



# ストレージアレイ SANtricity 11.8

NetApp  
December 16, 2024

# 目次

ストレージアレイ.....	1
検出の概要.....	1
概念.....	1
アレイの検出.....	3
アレイの管理.....	6

# ストレージアレイ

## 検出の概要

ストレージリソースを管理するには、まずネットワーク内のストレージアレイを検出する必要があります。

### アレイの検出方法

[追加/検出]ページを使用して、組織のネットワークから管理するストレージアレイを検索して追加します。複数のアレイを検出することも、単一のアレイを検出することもできます。そのためには、ネットワークIPアドレスを入力すると、Unified Managerはその範囲内の各IPアドレスへの接続を個別に試行します。

詳細：

- ["アレイの検出に関する考慮事項"](#)
- ["複数のストレージアレイの検出"](#)
- ["単一のアレイの検出"](#)

### アレイの管理方法

アレイを検出したら、\* Manage-All \*ページに移動します。このページでは、ネットワーク内で検出されたストレージアレイのリストをスクロールしてステータスを表示し、単一のアレイまたはアレイのグループに対して処理を実行できます。

単一のアレイを管理する場合は、アレイを選択してSystem Managerを開くことができます。

詳細：

- ["System Managerへのアクセスに関する考慮事項"](#)
- ["個々のストレージアレイの管理"](#)
- ["ストレージアレイのステータスの表示"](#)

## 概念

### アレイの検出に関する考慮事項

Unified Managerでストレージリソースを表示および管理するには、組織のネットワークで管理するストレージアレイを検出する必要があります。複数のアレイを検出することも、単一のアレイを検出することもできます。

#### 複数のストレージアレイの検出

複数のアレイを検出する場合は、ネットワークIPアドレスの範囲を入力すると、その範囲の各IPアドレスへの接続がUnified Managerで個別に試行されます。到達したストレージアレイが検出ページに表示され、管理ドメインに追加されることがあります。

## 単一のストレージアレイの検出

単一のアレイを検出する場合は、ストレージアレイ内のいずれかのコントローラのIPアドレスを1つ入力すると、個々のストレージアレイが追加されます。



Unified Managerは、あるコントローラに割り当てられている1つのIPアドレスまたは範囲内のIPアドレスのみを検出して表示します。代替のコントローラまたはそれらのコントローラに割り当てられているIPアドレスがあっても、この1つのIPアドレスまたはIPアドレス範囲に含まれていなければ、Unified Managerでは検出または表示されません。ただし、ストレージアレイを追加すると、関連付けられているすべてのIPアドレスが検出されて[管理]ビューに表示されません。

## ユーザクレデンシャル

検出プロセスでは、追加する各ストレージアレイの管理者パスワードを指定する必要があります。

## Webサービスの証明書

検出プロセスでは、検出されたストレージアレイに信頼できるソースからの証明書があるかどうかUnified Managerで確認されます。Unified Managerでは、ブラウザで確立するすべての接続に対して2種類の証明書ベースの認証を使用します。

- 信頼された証明書

Unified Managerで検出されたアレイについては、認証局が発行する信頼された証明書が追加が必要となる場合があります。

これらの証明書をインポートするには、\* Import \*ボタンを使用します。このアレイに前に接続したことがある場合は、一方または両方のコントローラの証明書が期限切れになっているか、失効しているか、証明書チェーンにルート証明書または中間証明書がない可能性があります。ストレージアレイの管理を開始する前に、期限切れまたは失効した証明書を差し替えるか、不足しているルート証明書または中間証明書を追加する必要があります。

- 自己署名証明書

自己署名証明書を使用することもできます。署名済みの証明書をインポートせずにアレイを検出しようとすると、Unified Managerにエラーダイアログボックスが表示されます。このダイアログボックスで自己署名証明書を承認することができます。自己署名証明書が信頼済みとしてマークされ、Unified Managerにストレージアレイが追加されます。

