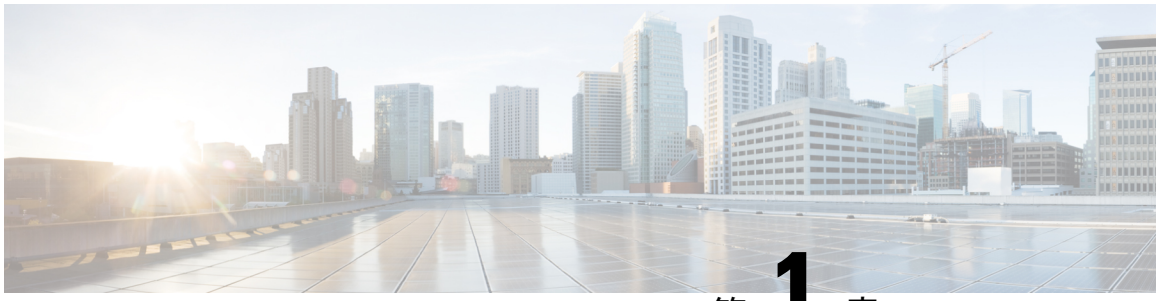
Cisco DNA Center リリース 2.3.5 管理者ガイド

初版：2022 年 12 月 21 日

最終更新：2023 年 3 月 3 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/

目 次



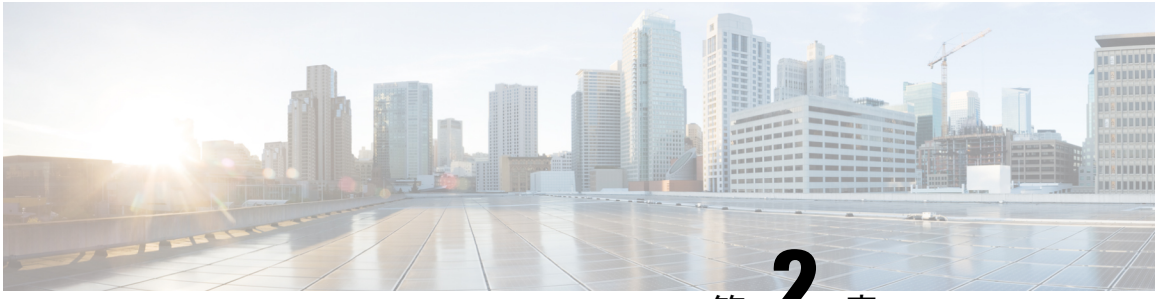
第 1 章

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 *2.3.5* の新機能および機能変更

機能	説明
AppX MS-Teams のアクティブ化または非アクティブ化	Cisco DNA Center または Cisco DNA - Cloud から AppX MS-Teams 統合をアクティブ化または非アクティブ化できるようになりました。 AppX MS-Teams 統合の構成 （76 ページ）およびCisco DNA - Cloud を使用した AppX MS-Teams 統合の構成 （78 ページ）を参照してください。



第 2 章

システム設定の構成

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、サーバー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ー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）
- プロキシサーバー設定の変更など、Cisco DNA Center の構成を変更する場合、すべて 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 サーバー、または **maglev** ユーザーパスワードの変更は、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。

ユーザープロファイルの役割および権限

Cisco DNA Center は、ロールベース アクセス コントロール（RBAC）をサポートします。ユーザープロファイルに割り当てられたロールは、ユーザーが実行する権限を持つ機能を定義します。Cisco DNA Center には、次の 3 つの主要なデフォルトユーザーロールがあります。

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

SUPER-ADMIN-ROLE は、ユーザーに幅広い機能を提供し、カスタムロールの作成やユーザープロファイルへの割り当てなど、Cisco DNA Center GUI ですべてのアクションを実行できるようにします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE は、Cisco DNA Center GUI での機能が制限されます。

Cisco DNA Center でアクションを実行できない場合、それを許可しないロールがユーザープロファイルに割り当てられていることが原因である可能性があります。詳細については、システム管理者に確認するか、またはロールベースアクセスコントロールの設定（125 ページ）を参照してください。

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

をトラブルシューティングすることができます。Kibana の詳細については、https://www.elastic.co/products/kibana を参照してください。

- [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 サーバーの IP アドレスとステータスを含む Cisco ISE 設定データを表示します。Cisco ISE と統合するように 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ーリングデータとログを表示できます。

ステップ 1 メニューアイコン（☰）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] ウィンドウで、[Service Explorer] タブをクリックします。

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、シリアル番号、製品 ID、インターフェイスなどの詳細が表示されます。
- サービステーブルには、ノードに関連付けられているすべてのサービスが表示されます。マネージドサービスは「（M）」というマークで示されます。

- グローバルフィルタアイコンをクリックすると、サービステーブルのサービスをアプリケーションスタック名、サービス正常性ステータス（[Up]、[Down]、または [In Progress]）、またはマネージドサービスかどうかに基づいてフィルタ処理できます。
- [Global Search] フィールドにサービス名を入力してサービスを検索できます。サービス名をクリックすると、関連付けられているノードでサービスが表示されます。

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。

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

[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ーし、発生する可能性がある問題を監視できます。この機能を有効にして実稼働環境で使用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。

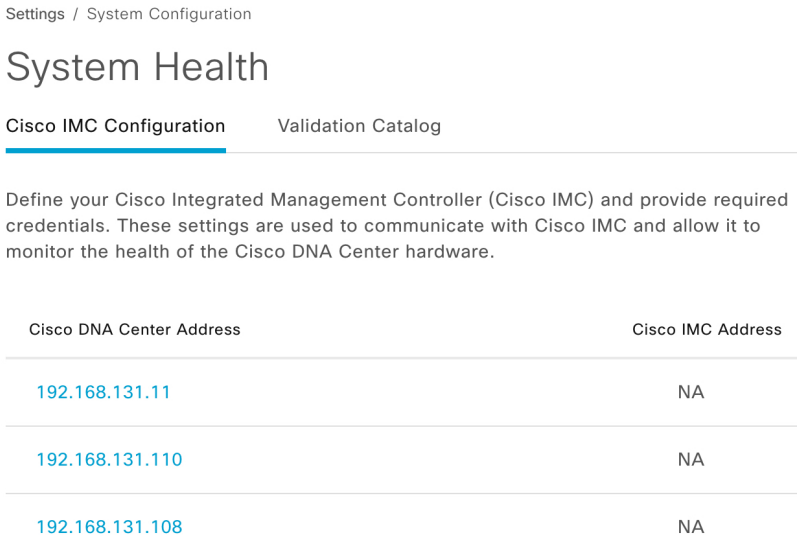
Cisco IMC 接続の確立

[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。この接続により、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 権限を持つユーザーのみです。

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[Settings]** > **[System Configuration]** > **[System Health]** の順に選択します。

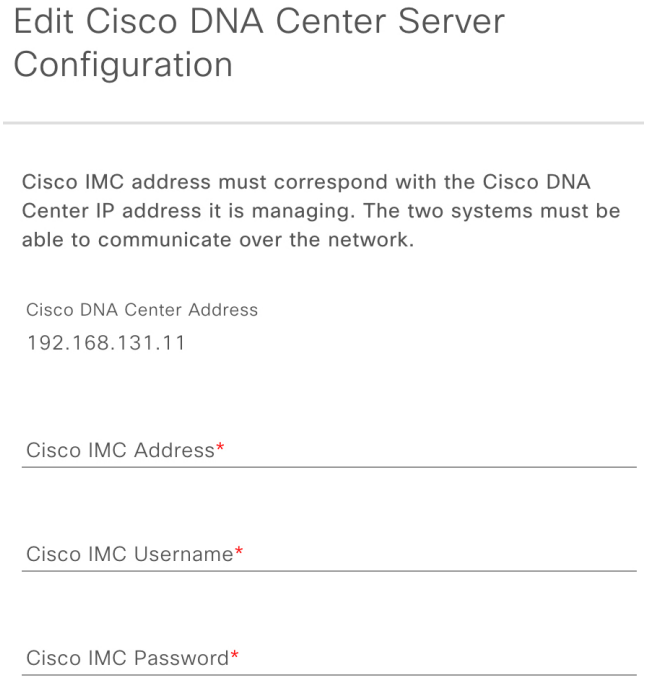
クラスタの各アプライアンスの IP アドレスが [Cisco DNA Center Address] 列に表示されます。



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ー名とパスワード。

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この手順を繰り返します。

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 権限を持つユーザーのみです。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[System Configuration]** > **[System Health]** 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] 列で対応する [Delete] アイコン（🗑）をクリックします。

ステップ 3 確認ウィンドウで、**[OK]** をクリックします。

システムイベント通知の登録

システムイベント通知に関する情報。

Cisco IMC との接続が確立されると、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。ルールエンジンによって、これらの未処理イベントは処理され、システムヘルストポロジに表示されるシステムイベント通知に変換されます。『Cisco DNA Center Platform User Guide』の「Work with Event Notifications」で説明されている手順を完了することにより、これらの通知を、利用可能な形式のいずれかでも受信できます。この手順を完了するときは、次のイベントを選択してサブスクライブしてください。

- 証明書の有効期限のイベント：
  - SYSTEM-CERTIFICATE
  - SYSTEM-NODE-CERTIFICATE
- 接続された外部システムのイベント：
  - SYSTEM-EXTERNAL-CMX
  - SYSTEM-EXTERNAL-IPAM
  - SYSTEM-EXTERNAL-ISE-AAA-TRUST
  - SYSTEM-EXTERNAL-ISE-PAN-ERS
  - SYSTEM-EXTERNAL-ISE-PXGRID
  - SYSTEM-EXTERNAL-ITSM
- ディザスタリカバリシステムのイベント：SYSTEM-DISASTER-RECOVERY
- 一般的なシステムのイベント：
  - SYSTEM-CIMC
  - SYSTEM-CONFIGURATION
  - SYSTEM-HARDWARE
  - SYSTEM-MANAGED-SERVICES

（注） マネージドサービスの場合、プローブ間隔（Cisco DNA Center が古いイベントをデータベースから削除するのにかかる時間）は60分です。マネージドサービスがダウンして再びアクティブになった場合、サービスが復元されたことをシステムの正常性GUIに反映するには、この時間がかかります。

- SYSTEM-SCALE-LIMITS

イベント通知情報

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

サブドメイン	タグ	インスタンス	状態	メッセージ
ドメイン：システム				
CPU	CPU	<*node-hostname*>:CPU-1	OK	Cisco DNA Center CPU-1 is working as expected on <*node-hostname*>
			NotOk	Cisco DNA Center CPU-1 has failed on <*node-hostname*>
			ディセーブル	Cisco DNA Center CPU-1 is disabled on <*node-hostname*>
メモリ	メモリ	<*node-hostname*>:DIMM_A1	Ok	Cisco DNA Center RAM DIMM_A1 is working as expected on <*node-hostname*>
			NotOk	Cisco DNA Center RAM DIMM_A1 has failed on <*node-hostname*>
ディスク	Disk	<*node-hostname*>:Disk1	Ok	Cisco DNA Center Disk 2 is working as expected on <*node-hostname*>
			NotOk	Cisco DNA Center Disk 2 has failed on <*node-hostname*>
RAID コントローラ	RAIDController	<*node-hostname*>:Controller-1	Ok	Cisco DNA Center RAID VD-2 is working as expected on <*node-hostname*>
			NotOk	Cisco DNA Center RAID VD-2 has degraded on <*node-hostname*>
			ディセーブル	Cisco DNA Center RAID VD-2 is offline on <*node-hostname*>
ネットワーク インターフェイス	NIC	<*node-hostname*>:nic-1	Ok	Cisco DNA Center network interfaces are working as expected
			NotOk	Cisco DNA Center: <*x*> network interfaces are missing for <*node-hostname*>: nic-1

サブドメイン	タグ	インスタンス	状態	メッセージ
PSU_FAN	PSU	<*node-hostname*>:psu-1	Ok	Cisco DNA Center power supply (PSU-1) is powered on and thermal condition is normal for <*node-hostname*>
			NotOk	Cisco DNA Center power supply (PSU-2) is powered off and thermal condition is critical for <*node-hostname*>
ディザスタ リカバリ	DisasterRecovery	<*disaster-recovery-hostname*>	Ok	• Disaster recovery cluster is up • Disaster recovery failover succeeded to <*site-name*>
			Degraded	• Disaster recovery failover triggered from <*site-name*> to *site-name* • Disaster recovery failed while failing over to <*site-name*> • Disaster recovery standby cluster on <*site-name*> is down; cannot failover • Disaster recovery witness is down; cannot failover • Disaster recovery replication halted; recovery point objective will be impacted • Disaster recovery pause failed • Disaster recovery route advertisement failed • Disaster recovery IPSec communication failed
			NotOk	• Disaster recovery configuration failed • Disaster recovery failed to rejoin the standby system
プラットフォーム サービス	ManagedServices	<hostname>:<name>	OK	Managed Service <*service-name*> is Running
			NOTOK	Managed Service <*service-name*> is Interrupted

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

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

サブドメイン	タグ	インスタンス	状態	メッセージ
			DEGRADED	The number of sites exceeded 425 (85% of limit)
			注意\t	The number of sites exceeded 375 (75% of limit)
	transient_clients	<hostname>:<name>	OK	OK
			NOTOK	The number of transient clients exceeded 71250 (95% of limit)
			DEGRADED	The number of transient clients exceeded 63750 (85% of limit)
			注意\t	The number of transient clients exceeded 56250 (75% of limit)
ソフトウェアアップグレード	Upgrade	<hostname>:<name>	OK	Successfully finished downloading package <*package-name*> with version <*package-version*>
			NOTOK	Catalog package download failed for <*package-name*>
バックアップ	Backup	<hostname>:<name>	OK	Successfully completed backup
			NOTOK	Failed to backup
Restore	Restore	<hostname>:<name>	OK	Successfully restored
			NOTOK	Failed to restore configuration
ドメイン：接続性				
ISE	ISE_ERS	<*Cisco-ISE-hostname*>	Success	ISE AAA trust establishment succeeded for ISE server <*ISE-server-details*>
			Failed	ISE AAA trust establishment failed for ISE server <*ISE-server-details*>
ドメイン：統合				
IPAM	IPAM	<*IPAM-hostname*>	Ok	IPAM connection to Cisco DNA Center established. IPAM <*IPAM-IP-address*>.
			Critical	IPAM connection to Cisco DNA Center offline. IPAM <*IPAM-IP-address*>.

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

システム正常性スケール番号

第 2 世代 Cisco DNA Center アプライアンスには、次のバージョンがあります。

- 44 コアアプライアンス：シスコ製品番号 DN2-HW-APL
- 44 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-U
- 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：シスコ製品番号 DN2-HW-APL-XL-U

システムヘルスにより、これらのアプライアンスがモニターされ、次の表に示されているネットワークコンポーネントが特定のしきい値を超えるたびに通知が生成されます。生成される通知の優先順位は、測定されたしきい値のパーセンテージによって異なります。

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

（注） すべてのアプライアンス（タイプに関係なく）について 1,000,000 件の通知が監査ログに保持され、1 年間保存されます。

表 *2:* スタンドアロン アプライアンスにおける規模の数

ネットワークコンポーネント	44 コアアプライアンス	56 コアアプライアンス	112 コアアプライアンス
[Total devices] ネットワーク内の有線デバイスとワイヤレスデバイスの合計数が、この値を超えないようにする必要があります。	**5000**	**8000**	**18,000**
有線デバイス（ルータ、スイッチ、スタック、およびワイヤレスコントローラ）	2000	4000	5000
ワイヤレスデバイス（アクセスポイントおよびセンサー）	4000	6000	13,000
インベントリの物理ポート	48,000	192,000	480,000
論理および物理インターフェイス	120,000	480,000	1,500,000
Total clients ネットワーク内の有線クライアントおよび無線クライアントの合計数は、この値を超えないようにする必要があります。	**25,000**	**40,000**	**100,000**
有線クライアント（同時）	25,000	40,000	100,000
ワイヤレスクライアント（同時）	25,000	40,000	100,000
一時的なクライアント	75,000	120,000	250,000
サイト	1500	3000	6000
着信 NetFlow	30,000	48,000	120,000
IP プール	50,000	75,000	100,000
ポリシーマトリックスサイズ	25,000	25,000	25,000
セキュリティ グループ	4000	4000	4000

表 *3:3* ノード クラスタ アプライアンスにおける規模の数

ネットワークコンポーネント	**56** コアアプライアンス	**112** コアアプライアンス
[Total devices] ネットワーク内の有線デバイスとワイヤレスデバイスの合計数が、この値を超えないようにする必要があります。	**8000**	**24000**
有線デバイス（ルータ、スイッチ、スタック、およびワイヤレスコントローラ）	4000	10,000
ワイヤレスデバイス（アクセスポイントおよびセンサー）	6000	18,000
インベントリの物理ポート	192,000	768,000
論理および物理インターフェイス	480,000	2,000,000
Total clients ネットワーク内の有線クライアントおよび無線クライアントの合計数は、この値を超えないようにする必要があります。	**60,000**	**300,000**
有線クライアント（同時）	60,000	300,000
ワイヤレスクライアント（同時）	60,000	300,000
一時的なクライアント	180,000	750,000
サイト	3000	6000
着信 NetFlow	48,000	250,000
IP プール	75,000	100,000
ポリシーマトリックスサイズ	25,000	25,000
セキュリティ グループ	4000	4000

（注） システム正常性は、3 つの 44 コア アプライアンスで構成される Cisco DNA Center クラスタではサポートされていません。

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 （8 ページ）
- システムイベント通知の登録 （11 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。

次の点に注意してください。

- Cisco DNA Center は IPv6 をサポートするようになりました。IPv6 が有効になっているクラスタを表示すると、トポロジには、そのクラスタのエンタープライズ仮想 IP アドレスに関する次の情報も表示されます。
  - [Pre] フィールド：16 ビットのプレフィックス
  - [GID] フィールド：32 ビットのグローバル ID
  - [Subnet] フィールド：16 ビットのサブネット値

  クラスタのエンタープライズ仮想 IP アドレスの残りは、クラスタのトポロジアイコンのラベル付けに使用されます。
- IPv6 対応のクラスタは、やはり IPv6 対応の外部システムにのみ、接続してデータを取得することができます。
- 接続されているアプライアンスまたは外部システムに、有効期限が設定されている証明書がインストールされている場合は常に、トポロジで次のことが実行されます。
  - 証明書が 90 日以内に期限切れになるように設定されている場合、トポロジに警告が表示されます。
  - 証明書が 30 日以内に期限切れになるように設定されている場合は、トポロジにエラーが表示されて問題への注意が喚起されます。
- システムヘルスはハードウェア コンプライアンス チェックを定期的に実行し、接続されているアプライアンスまたは外部システムが最小構成要件を満たしていない場合は常に、そのことを示します。たとえば、接続されている仮想ドライブに関して**ライトスルー**キャッシュ書き込みポリシーが設定されていない場合、システムヘルスはトポロジを更新して、そのことを示します。

- 実稼働環境でディザスタリカバリが正常に機能している場合、システムヘルスは、メインサイトとリカバリサイトの両方のアプライアンスに関するハードウェア情報を提供します。以前は、メインサイトのアプライアンスに関してのみ、ハードウェア情報が提供されていました。

アプライアンスと外部システムの問題のトラブルシューティング

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シビラティ（重大度）。
- 問題に関連するドメイン、サブドメイン、および IP アドレスまたはロケーション。

接続された外部システムに問題がある関連サーバーが 3 つ以上ある場合や 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、該当するサーバーまたはコンポーネントのリストが表示されます。それらの各項目の [>] をクリックしてエントリを展開することで、特定の項目の情報を確認できます。

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ーにそのロールを割り当てます。[Create a User Role] ウィザードでこのパラメータにアクセスするには、[Define the Access] ページの [System] 行を展開します。詳細については、『*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] ウィンドウの右上部分から、**[Tools]** > **[Network Ping]** を選択して [Ping Device] ウィンドウを開きます。

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

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。

検証ツールの使用

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

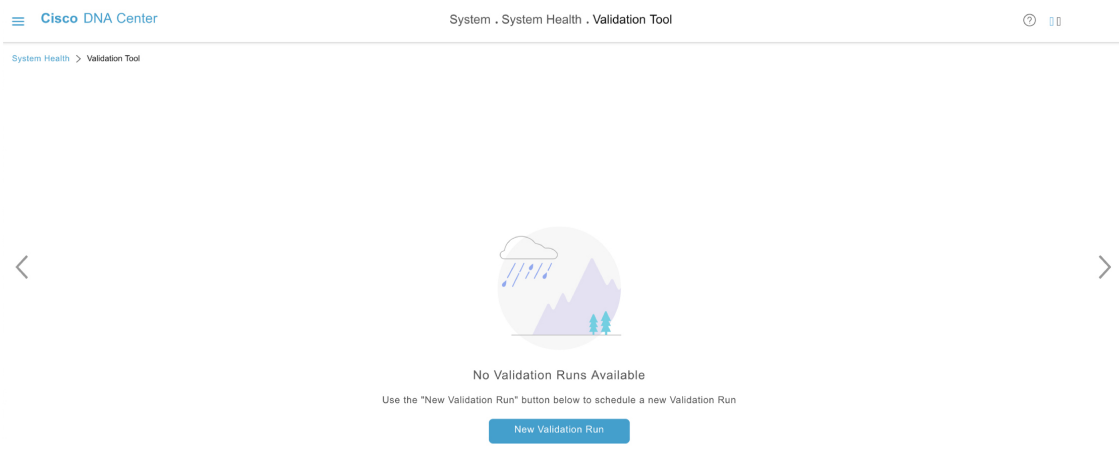
- ciscoconnectdna.com への接続機能（システムおよびパッケージの更新をダウンロードするため）。
- 期限切れの証明書の有無。
- アプライアンスハードウェアとバックエンドサービスの現在の状態。
- スケール番号のしきい値を超えたネットワークコンポーネント。

検証ツールにアクセスするには、次の手順を実行します。

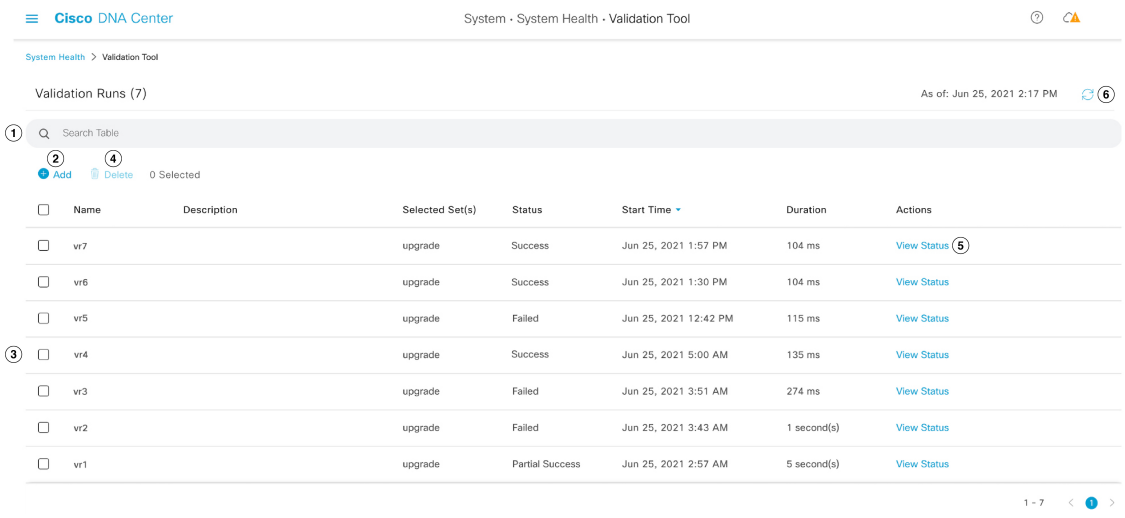
1. メニューアイコン（☰）をクリックして、**[System]** > **[System Health]** をクリックして、[System Health] ページを開きます。
2. [Tools] ドロップダウンメニューから、[Validation Tool] を選択します。

検証ツールページの移動

[Validation Tool] ページの内容は、以前に完了した検証処理に関する情報があるかどうかによって異なります。Cisco DNA Center情報がない場合、ページは次のようになります。



Cisco DNA Center に検証処理に関する情報がある場合、ページは次のようになります。



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

引き出し線	説明
1	[Search Table] フィールド：このページにリストされている検証処理をフィルタリングするための検索文字列を入力します。
2	[Add] ボタン：クリックして [New Validation Run] スライドインペインを開き、新しい処理のために必要な設定を入力します。詳細については、検証処理の開始 （24 ページ） を参照してください。

引き出し線	説明
3	[Validation Runs] テーブル：以前に完了した検証処理がリストされます。このテーブルには、処理ごとの名前、適用可能な検証セット、完了ステータスなどの情報が表示されます。次の点に注意してください。 • デフォルトでは、処理は開始時刻順に並べられ、最新の処理が最初にリストされます。 • 現在進行中のすべての処理に対しては、期間はゼロと表示されます。
4	[Delete] ボタン：検証処理のチェックボックスをオンにした状態でこのボタンをクリックすると、処理が削除されます。次に [Warning] ダイアログボックスで [OK] をクリックして、削除を確定します。 （注）　進行中の処理は削除できません。
5	[View Status] リンク：特定の処理の詳細を表示します。詳細については、検証処理の詳細の表示 （25 ページ）を参照してください。
6	[Refresh] ボタン：クリックすると、このページに表示されている情報が更新されます。

検証処理の開始

検証処理を開始するには、以下の手順を実行します。

（注）　一度に実行できる検証は 1 つだけです。検証処理がすでに進行中の場合は、完了するまで待ってから、別の処理を開始する必要があります。

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

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

[New Validation Run] スライドインペインが開きます。

ステップ 2　[Name] フィールドに、検証処理の名前を入力します。

入力する名前は一意で、英数字のみを使用してください。特殊文字は使用できません。

ステップ 3　（任意） [Description] フィールドに、これから開始する検証処理に関する簡単な説明を入力します。

説明は最大 250 文字まで入力できます。

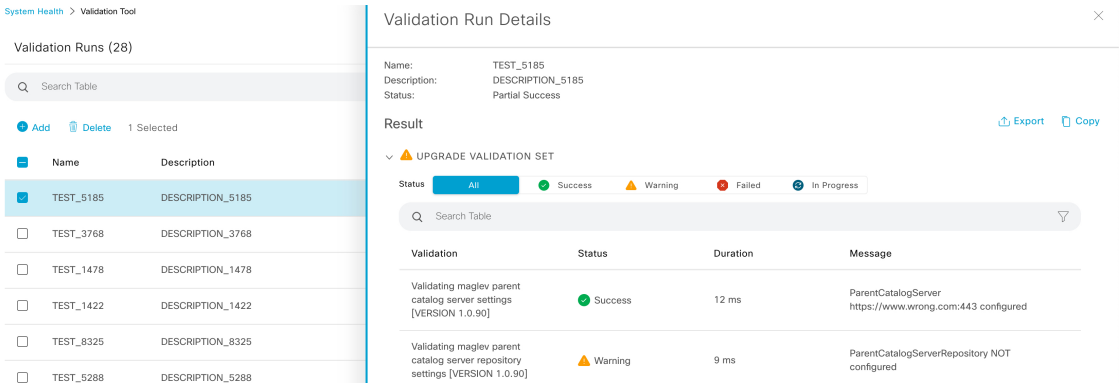
ステップ 4 [Validation Set(s) Selection] エリアで、実行する検証セットのチェックボックスをオンにします。

検証セットを最大化して、実行するチェックを表示できます。

ステップ 5 [Run] をクリックします。

検証処理の詳細の表示

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



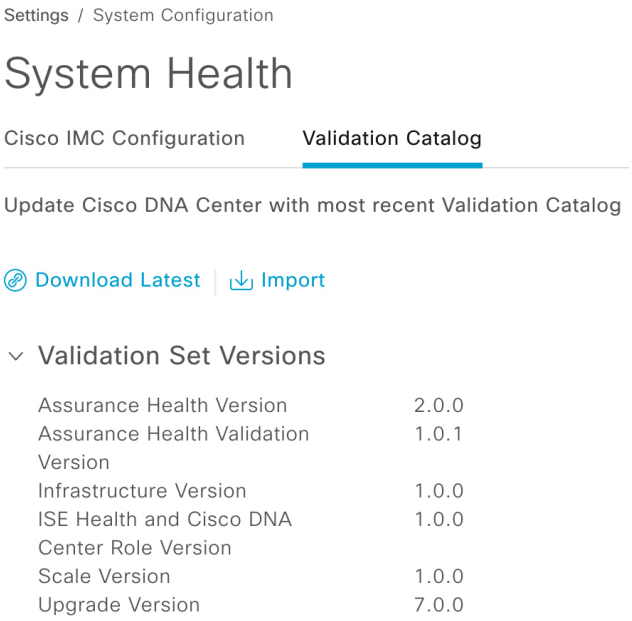
ここでは次の操作も実行できます。

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

検証セットの更新

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

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[System Configuration]** > **[System Health]** の順に選択します。

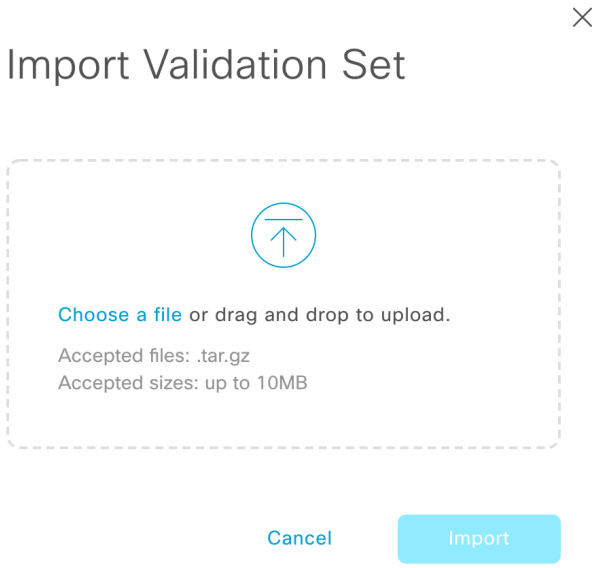


ステップ 2 [Validation Catalog] タブをクリックします。

ステップ 3 [Download Latest] をクリックして、使用可能な最新の検証セットのローカルコピーをダウンロードします。

ステップ 4 検証セットを Cisco DNA Center にインポートします。

a) [Import] をクリックし、[Import Validation Set] ダイアログボックスを開きます。



b) 次のいずれかを実行します。

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

c) **[インポート (Import)]** をクリックします。

System Analyzer ツールの使用

トラブルシューティングが必要な問題が発生した場合は、System Analyzer ツールを使用してログファイルを取得できます。システムレベルのログファイルに加えて、Cisco SD-Access とソフトウェアイメージ管理（SWIM）に固有のログファイルを取得できます。[System Analyzer] ツールにアクセスするには、次の手順を実行します。

1. メニューアイコン（☰）をクリックして、**[System]** > **[System Health]**の順に選択します。

   [System Health] ウィンドウが開きます。

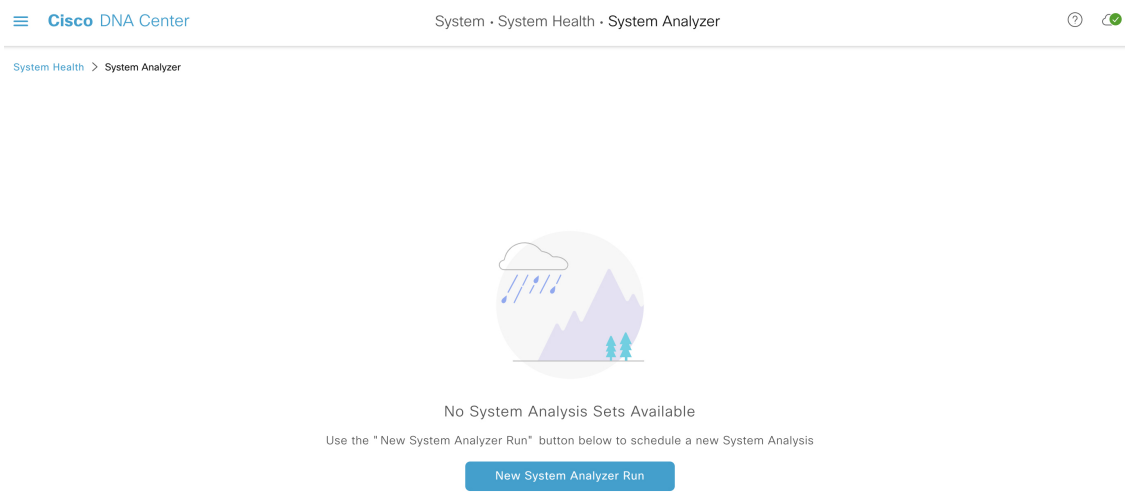
2. [Tools] ドロップダウンリストから、[System Analyzer] を選択します。

