Active IQ® Unified Manager 9.6

システム構成ガイド

2019年5月 | 215-14144_A0
ng-gpso-jp-documents@netapp.com

NetApp®

目次

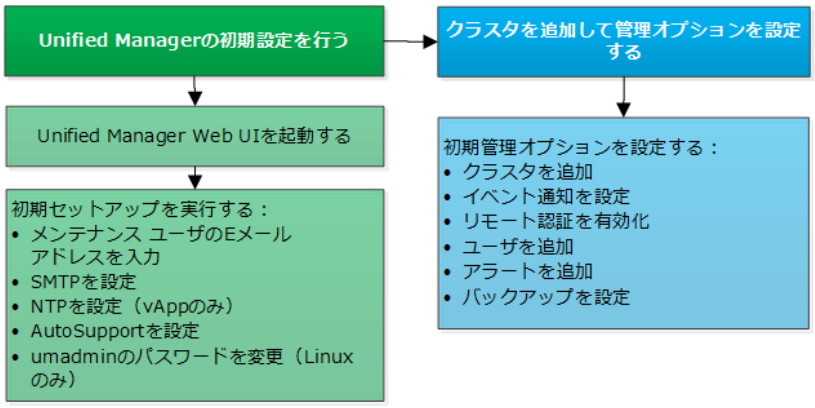
Active IQ Unified Managerの設定

Active IQ Unified Manager（旧OnCommand Unified Manager）をインストールしたら、Web UIにアクセスするために初期セットアップ（初期設定ウィザード）を完了する必要があります。初期セットアップを完了すると、クラスタの追加、リモート認証の設定、ユーザの追加、アラートの追加など、その他の設定作業を実行できるようになります。

このマニュアルに記載されている手順の一部は、Unified Managerインスタンスの初期セットアップを完了するための必須の手順です。それ以外の手順は新しいインスタンスをセットアップする際に推奨される設定か、またはONTAPの定期的な監視を開始する前に把握しておくことが推奨される設定です。

設定手順の概要

以下は、Unified Managerを使用する前に必要な設定作業のワークフローです。



Unified Manager Web UIへのアクセス

Unified Managerをインストールしたら、ONTAPシステムの監視を開始できるように、Web UIにアクセスしてUnified Managerをセットアップします。

開始する前に

- Web UIへのアクセスが初めての場合は、メンテナンス ユーザ（Linux環境の場合はumadminユーザ）としてログインする必要があります。
- 完全修飾ドメイン名（FQDN）またはIPアドレスの代わりに短縮名を使用してUnified Managerへのアクセスをユーザに許可する場合は、短縮名が有効なFQDNに解決されるようにネットワークを設定する必要があります。
- 自己署名のデジタル証明書がサーバで使用されている場合、信頼されていない証明書であることを伝える警告がブラウザ画面に表示されることがあります。その場合は、危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をインストールしてサーバを認証します。

手順

1. インストールの完了時に表示されたURLを使用して、ブラウザからUnified Manager Web UIを起動します。URLは、Unified Managerサーバの IPアドレスまたは完全修飾ドメイン名（FQDN）です。

リンクの形式は、https://*URL*です。

2. メンテナンス ユーザのクレデンシャルを使用して、Unified Manager Web UIにログインします。

Unified Manager Web UIの初期セットアップの実行

Unified Managerを使用するには、NTPサーバ、メンテナンス ユーザのEメール アドレス、SMTPサーバのホスト名とオプションなどを最初に設定する必要があります。

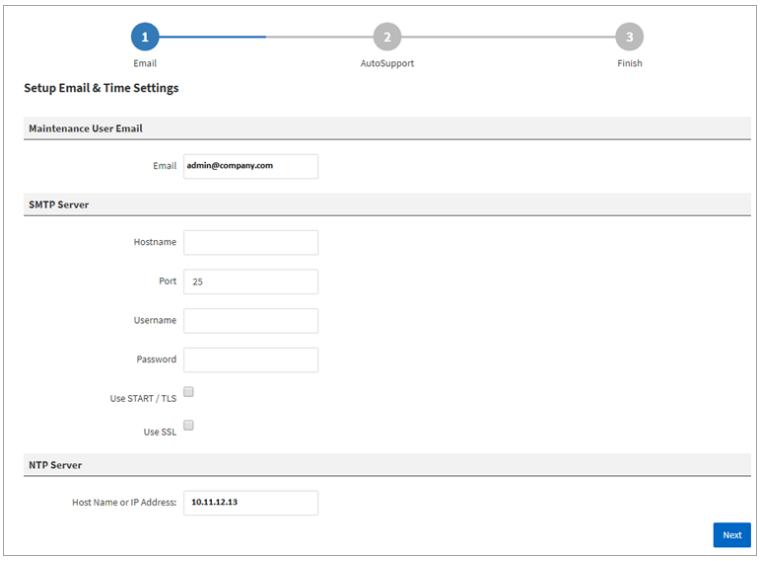
開始する前に

次の作業を完了しておきます。

- インストールの完了時に表示されたURLを使用してUnified Manager Web UIを起動します。
- インストール時に作成したメンテナンス ユーザ（Linux環境の場合はumadminユーザ）の名前とパスワードを使用してログインします。

タスク概要

Active IQ Unified Managerの初期セットアップ ページは、Web UIへの初回アクセス時にのみ表示されます。次のページはVMware環境の場合の例を示したものです。



これらのオプションをあとで変更する場合は、Unified Managerツールバーの  をクリックして[管理]オプションを使用します。NTP設定はVMware専用です。この設定はあとからUnified Managerメンテナンス コンソールを使用して変更できます。

手順

1. Active IQ Unified Managerの初期セットアップ ページで、メンテナンス ユーザのEメール アドレス、SMTPサーバのホスト名とその他のSMTPオプション、およびNTPサーバ（VMwareの場合のみ）を入力します。**[次]**をクリックします。
2. **[AutoSupport]**ページで、**[同意して続行]**をクリックしてUnified ManagerからNetApp Active IQへAutoSupportメッセージが送信されるようにします。

インターネット アクセスを提供するプロキシを指定してAutoSupportのコンテンツを送信する場合や、AutoSupportを無効にする場合は、Web UIの[管理]オプションを使用してください。

3. Red HatおよびCentOSのシステムの場合、umadminユーザのパスワードをデフォルトの「admin」から独自のパスワードに変更できます。

タスクの結果

初期セットアップのウィンドウが閉じ、Unified Manager Web UIが表示されます。[設定/クラスタ データ ソース]ページが表示され、システムにクラスタを追加することができます。

クラスタの追加

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

- 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。
  - ホスト名またはクラスタ管理IPアドレス
    ホスト名は、Unified Managerがクラスタに接続するために使用する完全修飾ドメイン名（FQDN）または短縮名です。ホスト名は、クラスタ管理IPアドレスに解決できる必要があります。
    クラスタ管理IPアドレスは、管理用Storage Virtual Machine（SVM）のクラスタ管理LIFであることが必要です。ノード管理LIFを使用すると処理に失敗します。
  - ONTAP管理者のユーザ名とパスワード
    このアカウントには、アプリケーション アクセスが*ontapi*、*ssh*、および*http*に設定された*admin*ロールが必要です。
  - クラスタに設定できるプロトコルのタイプ（HTTPまたはHTTPS）、およびクラスタへの接続に使用するポート番号

    注： NAT / ファイアウォールの背後にあるクラスタは、Unified ManagerのNAT IPアドレスを使用して追加できます。接続されたWorkflow AutomationやSnapProtectのシステムもNAT / ファイアウォールの背後に配置する必要があり、SnapProtectのAPI呼び出しではNAT IPアドレスを使用してクラスタを識別する必要があります。
- Unified ManagerのFQDNを使用して、ONTAPシステムにpingを実行できる必要があります。
  これを確認するには、次のONTAPコマンドを使用します：`ping -node <node_name> -destination <Unified_Manager_FQDN>`.
- Unified Managerサーバに十分なスペースが必要です。データベース ディレクトリの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。

タスク概要

MetroCluster構成では、ローカル クラスタとリモート クラスタの両方を追加し、追加したクラスタを正しく設定する必要があります。

クラスタに2つ目のクラスタ管理LIFを設定し、Unified Managerのそれぞれのインスタンスを別のLIFを介して接続すれば、1つのクラスタをUnified Managerの2つのインスタンスで監視できます。

手順

1. 左側のナビゲーション ペインで、**[設定]** > **[クラスタ データ ソース]**をクリックします。
2. **[設定/クラスタ データ ソース]**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、クラスタのホスト名またはIPアドレス、ユーザ名、パスワード、通信プロトコル、ポート番号など、必要な値を指定します。

   デフォルトでは、HTTPSプロトコルとポート443が選択されます。

   クラスタ管理IPアドレスは、IPv6からIPv4またはIPv4からIPv6に変更できます。次の監視サイクルが完了すると、クラスタ グリッドとクラスタ設定ページに新しいIPアドレスが反映されます。
4. **[送信]**をクリックします。
5. HTTPSを選択した場合は、次の手順を実行します。
   a. **[ホストの承認]**ダイアログ ボックスで、**[証明書を表示する]**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。
   b. **[はい]**をクリックします。

      Unified Managerでは、クラスタが最初に追加されたときにのみ証明書がチェックされます。Unified Managerでは、ONTAPに対するAPI呼び出しごとには証明書がチェックされません。

      証明書の期限が切れると、新しいクラスタを追加できなくなります。まずSSL証明書を更新してから、クラスタを追加する必要があります。

タスクの結果

新しいクラスタのオブジェクトがすべて検出されると（約15分後）、Unified Managerが過去15日間の履歴パフォーマンス 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）。

