



バックアップと復元

- [バックアップと復元について](#) (1 ページ)
- [バックアップサーバの要件](#) (2 ページ)
- [バックアップストレージ要件](#) (4 ページ)
- [NFS サーバの設定例：Ubuntu](#) (4 ページ)
- [NFS サーバの設定例：CentOS](#) (5 ページ)
- [NFS を許可するファイアウォールルールの設定](#) (6 ページ)
- [バックアップサーバの設定](#) (7 ページ)
- [今すぐデータをバックアップ](#) (9 ページ)
- [データのバックアップスケジュール](#) (10 ページ)
- [バックアップからデータを復元](#) (11 ページ)

バックアップと復元について

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

バックアップ

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

自動化データは、Cisco DNA Center データベース、クレデンシヤル、ファイルシステム、およびファイルで構成されています。自動化バックアップは完全バックアップです。

アシュアランスデータは、ネットワークアシュアランスと分析データで構成されています。アシュアランスデータの最初のバックアップは完全バックアップで、その後は増分バックアップです。



重要 バックアップファイルは変更しないでください。変更すると、バックアップファイルを Cisco DNA Center に復元できない場合があります。

Cisco DNA Center はバックアップファイルを作成して、リモートサーバにポストします。各バックアップは、ディレクトリ名としてUUIDを使用して一意に格納されます。リモートサーバの要件の詳細については、[バックアップサーバの要件 \(2 ページ\)](#) を参照してください。

一度に1つのバックアップのみ実行できます。一度に複数のバックアップを実行することはできません。

バックアップの実行中は、ファイルサービスにアップロードされたファイルを削除することはできず、ファイルに加えた変更はバックアッププロセスによってキャプチャされないことがあります。

次の点を推奨します。

- データベースとファイルの現在のバージョンを維持するために毎日バックアップを実行する。
- 設定に変更を加えた後はバックアップを実行する（デバイスで新しいポリシーを作成または変更した場合など）。
- バックアップは影響の少ない時間帯かメンテナンス時間にのみ実行する。

週の特定期の時刻に週単位のバックアップをスケジュールできます。

Restore

Cisco DNA Center を使用してリモートサーバからバックアップファイルを復元できます。

バックアップファイルを復元すると、Cisco DNA Center によって既存のデータベースとファイルが削除され、バックアップデータベースとファイルで置き換えられます。復元を実行している間、Cisco DNA Center は使用できません。

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

バックアップは、別の IP アドレスを持つ Cisco DNA Center アプライアンスに復元することができます。この状況は、Cisco DNA Center の IP アドレスが変更されていて、古いシステムから復元する必要がある場合に生じる可能性があります。

バックアップサーバの要件

バックアップサーバは、次のいずれかのオペレーティングシステムを実行している必要があります。

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

自動化データバックアップのサーバ要件

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

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

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

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

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

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

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

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

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

アシュアランスバックアップのサーバ要件

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

- NFS v4 および NFS v3 をサポートしている (このサポートを確認するには、サーバから **nfsstat -s** を入力します)。
- NFS エクスポートディレクトリに対する読み取り/書き込み権限がある。
- Cisco DNA Center と NFS サーバ間のネットワーク接続が安定している。
- Cisco DNA Center と NFS サーバ間のネットワーク速度が十分速い。



(注) NFS 搭載ディレクトリを Cisco DNA Center のバックアップサーバディレクトリとして使用することはできません。カスケードされた NFS マウントは遅延の層が増えるため、サポートされません。

バックアップストレージ要件

Cisco DNA Center は、外部 NFS デバイスに アシユアランス データのバックアップコピーを保存し、外部リモート同期 (rsync) のターゲットの場所に自動化データのバックアップコピーを保存します。バックアップには、必要な保存期間をカバーするのに十分な外部ストレージを割り当てる必要があります。次のストレージを推奨します。