このツールを使用する前に、次の点に注意してください。

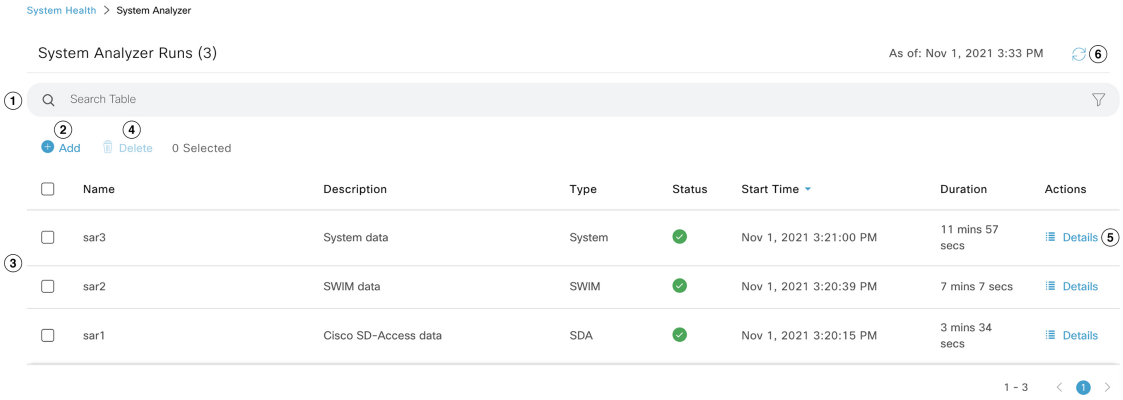
- 管理者ユーザーのみが、システム分析の実行を開始し、結果のログファイルをダウンロードし、完了した実行を削除できます。すべてのユーザーは、選択した実行の [System Analysis Details] スライドインペインを開いて表示できます。
- System Analyzer ツールでは、Cisco DNA Center の GlusterFS ファイルシステムに 5 GB のディスク容量が必要です。
- Cisco DNA Center は、5 GB または過去 3 か月分のシステム分析実行のいずれか小さい方を保存します。
- いずれかのストレージ制限に達すると、Cisco DNA Center は古い実行を 1 日 1 回削除します。また、新しい実行が開始される前にも、古い実行が削除されます。
- ログファイル情報はトラブルシューティングにのみ役立つため、システム分析実行のデータはバックアップされません。
- HA が有効になっている展開では、実行の進行中にシステムヘルスサービスがダウンした場合、システムヘルスが再び起動した後に実行を再開する必要があります。
- ディザスタリカバリが有効になっている展開では、実行データはディザスタリカバリシステムのサイト全体にレプリケートされません。システムのアクティブサイトとスタンバイサイトは、独自の実行履歴を保持します。

[System Analyzer] ページをナビゲートする

[System Analyzer] ページの内容は、Cisco DNA Center に以前に完了した処理に関する情報があるかどうかによって異なります。情報がない場合、ページは次のようになります。



Cisco DNA Center に処理に関する情報がある場合、ページは次のようになります。



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

引き出し線	説明
1	[Search Table] フィールド：このページにリストされている処理をフィルタリングするための検索文字列を入力します。
2	[Add] ボタン：クリックして [New System Analyzer Run] スライドインペインを開き、処理のために必要な設定を入力します。詳細については、System Analyzer 処理の開始 （29 ページ） を参照してください。

引き出し線	説明
3	[System Analyzer Runs] テーブル：現在進行中または以前に完了した処理をリストします。処理ごとに、名前、関連する Cisco DNA Center コンポーネント、処理の完了にかかった時間などの情報がテーブルに表示されます。 次の点に注意してください。 • デフォルトでは、処理は開始時刻順に並べられ、最新の処理が最初にリストされます。 • 現在進行中のすべての処理に対しては、期間はゼロと表示されます。
4	[Delete] ボタン：処理のチェックボックスをオンにした状態で、[Delete] をクリックして削除します。 （注）　進行中の処理は削除できません。
5	[Details] リンク：特定の処理の詳細を表示します。詳細については、System Analyzer 処理の詳細の表示 （30 ページ）を参照してください。
6	[Refresh] ボタン：クリックすると、このページに表示されている情報が更新されます。

System Analyzer 処理の開始

System Analyzer 処理を開始するには、次の手順を実行します。

ステップ 1 [System Analyzer Runs] テーブルが表示されているかどうかに応じて、[System Analyzer] ページで次のいずれかを実行します。

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

[New System Analyzer Run] スライドインペインが開きます。

ステップ 2 [Name] フィールドに、処理の名前を入力します。

入力する名前は一意で、英数字のみを使用してください。特殊文字は使用できません。

ステップ 3 （任意） [Description] フィールドに、これから開始する処理に関する簡単な説明を入力します。

説明は最大 250 文字まで入力できます。

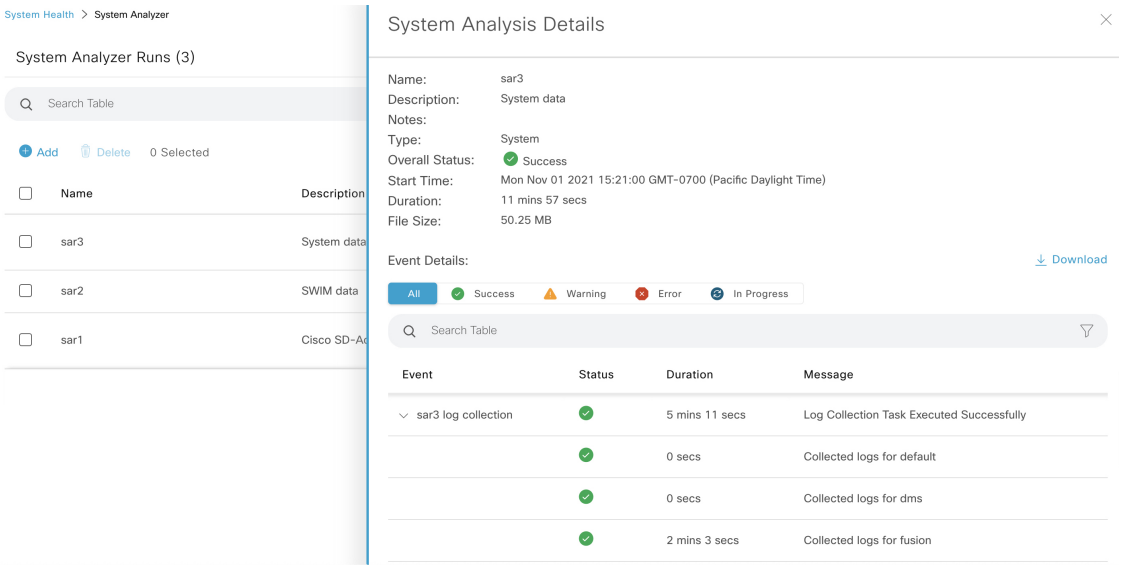
ステップ 4 （任意） [Notes] フィールドに、処理に指定する追加情報（最大 250 文字）を入力します。

ステップ 5 [Select a System Analyzer to run] エリアで、ログファイルを取得する Cisco DNA Center コンポーネントのラジオボタンをクリックします。

ステップ 6 [Run] をクリックします。

System Analyzer 処理の詳細の表示

[System Analysis Details] スライドインペインから、取得したログファイルの合計ファイルサイズや関連する Cisco DNA Center コンポーネントなど、選択した実行に関する追加情報を表示できます。実行中に問題が発生したログファイルも特定できます。



ここでは次の操作も実行できます。

- [Search Table] フィールドに、表示される情報をフィルタリングするための検索文字列を入力します。
- [Download] をクリックして、取得したログファイルを .tar.gz ファイルとしてダウンロードします。

特定の実行の [System Analysis Details] スライドインペインを開くには、[Actions] 列の [Details] リンクをクリックします。

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。通知は対応するシビラティ（重大度）に応じてグループ化されています。

- シビラティ（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。
- シビラティ（重大度） 2（警告）：Cisco ISE サーバーとの信頼を確立できないなどの問題を示します。

- シビラティ（重大度）3（成功）：サーバーやハードウェアコンポーネントが想定どおりに動作していることを示します。

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

表 *4 : Cisco DNA Center* アプライアンスの通知

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

表 *5 :* 接続されている外部システムの通知

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

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

Disk Utilization Event Notifications

システムヘルスは、システム内のノードごとのディスク使用率を監視し、これらのノードの使用率がネットワーク操作に影響を与える可能性のあるレベルに達すると通知を送信します。使用率が 75% を超えると、システムヘルスは警告通知を送信します。また、使用率が 85% を超えると、システムヘルスは重大な通知を送信します。これらの通知を設定およびサブスクライブするには、『*Cisco DNA CenterPlatform User Guide*』の「Work with Event Notifications」トピックに説明されている手順を実行してください。この手順を完了するときは、必ず [System Performance: Filesystem Utilization] イベントを選択してサブスクライブしてください。

ディスク使用率の監視に関して、次の点に注意してください。

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

推奨されるアクション

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

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

コンポーネント	サブコンポーネント	問題	推奨されるアクション
			1. Cisco DNA Center で現在設定されている AAA 設定を削除します。 2. 適切な AAA 設定を再入力します。詳細については、『*Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide*』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。 3. 信頼を再確立します。詳細については、『*Cisco Identity Services Engine Administration Guide*』の「Enable PKI in Cisco ISE」を参照してください。
	信頼：到達可能性	HTTPS 接続を確立できない。	AAA 設定のログイン情報と Cisco ISE のログイン情報が同じであるかどうかを確認します。
		Cisco ISE 証明書チェーンのアップロード用に設定された Cisco DNA Center エンドポイント URL に到達できない。	• Cisco DNA Center と Cisco ISE の間のプロキシサーバーのプロキシ設定を確認します。 • Cisco DNA Center から Cisco ISE に到達できるかどうかを確認します。
	信頼：設定	Cisco ISE 証明書チェーンが無効である。	• 必要に応じて、Cisco ISE 内部ルート CA チェーンを再生成します。詳細については、『*Cisco Identity Services Engine Administration Guide*』の「ISE CA Chain Regeneration」を参照してください。 • 内部 CA 証明書チェーンが Cisco ISE から削除されていないことを確認します。
		Cisco ISE 証明書チェーンのアップロード用に設定された Cisco DNA Center エンドポイント URL が禁止されている。	

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
			• URL を起動し、エンドポイントの /aaa/Cisco ISE/certificate ディレクトリにアクセスできるかどうかを確認します。 • Cisco ISE で [Use CSRF Check for Enhanced Security] オプションが有効になっているかどうかを確認します。詳細については、『*Cisco Identity Services Engine Administration Guide*』の「Enable External RESTful Services APIs」を参照してください。
	信頼：認証	Cisco ISE パスワードの期限が切れている。	• Cisco ISE 管理者パスワードを再生成します。詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Administrative Access to Cisco ISE」を参照してください。 • Cisco ISE GUI にログインできることを確認します。
	信頼：未分類または一般的なエラー	未定義の診断エラーが発生する。	1. Cisco DNA Center で現在設定されている AAA 設定を削除します。 2. 適切な AAA 設定を再入力します。詳細については、『*Cisco Digital Network Architecture Center Second Generation Appliance Installation Guide*』の「Integrate Cisco ISE with Cisco DNA Center」を参照してください。 3. 信頼を再確立します。詳細については、『*Cisco Identity Services Engine Administration Guide*』の「Enable PKI in Cisco ISE」を参照してください。

コンポーネント	サブコンポーネント	問題	推奨されるアクション
Cisco Connected Mobile Experiences（CMX）サーバー IP アドレス管理（IPAM）サーバー IT サービス管理（ITSM）サーバー	到達可能性	サーバーとの接続を確立できない。	該当するサーバーがダウンしていないかどうかを確認します。
	認証	サーバー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		
	ネットワーキング	インターフェイスがない。	**1.** Cisco IMC に接続します。 **2.** PID が UCSC-C220-M4、UCSC-C220-M4S、または DN1-HW-APL の場合は、次の手順を実行します。 **1.** メインメニューから、**[Compute]** > **[BIOS]** > **[Configure BIOS]** を選択します。 **2.** [Advanced] タブをクリックします。 **3.** [LOM and PCIe Slots Configuration] を展開します。 **4.** 無効な mLOM を有効にして、ホストを再起動します。 **3.** その他すべての PID について、問題のあるコンポーネントを交換します。

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
System configuration	ハードウェア構成	Cisco DNA Center <IP_address> 仮想ドライブの書き込みキャッシュポリシーとしてライトバックを指定することはできません。書き込みポリシーはライトスルーである必要があります。	1. Cisco IMC に接続します。 2. メインメニューから、**[Storage]** > **[Raid Controller]** を選択します。 3. [Virtual Drive] タブをクリックします。 4. 仮想ドライブを選択し、[Edit] を右クリックします。書き込みポリシーがライトスルーでない場合は、仮想ドライブを更新します。書き込みポリシーはライトスルーである必要があります。
システム リソース	ストレージ	指定したマウントディレクトリに空きがない。	• 現在のディレクトリから不要なデータを削除して記憶域を解放します。 • 記憶域が多い新しいマウントディレクトリを指定します。

サポートされている REST API

システムヘルスでは、次の表に示す REST API がサポートされています。これらの API のいずれかを実行するには、API のパスに次の URL を追加します。
https://CDNAC-server-IP-address/api/v1/API-path

Method	API パス	説明
GET	diagnostics/system/health	接続されているすべての Cisco DNA Center アプライアンスと外部システムの最新の正常性関連イベントが表示されます。
	diagnostics/system/health?summary=true	シビラティ（重大度）が最も高い最新の正常性イベントが表示されます。
	diagnostics/system/health?domain=DNAC-Appliance	接続されているアプライアンスのすべてのハードウェアイベントが表示されます。
	diagnostics/system/health?domain=Integrations&subdomain-AAA Trust Establishment	すべての統合および AAA 信頼の確立イベントが表示されます。
	diagnostics/system/health?limit=5	最新の 5 つの正常性関連イベントが表示されます。
	diagnostics/system/performance	接続されたアプライアンスのパフォーマンス情報が要約され、過去 15 分間の平均が表示されます。
	diagnostics/system/performance?range=now-1h	過去 1 時間の重要業績評価指標（KPI）メトリックが表示されます。
	diagnostics/system/performance?range=now-1d	過去 1 日間の KPI メトリックが表示されます。
	diagnostics/system/performance?range=now-1w	過去 1 週間の KPI メトリックが表示されます。
	diagnostics/system/performance?function=max	指定した期間の最大値、現在値が表示されます。デフォルトは平均値です。
	diagnostics/system/nodes/performance?range=now-1d	過去 1 日間の接続された各アプライアンスの KPI メトリックが表示されます。
	diagnostics/system/performance?kpi=cpu,memory	デフォルトの期間（15 分）の CPU およびメモリ使用率が表示されます。
	diagnostics/system/nodes/performance/history?kpi=cpu	デフォルト期間の指定された KPI の履歴メトリックが表示されます。複数の KPI を指定する場合は、カンマで区切ります。
	diagnostics/system/nodes/performance/history?kpi=cpu&range=now-1d	過去 1 日間の指定された KPI の履歴メトリックが表示されます。
	/system/health/summary/	最新の重大クラスタイベントが表示されます。クラスタイベントには、すべてのハードウェアコンポーネントと外部サブシステムのイベントが含まれます。
	/system/health/externalsubsystems/*subdomain*	指定されたサブドメインの最新のイベントが表示されます。有効なサブドメイン値は、IPAM、ISE、CMX、および ITSM です。

Method	API パス	説明
	/system/health/hardware	最新の重大なハードウェアイベントが表示されます。
	/system/health/hardware/hardware_component	指定されたハードウェアコンポーネントの最新のイベントが表示されます。有効なハードウェアコンポーネントの値には、CPU、RAID、MEMORY、POWER、NIC、および DISK があります。
	/diagnostics/system/health/externalsubsystems/ISE	この API によって提供される出力は、接続されている Cisco ISE サーバーの現在の状態によって異なります。この出力の例については、サンプル API 出力 （39 ページ）を参照してください。
	/diagnostics/system/health/externalsubsystems/IPAM	この API によって提供される出力は、接続されている Cisco Prime Network Registrar IP アドレスマネージャ（IPAM）の現在の状態によって異なります。この出力の例については、サンプル API 出力 （39 ページ）を参照してください。

サンプル API 出力

次の表に、/diagnostics/system/health/externalsubsystems/ISE または /diagnostics/system/health/externalsubsystems/IPAM API を実行したときに表示される出力の例を示します。

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：Cisco ISE サーバーが Cisco DNA Center と統合されていません。

Output:

```
{
"DNAC-Cluster": {
"Status": "Warning",
"TooltipInfo": "No data available"
}
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：Cisco ISE サーバーが Cisco DNA Center に統合されており、正常に機能しています。

Output:


```
{
"DNAC-Cluster": {
"Status": "Ok",
"Group": "ISE",
"Label": {
"hostname": "ISE-60-38.example.com",
"ip": "172.28.80.37"
},
"Family": "ExternalSystems",
"Id": 1,
"TooltipInfo": [
{
"_id": "-429109689",
"tenantId": "TNT0",
"severity": 3,
"timestamp": "1591072373412",
"source": "ISE ERS Client",
"actualState": "",
"description": "ISE PAN ERS connection : ERS reachability with ISE - Success",
"group": "ISE",
"family": "External Subsystem",
"drUsability": "No",
"state": "SUCCESS",
"eventInstanceIdentity": {
"subDomain": "ISE",
"domain": "Connectivity",
"namespace": "SystemRawEvent",
"id": "SYSTEM-EXTERNAL-ISE-PAN-ERS",
"type": "SYSTEM",
"tags": "ISE_ERS",
"event_instance_id": {
"component": "primary",
"hostname": "ISE-60-38.example.com",
"ip": "172.28.80.37"
}
}
}
]
}
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：警告ステータスを持つ Cisco ISE イベントが発生しました。

Output:


```
{
"DNAC-Cluster": {
"Status": "Warning",
"Group": "ISE",
"Label": {
"hostname": "pi-system-200.example.com",
"ip": "10.197.73.213"
},
"Family": "ExternalSystems",
"Id": 1,
"TooltipInfo": [
{
"_id": "-440073227",
"tenantId": "TNT0",
"severity": 2,
"timestamp": "1591072804646",
"source": "AAA Trust Establishment",
"actualState": "",
"description": "ISE AAA Trust Establishment : Trust Establishment - Error-IP/FQDN not reachable",
"group": "ISE",
"family": "External Subsystem",
"drUsability": "No",
"state": "FAILED",
"eventInstanceIdentity": {
"subDomain": "ISE",
"domain": "Integrations",
"namespace": "SystemRawEvent",
"id": "SYSTEM-EXTERNAL-ISE-AAA-TRUST",
"type": "SYSTEM",
"tags": "ISE_AAA",
"event_instance_id": {
"hostname": "pi-system-200.example.com",
"component": "primary",
"ip": "10.197.73.213"
}
}
}
]
}
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：接続された Cisco ISE サーバーで外部 RESTful サービス（ERS）が無効になっています。

Output:


```
{
    "DNAC-Cluster": {
        "Status": "Warning",
        "Group": "ISE",
        "Label": {
            "hostname": "csg-nscg-0861.example.com",
            "ip": "10.63.107.41"
        },
        "Family": "ExternalSystems",
        "Id": 1,
        "TooltipInfo": [
            {
                "_id": "-915009445",
                "tenantId": "TNT0",
                "severity": 2,
                "timestamp": "1591357663101",
                "source": "ISE ERS Client",
                "actualState": "",
                "description": "ISE PAN ERS connection : Timeout elapsed",
                "group": "ISE",
                "family": "External Subsystem",
                "state": "FAILED",
                "eventInstanceIdentity": {
                    "subDomain": "ISE",
                    "domain": "Connectivity",
                    "namespace": "SystemRawEvent",
                    "id": "SYSTEM-EXTERNAL-ISE-PAN-ERS",
                    "type": "SYSTEM",
                    "tags": "ISE_ERS",
                    "event_instance_id": {
                        "hostname": "csg-nscg-0861.example.com",
                        "component": "primary",
                        "ip": "10.63.107.41"
                    }
                }
            }
        ]
    }
}
```

/diagnostics/system/health/externalsubsystems/ISE の出力例

シナリオ：接続された Cisco ISE サーバーで ERS が有効になっています。

Output:


```
{
    "DNAC-Cluster": {
        "Status": "Ok",
        "Group": "ISE",
        "Label": {
            "hostname": "csg-nscg-0861.example.com",
            "ip": "10.30.148.52"
        },
        "Family": "ExternalSystems",
        "Id": 1,
        "TooltipInfo": [
            {
                "_id": "-915009445",
                "tenantId": "TNT0",
                "severity": 3,
                "timestamp": "1591359643926",
                "source": "ISE ERS Client",
                "actualState": "",
                "description": "ISE PAN ERS connection : ERS reachability with ISE - Success",
                "group": "ISE",
                "family": "External Subsystem",
                "state": "SUCCESS",
                "eventInstanceIdentity": {
                    "subDomain": "ISE",
                    "domain": "Connectivity",
                    "namespace": "SystemRawEvent",
                    "id": "SYSTEM-EXTERNAL-ISE-PAN-ERS",
                    "type": "SYSTEM",
                    "tags": "ISE_ERS",
                    "event_instance_id": {
                        "hostname": "csg-nscg-0861.example.com",
                        "component": "primary",
                        "ip": "10.30.148.52"
                    }
                }
            }
        ]
    }
}
```


/diagnostics/system/health/externalsubsystems/IPAM の出力例

シナリオ：Cisco Prime Network Registrar IPAM が Cisco DNA Center に接続されていません。

Output:


```
{
"DNAC-Cluster": {
"Status": "Warning",
"TooltipInfo": "No data available"
}
}
```

/diagnostics/system/health/externalsubsystems/IPAM の出力例

シナリオ：IPAM が Cisco DNA Center に接続されており、正常に機能しています。

Output:


```
{
"DNAC-Cluster": {
"Status": "Ok",
"Group": "IPAM Integration",
"Label": {
"hostname": "",
"ip": "192.168.101.72"
},
"Family": "ExternalSystems",
"Id": 1,
"TooltipInfo": [
{
"_id": "1328761079",
"tenantId": "TNT0",
"severity": 3,
"timestamp": "1591072639889",
"source": "INFOBLOX: https://192.168.101.72",
"actualState": "",
"description": "A third-party IPAM provider is connected.",
"group": "IPAM",
"family": "External Subsystem",
"drUsability": "No",
"state": "OK",
"eventInstanceIdentity": {
"subDomain": "IPAM Integration",
"domain": "Integrations",
"namespace": "SystemRawEvent",
"id": "SYSTEM-EXTERNAL-IPAM",
"type": "SYSTEM",
"tags": "IPAM",
"event_instance_id": {
"hostname": "",
"ip": "192.168.101.72"
}
}
}
]
}
}
```

/diagnostics/system/health/externalsubsystems/IPAM の出力例

シナリオ：IPAM が Cisco DNA Center に接続されており、エラーが発生しました。

Output:


```
{
    "DNAC-Cluster": {
        "Status": "Error",
        "Group": "IPAM Integration",
        "Label": {
            "hostname": "",
            "ip": "192.168.101.72"
        },
        "Family": "ExternalSystems",
        "Id": 1,
        "TooltipInfo": [
            {
                "_id": "1328761079",
                "tenantId": "TNT0",
                "severity": 1,
                "timestamp": "1591363687041",
                "source": "INFOBLOX: https://192.168.101.72",
                "actualState": "",
                "description": "There is a critical issue with the connected third-party IPAM provider.",
                "group": "IPAM",
                "family": "External Subsystem",
                "state": "CRITICAL",
                "eventInstanceIdentity": {
                    "subDomain": "IPAM Integration",
                    "domain": "Integrations",
                    "namespace": "SystemRawEvent",
                    "id": "SYSTEM-EXTERNAL-IPAM",
                    "type": "SYSTEM",
                    "tags": "IPAM",
                    "event_instance_id": {
                        "hostname": "",
                        "ip": "192.168.101.72"
                    }
                }
            }
        ]
    }
}
```


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 はユーザー、デバイス、クライアント認証用の AAA（「トリプル A」と発音）サーバーとして使用できます。アクセス コントロール ポリシーを使用していない場合、または Cisco ISE をデバイス認証用の AAA サーバーとして使用していない場合は、Cisco ISE のインストールおよび設定は不要です。
2. アクセス コントロール ポリシーは Cisco ISE を使用してアクセス制御を適用します。アクセス コントロール ポリシーを作成および使用する前に、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ー認証に Cisco ISE を使用している場合、Cisco ISE を統合するために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（ユーザー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 サーバー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 サーバー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、Cisco ISE 自体による拒否が原因で入力検証エラーとして失敗した場合、再試行は行われません。

Cisco ISE について RADIUS の共有秘密を変更しても、Cisco ISE が 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 サーバーを編集します。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 サーバーがダウンした場合、Cisco DNA Center に Cisco ISE サーバーが赤色（到達不能）で表示されます。

Cisco ISE サーバーに到達不能な場合、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 サーバーのステータスを [信頼できない（Untrusted）] に更新します。この場合、Cisco DNA Center と Cisco ISE サーバー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 サーバー経由ではサポートされていません。プロキシサーバーを使用して設定されている Cisco ISE がネットワークにある場合、そのプロキシサーバーを使用しないように Cisco DNA Center を設定します。設定するにはプロキシサーバーの IP アドレスをバイパスします。
- 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 ISE での管理者レベルのアクセス権が必要です。
- Cisco ISE の管理者ユーザーのパスワードの有効期限を無効にします。または、期限が切れる前に、パスワードを忘れずに更新します。詳細については、*Cisco Identity Services Engine Administrator 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 サーバー（Cisco ISE）を編集し、パスワードを再入力して保存します。これにより、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、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]** で Cisco ISE を AAA サーバーとして設定する際に指定しています。シークレットパスワードを変更するには、**[Design]** > **[Network Settings]** > **[Network]** の順に選択し、[Change Shared Secret] リンクをクリックします。これにより、Cisco ISE は、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。
- 分散 Cisco ISE クラスタでは、各ノードは PAN（管理）、MnT（監視とトラブルシューティング）、PSN（ポリシーサービス）などの特定の機能のみを実行します。PAN ノードでは

管理証明書のみを使用し、PSN ノードでは EAP 認証証明書のみを使用することができます。ただし、この構成により pxGrid の Cisco DNA Center と Cisco ISE の統合が妨げられます。したがって、Cisco ISE プライマリ PAN ノードで EAP 認証証明書の使用を有効にすることをお勧めします。

- Cisco DNA Center は、CRL 配布ポイント（CDP）および Online Certificate Status Protocol（OCSP）による証明書失効チェックをサポートしています。統合中に、Cisco DNA Center はポート 9060 で Cisco ISE 管理証明書を受信し、その Cisco ISE 管理証明書内の CDP および OCSP URL に基づいてその有効性を検証します。CDP（CRL のリストを含む）と OCSP の両方が設定されている場合、Cisco DNA Center は OCSP を使用して証明書の失効ステータスを確認し、OCSP URL にアクセスできない場合は CDP にフォールバックします。CDP に複数の CRL がある場合、Cisco DNA Center は最初の CRL に到達できない場合は、次の CRL に接続します。ただし、JDK PKI Oracle のバグにより、すべての CRL エントリはチェックされません。

  プロキシは証明書の検証ではサポートされていません。Cisco DNA Center はプロキシなしで CRL および OCSP サーバーに接続します。

  - 証明書の OCSP および CRL エントリはオプションです。
  - LDAP は、証明書検証用のプロトコルとしてサポートされていません。CDP または AIA 拡張に LDAP URL を含めないでください。
  - Cisco DNA Center から CDP および OCSP のすべての URL に到達できる必要があります。到達不能な URL が原因で、統合の失敗など、統合エクスペリエンスの低下が生じる可能性があります。

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。ユーザー ID やデバイスのホスト名など、有線エンドポイントとワイヤレスエンドポイントの個人を特定できる情報をスクランブル化できます。

[Discovery] を実行する前に、匿名化が有効になっていることを確認します。[Discovery] を実行した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Anonymize Data]** の順に選択します。

ステップ 2 [Anonymize Data] ウィンドウで、[Enable Anonymization] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。
匿名化を有効にすると、デバイス検索時に、MAC アドレス、IP アドレスなどの匿名以外の情報しか指定できなくなります。

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 および Cisco ISE が統合されていることを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバーで Cisco DNA Center を登録します。これには、AAA サーバーと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバーで 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 サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、以下の点を確認してください。
  - Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
  - スタンドアロン ISE 展開環境がある場合は、Cisco DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

（注） 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 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合：
  - Cisco DNA Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

（注） PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

- 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
- TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

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

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、Cisco Cloud APIC リリースノート [英語] を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]**。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ 3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

ステップ 4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address]：Cisco ISE サーバーの IP アドレス。
- [Shared Secret]：デバイス認証のキー。
- [Username]：Cisco ISE に HTTPS 経由でログインするために使用するユーザー名。
- [Password]：Cisco ISE HTTPS ユーザー名のパスワード。

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

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

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

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

hostname.domainname.com

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

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

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

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

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

  このオプションを有効にする場合は、次のことを確認してください。

  - Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局（CA）によって生成されていること（そうでない場合、pxGrid 認証は失敗します）。
  - [Certificate Extended Key Use（EKU）] フィールドに「クライアント認証」が含まれていること。

- [Protocol]：[TACACS] と [RADIUS]（デフォルト）。両方のプロトコルを選択できます。

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

- [Authentication Port]：AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port]：AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port]：デフォルトの TACACS 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 サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

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

Cisco ISE サーバー登録フェーズ：

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

pxGrid サブスクリプション登録フェーズ：

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

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

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

Cisco AI Network Analytics の設定

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

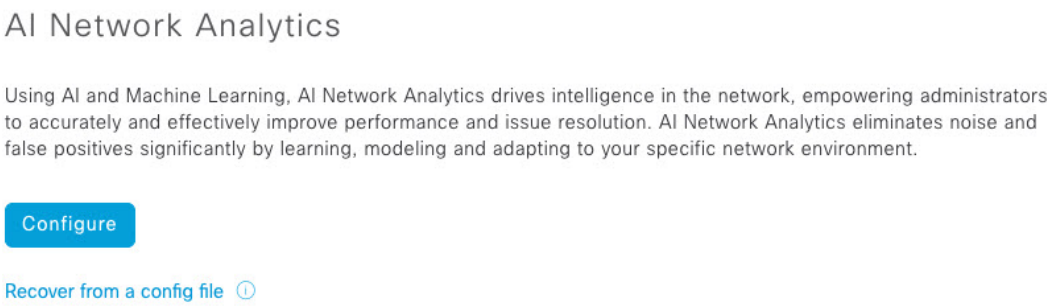
始める前に

- 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 Network Analytics アプリケーションの最新バージョンがインストールされていることを確認してください。アプリケーションの更新のダウンロードとインストール（118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 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
AI ネットワーク分析 ウィンドウが開きます。



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 Network Analytics がインストールされている場合は、次の手順を実行します。
  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開きます。
  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 Network Analytics の復元には数分かかる場合があり、その後、[Success] ダイアログボックスが表示されます。

- Cisco AI Network Analyticsを初めて構成する場合、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。

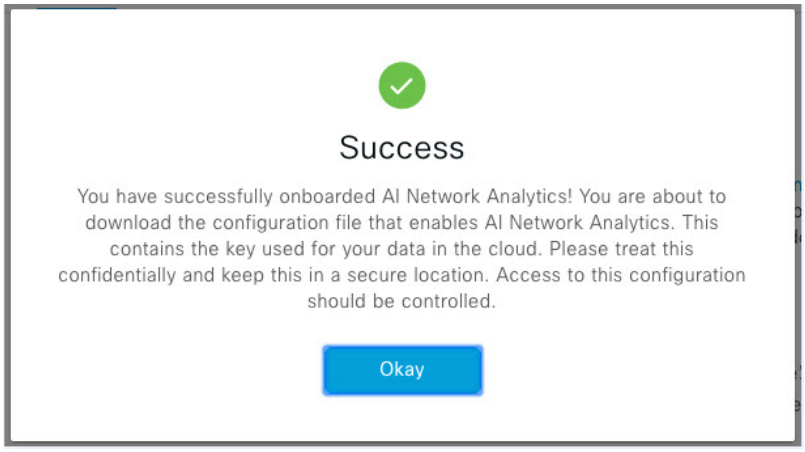
[Testing cloud connectivity...] タブで示されているように、システムはクラウド接続のテストを開始します。クラウド接続のテストが完了すると、[Testing cloud connectivity...] タブが [Cloud connection verified] に変わります。

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 Network Analytics が有効になるまでに数分かかる場合があり、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、[Enable AI Network Analytics] トグルボタンが表示されます。

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。

クライアント証明書の更新

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

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

ディセーブル Cisco AI Network Analytics

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

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
各機能のチェックマーク（☑）は、その機能が有効になっていることを示します。チェックボックスがオフの場合（☐）、機能は無効になっています。

ステップ 3 [AI Network Analytics] 領域で、[Enable AI Network Analytics] トグルボタンをクリックしてオフにします（☐）。

ステップ 4 [Update] をクリックします。

ステップ 5 Cisco AI Network Analytics クラウドからネットワークデータを削除するには、Cisco Technical Response Center（TAC）に連絡してサポートリクエストをオープンします。

ステップ 6 以前の設定が間違っ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は、機械推論ナレッジベースが毎日自動で更新されるようCisco DNA Centerを設定するか、手動で更新することで入手できます。

ステップ 1 メニューアイコン（≡）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に新しいアップデートがある場合は、[Machine Reasoning Knowledge Base] ウィンドウに [AVAILABLE UPDATE] が表示され、アップデートの [Version] と [Details] が示されます。

- [AUTO UPDATE] ：機械推論ナレッジベースが Cisco DNA Center で自動的に毎日更新されます。
- [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY]：自動構成を実行できる CX Cloud と Cisco DNA Center を統合します。この統合により、Cisco DNA Centerのセキュリティアドバイザリツールから直接デバイスの脆弱性を検出する機能が更に強化されました。

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。

ステップ 5 [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY] チェックボックスをオンにして、ネットワークバグ ID およびセキュリティアドバイザリとの Cisco CX Cloud の連携を有効にします。

ステップ 6 [Security Advisories Settings] エリアで、[RECURRING SCAN] トグルボタンをクリックして、毎週の定期的なスキャンを有効または無効にします。

ステップ 7 [CISCO CX CLOUD] トグルボタンをクリックして、Cisco CX Cloud を有効または無効にします。

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ー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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 シスコユーザー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 のログイン情報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、エンドユーザーライセンス契約（EULA）の承認が取り消されます。EULA の承認を再入力する方法については、ライセンス契約書の受諾 （66 ページ）を参照してください。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、ユーザ ロールの概要 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 メニューアイコン（☰）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。

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

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

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

スマートアカウント名にスペースやアンダースコアを使用しないでください。

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

c) [Test Connection] をクリックして Cisco SSM 接続を検証します。

d) [Save] をクリックしてから [Confirm] をクリックします。

e) 変更した SSM で再登録が必要なデバイスがある場合は、[Need to Re-Register Devices] ダイアログボックスが表示されます。ダイアログ ボックスで [OK] をクリックします。

f) **[Tools]** > **[License Manager]** > **[Devices]**のウィンドウで、再度登録するデバイスを選択し、[Finish Connection Mode Changes] をクリックします。

g) [Resync Devices] ダイアログボックスで、次の手順を実行します。

- [Smart Account] を入力します。
- [Virtual Account] を入力します。
- [Now] をクリックしてすぐに再同期を開始するか、[Later] をクリックして特定の時間に再同期をスケジュールします。
- [Resync] をクリックします。

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

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。

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

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** のユーザーのみがこの手順を実行することができます。

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

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

ステップ 1 メニューアイコン（☰）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アカウントを選択できます。

ステップ 4 必要な [IP] または [FQDN] オプションボタンをクリックします。

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

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 [Use as Default Controller Profile] チェックボックスをオンにして、この Cisco DNA Center コントローラを Cisco PnP Connect クラウドポータルにデフォルトコントローラとして登録します。

ステップ 8 [登録（Register）] をクリックします。

PnP イベント通知の作成

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

次の PnP イベントへのイベント通知を作成してください。

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

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

SUPER-ADMIN-ROLE 権限を取得しておきます。

ステップ 1 [System]メニューアイコン（☰）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。

a) 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。

b) **[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。

a) ドロップダウンリストから [Smart Account] を選択します。

b) **[Save]** をクリックします。

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。

ステップ 7 ライセンスを取得したスマートアカウントユーザーとそれに関連する履歴データを削除する場合は、[Delete historical information] をクリックします。

[Delete Historical Data] スライドインペインには、ライセンスを取得したスマートアカウントユーザーが表示されます。また、Cisco DNA Center に現在存在していない既存のスマートアカウントも表示されますが、それらの履歴データは引き続き利用できます。

ステップ 8 [Smart Account list] エリアで、削除するスマートアカウントの横にあるチェックボックスをオンにします。

ステップ 9 [削除（Delete）] をクリックします。

ステップ 10 次の確認ウィンドウで、[Delete] をクリックします。

ステップ 11 [Delete the associated license historical information] チェックボックスをオンにして、関連するライセンスの履歴情報を削除します。

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。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。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）。

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

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 （56 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 メニューアイコン（☰）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にのみ、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したくない場合は、手動で無効にします。詳細については、デバイスの可制御性の設定 （65 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とき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。

デバイスの制御可能性が有効になっている場合、Cisco DNA Centerがユーザーが提供した SNMP 資格情報を介してデバイスに接続できず、デバイス情報を収集できない場合、Cisco DNA Center がユーザーが提供した SNMP 資格情報をデバイスにプッシュします。 SNMPv3 の場合、ユーザーは [Default] グループの下に作成されます。

（注） Cisco AireOS デバイスの場合、ユーザ指定の SNMPv3 パスフレーズには 12 ～ 31 文字が含まれている必要があります。

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 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Device Controllability]**。
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 [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 メニューアイコン（☰）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 [Save] をクリックします。

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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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。

ICMP ping のイネーブル化

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

次の手順では、ICMP ping を有効にする方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[ICMP Ping]** の順に選択します。

ステップ 2 [Enable ICMP ping for unreachable access Points in FlexConnect mode] チェックボックスをオンにします。

ステップ 3 [Save] をクリックします。

イメージ配信サーバの設定

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

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Image Distribution Servers]**。

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

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

ステップ 3 [Add] をクリックして新しいイメージ配信サーバを追加します。

[Add a New Image Distribution Server]slide-in pane が表示されます。

ステップ 4 イメージ配信サーバについて、次の項目を設定します。

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

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

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

• [ポート番号]：イメージ配信サーバーが実行されているポート番号を入力します。

ステップ 5 [Save] をクリックします。

ステップ 6 一部のワイヤレスコントローラの旧バージョンのソフトウェアでは、SFTP の暗号方式として弱い暗号方式（SHA1 ベースの暗号など）しかサポートされていないため、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 サーバーでは、弱い暗号方式のサポートを最大 90 日間まで一時的に有効にすることができます。弱い暗号を許可するには、以下を実行します。

a) SFTP サーバーの IP アドレスの横にある [i] アイコンにカーソルを合わせ、[Click here] をクリックします。

b) [Compatibility Mode] slide-in paneで [Compatibility Mode] チェックボックスをオンにして期間（1 分～ 90 日）を入力します。

c) [Save] をクリックします。

ステップ 7 （任意） 設定を編集するには、対応するイメージ配信サーバーの横にある [Edit] アイコンをクリックし、必要な変更を行って [Save] をクリックします。

ステップ 8 （任意） イメージ配信サーバーを削除するには、イメージ配信サーバーの横にある [Delete] アイコンをクリックし、[Delete] をクリックします。

PnP デバイス許可の有効化

次の手順では、デバイスで許可を有効にする方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** の順に選択します。

ステップ 2 [Device Settings] ドロップダウンリストから [PnP Device Authorization] を選択します。

（注） デフォルトでは、デバイスは自動的に許可されます。

ステップ 3 [Device Authorization] チェックボックスをオンにしてデバイスで許可を有効にします。

ステップ 4 [Save] をクリックします。

デバイスプロンプトの構成

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

カスタムプロンプトの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Device Settings]** > **[Device Prompts]**の順に選択します。

[Device Prompts] ウィンドウが開きます。

ステップ 2 [Create Custom Prompt] をクリックします。

[Create Custom Prompt] スライドインペインが開きます。

ステップ 3 ユーザー名のカスタムプロンプトを作成するには、次の手順を実行します。

1. [Prompt Type] ドロップダウンリストから、[username] を選択します。
2. [Prompt Text] フィールドに、正規表現（Regex）でテキストを入力します。
3. [Save] をクリックします。

ステップ 4 パスワードのカスタムプロンプトを作成するには、次の手順を実行します。

1. [Prompt Type] ドロップダウンリストから、[password] を選択します。
2. [Prompt Text] フィールドに、正規表現（Regex）でテキストを入力します。
3. [Save] をクリックします。

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

ステップ 5 カスタムプロンプトを必要な順序でドラッグアンドドロップします。

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

ステップ 6 編集アイコンをクリックして、カスタムプロンプトを編集します。

ステップ 7 カスタムプロンプトを削除するには、削除アイコンをクリックします。

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

デバイス構成のバックアップ設定の構成

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

（注） デフォルトでは、構成のバックアップは毎週日曜日の午後 11 時 30 分（UTC タイムゾーン）にスケジュールされます。

ステップ 1 メニューアイコン（☰）をクリックして、 **[System]** > **[Settings]** > **[Configuration Archive]** を選択します。

ステップ 2 [Configuration Archive] ウィンドウで、[Internal] タブをクリックします。

ステップ 3 [Number of config drift per device] ドロップダウンリストをクリックし、デバイスごとに保存する構成ドリフトの数を選択します。

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

（注） デフォルトでは、デバイスごとに保存される構成ドリフトの数は 15 です。

ステップ 4 バックアップの日時を選択します。

選択したバックアップの日時は、ネットワークに展開された Cisco DNA Center クラスタのタイムゾーンに基づきます。

ステップ 5 [Save] をクリックします。

バックアップは、スケジュールした後にアクティビティセンターで表示できます。

ステップ 6 [External]タブをクリックして、デバイス構成をアーカイブするための外部サーバーを構成します。詳細については、アーカイブデバイス構成用の外部サーバーの構成 （70 ページ）を参照してください。

アーカイブデバイス構成用の外部サーバーの構成

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

ステップ 1 メニューアイコン（☰）をクリックして、 **[System]** > **[Settings]** > **[Configuration Archive]** を選択します。

ステップ 2 [Configuration Archive] ウィンドウで、[External] タブをクリックします。

ステップ 3 [Add] をクリックして、[External Repository] を追加します。

（注） 追加できる SFTP サーバーは 1 つだけです。

ステップ 4 [Add New External Repository] スライドインペインで、次の詳細を入力します。

a) [Host]：ホストの IP アドレスを入力します。

b) [Root Location]：ルートフォルダの場所を入力します。

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

d) [Backup Format] を選択します。

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

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

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

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

e) バックアップサイクルをスケジュールします。

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

ステップ 5 [Save] をクリックします。

ステップ 6 SFTP サーバーの詳細を編集するには、[Action] 列の編集ボタンをクリックします。

ステップ 7 SFTP サーバーを削除するには、[Action] 列の下にある削除ボタンをクリックします。

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 ワイヤレスコントローラ のクラウドプロビジョニングで表示して使用できます。

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 またはワイヤレスコントローラ 製品に登録し、ターゲットリージョンのイメージ ID を確認します。
- AWS での HA フェールオーバー時に CSR で使用するキーペアを特定します。そのリージョンの CSR をプロビジョニングする際は、このキーペアの名前を 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 （86 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。カタログサーバーからパッケージをダウンロードしてインストールする必要があります。詳細については、アプリケーションの更新のダウンロードとインストール （118 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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/cscrdr/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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 ユーザー。自動的にダウンロードされる場合、値は [System] です。
- [Imported Time]：KGV ファイルがインポートされた時刻。
- [Imported Mode]：ローカルまたはリモートのインポートモード。
- [Records]：処理されたレコード。
- [File Hash]：KGV ファイルのファイルハッシュ。
- [Published]：KGV ファイルの発行日。

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（IPAM）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 IPAM に伝達します。

始める前に

外部 IP アドレスマネージャがセットアップされ、機能していることを確認します。

ステップ 1 メニューアイコン（☰）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 [Server Name] フィールドに、IPAM サーバーの名前を入力します。

ステップ 3 [Server URL] フィールドに、IPAM サーバーの URL または IP アドレスを入力します。

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

a) 警告アイコンをクリックします。

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

b) 証明書の発行者、シリアル番号、および有効期限を確認します。

c) 情報が正しい場合は、チェックボックスをクリックして Cisco DNA Center による IP アドレスへのアクセスを許可し、信頼できない証明書をトラストプールに追加します。

d) [許可（Allowed）] をクリックします。

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

ステップ 5 [Provider] 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] をプロバイダとして選択した場合は、自分のユーザーに、BlueCat アドレスマネージャの API アクセスが許可されていることを確認します。1 人または複数のユーザーの API アクセスを設定する方法に関する詳細については、**BlueCat** のマニュアルを参照してください。

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

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

ステップ 7 [保存（**Save**）] をクリックします。

次のタスク

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

（注） トラストプールでは、証明書はサードパーティの信頼できる証明書として参照されます。

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

Webex 統合の設定

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

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Webex Integration]** の順に選択します。

ステップ 2 [Authenticate to Webex] をクリックします。

ステップ 3 [Cisco Webex] ポップアップウィンドウで、電子メールアドレスを入力し、[Sign In] をクリックします。

ステップ 4 パスワードを入力し、[Sign In] をクリックします。

Webex 認証が正常に完了します。

ステップ 5 [Default Email Domain for Webex Meetings Sign-In] で、Webex ユーザーの電子メールドメインを入力し、[Save] をクリックします。

Webex ドメインは組織全体に適用され、ドメインを使用するすべてのユーザーが会議を主催したり会議に参加したりできます。

ステップ 6 （任意） [Authentication Token] で、[Delete] をクリックして Webex 認証を削除します。

AppX MS-Teams 統合の構成

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

始める前に

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

ステップ 1 メニューアイコン（☰）をクリックして、 **[System]** > **[Settings]** > **[External Services]** > **[Cisco DNA - Cloud]** の順に選択します。

ステップ 2 [Region] ドロップダウンリストから目的の地域を選択します。

ステップ 3 🔍 アイコンをクリックし、名前で検索して、[AppX MS-Teams] を見つけます。

ステップ 4 [Activate] をクリックします。

[Cisco DNA - Cloud] ウィンドウにリダイレクトされます。

ステップ 5 [Cisco DNA - Cloud] ウィンドウで、次の手順を実行します。

a) [Activate application on your product] ウィンドウで、同意フローリンクをクリックして、次の手順を実行します。

- [Sign in to your account] ウィンドウで、Microsoft 管理者のユーザー名とパスワードを入力し、[Sign In] をクリックします。
- [承認（Accept）] をクリックします。

b) [Activate application on your product] ウィンドウで、アクティブ化する製品を選択し、[Next] をクリックします。

新しい製品を登録するには、**こちら**のリンクをクリックして、次の手順を実行します。

- [Host name/IP] フィールドに、製品の IP アドレスを入力します。
- [Name] フィールドに、製品の名前を入力します。
- [Type] フィールドに、製品のタイプを入力します。
- [登録（Register）] をクリックします。

c) Cisco DNA - Cloud が Cisco DNA Center と自動的に同期します。その後、[Choose the Scope for your Cisco DNA Center] ウィンドウにリダイレクトされます。[Next] をクリックします。

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

e) [終了（Exit）] をクリックします。
[Applications] ウィンドウに製品が表示されます。

（注） 製品を非アクティブ化するか、AppX MS-Teams アプリケーションから接続解除する場合は、Cisco DNA - Cloud を使用した AppX MS-Teams 統合の構成 （78 ページ）を参照してください。

Cisco DNA - Cloud を使用した AppX MS-Teams 統合の構成

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

始める前に

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

ステップ 1 cisco.com ログイン情報を使用して [Cisco DNA - Cloud]https://dna.cisco.com/にログインします。

cisco.com ログイン情報がない場合は、作成することができます。

ステップ 2 メニューアイコン（☰）をクリックして、**アプリケーション**。

ステップ 3 [Region] ドロップダウンリストから目的の地域を選択します。

ステップ 4 🔍 アイコンをクリックし、名前で検索して、[AppX MS-Teams] を見つけます。

ステップ 5 [AppX MS-Teams] タイルで、[Activate Product] をクリックします。詳細については、AppX MS-Teams 統合の構成 （76 ページ）を参照してください。

ステップ 6 製品がアクティブ化されたら、[Exit] をクリックします。

ステップ 7 [Applications] ウィンドウにリダイレクトされます。タイル内の緑色のチェックマークは、アプリケーションが接続済みになっていることを示します。

ステップ 8 [AppX MS-Team] タイルをクリックして、[App 360] ウィンドウに詳細を表示します。

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

a) [Product Activations] テーブルで、[Add] をクリックします。

b) アクティブ化する製品を選択し、[Next] をクリックします。

（注） 一度に複数の製品を選択することはできません。

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

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

a) [AppX MS-Teams] タイルをクリックします。

b) [Product Activations] テーブルで、非アクティブ化する製品の横にあるチェックボックスをオンにします。

c) [More Action] ドロップダウンリストから、[Deactivate] を選択します。

d) 確認ウィンドウで、[Deactivate] をクリックします。

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

a) [AppX MS-Teams] タイルをクリックして、[App 360] ウィンドウに詳細を表示します。

b) 上部のメニューバーで、[View all details] をクリックします。
[Details] slide-in pane が表示されます。

c) [Disconnect now] をクリックします。

ThousandEyes の統合の構成

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

始める前に

Cisco Catalyst 9300 および 9400 シリーズスイッチをサポートするアプリケーション ホスティングを介して ThousandEyes エージェントを展開したことを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[ThousandEyes Integration]** の順に選択します。

ステップ 2 [Insert new token here] フィールドに、認証トークンを入力します。

（注） OAuth ベアラートークンを受け取るには、[ThousandEyes] ページに移動します。 https://app.thousandeyes.com/

ステップ 3 [Save] をクリックします。

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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 （121 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 メニューアイコン（☰）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 [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、開始したユーザーを記録するシステムでもあります。監査ログを使用すると、監査用の別のログファイルにシステムの設定変更が記録されます。

ステップ1 メニューアイコン（☰）をクリックして、**[Activities]** > **[Audit Logs]** の順に選択します。

[Audit Logs] ウィンドウが開きます。このウィンドウで、ネットワーク内の現在のポリシーに関するログを表示できます。これらのポリシーは、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。

1. [Time Range] 領域で、[Last 2 Weeks]、[Last 7 Days]、[Last 24 Hours]、または [Last 3 Hours] の時間範囲を選択します。
2. 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。
3. [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 API で使用すると、イベント ID に基づく監査ログメッセージを取得できます。

監査ログの右側のペインに各ポリシーの **[説明（Description）]**、**[ユーザー（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 （任意）[Filter] をクリックして、[User ID]、[Log ID]、または [Description] でログをフィルタリングします。

ステップ 6 [Subscribe] をクリックして監査ログイベントを登録します。

syslog サーバーのリストが表示されます。

ステップ 7 登録する syslog サーバーのチェックボックスをオンにし、[Save] をクリックします。

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

ステップ 8 右側のペインで、[Search] フィールドを使用して、ログメッセージ内の特定のテキストを検索します。

ステップ 9 メニューアイコン（☰）をクリックして、**[Activities]** > **[Scheduled Tasks]** で、OS の更新やデバイスの交換などの予定、進行中、完了および失敗の管理タスクを確認します。

ステップ 10 メニューアイコン（☰）をクリックして、**[Activities]** > **[Work Items]** タブで、進行中、完了、および失敗の作業項目を確認します。

Syslog サーバーへの監査ログのエクスポート

セキュリティに関する推奨事項：より安全で簡単なログモニタリングのために、監査ログを Cisco DNA Center からネットワーク内のリモート Syslog サーバーにエクスポートすることを強く推奨します。

syslog サーバーを複数登録することで、監査ログを Cisco DNA Center から複数の syslog サーバーにエクスポートできます。

始める前に

[System] > **[Settings]** > **[External Services]** > **[Destinations]** > **[Syslog]** 領域で syslog サーバーを設定する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Activities]** > **[Audit Logs]** の順に選択します。

ステップ 2 [**Subscribe**] をクリックします。

ステップ 3 登録する syslog サーバーを選択し、[Save] をクリックします。

ステップ 4 （任意） 登録を解除するには、syslog サーバーの選択を解除し、[Save] をクリックします。

タスクと作業項目の表示

Cisco DNA Center で実行中のタスクと作業項目、完了したタスクと作業項目、および失敗したタスクと作業項目に関する情報を表示できます。

タスクは、ユーザーまたはシステムがスケジュール設定した操作であり、繰り返される可能性があります。

作業項目がある場合、これは、スケジュールどおりに展開する前に完了しなければならない割り当てがあることを意味します。作業項目が完了すると、対応するタスクが作成されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Activities]** > **[Tasks]**の順に選択します。

左側のペインの [SUMMARY] 領域には、次のリストが表示されます。

- [Status]：[Upcoming]、[In Progress]、[Success]、および [Failed] タスク。
- [Last Updated]：過去 [3 Hours]、[24 Hours]、または [7 Days] に更新されたタスク。
- [Categories]：複数のカテゴリに基づいたタスク。一度に複数のカテゴリを選択できます。
- [Recurring]： 定期タスク。

ステップ 2 タスクリンクをクリックして、[Starts]、[Status]、[Last updated]、および今後のタスク、進行中のタスク、完了したタスク、失敗したタスクに関する追加情報を示す slide-in pane を開きます。

ステップ 3 失敗したタスクの slide-in pane で、[Download Error Report] リンクをクリックして、それぞれのタスクのエラーレポートをダウンロードします。

tar ファイルが作成され、ローカルマシンに保存されます。

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

ステップ 4 進行中の作業項目、完了した作業項目、および失敗した作業項目を表示するには、ウィンドウ上部の [Work Items] タブをクリックします。

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 メニューアイコン（☰）をクリックして、**[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。

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

始める前に

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 メニューアイコン（☰）をクリックして、 **[System]** > **[設定]** > **[Integration Settings]** の順に選択します。

ステップ 2 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 3 [Apply] をクリックします。

ログインメッセージの設定

Cisco DNA Center にログインしたすべてのユーザーに表示されるメッセージを設定できます。

始める前に

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

ステップ 1 メニューアイコン（☰）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。

このメッセージは、Cisco DNA Center ログインページの [Log In] ボタンの下に表示されます。

後でこのメッセージを削除する場合は、次の手順を実行します。

1. [Login Message Settings] ページに戻ります。
2. [Clear] をクリックし、[Save] をクリックします。

プロキシの設定

Cisco DNA Center と管理しているネットワークデバイスとの間の仲介として設定されているプロキシサーバーがある場合は、プロキシサーバーへのアクセスを設定する必要があります。

（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ー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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[System Configuration]**の順に選択します。

ステップ 2 [System Configuration] ドロップダウンリストから、**[Proxy]** > **[Outgoing Proxy]**を選択します。

ステップ 3 プロキシ サーバーの URL アドレスを入力します。

ステップ 4 プロキシサーバーのポート番号を入力します。

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

ステップ 5 （オプション）プロキシサーバーが認証を必要とする場合、[Update] をクリックして、プロキシサーバーにアクセスするためのユーザー名とパスワードを入力します。

ステップ 6 [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 7 選択内容を確認し、[Save] をクリックします。

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

プロキシを設定した後、[Proxy] ウィンドウに設定を表示できます。

セキュリティに関する推奨事項

Cisco DNA Centerは、それ自体とモニターおよび管理対象のホスト/ネットワークデバイス用の多数のセキュリティ機能を提供します。セキュリティ機能は、明確に理解して、正しく設定する必要があります。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。
- 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 CenterUpgrade Guide』を参照してください。
- HTTPS プロキシサーバーを使用する 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、ユーザーフィードバックなどを提供したりするように設定されています。これらの目的でインターネット接続を提供することは必須要件です。ただし、HTTPS プロキシサーバーを介して安全な接続を提供します。
- 既知の IP アドレスおよび範囲のみを許可し、未使用のポートへのネットワーク接続をブロックすることにより、ファイアウォールを使用した 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。
- Cisco DNA Center の自己署名サーバー証明書を、内部認証局（CA）によって署名された証明書に置き換えてください。
- 使用しているネットワーク環境で可能な場合は、SFTP 互換モードを無効にします。このモードでは、レガシー ネットワーク デバイスが古い暗号スイートを使用して Cisco DNA Center に接続できます。
- ブラウザベースのアプライアンス設定ウィザードを無効にします。このウィザードには、自己署名証明書が付属しています。
- 最小 TLS バージョンをアップグレードします。 Cisco DNA Center では、TLSv1.1 および TLSv1.2 がデフォルトで有効になっています。使用しているネットワーク環境で可能な場合は、最小 TLS バージョンを 1.2 に設定することを推奨します。詳細については、最小

TLS バージョンの変更と RC4-SHA の有効化（安全でない） （88 ページ）を参照してください。

最小 TLS バージョンの変更と RC4-SHA の有効化（安全でない）

セキュリティに関する推奨事項：Cisco DNA Center の受信用の TLS 接続については、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。

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す。

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、SSL/TLS 接続の RC4 暗号はサポートしません。RC4 暗号には既知の弱点があるため、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しないことを推奨します。

Cisco DNA Center で TLS のバージョンを変更、または RC4-SHA を有効化するには、対応するアプライアンスにログインし、CLI を使用します。

（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。

（注） 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ー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。

次に、例を示します。

```
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 バージョンを以前のバージョンに変更する必要が生じることがあります。

次の例は、TLS バージョン 1.1 から 1.0 に変更する方法を示しています。

```
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
```

次の例は、TLS バージョン 1.1 から 1.2 に変更（RC4-SHA を有効にしていない場合のみ可能）する方法を示しています。

```
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 Cisco DNA Center と Catalyst 9000 デバイス間のストリーミングテレメトリ接続（TCP 25103 ポート経由）用の 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 管理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る場合は、現在の TLS バージョンを以前のバージョンに変更する必要が生じることがあります。

次の例は、TLS バージョン 1.1 から 1.2 に変更する方法を示しています。

```
Input
$ magctl service tls_version --tls-min-version 1.2 -a assurance-backend collector-iosxe-db
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.apps/collector-iosxe-db patched
```

ステップ 6 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。

次の例は、TLS バージョン 1.2 が有効になっていないことを示しています。

```
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 7 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。

次に、例を示します。

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

（注） 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 8 以前に有効にした RC4-SHA 暗号を無効にするには、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 9 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ー独自の証明書を使って、適切にプロビジョニングされた PKI トラストストアを保有する必要があります。

PnP検出/サービスによってデバイスのオンボード中にそのようなプロキシが配置されている場合は、ネットワークデバイスが安全に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サーバー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 （121 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 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[System Configuration]**の順に選択します。

ステップ2 [System Configuration] ドロップダウンリストから、**[Proxy]** > **[Incoming Proxy]** を選択します。

ステップ3 [Proxy Certificate] ウィンドウで、（存在する場合は）現在のプロキシゲートウェイ証明書のデータを表示します。

（注） [Expiration Date and Time] は、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ヵ月前に、Cisco DNA Centerの GUIにシステム通知が表示されます。

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

（注） PEMまたはDERファイル（公開キー暗号化標準のファイル形式）だけが、この領域を使用して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5 **[保存（Save）]** をクリックします。

ステップ6 [Proxy Certificate] ウィンドウを更新し、更新されたプロキシゲートウェイ証明書のデータを表示します。

[Proxy Certificate] ウィンドウに表示された情報は、新しい証明書名、発行者、および証明機関を反映するように変更する必要があります。

ステップ 7 プロキシゲートウェイ証明書の機能を有効にするには、[Enable] ボタンをクリックします。

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

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

SSL インターセプトプロキシ証明書のアップロード

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ーで SSL 復号が有効になっている場合、正式な認証局から発行された証明書を使用してプロキシが構成されていることを確認してください。プライベート証明書を使用している場合は、次の手順を実行します。

（注） セキュリティを強化するため、ルートシェルへのアクセスは Cisco DNA Center で無効になっています。制限付きシェルでは、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできないため、運用上のリスクが軽減されます。ただし、このセクションのコマンドを使用するには、Cisco TACに連絡して、ルートシェルに一時的にアクセスする必要があります。 制限付きシェルについて （107 ページ）を参照してください。

ステップ 1 プロキシサーバーの証明書（.pem 形式）を Cisco DNA Center サーバーの `/home/maglev` ディレクトリに転送します。

ステップ 2 maglev ユーザーとして Cisco DNA Center サーバーに SSH で接続し、次のコマンドを入力します。*<proxy.pem>* は、プロキシサーバーの TLS/SSL 証明書ファイルです。

```
$ sudo /usr/local/bin/update_cacerts.sh -v -a /home/maglev/<proxy.pem>
```

このコマンドは、次のような出力を返します。

```
Reading CA cert from file /tmp/sdn.pem
Adding certificate import_1E:94:6D:2C:81:22:BB:B2:2E:24:BD:72:57:AE:35:AD:EC:5E:71:44.crt
Updating /etc/ca-certificates.conf
Updating certificates in /etc/ssl/certs…
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d…
done.
Deleting tempfiles /tmp/file0PpQxV /temp/filePtmQ8U /tmp/filercR3cV
```

ステップ 3 コマンド出力で、「1 added」の行を探し、追加された数がゼロでないことを確認します。チェーン内の証明書に基づき、この数は 1 または 1 を超える場合があります。

ステップ 4 次のコマンドを入力して、docker およびカタログサーバーを再起動します。

```
sudo systemctl restart docker
magctl service restart -d catalogserver
```

ステップ 5 Cisco DNA Center GUI からクラウド接続を確認します。

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。ユーザー自身のキー管理システムで秘密キーを保護してください。秘密キーのモジュラスサイズは最小でも 2048 ビット必要です。

Cisco DNA Center 2.3.4.x 以前の場合、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。Cisco DNA Center 2.3.4.x 以前では、証明書チェーンに関連付けられたリーフ証明書を含む ECDH および ECDSA の形式はサポートされません。

Cisco DNA Center 2.3.5 以降では、すべてのキータイプがサポートされます。

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、プラグアンドプレイ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に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 のルート証明書が一緒に、インポートされる単一のファイルに追加される必要があります。これらの証明書を追加する場合は、認定の実際のチェーンと同じ順序で追加する必要があります。

次の証明書は、単一の PEM ファイルに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が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） 内部認証局（CA）による署名入りの証明書をインストールする場合は、Cisco DNA Center へのアクセスに使用するすべての DNS 名（Cisco DNA Center の FQDN を含む）が証明書の **alt_names** セクションで指定されていることを確認してください。詳細については、『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 サーバー証明書の更新

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 [Certificates] 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 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[System Certificates]** の順に選択します。

ステップ 2 [System] タブで、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） 有効期限の日時は、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 か月前に、Cisco DNA Center の GUI にシステム通知が表示されます。

[System] タブには次のフィールドが表示されます。

- [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。
- [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 [System Certificate] ウィンドウで、[Replace Certificate] をクリックします。

Cisco DNA Center 2.3.2 以降では、初めて CSR を生成する場合に、[Generate New CSR] リンクが表示されます。それ以外の場合は、[Download existing CSR] リンクが表示されます。既存の CSR をダウンロードしてプロバイダーに送信し、証明書を生成できます。既存の CSR を使用しない場合は、[Delete existing CSR] をクリックし、次の [Confirmation] ウィンドウで [Accept] をクリックします。[Generate New CSR] リンクが表示されます。

ステップ 4 [Generate New CSR] リンクをクリックします。

ステップ 5 [Certificate Signing Request Generator] ウィンドウで、必須フィールドに情報を入力します。

ステップ 6 [新規 CSR の生成（Generate New CSR）] をクリックします。

生成された新しい CSR は自動的にダウンロードされます。

[Certificate Signing] ウィンドウには、CSR のプロパティが表示され、次のことができます。

- CSR プロパティをプレーンテキストでコピーします。
- Base64 をコピーして MS CA に貼り付けます。
- Base64 をダウンロードします。

ステップ 7 （任意）ディザスタリカバリに同じ証明書を使用する場合は、[Use system certificate for Disaster Recovery as well] チェックボックスをオンにします。

ステップ 8 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 エンハンスト 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。

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

ステップ 9 証明書発行元から p7b で証明書の完全なチェーン（サーバーおよびCA）が提供されていることを確認します。不明な場合は、次の手順を実行し、チェーンを確認して組み立てます。

a) p7b バンドルを DER 形式でダウンロードし、dnac-chain.p7b として保存します。
b) dnac-chain.p7b 証明書を Cisco DNA Center クラスタに SSH を介してコピーします。
c) 次のコマンドを入力します。

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

d) すべての証明書が出力に記載され、発行者と Cisco DNA Center 証明書が含まれていることを確認します。PEM としてアップロードを続行します。証明書がルーズファイルにある場合は、次の手順を実行して、個々のファイルをダウンロードして組み立てます。

ステップ 10 証明書発行元からルーズファイルで証明書とその発行元 CA チェーンが提供された場合は、次の手順を実行します。

a) PEM（base64）ファイルを収集するか、openssl を使用して DER を PEM に変換します。
b) 証明書とその発行元 CA を連結し、証明書から下位 CA に続いてルート CA までを dnac-chain.pem ファイルに出力します。

cat certificate.pem subCA.pem rootCA.pem > dnac-chain.pem

c) PEM としてアップロードを続行します。

ステップ 11 [PEM] ファイルの場合、次のタスクを実行します。

- [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）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

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

（注） 秘密キーには、有効な秘密キー形式の拡張子（.key）が必須です。秘密キーの最大ファイルサイズは 10 MB です。

アップロードに成功すると、秘密キーが検証されます。

- 秘密キーの [Encrypted] 領域から、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ワードを入力します。

ステップ 12 [PKCS] ファイルの場合、次のタスクを実行します。

- [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 または .p12）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

- [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、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 13 **[Save]** をクリックします。

（注） Cisco DNA Center サーバーの SSL 証明書が置き換えられると、自動的にログアウトされるため、再度ログインする必要があります。

ステップ 14 [Certificates] ウィンドウに戻り、更新された証明書データを確認します。
[System] タブ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。

外部 SCEP ブローカーの使用

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

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

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[PKI Certificates]** の順に選択します。

ステップ 2 [PKI Certificates] ウィンドウで、[Use external SCEP broker] オプションボタンをクリックします。

ステップ 3 外部証明書をアップロードするには、次のいずれかのオプションを使用します。

- ファイルを選択する
- ドラッグアンドドロップしてアップロードする

（注） .pem、.crt、.cer などのファイルタイプのみ使用できます。ファイルサイズは 10 MB を超えることはできません。

ステップ 4 [Upload] をクリックします。

ステップ 5 デフォルトでは、[Manages Device Trustpoint] が有効になっています。つまり、デバイスで sdn-network-infra-iwan トラストポイントが設定されます。Cisco DNA Center次の手順を実行してください。

a) デバイスが SCEP 経由で証明書を要求する登録 URL を入力します。

b) （任意）証明書で使用される任意のサブジェクトフィールド（国、地域、州、組織、組織単位など）を入力します。共通名（CN）は、デバイスのプラットフォーム ID とデバイスのシリアル番号を使用して Cisco DNA Center によって自動的に設定されます。

c) [Revocation Check] フィールドで、ドロップダウンリストをクリックし、適切な失効チェックオプションを選択します。

d) （任意）[Auto Renew] チェックボックスをオンにして、自動登録の割合を入力します。

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

ステップ 6 **[保存（Save）]** をクリックします。

外部 CA 証明書がアップロードされます。

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

内部 PKI 証明書への切り替え

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

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[PKI Certificates]** の順に選択します。

ステップ 2 [PKI Certificates] ウィンドウで、[Use Cisco DNA Center] オプションボタンをクリックします。

ステップ 3 [Switching back to Internal PKI Certificate] アラートで、[Apply] をクリックします。

[Settings have been updated] メッセージが表示されます。詳細については、「PKI 証明書のロールをルートから下位に変更」を参照してください。.