注 : 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。また、データの継続性収集期間にUnified Managerを再起動すると、収集が停止し、その間のデータがパフォーマンス グラフに表示されません。

ヒント : 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。

Unified Managerでアラート通知を送信するための設定

Unified Managerでは、環境内のイベントについて警告する通知を送信するように設定することができます。通知を送信するには、Unified Managerのその他いくつかのオプションを設定する必要があります。

開始する前に

管理者のロールが必要です。

タスク概要

Unified Managerを導入して初期設定を完了したら、イベントの受信に対してアラートをトリガーし、通知EメールやSNMPトラップを生成するように設定することを検討する必要があります。

手順

1. イベント通知を設定する（9ページ）

   特定のイベントが発生したときにアラート通知を送信するには、SMTPサーバを設定し、アラート通知の送信元のEメール アドレスを指定する必要があります。SNMPトラップを使用する場合は、該当するオプションを選択し、必要な情報を指定します。

2. リモート認証を有効化する（10ページ）

   リモートLDAPユーザまたはActive Directoryユーザが Unified Managerインスタンスにアクセスしてアラート通知を受信できるようにするには、リモート認証を有効にする必要があります。

3. 認証サーバを追加する（12ページ）

   認証サーバを追加することで、認証サーバ内のリモート ユーザがUnified Managerにアクセスできるようにすることができます。

4. ユーザを追加する（14ページ）

   さまざまなタイプのローカル ユーザやリモート ユーザを追加し、特定のロールを割り当てることができます。アラートを作成する際に、アラート通知を受信するユーザを指定します。

5. アラートを追加する（15ページ）

   通知を送信するEメール アドレスの追加、通知を受信するユーザの追加、ネットワークの設定、環境に必要なSMTPオプションとSNMPオプションの設定が完了したら、アラートを割り当てることができます。

イベント通知の設定

Unified Managerでは、イベントが生成されたときやユーザに割り当てられたときにアラート通知を送信するように設定することができます。アラートの送信に使用するSMTPサーバの設定や、さまざまな通知メカニズムの設定が可能です。たとえば、アラート通知はEメールやSNMPトラップとして送信できます。

開始する前に

次の情報が必要です。

- アラート通知の送信元Eメール アドレス

このEメール アドレスは、送信されるアラート通知の「送信元」フィールドに表示されます。何らかの理由でEメールを配信できない場合の不達メールの送信先としても使用されます。

- SMTPサーバのホスト名とアクセスに使用するユーザ名およびパスワード
- SNMPトラップとSNMPバージョン、アウトバウンド トラップ ポート、コミュニティ、およびその他の必要なSNMP設定値を受信するトラップ送信先ホストのホスト名またはIPアドレス
  トラップの送信先を複数指定するには、各ホストをカンマで区切ります。この場合、他のすべてのSNMP設定（バージョンやアウトバウンド トラップ ポートなど）がリスト内のすべてのホストで同じである必要があります。

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. ツールバーで  をクリックし、左側の[セットアップ]メニューで**[通知]**をクリックします。
2. **[セットアップ/通知]**ページで、必要に応じて該当する項目を設定し、**[保存]**をクリックします。

   注：

   - [送信元アドレス]に「ActiveIQUnifiedManager@localhost.com」というアドレスが事前に入力されている場合、すべてのEメール通知が正しく送信されるように実際のEメール アドレスに変更する必要があります。
   - SMTPサーバのホスト名を解決できない場合は、SMTPサーバのホスト名の代わりにIPアドレス（IPv4またはIPv6）を指定できます。

リモート認証の有効化

Unified Managerサーバが認証サーバと通信できるように、リモート認証を有効にすることができます。認証サーバのユーザがUnified Managerのグラフィカル インターフェイスにアクセスしてストレージ オブジェクトとデータを管理できるようになります。

開始する前に

管理者のロールが必要です。

重要：Unified Managerサーバは認証サーバに直接接続する必要があります。SSSD（System Security Services Daemon）やNSLCD（Name Service LDAP Caching Daemon）などのローカルのLDAPクライアントは無効にする必要があります。

タスク概要

リモート認証は、Open LDAPまたはActive Directoryのいずれかを使用して有効にすることができます。リモート認証が無効になっていると、リモート ユーザはUnified Managerにアクセスできません。

リモート認証は、LDAPとLDAPS（セキュアなLDAP）でサポートされます。Unified Managerでは、セキュアでない通信にはポート389、セキュアな通信にはポート636がデフォルトのポートとして使用されます。

注：ユーザの認証に使用する証明書は、X.509形式に準拠している必要があります。

手順

1. ツールバーで  をクリックし、左側の[セットアップ]メニューで**[認証]**をクリックします。
2. **[セットアップ/認証]**ページで、**[リモート認証を有効化]**を選択します。
3. **[認証サービス]**フィールドで、サービスの種類を選択し、認証サービスを設定します。

認証タイプ	入力する情報
Active Directory	• 認証サーバの管理者の名前（次のいずれかの形式を使用） ◦ *domainname\username* ◦ *username@domainname* ◦ バインド識別名 （適切なLDAP表記を使用） • 管理者のパスワード • ベース識別名（適切なLDAP表記を使用）
Open LDAP	• バインド識別名（適切なLDAP表記を使用） • バインド パスワード • ベース識別名

   Active Directoryユーザの認証に時間がかかる場合やタイムアウトする場合は、認証サーバからの応答に時間がかかっている可能性があります。Unified Managerでネストされたグループのサポートを無効にすると、認証時間が短縮される可能性があります。

   認証サーバの設定で[セキュアな接続を使用]オプションを選択すると、Unified Managerと認証サーバの間の通信にSecure Sockets Layer（SSL）プロトコルが使用されます。

4. オプション：認証サーバを追加し、認証をテストします。
5. **[保存して閉じる]**をクリックします。

関連タスク

認証サーバの追加（12ページ）
*SAML*認証の有効化（22ページ）

リモート認証でのネストされたグループの無効化

リモート認証を有効にしている場合、ネストされたグループの認証を無効にすることで、リモートからのUnified Managerへの認証を個々のユーザにのみ許可し、グループのメンバーは認証されないようにすることができます。ネストされたグループを無効にすると、Active Directory認証の応答時間を短縮できます。

開始する前に

- 管理者のロールが必要です。
- ネストされたグループの無効化は、Active Directoryを使用している場合にのみ該当します。

タスク概要

Unified Managerでネストされたグループのサポートを無効にすると、認証時間が短縮される可能性があります。ネストされたグループが無効になっているUnified Managerにリモート

グループを追加した場合、Unified Managerで認証されるためには個々のユーザがそのリモート グループのメンバーである必要があります。

手順

1. ツールバーで  をクリックし、左側の[セットアップ]メニューで**[認証]**をクリックします。
2. **[セットアップ/認証]**ページで、**[ネストされたグループの検索を無効にする]**チェックボックスをオンにします。
3. **[保存]**をクリックします。

認証サーバの追加

認証サーバを追加して管理サーバでリモート認証を有効にすると、その認証サーバのリモート ユーザがUnified Managerにアクセスできるようになります。

開始する前に

- 次の情報が必要です。
  - 認証サーバのホスト名またはIPアドレス
  - 認証サーバのポート番号
- 認証サーバのリモート ユーザまたはリモート グループを管理サーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- 管理者のロールが必要です。

タスク概要

追加する認証サーバがハイアベイラビリティ（HA）ペアを構成している（同じデータベースを使用している）場合は、パートナーの認証サーバも追加できます。これにより、どちらかの認証サーバが到達不能になったときに、管理サーバはパートナーと通信できます。

手順

1. ツールバーで  をクリックし、左側の[セットアップ]メニューで**[認証]**をクリックします。
2. **[セットアップ/認証]**ページで、**[管理サーバ]** > **[認証]**をクリックします。
3. **[セキュアな接続を使用する]**認証オプションを有効または無効にします。

状況	操作
有効にする	**a.** [リモート認証を有効化]チェックボックスで、**[セキュアな接続を使用する]**オプションをオンにします。 **b.** [認証サーバ]領域で、**[追加]**をクリックします。 **c.** [認証サーバの追加]ダイアログ ボックスで、認証サーバの名前またはIPアドレス（IPv4またはIPv6）を入力します。 **d.** [ホストの承認]ダイアログ ボックスで、[証明書を表示する]をクリックします。 **e.** [証明書を表示する]ダイアログ ボックスで、証明書の情報を確認し、**[閉じる]**をクリックします。 **f.** [ホストの承認]ダイアログ ボックスで、**[はい]**をクリックします。 **注：[セキュアな接続を使用する]**認証オプションを有効にすると、Unified Managerは認証サーバと通信して証明書を表示します。Unified Managerでは、セキュアな通信にはポート636、セキュアでない通信にはポート389がデフォルトのポートとして使用されます。
無効にする	**a.** [リモート認証を有効化]チェックボックスで、**[セキュアな接続を使用する]**オプションをオフにします。 **b.** [認証サーバ]領域で、**[追加]**をクリックします。 **c.** [認証サーバの追加]ダイアログ ボックスで、サーバのホスト名またはIPアドレス（IPv4またはIPv6）を指定し、ポートの詳細を指定します。 **d.** **[追加]**をクリックします。

追加した認証サーバが[サーバ]領域に表示されます。

4. 認証テストを実行し、追加した認証サーバのユーザを認証できることを確認します。

認証サーバの設定のテスト

認証サーバの設定を検証し、管理サーバと通信できるかどうかを確認することができます。具体的には、認証サーバからリモート ユーザまたはリモート グループを検索し、設定されている情報を使用して認証を実行します。

