server
```

**ステップ 3** `sudo mkdir -p` コマンドを入力し、NFS サーバのネスト化したディレクトリを作成します。

たとえば、次のようにコマンドを入力します。

```
§ sudo mkdir -p /var/nfsshare/
```

**ステップ 4** `sudo chown nobody:nogroup` コマンドを入力し、`nobody` および `nogroup` グループの所有権を変更します。

たとえば、次のようにコマンドを入力します。

```
§ sudo chown nobody:nogroup /var/nfsshare
```

**ステップ 5** `sudo vi /etc/exports` コマンドを入力し、`/etc/exports` の末尾に次の行を追加します。

```
§ sudo vi /etc/exports  
/var/nfsshare *(rw,all_squash,sync,no_subtree_check)
```

**ステップ 6** `sudo exportfs -a` コマンドを入力し、NFS サーバのファイルシステムをエクスポートします。

たとえば、次のようにコマンドを入力します。

```
§ sudo exportfs -a
```

**ステップ 7** `sudo systemctl start nfs-server` コマンドを入力し、NFS サーバを再起動します。

たとえば、次のようにコマンドを入力します。

```
§ sudo systemctl start nfs-server
```

---

## NFS サーバの設定例 : CentOS

次の手順は、CentOS での NFS サーバの設定例を示しています。

**ステップ 1** `sudo yum check-update` コマンドを入力して、NFS サーバの Yellowdog Updater Modified (YUM) にアクセスし更新します。

たとえば、次のようにコマンドを入力します。

```
§ sudo yum check-update
```

**ステップ 2** `sudo apt-get install` コマンドを入力し、NFS の Advanced Packaging Tool をインストールします。

たとえば、次のようにコマンドを入力します。

```
$ sudo yum install -y nfs-utils
```

ステップ3 NFS サーバを有効にして起動します。

```
$ sudo systemctl enable nfs-server
$ sudo systemctl start nfs-server
```

ステップ4 `sudo mkdir -p` コマンドを入力し、NFS サーバのネスト化したディレクトリを作成します。

たとえば、次のようにコマンドを入力します。

```
$ sudo mkdir -p <your_NFS_directory>
```

ステップ5 `sudo chown nfsnobody` コマンドを入力して、グループの所有権を変更します。

たとえば、次のようにコマンドを入力します。

```
$ sudo chown nfsnobody:nfsnobody /var/nfsshare
```

ステップ6 `sudo vi /etc/exports` コマンドを入力し、`/etc/exports` の末尾に次の行を追加します。

```
$ sudo vi /etc/exports
/var/nfsshare *(rw,all_squash,sync,no_subtree_check)
```

ステップ7 `sudo exportfs -a` コマンドを入力し、NFS サーバのファイルシステムをエクスポートします。

たとえば、次のようにコマンドを入力します。

```
$ sudo exportfs -a
```

ステップ8 `sudo systemctl start nfs-server` コマンドを入力し、NFS サーバを再起動します。

たとえば、次のようにコマンドを入力します。

```
$ sudo systemctl start nfs-server
```

---

## NFS を許可するファイアウォールルールの設定

デフォルトでは、Debian/Ubuntu ディストリビューションでファイアウォールが無効に、RedHat/CentOS ディストリビューションでは有効になっています。ファイアウォールが Debian/Ubuntu ディストリビューションで有効になっているかどうかを確認し、有効になっている場合は、ファイアウォールルールを追加します。

### ファイアウォールルールの設定 : Debian/Ubuntu

Debian/Ubuntu では、次の手順を実行します。

ステップ1 次のコマンドを入力して、ファイアウォールが有効か無効かを確認します。

```
$ sudo ufw status
```

ファイアウォールが無効の場合、出力には次のように表示されます。

```
Status: inactive
```

ファイアウォールが有効になっている場合は、次のように出力されます。

```
Status: active
```

**ステップ 2** ファイアウォールが有効になっている場合は、簡単なファイアウォールルールを作成できるように、`mountd` プロセスの静的ポートを設定します。`mountd`の静的ポートを設定するには、次の行を変更して `--port 32767` を `/etc/default/nfs-kernel-server` に追加します。

```
RPCMOUNTDOPTS="--manage-gids --port 32767"
```

**ステップ 3** 次のコマンドを入力して、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
```

---

## ファイアウォールルールの設定 : RedHat/CentOS

RedHat/CentOS の場合は、次の手順を実行します。

**ステップ 1** `mountd` ポートをサービスと `nfs.conf` に追加します。

(注) RedHat/CentOS ベースのディストリビューションでは、Debian ベースのディストリビューションとは異なるポートを `mountd` に使用します。RedHat/CentOS ディストリビューションは、`/etc/service` ファイルの `mountd` にポート **20048** を使用します。

次の行が存在しない場合は、`/etc/nfs.conf` に追加します。

```
[mountd]
manage-gids = 1
port = 20048
```

**ステップ 2** 次のコマンドを入力して、NFS のサービスおよびファイアウォールを再起動します。

```
sudo systemctl restart nfs-server rpcbind nfs-mountd
```

**ステップ 3** 次のコマンドを入力して、NFS を許可するファイアウォールルールを追加します。

```
sudo firewall-cmd --permanent --add-service={nfs, rpc-bind, mountd}
sudo firewall-cmd --reload
```

---

## バックアップサーバの設定

自動化のデータのみをバックアップする場合は、Cisco DNA Center Core System サーバを設定する必要があります。自動化とアシュアランスの両方のデータをバックアップする場合は、Cisco

DNA Center Core System バックアップサーバと NFS バックアップサーバを設定する必要があります。

この手順では、両方のサーバを設定する方法を示します。

### 始める前に

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。詳細については、[ユーザ ロールの概要 \(81 ページ\)](#) を参照してください。
- データのバックアップに使用する予定のサーバは、[バックアップサーバの要件 \(114 ページ\)](#) で説明されている要件を満たす必要があります。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Backup & Restore] > [Configure]** の順に選択します。

**ステップ 2** Core System バックアップサーバを設定するには、次の操作を行います。

a) 次の設定を定義します。

フィールド	説明
SSH IP Address	SSH が可能なリモートサーバの IP アドレス。
SSH ポート	SSH が可能なリモートサーバのポートアドレス。
サーバパス	バックアップファイルが保存されるサーバ上のフォルダへのパス。
Username	暗号化されたバックアップを保護するために使用するユーザ名。
[Password]	暗号化されたバックアップを保護するために使用するパスワード。
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。  これは入力が必要とされる必須のパスフレーズで、バックアップファイルを復元するときに入力する必要があります。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。

b) [Apply] をクリックします。

**ステップ 3** NFS バックアップサーバを設定するには、[NFS] タブをクリックし、次の設定を定義します。

フィールド	説明
ホスト	SSH が可能なリモートサーバの IP アドレスまたはホスト名。
サーバパス	バックアップファイルが保存されるサーバ上のフォルダへのパス。



ステップ4 [Apply] をクリックします。

## 今すぐデータをバックアップ

次のデータセットのいずれかをバックアップするように選択できます。

- 自動化データのみ。
- 自動化データと アシユアランス のデータ。

バックアップを実行する場合は、設定したリモートサーバ上の場所に Cisco DNA Center がデータをコピーしてエクスポートします。



(注) データは SSH/rsync を使用してバックアップされます。Cisco DNA Center は、バックアップ実行時の FTP (ポート 21) の使用をサポートしていません。

### 始める前に

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。詳細については、[ユーザ ロールの概要 \(81 ページ\)](#) を参照してください。
- バックアップサーバが [バックアップサーバの要件 \(114 ページ\)](#) 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が Cisco DNA Center で設定されている。詳細については、[バックアップサーバの設定 \(119 ページ\)](#) を参照してください。

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Backup & Restore] > [Backups] の順に選択します。

(注) まだバックアップサーバを設定していない場合、続行する前に、Cisco DNA Center がバックアップサーバの設定を要求します。[Configure Settings] をクリックします。[バックアップサーバの設定 \(119 ページ\)](#) を参照してください。

ステップ2 [Add] をクリックします。

[Create Backup] ペインが表示されます。

ステップ3 [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。

ステップ4 バックアップをすぐに実行するには、[Create now] をクリックします。

ステップ5 バックアップの範囲を定義します。

- 自動化および アシユアランス データをバックアップするには、[Cisco DNA Center (All data)] をクリックします。
- 自動化データのみをバックアップするには、[Cisco DNA Center (without Assurance data)] をクリックします。

**ステップ 6** [作成 (Create)] をクリックします。

- (注) 現在のバックアップステータスと以前のバックアップの履歴は、[Activity] タブで確認できます。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作成できます。正常に完了したバックアップジョブは、[Backup] タブで確認できます。

バックアッププロセス中は、Cisco DNA 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、リモートサーバの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。バックアッププロセスが完了すると、「Backup done!」通知を受信します。

- (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。Cisco DNA Center にバックアップの失敗の原因を示すエラーメッセージが表示されます。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。

