クラスタを管理します。

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-918/storage-mgmt/concept_how_discovery_process_works.html on November 13, 2026. Always check docs.netapp.com for the latest.

目次

クラスタを管理します。 1
Active IQ Unified Manager におけるクラスター検出プロセスの仕組みについて説明します。 1
Active IQ Unified Manager で監視対象のクラスター一覧を表示する 2
Active IQ Unified Manager にクラスターを追加する 2
Active IQ Unified Manager でクラスター設定を編集する 4
Active IQ Unified Manager からクラスターを削除する 5
Active IQ Unified Manager でクラスターを再検出する 6

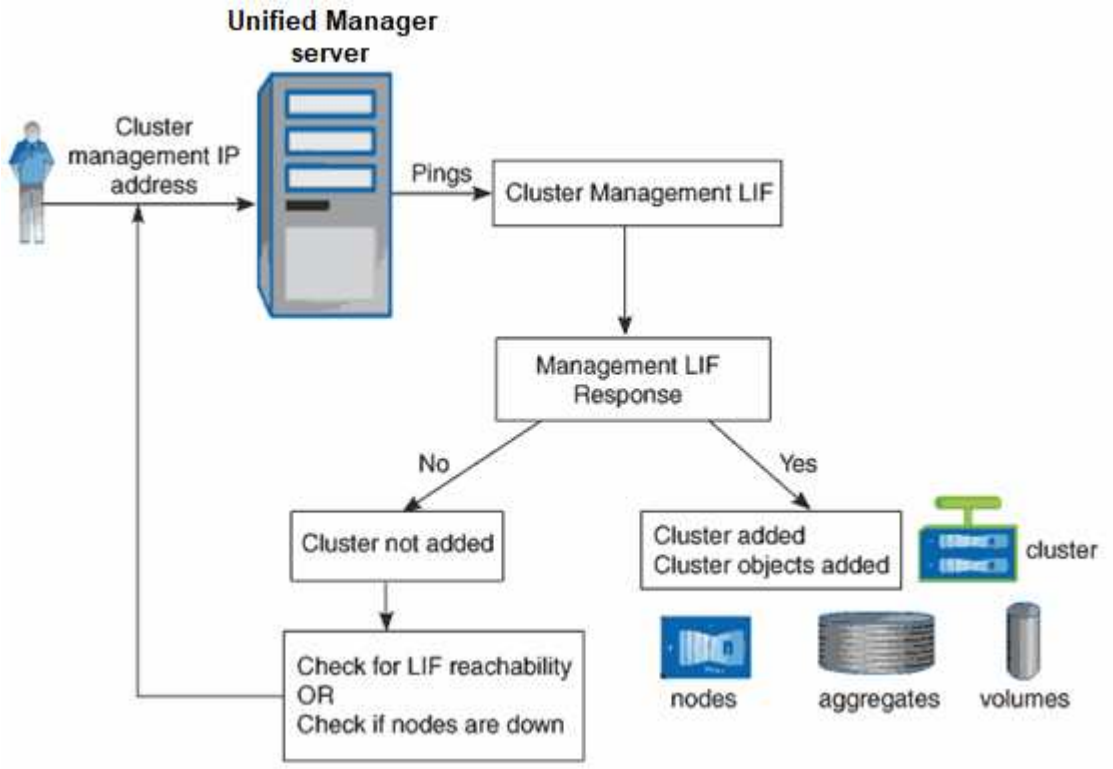
クラスタを管理します。

Active IQ Unified Manager におけるクラスター検出プロセスの仕組みについて説明します。

クラスタをUnified Managerに追加すると、サーバによってクラスタ オブジェクトが検出され、サーバのデータベースに追加されます。検出プロセスの仕組みを理解しておくと、使用するクラスタとそのオブジェクトを管理する際に役立ちます。

クラスタ構成情報を収集するための監視間隔は15分です。例えば、クラスタを追加した後、Unified ManagerのUIにクラスタオブジェクトが表示されるまで15分かかります。この時間枠は、クラスタに変更を加える場合にも当てはまります。例えば、クラスタ内のSVMに2つの新しいボリュームを追加した場合、それらの新しいオブジェクトは次のポーリング間隔（最大15分）後にUIに表示されます。