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

補足事項：

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

NFS サーバの設定例：Ubuntu

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

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

たとえば、次のようにコマンドを入力します。

```
§ sudo apt-get update
```

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

たとえば、次のようにコマンドを入力します。

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

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

たとえば、次のようにコマンドを入力します。

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

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

たとえば、次のようにコマンドを入力します。

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

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

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

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

たとえば、次のようにコマンドを入力します。

```
§ sudo exportfs -a
```

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

たとえば、次のようにコマンドを入力します。

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

NFS サーバの設定例 : CentOS

次の手順は、CentOS での NFS サーバの設定例を示しています。

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

たとえば、次のようにコマンドを入力します。

```
§ sudo yum check-update
```

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

たとえば、次のようにコマンドを入力します。

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

ステップ3 NFS サーバを有効にして起動します。

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

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

たとえば、次のようにコマンドを入力します。

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

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

たとえば、次のようにコマンドを入力します。

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

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

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

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

たとえば、次のようにコマンドを入力します。

```
$ sudo exportfs -a
```

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

たとえば、次のようにコマンドを入力します。

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

NFS を許可するファイアウォールルールの設定

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

ファイアウォールルールの設定 : Debian/Ubuntu

Debian/Ubuntu では、次の手順を実行します。

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

```
$ sudo ufw status
```

ファイアウォールが無効の場合、出力には次のように表示されます。

```
Status: inactive
```

ファイアウォールが有効になっている場合は、次のように出力されます。

```
Status: active
```

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

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

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

```
sudo ufw allow portmapper
sudo ufw allow nfs
sudo ufw allow mountd
```

ファイアウォールルールの設定 : RedHat/CentOS

RedHat/CentOS の場合は、次の手順を実行します。

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

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

次の行が存在しない場合は、`/etc/nfs.conf` に追加します。

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

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

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

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

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

バックアップサーバの設定

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

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

この手順では、両方のサーバを設定する方法を示します。

始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。
- データのバックアップに使用する予定のサーバは、[バックアップサーバの要件 \(2 ページ\)](#) で説明されている要件を満たす必要があります。

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

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

a) 次の設定を定義します。

フィールド	説明
SSH IP Address	SSH が可能なリモートサーバの IP アドレス。
SSH ポート	SSH が可能なリモートサーバのポートアドレス。
サーバパス	バックアップファイルが保存されるサーバ上のフォルダへのパス。
Username	暗号化されたバックアップを保護するために使用するユーザ名。
[Password]	暗号化されたバックアップを保護するために使用するパスワード。
Encryption Passphrase	バックアップのセキュリティの影響を受けやすいコンポーネントを暗号化するために使用するパスフレーズ。これらのセキュリティに影響を受けやすいコンポーネントには、証明書とクレデンシャルが含まれます。 これは入力が必要とされる必須のパスフレーズで、バックアップファイルを復元するときに入力する必要があります。このパスフレーズがなければ、バックアップファイルは復元されません。

b) [Apply] をクリックします。

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

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

ステップ4 [Apply] をクリックします。

今すぐデータをバックアップ

次のデータセットのいずれかをバックアップするように選択できます。

- 自動化データのみ。
- 自動化データと アシユアランス のデータ。

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



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

始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。
- バックアップサーバが[バックアップサーバの要件 \(2 ページ\)](#)で説明されている要件を満たしている。
- バックアップサーバが Cisco DNA Center で設定されている。詳細については、[バックアップサーバの設定 \(7 ページ\)](#)を参照してください。

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

(注) まだバックアップサーバを設定していない場合、続行する前に、Cisco DNA Center がバックアップサーバの設定を要求します。[Configure Settings] をクリックします。[バックアップサーバの設定 \(7 ページ\)](#)を参照してください。

ステップ2 [Add] をクリックします。

[Create Backup] ペインが表示されます。

ステップ3 [Backup Name] フィールドで、バックアップの一意の名前を入力します。

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

ステップ5 バックアップの範囲を定義します。

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

ステップ 6 [作成 (Create)] をクリックします。

- (注) 現在のバックアップステータスと以前のバックアップの履歴は、[Activity] タブで確認できます。進行中のバックアップジョブがない場合にのみ、新しいバックアップを作成できます。正常に完了したバックアップジョブは、[Backup] タブで確認できます。