---

## データのバックアップスケジュール

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ことができます。

### 始める前に

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。詳細については、[ユーザ ロールの概要 \(81 ページ\)](#) を参照してください。
- バックアップサーバが [バックアップサーバの要件 \(114 ページ\)](#) 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が Cisco DNA Center で設定されている。詳細については、[バックアップサーバの設定 \(119 ページ\)](#) を参照してください。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Backup & Restore] > [Schedule] の順に選択します。

[Schedule] ウィンドウが表示されます。

**ステップ2** [Add] をクリックします。

[Create Backup] ペインが表示されます。

**ステップ3** [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。

**ステップ4** [Schedule weekly] をクリックします。

**ステップ5** バックアップをスケジュールする日付と時刻を選択します。

**ステップ6** バックアップの範囲を定義します。

- 自動化およびアシュアランス データをバックアップするには、[Cisco DNA Center (All data)] をクリックします。
- 自動化データのみをバックアップするには、[Cisco DNA Center (without Assurance data)] をクリックします。

**ステップ7** [Schedule] をクリックします。

(注) スケジュール設定されたバックアップジョブは、[Schedule] タブで確認できます。バックアップが開始されたら、[Activity] タブでバックアップステータスを確認できます。

進行中のバックアップジョブがない場合のみ、新しいバックアップを作成できます。

正常に完了したバックアップジョブは、[Backup] タブで確認できます。

バックアッププロセス中は、Cisco DNA 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、リモートサーバの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。バックアッププロセスが完了すると、「Backup done!」通知を受信します。

(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。Cisco DNA Center にバックアップの失敗の原因を示すエラーメッセージが表示されます。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。

## バックアップからデータを復元

データをバックアップファイルから復元する際、Cisco DNA Center は既存のデータベースとファイルを削除し、バックアップのデータベースとファイルに置き換えます。復元されるデータは、バックアップの内容によって異なります。

- 自動化データバックアップ : Cisco DNA Center は完全な自動化データを復元します。
- 自動化とアシュアランス データのバックアップ : Cisco DNA Center は、選択した日付時点の完全な自動化データとアシュアランス データを復元します。



**注意** Cisco DNA 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。



- (注)
- Cisco DNA Center のあるバージョンをバックアップし、これを Cisco DNA Center の別のバージョンに復元することはできません。バックアップは、バックアップが行われたアプライアンスおよびアプリケーションと同じ Cisco DNA Center ソフトウェアバージョン、アプリケーション、およびアプリケーションバージョンを実行しているアプライアンスにのみ復元できます。現在のアプリケーションとバージョンを表示するには、**[System] > [Software Updates]** を選択します。
  - 複数のクラスタが同じ Cisco AI ネットワーク分析 の設定を共有し、同時にアクティブである場合、別の Cisco DNA Center クラスタの AI ネットワーク分析 設定を含むバックアップを復元すると、データの不整合やサービスの中断が発生する可能性があります。  
したがって、AI ネットワーク分析 の設定は単一のクラスタでアクティブにする必要があります。非アクティブなクラスタから AI ネットワーク分析 パッケージをアンインストールするには、**[System] > [Software Updates] > [Installed Apps] > [AI Network Analytics] > [Uninstall]** の順に選択します。

### 始める前に

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。詳細については、[ユーザ ロールの概要 \(81 ページ\)](#) を参照してください。
- 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、Cisco DNA 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。Cisco DNA 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。

(Cisco ISE または Cisco DNA Center 側で) バックアップから復元した場合、グループベースのアクセス コントロール ポリシー データは自動的に同期されません。ポリシー移行操作を手動で実行して、Cisco ISE と Cisco DNA Center が同期されていることを確認する必要があります。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Backup & Restore]** の順に選択します。

[Backup and Restore] ウィンドウには、[Backups]、[Schedule]、および [Activity] タブが表示されます。

リモートサーバにすでにバックアップが正常に作成されている場合、そのバックアップは[Backups]タブに表示されます。

**ステップ 2** [Backup Name] 列で、復元するバックアップを特定します。

**ステップ 3** [Actions] 列で、[Restore] を選択します。

Cisco DNA Center の復元プロセスで、データベースとファイルを復元します。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、作成された新しいネットワークポリシーや、新規または更新されたパスワード、新規または更新された証明書やトラストプールバンドルが含まれます。

復元中、バックアップファイルは現在のデータベースを削除して置き換えます。

復元プロセス中、Cisco DNA Center はメンテナンスモードになります。Cisco DNA Center がメンテナンスモードを終了するまで待つから、次に進んでください。

**ステップ 4** [Backups] タブをクリックすると、正常な復元の結果が表示されます。

---





## 第 8 章

# ディザスタリカバリの実装

- [概要 \(127 ページ\)](#)
- [前提条件 \(131 ページ\)](#)
- [監視サイトの設定 \(135 ページ\)](#)
- [ディザスタリカバリの設定 \(137 ページ\)](#)
- [フェールオーバー：概要 \(148 ページ\)](#)
- [ディザスタリカバリシステムの一時的停止 \(152 ページ\)](#)
- [システムへの再参加 \(154 ページ\)](#)
- [バックアップおよび復元の検討事項 \(157 ページ\)](#)
- [ディザスタリカバリイベントの通知 \(157 ページ\)](#)
- [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 \(158 ページ\)](#)

## 概要

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する Cisco DNA Center の高可用性 (HA) に基づいて構築されます。HA では、クラスタノードに障害が発生したときに、運用を接続されたクラスタノードに切り替えることで対処します。ディザスタリカバリでは、クラスタに障害が発生したときに、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。

Cisco DNA Center のディザスタリカバリの実装は、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、Cisco DNA 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。

実稼働環境でディザスタリカバリを設定して使用方法については、この章のトピックを参照してください。

## 主な用語

次に、Cisco DNA Center のディザスタリカバリの実装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設定 \(137ページ\)](#) 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。これにより、サイトで障害が発生した場合のスプリットブレイン状況を回避できます。この状況は、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。Cisco DNA 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 \(131ページ\)](#) 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設定 \(137ページ\)](#) 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Cisco DNA 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、Cisco DNA 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) 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：Cisco DNA Center では2種類のフェールオーバーがサポートされません。
  - システムトリガー：アクティブサイトがダウンしたことがわかった時点で、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Cisco DNA Centerで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のモニタリング](#)でモニタできます。
  - 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 \(148 ページ\)](#)を参照してください。
- 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。Cisco DNA 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Cisco DNA 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的停止 \(152 ページ\)](#)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。

## ディザスタリカバリの GUI のナビゲーション

次の表に、Cisco DNA 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	<p>[Monitoring] タブ：次の操作を実行する場合にクリックします。</p> <ul style="list-style-type: none"> <li>システムを構成するサイトのトポロジを表示します。</li> <li>システムの現在のステータスを確認します。</li> <li>ディザスタリカバリタスクを実行します。</li> <li>現在までに完了しているタスクのリストを表示します。</li> </ul>
2	<p>[Logical Topology]：サイトとそのメンバの現在のステータスを示すシステムのトポロジが表示されます。サイトの状態については、<a href="#">システムおよびサイトの状態（144 ページ）</a>を参照してください。</p>
3	<p>[Event Timeline]：システムのディザスタリカバリタスクについて、現在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、<a href="#">イベントタイムラインのモニタリング（142 ページ）</a>を参照してください。</p>
4	<p>[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、<a href="#">ディザスタリカバリの設定（137 ページ）</a>を参照してください。</p>
5	<p>[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、<a href="#">システムおよびサイトの状態（144 ページ）</a>を参照してください。</p>

引き出し線	説明
6	[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] ページの右下隅にある  をクリックします。
7	[Action] 領域 : 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。選択できるタスクは、サイトの設定が完了しているかどうかやシステムのステータスによって異なります。

## 前提条件

実稼働環境でディザスタリカバリを有効にする前に、次の前提条件を満たしていることを確認してください。



### 重要

最新の Cisco DNA Center 2.1.2.x リリース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。詳細については、「[アップグレード後のディザスタリカバリの設定 \(134ページ\)](#)」を参照してください。

### 一般的な前提条件

- ディザスタリカバリに、合計7台のノードで構成された3つのシステムを割り当てておきます。1つ目はメインサイトとして機能する3台のノードクラスタ、2つ目はリカバリサイトとして機能する3台のノードクラスタ、3つ目は監視サイトとして機能するシステム（仮想マシン上に常駐）となります。
- Cisco DNA 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。『[Cisco DNA Center Second-Generation Appliance Installation Guide](#)』で、次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 Browser-Based 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1GBリンクで、RTT遅延が200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
- サードパーティ証明書を生成し、メインサイトとリカバリサイトの両方にインストールしておきます。これがインストールされていないと、サイトの登録は失敗します。



(注) Cisco DNA 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。

それらのサイトで使用するすべての IP アドレスと完全修飾ドメイン名 (FQDN) が証明書に含まれていることを確認してください。サードパーティ証明書を生成する方法については、『Cisco DNA 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の前提条件