開始する前に

- リモート ユーザまたはリモート グループをUnified Managerサーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- 認証サーバのリモート ユーザまたはリモート グループを管理サーバで検索して認証できるように、認証サーバを追加しておく必要があります。
- 管理者のロールが必要です。

タスク概要

認証サービスがActive Directoryに設定されている場合、認証サーバのプライマリ グループに属するリモート ユーザの認証の検証では、認証結果にプライマリ グループに関する情報は表示されません。

手順

1. ツールバーで  をクリックし、左側の[セットアップ]メニューで**[認証]**をクリックします。
2. **[セットアップ/認証]**ページで、**[認証をテスト]**をクリックします。
3. **[ユーザテスト]**ダイアログ ボックスで、リモート ユーザのユーザ名とパスワードかリモート グループのユーザ名を指定し、**[テスト]**をクリックします。

   リモート グループを認証する場合、パスワードは入力しないでください。

ユーザの追加

[管理/ユーザ]ページを使用して、ローカル ユーザまたはデータベース ユーザを追加できます。また、認証サーバに属するリモート ユーザやリモート グループを追加することもできます。追加したユーザにロールを割り当てることで、ユーザはロールの権限に基づいてUnified Managerでストレージ オブジェクトやデータを管理したり、データベースのデータを参照したりすることができます。

開始する前に

- 管理者のロールが必要です。
- リモート ユーザまたはリモート グループを追加する場合は、リモート認証を有効にし、認証サーバを設定しておく必要があります。
- SAML認証を設定して、グラフィカル インターフェイスにアクセスするユーザをアイデンティティ プロバイダ（IdP）で認証する場合は、対象のユーザが「リモート」ユーザとして定義されていることを確認します。
  SAML認証が有効な場合、「ローカル」または「メンテナンス」のタイプのユーザにはUIへのアクセスが許可されません。

タスク概要

Windows Active Directoryのグループを追加した場合、そのグループの直接のメンバーに加え、ネストされたサブグループも（無効になっていなければ）すべてUnified Managerで認証されます。OpenLDAPまたはその他の認証サービスからグループを追加した場合は、そのグループの直接のメンバーだけがUnified Managerで認証されます。

手順

1. ツールバーで  をクリックし、左側の[管理]メニューで**[ユーザ]**をクリックします。
2. **[管理/ユーザ]**ページで、**[追加]**をクリックします。
3. **[ユーザの追加]**ダイアログ ボックスで、追加するユーザのタイプを選択し、必要な情報を入力します。

   ユーザに固有なEメール アドレスを指定する必要があります。複数のユーザで共有しているEメール アドレスは指定しないでください。
4. **[追加]**をクリックします。

関連タスク

リモート認証の有効化（10ページ）
*SAML*認証の有効化（22ページ）

アラートの追加

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

開始する前に

- イベントが生成されたときにActive IQ Unified Managerサーバからユーザに通知を送信できるように、通知に使用するユーザのEメール アドレス、SMTPサーバ、SNMPトラップホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名またはEメール アドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、[管理/スクリプト]ページを使用してUnified Managerにスクリプトを追加しておく必要があります。
- 管理者またはストレージ管理者のロールが必要です。

タスク概要

アラートは、ここで説明する手順に従って[設定/アラート生成]ページで作成できるほか、イベントを受け取ったあとに[イベントの詳細]ページで直接作成することもできます。

手順

1. 左側のナビゲーション ペインで、**[設定]** > **[アラート生成]**をクリックします。
2. **[設定/アラート生成]**ページで、**[追加]**をクリックします。
3. **[アラートの追加]**ダイアログ ボックスで、**[名前]**をクリックし、アラートの名前と説明を入力します。
4. **[リソース]**をクリックし、アラートの対象に含めるリソースまたは除外するリソースを選択します。

   リソースのグループを選択する場合は、**[名前に次の文字を含む]]**フィールドにテキスト文字列を指定してフィルタを設定できます。指定したテキスト文字列に基づいて、フィルタ ルールに一致するリソースのみが利用可能なリソースのリストに表示されます。テキスト文字列の指定では、大文字と小文字が区別されます。

   あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。
5. **[イベント]**をクリックし、アラートをトリガーするイベントをイベント名またはイベントの重大度タイプに基づいて選択します。

   ヒント : 複数のイベントを選択するには、Ctrlキーを押しながら選択します。
6. **[操作]**をクリックして、通知するユーザ、通知の頻度、およびSNMPトラップをトラップレシーバに送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。

   注 : 該当するユーザのEメール アドレスを変更し、その後アラートを編集するために開くと、[名前]フィールドは空欄になります。これは、Eメールが変更されたことでユーザとのマッピングが無効になったためです。また、選択したユーザのEメール アドレ

スを[管理/ユーザ]ページで変更した場合、変更後のEメール アドレスは反映されません。

SNMPトラップを使用してユーザに通知することもできます。

7. **[保存]**をクリックします。

アラートの追加例

ここでは、次の要件を満たすアラートを作成する例を示します。

- アラート名：HealthTest
- リソース：名前に「abc」を含むすべてのボリュームを対象に含め、名前に「xyz」を含むすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを対象に含める
- 処理：「テスト」スクリプトを割り当て、「sample@domain.com」のユーザに15分ごとに通知する

[アラートの追加]ダイアログ ボックスで、次の手順を実行します。

1. **[名前]**をクリックし、**[アラート名]**フィールドに「**`HealthTest`**」と入力します。
2. **[リソース]**をクリックし、[含める]タブで、ドロップダウン リストから**[ボリューム]**を選択します。
   a. **[名前に次の文字を含む]**フィールドに「**`abc`**」と入力して、名前に「abc」を含むボリュームを表示します。
   b. [使用可能なリソース]領域で**[<<名前に次の文字を含むすべてのボリューム - abc>>]**を選択し、[選択したリソース]領域に移動します。
   c. **[除外する]**をクリックし、**[名前に次の文字を含む]**フィールドに「**`xyz`**」と入力して**[追加]**をクリックします。
3. **[イベント]**をクリックし、[イベントの重大度]フィールドで**[重大]**を選択します。
4. [一致イベント]領域で**[すべての重大イベント]**を選択し、[選択したイベント]領域に移動します。
5. **[操作]**をクリックし、[アラートを通知するユーザ]フィールドに「**`sample@domain.com`**」と入力します。
6. **[通知間隔：15 分]**を選択して、ユーザに15分ごとに通知します。
   指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。
7. [実行するスクリプトを選択してください]メニューで、**[テスト]**スクリプトを選択します。
8. **[保存]**をクリックします。

Unified Managerに自動的に追加されるEMSイベント

Unified Managerには次のONTAP EMSイベントが自動的に追加されます。これらのイベントは、Unified Managerが監視しているいずれかのクラスタでトリガーされると生成されます。

ONTAP 9.5以降のソフトウェアを実行しているクラスタの監視では、次のEMSイベントを使用できます。

Unified Managerのイベント名	EMSのイベント名	影響を受けるリソース	ONTAPの重大度
アグリゲートの再配置でオブジェクト ストアへのアクセス拒否	arl.netra.ca.check.failed	アグリゲート	エラー
ストレージ フェイルオーバー時のアグリゲートの再配置でオブジェクト ストアへのアクセス拒否	gb.netra.ca.check.failed	アグリゲート	エラー
FabricPool スペースがほぼフル	fabricpool.nearly.full	クラスタ	エラー
NVMF の猶予期間 - 開始	nvmf.graceperiod.start	クラスタ	警告
NVMF の猶予期間 - アクティブ	nvmf.graceperiod.active	クラスタ	警告
NVMF の猶予期間 - 終了	nvmf.graceperiod.expired	クラスタ	警告
LUN を破棄	lun.destroy	LUN	情報
Cloud AWS メタデータ接続エラー	cloud.aws.metadataConnFail	ノード	エラー
Cloud AWS IAM クレデンシャルが期限切れ	cloud.aws.iamCredsExpired	ノード	エラー
Cloud AWS IAM クレデンシャルが無効	cloud.aws.iamCredsInvalid	ノード	エラー
Cloud AWS IAM クレデンシャルが見つからない	cloud.aws.iamCredsNotFound	ノード	エラー
Cloud AWS IAM クレデンシャルが初期化されていない	cloud.aws.iamNotInitialized	ノード	情報
Cloud AWS IAM ロールが無効	cloud.aws.iamRoleInvalid	ノード	エラー
Cloud AWS IAM ロールが見つからない	cloud.aws.iamRoleNotFound	ノード	エラー
オブジェクト ストアのホスト解決不可	objstore.host.unresolvable	ノード	エラー
オブジェクト ストアのクラスタ間 LIF が停止	objstore.interclusterlifDown	ノード	エラー
要求とオブジェクト ストアシグネチャの不一致	osc.signatureMismatch	ノード	エラー