次の図は検出プロセスを示しています。



新しいクラスタのオブジェクトがすべて検出されると、Unified Managerは過去15日間のパフォーマンス データの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から2週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルが完了すると、リアルタイムのクラスタ パフォーマンス データが収集されます（デフォルトでは5分間隔）。

15日分のパフォーマンス データを収集するとCPUに負荷がかかるため、新しいクラスタを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスタで実行されないように、時間差をつけて追加するようにしてください。

Active IQ Unified Manager で監視対象のクラスター一覧を表示する

[クラスタ セットアップ]ページを使用して、クラスタのインベントリを表示できます。クラスタに関する詳細（名前またはIPアドレス、通信ステータスなど）を参照できます。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、ストレージ管理 > *クラスタ設定*をクリックします。

   ストレージ環境内の、Unified Managerで管理されているクラスタがすべて表示され、収集状態の重大度レベル列でソートされます。列ヘッダーをクリックすると、別の列でクラスタをソートできます。

Active IQ Unified Manager にクラスターを追加する

Active IQ Unified Managerにクラスタを追加して監視することができます。たとえば、クラスタの健全性、容量、パフォーマンス、構成などの情報を取得して、発生する可能性がある問題を特定して解決したりできます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- 次の情報が必要です。
  - Unified Managerは、オンプレミスのONTAPクラスタ、ONTAP Select、Cloud Volumes ONTAPをサポートしています。
  - クラスタのホスト名またはクラスタ管理IPアドレス（IPv4またはIPv6）が必要です。

    ホスト名を使用する場合は、クラスタ管理LIFのクラスタ管理IPアドレスに解決される必要があります。ノード管理LIFを使用すると処理に失敗します。
  - クラスタにアクセスするためのユーザ名とパスワードが必要です。

    このアカウントには、アプリケーションアクセスが *ontapi*、*amqp*、*console*、および *http* に設定された *admin* ロールが必要です。
  - HTTPSプロトコルを使用してクラスタに接続するためのポート番号を確認しておく必要があります（通常はポート443）。
  - クラスタでONTAPバージョン9.9以降が実行されている必要があります。
  - Unified Managerサーバに十分なスペースが必要です。スペースの使用率が90%を超えている場合、サーバにクラスタを追加することはできません。
  - 必要な証明書を用意しておきます。

    SSL（HTTPS）証明書：この証明書はUnified Managerが所有しています。Unified Managerを新規イ

ンストールすると、デフォルトで自己署名SSL（HTTPS）証明書が生成されます。NetAppでは、セキュリティ向上のため、CA署名付き証明書へのアップグレードをお勧めします。サーバー証明書の有効期限が切れた場合は、証明書を再生成し、Unified Managerを再起動して、サービスに新しい証明書を反映させる必要があります。SSL証明書の再生成の詳細については、"HTTPSセキュリティ証明書の生成"を参照してください。

EMS証明書：この証明書はUnified Managerが所有しています。これは、ONTAPから受信したEMS通知の認証時に使用されます。

相互**TLS**通信用の証明書：Unified ManagerとONTAP間の相互TLS通信時に使用されます。証明書ベースの認証は、ONTAPのバージョンに基づいてクラスタに対して有効になります。クラスタで実行されているONTAPのバージョンが9.5より前の場合、証明書ベースの認証は有効になりません。

Unified Managerの旧バージョンを更新する場合、証明書ベースの認証はクラスタに対して自動的に有効になりません。ただし、クラスタの詳細を変更して保存することで有効にすることができます。証明書の有効期限が切れた場合は、新しい証明書を組み込むために証明書を再生成する必要があります。証明書の表示と再生成の詳細については、"クラスタの編集"を参照してください。