- メインサイトとリカバリサイトの両方について、同じ数のコアを持つ 3 つの Cisco DNA Center アプライアンスで構成する必要があります。つまり、1 つのサイトを 3 つの 56 コア第 2 世代アプライアンスで構成し、もう一方のサイトを 3 つの 112 コアアプライアンスで構成することはできません。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。

第 2 世代の Cisco DNA Center アプライアンス。Cisco UCS C220 M5 小型フォームファクタ (SFF) シャーシまたは Cisco UCS C480 M5 シャーシのいずれかをベースとします。	56 コアアプライアンス : シスコ製品番号 DN2-HW-APL-L
	56 コアプロモーションアプライアンス : シスコ製品番号 DN2-HW-APL-L-U
	112 コアアプライアンス : シスコ製品番号 DN2-HW-APL-XL
	112 コアプロモーションアプライアンス : DN2-HW-APL-XL-U

- 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『[Cisco DNA Center High Availability Guide](#)』を参照してください。
- 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、ネイバルータのローカル AS 番号です。
  - 64555 は、ネイバルータのリモート AS 番号です。
  - 10.30.197.57 はネイバルータの 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 Cisco DNA 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 DENYALL out
!
ip prefix-list deny-all seq 5 deny 0.0.0.0/0 le 32
!
route-map DENYALL 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 10 GB のハードドライブ領域を搭載した VMware ESXi ハイパーバイザーバージョン 6.0 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 サーバを設定しておきます。この NTP サーバをメインサイトとリカバリサイトで使用される NTP サーバと同期する必要があります。

## アップグレード後のディザスタリカバリの設定

システムを最新の Cisco DNA Center 2.1.2.x バージョンにアップグレードした後でディザスタリカバ리를正常に設定するには、状況に応じて次の手順を実行します。

### シナリオ 1

このシナリオでは、アプライアンスに最初にインストールされた Cisco DNA Center のバージョンは 1.3.x でしたが、最新の 2.1.2.x バージョンにアップグレードする必要があります。ディザスタリカバリは Cisco DNA Center 1.3.x からアップグレードされたアプライアンスでは正しく機能しないため、次の手順を実行してこの問題を回避する必要があります。

---

**ステップ 1** アプライアンスで、現在の Cisco DNA Center のバージョンから最新の 2.1.2.x バージョンにアップグレードします（『[Cisco DNA Center Upgrade Guide](#)』を参照）。

**ステップ 2** データをバックアップします（[今すぐデータをバックアップ（121 ページ）](#)を参照）。

次の手順でアプライアンスと仮想マシンのデータが完全に消去されるため、バックアップファイルがリモートサーバにあることを確認します。

**ステップ 3** アプライアンスに最新の Cisco DNA Center 2.1.2.x の ISO イメージをインストールします（『[Cisco DNA Center Second-Generation Appliance Installation Guide](#)』の「Reimage the Appliance」を参照）。

**ステップ 4** バックアップファイルからデータを復元します（[バックアップからデータを復元（123 ページ）](#)を参照）。

**ステップ 5** ディザスタリカバリシステムの設定に進みます。

---

### シナリオ 2

このシナリオでは、アプライアンスに最初にインストールされた Cisco DNA Center のバージョンは 2.1.x 以前でしたが、最新の 2.1.2.x バージョンにアップグレードする必要があります。また、これらのアプライアンスではディザスタリカバリが有効であり、動作可能です。次の手順を実行します。

---

**ステップ 1** システムの一時停止（[152 ページ](#)）。

**ステップ 2** メインサイトとリカバリサイトのアプライアンスを最新の 2.1.2.x バージョンにアップグレードします。『[Cisco DNA Center Upgrade Guide](#)』の「Upgrade to Cisco DNA Center 2.1.2.x」の章を参照してください。

**ステップ 3** 現在の監視サイトの置換（[141 ページ](#)）。

**ステップ 4** システムへの再参加（[154 ページ](#)）。

---

### シナリオ 3

このシナリオでは、アプライアンスに最初にインストールされた Cisco DNA Center のバージョンは 2.1.x 以前でしたが、最新の 2.1.2.x バージョンにアップグレードする必要があります。シ

ナリオ 2 とは異なり、これらのアプライアンスではディザスタリカバリが設定されていません。次の手順を実行します。

**ステップ 1** 監視サイトの設定 (135 ページ)。

**ステップ 2** ディザスタリカバリの設定 (137 ページ)。

## 監視サイトの設定

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。

**ステップ 1** 監視サイトで実行している Cisco DNA 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、Cisco DNA 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、Cisco DNA 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。

**ステップ 2** このパッケージを、VMware vSphere 6.0 または 6.5 を実行しているローカルマシンにコピーします。

**ステップ 3** vSphere クライアントで、[File] > [Deploy OVF Template] を選択します。

**ステップ 4** [Deploy OVF Template] ウィザードを完了します。

a) ウィザードの [Source] 画面で、次の手順を実行します。

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。

ウィザードの [OVF Template Details] 画面が開きます。

- b) **Next >** をクリックします。
- c) ウィザードの [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。

ウィザードの [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。  
ウィザードの [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。  
ウィザードの [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) ウィザードの [Network Mapping] 画面で、次の手順を実行してから [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。

ウィザードの [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表示されたら、[Close] をクリックします。

#### ステップ 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] ウィンドウが表示されます。

- b) 管理者ユーザ (*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 サーバの IP アドレス
- d) NTP サーバ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。

## ディザスタリカバリの設定

ディザスタリカバリシステムを使用するように設定するには、次の手順で説明するタスクを実行します。



(注) システムを設定する場合、いくつかのオプションがあります。

- ボーダー ゲートウェイ プロトコル (BGP) ルートアドバタイジングを使用する仮想 IP アドレスを指定できます。
- 仮想 IP アドレスを設定しないように選択することもできます。このオプションを選択した場合は、デバイスの可制御性を有効にして、フェールオーバー発生後にサイトの仮想 IP アドレスを再設定できるようにする必要があります。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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。

**ステップ 2** メインサイトを登録します。

(注) 手順 2d の前の任意の時点で、[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。メインサイトを登録する前に、手順 2 を繰り返して正しい設定を入力する必要があります。

- 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) [Setting up this cluster] 領域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。メインサイトのエンタープライズ仮想 IP アドレスをドロップダウンリストから選択します。

- [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。

c) [Additional Protocols] 領域に次の情報を入力します。

- [Routing Protocol] : 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かどうかを指定します。
- [Border Gateway Protocol Type] : [Border Gateway Protocol (BGP) ] オプションボタンをクリックした場合、BGP ピアが相互に外部 (外部 BGP (eBGP) ) セッションを確立するか、内部 (内部 BGP (iBGP) ) セッションを確立するかを指定します。
- [Enterprise VIP for Disaster Recovery] : 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)] オプションを選択した場合は、このフィールドに値を入力する必要があります。

- [Main Site Router Settings] : [Border Gateway Protocol (BGP)] オプションを選択した場合は、メインサイトのリモートルータの IP アドレスと、そのローカルおよびリモートの自律システム (AS) 番号を入力します。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。

(注) [iBGP] オプションを選択すると、Cisco DNA 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。

- [Recovery Site Router Settings] : [Border Gateway Protocol (BGP)] オプションを選択した場合は、リカバリサイトのリモートルータの IP アドレスと、そのローカルおよびリモートの AS 番号を入力します。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。

(注) [iBGP] オプションを選択すると、Cisco DNA 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。

- (オプション) [Management VIP for Disaster Recovery] : これはフローティング仮想 IP アドレスであり、設定しておけば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。

(注) 管理仮想 IP アドレスを設定し、[Border Gateway Protocol (BGP)] オプションを選択した場合は、適切なリモートルータ情報を入力する必要があります (エンタープライズ仮想 IP アドレスの場合と同様)。

- d) [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。
- e) [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。

**ステップ3** [Supplement] 領域で、[Copy Token] をクリックします。

**ステップ4** リカバリサイトを登録します。

- (注) 手順4dの前の任意の時点で、[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。  
リカバリサイトを登録する前に、手順4を繰り返して正しい設定を入力する必要があります。

- a) [Supplement] 領域で [Recovery Site] リンクを右クリックします。新しいブラウザタブでページが開きます。
- b) 必要に応じて、適切なユーザ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。

- (注) 手順2cで設定したエンタープライズVIPにブラウザから到達できない場合は、エンタープライズVIPをリカバリサイトの管理VIPに置き換えてURLを更新し、そのURLを開きます。

- c) 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。リカバリサイトのエンタープライズ仮想IPアドレスをドロップダウンリストから選択します。
  - 手順2で生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に対して設定されたユーザ名とパスワード。

- d) [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。
- e) [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。