Unified Managerのイベント名	EMSのイベント名	影響を受けるリソース	ONTAPの重大度
NFSv4 プールの 1 つに空きなし	Nblade.nfsV4PoolExhaust	ノード	重大
QoS 監視メモリの最大化	qos.monitor.memory.maxed	ノード	エラー
QoS 監視メモリの縮小	qos.monitor.memory.abated	ノード	情報
NVMe ネームスペースの破棄	NVMeNS.destroy	ネームスペース	情報
NVMe ネームスペース オンライン	NVMeNS.offline	ネームスペース	情報
NVMe ネームスペース オフライン	NVMeNS.online	ネームスペース	情報
NVMe ネームスペース スペース不足	NVMeNS.out.of.space	ネームスペース	警告
同期レプリケーションが同期されていない	sms.status.out.of.sync	SnapMirror関係	警告
同期レプリケーションをリストア	sms.status.in.sync	SnapMirror関係	情報
同期レプリケーションの自動再同期失敗	sms.resync.attempt.failed	SnapMirror関係	エラー
多数の CIFS 接続	Nblade.cifsManyAuths	SVM	エラー
最大 CIFS 接続数を超過	Nblade.cifsMaxOpenSameFile	SVM	エラー
ユーザあたりの最大 CIFS 接続数を超過	Nblade.cifsMaxSessPerUsrConn	SVM	エラー
CIFS NetBIOS 名が競合	Nblade.cifsNbNameConflict	SVM	エラー
存在しない CIFS 共有に対する試行	Nblade.cifsNoPrivShare	SVM	重大
CIFS シャドウ コピー処理が失敗	cifs.shadowcopy.failure	SVM	エラー
AV サーバがウィルスを検出	Nblade.vscanVirusDetected	SVM	エラー
ウィルス スキャン用の AV サーバ接続がない	Nblade.vscanNoScannerConn	SVM	重大
AV サーバが未登録	Nblade.vscanNoRegdScanner	SVM	エラー
応答する AV サーバ接続がない	Nblade.vscanConnInactive	SVM	情報
AV サーバがビジーのため新しいスキャン要求の受け入れ不可	Nblade.vscanConnBackPressure	SVM	エラー

Unified Managerのイベント名	EMSのイベント名	影響を受けるリソース	ONTAPの重大度
権限のないユーザが AV サーバへのアクセスを試行	Nblade.vscanBadUserPrivAccess	SVM	エラー
FlexGroup コンスティチュエントのスペースに問題あり	flexgroup.constituents.have.space.issues	ボリューム	エラー
FlexGroup コンスティチュエントのスペース ステータスがすべて正常	flexgroup.constituents.space.status.all.ok	ボリューム	情報
FlexGroup コンスティチュエントの inode に問題あり	flexgroup.constituents.have.inodes.issues	ボリューム	エラー
FlexGroup コンスティチュエントの inode ステータスがすべて正常	flexgroup.constituents.inodes.status.all.ok	ボリューム	情報
ボリューム論理スペースがほぼフル	monitor.vol.nearFull	ボリューム	警告
ボリューム論理スペースがフル	monitor.vol.full	ボリューム	エラー
ボリューム論理スペースが正常	monitor.vol.one.ok	ボリューム	情報
WAFL ボリュームのオートサイズが失敗	wafl.vol.autoSize.fail	ボリューム	エラー
WAFL ボリュームのオートサイズ完了	wafl.vol.autoSize.done	ボリューム	情報
WAFL READDIR ファイル処理タイムアウト	wafl.readdir.expired	ボリューム	エラー

ONTAP EMSイベントへの登録

ONTAPソフトウェアがインストールされているシステムで生成されたEvent Management System（EMS;イベント管理システム）イベントを受け取るように登録することができます。一部のEMSイベントはUnified Managerに自動的に報告されますが、それ以外のEMSイベントは登録している場合にのみ報告されます。

開始する前に

同じ問題に対するイベントを2つ受け取って混乱を招く可能性があるため、Unified Managerにすでに自動的に追加されているEMSイベントは登録しないでください。

タスク概要

EMSイベントはいくつでも登録できます。登録したすべてのイベントが検証され、検証済みのイベントだけがUnified Managerで監視しているクラスタに適用されます。『*ONTAP 9 EMS* イベント カタログ』には、指定したバージョンのONTAP 9ソフトウェアのすべてのEMSメッセージに関する詳細な情報が記載されています。該当するイベントの一覧については、ONTAP 9製品ドキュメントのページから該当するバージョンの『*EMS*イベント カタログ』を参照してください。

ONTAP 9製品ライブラリ

登録したONTAP EMSイベントにアラートを設定したり、それらのイベントに対して実行するカスタム スクリプトを作成したりできます。

注 : 登録したONTAP EMSイベントが届かない場合は、クラスタのDNS設定に問題があり、クラスタからUnified Managerサーバに到達できなくなっていることが考えられます。その場合は、クラスタ管理者がクラスタのDNS設定を修正し、Unified Managerを再起動する必要があります。これにより、保留中のEMSイベントがUnified Managerサーバに送信されます。

手順

1. 左側のナビゲーション ペインで、**[設定]** > **[イベントの管理]**をクリックします。
2. **[設定/イベントの管理]**ページで、**[EMS イベントにサブスクライブ]**ボタンをクリックします。
3. **[EMS イベントにサブスクライブ]**ダイアログ ボックスで、登録するONTAP EMSイベントの名前を入力します。

   登録可能なEMSイベントの名前を確認するには、ONTAPのクラスタ シェルで`event route show`コマンド（ONTAP 9より前）または`event catalog show`コマンド（ONTAP 9以降）を使用します。個々のEMSイベントを特定する詳しい手順については、ナレッジベースの回答1072320を参照してください。

   KB 1072320 - How to configure ONTAP EMS event subscriptions in Unified Manager
4. **[追加]**をクリックします。

   EMSイベントが[サブスクライブ済み EMS イベント]リストに追加されます。ただし、この時点では、追加したEMSイベントの[クラスタに該当]列のステータスは「不明」と表示されます。
5. **[保存して閉じる]**をクリックして、EMSイベントの登録内容をクラスタに登録します。
6. **[EMS イベントにサブスクライブ]**をもう一度クリックします。

   追加したEMSイベントの[クラスタに該当]列のステータスが「はい」に変わります。

   ステータスが「はい」にならない場合は、ONTAP EMSイベントの名前に間違いがないかを確認します。入力した名前に間違いがあった場合は、そのイベントを削除して追加し直す必要があります。

次のタスク

ONTAP EMSイベントが発生すると、そのイベントが[イベント]ページに表示されます。イベントを選択すると、EMSイベントに関する詳細を[イベントの詳細]ページで確認できます。イベントの処理を管理したり、イベントのアラートを作成したりすることもできます。

SAML認証の設定の管理

リモート認証を設定したら、Security Assertion Markup Language（SAML）認証を有効にして、Unified ManagerのWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

SAML認証を有効にしたあとでUnified Managerのグラフィカル ユーザ インターフェイスにアクセスできるのはリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソールにアクセスするユーザには影響しません。

アイデンティティ プロバイダの要件

すべてのリモート ユーザについてアイデンティティ プロバイダ（IdP）を使用してSAML認証を実行するようにUnified Managerで設定するときは、Unified Managerに正しく接続できるように、いくつかの必要な設定を確認しておく必要があります。

Unified ManagerのURIとメタデータをIdPサーバに入力する必要があります。この情報は、Unified Managerの[SAML 認証]ページからコピーできます。Unified Managerは、Security Assertion Markup Language（SAML）標準のサービス プロバイダ（SP）とみなされます。

サポートされる暗号化標準

- Advanced Encryption Standard（AES）：AES-128およびAES-256
- Secure Hash Algorithm（SHA）：SHA-1およびSHA-256

検証済みのアイデンティティ プロバイダ

- Shibboleth
- Active Directoryフェデレーション サービス（ADFS）

ADFSの設定要件

- 3つの要求規則を次の順序で定義する必要があります。これらは、この証明書利用者信頼エントリに対するADFS SAML応答をUnified Managerで解析するために必要です。

要求規則	値
SAM-account-name	Name ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Token groups – Unqualified Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- 認証方法を「フォーム認証」に設定する必要があります。これを行わないと、Internet Explorerを使用しているユーザがUnified Managerからログアウトするときにエラーが表示されることがあります。次の手順を実行します。

  1. ADFS管理コンソールを開きます。
  2. 左側のツリー ビューで[認証ポリシー]フォルダをクリックします。
  3. 右側の[操作]で、[グローバル プライマリ認証ポリシーの編集]をクリックします。
  4. [イントラネット認証方法]をデフォルトの「Windows認証」ではなく「フォーム認証」に設定します。

- Unified Managerのセキュリティ証明書がCA署名証明書の場合、IdP経由でのログインが拒否されることがあります。この問題の対処方法は2つあります。
  - 次のリンクの手順に従って、CA証明書チェーンの関連する証明書利用者についてのADFSサーバでの失効確認を無効にします。
    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/
  - ADFSサーバ内にあるCAサーバでUnified Managerサーバ証明書要求に署名します。

その他の設定要件

- Unified Managerのクロック スキューは5分に設定されているため、IdPサーバとUnified Managerサーバの時間の差が5分を超えないようにします。時間の差が5分を超えると認証が失敗します。

- ユーザがInternet Explorerを使用してUnified Managerにアクセスしようとしたときに、**「Webサイト側でページを表示できません」**というメッセージが表示されることがあります。この場合は、**[ツール]** > **[インターネット オプション]** > **[詳細設定]**で「HTTPエラーメッセージを簡易表示する」オプションをオフにします。

SAML認証の有効化

Security Assertion Markup Language（SAML）認証を有効にして、Unified Manager Web UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

開始する前に

- リモート認証を設定し、正常に動作することを確認しておく必要があります。
- 管理者ロールが割り当てられたリモート ユーザまたはリモート グループを少なくとも1つ作成しておく必要があります。
- アイデンティティ プロバイダ（IdP）がUnified Managerでサポートされ、設定が完了している必要があります。
- IdPのURLとメタデータが必要です。
- IdPサーバへのアクセスが必要です。