- クラスタはWeb UIから追加でき、証明書ベースの認証が自動的に有効になります。
- Unified Manager CLIを介してクラスターを追加できますが、証明書ベースの認証はデフォルトでは有効になっていません。Unified Manager CLIを使用してクラスターを追加した場合、Unified Manager UIを使用してクラスターを編集する必要があります。Unified Manager CLIを使用してクラスターを追加するには、"サポートされるUnified Manager のCLIコマンド"を参照してください。
- クラスターで証明書ベースの認証が有効になっている場合、サーバーからUnified Managerのバックアップを取得し、ホスト名またはIPアドレスが変更された別のUnified Managerサーバーに復元すると、クラスターの監視が失敗する可能性があります。このエラーを回避するには、クラスターの詳細を編集して保存してください。クラスターの詳細編集に関する詳細については、"クラスタの編集"を参照してください。
- クラスタ レベルでは、Active IQインターフェイスによって、認証方式「cert」に対して2つの新しいユーザ グループ エントリが追加されます。

+ クラスタ証明書：この証明書はONTAPが所有しています。有効期限切れの証明書では、Unified Managerにクラスタを追加できません。証明書の有効期限がすでに切れている場合は、クラスタを追加する前に証明書を再生成する必要があります。証明書の生成に関する情報については、ナレッジベース（KB）の記事 "System ManagerのユーザーインターフェイスでONTAPの自己署名証明書を更新する方法"を参照してください。

- Unified Managerの単一インスタンスは、特定の数のノードをサポートできます。サポートされているノード数を超える環境を監視する必要がある場合は、一部のクラスタを監視するために、Unified Managerの追加インスタンスをインストールする必要があります。サポートされているノード数のリストを表示するには、 "『Unified Manager Best Practices Guide』"を参照してください。

手順

1. 左側のナビゲーションペインで、ストレージ管理 > *クラスタ設定*をクリックします。
2. クラスター設定ページで、*追加*をクリックします。
3. 「クラスタの追加」ダイアログボックスで、必要な値を指定し、*送信*をクリックします。
4. 「ホストの認証」ダイアログボックスで、*証明書の表示*をクリックして、クラスタに関する証明書情報を表示します。

5. *はい*をクリックします。

   クラスタの詳細を保存したあとに相互TLS通信用の証明書を表示できます。

   証明書ベースの認証が有効になっていない場合、Unified Managerではクラスタの初回追加時にのみ証明書がチェックされます。ONTAPへのAPI呼び出しのたびに証明書がチェックされることはありません。

新しいクラスタのオブジェクトがすべて検出されると、Unified Managerは過去15日間のパフォーマンス データの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から2週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルが完了すると、リアルタイムのクラスタ パフォーマンス データが収集されます（デフォルトでは5分間隔）。

- 15日間のパフォーマンスデータの収集は、CPU負荷が高くなります。NetAppでは、データ継続性収集のポーリングが同時に多数のクラスタで実行されないように、新しいクラスタの追加を段階的に行うことを推奨しています。さらに、データ継続性収集の期間中にUnified Managerを再起動すると、収集が停止し、欠落した期間のパフォーマンスチャートに空白が生じます。
- バージョン9.14.1以降のONTAPクラスタを追加すると、通信はクラウドエージェント機能を介して行われます。ONTAPは、読み取り専用権限を持つ内部サービスアカウントユーザー（例：clus-agent-xxxx）を自動的に作成します。Unified Managerは、 `clus-agent`ユーザーが削除された場合、それらのクラスタからのデータ収集を停止します。

エラー メッセージが表示されてクラスタを追加できない場合は、次の問題がないかどうかを確認してください。

- 2つのシステムのクロックが同期されておらず、Unified ManagerのHTTPS証明書の開始日がクラスタの日付よりもあとの日付になっている。この場合、NTPなどのサービスを使用してクロックを同期する必要があります。
- クラスタのEMS通知の送信先が最大数に達しており、Unified Managerのアドレスを追加できない。デフォルトでは、クラスタで定義できるEMS通知の送信先は20個までです。

関連情報

"ユーザの追加"

"クラスタ リストおよび詳細の表示"