バックアッププロセス中は、Cisco DNA Center によりバックアップデータベースおよびファイルが作成されます。バックアップファイルは、リモートサーバの指定された場所に保存されます。バックアップファイルは単一のセットに限らず、一意の名前で識別される複数のバックアップファイルを作成できます。バックアッププロセスが完了すると、「Backup done!」通知を受信します。

- (注) バックアッププロセスが失敗しても、アプライアンスまたはそのデータベースへの影響はありません。Cisco DNA Center にバックアップの失敗の原因を示すエラーメッセージが表示されます。バックアップの失敗の最も一般的な原因は、ディスク領域の不足です。バックアッププロセスが失敗した場合は、リモートサーバに十分なディスク容量があるかどうかを確認し、別のバックアップを試行します。

データのバックアップスケジュール

定期的なバックアップをスケジュールし、実行する曜日と時間を定義することができます。

始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。
- バックアップサーバが[バックアップサーバの要件 \(2 ページ\)](#)で説明されている要件を満たしている。
- バックアップサーバが Cisco DNA Center で設定されている。詳細については、[バックアップサーバの設定 \(7 ページ\)](#)を参照してください。

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

[Schedule] ウィンドウが表示されます。

ステップ2 [Add] をクリックします。

[Create Backup] ペインが表示されます。

ステップ3 [Backup Name] フィールドで、バックアップの一意の名前を入力します。

ステップ4 [Schedule weekly] をクリックします。

ステップ5 バックアップをスケジュールする日付と時刻を選択します。

ステップ6 バックアップの範囲を定義します。

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

ステップ7 [Schedule] をクリックします。

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

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

正常に完了したバックアップジョブは、[Backup] タブで確認できます。

バックアッププロセス中は、Cisco DNA Center によりバックアップデータベースおよびファイルが作成されます。バックアップファイルは、リモートサーバの指定された場所に保存されます。バックアップファイルは単一のセットに限らず、一意の名前で識別される複数のバックアップファイルを作成できます。バックアッププロセスが完了すると、「Backup done!」通知を受信します。

(注) バックアッププロセスが失敗しても、アプライアンスまたはそのデータベースへの影響はありません。Cisco DNA Center にバックアップの失敗の原因を示すエラーメッセージが表示されます。バックアップの失敗の最も一般的な原因は、ディスク領域の不足です。バックアッププロセスが失敗した場合は、リモートサーバに十分なディスク容量があるかどうかを確認し、別のバックアップを試行します。

バックアップからデータを復元

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

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



注意 Cisco DNA Center の復元プロセスでは、データベースとファイルのみ復元します。復元プロセスでは、ネットワークの状態や、最後のバックアップ以降に加えられた変更は復元されません。これには、新しいネットワークポリシーやパスワード、証明書、トラストプールバンドル、または更新されたこれらのものが含まれます。



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

始める前に

次の要件が満たされていることを確認します。

- SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、[ユーザ ロールの概要](#)を参照してください。
- データを復元する元となるバックアップがあること。

データを復元する場合、Cisco DNA Center はメンテナンスモードに入り、復元プロセスが終わるまで使用できません。Cisco DNA Center を使用不可にできるときにデータを復元してください。

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

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

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

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

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

ステップ 3 [Actions] 列で、[Restore] を選択します。

Cisco DNA Center の復元プロセスで、データベースとファイルを復元します。復元プロセスでは、ネットワークの状態や、最後のバックアップ以降に加えられた変更は復元されません。これには、作成された新しいネットワークポリシーや、新規または更新されたパスワード、新規または更新された証明書やトラストプールバンドルが含まれます。

復元中、バックアップファイルは現在のデータベースを削除して置き換えます。

復元プロセス中、Cisco DNA Center はメンテナンスモードになります。Cisco DNA Center がメンテナンスモードを終了するまで待つてから、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。