タスク概要

Unified ManagerでSAML認証を有効にしたあと、Unified Managerサーバのホスト情報を使用してIdPを設定するまでは、ユーザはグラフィカル ユーザ インターフェイスにアクセスできません。そのため、設定プロセスを開始する前に、両方で接続の準備を完了しておく必要があります。IdPの設定は、Unified Managerの設定前にも設定後にも実行できます。

SAML認証を有効にしたあとでUnified Managerのグラフィカル ユーザ インターフェイスにアクセスできるのはリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソール、Unified Managerのコマンド、ZAPIにアクセスするユーザには影響しません。

注： このページでSAMLの設定を完了すると、Unified Managerが自動的に再起動されます。

手順

1. ツールバーで  をクリックし、左側の[セットアップ]メニューで**[認証]**をクリックします。
2. **[セットアップ/認証]**ページで、**[SAML 認証]**タブを選択します。
3. **[SAML 認証を有効にする]**チェックボックスを選択します。

   IdPの接続の設定に必要なフィールドが表示されます。
4. IdPのURIとUnified ManagerサーバをIdPに接続するために必要なIdPメタデータを入力します。

   IdPサーバにUnified Managerサーバから直接アクセスできる場合は、IdPのURIを入力したあとに**[IdP メタデータの読み込み]**をクリックすると、[IdP メタデータ]フィールドに情報が自動的に入力されます。
5. Unified Managerのホスト メタデータURIをコピーするか、メタデータをXMLテキストファイルに保存します。

   この情報を使用してIdPサーバを設定できます。

6. **[保存]**をクリックします。

   設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

7. **[確認してログアウト]**をクリックします。Unified Managerが再起動されます。

タスクの結果

許可されたリモート ユーザがUnified Managerのグラフィカル インターフェイスにアクセスする際にクレデンシャルを入力するページが、次回からUnified Managerのログイン ページではなくIdPのログイン ページに変わります。

次のタスク

まだ完了していない場合は、IdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。

重要：アイデンティティ プロバイダにADFSを使用している場合は、Unified Manager GUIでADFSのタイムアウトが考慮されず、Unified Managerのセッション タイムアウトに達するまでセッションが続行されます。Unified ManagerをWindows、Red Hat、またはCentOSに導入している場合は、次のUnified Manager CLIコマンドを使用してGUIのセッション タイムアウトを変更できます。`um option set absolute.session.timeout=00:15:00`

このコマンドを実行すると、Unified ManagerのGUIのセッション タイムアウトが15分に設定されます。

関連タスク

リモート認証の有効化（10ページ）
ユーザの追加（14ページ）

関連資料

アイデンティティ プロバイダの要件（21ページ）

データベース バックアップの設定

Unified Managerのデータベース バックアップ設定で、データベースのバックアップ パス、保持数、およびバックアップ スケジュールを設定できます。日単位または週単位のスケジュールされたバックアップを有効にすることができます。デフォルトでは、スケジュールされたバックアップは無効になっています。

開始する前に

- オペレータ、管理者、またはストレージ管理者のロールが必要です。
- バックアップ パスとして定義する場所に150GB以上の利用可能なスペースが必要です。Unified Managerホスト システムとは別のリモートの場所を使用することを推奨します。
- Unified ManagerをLinuxシステムにインストールしている場合は、「jboss」ユーザにバックアップ ディレクトリへの書き込み権限が割り当てられていることを確認してください。
- 新しいクラスタの追加後にUnified Managerで15日分の履歴パフォーマンス データを収集している間は、バックアップ処理を実行しないようにスケジュールしてください。

タスク概要

初回のバックアップではフル バックアップが実行されるため、2回目以降のバックアップよりも時間がかかります。フル バックアップは1GBを超えることもあり、3～4時間かかる場合があります。2回目以降は増分バックアップとなるため、所要時間は短くなります。

手順

1. ツールバーで  をクリックし、**[管理]** > **[データベース バックアップ]**をクリックします。
2. **[管理/データベース バックアップ]**ページで、**[操作]** > **[データベース バックアップ設定]**をクリックします。
3. バックアップ パスと保持数の値を設定します。

   保持数のデフォルト値は10です。バックアップを無制限に作成する場合は0に設定します。
4. **[スケジュール頻度]**セクションで、**[有効化]**チェックボックスをオンにし、日単位または週単位のいずれかのスケジュールを指定します。

   毎日

   このオプションを選択する場合は、バックアップを作成する時刻を24時間形式で入力する必要があります。たとえば、18:30と指定すると、毎日午後6:30にバックアップが作成されます。

   毎週

   このオプションを選択する場合は、バックアップを作成する時刻と曜日を指定する必要があります。たとえば、曜日を月曜日、時刻を16:30と指定すると、毎週月曜日の午後4:30にバックアップが作成されます。
5. **[保存して閉じる]**をクリックします。

ローカル ユーザのパスワードの変更

潜在的なセキュリティ リスクを回避するために、ローカル ユーザのログイン パスワードを変更することができます。

開始する前に

ローカル ユーザとしてログインする必要があります。

タスク概要

リモート ユーザとメンテナンス ユーザのパスワードについては、この手順では変更できません。リモート ユーザのパスワードを変更するには、パスワードの管理者に連絡してください。メンテナンス ユーザのパスワードを変更するには、「*Active IQ Unified Managerワークフロー ガイド - クラスタ健全性管理*」の「メンテナンス コンソールの使用」の章を参照してください。

手順

1. Unified Managerにログインします。
2. 上部のメニュー バーから、ユーザのアイコンをクリックして**[パスワードの変更]**をクリックします。

   [パスワードの変更オプションは、リモート ユーザには表示されません。

3. **[パスワードの変更]**ダイアログ ボックスで、現在のパスワードと新しいパスワードを入力します。
4. **[保存]**をクリックします。

次のタスク

Unified Managerがハイアベイラビリティ構成の場合は、セットアップのもう一方のノードでパスワードを変更する必要があります。パスワードは両方のインスタンスで同じにする必要があります。

Unified Managerのホスト名の変更

必要に応じて、Unified Managerをインストールしたシステムのホスト名をあとから変更することができます。たとえば、タイプ、ワークグループ、監視対象のクラスタ グループなどがわかるような名前に変更すると、Unified Managerサーバを識別しやすくなります。

ホスト名を変更する手順は、Unified ManagerをVMware ESXiサーバ、Red Hat Linuxサーバまたは CentOS Linuxサーバ、Microsoft Windowsサーバのいずれで実行しているかによって異なります。

Unified Manager仮想アプライアンスのホスト名の変更

ネットワーク ホストの名前は、Unified Manager仮想アプライアンスの導入時に割り当てられます。このホスト名は導入後に変更することができます。ホスト名を変更する場合は、HTTPS証明書も再生成する必要があります。

開始する前に

このタスクを実行するには、Unified Managerにメンテナンス ユーザとしてログインするか、管理者ロールが割り当てられている必要があります。

タスク概要

Unified Manager Web UIには、ホスト名（またはホストのIPアドレス）を使用してアクセスできます。導入時に静的IPアドレスを使用してネットワークを設定した場合は、指定したネットワーク ホストの名前を使用します。DHCPを使用してネットワークを設定した場合は、DNSからホスト名を取得します。DHCPまたはDNSが適切に設定されていないと、「Unified Manager」というホスト名が自動的に割り当てられ、セキュリティ証明書に関連付けられます。

ホスト名を変更した場合、Unified Manager Web UIへのアクセスに新しいホスト名を使用するには、ホスト名の元の割り当て方法に関係なく、必ず新しいセキュリティ証明書を生成する必要があります。

ホスト名ではなくサーバのIPアドレスを使用してWeb UIにアクセスする場合は、ホスト名の変更時に新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。

Unified Managerでホスト名を変更したら、OnCommand Workflow Automation（WFA）で手動でホスト名を更新する必要があります。ホスト名はWFAでは自動的に更新されません。

新しい証明書は、Unified Manager仮想マシンを再起動するまで有効になりません。

手順

1. *HTTPS*セキュリティ証明書を生成する（26ページ）

   新しいホスト名を使用してUnified Manager Web UIにアクセスする場合は、HTTPS証明書を再生成して新しいホスト名に関連付ける必要があります。

2. *Unified Manager*仮想マシンを再起動する（27ページ）

   HTTPS証明書を再生成したら、Unified Manager仮想マシンを再起動する必要があります。

HTTPSセキュリティ証明書の生成

別の認証局の署名を使用する場合や現在のセキュリティ証明書の期限が切れた場合など、さまざまな理由で新しいHTTPSセキュリティ証明書を生成することがあります。新しい証明書を生成すると既存の証明書が置き換えられます。

開始する前に

管理者のロールが必要です。

タスク概要

Unified Manager Web UIにアクセスできない場合は、メンテナンス コンソールを使用して同じ値でHTTPS証明書を再生成できます。

手順

1. ツールバーで  をクリックし、**[セットアップ]**メニューの**[HTTPS 証明書]**をクリックします。
2. **[HTTPS 証明書の再生成]**をクリックします。