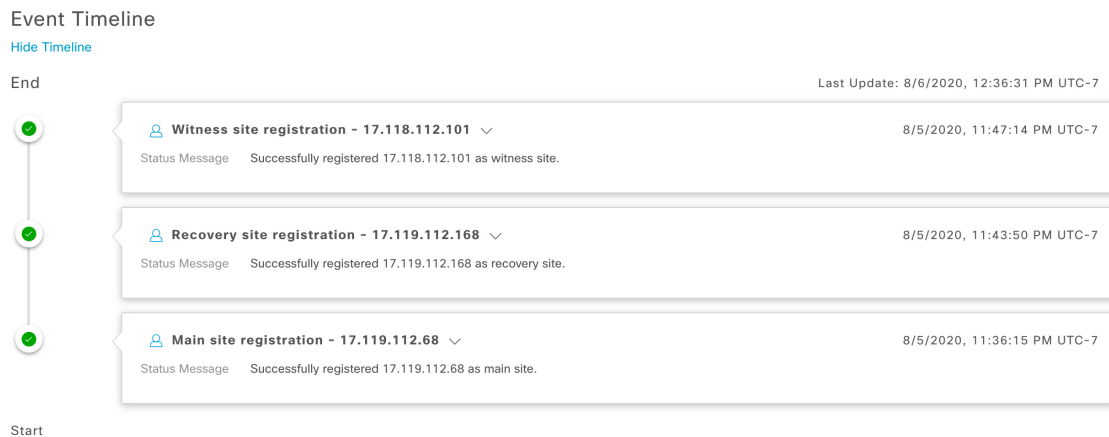
**ステップ5** 監視サイトを登録します。

- a) メインサイトのブラウザタブに戻ります。
- b) [Supplement] 領域で、[Copy Witness Login Cmmd] をクリックします。
- c) 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。
- d) 要求された場合は、デフォルトのユーザ (maglev) のパスワードを入力します。
- e) [Supplement] 領域に戻り、[Copy Witness Register Cmmd] をクリックします。

- f) SSH コンソールで、コピーしたコマンドを貼り付けます。
- g) <main\_admin\_user> をネットワーク管理者ユーザのユーザ名に置換してコマンドを実行します。
- h) 要求された場合は、ネットワーク管理者ユーザのパスワードを入力します。

**ステップ 6** 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。



**ステップ 7** [Actions] 領域で [Activate] をクリックします。

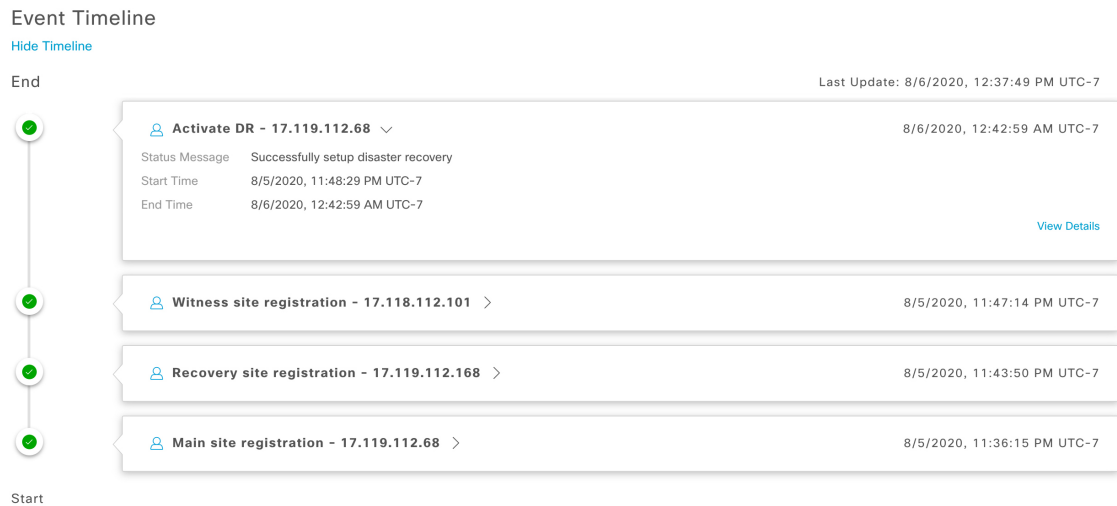
リカバリサイトに現在存在するすべてのデータが消去されることを示すダイアログが表示されます。

**ステップ 8** 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。

(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。進捗状況をモニタするには、イベントのタイムラインを表示します。

**ステップ 9** Cisco DNA 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。

1. 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。
  - メインサイト : [Active]
  - リカバリサイト : [Standby]
  - 監視サイト : [Up]
2. イベントのタイムラインを表示し、[Activate DR] タスクが正常に完了したことを確認します。



3. 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。

## 現在の監視サイトの置換

現在の監視サイトをアップグレードまたは置換する必要がある場合は、次の手順を実行します。

**ステップ 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 (maglev) のパスワードを入力します。

**ステップ 2** `witness reset` コマンドを実行します。

**ステップ 3** 現在の監視サイトの仮想マシンを削除します。

**ステップ 4** [監視サイトの設定 \(135 ページ\)](#) 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。

**ステップ 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 (maglev) のパスワードを入力します。

**ステップ 6** `witness reconnect` コマンドを実行します。

## システムの登録解除

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。この手順を実行すると、システム内のすべてのサイトについての現在の設定がクリアされることに注意してください。

**ステップ 1** [Action] 領域で、[Pause DR] 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（152 ページ）](#)」を参照してください。

**ステップ 2** [Action] 領域で、[Deregister] をクリックします。

Cisco DNA 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。

**ステップ 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設定（137 ページ）](#) で説明されているタスクを実行します。

## イベントタイムラインのモニタリング

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. Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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。Cisco DNA 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 (👤) のどちらによって開始されたかが示されます。

### Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:39:04 PM UTC-7

👤	Re-Join - 17.119.112.168 >	8/6/2020, 11:33:08 AM UTC-7
👤	Manual failover - 17.119.112.168 >	8/6/2020, 10:41:16 AM UTC-7
👤	Re-Join - 17.119.112.168 >	8/6/2020, 10:14:44 AM UTC-7
👤	Manual failover - 17.119.112.68 >	8/6/2020, 1:12:00 AM UTC-7

たとえば、システムの一部停止後の復元についてモニタするとします。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、Cisco DNA 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](#)

End

Last Update: 8/6/2020, 12:42:01 PM UTC-7

The screenshot shows an event timeline with two main entries. The first entry is 'Re-Join - 17.119.112.168' with a status message 'Successfully setup disaster recovery', start time '8/6/2020, 10:44:57 AM UTC-7', and end time '8/6/2020, 11:33:08 AM UTC-7'. A 'View Details' link is visible. The second entry is 'Manual failover - 17.119.112.168' with a start time of '8/6/2020, 10:41:16 AM UTC-7'.

タスクに対して [ViewDetails] リンクが表示されている場合は、そのリンクをクリックすると、完了した関連するサブタスクのリストが表示されます。

#### Event Timeline

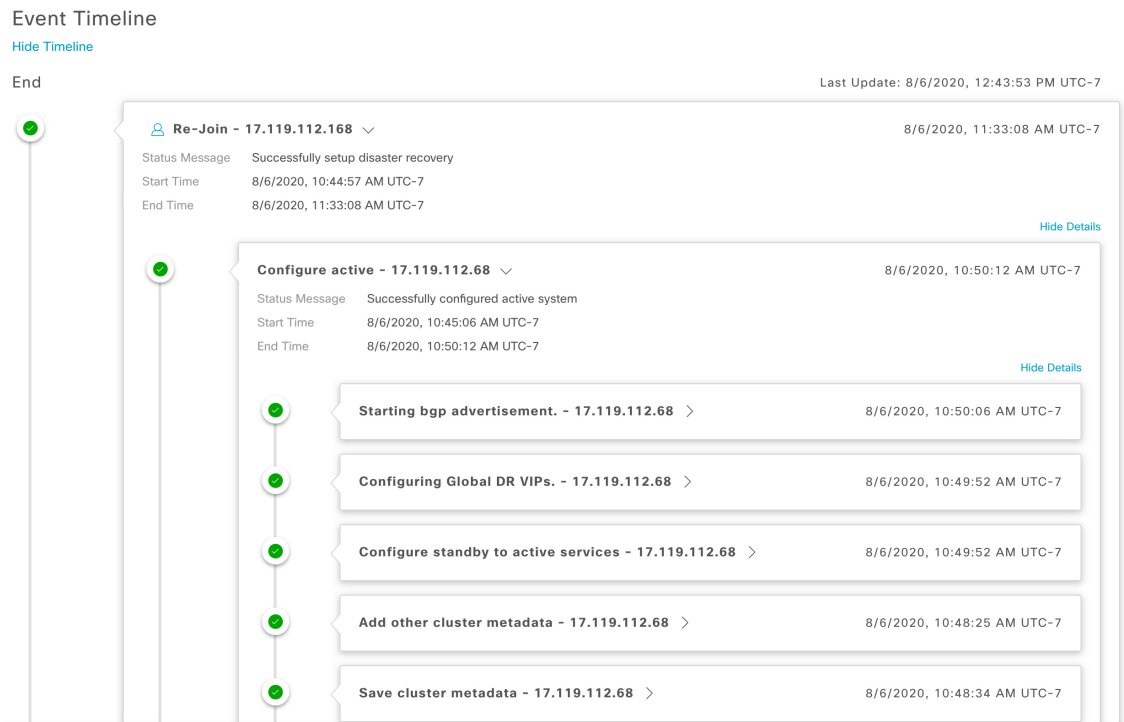
[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:42:39 PM UTC-7

This screenshot shows the 'Re-Join' task expanded to show its sub-tasks. The main task details are the same as in the previous screenshot. Below it, two sub-tasks are listed: 'Configure active - 17.119.112.68' (start: 8/6/2020, 10:50:12 AM UTC-7) and 'Configure standby - 17.119.112.168' (start: 8/6/2020, 11:33:05 AM UTC-7). The 'Manual failover' task is also visible at the bottom.