ストレージアレイへの接続を信頼しない場合は、Unified Managerにストレージアレイを追加する前に\* Cancel \*を選択し、ストレージアレイのセキュリティ証明書戦略を検証します。

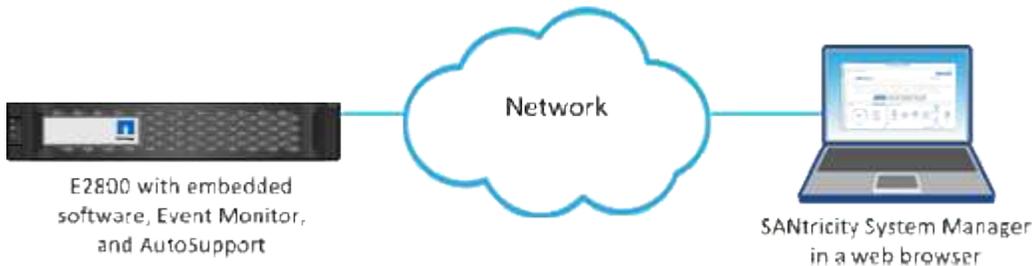
## System Managerへのアクセスに関する考慮事項

ストレージアレイを設定および管理する場合は、1つ以上のストレージアレイを選択し、[起動]オプションを使用してSystem Managerを開きます。

System Managerはコントローラに組み込まれたアプリケーションで、イーサネット管理ポートを介してネットワークに接続されます。これには、アレイベースのすべての関数が含まれます。

System Managerにアクセスするには、以下を準備しておく必要があります。

- 次のいずれかのアレイモデルを参照してください。"[E シリーズハードウェアの概要](#)"
- Webブラウザを使用したネットワーク管理クライアントへのアウトオブバンド接続。



## アレイの検出

### 複数のストレージアレイの検出

複数のアレイを検出すると、管理サーバが配置されているサブネット全体ですべてのストレージアレイが検出され、検出されたアレイが管理ドメインに自動的に追加されます。

開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。
- ストレージアレイが正しくセットアップおよび設定されている必要があります。
- ストレージアレイのパスワードは、System Managerの[アクセス管理]タイルを使用して設定する必要があります。
- 信頼されていない証明書を解決するには、認証局（CA）の信頼された証明書ファイルが必要です。証明書ファイルがローカルシステムにある必要があります。

アレイの検出は複数の手順で構成されます。

手順1：ネットワークアドレスを入力します

ローカルサブネットワーク全体を検索するには、ネットワークアドレス範囲を入力します。到達したストレージアレイが検出ページに表示され、管理ドメインに追加されることがあります。

何らかの理由で検出操作を停止する必要がある場合は、\*検出の停止\*をクリックします。

手順

1. [管理] ページで、[\* 追加 / 検出 \*] を選択します。

[Add/Discover]ダイアログボックスが表示されます。

2. [ネットワーク範囲内のすべてのストレージアレイを検出する]ラジオボタンを選択します。
3. 開始ネットワークアドレスと終了ネットワークアドレスを入力して、ローカルサブネットワーク全体を検索し、\*検出の開始\*をクリックします。

検出プロセスが開始されます。この検出プロセスが完了するまでに数分かかることがあります。ストレージアレイが検出されると、検出ページの表にデータが表示されます。



管理可能なアレイが検出されない場合は、ストレージアレイがネットワークに適切に接続されており、割り当てられたアドレスが範囲内にあることを確認してください。[新規検出パラメータ\*]をクリックして、[追加/検出]ページに戻ります。

4. 検出されたストレージアレイのリストを確認します。
5. 管理ドメインに追加するストレージアレイの横にあるチェックボックスをオンにし、[次へ]をクリックします。

管理ドメインに追加する各アレイについて、Unified Managerでクレデンシャルのチェックが実行されます。そのアレイに関連付けられている自己署名証明書や信頼されていない証明書の解決が必要になる場合があります。