   [HTTPS 証明書の再生成]ダイアログ ボックスが表示されます。
3. 証明書を生成する方法に応じて、次のいずれかを実行します。

目的	操作
現在の値で証明書を再生成する	**[現在の証明書属性を使用して再生成]**オプションをクリックします。
別の値で証明書を生成する	**[現在の証明書属性を更新]**オプションをクリックします。 [共通名]フィールドと[別名]フィールドについては、新しい値を入力しなければ既存の証明書の値が使用されます。それ以外のフィールドの値は必須ではありませんが、証明書に表示する場合は[市町村]、[都道府県]、[国]などの値を入力できます。 **注：** 証明書の[別名]フィールドにローカルの識別情報を含めない場合は、[ローカルの識別情報を除外する（ローカルホストなど）]チェックボックスを選択します。このチェックボックスを選択すると、このフィールドで入力した情報だけが[別名]フィールドで使用されます。このフィールドを空白にした場合は、[別名]フィールドを含めずに証明書が生成されます。

4. **[はい]**をクリックして証明書を再生成します。
5. 新しい証明書を有効にするためにUnified Managerサーバを再起動します。

次のタスク

HTTPS証明書を表示して新しい証明書の情報を確認します。

関連タスク

*Unified Manager*仮想アプライアンスのホスト名の変更（25ページ）

Unified Manager仮想マシンの再起動

仮想マシンは、Unified Managerのメンテナンス コンソールから再起動できます。新しいセキュリティ証明書を生成した場合や仮想マシンで問題が発生した場合、仮想マシンの再起動が必要になります。

開始する前に

仮想アプライアンスの電源をオンにします。

メンテナンス コンソールにメンテナンス ユーザとしてログインします。

タスク概要

仮想マシンは、vSphereから**[Restart Guest]**オプションを使用して再起動することもできます。詳細については、VMwareのドキュメントを参照してください。

手順

1. メンテナンス コンソールにアクセスします。
2. **[System Configuration]** > **[Reboot Virtual Machine]**を選択します。

関連タスク

*Unified Manager*仮想アプライアンスのホスト名の変更（25ページ）

LinuxシステムでのUnified Managerホスト名の変更

必要に応じて、Unified ManagerをインストールしたRed Hat Enterprise LinuxまたはCentOSマシンのホスト名をあとから変更することができます。たとえば、タイプ、ワークグループ、監視対象のクラスタ グループなどがわかるような名前に変更すると、Linuxマシンのリストでの Unified Managerサーバを識別しやすくなります。

開始する前に

Unified ManagerがインストールされているLinuxシステムへのrootユーザ アクセスが必要です。

タスク概要

Unified Manager Web UIには、ホスト名（またはホストのIPアドレス）を使用してアクセスできます。導入時に静的IPアドレスを使用してネットワークを設定した場合は、指定したネットワーク ホストの名前を使用します。DHCPを使用してネットワークを設定した場合は、DNSサーバからホスト名を取得します。

ホスト名を変更した場合、Unified Manager Web UIへのアクセスに新しいホスト名を使用するには、ホスト名の元の割り当て方法に関係なく、必ず新しいセキュリティ証明書を生成する必要があります。

ホスト名ではなくサーバのIPアドレスを使用してWeb UIにアクセスする場合は、ホスト名の変更時に新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。新しい証明書は、Linuxマシンを再起動するまで有効になりません。

Unified Managerでホスト名を変更したら、OnCommand Workflow Automation（WFA）で手動でホスト名を更新する必要があります。ホスト名はWFAでは自動的に更新されません。

手順

1. 変更するUnified Managerシステムにrootユーザとしてログインします。
2. 次のコマンドを記載された順序で入力して、Unified Managerソフトウェアと関連するMySQLソフトウェアを停止します。

   ```
   service ocieau stop
   service ocie stop
   service mysqld stop
   ```

3. Linuxの`hostnamectl`コマンドを使用してホスト名を変更します。

   ```
   hostnamectl set-hostname new_FQDN
   ```

   例

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. サーバのHTTPS証明書を再生成します。

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. ネットワーク サービスを再起動します。

   ```
   service network restart
   ```

6. サービスが再起動されたら、新しいホスト名でpingを実行できるかどうかを確認します。

   ```
   ping new_hostname
   ```

   例

   ```
   ping nuhost
   ```

   元のホスト名に対して設定していた同じIPアドレスが返されることを確認します。

7. ホスト名を変更して確認したら、次のコマンドを記載された順序で入力してUnified Managerを再起動します。

   ```
   service mysqld start
   service ocie start
   service ocieau start
   ```

メンテナンス コンソールの使用

メンテナンス コンソールでは、ネットワークの設定、Unified Managerがインストールされているシステムの設定と管理、潜在的な問題の防止とトラブルシューティングに役立つその他のメンテナンス タスクを実行することができます。

関連概念

メンテナンス コンソールで提供される機能（29ページ）
診断ユーザの権限（30ページ）

メンテナンス コンソールで提供される機能

Unified Managerのメンテナンス コンソールでは、Unified Managerシステムの設定を管理し、問題の発生を防ぐために必要な変更を行うことができます。

メンテナンス コンソールでは、Unified Managerをインストールしたオペレーティング システムに応じて次の機能が提供されます。

- 仮想アプライアンスに関する問題のトラブルシューティング（特に、Unified Manager Web インターフェイスを使用できない場合）
- Unified Managerの新しいバージョンへのアップグレード
- テクニカル サポートに送信するサポート バンドルの生成
- ネットワークの設定
- メンテナンス ユーザのパスワードの変更
- パフォーマンス統計の送信を目的とした外部データ プロバイダへの接続
- パフォーマンス データ収集の内部変更
- 以前にバックアップしたバージョンからのUnified Managerデータベースと設定のリストア

関連タスク

メンテナンス コンソールの使用（29ページ）

メンテナンス ユーザの役割

Unified ManagerをRed Hat Enterprise LinuxまたはCentOSシステムにインストールする場合、インストール時にメンテナンス ユーザが作成されます。メンテナンス ユーザの名前は「umadmin」です。メンテナンス ユーザは、Web UIで管理者ロールが割り当てられ、他のユーザを作成してロールを割り当てることができます。

メンテナンス ユーザまたはumadminユーザは、Unified Managerのメンテナンス コンソールにもアクセスできます。

関連タスク

メンテナンス コンソールの使用（29ページ）

診断ユーザの権限

診断アクセスの目的は、テクニカル サポートからトラブルシューティングのサポートを受けられるようにすることです。このため、テクニカル サポートから指示された場合にのみ診断アクセスを使用する必要があります。

診断ユーザは、テクニカル サポートからの指示を受けて、トラブルシューティングの目的でOSレベルのコマンドを実行できます。

関連タスク

メンテナンス コンソールの使用（29ページ）

メンテナンス コンソールへのアクセス

Unified Managerユーザ インターフェイスが動作状態でない場合、またはこのユーザ インターフェイスにない機能を実行する必要がある場合は、メンテナンス コンソールにアクセスしてUnified Managerシステムを管理できます。

開始する前に

Unified Managerをインストールして設定しておく必要があります。

タスク概要

15分間操作しないと、メンテナンス コンソールからログアウトされます。

注： VMwareにインストールした場合、VMwareコンソールからメンテナンス ユーザとしてすでにログインしているときは、Secure Shellを使用して同時にログインできません。

手順

1. 次の手順に従ってメンテナンス コンソールにアクセスします。

オペレーティング システム	手順
VMware	a. Secure Shellを使用して、Unified Manager仮想アプライアンスのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。
Linux	a. Secure Shellを使用して、Unified ManagerシステムのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ（umadmin）の名前とパスワードでシステムにログインします。 c. コマンド`maintenance_console`を入力し、Enterキーを押します。

オペレーティング システム	手順
Windows	a. 管理者のクレデンシャルでUnified Managerシステムにログインします。 b. Windows管理者としてPowerShellを起動します。 c. コマンド**maintenance_console**を入力し、Enterキーを押します。 **注：** Microsoft Windows Server 2012で実行ポリシー エラーが表示された場合は、次のコマンドを入力したあとに手順cをもう一度実行してください。**PowerShell.exe -ExecutionPolicy RemoteSigned**

Unified Managerメンテナンス コンソール メニューが表示されます。

関連タスク

メンテナンス コンソールの使用（29ページ）

vSphere VMコンソールを使用したメンテナンス コンソールへのアクセス

Unified Managerユーザ インターフェイスが動作状態でない場合、またはこのユーザ インターフェイスにない機能を実行する必要がある場合は、メンテナンス コンソールにアクセスして仮想アプライアンスを再設定できます。

開始する前に

メンテナンス ユーザである必要があります。メンテナンス コンソールにアクセスするには、仮想アプライアンスの電源をオンにする必要があります。

タスク概要

手順

1. vSphere Clientで、Unified Manager仮想アプライアンスを見つけます。
2. **[Console]**タブをクリックします。
3. コンソール ウィンドウ内をクリックしてログインします。
4. ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。

   15分間操作しないと、メンテナンス コンソールからログアウトされます。

関連タスク

メンテナンス コンソールの使用（29ページ）

メンテナンス コンソールのメニュー

メンテナンス コンソールは各種のメニューで構成され、Unified Managerサーバの特別な機能や設定の保守と管理を実行できるようになっています。

Unified Managerをインストールしたオペレーティング システムに応じて、メンテナンス コンソールは次のメニューで構成されます。

- Upgrade Unified Manager（VMwareのみ）
- Network Configuration（VMwareのみ）
- System Configuration（VMwareのみ）
- Support/Diagnostics
- Reset Server Certificate
- External Data Provider
- Performance Polling Interval Configuration

[Network Configuration]メニュー

[Network Configuration]メニューでは、ネットワーク設定を管理することができます。このメニューは、Unified Managerユーザ インターフェイスを使用できない場合に使用してください。

注 : Unified ManagerがRed Hat Enterprise Linux、CentOS、またはMicrosoft Windowsにインストールされている場合は、このメニューを使用できません。