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。



## システムおよびサイトの状態

次の表に、[Status] 領域に表示されるシステムの状態とトポロジに表示されるサイトの状態について、それぞれの状態の意味を示します。

表 10: ディザスタリカバリシステムの状態

状態	説明
未構成	新規に導入されたシステムです。ディザスタリカバリはまだ設定されていません。
<b>Registered</b>	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登録され、登録に関するすべての検証チェックが正常に完了しました。3つのサイトの間で相互に通信できます。
の設定	この状態は、次のいずれかの状況を示しています。 <ul style="list-style-type: none"> <li>[Action] 領域で [Activate DR] をクリックしました。アクティブサイトとスタンバイサイトの両方で複数のワークフローが開始されます。これらのワークフローのいずれかが失敗した場合、このサイトは [Registered] 状態に戻ります。</li> <li>システムのアクティブサイトとスタンバイサイトを設定するために事前に実行するタスクが正常に完了しました。</li> </ul>



状態	説明
<b>Up</b>	この状態は、次のいずれかの状況を示しています。 <ul style="list-style-type: none"> <li>ディザスタリカバリが設定済みで、システムトリガーのフェールオーバーを開始できます。</li> <li>ディザスタリカバリが設定されています。ただし、監視サイトが設定されていないか停止しているため、システムトリガーのフェールオーバーを開始できません。</li> <li>スタンバイシステムが使用できず、データの複製が行われていません。</li> <li>システムトリガーまたは手動のフェールオーバーが正常に完了しました。</li> </ul>
<b>Up (with no Failover)</b>	システムは、次のいずれかの場合にこの状態になります。 <ul style="list-style-type: none"> <li>アクティブサイトおよびスタンバイサイトと監視サイトの接続が失われている。</li> <li>アクティブサイトおよび監視サイトとスタンバイサイトの接続が失われている。</li> </ul>
<b>Down</b>	アクティブサイトが停止したことが検出され、ディザスタリカバリシステムでフェールオーバーが開始されましたが、フェールオーバーに失敗しました。システムがこの状態の場合は、問題を解決してから手動フェールオーバーを開始します。
<b>Failover in progress</b>	アクティブサイトが停止したことが検出され、ディザスタリカバリシステムでフェールオーバーがトリガーされました。
<b>Deregistering</b>	登録解除が進行中です。このプロセスが完了すると、すべての登録情報と関連するネットワーク設定がリセットされます。
<b>Deregistered</b>	メインサイト、リカバリサイト、および監視サイトがディザスタリカバリシステムから登録解除されています。
<b>Pausing Disaster Recovery System</b>	メンテナンスなどのアクティビティのために、ディザスタリカバリシステムを一時停止しています。
<b>Disaster Recovery System Paused</b>	ディザスタリカバリシステムが一時停止されました。現在はメインサイトとリカバリサイトが2つのスタンドアロンクラスタとして機能しています。サイト間のデータの複製は行われていません。システムを再起動してデータの複製を再開するには、[Rejoin] をクリックします。
<b>Pausing Disaster Recovery Failed</b>	ディザスタリカバリシステムの一時停止中にエラーが発生しました。
<b>User intervention required</b>	メインサイトとリカバリサイトの両方がオフラインになり、再起動されました。ただし、ディザスタリカバリシステムは切断された状態のままになっています。システムを一時停止してから再起動し、問題が解決したかどうかを確認します。

表 11: Active Site States

状態	説明
未構成	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	このサイトがアクティブサイトとして指定されました。検証チェックと登録も正常に完了しています。
Configuring Active	サイトをアクティブサイトとして設定するためのワークフローを実行中です。
アクティブ	サイトをアクティブサイトまたはスタンバイサイトのいずれかとして設定するためのワークフローが正常に完了しました。
Failed to Configure	サイトをアクティブサイトとして設定するためのワークフローを完了できません。
アクティブ	このサイトがアクティブサイトとして正常に設定されました。
Isolating	このサイトをディザスタリカバリシステムから分離する処理を実行中です。これは、手動フェールオーバーを開始した後、それまでアクティブサイトとして機能していたサイトがオンラインに戻るとトリガーされます。
隔離 (Isolated)	このサイトがディザスタリカバリシステムから正常に分離されました。
Isolate Failed	このサイトをディザスタリカバリシステムから分離できません。
Down	自動ヘルスマニタで監視システムが停止していることが確認されたか、設定されている時間しきい値の間にシステムから正常性の更新情報が提供されませんでした。
Pausing Active	メンテナンスなどのアクティビティのために、アクティブサイトを一時停止しています。
Active Paused	アクティブサイトが一時停止されました。現在はアクティブサイトとスタンバイサイトが2つのスタンドアロンクラスタとして機能し、サイト間のデータの複製は行われていません。システムを再起動してデータの複製を再開するには、[Rejoin]をクリックします。
Pausing Active Failed	アクティブサイトの一時停止中にエラーが発生しました。

表 12: スタンバイサイトの状態

状態	説明
未構成	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	このサイトがスタンバイ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。
Configuring Standby	サイトをスタンバイサイトとして設定するためのワークフローを実行中です。

状態	説明
<b>Standby</b>	サイトをスタンバイサイトとして設定するためのワークフローが正常に完了しました。
<b>Failed to Configure</b>	サイトをスタンバイサイトとして設定するためのワークフローを完了できません。
パッシブ	このサイトがスタンバイサイトとして正常に設定されました。
<b>Activating passive</b>	システムトリガーまたは手動のフェールオーバーが進行中であることを示します。これにより、スタンバイサイトが新しいアクティブサイトに変換されます。
<b>Failover success</b>	システムトリガーまたは手動のフェールオーバーが正常に完了し、ディザスタリカバリシステムを運用可能な状態です。
<b>Failover failed</b>	システムトリガーまたは手動のフェールオーバーが正常に完了しませんでした。
<b>Standby ready</b>	前にアクティブサイトとして機能していたサイトを新しいスタンバイサイトとして設定する準備ができました。
<b>Down</b>	自動ヘルスマニタで監視システムが停止していることが確認されたか、設定されている時間しきい値の間にシステムから正常性の更新情報が提供されませんでした。
<b>Pausing Standby</b>	メンテナンスなどのアクティビティのために、スタンバイサイトを一時停止しています。
<b>Standby Paused</b>	スタンバイサイトが一時停止されました。現在はアクティブサイトとスタンバイサイトが2つのスタンドアロンクラスタとして機能し、サイト間のデータの複製は行われていません。システムを再起動してデータの複製を再開するには、[Rejoin] をクリックします。
<b>Pausing Standby Failed</b>	スタンバイサイトの一時停止中にエラーが発生しました。

表 13: 監視サイトの状態

状態	説明
未構成	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。
<b>Registered</b>	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。
<b>Up</b>	監視サイトの設定が正常に完了しました。
<b>Down</b>	自動ヘルスマニタで監視サイトが停止していることが確認されたか、設定されている時間しきい値の間に監視サイトから正常性の更新情報が提供されませんでした。
<b>Up and Replicating</b>	ディザスタリカバリシステムは稼働中です。複製が進行中です。
<b>Up (Manual failover)</b>	監視サイトから提供されるクォーラムなしでディザスタリカバリシステムが稼働しています。現在、システムトリガーのフェールオーバーは開始できません。

状態	説明
<b>Failover in progress</b>	フェールオーバーが進行中です。フェールオーバーが完了したら、新しいスタンバイサイトに問題がある場合は解決してから [Rejoin] をクリックします。
<b>Failover in progress (User initiated)</b>	手動で開始されたフェールオーバーが進行中です。現在は監視サイトに到達できません。
<b>Up (No failover)</b>	ディザスタリカバリシステムの設定とアクティブ化が完了しました。ただし、監視サイトに到達できないため、現在はフェールオーバーを開始できません。
<b>Down (User intervention required)</b>	フェールオーバーが正常に完了しませんでした。監視システムに到達できません。システムを一時停止してから再起動し、問題が解決したかどうかを確認します。