6. 「\*次へ\*」をクリックして、ウィザードの次の手順に進みます。

#### 手順2：検出時に自己署名証明書を解決する

検出プロセスでは、ストレージアレイに信頼できるソースからの証明書があるかどうかを確認されます。

##### 手順

1. 次のいずれかを実行します。
  - 検出されたストレージアレイへの接続を信頼する場合は、ウィザードの次のカードに進みます。自己署名証明書が信頼済みとしてマークされ、ストレージアレイがUnified Managerに追加されます。
  - ストレージアレイへの接続を信頼しない場合は、\*キャンセル\*を選択し、各ストレージアレイのセキュリティ証明書戦略を検証してからUnified Managerに追加してください。
2. 「\*次へ\*」をクリックして、ウィザードの次の手順に進みます。

#### 手順3：検出時に信頼されていない証明書を解決する

信頼されていない証明書は、ストレージアレイからUnified Managerへのセキュアな接続を確立しようとしたときに、接続がセキュアであることを確認できない場合に発生します。アレイの検出プロセスで信頼されていない証明書を解決するには、信頼できるサードパーティが発行した認証局（CA）証明書（CA署名証明書）をインポートします。

信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合があります。

- ストレージアレイを最近追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

##### 手順

1. 信頼されていない証明書を解決するストレージアレイの横にあるチェックボックスをオンにして、[インポート]ボタンを選択します。

信頼された証明書ファイルをインポートするためのダイアログボックスが開きます。

2. Browse (参照) \* をクリックして、ストレージレイの証明書ファイルを選択します。

ダイアログボックスにファイル名が表示されます。

3. [\* インポート \*] をクリックします。

ファイルがアップロードされて検証されます。



信頼されていない証明書の問題が未解決のストレージレイはUnified Managerに追加されません。

4. 「\* 次へ \*」 をクリックして、ウィザードの次の手順に進みます。

#### 手順4：パスワードを入力する

管理ドメインに追加するストレージレイのパスワードを入力する必要があります。

#### 手順

1. Unified Managerに追加する各ストレージレイのパスワードを入力します。
2. \*オプション：\*ストレージレイをグループに関連付けます。ドロップダウンリストから、選択したストレージレイに関連付ける目的のグループを選択します。
3. [完了] をクリックします。

#### 終了後

ストレージレイが管理ドメインに追加され、選択したグループ（指定されている場合）に関連付けられません。



指定したストレージレイへのUnified Managerの接続には数分かかることがあります。

## 単一のレイの検出

単一のストレージレイを手動で検出して組織のネットワークに追加するには、[単一のストレージレイの追加/検出]オプションを使用します。

#### 開始する前に

- ストレージレイが正しくセットアップおよび設定されている必要があります。
- ストレージレイのパスワードは、System Managerの[アクセス管理]タイルを使用して設定する必要があります。

#### 手順

1. [管理] ページで、[\* 追加 / 検出 \*] を選択します。

[Add/Discover]ダイアログボックスが表示されます。

2. [Discover a single storage array]オプションボタンを選択します。

3. ストレージアレイ内のいずれかのコントローラのIPアドレスを入力し、\*検出の開始\*をクリックします。

指定したストレージアレイへのUnified Managerの接続には数分かかることがあります。



指定したIPアドレスでコントローラに接続できない場合、「ストレージアレイにアクセスできません」というメッセージが表示されます。

4. プロンプトが表示されたら、自己署名証明書を解決します。

検出プロセスでは、検出されたストレージアレイに信頼できるソースからの証明書があるかどうかを確認されます。ストレージアレイのデジタル証明書が見つからない場合は、認識された認証局 (CA) によって署名されていない証明書を解決するためにセキュリティ例外を追加するように求められます。

5. 信頼されていない証明書があれば解決します。

信頼されていない証明書は、ストレージアレイからUnified Managerへのセキュアな接続を確立しようとしたときに、接続がセキュアであることを確認できない場合に発生します。信頼されていない証明書を解決するには、信頼できる第三者機関から発行された認証局 (CA) 証明書をインポートします。