"CAの署名を受けて返されたHTTPS証明書のインストール"

Active IQ Unified Manager でクラスター設定を編集する

[クラスタを編集]ダイアログ ボックスを使用して、ホスト名またはIPアドレス、ユーザ名、パスワード、ポートなど、既存のクラスタの設定を変更することができます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

Unified Manager 9.7以降では、クラスタを追加する際にHTTPSのみを使用できます。

手順

1. 左側のナビゲーションペインで、ストレージ管理 > *クラスタ設定*をクリックします。
2. *クラスタ設定*ページで、編集するクラスタを選択し、*編集*をクリックします。
3. 「クラスターの編集」ダイアログボックスで、必要に応じて値を変更します。+ Unified Managerに追加されたクラスターの詳細を変更した場合は、ONTAPバージョンに基づいて、相互TLS通信の証明書の詳細を表示できます。ONTAPバージョンの詳細については、"相互TLS通信用の証明書"を参照してください。+ 「証明書の詳細」をクリックすると、証明書の詳細を表示できます。証明書の有効期限が切れている場合は、「再生成」ボタンをクリックして新しい証明書を組み込んでください。
4. 「送信」をクリックしてください。
5. 「ホストの認証」ダイアログボックスで、*証明書の表示*をクリックして、クラスタに関する証明書情報を表示します。
6. *はい*をクリックします。

関連情報

"ユーザの追加"

"クラスタ リストおよび詳細の表示"

Active IQ Unified Manager からクラスターを削除する

[クラスタ セットアップ]ページを使用してUnified Managerからクラスタを削除することができます。たとえば、クラスタの検出が失敗した場合やストレージ システムを運用停止する場合に、クラスタを削除できます。

開始する前に

アプリケーション管理者またはストレージ管理者のロールが必要です。

このタスクでは、選択したクラスタをUnified Managerから削除します。削除したクラスタは監視されなくなります。削除したクラスタに登録されていたUnified Managerのインスタンスは、クラスタから登録解除されます。

クラスタを削除すると、そのストレージ オブジェクト、履歴データ、ストレージ サービス、関連するイベントもすべてUnified Managerから削除されます。この変更は、次回のデータ収集サイクルのあとでインベントリ ページと詳細ページに反映されます。



クラスターを廃止する前に、Unified Managerからクラスターを削除する必要があります。クラスターを削除しようとした時点で、クラスターが既にオフライン状態であるか、アクセス不能な状態である場合、Unified Manager はクラスターと通信してアプリケーションレコードや構成済みのイベント管理システム （EMS） サブスクリプションを削除できません。これにより、削除処理が完了する前に失敗するか、応答しなくなる可能性があります。

手順

1. 左側のナビゲーションペインで、ストレージ管理 > *クラスタ設定*をクリックします。
2. クラスター設定ページで、削除するクラスターを選択し、*削除*をクリックします。
3. 「データソースの削除」メッセージダイアログで、「削除」をクリックして削除要求を確定します。

関連情報

"ユーザの追加"

"クラスタ リストおよび詳細の表示"

Active IQ Unified Manager でクラスターを再検出する

[クラスタ セットアップ]ページでクラスタを手動で再検出することで、クラスタの健全性、監視ステータス、パフォーマンス ステータスに関する最新情報を得られます。

クラスタを更新し（スペースが不足しているためにアグリゲートのサイズを増やす場合など）、その変更をUnified Managerで検出するには、クラスタを手動で再検出します。

Unified ManagerとOnCommand Workflow Automation（WFA）を連携させている場合は、WFAでキャッシュされたデータの再取得がトリガーされます。

手順

1. 左側のナビゲーションペインで、ストレージ管理 > *クラスタ設定*をクリックします。
2. 「クラスター設定」ページで、「再検出」をクリックします。

   Unified Managerは選択されたクラスターを再検出し、最新の健全性およびパフォーマンスステータスを表示します。

関連情報

"クラスタ リストおよび詳細の表示"

著作権に関する情報

Copyright © 2026 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。