## フェールオーバー：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。Cisco DNA 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。Cisco DNA Center では、アクティブサイトが残りのエンタープライズネットワーク（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ため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 Cisco DNA 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 Cisco DNA 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。

## 手動フェールオーバーの開始

手動でフェールオーバーを開始する場合は、Cisco DNA 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。これは、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。

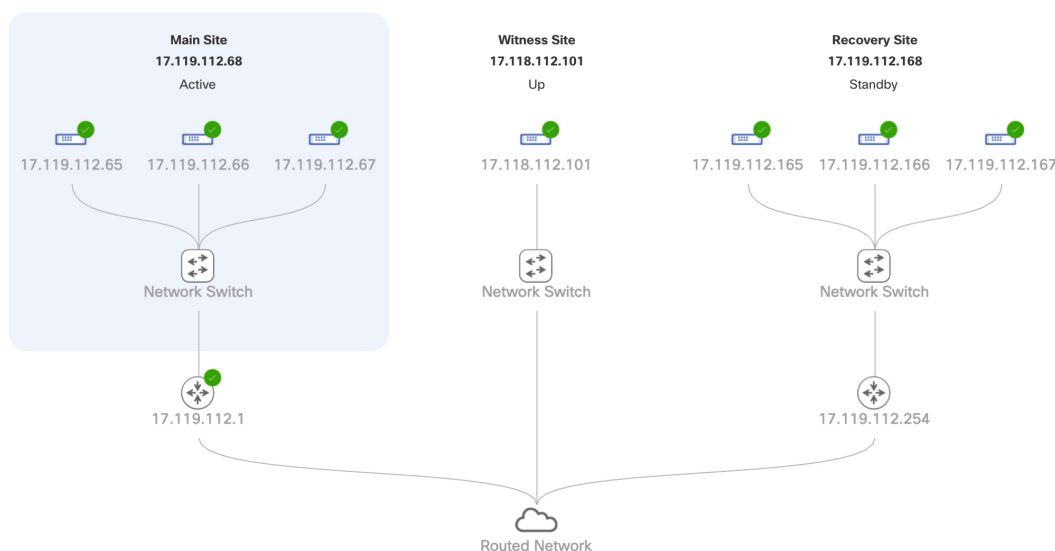


(注) 手動フェールオーバーは、監視サイトから開始することはできません。これは、現在アクティブなサイトからのみ実行できます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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、ユーザは現在のアクティブサイトにログインしています。

Logical Topology



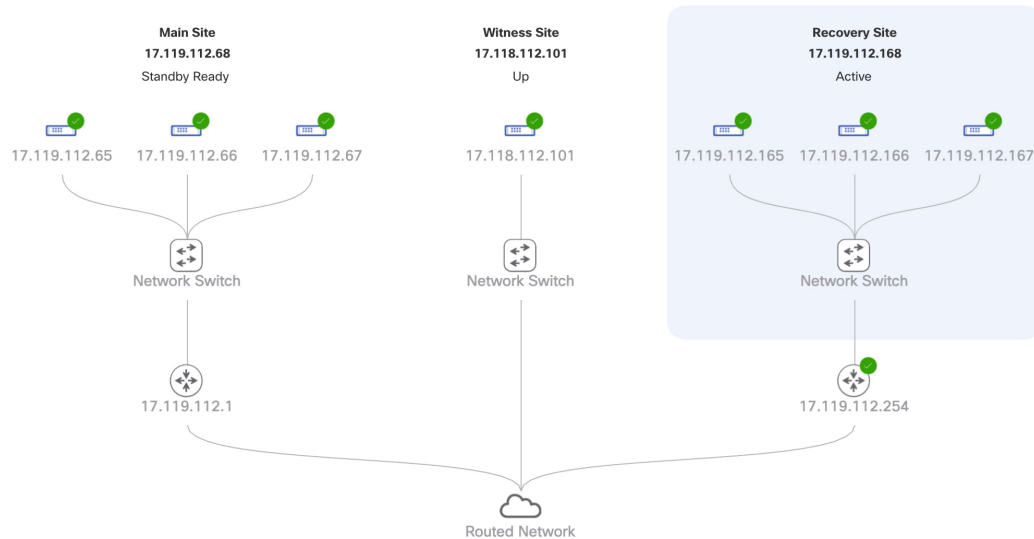
**ステップ 2** [Action] 領域で、[Manual Failover] をクリックします。

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。

**ステップ 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て [Standby Ready] 状態になります。

## Logical Topology



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。

**ステップ 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。

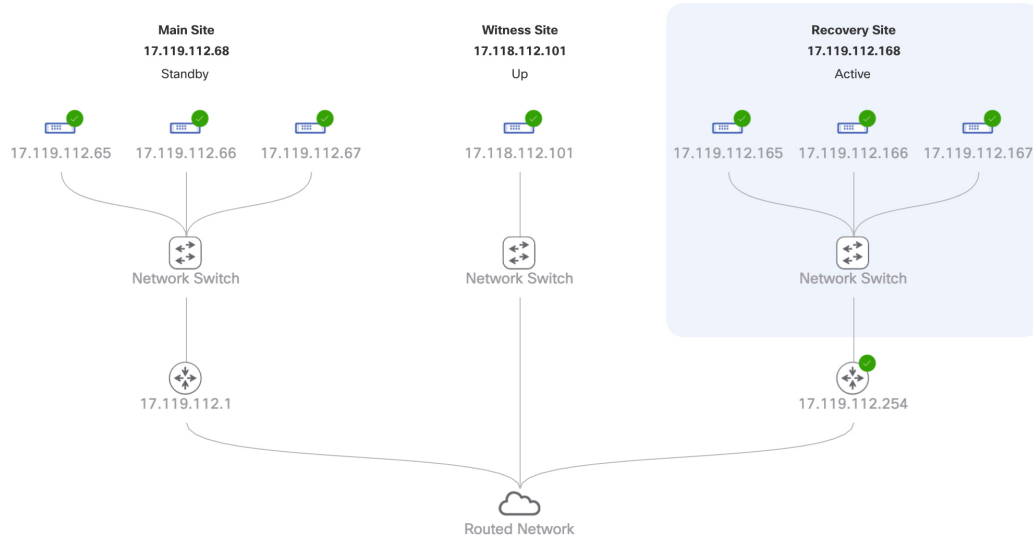
1. リカバリサイトにログインします。
2. [Action] 領域で、[Rejoin] をクリックします。

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。

**ステップ 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。

Cisco DNA 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。

## Logical Topology



**ステップ 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。

1. [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。
2. 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](#)

End

Last Update: 8/6/2020, 3:28:55 PM UTC-7

The Event Timeline shows the following tasks:

- Re-Join - 17.119.112.168** (8/6/2020, 3:27:11 PM UTC-7)
  - Status Message: Successfully setup disaster recovery
  - Start Time: 8/6/2020, 1:14:04 PM UTC-7
  - End Time: 8/6/2020, 3:27:11 PM UTC-7
- Configure active - 17.119.112.168** (8/6/2020, 1:21:34 PM UTC-7)
  - Status Message: Successfully configured active system
  - Start Time: 8/6/2020, 1:14:09 PM UTC-7
  - End Time: 8/6/2020, 1:21:34 PM UTC-7
- Configure standby - 17.119.112.68** (8/6/2020, 3:27:10 PM UTC-7)
  - Status Message: Successfully configured standby system
  - Start Time: 8/6/2020, 1:14:05 PM UTC-7
  - End Time: 8/6/2020, 3:27:10 PM UTC-7

# ディザスタリカバリシステムの一時停止

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、追加パッケージのインストールなどの管理タスクを実行する必要がある場合も、システムを一時停止します。ディザスタリカバリシステムを一時停止することで、Cisco DNA Center を計画的なネットワークの中断から保護したり、システムの設定を削除することなくディザスタリカバリを無効にしたりできます。

## システムの一時的停止

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。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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。