表示されるメニュー項目は次のとおりです。

Display IP Address Settings

仮想アプライアンスの現在のネットワーク設定が表示されます（IPアドレス、ネットワーク、ブロードキャスト アドレス、ネットマスク、ゲートウェイ、DNSサーバなど）。

Change IP Address Settings

仮想アプライアンスのネットワーク設定を変更することができます（IPアドレス、ネットマスク、ゲートウェイ、DNSサーバなど）。メンテナンス コンソールでネットワーク設定をDHCPから静的ネットワークに切り替えた場合は、ホスト名を編集できません。変更を有効にするには、**[Commit Changes]**を選択する必要があります。

Display Domain Name Search Settings

ホスト名の解決に使用されるドメイン名検索リストが表示されます。

Change Domain Name Search Settings

ホスト名を解決する際に検索するドメイン名を変更することができます。変更を有効にするには、**[Commit Changes]**を選択する必要があります。

Display Static Routes

現在の静的ネットワーク ルートが表示されます。

Change Static Routes

静的ネットワーク ルートを追加または削除することができます。変更を有効にするには、**[Commit Changes]**を選択する必要があります。

Add Route

静的ルートを追加することができます。

Delete Route

静的ルートを削除することができます。

Back

[Main Menu]に戻ります。

Exit

メンテナンス コンソールを終了します。

Disable Network Interface

使用可能なネットワーク インターフェイスを無効にします。使用可能なネットワーク インターフェイスが1つしかない場合は、それを無効にすることはできません。変更を有効にするには、**[Commit Changes]**を選択する必要があります。

Enable Network Interface

使用可能なネットワーク インターフェイスを有効にします。変更を有効にするには、**[Commit Changes]**を選択する必要があります。

Commit Changes

仮想アプライアンスのネットワーク設定に加えた変更を適用します。変更を有効にするには、必ずこのオプションを選択します。そうしないと、変更は適用されません。

Ping a Host

IPアドレスの変更やDNS設定を確認するために、ターゲット ホストにpingを実行します。

Restore to Default Settings

すべての設定を工場出荷時のデフォルトにリセットします。変更を有効にするには、**[Commit Changes]**を選択する必要があります。

Back

[Main Menu]に戻ります。

Exit

メンテナンス コンソールを終了します。

[System Configuration]メニュー

[System Configuration]メニューには、仮想アプライアンスを管理するためのさまざまなオプションが用意されています（サーバ ステータスの表示、仮想マシンのリブートとシャットダウンなど）。

注 : Unified ManagerがRed Hat Enterprise Linux、CentOS、またはMicrosoft Windowsにインストールされている場合は、[System Configuration]メニューを使用できません。

表示されるメニュー項目は次のとおりです。

Display Server Status

現在のサーバ ステータスを表示します。ステータスには「Running」と「Not Running」があります。

サーバが実行されていない場合は、テクニカル サポートに連絡することを推奨します。

Reboot Virtual Machine

すべてのサービスを停止して仮想マシンをリブートします。リブート後、仮想マシンとサービスが再起動します。

Shut Down Virtual Machine

すべてのサービスを停止して仮想マシンをシャットダウンします。

このオプションは、仮想マシン コンソールからのみ選択できます。

Change <logged in user> User Password

現在ログインしているユーザ（メンテナンス ユーザ）のパスワードを変更します。

Increase Data Disk Size

仮想マシンのデータ ディスク（ディスク3）のサイズを拡張します。

Increase Swap Disk Size

仮想マシンのスワップ ディスク（ディスク2）のサイズを拡張します。

Change Time Zone

タイムゾーンを現在の場所に変更します。

Change NTP Server

NTPサーバの設定を変更します（IPアドレスや完全修飾ドメイン名（FQDN）など）。

Restore from a Unified Manager Backup

以前にバックアップしたバージョンからUnified Managerデータベースと設定をリストアします。

Reset Server Certificate

サーバ セキュリティ証明書をリセットします。

Change hostname

仮想アプライアンスがインストールされているホストの名前を変更します。

Back

[System Configuration]メニューを終了して[Main Menu]に戻ります。

Exit

メンテナンス コンソール メニューを終了します。

[Support and Diagnostics]メニュー

[Support and Diagnostics]メニューでは、サポート バンドルを生成することができます。

表示されるメニュー オプションは次のとおりです。

Generate Support Bundle

診断ユーザのホーム ディレクトリに、詳細な診断情報を収めた7-Zipファイルを作成することができます。このファイルには、AutoSupportメッセージで生成された情報、Unified Managerデータベースの内容、Unified Managerサーバの内部に関する詳細なデータ、およびAutoSupportメッセージには通常含まれない詳細なログが収められます。

その他のメニュー オプション

次に示すメニュー オプションでは、Unified Managerサーバでさまざまな管理タスクを実行することができます。

表示されるメニュー項目は次のとおりです。

Reset Server Certificate

HTTPSサーバ証明書を再生成します。

Unified Manager GUIでサーバ証明書を再生成するには、  > **[HTTPS 証明書]** > **[HTTPS 証明書の再生成]**をクリックします。

Disable SAML authentication

SAML認証を無効にし、Unified ManagerのGUIにアクセスするユーザのアイデンティティ プロバイダ（IdP）によるサインオン認証を中止します。このコンソールオプションは、一般に、IdPサーバまたはSAMLの設定の問題が原因でUnified ManagerのGUIへのアクセスがブロックされる場合に使用します。

External Data Provider

Unified Managerを外部データ プロバイダに接続するためのオプションを提供します。接続が確立されると、パフォーマンス データが外部サーバに送信されて、ストレージ パフォーマンスのエキスパートがサードパーティ ソフトウェアを使用してパフォーマンス指標をグラフ化できるようになります。次のオプションが表示されます。

- **Display Server Configuration**：外部データ プロバイダに対する現在の接続設定と構成設定を表示します。
- **Add / Modify Server Connection**：外部データ プロバイダに対する新しい接続設定を入力したり、既存の設定を変更したりすることができます。
- **Modify Server Configuration**：外部データ プロバイダに対する新しい設定を入力したり、既存の設定を変更したりすることができます。
- **Delete Server Connection**：外部データ プロバイダとの接続を削除します。接続を削除すると、Unified Managerは外部サーバとの接続を失います。

Performance Polling Interval Configuration

Unified Managerがクラスタからパフォーマンス統計データを収集する頻度を設定するためのオプションを提供します。デフォルトの収集間隔は5分です。

大規模なクラスタからの収集が時間内に完了しない場合は、この間隔を10分または15分に変更できます。

Disable SAML authentication

Unified Manager GUIにアクセスできない場合にSAML認証を無効にする手段となります。この状況は、設定に誤りがある場合やIdPにアクセスできない場合に発生します。

View/Change Application Ports

Unified ManagerがHTTPおよびHTTPSプロトコルに使用するデフォルトのポートを変更するためのオプションを提供します（セキュリティ上必要である場合）。デフォルトのポートは、HTTPの場合は80、HTTPSの場合は443です。

Exit

メンテナンス コンソール メニューを終了します。

関連タスク

*Unified Manager*が*HTTP*および*HTTPS*プロトコルに使用するポートの変更（37ページ）

Windowsでのメンテナンス ユーザのパスワードの変更

Unified Managerのメンテナンス ユーザのパスワードを必要に応じて変更することができます。

手順

1. Unified Manager Web UIのログイン ページで、**[パスワードを忘れた場合]**をクリックします。

パスワードをリセットするユーザの名前を入力するように求めるページが表示されます。

2. ユーザ名を入力し、**[送信]**をクリックします。

   入力したユーザ名に定義されているEメール アドレスに、パスワードをリセットするためのリンクが記載されたEメールが送信されます。

3. Eメールの**[パスワードのリセット リンク]**をクリックし、新しいパスワードを定義します。

4. Web UIに戻り、新しいパスワードを使用してUnified Managerにログインします。

次のタスク

Unified ManagerがMicrosoft Cluster Server（MSCS）環境にインストールされている場合は、MSCSセットアップの2つ目のノードでメンテナンス ユーザのパスワードを変更する必要があります。メンテナンス ユーザのパスワードは、両方のノードで同じである必要があります。

Linuxシステムでのumadminパスワードの変更

セキュリティ上の理由から、インストール プロセスの完了後すぐにUnified Managerのumadminユーザのデフォルト パスワードを変更する必要があります。このパスワードは、必要に応じてあとからいつでも再変更できます。

開始する前に

- Unified ManagerがRed Hat Enterprise LinuxシステムまたはCentOS Linuxシステムにインストールされている必要があります。
- Unified Managerがインストールされ ているLinuxシステムのrootユーザのクレデンシャルが必要です。

手順

1. Unified Managerが実行されているLinuxシステムにrootユーザとしてログインします。
2. umadminパスワードを変更します。

   ```
   passwd umadmin
   ```

   umadminユーザの新しいパスワードを入力するように求められます。

次のタスク

Unified ManagerがVeritas Cluster Server（VCS）環境にインストールされている場合は、VCSセットアップのもう一方のノードでumadminパスワードを変更する必要があります。umadminパスワードは両方のノードで同じにする必要があります。

Unified ManagerがHTTPおよびHTTPSプロトコルに使用するポートの変更

Unified ManagerがHTTPおよびHTTPSプロトコルに使用するデフォルトのポートは、インストール後に変更できます（セキュリティ上必要な場合）。デフォルトのポートは、HTTPの場合は80、HTTPSの場合は443です。