Cisco DNA Center PKI 証明書のエクスポート

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

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[PKI Certificates]** の順に選択します。

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

証明書の管理

デバイス証明書の管理

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

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Device Certificate]** の順に選択します。

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

- [Expired] ステータスタブ：有効期限が切れた証明書のリストを表示します。
- [Expiring] ステータスタブ：有効期限が近づいている証明書のリストを昇順で表示します。
- [All] ステータスタブ：有効な証明書、期限切れの証明書、および期限切れ間近の証明書のリストを表示します。
- [Revoked] ステータスタブ：取り消された証明書を表示します。

ステップ 2 [Device Name] と [Issue To] の値に基づいて、証明書をフィルタリングできます。

ステップ 3 有効な証明書を取り消す場合は、次の手順を実行します。

a) [All] ステータスタブをクリックします。
b) [Actions] 列で、取り消す証明書に対応する [Revoke] アイコンをクリックします。
c) 確認ウィンドウで、[OK] をクリックします。

ステップ 4 証明書の詳細をエクスポートする場合は、[Export] をクリックします。

証明書の詳細が CSV 形式でエクスポートされます。

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。

ステップ 1 メニューアイコン（≡）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Device Certificate]** の順に選択します。

ステップ 2 デバイス証明書と現在のデバイス証明書の有効期間を確認します。

ステップ 3 [Device Certificate] ウィンドウで、[Modify] をクリックします。

ステップ 4 [Device Certificate Lifetime] ダイアログボックスに、新しい値を入力します（日数）。

ステップ 5 [Save] をクリックします。

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、サーバーとクライアントの間の接続の確立と保護に使用される証明書やキーを管理します。デバイス PKI CA 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。

[PKI Certificate Management] ウィンドウの GUI を使用して、プライベート（内部）Cisco DNA Center CA のロールをルート CA から下位 CA に変更できます。このロールを変更する際は、次の手順を実行します。

- 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 から下位 CA への切り替え前にデバイスの制御可能性が有効になっている場合（デフォルト）、新しいデバイス証明書は自動的に更新されます。
- 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同じ時間に GUI で見ると、証明書の有効期間は 1 年間と表示されます。
- 下位 CA 証明書として 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。

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 メニューアイコン（☰）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。

次に例を示します。

- ルート CA から下位 CA に変更するプロセスは元に戻すことができません。
- ルート CA モードで登録された、または証明書が発行されたネットワーク デバイスがないことを確認する必要があります。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す。

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す。

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、ユーザー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（100 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す。
- 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 メニューアイコン（☰）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。

デバイス証明書トラストポイントの設定

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

SCEP を介して外部 CA から登録するには、次の手動設定が必要です。

ステップ 1 次のコマンドを入力します。

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

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

```
auto-enroll 80 regenerate
```

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

```
source interface <interface>
```

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 メニューアイコン（☰）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。

制限付きシェルについて

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

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

必要に応じて、次の限定されたリストのコマンドを使用できます。

```
$ ?
Help:
  cat                  concatenate and print files in restricted mode
  clear                clear the terminal screen
  date                 display the current time in the given FORMAT, or set the system
date
  debug                enable console debug logs
  df                   file system information
  dmesg                print or control the kernel ring buffer.
  du                   summarize disk usage of the set of FILEs, recursively for
directories.
  free                 quick summary of memory usage
  history              enable shell commands history
  htop                 interactive process viewer.
  ip                   print routing, network devices, interfaces and tunnels.
  last                 show a listing of last logged in users.
  ls                   restricted file system view chrooted to maglev Home
  lscpu                print information about the CPU architecture.
  magctl               tool to manage a Maglev deployment
  maglev               maglev admin commands
  maglev-config        tool to configure a Maglev deployment
  manufacture_check    tool to perform manufacturing checks
  netstat              print networking information.
  nslookup             query Internet name servers interactively.
  ntpq                 standard NTP query program.
  ping                 send ICMP ECHO_REQUEST to network hosts.
  ps                   check status of active processes in the system
  rca                  root cause analysis collection utilities
  reboot               Reboot the machine
  rm                   delete files in restricted mode
  route                print the IP routing table.
  runonce              Execute runonce scripts
  scp                  restricted secure copy
  sftp                 secure file transfer
```

```
shutdown            Shutdown the machine
ssh                 OpenSSH SSH client.
tail                Print the last 10 lines of each FILE to standard output
top                 display sorted list of system processes
traceroute          print the route packets trace to network host.
uname               print system information.
uptime              tell how long the system has been running.
vi                  text editor
w                   show who is logged on and what they are doing.
```

製品使用状況テレメトリの収集について

Cisco DNA Center ではデフォルトでテレメトリデータが収集されますが、一部のデータ収集をオプトアウトできます。データ収集は、製品機能の開発を支援し、運用上の問題に対処して、より優れた価値と投資回収率（ROI）を実現することを目的としています。シスコが収集するデータの種類は、Cisco.com ID、システム、機能の使用状況、ネットワーク デバイス インベントリ、およびソフトウェア利用資格です。収集されるデータの詳しいリストについては、「*Cisco DNA Center* のデータシート」を参照してください。一部のデータ収集をオプトアウトするには、シスコのアカウント担当者および Cisco Technical Assistance Center（TAC）にお問い合わせください。

メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Terms and Conditions]** > **[Telemetry Collection]** の順に選択します。[Telemetry Collection] ウィンドウから、ライセンス契約、プライバシーポリシー、プライバシーデータシートを確認できます。

vManage プロパティの設定

Cisco DNA Center は、統合 vManage 設定を使用して Cisco 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] ウィンドウで vManage の詳細を保存できます。

ステップ 1 メニューアイコン（☰）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 [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、ユーザーによるログインの試行、アカウントのロックアウト期間、ログインの再試行回数を管理できます。

ステップ 1 メニューアイコン（☰）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] にカーソルを合わせると、各パラメータの詳細が表示されます。

ステップ 4 ドロップダウンリストから [Idle Session Timeout] の値を選択します。

ステップ 5 [保存（**Save**）] をクリックします。

セッションをアイドル状態のままにすると、セッションタイムアウトの 5 分前に [Session Timeout] ダイアログボックスが表示されます。セッションを続行する場合は、[Stay signed in] をクリックします。[Sign out] をクリックすると、すぐにセッションを終了できます。

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、以下を管理できます。

- パスワードの有効期限の通知間隔。
- パスワードが期限切れになる前にユーザーに通知が表示される日数。
- 猶予期間。

ステップ 1 メニューアイコン（☰）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] にカーソルを合わせると、各パラメータの詳細が表示されます。

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。

IP アクセス制御

IP アクセス制御を使用すると、ホストまたはネットワークの IP アドレスに基づいて Cisco DNA Center へのアクセスを制御できます。Cisco DNA Center では、IP アクセス制御に次のオプションがあります。

- すべての IP アドレスに Cisco DNA Center へのアクセスを許可します。デフォルトでは、すべての IP アドレスが Cisco DNA Center にアクセスできます。
- 選択した IP アドレスのみに Cisco DNA Center へのアクセスを許可します。

IP アクセス制御の構成

IP アクセス制御を構成し、選択した IP アドレスのみに Cisco DNA Center へのアクセスを許可するには、次の手順を実行します。

1. IP アクセス制御の有効化 （110 ページ）
2. IP アクセスリストへの IP アドレスの追加 （111 ページ）
3. （任意） IP アクセスリストからの IP アドレスの削除 （112 ページ）

IP アクセス制御の有効化

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [リストされている IP アドレスのみに接続を許可する（Allow only listed IP addresses to connect）] オプションボタンをクリックします。

ステップ 3 [Add IP List] をクリックします。

ステップ 4 [Add IP] スライドインペインの [IP Address] フィールドに、IPv4 アドレスを入力します。

（注） IP アドレスを IP アクセスリストに追加しないと、Cisco DNA Center にアクセスできなくなる可能性があります。

ステップ 5 [Subnet Mask] フィールドにサブネット マスクを入力します。

サブネットマスクの有効範囲は 0 ～ 32 です。

ステップ 6 [Save] をクリックします。

IP アクセスリストへの IP アドレスの追加

IP アクセスリストに IP アドレスを追加するには、次の手順を実行します。

始める前に

IP アクセス制御が有効になっていることを確認してください。詳細については、IP アクセス制御の有効化 （110 ページ）を参照してください。

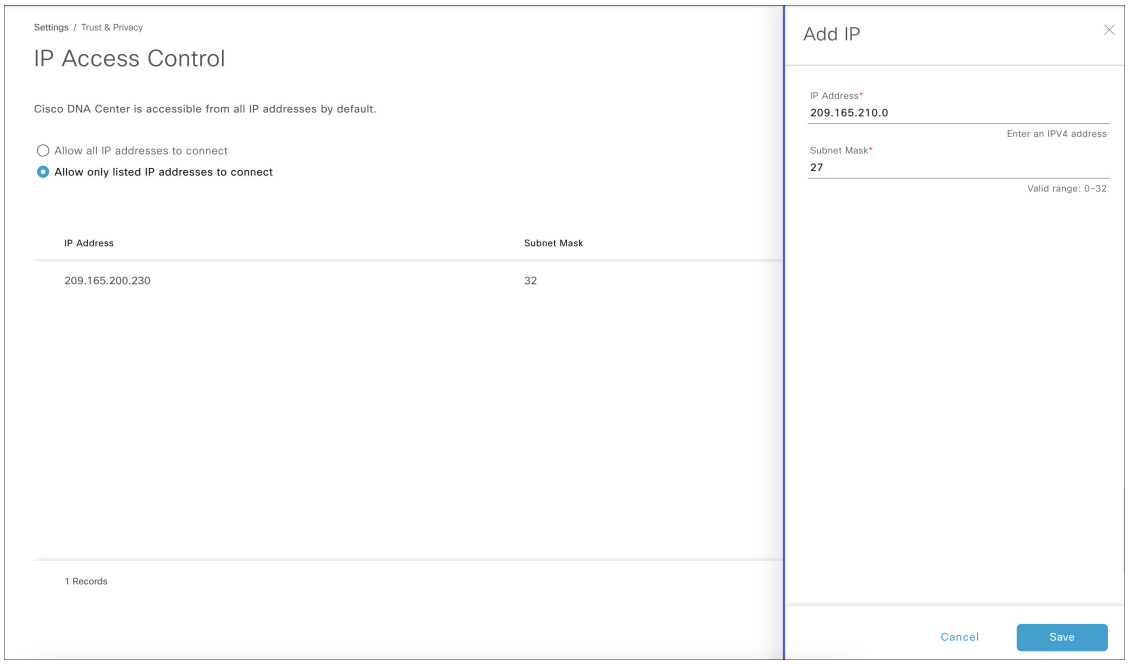
ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Add IP] スライドインペインの [IP Address] フィールドに、ホストまたはネットワークの IPv4 アドレスを入力します。

ステップ 4 [Subnet Mask] フィールドにサブネット マスクを入力します。

サブネットマスクの有効範囲は 0 ～ 32 です。



ステップ 5 [Save] をクリックします。

IP アクセスリストからの IP アドレスの削除

IP アクセスリストから IP アドレスを削除して Cisco DNA Center へのアクセスを無効にするには、以下の手順を実行します。

始める前に

IP アクセスコントロールを有効にして、IP アドレスを IP アクセスリストに追加したことを確認します。詳細については、IP アクセス制御の有効化（110 ページ）および IP アクセスリストへの IP アドレスの追加（111 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [Action] 列で、対応する IP アドレスの [Action] アイコンをクリックします。

ステップ 3 [Delete] をクリックします。

IP アクセス制御の無効化

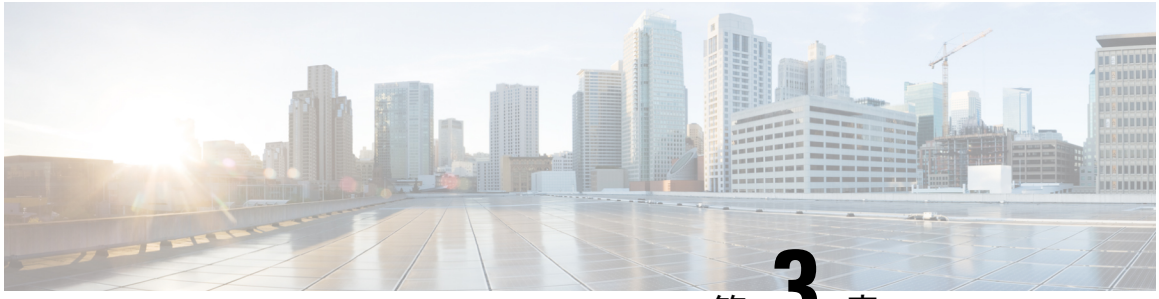
IP アクセス制御を無効化し、すべての IP アドレスに Cisco DNA Center へのアクセスを許可するには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を取得しておきます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[IP Access Control]** の順に選択します。

ステップ 2 [Allow all IP addresses to connect] オプションボタンをクリックします。



第 3 章

アプリケーションの管理

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、ユーザーは設定に応じて、必要なアプリケーションをインストールして実行し、使用していないアプリケーションをアンインストールできます。

[Software Management] ウィンドウに表示されるアプリケーションパッケージの数とタイプは、Cisco DNA Center のバージョンおよび Cisco DNA Center 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。パッケージの説明については、[Currently Installed Applications] リンクをクリックし、その名前の上にカーソルを置きます。

各 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、この方法はお勧めしません。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。

最新のシステムバージョンのダウンロードとインストール

[Software Management] ウィンドウには、最新の Cisco DNA Center バージョンがいつ利用可能であるかが示されます。最新バージョンをダウンロードしてインストールするには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、「ユーザ ロールの概要 （121 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Software Management]** の順に選択します。

重要 この時点で、Cisco DNA Center によって接続性チェックが実行されます。接続に問題がある場合、[Software Management] ウィンドウに、現在利用可能なシステムアップデートは表示されません。

ステップ 2 システムアップデートが利用可能であることがウィンドウに示されている場合は、[Download now] をクリックします。

ステップ 3 Cisco DNA Center の事前チェック完了後、[Download] をクリックします。

ステップ 4 パッケージのダウンロード完了後、[Install now] をクリックします。

ステップ 5 Cisco DNA Center の事前チェック完了後、[Install] をクリックします。

ステップ 6 Cisco DNA Center はメンテナンスモードになり、システムアップデートが実行されるため使用できません。アップデートが完了したら、Cisco DNA Center に再度ログインします。

ステップ 7 メニューアイコン（☰）をクリックして、**[System]** > **[Software Management]**をクリックして、[Software Management] ウィンドウを再度開きます。

ウィンドウの上部にあるメッセージは、システムが最新であることを示しています。

以前のシステムバージョンのダウンロードとインストール

最新バージョン以外の使用可能な Cisco DNA Center バージョンをダウンロードしてインストールする場合は、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。詳細については、「ユーザ ロールの概要 （121 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Software Management]** の順に選択します。

ステップ 2 [Looking for other releases?] フィールドで、[Click here] リンクをクリックします。

ステップ 3 Cisco DNA Center のダウンロードするバージョンのラジオボタンをクリックし、[Select] をクリックします。

（注） 現在インストールされているバージョンを確認するには、[Installed version] フィールドを参照してください。

ステップ 4 Cisco DNA Center の事前チェック完了後、[Download] をクリックします。

プロセスが実行されると、ダウンロードの全体的な進行状況が更新されます。[More details] リンクをクリックして、システムにダウンロードされている個々のアプリケーションの進行状況を表示するスライドインペインを開きます。

ダウンロードが完了すると、[Software Management] ウィンドウが更新され、以前の Cisco DNA Center バージョンをインストールできることが示されます。

ステップ 5 [Available installations] リンクをクリックします。

ステップ 6 インストールするバージョンのラジオボタンをクリックし、[Select] をクリックします。

ステップ 7 Cisco DNA Center の事前チェック完了後、[Install] をクリックします。

プロセスが実行されると、インストールの全体的な進行状況が更新されます。[More details] リンクをクリックして、システムにインストールされている個々のアプリケーションの進行状況を表示するスライドインペインを開きます。

ステップ 8 インストールの完了後にプロンプトが表示されたら、[Refresh] をクリックして [Software Management] ウィンドウを更新します。

アプリケーションの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す。具体的には、アプリケーションの個別のパッケージをインストールして、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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Software Management]** の順に選択します。

重要 この時点で、Cisco DNA Center によって接続性チェックが実行されます。接続に問題がある場合、[Software Management] ウィンドウに、現在利用可能なシステムアップデートは表示されません。

ステップ 2 アプリケーション更新が利用可能な場合は、ウィンドウの下部に表示されます。次のいずれかを実行します。

1. 利用可能なすべてのシステムアップデートをインストールするには、[Select All] リンクをクリックします。
2. 個々のアプリケーション更新をインストールするには、該当するチェックボックスをオンにします。

（注） [More details] リンクをクリックすると、該当するアプリケーションのファイルサイズと簡単な説明を記したスライドインペインが開きます。

ステップ 3 [Install] をクリックします。

ステップ 4 Cisco DNA Center による依存関係のチェックが完了したら、[Continue] をクリックします。

更新中の各アプリケーションの進行状況バーがウィンドウに表示されます。すべての更新がインストールされると、[Software Management] ウィンドウが更新されます。

ステップ 5 [Currently Installed Applications] リンクをクリックし、選択したアプリケーションが更新されていることを確認します。

パッケージのダウンロードとアップグレードのイベント通知

パッケージのダウンロードまたはアップグレードイベントが発生するたびに通知を受信できます。これらの通知を設定および登録するには、『Cisco DNA Center Platform User Guide』の「*Work with Event Notifications*」トピックで説明されている手順を実行してください。この手順

を完了したらSYSTEM-SOFTWARE-UPGRADEイベントを選択し、サブスクライブしていることを確認します。

次の場合に通知が生成され、送信されます。

- パッケージのアップグレードのダウンロードに失敗しました。これは通常、Cisco DNA Centerアプライアンスに必要なディスク容量がないか、破損したパッケージをダウンロードしようとしているために発生します。
- パッケージのアップグレードのインストールに失敗しました（パッケージに関連付けられているサービスが現在ダウンしているためと考えられます）。
- パッケージのアップグレードのダウンロードまたはインストールが成功しました。

（注） 通知は、以前にこの操作を完了するために行った試行が失敗した場合にのみ送信されます。

アプリケーション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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Software Management]** の順に選択します。

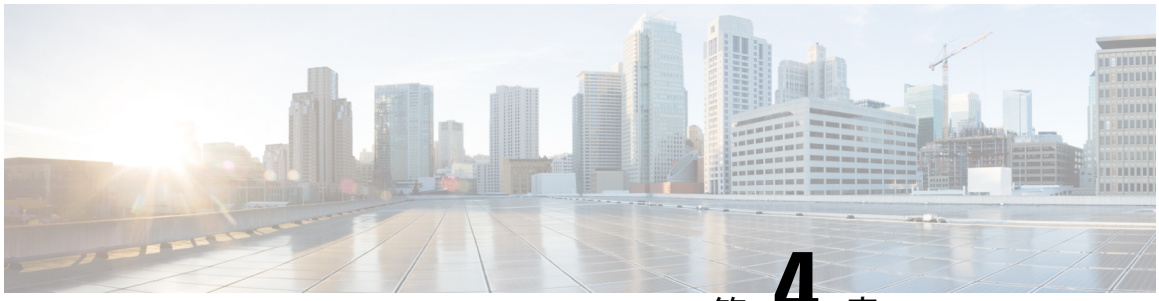
ステップ 2 [Currently Installed Applications] リンクをクリックして、Cisco DNA Center アプライアンスにインストールされているすべてのアプリケーションを表示します。

ステップ 3 削除するパッケージで、[Uninstall] リンクをクリックします。

（注） 同時に複数のパッケージをアンインストールすることはできません。

ステップ 4 [Uninstall] をクリックして、アプリケーションを削除することを確認します。

Cisco DNA Center はアプリケーションが削除された後にメッセージを表示します。



第 4 章

ユーザの管理

ユーザー プロファイルについて

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

ユーザー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。内部ユーザープロファイルは Cisco DNA Center に配置され、外部ユーザープロファイルは外部 AAA サーバーに配置されます。

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ー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。

内部ユーザーの作成

ユーザーを作成し、このユーザー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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 新しいユーザーの姓、名、電子メールアドレス、およびユーザー名を入力します。

電子メールアドレスは、標準の Apache EmailValidator クラスの要件を満たしている必要があります。

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 パスワードを入力し、確認します。パスワードの要件：

- 最低 8 文字
- 次のカテゴリのうち少なくとも 3 つのカテゴリに属する文字：
  - 小文字の英字
  - 大文字の英字
  - 番号（Number）
  - 特殊文字

ステップ 6 [Save] をクリックします。

ユーザーの編集

一部のユーザープロパティは編集できますが、ユーザー名は編集できません。

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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 編集するユーザー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 必要に応じて、姓名または電子メールアドレスを編集します。

ステップ 5 [Role List] で、必要に応じて新しいロール（[SUPER-ADMIN-ROLE]、[NETWORK-ADMIN-ROLE]、または [OBSERVER-ROLE]）を選択します。

ステップ 6 [Save] をクリックします。

ユーザーの削除

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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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 削除するユーザー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。

ユーザーパスワードのリセット

別のユーザーのパスワードをリセットできます。

セキュリティ上の理由から、パスワードは、どのユーザーに対しても（管理者権限を持つユーザーに対しても）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 （121 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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ー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。新しいパスワードの要件：

- 最低 8 文字
- 次のカテゴリのうち少なくとも 3 つのカテゴリに属する文字：
  - 小文字の英字
  - 大文字の英字
  - 番号（Number）
  - 特殊文字

ステップ 5 [Save] をクリックします。

自身のユーザーパスワードの変更

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」を参照してください。

ステップ 1 メニューアイコン（☰）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。

管理者権限なしでのユーザーパスワードの変更

次の手順では、管理者権限なしでパスワードを変更する方法について説明します。

ステップ 1 メニューアイコンをクリックし、[admin] にカーソルを合わせて、**[My Profile and Settings]** > **[My Account]** の順に選択します。

ステップ 2 [パスワードを更新（Update Password）] をクリックします。

ステップ 3 現在のパスワード、新しいパスワードを入力し、パスワードを確認入力します。

ステップ 4 [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ーが作成されているかどうかを確認するには、次のコマンドを入力します。

```
magctl user display <username>
```