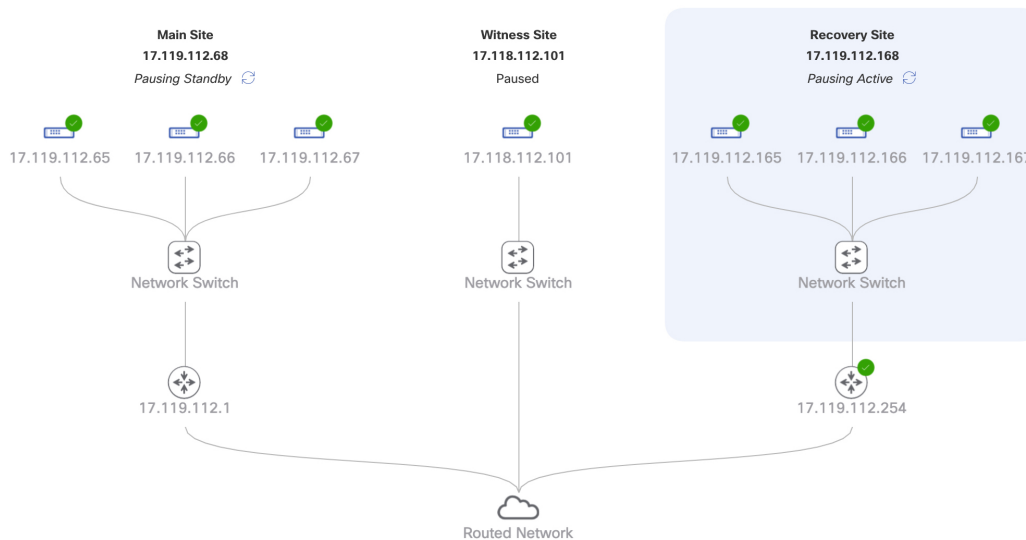
**ステップ 2** [Action] 領域で、[Pause DR] をクリックします。

**ステップ 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。システムを一時停止するために、Cisco DNA 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。

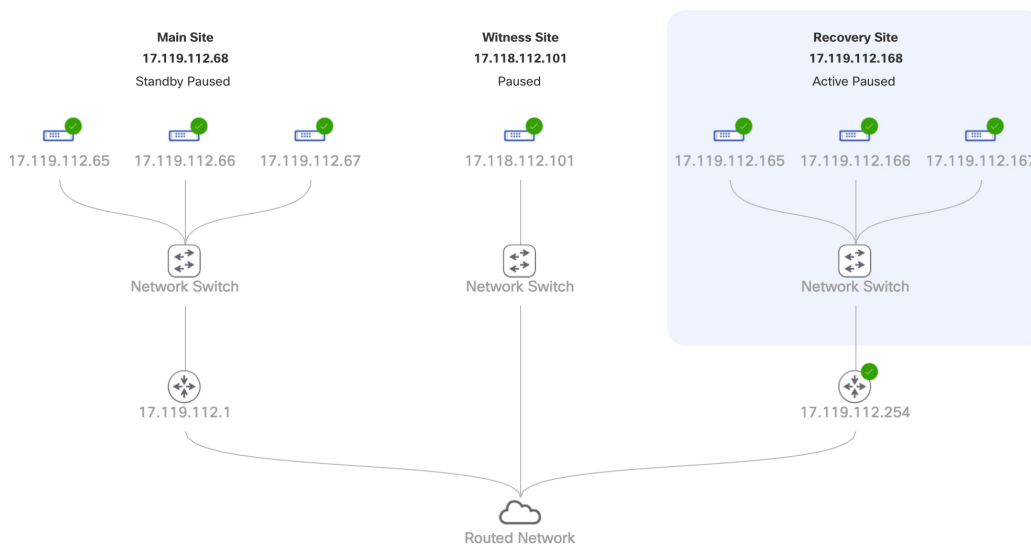


## Logical Topology



Cisco DNA 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。

## Logical Topology



**ステップ 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。

1. [Monitoring] タブの右上隅に表示されたステータスが [Disaster Recovery System Paused] になっていることを確認します。
2. イベントのタイムラインで、[Pause DR] タスクが正常に完了したことを確認します。

Event Timeline

[Hide Timeline](#)

End Last Update: 8/6/2020, 3:42:47 PM UTC-7

**Pause DR - 17.119.112.168** 8/6/2020, 3:41:04 PM UTC-7

Status Message: Successfully prepared clusters for pause DR.

Start Time: 8/6/2020, 3:30:15 PM UTC-7

End Time: 8/6/2020, 3:41:04 PM UTC-7

[Hide Details](#)

**Active cluster standalone - 17.119.112.168** 8/6/2020, 3:33:14 PM UTC-7

Status Message: Successfully prepared active cluster for pause DR.

Start Time: 8/6/2020, 3:30:17 PM UTC-7

End Time: 8/6/2020, 3:33:14 PM UTC-7

[View Details](#)

**Standby cluster standalone - 17.119.112.68** 8/6/2020, 3:40:59 PM UTC-7

Status Message: Successfully prepared standby cluster for pause DR.

Start Time: 8/6/2020, 3:30:21 PM UTC-7

End Time: 8/6/2020, 3:40:59 PM UTC-7

[View Details](#)

## 監視サイトのリリース 2.1.2.x へのアップグレード

Cisco DNA Center 2.1.2.x より前のバージョンを実行しているアプライアンスでディザスタリカバリを設定した場合は、次の手順を実行して最新の Cisco DNA Center 2.1.2.x バージョンにアップグレードした後、監視サイトが正しく動作することを確認する必要があります。

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Disaster Recovery]** の順に選択して [Disaster Recovery] ページを開きます。
- ステップ 2 [Action] 領域で、[Pause DR] をクリックします。
- ステップ 3 メインサイトとリカバリサイトのアプライアンスを最新の Cisco DNA Center 2.1.2.x バージョンにアップグレードします。『[Cisco DNA Center Upgrade Guide](#)』の「Upgrade to Cisco DNA Center 2.1.2.x」章にある最初のトピックを参照してください。
- ステップ 4 監視サイトの OVF パッケージをインストールします ([現在の監視サイトの置換 \(141 ページ\)](#) を参照)。
- ステップ 5 Cisco DNA Center の GUI で [Disaster Recovery] ページに戻り、[Action] 領域の [Rejoin] をクリックします。

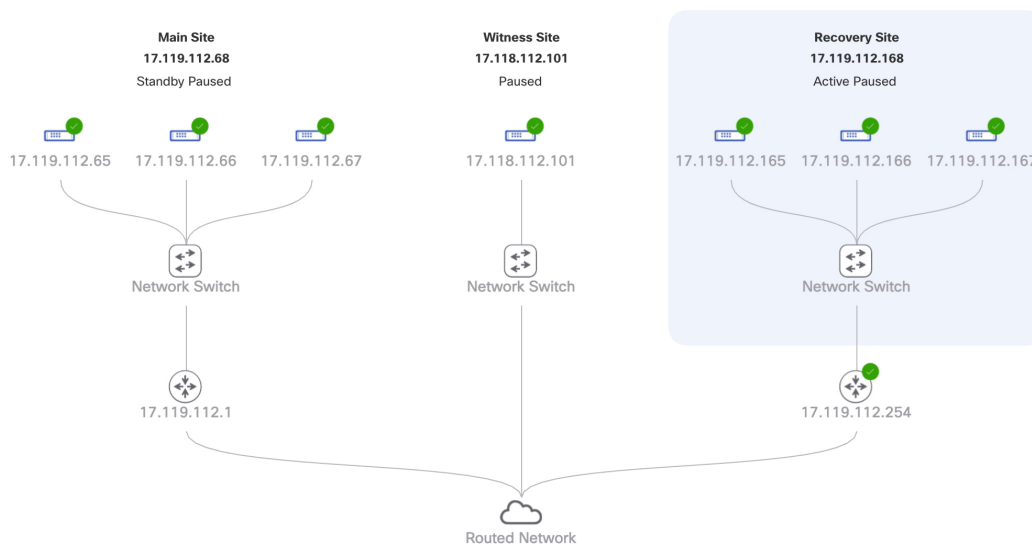
## システムへの再参加

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には、次の手順を実行します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [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。

Logical Topology



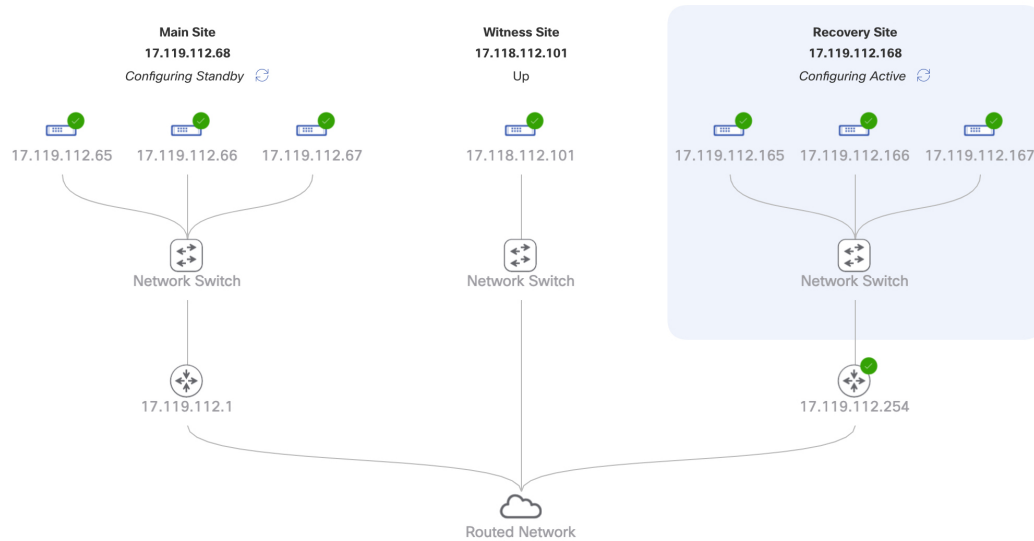
**ステップ 2** [Action] 領域で、[Rejoin] をクリックします。