開始する前に

Unified Managerサーバのメンテナンス コンソールへのログインが許可されているユーザIDとパスワードが必要です。

注：Mozilla FirefoxまたはGoogle Chromeブラウザでは、安全でないとみなされるポートがいくつかあります。HTTPトラフィックとHTTPSトラフィックに新しいポート番号を割り当てる前にブラウザで確認してください。安全でないポートを選択すると、システムにアクセスできなくなる可能性があります。その場合、カスタマー サポートに連絡して解決を依頼する必要があります。

タスク概要

ポートを変更するとUnified Managerのインスタンスが自動的に再起動されるため、システムを短時間停止しても問題のないタイミングであることを確認してください。

手順

1. SSHを使用して、Unified Managerホストにメンテナンス ユーザとしてログインします。

   Unified Managerのメンテナンス コンソールにプロンプトが表示されます。

2. **[View/Change Application Ports]**メニュー オプションの番号を入力し、Enterキーを押します。
3. プロンプトが表示されたら、メンテナンス ユーザのパスワードをもう一度入力します。
4. HTTPポートとHTTPSポートの新しいポート番号を入力し、Enterキーを押します。

   ポート番号を空白のままにした場合は、プロトコルのデフォルトのポートが割り当てられます。

   ポートを変更してUnified Managerをすぐに再起動するかどうかを確認するメッセージが表示されます。

5. **「y」**を入力してポートを変更し、Unified Managerを再起動します。
6. メンテナンス コンソールを終了します。

タスクの結果

この変更後にUnified Manager Web UIにアクセスする際にはURLに新しいポート番号を指定する必要があります（例：*https://host.company.com:1234*、*https://12.13.14.15:1122*、*https://[2001:db8:0:1]:2123*など）。

ネットワーク インターフェイスの追加

ネットワーク トラフィックを分離する必要がある場合は、新しいネットワーク インターフェイスを追加できます。

開始する前に

vSphereを使用して仮想アプライアンスにネットワーク インターフェイスを追加しておく必要があります。

仮想アプライアンスの電源をオンにする必要があります。

タスク概要

注 : Unified ManagerがRed Hat Enterprise LinuxまたはMicrosoft Windowsにインストールされている場合は、この処理を実行できません。

手順

1. vSphereコンソールの**[Main Menu]**で、**[System Configuration]** > **[Reboot Operating System]**を選択します。

   再起動すると、新たに追加したネットワーク インターフェイスがメンテナンス コンソールで検出されます。

2. メンテナンス コンソールにアクセスします。
3. **[Network Configuration]** > **[Enable Network Interface]**を選択します。
4. 新しいネットワーク インターフェイスを選択し、**Enter**キーを押します。

   例

   [eth1]を選択し、**Enter**キーを押します。

5. **「y」**を入力してネットワーク インターフェイスを有効にします。
6. ネットワークの設定を入力します。

   静的インターフェイスを使用している場合、またはDHCPが検出されない場合は、ネットワークの設定を入力するよう求められます。

   ネットワークの設定の入力が終了すると、自動的に**[Network Configuration]**メニューに戻ります。

7. **[Commit Changes]**を選択します。

   ネットワーク インターフェイスを追加するには、変更をコミットする必要があります。

関連タスク

*vSphere VM*コンソールを使用したメンテナンス コンソールへのアクセス（31ページ）

Unified Managerデータベース ディレクトリへのディスク スペースの追加

ONTAPシステムから収集された健全性とパフォーマンスのデータは、すべてUnified Managerデータベース ディレクトリに格納されます。状況によっては、データベース ディレクトリのサイズの拡張が必要になることがあります。

たとえば、Unified Managerで多数のクラスタからデータを収集している場合、各クラスタに大量のノードがあると、データベース ディレクトリがいっぱいになることがあります。データベース ディレクトリの容量の90%に達すると警告イベントが生成され、90%に達すると重大イベントが生成されます。

重要：ディレクトリの容量の90%に達すると、クラスタからデータが収集されなくなります。

データ ディレクトリの容量を追加する手順は、Unified ManagerをVMware ESXiサーバ、Red Hat LinuxサーバまたはCentOS Linuxサーバ、Microsoft Windowsサーバのいずれで実行しているかによって異なります。

Linuxホストのデータ ディレクトリへのスペースの追加

Linuxホストを最初にセットアップした時点でUnified Managerをサポートするための十分なディスク スペースを`/opt/netapp/data`に割り当てていなかった場合は、Unified Managerのインストール後に`/opt/netapp/data`ディレクトリのディスク スペースを増やして拡張することができます。

開始する前に

Unified ManagerがインストールされているRed Hat Enterprise LinuxマシンまたはCentOS Linuxマシンへのrootユーザ アクセスが必要です。

タスク概要

データ ディレクトリのサイズを拡張する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するLinuxマシンにrootユーザとしてログインします。
2. Unified Managerサービスと関連するMySQLソフトウェアを次の順序で停止します。

   ```
   service ocieau stop
   service ocie stop
   service mysqld stop
   ```

3. 現在の`/opt/netapp/data`ディレクトリのデータを格納できる十分なディスク スペースがある一時バックアップ フォルダ（例：`/backup-data`）を作成します。
4. 既存の`/opt/netapp/data`ディレクトリの内容と権限の設定をバックアップ データ ディレクトリにコピーします。

   ```
   cp -rp /opt/netapp/data/* /backup-data
   ```

5. SE Linuxが有効になっている場合は、次の手順を実行します。
   a. 既存の`/opt/netapp/data`フォルダにあるフォルダに対するSE Linuxタイプを取得します。

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print
$3}' | head -1`
```

次のような情報が返されます。

```
echo $se_type
mysqld_db_t
```

b. chconコマンドを実行して、バックアップ ディレクトリに対してSE Linuxタイプを設定します。

```
chcon -R --type=mysqld_db_t /backup-data
```

6. /opt/netapp/dataディレクトリの内容を削除します。

```
cd /opt/netapp/data
```

```
rm -rf *
```

7. LVMのコマンドを使用するかディスクを追加して、/opt/netapp/dataディレクトリのサイズを750GB以上に拡張します。

重要： /opt/netapp/dataディレクトリをNFSエクスポートまたはCIFS共有にマウントすることはサポートされていません。

8. /opt/netapp/dataディレクトリの所有者（mysql）とグループ（root）が変更されていないことを確認します。

```
ls -ltr / | grep opt/netapp/data
```

次のような情報が返されます。

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. SE Linuxが有効になっている場合は、/opt/netapp/dataディレクトリのコンテキストがmysqld_db_tに設定されたままであることを確認します。

```
touch /opt/netapp/data/abc
```

```
ls -Z /opt/netapp/data/abc
```

次のような情報が返されます。

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0 /opt/
netapp/data/abc
```

10. 拡張した/opt/netapp/dataディレクトリにbackup-dataの内容をコピーします。

```
cp -rp /backup-data/* /opt/netapp/data/
```

11. MySQLサービスを開始します。

```
service mysqld start
```

12. MySQLサービスが開始されたら、ocieサービスとocieauサービスを次の順序で開始します。

```
service ocie start
```

```
service ocieau start
```

13. すべてのサービスが開始されたら、バックアップ フォルダ/backup-dataを削除します。

```
rm -rf /backup-data
```

VMware仮想マシンのデータ ディスクへのスペースの追加

Unified Managerデータベースのデータ ディスクのスペースを増やす必要がある場合は、インストール後にdisk 3のディスク スペースを増やして容量を追加できます。

開始する前に

- vSphere Clientへのアクセス権が必要です。
- 仮想マシンにスナップショットがローカルに格納されていない必要があります。
- メンテナンス ユーザのクレデンシャルが必要です。

タスク概要

仮想ディスクのサイズを拡張する前に仮想マシンをバックアップすることを推奨します。

手順

1. vSphere Clientで、Unified Manager仮想マシンを選択し、データdisk 3にディスク容量を追加します。詳細については、VMwareのドキュメントを参照してください。
2. vSphere Clientで、Unified Manager仮想マシンを選択し、**[Console]**タブを選択します。
3. コンソール ウィンドウ内をクリックし、ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。
4. **[Main Menu]**で、**[System Configuration]**オプションの番号を入力します。
5. **[System Configuration Menu]**で、**[Increase Data Disk Size]**オプションの番号を入力します。

Microsoft Windowsサーバの論理ドライブへのスペースの追加

Unified Managerデータベースのディスク スペースを増やす必要がある場合は、Unified Managerがインストールされている論理ドライブに容量を追加できます。

開始する前に

Windowsの管理者権限が必要です。

タスク概要

ディスク スペースを追加する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するWindowsサーバに管理者としてログインします。
2. スペースを追加する方法に応じて、該当する手順を実行します。

オプション	説明
物理サーバで、Unified Managerサーバがインストールされている論理ドライブに容量を追加する。	Microsoftの次のトピックの手順に従います。 *Extend a Basic Volume*

オプション	説明
物理サーバで、ハード ディスク ドライブを追加する。	Microsoftの次のトピックの手順に従います。 *Adding Hard Disk Drives*
仮想マシンで、ディスク パーティションのサイズを拡張する。	VMwareの次のトピックの手順に従います。 *Increasing the size of a disk partition*

著作権に関する情報

商標に関する情報

NetApp、NetAppのロゴ、ネットアップの商標一覧のページ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。

http://www.netapp.com/jp/legal/netapptmlist.aspx

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitter アカウントもあります。

本マニュアルの改善についてご提案がある場合は、次のアドレスまでコメントをEメールでお送りください。

ng-gpso-jp-documents@netapp.com

その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。