6. 「\*次へ\*」をクリックします。

7. \*オプション\*: 検出されたストレージアレイをグループに関連付けます。ドロップダウンリストから、ストレージアレイに関連付ける目的のグループを選択します。

デフォルトでは「All」グループが選択されています。

8. 管理ドメインに追加するストレージアレイの管理者パスワードを入力し、\* OK \*をクリックします。

終了後

ストレージアレイがUnified Managerに追加され、指定した場合は選択したグループにも追加されます。

サポートデータの自動収集が有効になっている場合は、追加したストレージアレイのサポートデータが自動的に収集されます。

## アレイの管理

### ストレージアレイのステータスの表示

Unified Managerには、検出された各ストレージアレイのステータスが表示されます。

[\* Manage-All\*]ページに移動します。このページでは、Web Services Proxyとそのストレージアレイの間の接続のステータスを確認できます。

ステータスインジケータについては、次の表で説明します。

ステータス	を示します。
最適	ストレージアレイが最適な状態です。証明書の問題はなく、パスワードは有効です。

ステータス	を示します。
無効なパスワード	無効なストレージレイパスワードが指定されました。
信頼されない証明書	HTTPS証明書が自己署名証明書でインポートされていないか、CA署名証明書でルート証明書と中間CA証明書がインポートされていないため、ストレージレイとの1つ以上の接続が信頼されていません。
要注意	ストレージレイにユーザによる修正が必要な問題があります。
ロックダウン	ストレージレイがロックダウン状態です。
不明	ストレージレイに一度も接続されていません。この状況は、Web Services Proxyが起動中でまだストレージレイに接続していない場合や、ストレージレイがオフラインでWeb Services Proxyの起動後に一度も接続されていない場合に発生します。
オフライン	Web Services Proxyは以前にストレージレイに接続していましたが、現在はすべての接続が失われています。

## 個々のストレージレイの管理

[起動]オプションを使用すると、管理処理を実行する場合に1つ以上のストレージレイに対してブラウザベースのSystem Managerを開くことができます。

### 手順

1. [管理]ページで、管理するストレージレイを1つ以上選択します。
2. [\* 起動 \*] をクリックします。

新しいウィンドウが開き、System Managerのログインページが表示されます。

3. ユーザー名とパスワードを入力し、\*ログイン\*をクリックします。

## ストレージレイのパスワードの変更

Unified Managerでストレージレイを表示したりアクセスしたりするために使用するパスワードを更新できます。

### 開始する前に

- Storage Adminの権限を含むユーザプロファイルでログインする必要があります。
- ストレージレイの現在のパスワード（System Managerで設定されているパスワード）を確認しておく必要があります。

### タスクの内容

このタスクでは、Unified Managerからストレージレイにアクセスできるようにストレージレイの現在のパスワードを入力します。これは、System Managerでレイのパスワードが変更されたために、Unified

Managerでも変更が必要になった場合などに行います。

手順

1. 管理ページで、1つ以上のストレージレイを選択します。
2. [メニュー]: [一般的でないタスク][ストレージレイパスワードの入力]を選択します。
3. 各ストレージレイのパスワードを入力し、\*保存\*をクリックします。

## SANtricity Unified Managerからのストレージレイの削除

Unified Managerで管理する必要がなくなったストレージレイは、削除することができません。

タスクの内容

削除したストレージレイにはアクセスできません。ただし、ブラウザでIPアドレスまたはホスト名を直接指定することで、削除したストレージレイへの接続を確立できます。

ストレージレイを削除しても、ストレージレイやそのデータには影響しません。ストレージレイを誤って削除した場合は、再度追加することができます。

手順

1. [\* Manage \* (管理) ]ページを選択します。
2. 削除するストレージレイを1つ以上選択します。
3. メニューから「Uncommon Tasks (一般的でないタスク)」を選択します。

ストレージレイがSANtricity Unified Managerのすべてのビューから削除されます。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。