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。

**ステップ 3** [Continue] をクリックして進みます。

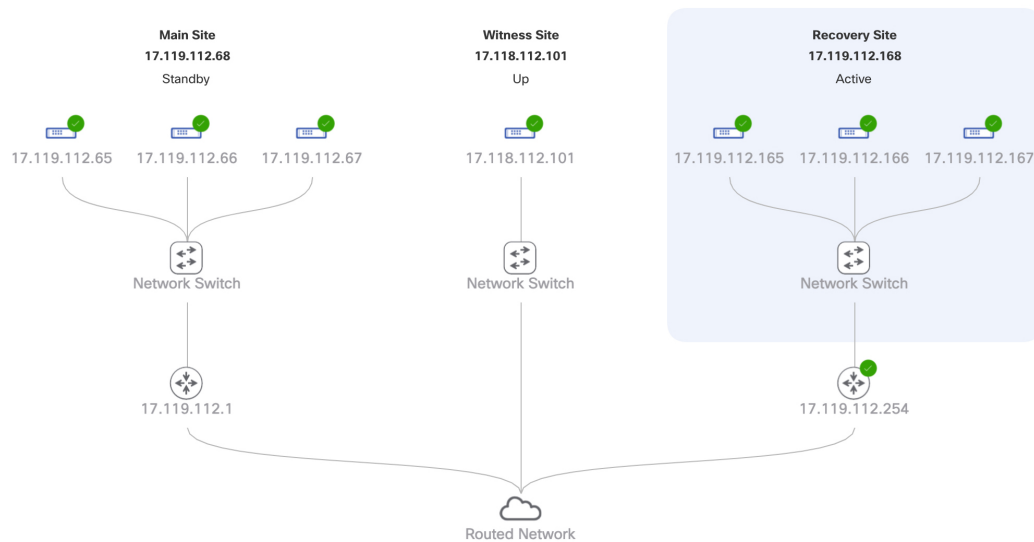
ページの右下隅に、メインサイト、リカバリサイト、および監視サイトを再接続するプロセスが開始されたことを示すメッセージが表示されます。このプロセスの実行中は、トポロジにおいて、メインサイトとリカバリサイトのステータスが [Configuring] に設定されます。

## Logical Topology



Cisco DNA 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。

## Logical Topology



**ステップ 4** [Monitoring] タブの右上隅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。

## バックアップおよび復元の検討事項

ディザスタリカバリシステムをバックアップおよび復元する際は、次の点に注意してください。

- 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 \(152 ページ\)](#)」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 \(154 ページ\)](#)」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 Cisco DNA 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。

ディザスタリカバリシステムのバックアップと復元の詳細については、[バックアップと復元 \(113 ページ\)](#) を参照してください。

## ディザスタリカバリイベントの通知

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 Cisco DNA 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 DNA Center Platform User Guide](#)』の「Work with Events」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]** 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。

サブスクライブ後、Cisco DNA 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。この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 \(152 ページ\)](#)。
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。Cisco DNA Center GUI で **[Menu]** アイコン (☰) をクリックして **[System] > [Settings] > [Trust & Privacy] > [System Certificate]** の順に選択します。
3. [システムへの再参加 \(154 ページ\)](#)。

## サポートされるイベント

次の表に、ディザスタリカバリイベントを示します。Cisco DNA 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
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
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

## 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

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。

表 14:ディザスタリカバリシステムの問題

エラーコード (Error Code)	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 <b>[Disaster Recovery]</b> > <b>[Configuration]</b> タブで、 <b>[Copy Token]</b> 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	クレデンシャルが無効である。	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。

エラーコード (Error Code)	メッセージ	ソリューション
SODR10076	High availability should be enabled on (main or recovery) site cluster.	次の手順を実行して、高可用性 (HA) を有効にします。 <ol style="list-style-type: none"> <li>1. HA を有効にする必要があるサイトにログインします。</li> <li>2. Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] &gt; [Settings] &gt; [System Configuration] &gt; [High Availability] の順に選択します。</li> <li>3. [Activate High Availability] をクリックします。</li> </ol>
SODR10100	(Main or recovery) site has no third party certificate.	Cisco DNA 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、「 <a href="#">Cisco DNA Center サーバ証明書の更新 (64 ページ)</a> 」を参照してください。
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、「 <a href="#">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 (166 ページ)</a> 」を参照してください。
SODR10122	Failed to stop BGP advertisement. Reason: ().	詳細については、「 <a href="#">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 (166 ページ)</a> 」を参照してください。



エラーコード (Error Code)	メッセージ	ソリューション
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。サポートについては、Cisco TAC にお問い合わせください。
SODR10124	Cannot ping VIP: (main, recovery, or witness site's VIP or IP address).	次の手順を実行します。 <ul style="list-style-type: none"> <li>指定したアドレスが正しいことを確認します。</li> <li>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。</li> </ul>
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. 操作をやり直します。 ()	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に依存します。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。 <p>このエラーは、1つまたは複数のサイトに設定されたIPアドレス/仮想IPアドレスが、通信にエンタープライズインターフェイス以外のインターフェイスを使用していることを示します。</p>

エラーコード (Error Code)	メッセージ	ソリューション
SODR10134	The disaster recovery management VIP (VIP address) and the IPs (IP addresses) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration.	ディザスタリカバリシステムの管理仮想IPアドレスは、管理インターフェイスで設定する必要があります。このエラーは、管理クラスタの仮想IPアドレスが設定されていないインターフェイスで仮想IPアドレスが現在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] > [Trust & Privacy] > [System Certificate] 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.	—
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。

エラーコード (Error Code)	メッセージ	ソリューション
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。Cisco DNA 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、Cisco DNA 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 (Error Code)	メッセージ	ソリューション
—	External postgres services does not exists to check service endpoints.	<p>次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. エラーが発生したサイトにログインします。</li> <li>2. 次のコマンドを実行します。 <ul style="list-style-type: none"> <li>• <b>Kubectl get sep -A</b></li> <li>• <b>kubectl get svc -A   grep external</b></li> </ul> </li> <li>3. 結果の出力で、external-postgres を検索します。</li> <li>4. 存在する場合は、<b>kubectl delete sep external-postgres -n fusion</b> コマンドを実行します。</li> <li>5. 以前に失敗した操作を再試行します。</li> </ol>
—	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 (Error Code)	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.	<p>スタンバイサイトがダウンしたときに、そのサイトを Cisco DNA 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。</p> <p>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。</p> <ol style="list-style-type: none"> <li>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。</li> <li>2. <b>maglev maintenance disable</b> 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。</li> <li>3. Cisco DNA Center にログインします。</li> <li>4. GUI で [Menu] アイコン (☰) をクリックし、<b>[System] &gt; [Disaster Recovery]</b> 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。</li> <li>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 <b>[Rejoin]</b> をクリックします。</li> </ol>

エラーコード (Error Code)	メッセージ	ソリューション
—	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。 <ul style="list-style-type: none"> <li>• <b>kubectl get svc --all-namespaces   grep mongodb</b></li> <li>• <b>magctl service unexpose mongodb &lt;port-number&gt;</b></li> </ul>
—	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。 <ul style="list-style-type: none"> <li>• <b>kubectl get svc --all-namespaces   grep postgres</b></li> <li>• <b>magctl service unexpose postgres &lt;port-number&gt;</b></li> </ul>

## 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

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ティングします。

**ステップ 1** Cisco DNA Center クラスタから、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かどうかを確認します ([Activate DR] > [View Details] > [Configure active] 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ータが稼働しているかどうかを確認する。
2. ネイバルータと Cisco DNA Center の接続があるかどうかを確認する。接続がない場合は、接続を復元してから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) Cisco DNA 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、Cisco DNA Center クラスタが 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。設定されていない場合は、クラスタをネイバーとして設定し、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て再試行します。

- c) 次のコマンドを実行して、Cisco DNA Center とそのネイバルータ間の BGP セッションのステータスを確認します。

```
etcdctl get /maglev/config/network_advertisement/bgp/address1_address2 | jq
```

引数の説明

- *address1* は Cisco DNA Center クラスタの仮想 IP アドレスです。
- *address2* は、ネイバルータの IP アドレスです。

[Established] が [state] フィールドにリストされている場合は、セッションがアクティブであり、正しく機能していることを示します。

- d) 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。

- e) 次のコマンドを実行して、Cisco DNA Center とそのネイバルータ間の 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'**

コマンド出力で、ネイバルータの 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。

**ステップ 2** エラーメッセージに示されているネイバルータから、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、Cisco DNA Center クラスタの仮想 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、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、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、アドバタイズされていることを確認します。