このコマンドは、パスワードをリセットするために使用できるテナント名を返します。出力は、次のようになります。

```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```

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 権限を持つユーザーは、特定の Cisco DNA Center 機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

カスタムロールを定義し、定義したロールにユーザーを割り当てるには、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) メニューアイコン（☰）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、ユーザーを新しいロールに割り当てるように求められます。

c) タスクの概要ウィンドウが開いたら、[Let's do it] をクリックして、ワークフローに直接移動します。
[Create a New Role] ウィンドウが開きます。

d) ロール名を入力し、[Next] をクリックします。
[Define the Access] ウィンドウが開き、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ーは該当する機能を GUI で表示できなくなります。

g) [Next] をクリックします。
[Summary] ウィンドウが開きます。

h) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。
[Done, Role-Name] ウィンドウが開きます。

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

[User Management] > **[Internal Users]** ウィンドウが開きます。このウィンドウでは、カスタムロールを既存のユーザーまたは新規ユーザーに割り当てることができます。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。

  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ー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開きます。

  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ーに割り当てるには、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開きます。

  2. 表示されるフィールドに氏名とユーザー名を入力します。

  3. [Role List] ドロップダウンリストから、新規ユーザー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. [Save] をクリックします。

ステップ 3 既存のユーザーのログイン中に管理者がそのユーザーのアクセス権限を更新した場合、新しい権限設定を有効にするには、ユーザーが 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 ユーザー ロール権限

表 *6 : Cisco DNA Center* ユーザー 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。
モニターリングおよびトラブルシューティング	問題のトラブルシューティングと修復、プロアクティブなネットワークモニタリング、および AI ネットワーク分析 から得られるインサイトにより、ネットワークの正常性のモニタリングと管理を行います。 このロールでは次のことが可能です。 • 問題の解決、クローズ、無視。 • 機械推論エンジン（MRE）のワークフローの実行。 • トレンドとインサイトの分析。 • パストレース、センサーダッシュボード、不正管理などの問題のトラブルシューティング。 • 不正および Cisco Advanced Wireless Intrusion Prevention System（aWIPS）のワークフローの実行。これらのワークフローには、AP 許可リスト、ベンダー許可リスト、aWIPS プロファイルの作成、aWIPS プロファイルの割り当てなどが含まれます。
モニターリングの設定（Monitoring Settings）	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。 注：[Monitoring and Troubleshooting] に対する読み取りアクセス許可が最低限必要です。
トラブルシューティング ツール	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。 注：[Monitoring and Troubleshooting] に対する読み取りアクセス許可が最低限必要です。
ネットワーク分析	ネットワーク分析関連のコンポーネントを管理します。

機能	説明
データアクセス	クエリエンジン API へのアクセスを有効にします。グローバル検索、不正管理、aWIPS などの制御機能。 注：許可を [Deny] に設定すると、検索と アシュアランス 機能に影響します。
ネットワーク設計	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。
詳細ネットワーク設定	• グローバルデバイスログイン情報、認証サーバーとポリシーサーバー、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。 • 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。 （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。
イメージリポジトリ	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。
ネットワーク階層	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ーは、**[System]** > **[Settings]** で CMX サーバーを追加することもできます。
ネットワーク プロファイル	ルーティング、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ます。サイトへプロファイルを割り当てます。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ーは、**[System]** > **[Settings]** で SFTP サーバー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、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。

機能	説明
EoX	ネットワーク内のハードウェアおよびソフトウェアの [End of Life]、[End of Sales]、または [End of Support] に関連する公開情報の詳細について、ネットワークをスキャンします。
イメージの更新	完全なアップグレードライフサイクルの後で、ゴールデンイメージ設定に一致しないデバイスのソフトウェアイメージを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：デバイスを交換するには、**[Network Provision]** > **[PnP]** に対する書き込み権限が必要です。
[Inventory Management] > [Device Configuration]	デバイス設定：デバイスの実行構成を表示します。
[Inventory Management] > [Discovery]	ディスカバリ：ネットワーク内の新しいデバイスを検出します。
[Inventory Management] > [Network Device]	ネットワークデバイス：インベントリからデバイスを追加し、デバイスの詳細を表示し、デバイスレベルのアクションを実行します。
[Inventory Management] > [Port Management]	ポート管理：デバイスでポートアクションを許可します。
[Inventory Management] > [Topology]	トポロジ：ネットワークデバイスとリンク接続を表示します。デバイスロールの管理、デバイスのタグ付け、表示のカスタマイズ、およびカスタムトポロジレイアウトの保存を行います。 注：[SD-Access Fabric] ウィンドウを表示するには、少なくとも**[Network Provision]** > **[Inventory Management]** > **[Topology]**に対する読み取りアクセス許可が必要です。
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。このロールは、cisco.com およびスマートアカウントの権限も管理します。
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
プロビジョニング	サイト固有の設定とネットワークに対して設定されたポリシーを使用してデバイスをプロビジョニングします。このロールには、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、同期開始と実行設定、および Umbrella プロビジョニングが含まれます。 不正および aWIPS のメインダッシュボードでは、不正封じ込めなどの特定のアクションを有効または無効にできます。 デバイスをプロビジョニングするには、[Network Design] と [Network Provisioning] に対する書き込み権限が必要です。
ネットワーク サービス	基本的なネットワーク接続とアクセスの枠を超えたネットワークの追加機能を設定します。
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、およびモニターします。
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	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。 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。 • **[Network Design]** > **[Network Settings]** • **[Network Provision]** > **[Provision]** • **[Network Services]** > **[Stealthwatch]** • **[Network Design]** > **[Advanced Settings]**
Umbrella	サイバーセキュリティの脅威に対する最前線の防御策として、ネットワーク要素で Cisco Umbrella を使用するように設定します。 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。 • **[Network Design]** > **[Network Settings]** • **[Network Provision]** > **[Provision]** • **[Network Provision]** > **[Scheduler]** • **[Network Services]** > **[Umbrella]** また、[Advanced Network Settings] に対する読み取り権限も必要です。

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、**[System]** > **[Settings]** > **[Destinations]** で設定できます。
レポート	事前定義されたレポーティング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。 不正デバイスおよび aWIPS のレポートを生成します。 ウェブフックは、**[System]** > **[Settings]** > **[Destinations]** 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。ユーザーロールを管理し、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、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 サーバー、Cisco AI Analytics、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。

機能	説明
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。
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。
イベント ビューア	トラブルシューティングのためのネットワークデバイスおよびクライアントイベントの表示。
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。
リモートデバイスのサポート	シスコサポートチームが Cisco DNA Center によって管理されているネットワークデバイスをリモートでトラブルシューティングできるようにします。このロールを有効にすると、Cisco Technical Assistance Center（TAC）のエンジニアは、トラブルシューティングのためにお客様の Cisco DNA Center のセットアップにリモートで接続できます。
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、プロビジョニング、ネットワークのアップグレードなどのタスクやアクティビティの実行、スケジュール、および監視が行えます。 不正封じ込めをスケジュールすることもできます。
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

各ユーザーロールに属しているユーザーの数を示す統計を表示できます。ドリルダウンして、選択したロールを持つユーザーのリストを表示することもできます。

ステップ 1 メニューアイコン（☰）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ーロールとカスタムロールが表示されます。

ステップ 2 各ユーザーロールに対応する番号をクリックすると、そのロールを持つユーザーのリストが表示されます。

外部認証の設定

外部ユーザーの認証と許可に外部サーバーを使用している場合、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 （121 ページ）を参照してください。
- 少なくとも 1 つの認証サーバーを設定する必要があります。

（注） 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 サーバーに到達できないか、AAA サーバーが不明なユーザー名を拒否すると、ローカルユーザーにフォールバックしていました。現在のリリースでは、AAA サーバーに到達できない場合や AAA サーバーが不明なユーザー名を拒否した場合に Cisco DNA Center がローカルユーザーにフォールバックすることはありません。

外部認証フォールバックが有効になっている場合、外部ユーザーとローカル管理者は Cisco DNA Center にログインできます。

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 メニューアイコン（☰）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。

TACACS 認証では、次の AAA 属性がサポートされています。

Cisco DNA Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

RADIUS 認証では、次の AAA 属性がサポートされています。

Cisco DNA Center	RADIUS
Empty	cisco-av-pair

Cisco DNA Center	RADIUS
Cisco-AVPair	cisco-av-pair

a) 前の表で説明されているように、[AAA Attribute] フィールドに、ユースケースに適した属性を入力します。
b) [更新（Update）] をクリックします。

ステップ 4 （任意） AAA サーバーを設定します。

これらの設定は、現在のプライマリ AAA サーバーとセカンダリ AAA サーバーを交換したり、異なる AAA サーバーを定義したりする場合にのみ行います。メニューアイコン（☰）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 サーバーの IP アドレスを選択します。
b) [Secondary AAA Server IP Address] ドロップダウンリストで、事前設定されたいずれかの AAA サーバーの IP アドレスを選択します。
c) （任意） Cisco ISE サーバーを使用している場合は、必要に応じて設定を更新できます。

Cisco ISE ポリシーの詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Configure and Manage Policies」を参照してください。

表 *7 : Cisco ISE*サーバーの設定

名前	説明
Shared Secret	デバイスの認証キー。共有秘密の長さは、最大 100 文字です。 AAA アドレスを更新する前に、共有秘密を指定する必要があります。
Username	Cisco ISE CLI にログインするために使用する名前。
Password	Cisco ISE CLI ユーザー名のパスワード。
FQDN	Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。 *hostname.domainname.com* たとえば Cisco ISE サーバーの FQDN は、ise.cisco.com である可能性があります。
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。
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 *8 : AAA* サーバー詳細設定

名前	説明
Protocol	TACACS または RADIUS。
Authentication Port	AAA サーバーへの認証メッセージのリレーに使用されるポート。 • RADIUS の場合、デフォルトは UDP ポート 1812 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Accounting Port	AAA サーバーへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。 • RADIUS の場合、デフォルトの UDP ポートは 1813 です。 • TACACS の場合、ポートは 49 であり、変更できません。
Retries	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。

二要素認証

二要素認証（2FA）は、ユーザー名とパスワードに加えて識別子手法を使用することで、ユーザー認証のセキュリティを強化するものです。識別子手法は、一般に、実際の対象ユーザーだけが所持し（スマホアプリやキーフォブなど）、元のログイン方法と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）、トークンサーバー（トークンコードを検証）、およびユーザーのアクセスを管理する認証サーバーを使用できます。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 ユーザーの RBAC ロール認可を伝達する属性値ペアを返すことができる認証サーバー。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。
- 認証サーバーと統合する二要素トークンサーバー。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ー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、ユーザーは 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、ユーザー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 サーバーに要求を送信します。
5. RSA Authentication Manager でトークンコードを検証し、ユーザーが正常に認証されたことを Cisco ISE に通知します。
6. Cisco ISE は認証されたユーザー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 ユーザーのロールベース アクセス コントロール（RBAC）ロールに関連付けられている機能およびページへのアクセス権を付与します。

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 つのユーザー、すなわち **cdnac_admin**（管理者ユーザーロール用）と **cdnac_observer**（オブザーバロール用）を作成します。

詳細については、RSA Self-Service Console Help の「Add a User to the Internal Database」のトピックを参照してください。このトピックにアクセスするには、次の手順を実行します。

1. *RSA Self-Service Console Help* を開きます。
2. [Search help] フィールドで、「**`Add a User To the Internal Database`**」と入力して、[Search help] をクリックします。

b) 新しい認証エージェントを作成します。

詳細については、*RSA Self-Service Console Help* の「Add an Authentication Agent」のトピックを参照してください。

c) 認証マネージャエージェント設定ファイル（sdconf.rec）を生成します。

1. RSA セキュリティコンソールで、**[Access]** > **[Authentication Agents]** > **[Generate Configuration File]** の順に選択します。

   [Configure Agent Timeout And Retries] タブが開きます。
2. [Maximum Retries] と [Maximum Time Between Each Retry] フィールドについては、デフォルト値を使用します。
3. [Generate Configuration File] をクリックします。

   [Download Configuration File] タブが開きます。
4. [Download Now] リンクをクリックします。
5. 画面に指示が表示されたら、[Save to Disk] をクリックして、zip ファイルのローカルコピーを保存します。
6. ファイルを解凍し、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`** ユーザーと **`cdnac_observer`** ユーザーの PIN を生成します。

詳細については、*RSA Self-Service Console Help* の「Create My On-Demand Authentication PIN」のトピックを参照してください。

e) Cisco ISE を開始するには、**[Administration]** > **[Identity Management]** > **[External Identity Sources]** > **[RSA SecurID]** の順に選択して、[Add] を選択します。

f) [RSA SecurID Identity Sources] ページで、[Browse] をクリックし、ダウンロードした sdconf.rec ファイルを選択して、[Open] をクリックします。

g) [Reauthenticate on Change PIN] チェックボックスをオンにして、[Submit] をクリックします。

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 ユーザーロール用、もう 1 つは オブザーバユーザーロール用です。

a) Cisco ISE で、**[Policy]** > **[Policy Elements]** > **[Results]** > **[Authorization]** > **[Authorization Profiles]** を選択します。

b) 両方のプロファイルについて、次の情報を入力します。

- [Name] フィールド：プロファイル名を入力します。

- [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 ユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=NETWORK-ADMIN-ROLE] を選択します。

  オブザーバユーザーロールの認証プロファイルを作成する場合は、2 番目のドロップダウンリストから [Role=OBSERVER-ROLE] を選択します。

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*』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 ユーザーロール用、もう 1 つは オブザーバユーザーロール用です。

『*Cisco Identity Services Engine Administrator Guide*』の「Configure Authorization Policies」のトピックを参照してください。

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ーに割り当てられていることを確認します。

詳細については、*RSA Self-Service Console Help* の「View a Token」のトピックを参照してください。

（注） トークンを割り当てる必要がある場合は、「Assign a Software Token to a User」のトピックで説明されている手順を実行します。

RADIUS を使用した二要素認証の有効化

RADIUS 用に設定された Cisco ISE サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

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 サーバーを使用するよう 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 サーバーを使用する二要素認証を有効にするには、次の手順を実行します。

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、その内容を表示します。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 ユーザーロールの TACACS+ プロファイルを作成します。

a) [Add] をクリックします。

b) 次のタスクを実行します。

- 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 ユーザーロールの場合は、**`Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`** と入力します。
  - cdnac_observer ユーザーロールの場合は、**`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 サーバーを使用するよう 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、適切なユーザー名を入力します。

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。

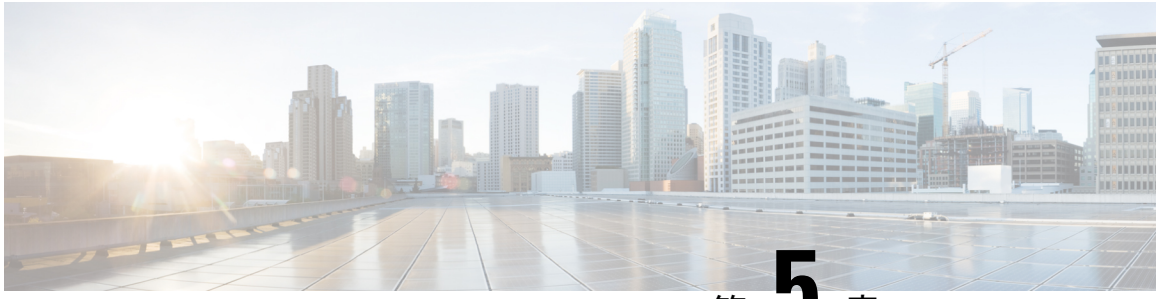
ステップ 4 [Log In] をクリックします。

外部ユーザーの表示

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

ステップ 1 メニューアイコン（☰）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] 領域に外部ユーザーのリストが表示されます。



第 5 章

ライセンスの管理

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。メニューアイコン（≡）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。[License Manager] ウィンドウには、次の情報のタブが含まれています。

- [Overview]：
  - [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。

- [Licenses]：[License Summary] には、すべてのシスコデバイスにわたるすべてのタイプのライセンスについて、Cisco Smart Software Management（CSSM）から購入したライセンスの総数、期限切れ間近のライセンスの数、コンプライアンス違反の詳細が表示されます。
- [Devices]：[Devices] テーブルには、ライセンスタイプ、ライセンスの有効期限、ライセンスモード、仮想アカウント、関連サイト、および Cisco DNA Center による管理対象の各デバイスの登録ステータスが表示されます。
- [Reporting]：[Smart License Readiness] には、デバイスを簡易モデルに更新する前に実行する手順が表示されます。[Smart License Compliance] カードを使用すると、[Smart License Update] ワークフローを開始できます。
- [Sync Status]：スマートライセンスポリシー（SLP）に関するコンプライアンスの表には、Cisco DNA Center から CSSM に送信されるライセンス使用状況レポートのデバイスおよびタイムライングラフが表示されます。ステータスに基づいてデバイスをフィルタリングし、コンプライアンスレポートを CSV または PDF 形式でエクスポートできます。

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。

（注） すべてのタブですべてのコントロールを使用できるわけではありません。

表 *9*：ライセンス管理のコントロール

制御	説明
Filter	[Filter] をクリックして 1 つ以上のフィルタ値を指定し、[Apply] をクリックします。複数のフィルタを適用することができます。フィルタを削除するには、対応するフィルタ値の横にある **x** アイコンをクリックします。
Change Cisco DNA License	1 つ以上のライセンスを選択し、**[Actions]** > **[Change Cisco DNA License]** の順に選択して、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、ライセンスレベルの変更 （150 ページ）を参照してください。
Change Virtual Account	1 つ以上のライセンスを選択し、**[Actions]** > **[Change Virtual Account]** の順に選択して、ライセンスの管理に使用されるバーチャルアカウントを指定します。

制御	説明
[Manage Smart License] > [Register]	スマートライセンスが有効になっているデバイスを 1 つ以上選択し、**[Actions]** > **[Manage Smart License]** > **[Register]** の順に選択して、スマートライセンスが有効になっているデバイスを登録します。
[Manage Smart License] > [Deregister]	スマートライセンスが有効になっているデバイスを 1 つ以上選択し、**[Actions]** > **[Manage Smart License]** > **[Deregister]** の順に選択して、スマートライセンスが有効になっているデバイスを登録解除します。
[Manage License Reservation] > [Enable License Reservation]	特定ライセンス予約（SLR）または永久ライセンス予約（PLR）を適用するデバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Enable License Reservation]** の順に選択します。
[Manage License Reservation] > [Update License Reservation]	デバイスが SLR 登録済みの状態である必要があります。 ワイヤレスデバイスまたはスイッチに適用されている SLR を、ワイヤレス コントローラ パッケージで更新できます。 SLR を更新するデバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Update License Reservation]** の順に選択します。
[Manage License Reservation] > [Cancel/Return License Reservation]	デバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Cancel/Return License Reservation]** の順に選択して、デバイスに適用された SLR または PLR を取り消すか、返却します。
[Manage License Reservation] > [Factory License Reservation]	デバイスを選択し、**[Actions]** > **[Manage License Reservation]** > **[Factory License Reservation]** の順に選択して、工場出荷時にデバイスにインストールされている SLR を有効にします。
Recent Tasks	[Recent Tasks] をクリックして、最近実行された 50 件すべての Cisco DNA Center タスクを表示します。ドロップダウンを使用してリストをフィルタリングし、ステータスが [Success]、[Failure]、または [In Progress] のタスクのみを表示します。
License Usage	[License Usage] をクリックすると、すべてのタイプのライセンスについて、ライセンス使用率が表示されます。
Refresh	[Refresh] をクリックすると、現在のデータを使用してウィンドウがリロードされます。
Export	[Export] をクリックすると、表示されているライセンスのリストが CSV ファイルとしてエクスポートされます。詳細については、ライセンス情報のエクスポート（151 ページ）を参照してください。
Find	[Find] フィールドに検索用語を入力し、いずれかの列にその用語が含まれている、リスト内のライセンスをすべて検索します。検索文字列の任意の場所で、ワイルドカードとしてアスタリスク（*）を使用します。
Show Entries	テーブルの各ページに表示するエントリの総数を選択します。

ライセンステーブルには、各デバイスに表示される情報が表示されます。すべての列はソートに対応しています。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

（注） すべてのタブですべての列が使用されるわけではありません。また一部の列は、デフォルトの列ビュー設定で非表示になります。非表示の列を表示するには、歯車アイコンをクリックし、[Edit Table Columns] で、テーブルに表示する列を選択します。

表 *10* : 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 スタッカブル スイッチ）。詳細については、ライセンス詳細の表示 （149 ページ）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。
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 *11* : すべてのライセンス情報

カラム	説明
Device Name	デバイスの名前。詳細については、ライセンス詳細の表示 （149 ページ）を参照してください。
Device Family	スイッチやハブなど、Cisco DNA Center で定義されているデバイスのカテゴリ。
IP Address	デバイスの IP アドレス。
Device Series	表示されているデバイスが属しているシスコ製品シリーズの正式名称（例：Cisco Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ）。
Cisco DNA License	Cisco DNA Center のライセンスレベル。

カラム	説明
Cisco DNA License Expiry	Cisco DNA Center ライセンスの有効期限。
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。
Virtual Account	デバイスのライセンスを管理しているシスコバーチャルアカウントの名前。
Site	デバイスが設置されている Cisco DNA Center サイト。
Registration Status	デバイスの登録ステータス。
Authorization Status	デバイスの認証ステータス。
Reservation Status	デバイスの予約ステータス。
Last Updated Time	テーブル内のこのエントリが最後に更新された時刻。
MAC Address	ライセンスデバイスの MAC アドレス。
Term	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。
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。
Software Version	デバイスで現在実行されているネットワーク オペレーティング システムのバージョン。

Cisco 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 ユーザー ID とパスワードを収集します。
- スマートアカウントが複数ある場合：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ー 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可能なポート、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ー名とパスワードを使用してログインします。

ステップ 2 メニューアイコン（☰）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ー名とパスワードを入力します。

ステップ 4 メニューアイコン（☰）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ー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 メニューアイコン（☰）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]、[Licenses]、または [Reporting] のいずれかです。

ウィンドウの上部の [License Usage] 円グラフには、購入済みのライセンスの総数と選択したデバイスカテゴリで現在使用中のライセンスの数が表示されます。また、グラフには各合計内での Essentials ライセンスと Advantage ライセンスの割合も示されます。

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の詳細な比較を表示するには、[Device Series] 列で目的の製品ファミリ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に関する詳細が表示されます。

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、[License Timeline] セクションまでスクロールダウンします。各製品ファミリのタイムライングラフは、その製品ファミリ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。

ライセンス使用量の履歴傾向の表示

Cisco DNA Center では、CSSM で購入および使用されたすべてのライセンス使用量の履歴傾向を、日次、週次、および月次で表示できます。CSSM には、最大 1 年間の履歴情報が保存されます。

始める前に

Cisco DNA Center を CSSM の特定のスマートアカウントに登録する必要があります。詳細については、Cisco スマート アカウントとの統合 （145 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Tools]** > **[License Manager]** > **[Licenses]** の順に選択します。

- [License Summary] エリアには、CSSM から購入した Cisco DNA Center サブスクリプション ライセンスの総数が表示されます。
- [Smart Account] エリアには、スマートアカウントに関する詳細が表示されます。
- [ESSENTIALS]、[ADVANTAGE]、および [PREMIER] エリアでは、[Total Licenses]、[About to Expire]、および [Out of Compliance] の Cisco DNA Center サブスクリプション ライセンスの数を分類します。
- [License] ウィンドウのテーブルは、[Focus] ドロップダウンリストからの次のビューに基づいて、検出されたデバイスとそのライセンスをフィルタ処理します。
  - バーチャルアカウントビュー
  - ライセンスビュー
  - デバイスシリーズビュー
  - デバイスタイプビュー
  - ライセンスタイプビュー

ステップ 2 選択したライセンスの履歴情報を表示するには、そのデバイスの行にあるライセンスリンクをクリックします。

ライセンス詳細 slide-in pane に、選択したデバイスの完全なライセンスの詳細とライセンスの履歴が表示されます。

（注） ライセンス詳細 slide-in pane のタイトルが、選択したデバイスのタイトルと一致します。

ステップ 3 ライセンス詳細 slide-in pane で、[Frequency] ドロップダウンリストから履歴情報の頻度を選択します。

使用可能な頻度は次のとおりです。

- [Daily]：最初の日におけるライセンスデータのスナップショットを表示します。
- [Weekly]：月曜日のライセンスデータのスナップショットを表示します。
- [Monthly]：その月の 1 日におけるライセンスデータのスナップショットを表示します。

頻度の選択に応じて、[Purchased]、[In Use]、および [Balance] のライセンスに基づいたライセンスデータを示すグラフが表示されます。

[License History] テーブルは、頻度の選択に応じて、[Date]、[Purchased]、[In Use]、および [Balance] に基づいてライセンス履歴情報をフィルタ処理します。

（注） CSSM は以前のデータからこの情報を提供するため、ライセンス履歴情報は常に 1 日前のデータです。Cisco DNA Center は、CSSM からライセンスの履歴情報を毎日定期的に取得します。

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 [Devices] 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。各グラフに、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表示されます。

次に、[License Manager] の [Devices] テーブルを使用して 1 つのデバイスに関する包括的なライセンスの詳細を取得する方法について説明します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

[License Manager] ウィンドウには、検出されたすべてのデバイスと、それらのライセンスの一覧を示すテーブルが表示されます。テーブルの情報には、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]：▽ をクリックして、該当するフィールドにフィルタ条件を入力します。（たとえば、[Device Name] フィールドにデバイス名の全体または一部を入力）。フィルタ条件を複数のフィールドに入力

することができます。[Apply]をクリックすると、テーブルにはフィルタ条件に一致する情報を表示する行のみが表示されます。

特定のサイトに属するデバイスを表示する場合は、左側のペインでそのサイトまで移動してクリックします。フィルタ処理されて該当するデバイスが表示されます。サイト階層を示すサイトマーカーがページの上部に表示されます。

- [Find]：[Find] フィールドをクリックし、テーブルの列のいずれかに検索するテキストを入力します。**Enter** を押すと、テーブルは [Find] フィールドの入力に一致するテキストが含まれる最初の行にスクロールします。
- [Customize]：歯車アイコンをクリックし、[Edit Table Columns] で、テーブルに表示する列を選択します。たとえば、[Device Series] を選択解除するか、[Days to Expiry] を選択します。[Apply] をクリックすると、テーブルに選択した列のみが表示されます。

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

Cisco DNA Center に [License Details] slide-in pane が表示され、選択したデバイスのすべてのライセンス詳細情報とライセンス履歴が示されます。[Actions] には、デバイスまたはそのライセンスで実行できるアクションが表示されます。

完了したら × をクリックし、[License Details] slide-in pane 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にはデバイスのリブートが必要になるため、License Manager からユーザーに、ライセンスレベルの変更が完了した後にデバイスをリブ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ブートしないようにも選択できますが、その場合は後でリブートをスケジュールする必要があります。リブートしなければ、ライセンスレベルの変更は適用されません。

ステップ 1 メニューアイコン（≡）をクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

[License Manager] ウィンドウには、検出されたすべてのデバイスと、それらのライセンスの一覧を示すテーブルが表示されます。

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（149 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、そのライセンスのステータスを更新すると、デバイスを再起動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る場合は、[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、このライセンスを使用するデバイスがリブートされます。
- 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。最大 100 台のデバイスのライセンス情報をエクスポートできます。これらのライセンス バックアップ ファイルの目的は、組織のアカウンティングとレポートのニーズを支援することです。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 [Devices] をクリックします。

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 （任意）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ー名とパスワードを使用してログインします。

ステップ 2 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Cisco Accounts]** > **[Smart Account]**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イゼロ設定

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 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** > **[Devices]** の順に選択します。

[License Manager] ウィンドウには、自動登録されていない SL 対応デバイスの数と、検出されたデバイスとそのライセンスの一覧が表示されたテーブルのバナーメッセージが、自動登録を設定するリンクとともに表示されます。

また、[Registration Status] 列を使用して、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では、スマートデバイスのインスタンスによって Cisco Smart Software Management（CSSM）と定期的に同期して、ライセンスステータスの最新化とコンプライアンスの報告が行われるようにする必要があります。一部のお客様は、インターネットアクセスが制限された高度に保護されたネットワーク内にあるデバイスを使用しています。このようなタイプのネットワークでは、デバイスは定期的にCSSMと同期してコンプライアンス違反を表示することができません。このようなお客様の環境をサポートするため、特定ライセンス予約（SLR）およびパーマネントライセンス予約（PLR）が導入されました。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 から安全にライセンスを予約できます。Cisco DNA Center では、ステージング環境で CSSM に一度接続すれば、デバイスから SLR モードまたは PLR モードでシスコに接続する必要はありません。CSSMへの接続やステージングが実行できない場合は、CSSMで利用できる手動SLR/PLRワークフローが使用できます。

SLRによってお客様は、製品インスタンスにノードロックライセンスファイル（SLR承認コード）をインストールできます。このライセンスファイルによって、個別の（特定の）ライセンス（権限付与タグ）が有効化されます。

PLRによってお客様は、製品にすべてのライセンス済み機能を有効化する承認コードをインストールできます。

SLR と PLR の両方に、スマートアカウントのレベルでの事前承認が必要です。サポートが必要な場合は、licensing@cisco.com にご連絡ください。

デバイスと Cisco DNA Center の両方が CSSM に接続されている場合に SLR または PLR を有効にする方法については、デバイスと Cisco DNA Center が CSSM に接続されている場合の SLR/PLR の有効化 （153 ページ） を参照してください。

デバイスと Cisco DNA Center が CSSM に接続されていない場合に SLR または PLR を有効にする方法については、デバイスと Cisco DNA Center が CSSM に接続されていない場合の SLR/PLR の有効化 （154 ページ） を参照してください。

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

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** > **[Devices]** 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] ウィンドウの [Reservation Status] に、更新された最新のデバイスのステータスを表示できるようになりました。

デバイスとCiscoDNACenterがCSSMに接続されていない場合の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 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** > **[Devices]** 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 から各デバイスの承認コードを取得し、CSV ファイル内で更新します。「CSSM からの承認コードの生成」を参照してください。

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。選択したデバイスに SLR または PLR が適用されます。

[All Licenses] ウィンドウの [Reservation Status] に、更新された最新のデバイスのステータスを表示できるようになりました。

CSSM 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 メニューアイコン（☰）をクリックして、 **[Tools]** > **[Licenses]** > **[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。

承認コードをインストールし、高セキュリティライセンスを有効にする

シスコでは、デフォルトで250 Mbpsのスループットを提供しています。デバイスのスループットを 250 Mbps 超に増やすには、シスコから承認コードを取得する必要があります。必要に応じて、単一のワークフローまたは個別のワークフローで承認コードをインストールし、高セキュリティ（HSEC）ライセンスを有効にできます。

始める前に

デバイスで Cisco IOS XE リリース 17.3.2 以降が実行されていることを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 [Reporting] タブをクリックします。

ステップ 3 [Smart License Compliance] カードをクリックします。

ステップ 4 [Smart License Update] ウィンドウで、[Let's Do It] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 5 [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Choose Sites and Devices] ウィンドウで、承認コードをインストールするデバイスを選択し、[Next] をクリックします。

ステップ 8 [Policy Settings] ウィンドウで、CSSM ポリシーを確認し、[Next] をクリックします。

ステップ 9 [Choose Device Features] ウィンドウで、次の手順を実行します。

a) デバイスを選択します。
b) [Auth Codes] ドロップダウンリストから、[Install] を選択します。
c) [HSEC] ドロップダウンリストから、[Enable] を選択します。
d) [Next] をクリックします。

ステップ 10 [Review Device Features]ウィンドウで、[Next]をクリックします。

ステップ 11 [Installing Device Features] ウィンドウで、承認コードと HSEC インストールステータスを確認し、[Next] をクリックします。

ステップ 12 [Sync Data with Cisco] ウィンドウで [Next] をクリックします。

ステップ 13 [Summary] ウィンドウに、承認コードと HSEC インストールステータスが表示されます。

ステップ 14 [Finish] をクリックします。

高セキュリティライセンスの無効化

HSEC ライセンスを不必要に消費しないように、デバイスの HSEC ライセンスを無効にすることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 [Reporting] タブをクリックします。

ステップ 3 [Smart License Compliance] カードをクリックします。

ステップ 4 [Smart License Update] ウィンドウで、[Let's Do It] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 5 [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Choose Sites and Devices] ウィンドウで、高セキュリティライセンスを無効にするデバイスを選択し、[Next] をクリックします。

ステップ 8 [Policy Settings] ウィンドウで、[Next] をクリックします。

ステップ 9 [Choose Device Features] ウィンドウで、次の手順を実行します。

a) デバイスを選択します。

b) [HSEC] ドロップダウンリストから、[Disable] を選択します。

c) [Next] をクリックします。

ステップ 10 [Review Device Features]ウィンドウで、[Next]をクリックします。

ステップ 11 [Installing Device Features] ウィンドウで、 HSEC 無効化操作のステータスを確認し、[Next] をクリックします。

ステップ 12 [Sync Data with Cisco] ウィンドウで [Next] をクリックします。

ステップ 13 [Summary]ウィンドウに HSEC 無効化操作のステータスが表示されます。

ステップ 14 [Finish] をクリックします。

CSSM へのリソース使用率の詳細のアップロード

リソース使用率の詳細を CSSM に即座にアップロードしたり、アップロードイベントをスケジュールすることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 [Reporting] タブをクリックします。

ステップ 3 [Smart License Compliance] カードをクリックします。

ステップ 4 [Smart License Update] ウィンドウで、[Let's Do It] をクリックします。

今後このウィンドウをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 5 [Select Smart Account] ウィンドウで、ドロップダウンリストから [Smart Account] と [Virtual Account] を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Choose Sites and Devices] ウィンドウで、リソース使用率の詳細を取得するデバイスを選択し、[Next] をクリックします。

ステップ 8 リソース使用率の詳細を即座にアップロードするには、[Modify Policy] ウィンドウで [Next] をクリックします。定期レポートの頻度を変更するには、次の手順を実行します。

a) [Policy Settings] で、[Reporting Interval] フィールドに対応する [Modify] をクリックします。

b) [Change Reporting Interval] ウィンドウで、値を入力します。

レポート間隔（日数）は、Cisco DNA Center から CSSM へのリソース使用率の詳細の定期的なアップロードの頻度を示します。アップロードの頻度は増やすことができますが、最小レポート頻度未満に減らすことはできません。

c) [**保存（Save）**] をクリックします。

ステップ 9 [Sync Data with Cisco] ウィンドウで [Next] をクリックします。

[Summary] ウィンドウには、このワークフローで実行される操作のステータスが表示されます。

ステップ 10 [Finish] をクリックします。

CSSM とのデータの同期が成功すると、Cisco DNA Center が確認応答をデバイスに送信します。

次のタスク

ライセンス使用状況レポートが失敗したデバイスの数は、別の [Smart License Compliance] カードに [Retry] オプションとともに表示されます。[Smart License Compliance] カードをクリックし、上記の手順をやり直して、失敗したデバイスから CSSM にライセンス使用状況レポートを送信します。

デバイスのスループットの変更

スマートライセンス対応ルータのスループットを変更できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 [Reporting] タブをクリックします。

[Reporting] ウィンドウに、すべてのスマートライセンス対応デバイスとそのライセンスを示すテーブルが表示されます。

ステップ 3 変更するデバイスを選択します。

ステップ 4 [More Actions] をクリックし、[Change Throughput] を選択します。

ステップ 5 [Choose Throughput] ウィンドウでスループット値を選択し、[Next] をクリックします。

ステップ 6 [Apply Throughput] ウィンドウで [Next] をクリックします。

ステップ 7 [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。

[Recent Task] ウィンドウで [Change Throughput] タスクのステータスを確認できます。

バーチャルアカウント間のライセンスの転送

バーチャルアカウント間でライセンスを転送できます。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Tools]** > **[License Manager]** > **[Licenses]** の順に選択します。

ステップ 2 転送するライセンスを選択し、[Transfer Licenses] をクリックします。

ステップ 3 [Transfer Licenses] ウィンドウで、バーチャルアカウントを選択します。

ステップ 4 選択した各ライセンスの [Transfer License Count] を入力し、[Transfer] をクリックします。

ステップ 5 [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。

[Recent Task] ウィンドウで [License Transfer] タスクのステータスを確認できます。

スマートライセンス対応デバイスに対する顧客タグの管理

スマートライセンス対応デバイスに最大4つの顧客タグを追加して、製品インスタンスのテレメトリデータの識別を容易にすることができます。顧客タグを更新および削除することもできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。

ステップ 2 [Reporting] タブをクリックします。

[Reporting] ウィンドウに、すべてのスマートライセンス対応デバイスとそのライセンスを示すテーブルが表示されます。

ステップ 3 顧客タグを追加するデバイスを選択します。

ステップ 4 [More Actions] をクリックし、[Manage Free Form Fields] を選択して、顧客タグを追加、更新、または削除します。

ステップ 5 顧客タグを追加または更新するには、[Free Form Fields] ウィンドウで次の手順を実行します。

a) 顧客タグを入力します。
b) [**保存（Save**）] をクリックします。

ステップ 6 顧客タグを削除するには、[Free Form Fields] ウィンドウで次の手順を実行します。

a) 削除する顧客タグの削除アイコンをクリックします。
b) [**保存（Save**）] をクリックします。
c) [Warning] ウィンドウで [Continue] をクリックします。

ステップ 7 [Recent Tasks] リンクをクリックして、[Recent Tasks] ウィンドウを起動します。

[Recent Task] ウィンドウで [Manage Customer Tags] タスクのステータスを確認できます。

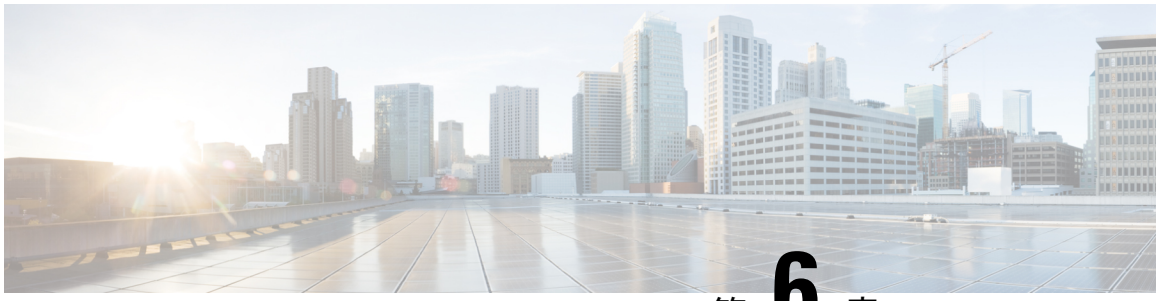
ライセンスポリシーの変更

ネットワークデバイスが CSSM に機能の使用状況を報告するレポート間隔を変更できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[License Manager]** の順に選択します。
ステップ 2 [Reporting] タブをクリックします。
ステップ 3 [Smart License] テーブルで、[Modify Policy] をクリックします。

[Modify Policy] ウィンドウに、ポリシー設定と CSSM ポリシーの詳細が表示されます。

ステップ 4 [Policy Settings] で、[Modify] をクリックします。
ステップ 5 [Change Reporting Interval] ウィンドウで、レポート間隔の値を入力します。
ステップ 6 [Save] をクリックします。



第 6 章

バックアップと復元

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、リモートサーバーにポストします。各バックアップは、ディレクトリ名としてUUIDを使用して一意に格納されます。リモートサーバーの要件の詳細については、バックアップサーバーの要件（163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。

週の特定日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ーからバックアップファイルを復元できます。

バックアップファイルを復元すると、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。

重要 Cisco DNA Center のバックアップおよび復元後、[Integration Settings] ページにアクセスし、（必要に応じて）[Callback URL Host Name] または [IP Address] を更新する必要があります。詳細については、「統合設定の設定」を参照してください。

バックアップと復元のイベント通知

バックアップまたは復元イベントが発生するたびに通知を受信できます。これらの通知を設定およびサブスクライブするには、『*Cisco DNA CenterPlatform User Guide*』の「Work with Event Notifications」トピックに説明されている手順を実行してください。この手順を完了したら、[SYSTEM-BACKUP]イベントと[SYSTEM-RESTORE]イベントを選択し、サブスクライブしていることを確認します。

通知は、次の表に示すイベントのいずれかが発生するたびに生成および送信されます。

動作	イベント
バックアップ	システムのバックアップファイルを作成するプロセスが開始された。
	システムのバックアップファイルが正常に作成された。
	システムのバックアップファイルを作成できなかった。このイベントは通常、次の理由で発生します。 • 必要なディスク領域がリモートストレージにありません。 • システムのNFSサーバーのステータスを取得できません。これは、バックアップ操作のための事前チェックです。 • システムのNFSサーバーでバックアップファイルを作成中に、接続の問題や遅延が発生しました。
復元	バックアップファイルを復元するプロセスが開始された。
	バックアップファイルの復元に成功した。
	バックアップファイルの復元に失敗した。このイベントは通常、次の理由で発生します。 • バックアップファイルが破損しています。 • システムのNFSサーバーでバックアップファイルを作成中に、接続の問題や遅延が発生しました。

バックアップサーバーの要件

バックアップサーバーは、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ー要件

自動化データのバックアップをサポートするには、サーバー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。
- （RedHat 7/CentOS 7 には適用されません）C.UTF-8 ロケールがインストールされている必要があります。C.UTF-8 がインストールされているかどうかを確認するには、次のように入力します。

```
# localectl  list-locales | grep -i c.utf
C.utf8
en_SC.utf8
```

- バックアップユーザー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、ユーザー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ーが「バックアップ」でユーザーのグループが「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」ユーザーが所有している。

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

  - 例 2：「バックアップ」ユーザー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。

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

アシュアランスバックアップのサーバー要件

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、サーバーが次の要件を満たすLinux ベースの NFS サーバー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、サーバーから **nfsstat -s** を入力します）。

- NFS エクスポートディレクトリに対する読み取り/書き込み権限がある。
- Cisco DNA Center と NFS サーバー間のネットワーク接続が安定している。
- Cisco DNA Center と NFS サーバー間のネットワーク速度が十分速い。
- C.UTF-8 ロケールがインストールされている。C.UTF-8 がインストールされているかどうかを確認するには、次のように入力します。

```
# localectl  list-locales | grep -i c.utf
C.utf8
en_SC.utf8
```

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

複数の Cisco DNA Center を展開するための要件

ネットワークに複数の Cisco DNA Center クラスタが含まれている場合は、同じバックアップロケーションを自動化と アシュアランス のバックアップに使用することはできません。複数の Cisco DNA Center を展開する場合、ベストプラクティスは各 Cisco DNA Center クラスタのバックアップディレクトリ構造を分離することです。次の設定例は、バックアップディレクトリ構造を分離する方法を示しています。

リソース	設定例
Cisco DNA Center クラスタ	1. *cluster1* 2. *cluster2*
自動化とアシュアランスのバックアップをホストするバックアップサーバー	例示したディレクトリは /data/ で、両方のタイプのバックアップをホストする十分なスペースがあります。
ディレクトリの所有権と権限	このセクションの前半にある「自動化データバックアップのサーバー要件」を参照してください。
ディレクトリの所有権と権限	このセクションの前半にある「アシュアランスバックアップのサーバー要件」を参照してください。
NFS エクスポート設定	/etc/exports ファイルの内容： `/data/assurance/cluster1 *(rw,sync,no_subtree_check,all_squash) /data/assurance/cluster2 *(rw,sync,no_subtree_check,all_squash)`

新しい Cisco DNA Center ハードウェアに移行する場合の要件

Cisco DNA Center クラスタを新しいハードウェアにアップグレードする場合、または返品許可（RMA）プロセスの一部として既存のクラスタハードウェアを交換する場合は、既存のバックアップ場所から復元した後で、バックアップのために別のディレクトリ構造を使用します。

（注） 既存の 3 ノードクラスタから 1 つまたは 2 つのノードを交換する場合、バックアップディレクトリ構造を変更する必要はありません。

バックアップサーバーのディレクトリレイアウト

バックアップを簡素化するために、バックアップサーバーに次のディレクトリレイアウトを使用することをお勧めします。

単一の Cisco DNA Center クラスタ展開

- 完全バックアップ（自動化とアシュアランス）：
  - cluster1：/data/automation/cluster1
  - cluster1：/data/assurance/cluster1
- 自動化のみのバックアップ：

  cluster1：/data/automation/cluster1

複数の Cisco DNA Center クラスタ展開

- 完全バックアップ（自動化とアシュアランス）：
  - cluster1：/data/automation/cluster1
  - cluster1：/data/assurance/cluster1
  - cluster2：/data/automation/cluster2
  - cluster2：/data/assurance/cluster2
- 自動化のみのバックアップ：
  - cluster1：/data/automation/cluster1
  - cluster2：/data/automation/cluster2

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 アシュアランス 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、アシュアランス 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、アシュアランス 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 サーバーの設定例：Ubuntu

アシュアランス 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 サーバー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 サーバーの 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 サーバー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 サーバー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 サーバーを再起動します。

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 サーバーの設定例：CentOS

次の手順は、CentOS での NFS サーバー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 サーバーの 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 サーバー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 サーバー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 サーバー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 サーバーを再起動します。

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ーの設定

自動化のデータのみをバックアップする場合は、Cisco DNA Center 自動バックアップサーバー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 自動バックアップサーバーと NFS バックアップサーバーを設定する必要があります。

この手順では、両方のサーバー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 （121 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ーは、バックアップサーバーの要件 （163 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 メニューアイコン（☰）をクリックして、**[System]** > **[Backup & Restore]** > **[Configure]** の順に選択します。

ステップ 2 自動化バックアップサーバーを設定するには、次の手順を実行します。

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ーの IP アドレス。
SSH ポート	SSH が可能なリモートサーバーのポートアドレス。
サーバー パス	バックアップファイルが保存されるサーバー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ー名。
[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。 このパスフレーズは必須で、バックアップファイルを復元するときに入力を求められます。このパスフレーズがなければ、バックアップファイルは復元されません。

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ーを設定するには、[NFS] タブをクリックし、次の手順を実行します。

a) 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ーの IP アドレスまたはホスト名。
サーバー パス	バックアップファイルが保存されるサーバー上のフォルダへのパス。

b) [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 アシュアランス 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ー上の場所に 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 （121 ページ）を参照してください。
- バックアップサーバーがバックアップサーバーの要件 （163 ページ）で説明されている要件を満たしている。
- バックアップサーバーが 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ーの設定 （170 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）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ー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ー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ーの設定 （170 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 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、リモートサーバー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、リモートサーバーに十分なディスク容量があるかどうかを確認し、別のバックアップを試行します。

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 （121 ページ）を参照してください。
- バックアップサーバーがバックアップサーバーの要件 （163 ページ）で説明されている要件を満たしている。
- バックアップサーバーが 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ーの設定 （170 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Backup & Restore]** > **[Schedule]** 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 [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。

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 5 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 6 [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、リモートサーバー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、リモートサーバーに十分なディスク容量があるかどうかを確認し、別のバックアップを試行します。

バックアップからデータを復元

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 Network Analytics 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 （121 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 メニューアイコン（☰）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。

リモートサーバー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。

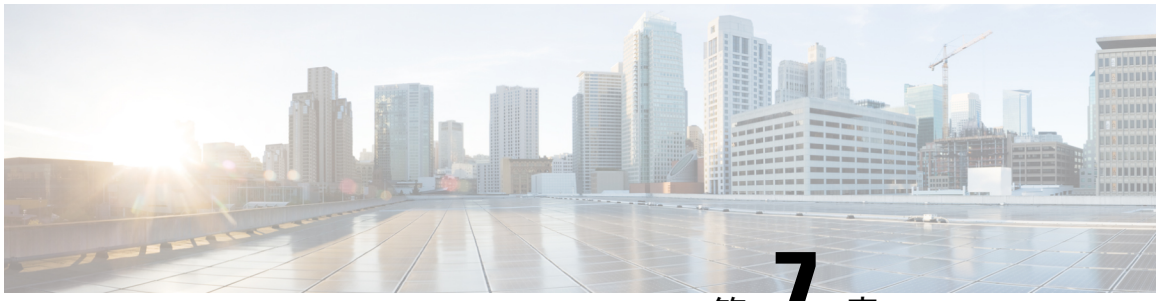
ステップ 3 [Actions] 列で、[Restore] を選択します。

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ってから、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 7 章

ディザスタリカバリの実装

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します。クラスタに障害が発生すると、ネットワーク管理作業を接続されたクラスタ（転送先サイト）に移すことで対処します。Cisco DNA Center でのディザスタリカバリの導入は、メインサイト、リカバリサイト、および監視サイトの 3 つのコンポーネントで構成されます。メインサイトとリカバリサイトは、常にアクティブまたはスタンバイのいずれかの役割を担います。アクティブサイトでネットワークが管理され、アクティブサイトで更新されたデータおよびマネージドサービスの最新のコピーがスタンバイサイトで維持されます。アクティブサイトがダウンすると、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。

次のトピックでは、運用環境でディザスタリカバリをセットアップして使用する方法について説明します。

主な用語

次に、Cisco DNA Center でのディザスタリカバリの導入について理解する上で重要な用語を示します。

- メインサイト：ディザスタリカバリシステムを設定するときに設定する1つ目のサイト。デフォルトでは、ネットワークを管理するアクティブサイトとして動作します。システムでサイトを設定する方法については、ディザスタリカバリの設定（191ページ）を参照してください。
- リカバリサイト：ディザスタリカバリシステムを設定するときに設定する2つ目のサイト。デフォルトでは、システムのスタンバイサイトとして機能します。
- 監視サイト：ディザスタリカバリシステムを設定するときに設定する3つ目のサイト。このサイトは、仮想マシンまたは別のサーバーにあり、データやマネージドサービスの複製には関与しません。このサイトには、現在アクティブなサイトにディザスタリカバリタスクを実行するために必要なクォーラムを割り当てる役割があります。いずれかのサイトに障害が発生した場合、監視サイトによってスプリットブレーン状況が回避されます。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（183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（191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） システムのスタンバイサイトを現在表示していることを示すメッセージが表示されます。アクティブサイトからすべてのディザスタリカバリタスクを開始する必要があります。

- フェールオーバー：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す。
  - 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ーリングでモニターできます。
  - 手動：手動でフェールオーバーを開始して現在のスタンバイサイトを新しいアクティブサイトとして指定できます。詳細については、手動フェールオーバーの開始 （210 ページ）を参照してください。

重要

- フェールオーバー後はアシュアランスが再起動され、新しいアクティブサイトで新規のデータセットが処理されます。アシュアランスデータの履歴は前のアクティブサイトから移行されません。
- フェールオーバー後、Cisco DNA Center インベントリサービスはデバイスの完全な同期をトリガーします。これには、管理対象のデバイスの数に応じて、数分から数時間かかる場合があります。Cisco DNA Center の通常スケジュールされたデバイス同期が実行されている場合と同様に、フェールオーバーによってトリガーされたデバイス同期が完了するまで、新しくアクティブ化されたクラスタでデバイスをプロビジョニングすることはできません。

- 分離：フェールオーバーの際に前のアクティブサイトがディザスタリカバリシステムから切り離されます。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停止 （213 ページ）を参照してください。
- 再参加：フェールオーバーの発生後にスタンバイ準備完了または一時停止状態のサイトをディザスタリカバリシステムに新しいスタンバイサイトとして追加するには、**[Disaster Recovery]** > **[Monitoring]**タブの [Action] 領域で [Rejoin] ボタンをクリックします。また、現在一時停止しているディザスタリカバリシステムを再起動する場合もこのボタンをクリックします。
- DR のアクティブ化：システムのアクティブサイトとスタンバイサイトを作成するユーザー始動型の操作。この操作では、クラスタ内通信を設定し、サイトがディザスタリカバリの前提条件を満たしていることを確認し、2 つのサイト間でデータを複製します。

- 登録解除：ディザスタリカバリシステム用に設定した3つのサイトを削除するには、[Action] 領域で [Deregister] ボタンをクリックします。前に入力したサイト設定を変更するには、この操作を実行する必要があります。
- 再試行：前に失敗したアクションを再度実行するには、[Action] 領域で [Retry] ボタンをクリックします。

データレプリケーションの概要

データ レプリケーション プロセスは、ディザスタリカバリシステムのメインサイトとリカバリサイトの間でデータを同期します。その期間は、複製する必要があるデータの量、ネットワークの有効な帯域幅、およびメインサイトとリカバリサイトの間に存在する待機時間など、いくつかの要因によって異なります。Cisco DNA Center の展開でディザスタリカバリがアクティブになっている場合、データレプリケーションは、現在アクティブなサイト（ネットワークを管理している）での操作やアプリケーションの使用に影響を与えません。

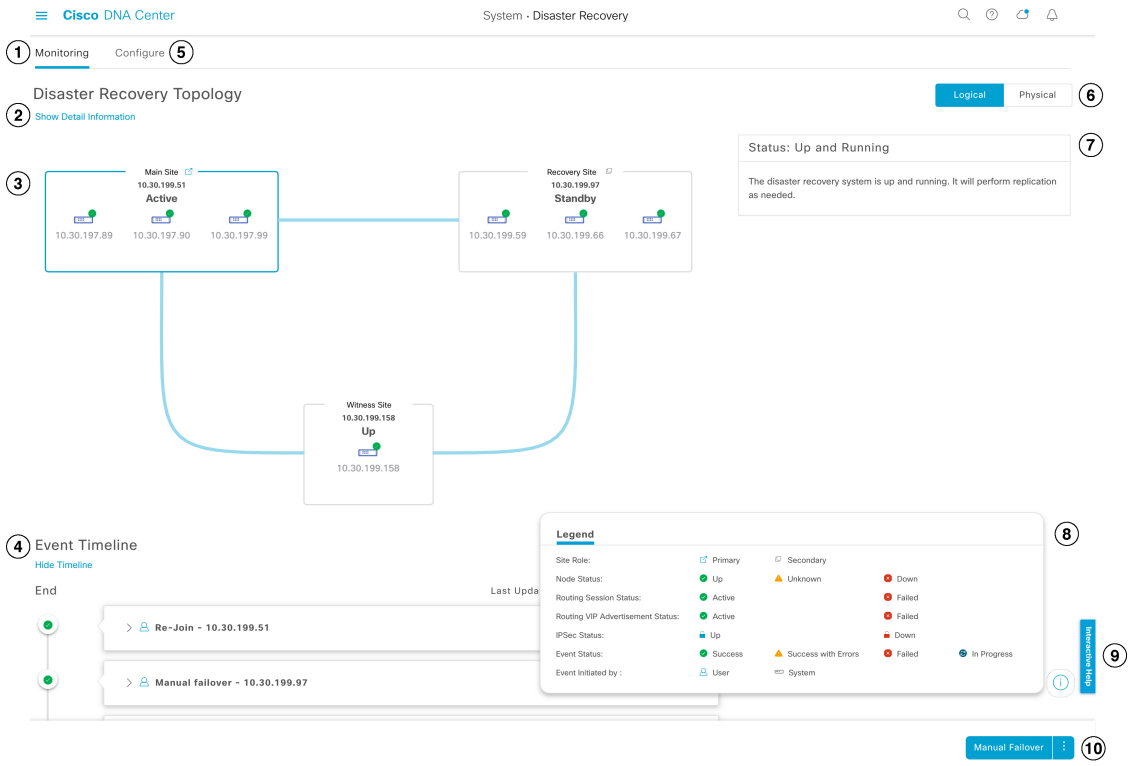
重要 フェールオーバーが発生した後、障害が発生したサイトからのアシュアランスデータは複製されません。システムのアクティブサイトを引き継ぐサイトは、新しいアシュアランスデータセットを収集します。

次のシナリオのどれが該当するかに応じて、データの完全レプリケーションまたは増分レプリケーションが実行されます。

- **初期アクティブ化後**：ディザスタリカバリシステムの初期構成とアクティブ化の後で、リカバリサイトにデータがありません。このシナリオでは、メインサイトとリカバリサイトの間でデータの完全なレプリケーションが行われます。
- **フェールオーバー後**：現在アクティブなサイトで障害が発生すると、ディザスタリカバリシステムがフェールオーバーをトリガーします。このシナリオでは、障害が発生したサイトがシステムに再参加した後に、メインサイトとリカバリサイト間でデータの完全なレプリケーションが発生します。
- **通常の操作時**：これは通常の状況でシステムに適用されるシナリオです。日常の運用中に、現在のアクティブサイトで発生した変更は、現在のスタンバイサイトと継続的に同期されます。

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。



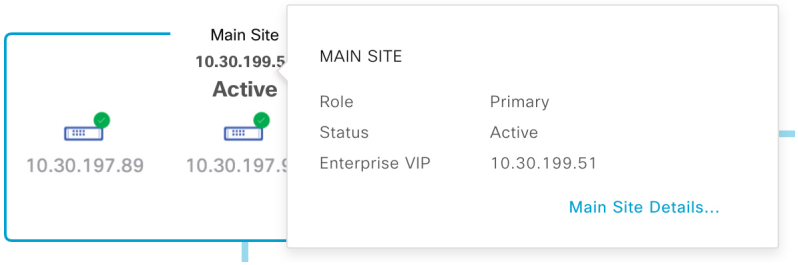
引き出し線	説明
1	[Monitoring] タブ：次の操作を実行する場合にクリックします。 • システムを構成するサイトのトポロジを表示します。 • システムの現在のステータスを確認します。 • ディザスタリカバリタスクを実行します。 • 現在までに完了しているタスクのリストを表示します。
2	[Show Detail Information] リンク：クリックして、[Disaster Recovery System] slide-in pane を開きます。詳細については、ディザスタリカバリシステムのステータスの表示 （182 ページ） を参照してください。
3	[Topology]：サイトとそのメンバーの現在のステータスを示すシステムの論理トポロジまたは物理トポロジが表示されます。 • 論理トポロジと物理トポロジの両方で、青色のボックスは、現在システムのアクティブサイトとして機能しているサイトを示します。 • 論理トポロジでは、青色の線は2つのサイトを接続する IPSec トンネルが動作していることを示し、赤色の線はトンネルが現在ダウンしていることを示します。 • サイトの状態については、システムおよびサイトの状態 （204 ページ）を参照してください。

引き出し線	説明
4	[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、イベントタイムラインのモニターリング （202 ページ）を参照してください。
5	[Configure] タブ：ディザスタリカバリシステムのサイト間の接続を確立するために必要な設定を入力する場合にクリックします。詳細については、ディザスタリカバリの設定 （191 ページ）を参照してください。
6	[Logical] タブと [Physical] タブ：適切なタブをクリックして、システムの論理トポロジと物理トポロジを切り替えます。
7	[Status] 領域：システムの現在のステータスを示します。システムの状態については、システムおよびサイトの状態 （204 ページ）を参照してください。
8	[Legend]：トポロジのアイコンの意味を示します。凡例を表示するには、[Disaster Recovery] ウィンドウの右下隅にある をクリックします。
9	[Interactive Help] ボタン：クリックすると、slide-in pane が開き、Cisco DNA Center の特定のタスクを完了するための画面上のガイダンスを示すウォークスルーへのリンクが表示されます。
10	[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。

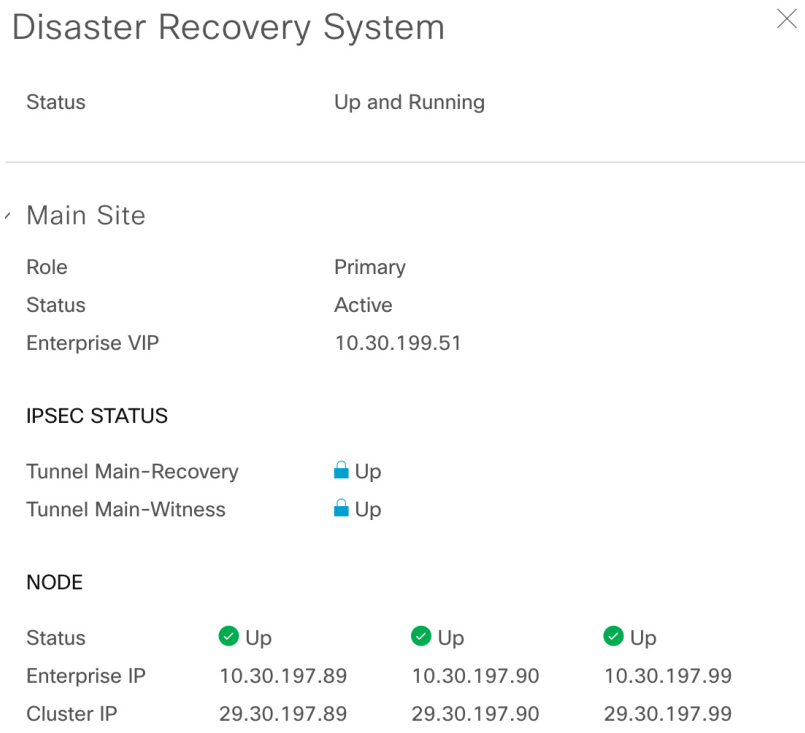
ディザスタリカバリシステムのステータスの表示

トポロジでは、ディザスタリカバリシステムの現在のステータスが視覚的に表示されます。[Disaster Recovery System] slide-in pane では、この情報を表形式で確認できます。このペインを開くには、次のいずれかを実行します。

- [Show Detail Information] リンクをクリックします。次に、slide-in pane でステータスを確認するサイトを展開します。
- トポロジで、サイトのエンタープライズ仮想 IP アドレスまたは特定のノードのアイコンにカーソルを合わせます。開いたダイアログボックスで、ウィンドウの右下隅にあるリンクをクリックします。



slide-in pane が開き、関連するサイト情報が表示されます。



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 Cisco DNA Center をこのバージョンにアップグレードする場合は、アップグレード後にディザスタリカバリが適切に機能するように、いくつかの手順を実行する必要があります。詳細については、「アップグレードされた Cisco DNA Center アプライアンスでのディザスタリカバリの設定 （187 ページ）」を参照してください。

一般的な前提条件

- Cisco DNA Center は、次の 2 つのディザスタリカバリ設定をサポートしています。
  - **1+1+1 セットアップ**：1 つ目の Cisco DNA Center アプライアンスはメインサイトとして機能し、2 つ目のアプライアンスはリカバリサイトとして機能し、3 つ目のシステム（仮想マシン上に常駐）は監視サイトとして機能します。次のアプライアンスとバージョンがこのセットアップをサポートしています。
    - DN1-HW-APL/DN2-HW-APL（44 コアアプライアンス）：Cisco DNA Center 2.2.2.x 以降
    - DN2-HW-APL-L（56 コアアプライアンス）：Cisco DNA Center 2.2.1.x 以降

- DN2-HW-APL-XL（112 コアアプライアンス）：Cisco DNA Center 2.2.1.x 以降

- **3+3+1 セットアップ**：1 つ目の 3 ノード Cisco DNA Center クラスタはメインサイトとして機能し、2 つ目の 3 ノードクラスタはリカバリサイトとして機能し、3 つ目のシステム（仮想マシン上に常駐）は監視サイトとして機能します。次のアプライアンスとバージョンがこのセットアップをサポートしています。
  - DN1-HW-APL/DN2-HW-APL（44 コアアプライアンス）：Cisco DNA Center 2.2.2.x 以降
  - DN2-HW-APL-L（56 コアアプライアンス）：Cisco DNA Center 2.1.2.x 以降
  - DN2-HW-APL-XL（112 コアアプライアンス）：Cisco DNA Center 2.1.2.x以降

- 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 Advanced Install Configuration Wizard」のトピックを参照してください。
- ディザスタリカバリタスクを実行できるように、ネットワーク管理者ユーザーを割り当てておきます。この機能には、この特権レベルのユーザーしかアクセスできません。
- 次の両サイトを接続するリンクが 1 GB リンクで、RTT 遅延が 350 ミリ秒以下であることを確認しておきます。
  - メインサイトとリカバリサイト
  - メインサイトと監視サイト
  - リカバリサイトと監視サイト
- 『Cisco DNA CenterSecurity Best Practices Guide』の「Disaster Recovery Ports」トピックに記載されているすべてのポートを開いておきます。

メインサイトとリカバリサイトの前提条件

- メインサイトとリカバリサイトの両方が同じ数のノードで構成されている必要があります。Cisco DNA Center では、この要件を満たさないディザスタリカバリシステムを登録してアクティブにすることはできません。
- メインサイトとリカバリサイトの両方について、同じ数のコアを持つ 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 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 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。

サポートされる Cisco DNA Center アプライアンス	シスコ製品番号
第 1 世代および第 2 世代の 44 コアアプライアンス	• DN1-HW-APL • DN1-HW-APL-U • DN2-HW-APL • DN2-HW-APL-U
第 2 世代 56 コアアプライアンス	• DN2-HW-APL-L • DN2-HW-APL-L-U
第 2 世代 112 コアアプライアンス	• DN2-HW-APL-XL • DN2-HW-APL-XL-U

また、メインサイトとリカバリサイトが同じバージョンの Cisco DNA Center を実行していることを確認してください。

- メインサイトとリカバリサイトの両方で、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。

重要 これは、3 ノードセットアップにのみ適用されます。

- 1 つの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。

- メインサイトのエンタープライズ VIP には、リカバリサイトの Cisco DNA Center クラスタから到達可能です。
- リカバリサイトのエンタープライズ VIP には、メインサイトの Cisco DNA Center クラスタから到達可能です。
- メインサイトとリカバリ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）がこの証明書に含まれていることを確認してください。また、証明書の [keyUsage] パラメータに [nonRepudiation] と [DigitalSignature] が指定されていることを確認します。

サードパーティ証明書を生成する方法については、『*Cisco DNA CenterSecurity 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連邦情報処理標準（FIPS）モード設定が同じであることを確認します。FIPSモードが一方のサイトで有効になっていて、もう一方のサイトで無効になっている場合、検証エラーが原因でディザスタリカバリシステムの登録が失敗します。FIPS モードの詳細については、[IP addressing mode used for the services] 画面の説明を参照してください（『Cisco DNA Center Second-Generation Appliance Installation Guide』の「Configure the Primary Node Using the Maglev Wizard」トピックにあります）。
- ボーダー ゲートウェイ プロトコル（BGP）を使用してシステムの仮想 IP アドレスルートをアドバタイズする場合は、メインサイトとリカバリサイトの各ネイバールータでシステムのエンタープライズ仮想 IP アドレスを設定する必要があります。入力する必要がある設定は、次の例のようになります。

  内部 BGP（iBGP）の設定例

  ```
  router bgp 64555
   bgp router-id 10.30.197.57
   neighbor 172.25.119.175 remote-as 64555
   neighbor 172.25.119.175 update-source 10.30.197.57
   neighbor 172.25.119.175 next-hop-self
  ```

  引数の説明

  - `64555` は、ネイバールータのローカルおよびリモート AS 番号です。
  - `10.30.197.57` はネイバールータの 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、ネイバールータのローカル AS 番号です。
  - `64555` は、ネイバールータのリモート AS 番号です。
  - `10.30.197.57` はネイバールータの 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 DENY_ALL out
  !
  ip prefix-list DENY_ALL seq 5 deny 0.0.0.0/0 le 32
  ```

```
!
route-map DENY_ALL permit 10
match ip address prefix-list DENY_ALL
```

監視サイトの前提条件

- 監視サイトをホストする仮想マシンが、最低でも 2.1 GHz コアと 2 つの仮想 CPU、4 GB の RAM、および 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 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。
- パブリッククラウドでの監視サイトの展開はサポートされていません。
- 監視サイトをメインサイトおよびリカバリサイトとは別の場所に用意し、それらの両方のサイトから到達可能であることを確認しておきます。
- 監視サイトからアクセス可能な NTP サーバーを設定しておきます。この NTP サーバーをメインサイトとリカバリサイトで使用される NTP サーバーと同期する必要があります。

アップグレードされた Cisco DNA Center アプライアンスでのディザスタリカバリの設定

システムを最新バージョンの Cisco DNA Center にアップグレードした後でディザスタリカバリを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、アプライアンスにインストールされた最初の Cisco DNA Center バージョンは2.1.x より前のバージョンです。ここで、2.1.x から最新バージョンにアップグレードします。アップグレード後にディザスタリカバリが正しく機能するように、次の手順を実行します。

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 （172 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ー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バージョンの Cisco DNA Center イメージをインストールします（『*Cisco DNA CenterSecond-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 （174 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 のバージョンは以前の 2.1.x でしたが、最新のバージョンにアップグレードする必要があります。次の手順を実行します。

ステップ 1 監視サイトのインストール （189 ページ）。

ステップ 2 ディザスタリカバリの設定 （191 ページ）。

ディザスタリカバリ証明書の追加

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。ディザスタリカバリ証明書は、クラスタ内通信に使用されます。

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。

（注）

- Cisco DNA Center で使用するのと同じ証明書をディザスタリカバリシステムで使用する場合は、この手順をスキップできます。証明書を設定する場合は、[Use system certificate for Disaster Recovery as well] チェックボックスをオンにします（Cisco DNA Center サーバー証明書の更新 （95 ページ）を参照）。
- ディザスタリカバリ証明書の要件の詳細については、『Security Best Practices Guide』を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Certificates]** > **[Disaster Recovery]** の順に選択します。

ステップ 2 [Add Certificate] 領域で、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 エンハンスト 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 3 [PEM] を選択した場合、次のタスクを実行します。

a) 強調表示されている領域に PEM ファイルをドラッグアンドドロップして、証明書をインポートします。

（注） PEM ファイルには、有効な PEM 形式の拡張子（.pem）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

b) [Private Key] 領域で、強調表示されている領域に秘密キーをドラッグアンドドロップしてインポートします。

（注） 秘密キーには、有効な秘密キー形式の拡張子（.key）が必須です。秘密キーの最大ファイルサイズは 10 MB です。

アップロードに成功すると、秘密キーが検証されます。

c) 適切なオプションボタンをクリックして、秘密キーを暗号化するかどうかを指定します。

d) 秘密キーを暗号化する場合、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 4 [PKCS] を選択した場合、次のタスクを実行します。

a) 強調表示されている領域に PKCS ファイルをドラッグアンドドロップして、証明書をインポートします。

（注） PKCS ファイルには、有効な PKCS 形式の拡張子（.pfx または .p12）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

b) [Password] フィールドに、証明書のパスワードを入力します（PKCS の要件）。

c) 適切なオプションボタンをクリックして、秘密キーを暗号化するかどうかを指定します。

d) 秘密キーを暗号化する場合、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 5 **[Save]** をクリックします。

Cisco DNA Center サーバーの SSL 証明書が置き換えられると、自動的にログアウトされるため、再度ログインする必要があります。

監視サイトのインストール

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開いたら、[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] ウィンドウが開きます。

b) 管理者ユーザー（*maglev*）のパスワードを入力して確認用にもう一度入力し、N を押して次に進みます。
c) 次の設定を入力し、N を押して次に進みます。

- IP アドレス
- 仮想マシンの IP アドレスに関連付けられているネットマスク
- デフォルトゲートウェイの IP アドレス
- **（オプション）**優先 DNS サーバーの IP アドレス

d) NTP サーバーのアドレスまたはホスト名を 1 つ以上入力し（複数の場合はカンマで区切る）、S を押して設定を送信します。監視サイトの設定が開始されます。

1 つ以上の NTP アドレスまたはホスト名が必要です。

e) 監視サイトに設定した IP アドレスに SSH ポート 2222 を使用してログインし、設定が完了したことを確認します。

（注） 後で、監視サイトの VM で **maglev** ユーザー用に設定された**パスワード**を変更する必要がある場合は、標準の Linux passwd ユーティリティを使用します。これを行う前にディザスタリカバリシステムを一時停止する必要はありません。また、パスワードを変更しても、ディザスタリカバリ操作に機能上の影響はありません。

ディザスタリカバリの設定

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。

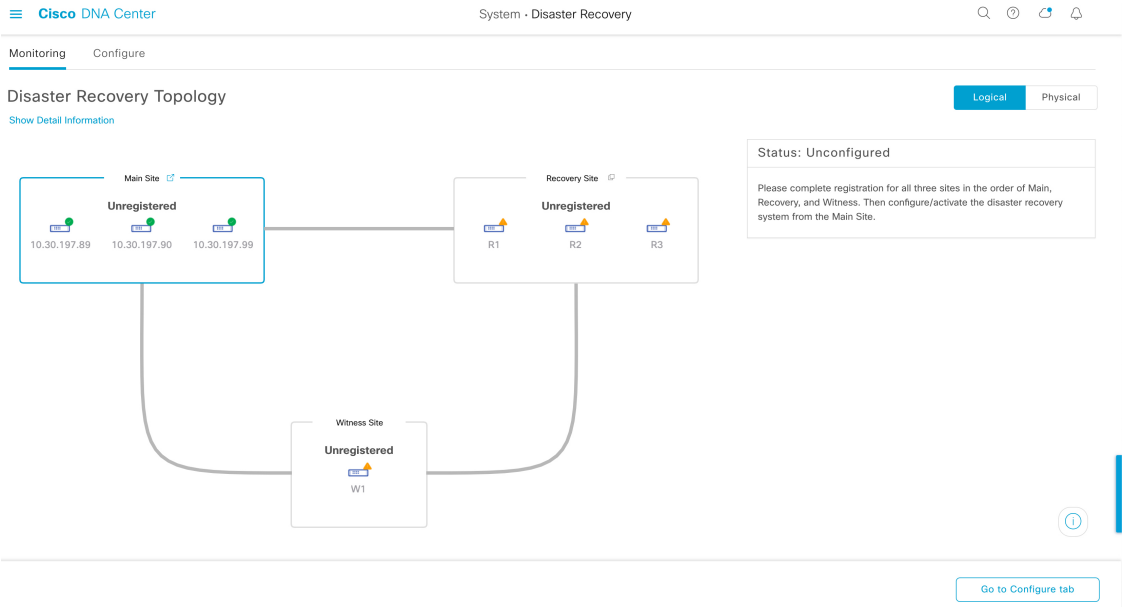
- ボーダー ゲートウェイ プロトコル（BGP）ルート アドバタイジングを使用する仮想 IP アドレスを指定できます。
- 仮想 IP アドレスを設定しないように選択することもできます。このオプションを選択した場合は、デバイスの可制御性を有効にして、フェールオーバー発生後にサイトの仮想IP アドレスを再設定できるようにする必要があります。詳細については、デバイスの可制御性 （63 ページ）を参照してください。

始める前に

アシュアランスデータ（Elasticsearch）と展開のバックアップスケジュールは、フェールオーバー後にレプリケートされません。ディザスタリカバリシステムのメインサイトとリカバリサイトが存在するクラスタの場合は、システムを構成する前に次の手順を実行します。

- サイトごとに個別の NFS デバイスを構成します。
- 同じバックアップスケジュールを設定します。

ステップ 1 メニューアイコン（☰）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。

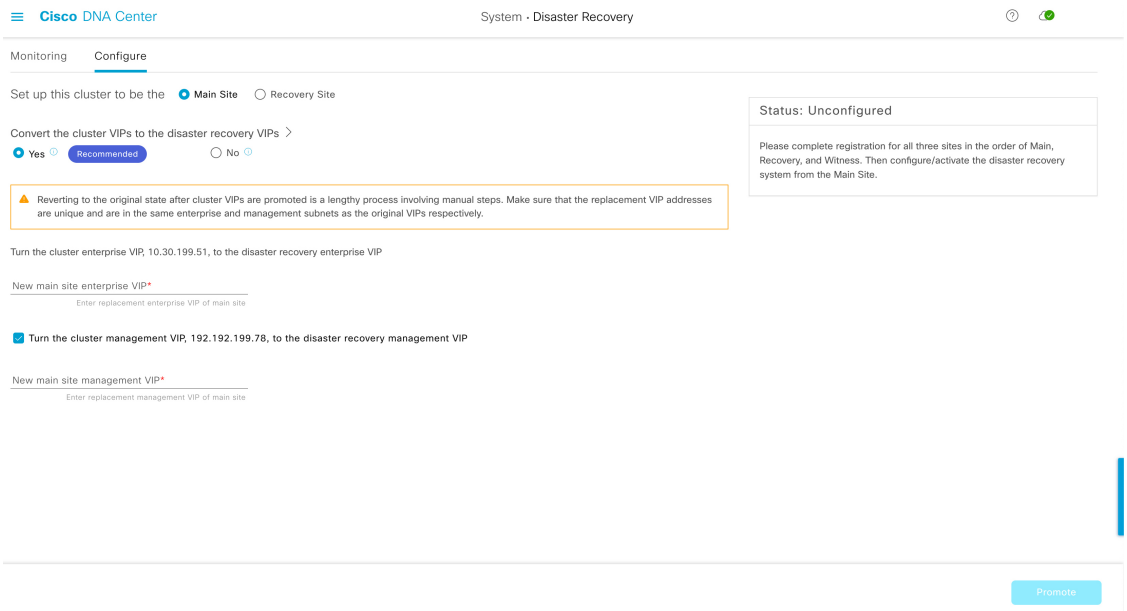


デフォルトでは、[Monitoring] タブが選択されています。

ステップ 2 メインサイトを登録します。

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) [Convert the cluster VIPs to the disaster recovery VIPs] 領域で、次のいずれかのオプションボタンをクリックします。

- クラスタをメインサイトとして設定し、このクラスタに接続されているデバイスに仮想 IP アドレスの変更を自動的に伝達するには、[Yes] をクリックします。これは、クラスタに現在設定されている仮想 IP アドレスを昇格させ、それらをディザスタリカバリシステムのグローバル仮想 IP アドレスとして割り当てることによって実現します。多数のデバイスが接続されているクラスタでディザスタリカバリを有効にする場合は、このオプションを選択することをお勧めします。このオプションを選択しない場合、新しいディザスタリカバリ仮想 IP アドレスと通信するようにこれらのデバイスを再設定する必要があります。このオプションを選択する場合は、次の手順を実行します。

  1. [New main site enterprise VIP] フィールドに、サイトのエンタープライズ ネットワークの新しい仮想 IP アドレスを入力します。これにより、昇格するアドレスが置き換えられます。このアドレスがまだ使用されていない一意のアドレスであり、以前の仮想 IP アドレスと同じサブネットにあることを確認します。

  2. （オプション）[Turn the cluster management VIP, <IP-address>, to the disaster recovery management VIP] チェックボックスをオンにします。

  3. （オプション）[New main site management VIP] フィールドに、サイトの管理ネットワークの新しい仮想IPアドレスを入力します。これにより、昇格するアドレスが置き換えられます。このアドレスがまだ使用されていない一意のアドレスであり、以前の仮想 IP アドレスと同じサブネットにあることを確認します。

- 仮想 IP アドレスの変更を接続デバイスに伝達せず、クラスタをメインサイトとして設定するには、[No] をクリックします。まだどのデバイスにも接続されていない、または少数のデバイス

にのみ接続されている新しいクラスタには、このオプションをお勧めします。このオプションを選択する場合は、ステップ 2f に進みます。

c) [Action] 領域で、[Promote] をクリックします。

[Disaster Recovery VIP Promotion] ダイアログが開きます。

d) [Continue] をクリックします。

Cisco DNA Center は、入力した仮想 IP アドレスを検証します。

e) [Details] 領域に検証ステータスが表示されます。

- 入力したアドレスのいずれかが無効である場合（アドレスが置換するアドレスと同じサブネットに存在しない可能性があります）、必要な修正を行い、ステップ 2c を繰り返します。
- 入力したアドレスが正常に検証されると、ディザスタリカバリシステム用に設定されるすべての仮想 IP アドレスが [Details] 領域に表示されます。次のステップに進みます。

f) 次の情報を [Site VIP/IPs] 領域に入力します。

- [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。Cisco DNA Center では、このフィールドはシステムの情報に基づいて入力されます。
- [Recovery Site VIP]：リカバリサイトのクラスタノードとエンタープライズ ネットワークの間のトラフィックを管理するエンタープライズ仮想 IP アドレス。
- [Witness Site IP]：監視サイトの仮想マシンとエンタープライズ ネットワークの間のトラフィックを管理する IP アドレス。

重要 入力したアドレスが現在到達可能であることを確認します。到達できない場合、システムのサイトの登録は失敗します。

（注） 手順 2f および 2j の間の任意の時点で、[Reset] をクリックして、入力したすべての設定をクリアできます。その後、メインサイトを登録する前に、手順 2f を繰り返して正しい設定を入力する必要があります。

g) [Route advertisement] 領域で、次のいずれかのオプションボタンをクリックします。

- [Border Gateway Protocol (BGP)]：このオプションは、ほとんどのディザスタリカバリシステムで推奨されており、デフォルトで選択されています。BGP ルートアドバタイズメントにより、システムの現在アクティブなサイトに確実にアクセスすることができます。これはフェールオーバーの発生後に重要になります。
- [Disaster recovery VIPs without route advertisement]：ルートが BGP を使用してアドバタイズされないシステムの仮想 IP アドレスを設定する場合は、このオプションを選択します。このオプションは、メインサイトとリカバリサイトの両方が、システムのグローバル仮想 IP アドレスが存在するサブネットにアクセスできるデータセンターに適しています。

- [No disaster recovery VIPs]：このオプションを選択すると、サイトに設定された仮想 IP アドレスが、そのサイトに属するデバイスで自動的に設定されます。フェールオーバーが発生するたびに、これらの仮想 IP アドレスがデバイスで再設定されます。手順 2k に進みます。

h) 前の手順で最初の 2 つのオプションボタンのいずれかをクリックした場合は、[Enterprise VIP for Disaster Recovery] フィールドに値を入力します。

このフローティング仮想 IP アドレスを設定しておくと、ネットワークのアクティブサイトとして現在動作しているサイトに自動的に切り替えて運用されます。このアドレスは、ディザスタリカバリシステムとエンタープライズ ネットワークの間のトラフィックを管理します。

（注）
- [Border Gateway Protocol (BGP)] オプションボタンをクリックし、管理仮想 IP アドレスを設定しない場合は、手順 2j に進みます。
- [Disaster recovery VIPs without route advertisement] をクリックし、管理仮想 IP アドレスを設定しない場合は、手順 2k に進みます。

i) （任意） [Management VIP for Disaster Recovery] フィールドに値を入力します。

このフローティング仮想 IP アドレスを設定しておくと、ネットワークのアクティブサイトとして現在動作しているサイトに自動的に切り替えて運用されます。このアドレスは、ディザスタリカバリシステムと管理ネットワークの間のトラフィックを管理します。

j) [Border Gateway Protocol (BGP)] オプションボタンをクリックした場合は、ルートアドバタイズメントを有効にするために必要な情報を入力します。

- [Border Gateway Protocol Type] 領域で、BGP ピアが相互に外部（[Exterior BGP (eBGP)]）セッションを確立するか、内部（[Interior BGP (iBGP)]）セッションを確立するかを指定します。
- [Main Site Router Settings for Enterprise Network] 領域および [Recovery Site Router Settings for Enterprise Network] 領域に、ディザスタリカバリシステムのメインサイトとリカバリサイトに設定されているエンタープライズ仮想 IP アドレスのアドバタイズのために Cisco DNA Center が使用するリモートルータの IP アドレスを入力します。また、ルータのリモートおよびローカル AS 番号も入力します。

  次の点に注意してください。

  - 追加のリモートルータを設定する場合は、[Add]（+）アイコンをクリックします。サイトごとに最大 2 台のルータを設定できます。
  - AS 番号を入力する場合は、1 ー 4,294,967,295 の範囲内の 32 ビットの符号なし数であることを確認します。
  - [iBGP] オプションを選択すると、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。
  - 前の手順で管理仮想 IP アドレスを設定した場合は、[Main Site Router Settings for Management Network] 領域および [Recovery Site Router Settings for Management Network] 領域も表示されます。Cisco DNA Center でこの仮想 IP アドレスのアドバタイズに使用されるリモートルータに関する適切な情報を入力します。

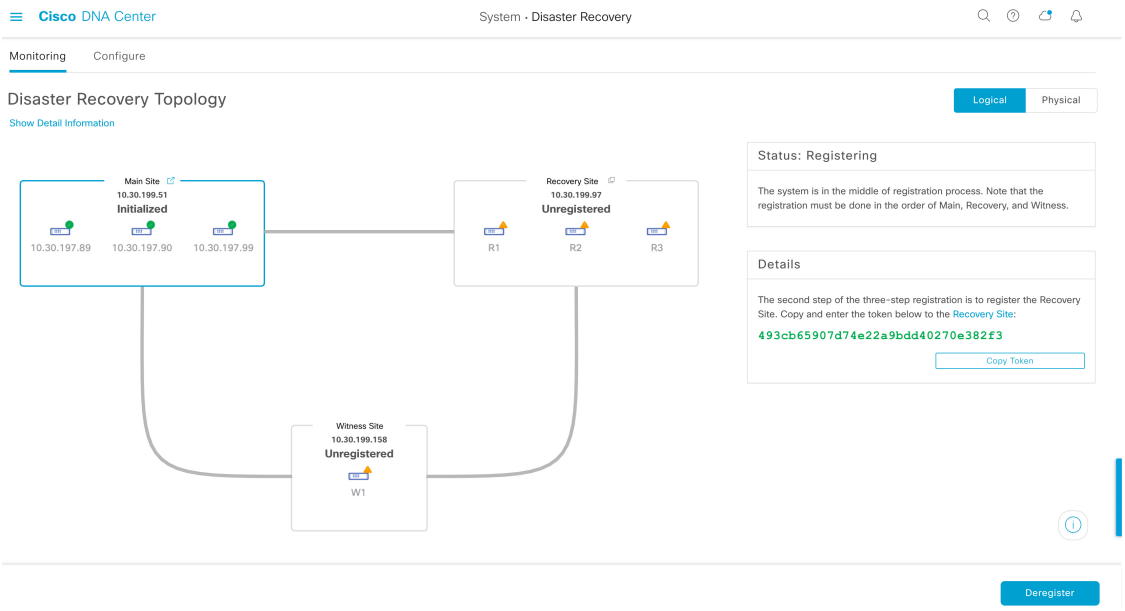
k) [Action] 領域で、[Register] をクリックします。

[Disaster Recovery Registration] ダイアログが開きます。

l) [Continue] をクリックします。

リカバリサイトおよび監視サイトをメインサイトに登録するために必要なトークンが生成されます。

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



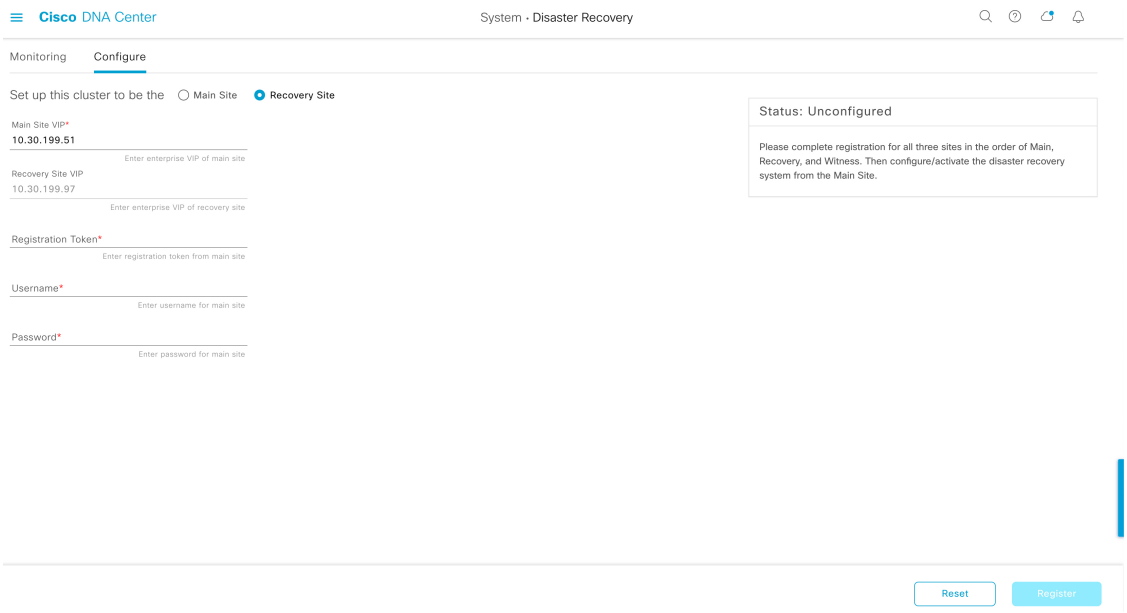
ステップ 4 リカバリサイトを登録します。

（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) [Details] 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、適切なユーザー名とパスワードを入力してリカバリサイトにログインします。

[Disaster Recovery] ページに、[Recovery Site] オプションボタンがすでに選択された状態で [Configure] タブが開きます。



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。Cisco DNA Center では、このフィールドはシステムの情報に基づいて入力されます。
- 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ーに対して設定されたユーザー名とパスワード。

d) [Action] 領域で、[Register] をクリックします。

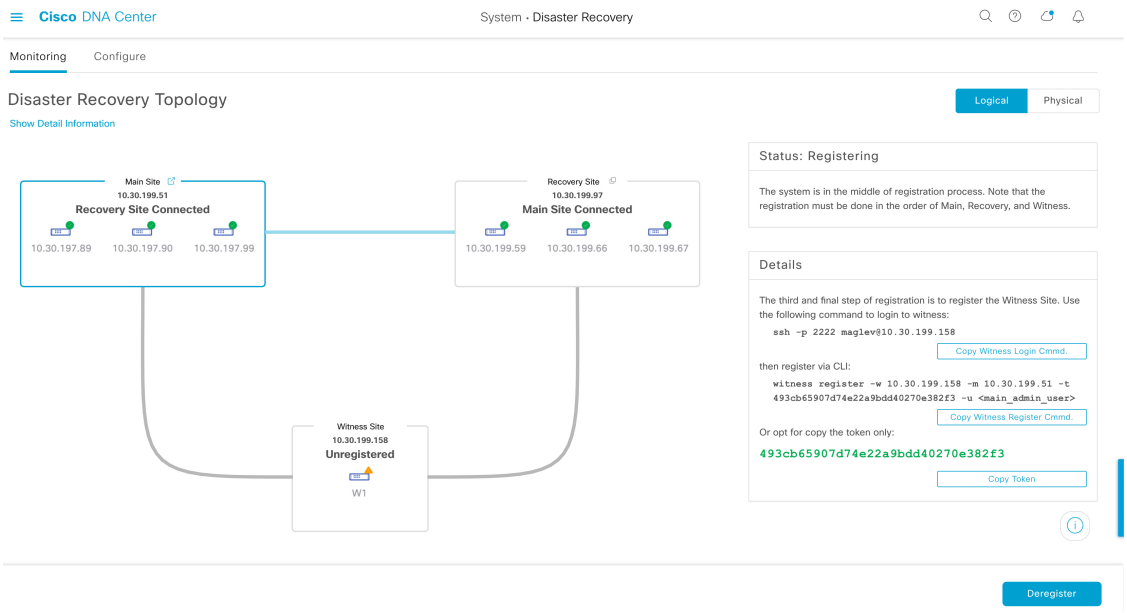
[Disaster Recovery Registration] ダイアログが開きます。

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。

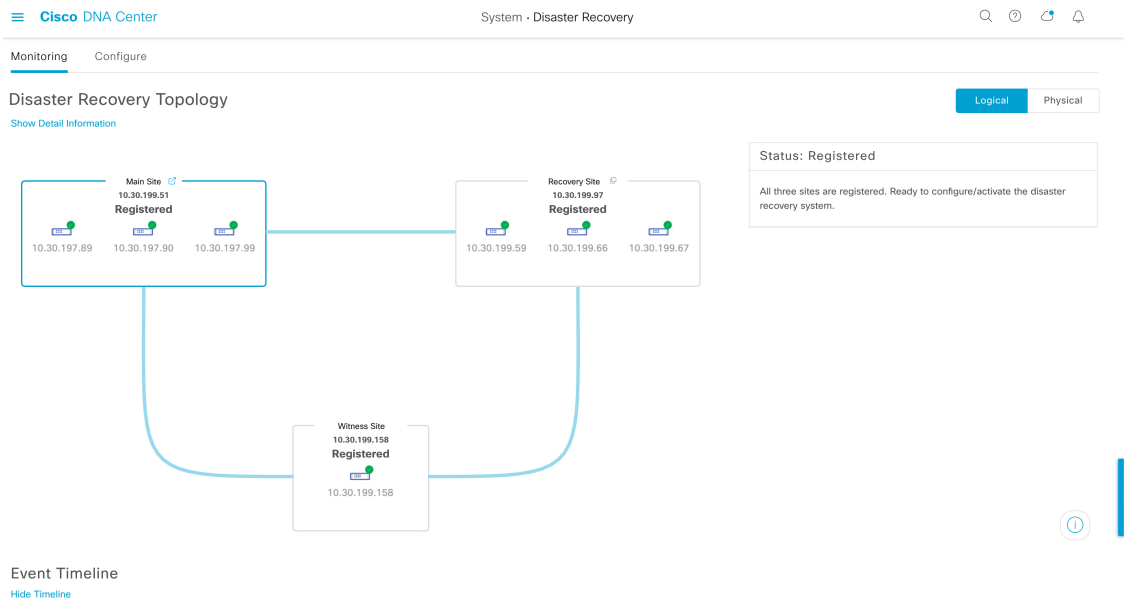
a) メインサイトのブラウザタブに戻ります。



b) [Details] 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ー（maglev）のパスワードを入力します。
e) [Details] 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ーのユーザー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ーのパスワードを入力します。

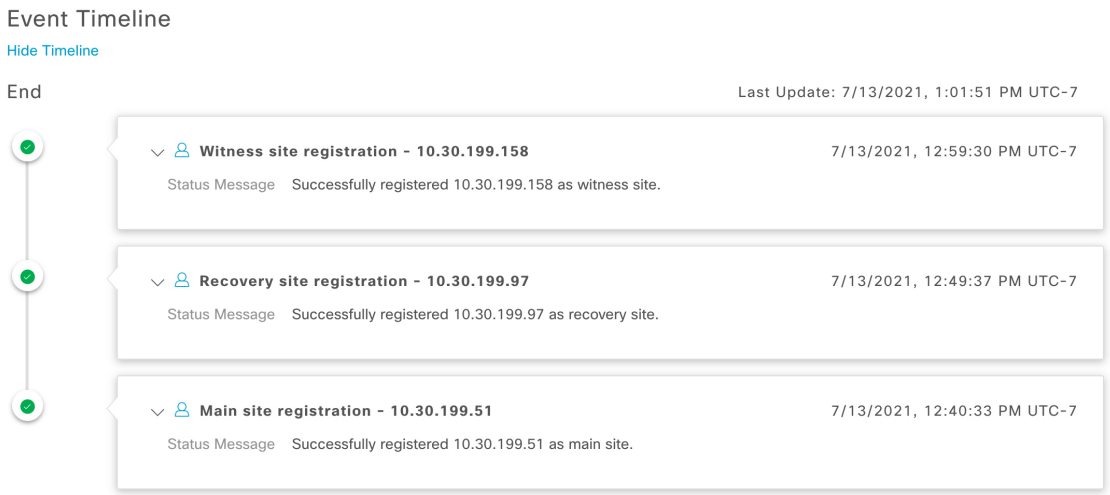
ステップ 6 メインサイト、リカバリサイト、および監視サイトが正常に登録されていることを確認します。

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開きます。

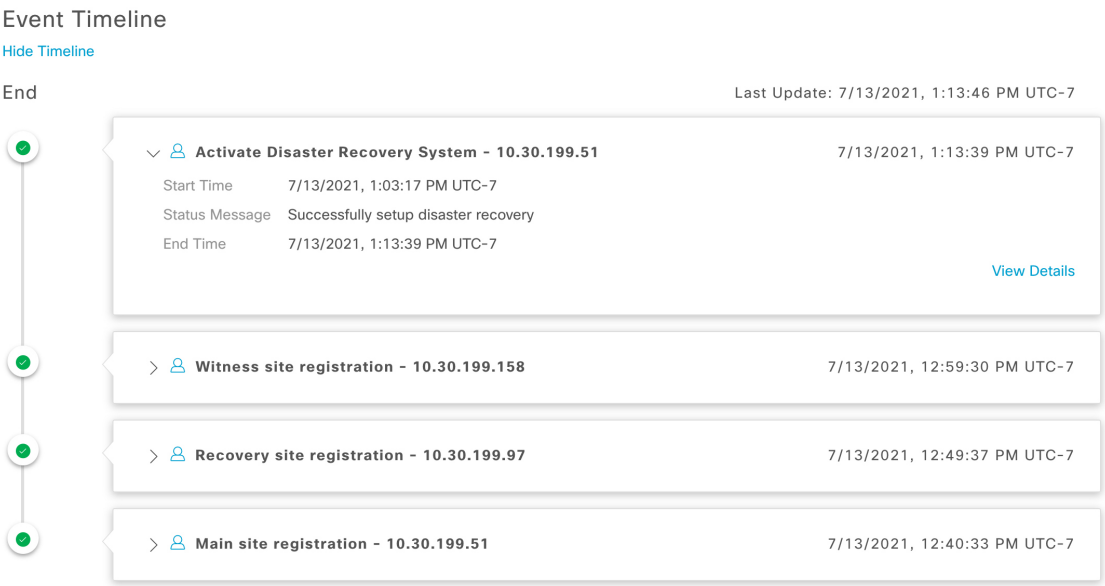
ステップ 8 ディザスタリカバリシステムの設定とメインサイトのデータのリカバリサイトへの複製を開始するには、[Continue] をクリックします。

（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。進捗状況をモニターするには、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。

2. イベントのタイムラインを表示し、[Activate Disaster Recovery System] タスクが正常に完了したことを確認します。



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ー（maglev）のパスワードを入力します。

（注） 次の手順に進む前に、監視サイトの IP アドレスをメモしておきます。監視サイトをアップグレードした後、同じアドレスを設定する必要があります。設定しない場合、監視サイトは期待どおりには機能しません。

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 監視サイトのインストール （189 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ー（maglev）のパスワードを入力します。

ステップ 6 **witness reconnect -w *witness-site's-IP-address* -m *system's-virtual-IP-address* -u *admin-username*** コマンドを実行します。

次の点に注意してください。

- メインサイトの現在のディザスタリカバリ ステータスに関係なく、監視サイトを再接続するときは、メインサイトのエンタープライズ VIP を使用します。
- このコマンドの実行後に監視サイトが動作していることを確認するには、次の手順を実行します。
  1. ディザスタリカバリトポロジから、[Show Detail Information] リンクをクリックして、[Disaster Recovery System] スライドインペインを開きます。
  2. [Witness Site] セクションで、監視サイトと設定済みの IPSec リンクのステータスが `[Up]` であることを確認します。
- このコマンドで使用可能なすべてのオプションを表示するには、**witness reconnect --help** コマンドを実行します。

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。

（注） システムを登録解除すると、システム内のすべてのサイトに関する現在の設定がクリアされます。

ステップ 1 [Action] 領域で、[Pause] をクリックしてシステムの運用を一時停止します。

詳細については、システムの一時停止 （213 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 （191 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ーリング

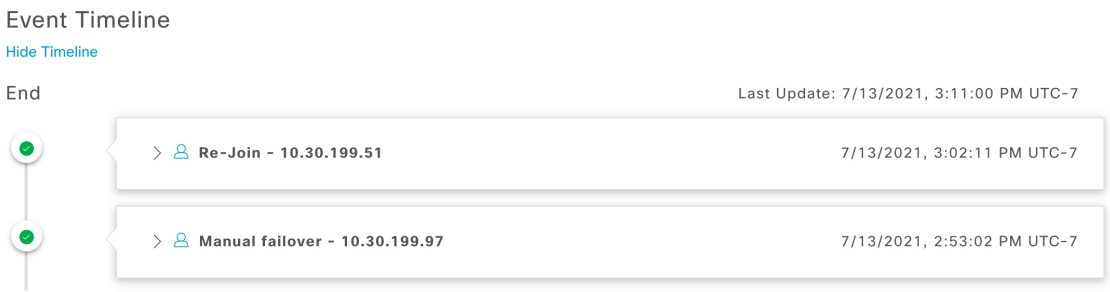
イベントのタイムラインから、現在実行されているディザスタリカバリタスクの進捗状況を追跡し、それらのタスクが完了したときに確認できます。タイムラインを表示するには、次の手順を実行します。

1. メニューアイコン（☰）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。

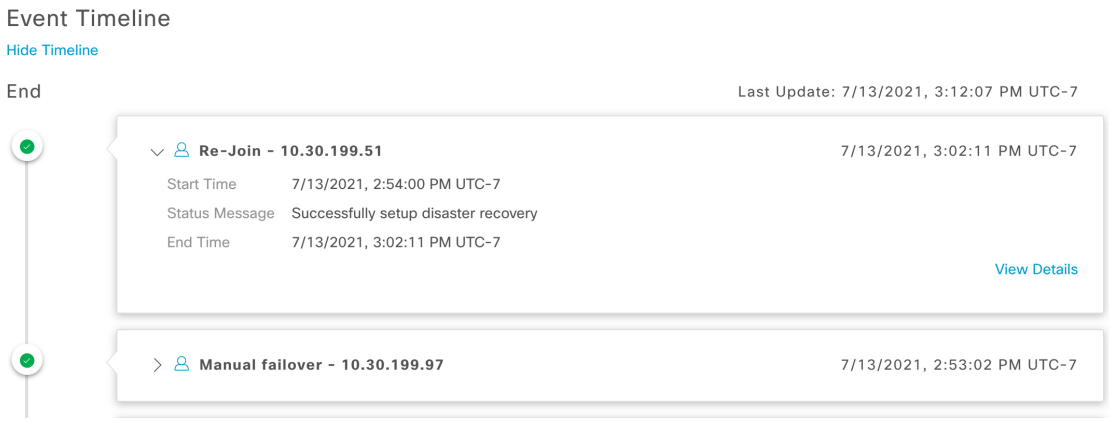
   デフォルトでは、[Monitoring] タブが選択されています。

2. ページの下部までスクロールします。

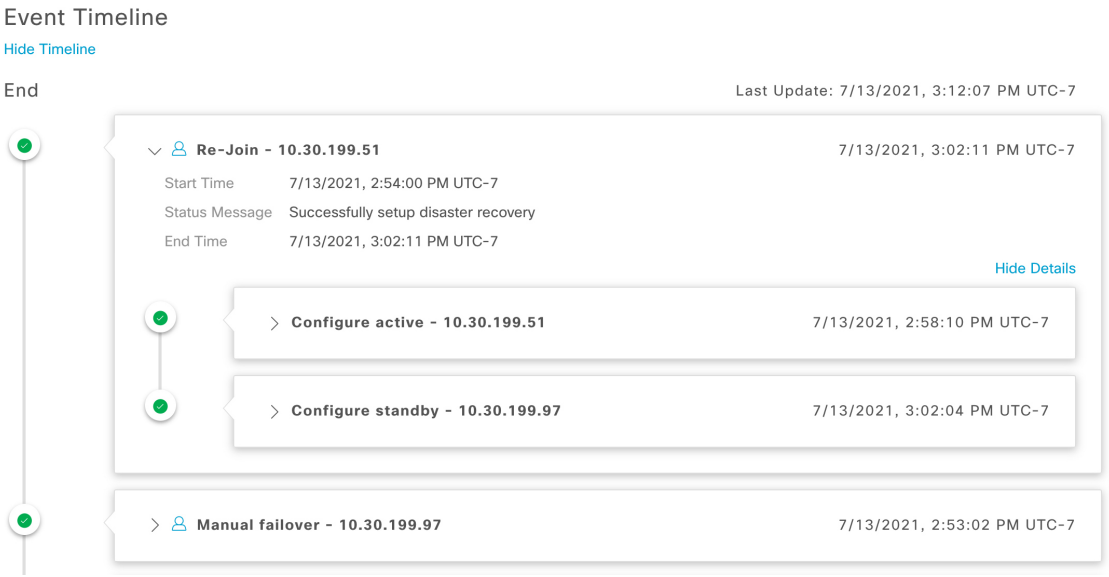
システムに対する進行中のタスクと完了したタスクが、最新のタスク（完了時のタイムスタンプに基づく）から順番に降順で表示されます。Cisco DNA Center では、それぞれのタスクについて、システム（▭）またはユーザー（👤）のどちらによって開始されたかが示されます。



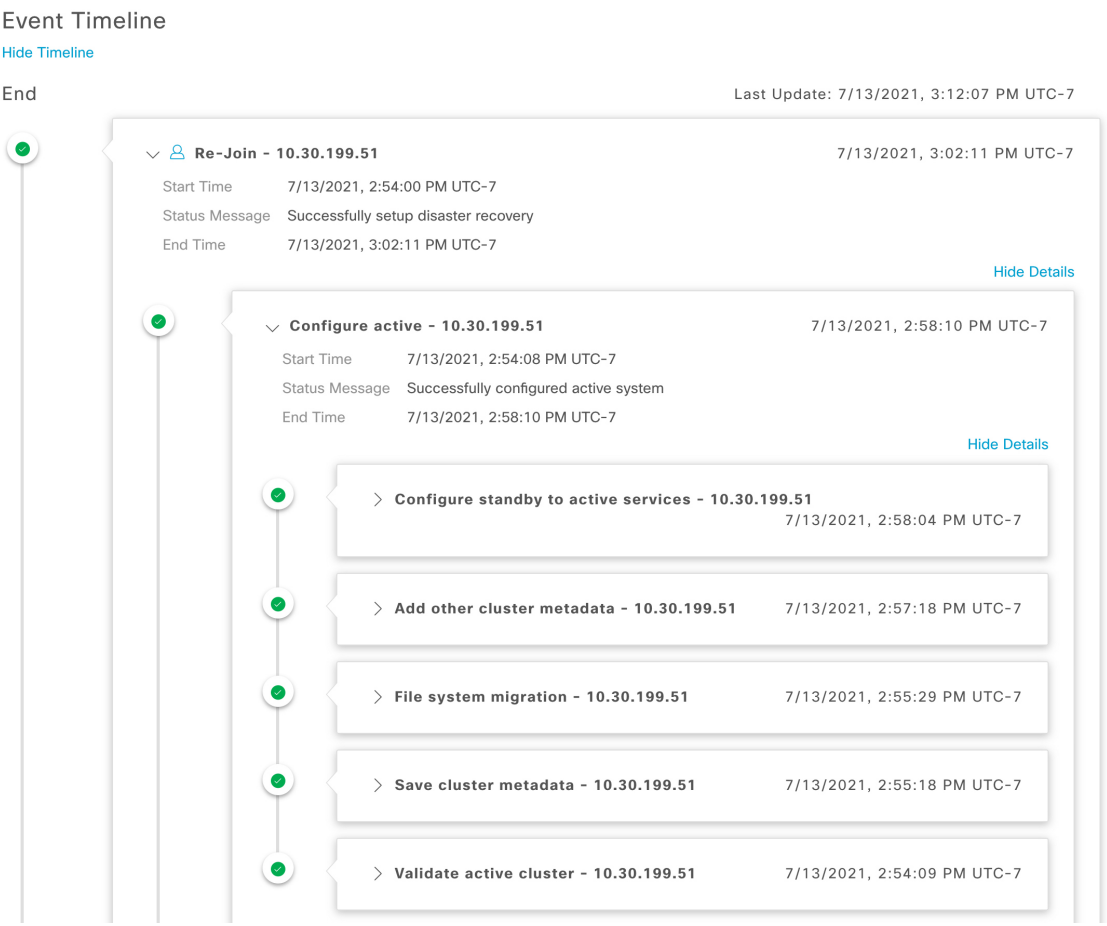
たとえば、システムの一時停止後の復元についてモニターするとします。この場合、復元プロセスの各タスクが開始されたときと完了したときに、Cisco DNA Center でイベントのタイムラインが更新されます。特定のタスクにおける処理の概要を表示するには、[>] をクリックします。



タスクに対して [View Details] 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。



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。



イベントタイムラインのモニタリング中に発生する可能性のある問題とその解決方法については、ディザスタリカバリシステムのトラブルシューティング（221ページ）を参照してください。

システムおよびサイトの状態

ディザスタリカバリ GUI の [Status] 領域には、システムの現在の状態が表示されます。次の表で、システムトポロジに表示される個々のサイトの状態を説明します。

表 *12*：アクティブサイトの状態

状態	説明
Unregistered	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Initializing	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために、他のサイトが必要とするデータを送信する準備をしています。
Initialized	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトに送信するデータを正常に準備しました。

状態	説明
Failed to Initialize	登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトが必要とするデータを送信する準備をしているときに、サイトでエラーが発生しました。
Connecting Recovery	メインサイトは、リカバリサイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Connecting Witness	メインサイトは、監視サイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Recovery Site Connected	メインサイトは、リカバリサイトとのセキュア通信を正常に確立しました。
Failed to Connect Recovery	リカバリサイトとの安全なチャネルを確立しているときに、メインサイトでエラーが発生しました。
Failed to Connect Witness	監視サイトとの安全なチャネルを確立しているときに、メインサイトでエラーが発生しました。
Registered	アクティブサイトは、他の 2 つのサイトとのセキュア通信を正常に確立しました。
Deregistering	システムから現在のディザスタリカバリ構成を削除します。
Deregister Failed	システムから現在のディザスタリカバリ構成を削除しているときにエラーが発生しました。
Validating	ディザスタリカバリ構成を開始する前に、システムの状態を検証しています。
Validated	ディザスタリカバリ構成を開始する前に、システムの状態を正常に検証しました。
Validation Failed	ディザスタリカバリ構成を開始する前のシステムの状態を検証中にエラーが発生しました。
Configuring Active	このサイトをアクティブサイトとして確立するためのワークフローを実行しています。
Failed to Configure	このサイトでディザスタリカバリを有効にするワークフローの実行中にエラーが発生しました。
Syncing Config Data	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しています。
Config Data Synced	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを正常に同期しました。
Active Sync Failed	保留中のアクティブサイトが、ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しているときにエラーが発生しました。

状態	説明
Waiting Standby Configuration	このサイトをアクティブサイトとして確立するためのワークフローが正常に完了しました。スタンバイサイトのワークフローが完了するのを待っています。
Active	サイトは、アクティブサイトとしてネットワークを正常に管理しています。
Failed to Configure	サイトは、ディザスタリカバリクラスタのアクティブサイトとして自身を有効にするワークフローの一部を実行できませんでした。
Isolating	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができているため、自身を隔離するワークフローを実行しています。
Isolated	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができているため、自身を隔離するワークフローを正常に実行しました。
Failed to Isolate	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができているため、自身を隔離するワークフローを実行中にエラーが発生しました。
Configuring Active	（システムトリガーまたは手動フェールオーバーの一部として）以前のスタンバイサイトをアクティブサイトとして構成しています。
Failed during Failover	（フェールオーバーまたは 2 つのシステムの障害からのリカバリの一部として）このサイトをアクティブサイトとして確立するワークフローの実行中にエラーが発生しました。
Pausing Active	（管理操作または計画的な停止に備えるために）アクティブサイトでディザスタリカバリ操作を無効にするワークフローを実行しています。
Active Paused	アクティブサイトでディザスタリカバリ操作を無効にしました。
Failed to Pause Active	アクティブサイトでディザスタリカバリ操作を無効にしているときにエラーが発生しました。
Active Stand Alone	他の 2 つのサイトとの接続を失った以前のアクティブサイトを、すべてのディザスタリカバリ構成を削除することにより、独立したシステムとして確立するワークフローを実行しています。
Down	アクティブサイトは、他の 2 つのサイトとの接続を失いました。

表 *13 :* スタンバイサイトの状態

状態	説明
Unregistered	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。

状態	説明
Initializing	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために、他のサイトが必要とするデータを送信する準備をしています。
Initialized	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトに送信するデータを正常に準備しました。
Failed to Initialize	登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトが必要とするデータを送信する準備をしているときに、サイトでエラーが発生しました。
Connecting Main	リカバリサイトは、メインサイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Connecting Witness	リカバリサイトは、監視サイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Main Site Connected	リカバリサイトは、メインサイトとのセキュア通信を正常に確立しました。
Failed to Connect Main	メインサイトとの安全なチャネルを確立しているときに、リカバリサイトでエラーが発生しました。
Failed to Connect Witness	監視サイトとの安全なチャネルを確立しているときに、リカバリサイトでエラーが発生しました。
Registered	スタンバイサイトは、他の 2 つのサイトとのセキュア通信を正常に確立しました。
Deregistering	システムから現在のディザスタリカバリ構成を削除します。
Deregister Failed	システムから現在のディザスタリカバリ構成を削除しているときにエラーが発生しました。
Validating	ディザスタリカバリ構成を開始する前に、システムの状態を検証しています。
Validated	ディザスタリカバリ構成を開始する前に、システムの状態を正常に検証しました。
Validation Failed	ディザスタリカバリ構成を開始する前のシステムの状態を検証中にエラーが発生しました。
Configuring Standby	このサイトをスタンバイサイトとして確立するためのワークフローを実行しています。
Failed to Configure	このサイトでディザスタリカバリを有効にするワークフローの実行中にエラーが発生しました。
Syncing Config Data	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しています。

状態	説明
Config Data Synced	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを正常に同期しました。
Standby Sync Failed	保留中のスタンバイサイトが、ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しているときにエラーが発生しました。
Waiting Active Configuration	このサイトをスタンバイサイトとして確立するためのワークフローが正常に完了しました。アクティブサイトのワークフローが完了するのを待っています。
Standby	サイトは、ディザスタリカバリクラスタのスタンバイサイトとして正常に構成されています。
Failed to Configure	サイトは、ディザスタリカバリクラスタのスタンバイサイトとして自身を有効にするワークフローの一部を実行できませんでした。
Isolating	他の 2 つのサイトとの接続が失われたため、サイトは自身を隔離するワークフローを実行しています。
Isolated	他の 2 つのサイトとの接続が失われたため、サイトは自身を隔離するワークフローを正常に実行しました。
Failed to Isolate	他の 2 つのサイトとの接続が失われたため、サイトが自身を隔離するワークフローを実行中にエラーが発生しました。
Configuring Standby	（手動フェールオーバーの一部として）以前のアクティブサイトをスタンバイ準備サイトとして構成しています。
Standby Ready	以前のアクティブシステムは、（フェールオーバーの結果として）スタンバイシステムとして構成する準備ができています。
Pausing Standby	（管理操作または計画的な停止に備えるために）スタンバイサイトでディザスタリカバリ操作を無効にするワークフローを実行しています。
Standby Paused	スタンバイサイトでディザスタリカバリ操作を無効にしました。
Failed to Pause Standby	スタンバイサイトでディザスタリカバリ操作を無効にしているときにエラーが発生しました。
Standby Stand Alone	他の 2 つのサイトとの接続を失った以前のスタンバイサイトを、すべてのディザスタリカバリ構成を削除することにより、独立したシステムとして確立するワークフローを実行しています。
Down	サイトは、他の 2 つのサイトとの接続を失いました。

表 *14* : 監視サイトの状態

状態	説明
Unregistered	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Registered	このサイトが監視サイトとして指定され、検証チェックが正常に完了しました。
Up	監視サイトの設定が正常に完了しました。
Down	サイトは、他の 2 つのサイトとの接続を失いました。

ディザスタリカバリシステムのアップグレード

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 のバージョンは以前の 2.1.x でしたが、最新の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。アップグレードを完了するには、次の手順を実行します。

ステップ 1 システムの一時停止 （213 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 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*』を参照）。

ステップ 3 現在の監視サイトの置換 （201 ページ）。

ステップ 4 システムへの再参加 （216 ページ）。

（注） Cisco DNA Center のバージョンを 2.3.4 以前から 2.3.5 にアップグレードした後、再参加操作が最初に開始されたときにデータ移行が行われます。そのため、この操作の完了には時間がかかります。この移行により、存在する Cisco DNA Center データの量に応じて、完了までに数分または数時間かかる場合があります。このデータ移行は、アップグレード後にのみ行われることに注意してください。データ移行は、その後の再参加操作には影響しません。

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エンタープライズネットワークの他の要素（およびスタンバイサイトと監視サイト）と 7 分間通信できなかったことを認識すると、スタンバイサイトがその役割

を引き受けるのに必要なタスクを完了するため、中断することなくネットワーク動作を継続できます。

- 手動：ネットワーク管理者であるユーザーがシステムのアクティブサイトとスタンバイサイトの現在の役割を入れ替えるように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。手動フェールオーバーは、現在のアクティブサイトで問題が発生していることが判明し、スタンバイサイトを新しいアクティブサイトとしてプロアクティブに指定する場合に便利です。手動フェールオーバーを開始するには、次の手順を実行します。

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

ステップ1 メニューアイコン（☰）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。

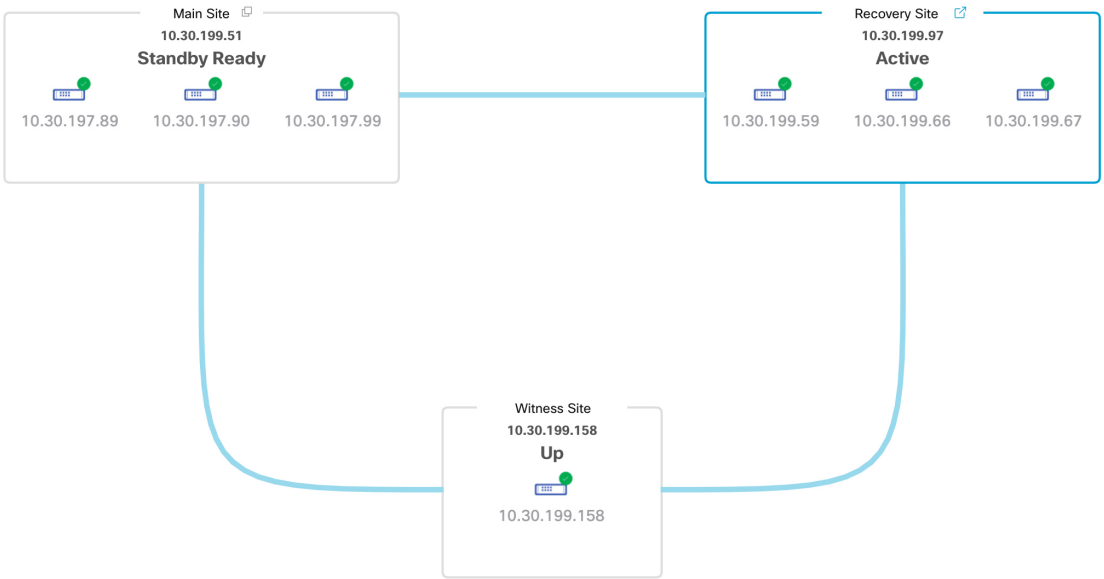
デフォルトでは、[Monitoring]タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。次の例では、ユーザーは現在のアクティブサイトにログインしています。

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。



この時点で、メインサイトとリカバリサイトの接続が解除され、データの複製は行われなくなります。前のアクティブサイトに問題がある場合は、この間にそれらの問題を解決します。

前のアクティブサイトをディザスタリカバリシステムに再度追加するまで、次のフェールオーバー（システムによるフェールオーバーとユーザーによるフェールオーバーの両方）を開始することはできません。

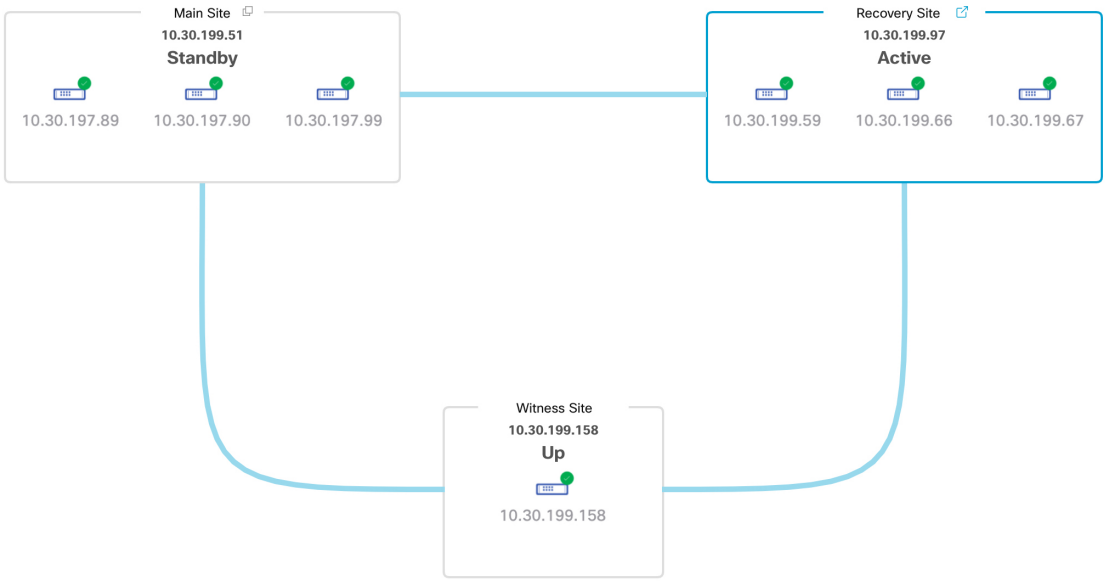
ステップ 4 メインサイトとリカバリサイトを再接続し、ディザスタリカバリシステムを再設定します。

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。

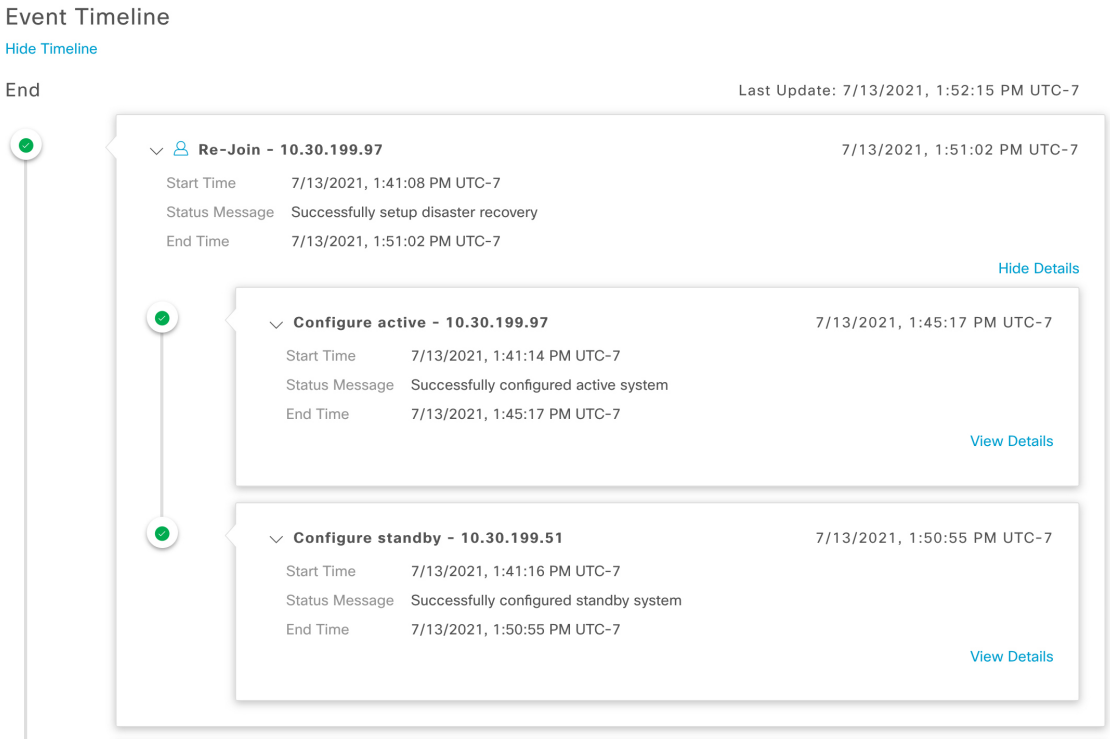
ステップ 5 [Continue] をクリックして次に進み、データの複製を再開します。

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。



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。



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、ディザスタリカバリシステムを一時停止して、次のいずれかを実行します。

- クラスタのアップグレードや追加パッケージのインストールなどの管理タスクを完了します。
- システムまたはディザスタリカバリ証明書を置き換えます。
- メイン、リカバリ、または監視サイトクラスタでメンテナンスを実行します。
- 計画的なネットワーク停止または停電に備えます。

システムの一時停止

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 メニューアイコン（☰）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] をクリックします。

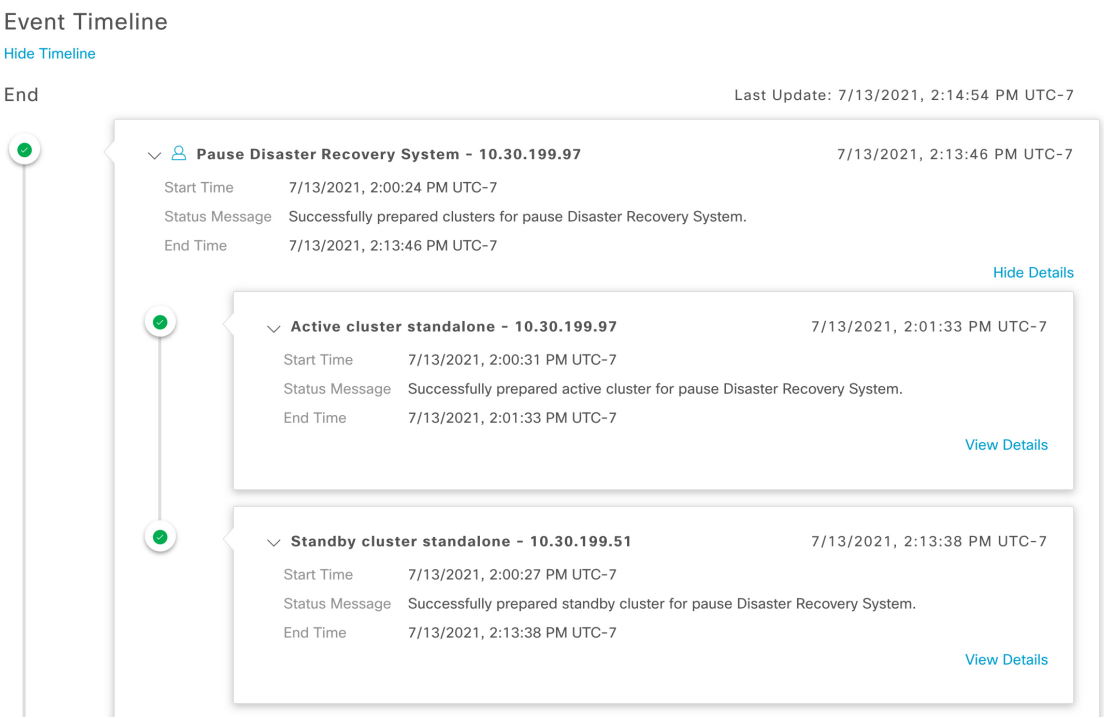
ステップ 3 表示されたダイアログで、[Continue] をクリックして次に進みます。

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。

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。

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] タブの右上に表示されたステータスが [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 Disaster Recovery System] タスクが正常に完了したことを確認します。



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 メニューアイコン（☰）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。

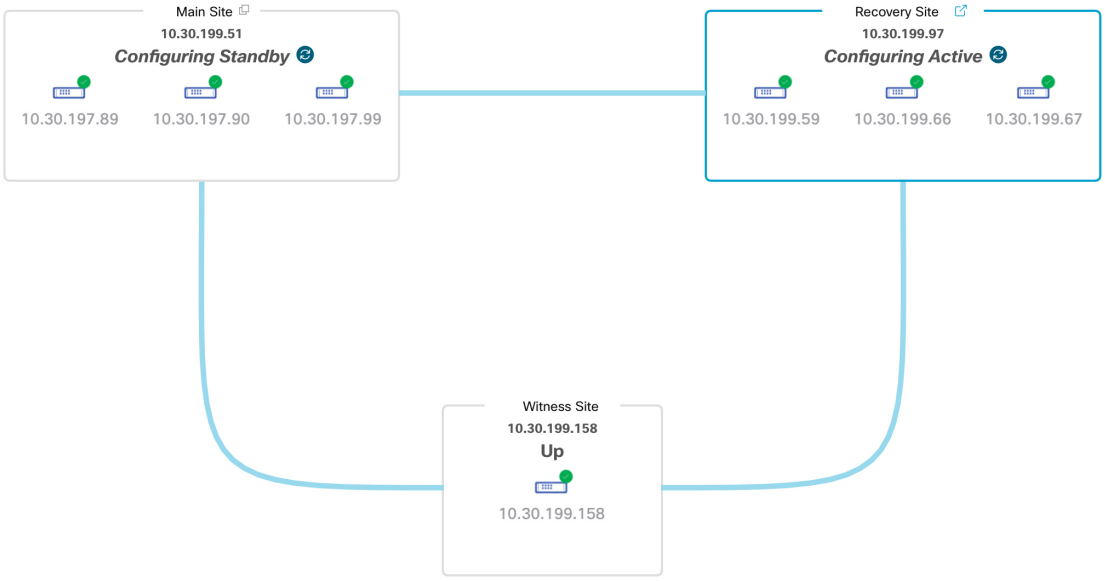
デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。

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

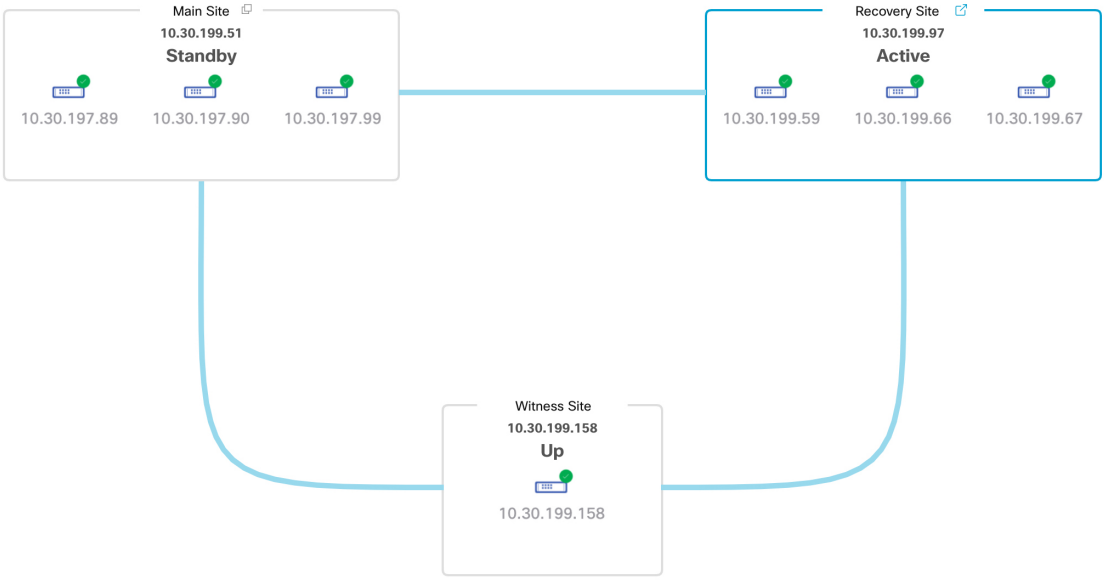
スタンバイサイトのすべてのデータが消去されることを示すダイアログが表示されます。

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。



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。



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。

ディザスタリカバリシステムの考慮事項

このセクションでは、ディザスタリカバリシステムを管理する際の注意事項について説明します。

バックアップおよび復元の検討事項

- 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 （213 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 （216 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。
- フェールオーバーが発生すると、展開のバックアップと復元の設定およびスケジュールは、新しいアクティブサイトに複製されません。再度構成する必要があります。
- 展開に適用する場合は、Cisco DNA Center への着信 TLS 接続の TLS バージョンをアップグレードすることをお勧めします。『Cisco DNA CenterSecurity Best Practices Guide』の「Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)」トピックを参照してください。メインサイトをすでにアップグレードしている場合は、リカバリサイトもアップグレードすることをお勧めします（理想的には、ディザスタリカバリシステムをアクティブ化する前、またはフェールオーバーが発生した後）。

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（161 ページ）を参照してください。

ノードまたはクラスタの交換に関する考慮事項

ディザスタリカバリシステムの構成を壊さずに、次のいずれかを実行することはできません。

- 1+1+1 セットアップでノードの 1 つを置き換える。
- 3+3+1 セットアップで 1 つのサイトのすべてのノードを置き換える。

この必要がある場合は、システムの登録解除（202 ページ）で説明されている手順を完了して、システムを再起動してください。

再構成に関する考慮事項

リカバリサイトにあるアプライアンスに存在するデータは、次のシナリオで削除されます。

- ディザスタリカバリシステムを初めてセットアップし、システムをアクティブ化するとき。
- リカバリサイトが現在アクティブなサイトである場合に、システムを一時停止し、登録を解除してから、リカバリサイトとして再登録するとき。

既存のディザスタリカバリシステムを再構成するときは、どのサイトが現在アクティブなサイトであるかを確認し、それをシステムのメインサイトとして登録してください。または、リカバリサイトのデータ（現在アクティブな場合）のバックアップを作成し、システムの再構成の前にこのデータをシステムのメインサイトに復元することもできます。

HA に関する考慮事項

ディザスタリカバリシステムの構成を壊さずに、メインサイトとリカバリサイトを単一ノードクラスタから HA クラスタに変換することはできません。必要な場合は、次の手順を実行します。

1. システムの登録解除 （202 ページ）。
2. 両方のサイトを HA クラスタに変換します。
3. 再登録し、ディザスタリカバリを再アクティブ化します（ディザスタリカバリの設定 （191 ページ）を参照）。

サイト障害に関する考慮事項

デフォルトでは、ディザスタリカバリシステムは7分間待機してから、サイトに障害が発生したことを認識し、次のいずれかのアクションを実行します。

- アクティブサイトがダウンすると、フェールオーバープロセスが開始されます。
- スタンバイサイトまたは監視サイトのいずれかがダウンすると、システムはそのサイトをダウンとしてマークし、[Action] 領域からタスクを開始する機能を無効にします。

7分が経過する前にタスクを開始しようとすると、完了できない理由を示すメッセージが [Details] 領域に表示されます。

ディザスタリカバリイベントの通知

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 Event Notifications」を参照してください。この手順を完了

したら、**[Platform]** > **[Developer Toolkit]** > **[Events]** テーブルで [SYSTEM-DISASTER-RECOVERY] 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 （213 ページ）。
2. メインサイトとリカバリサイトの両方で、現在のシステム証明書を置き換えます。メニューアイコン（☰）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 （216 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`
OK	メインサイトの登録が正常に完了しました。	`Successfully Registered Main Site`
OK	リカバリサイトの登録が正常に完了しました。	`Successfully Registered Recovery Site`
OK	監視サイトの登録が正常に完了しました。	`Successfully Registered Witness Site`
OK	ディザスタリカバリシステムが正常に一時停止しました。	`DR Pause Success`
OK	スタンバイサイトが動作しています。	`Standby Site Up`
OK	監視サイトが動作しています。	`Witness Site Up`
OK	ディザスタリカバリシステムが正常に登録解除されました。	`Unregister Success`
Degraded	メインサイトまたはリカバリサイトへのフェールオーバーが失敗しました。	`Failover Failed`

システムのヘルスステータス	イベント	通知
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`
NotOk	ディザスタリカバリシステムの登録解除に失敗しました。	`Unregistration Failed`
NotOk	メインサイトの登録に失敗しました。	`Main Registration Failed`
NotOk	リカバリサイトの登録に失敗しました。	`Recovery Registration Failed`
NotOk	監視サイトの登録に失敗しました。	`Witness Registration Failed`

ディザスタリカバリシステムのトラブルシューティング

次の表に、ディザスタリカバリシステムで発生する可能性がある問題とその対処方法を示します。

（注） ディザスタリカバリ操作が失敗またはタイムアウトした場合は、[Retry] をクリックして操作を再度実行します。問題が解消されず、その解決策が次の表に記載されていない場合は、Cisco TAC にお問い合わせください。

表 *15* : ディザスタリカバリシステムの問題

エラーコード	メッセージ	ソリューション
SODR10007	`Token does not match.`	リカバリサイトの登録時に提供されたトークンが、メインサイトの登録時に生成されたトークンと一致しません。メインサイトの **[Disaster Recovery]** > **[Configuration]** タブで、[Copy Token] をクリックして正しいトークンをコピーします。
SODR10048	`Packages (package names) 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	`() site is trying to () with invalid IP address. Expected is (); actual is ().`	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 (recovery or witness site).`	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 (main or recovery site).`	サイトの 3 台のノードすべてが稼働しているかどうかを確認します。
SODR10076	`High availability should be enabled on (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。 1. HA を有効にする必要があるサイトにログインします。 2. メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[System Configuration]** > **[High Availability]** の順に選択します。 3. [Activate High Availability] をクリックします。
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、「Cisco DNA Center サーバー証明書の更新 （95 ページ）」を参照してください。
SODR10113	`Save cluster metadata failed.`	適切なリカバリ手順の実行については、Cisco TAC にお問い合わせください。

エラーコード	メッセージ	ソリューション
SODR10118	`Appliance mismatch between main () and recovery ().`	メインサイトとリカバリサイトで異なるアプライアンスが使用されています。ディザスタリカバリを正常に登録するには、両方のサイトで同じ 56 または 112 コアアプライアンスを使用する必要があります。
SODR10121	`Failed to advertise BGP. Reason: ().`	詳細については、「BGP ルートアドバタイズメントに関する問題のトラブルシューティング （231 ページ）」を参照してください。
SODR10122	`Failed to stop BGP advertisement. Reason: ().`	詳細については、「BGP ルートアドバタイズメントに関する問題のトラブルシューティング （231 ページ）」を参照してください。
SODR10123	`Failed to establish secure connection between main () and ()().`	この問題に対する解決策はありません。Cisco TAC に連絡して、サポートを受けてください。
SODR10124	`Cannot ping VIP: (main, recovery, or witness site's VIP or IP address).`	次の手順を実行します。 • 指定したアドレスが正しいことを確認します。 • アドレスが他のアドレスから到達可能であるかどうかを確認します。
SODR10129	`Unable to reach main site. ()`	メインサイトに設定されたエンタープライズ仮想 IP アドレスが、リカバリサイトと監視サイトから到達可能であるかどうかを確認します。
SODR10132	`Unable to check IP addresses are on the same interface. 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。 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。

エラーコード	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 Certificates]** の順に選択）からサードパーティ証明書を再度アップロードして、登録を再試行します。問題が解決しない場合は、Cisco TAC にお問い合わせください。
SODR10138	`Self-signed certificate is not allowed. Upload a third-party certificate and retry.`	—
SODR10139	`Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate.`	メインサイトとリカバリサイトにインストールされているサードパーティ証明書に、ディザスタリカバリシステム用に指定された別のDNS名があります。お使いのシステムの DNS 名を指定するサードパーティ証明書を生成し、この証明書を両方のサイトにアップロードします。 （注） DNS名にワイルドカードが使用されていないことを確認します。
SODR10140	`Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.`	メインサイトとリカバリサイトにインストールされているサードパーティ証明書で、ディザスタリカバリシステムの DNS 名が指定されていません。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。

エラーコード	メッセージ	ソリューション
—	—	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。
—	`External postgres services does not exists to check service endpoints.`	次の手順を実行します。 **1.** エラーが発生したサイトにログインします。 **2.** 次のコマンドを実行します。 • **Kubectl get sep -A** • **kubectl get svc -A | grep external** **3.** 結果の出力で、`external-postgres` を検索します。 **4.** 存在する場合は、**kubectl delete sep external-postgres -n fusion** コマンドを実行します。 **5.** 以前に失敗した操作を再試行します。
—	`Success with errors.`	フェールオーバーの開始後またはディザスタリカバリシステムの一時停止後にこのメッセージが表示される場合は、1 つ以上のサービスで軽微なエラーが発生したにもかかわらず操作が正常に完了したことを示しています。先に進み、[Rejoin] をクリックすることで、システムを再起動できます。これらのエラーは、その操作によって解決されます。
—	`Failed.`	このメッセージは、1 つ以上のサービスで重大なエラーが発生したためにディザスタリカバリ操作が失敗したことを示しています。この障害をトラブルシューティングするために、イベントタイムラインを表示し、関連するエラーにドリルダウンすることをお勧めします。このメッセージが表示されたら、[Retry]をクリックして操作を再実行します。
—	`Cannot ping VIP: (`*`VIP address`*`).`	システムに設定されているエンタープライズ VIP アドレスが到達可能であることを確認します。
—	`VIP drop-down list is empty.`	システムの VIP アドレスとクラスタ内リンクが正しく設定されていることを確認します。

エラーコード	メッセージ	ソリューション
—	`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。
—	`The GUI indicates that the standby site is still down after it has come back online.`	スタンバイサイトがダウンしたときに、そのサイトを 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。 スタンバイサイトを復元するには、次の手順を実行します。 1. SSH クライアントで、スタンバイサイトにログインします。 2. **maglev maintenance disable** コマンドを実行して、サイトをメンテナンスモードから復旧させます。 3. Cisco DNA Center にログインします。 4. メニューアイコン（☰）をクリックして、**[System]** > **[Disaster Recovery]** の順に選択します。 デフォルトでは、[Monitoring] タブが選択されています。 5. ディザスタリカバリシステムを再起動するために、[Action] 領域で [Rejoin] をクリックします。
—	`Multiple services exists for MongoDB to check node-port label.`	デバッグ用に、MongoDB ノードポートがサービスとして公開されます。このポートを特定して非表示にするには、次のコマンドを実行します。 • **kubectl get svc --all-namespaces | grep mongodb** • **magctl service unexpose mongodb** <*port-number*>
—	`Multiple services exist for Postgres to check node-port label.`	デバッグ用に、Postgres ノードポートがサービスとして公開されます。このポートを特定して非表示にするには、次のコマンドを実行します。 • **kubectl get svc --all-namespaces | grep postgres** • **magctl service unexpose postgres** <*port-number*>

2 サイト障害シナリオ

2 サイト障害は、ディザスタリカバリシステムにある 3 つのサイトのうち少なくとも 2 つが同時にダウンした場合、またはサイトがパーティション化された場合に発生します。Cisco DNA Center がさまざまな障害シナリオにどのように対応するか、および実行する必要があるユーザーアクションについては、次の表を参照してください。

障害シナリオ	システムおよびユーザーの応答
シナリオ1：システムの2つのサイトがダウンします。	**1.** システムは、まだオンラインのサイトを分離します。 **重要** この操作が失敗した場合でも、このサイトをスタンドアロンサイトとして運用する場合は、手順 3 で説明されている最初のタスクを完了します。 **2.** このサイトにログインします。 **3.** サイトをスタンドアロンサイトとして動作させる場合は、[Standalone] をクリックし、表示されるダイアログボックスで [Continue] をクリックします。 サイトをスタンドアロンサイトとして動作させたくない場合は、まず、ダウンした 2 つのサイトを復旧します。次のいずれかを実行します。 • 監視サイトがオフラインのままである場合は、シナリオ 3 のシステムとユーザーの応答を参照してください。 • スタンバイサイトがオフラインのままの場合は、シナリオ 4 のシステムとユーザーの対応を参照してください。 • アクティブサイトがオフラインのままである場合は、シナリオ 5 のシステムとユーザーの応答を参照してください。 サイトがスタンドアロンモードになると、システムはそのサイトの仮想 IP アドレスを自動的に構成します。また、ネットワークの再プロビジョニングを防ぐために、仮想 IP アドレスルートをアドバタイズします。

障害シナリオ	システムおよびユーザーの応答
シナリオ2：アクティブサイト、スタンバイサイト、および監視サイトがダウンし、ほぼ同時にオンラインに戻ります。	1. システムは、アクティブサイトとスタンバイサイトを分離します。 2. システムはアクティブサイトを復元し、スタンバイサイトは [Standby Ready] 状態に入ります。 3. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 4. ディザスタリカバリの設定 （191 ページ）。
シナリオ3：アクティブサイト、スタンバイサイト、および監視サイトがダウンします。アクティブサイトとスタンバイサイトはオンラインに戻りますが、監視サイトはオフラインのままです。	1. システムは、アクティブサイトとスタンバイサイトを分離します。 2. システムはアクティブサイトを復元し、スタンバイサイトは [Standby Ready] 状態に入ります。 3. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 4. 次のいずれかを実行します。 • 監視サイトがオンラインに戻った後、ディザスタリカバリの設定 （191 ページ）に従います。 • システムの一時停止 （213 ページ）。

障害シナリオ	システムおよびユーザーの応答
シナリオ4：アクティブサイト、スタンバイサイト、および監視サイトがダウンします。アクティブサイトと監視サイトはオンラインに戻りますが、スタンバイサイトはオフラインのままです。	1. システムはアクティブサイトを分離してから復元します。 2. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 3. 以前のアクティブサイトがオンラインに戻り、[Standby Ready] 状態になった後、ディザスタリカバリの設定（191 ページ）に従います。 スタンバイサイトのノードを交換する必要があると判断した場合は、代わりに次の手順を実行します。 1. 監視サイトにログインして **witness reset** コマンドを実行します。 2. アクティブサイトにログインし、[Standalone] をクリックしてから、[Continue] をクリックします。 3. スタンバイサイトのノードを交換します。 4. 監視サイトが以前に使用されていたものよりも新しい仮想マシンを使用する場合は、監視サイトのインストール（189 ページ）で説明されている手順を実行します。それ以外の場合は、次のステップに進みます。 5. ディザスタリカバリの設定（191 ページ）。

障害シナリオ	システムおよびユーザーの応答
シナリオ5：アクティブサイト、スタンバイサイト、および監視サイトがダウンします。スタンバイサイトと監視サイトはオンラインに戻り、アクティブサイトはオフラインのままです。	1. システムはスタンバイサイトを分離し、新しいアクティブサイトとして確立します。 2. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 3. 以前のアクティブサイトがオンラインに戻り、[Standby Ready] 状態になった後、ディザスタリカバリの設定（191 ページ）に従います。 スタンバイサイトのノードを交換する必要があると判断した場合は、代わりに次の手順を実行します。 1. 監視サイトにログインして **witness reset** コマンドを実行します。 2. アクティブサイトにログインし、[Standalone] をクリックしてから、[Continue] をクリックします。 3. スタンバイサイトのノードを交換します。 4. 監視サイトが以前に使用されていたものよりも新しい仮想マシンを使用する場合は、監視サイトのインストール（189 ページ）で説明されている手順を実行します。それ以外の場合は、次のステップに進みます。 5. ディザスタリカバリの設定（191 ページ）。

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トします。

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 Disaster Recovery System]** > **[View Details]** > **[Configure active]** > **[View Details]** の順に選択）。

タスクが失敗した場合は、次を実行してから手順 1b に進みます。

1. エラーメッセージに示されているネイバールータが稼働しているかどうかを確認する。
2. ネイバールータと 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、ネイバー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) 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 | lql**

ログファイルを表示するときは、エラーメッセージがないか確認します。メッセージがない場合は、BGP セッションが正しく機能していることを示します。

d) 次のコマンドを実行して、Cisco DNA Center とそのネイバールータ間の 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、ネイバールータの 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ールータから、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 であるとします。これが出力に表示される最初の IP アドレスである場合は、アドバタイズされていることを確認します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。