CA08871-174-01

FUJITSU Storage ETERNUS AX/HX Series
Active IQ® Unified Manager 9.11.1
設定タスクと管理タスクの実行

目次

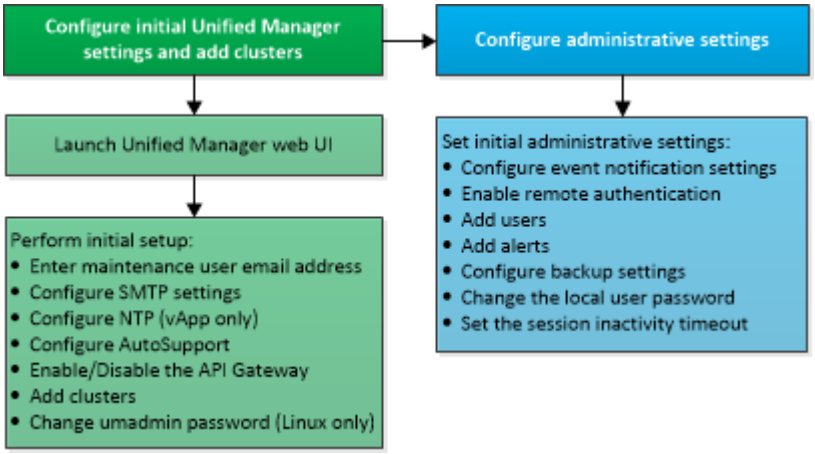
Active IQ Unified Managerの設定

Active IQ Data Center 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、設定タスクと管理タスクの実行、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。

必要なもの

- 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://です。「`https://URL`」

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。

1 時間以内に Web UI へのログインに 3 回連続して失敗すると、システムがロックアウトされ、システム管理者に連絡する必要があります。これはローカルユーザにのみ該当します。

Unified Manager Web UIの初期セットアップの実行

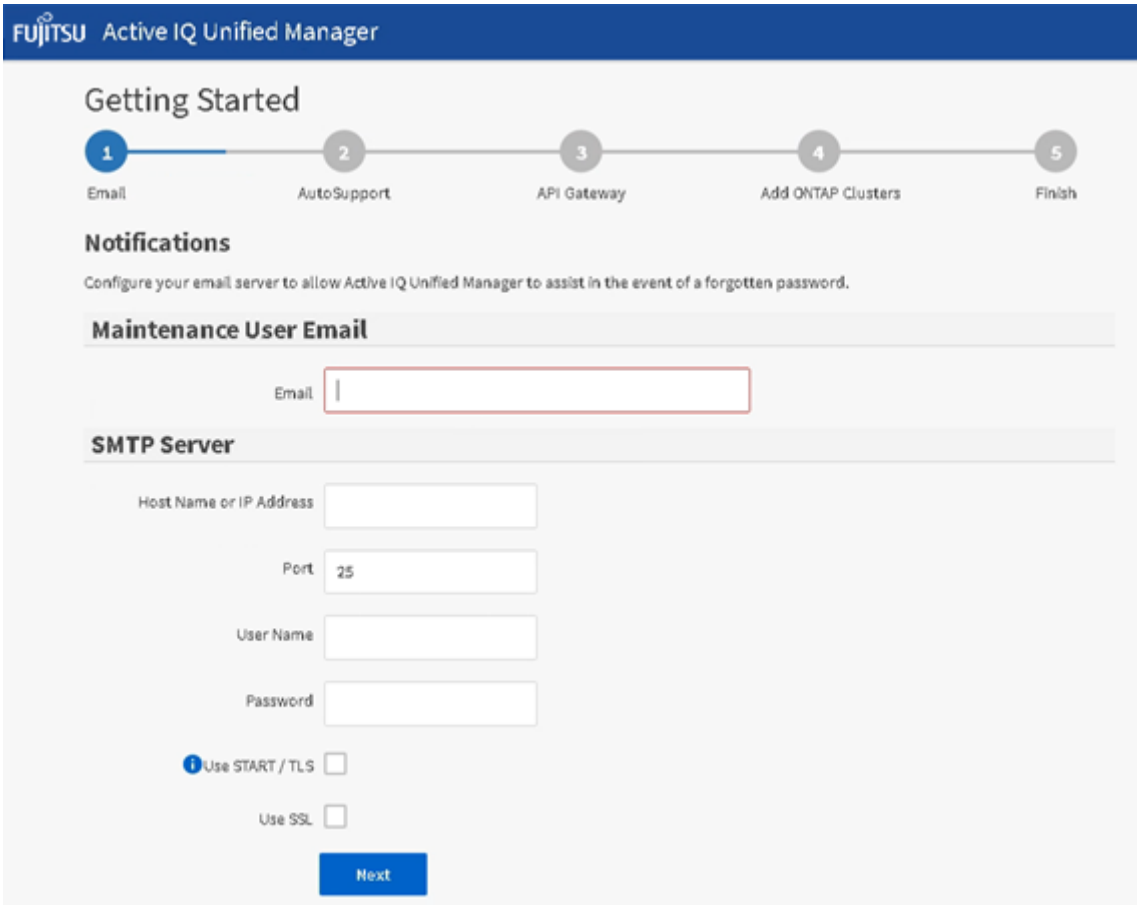
Unified Managerを使用するには、NTPサーバ、メンテナンス ユーザのEメール アドレス、SMTPサーバのホストなどを最初に設定し、ONTAPクラスタを追加する必要があります。

必要なもの

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。

Active IQ Unified Managerの[はじめに]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の左側のナビゲーション ペインの[全般]オプションから選択できます。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。完了したら[続行]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Fujitsu 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のコンテンツをサポートに送信する場合や、AutoSupportを無効にする場合は、Web UIの[全般] > [AutoSupport]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。
4. [APIゲートウェイのセットアップ]ページで、監視対象のONTAPクラスタをUnified ManagerでONTAP REST APIを使用して管理できるようにAPIゲートウェイ機能を使用するかどうかを選択します。完了したら[続行]をクリックします。

   この設定は、 Web UI であとから [一般]>[機能設定]> [API ゲートウェイ] を選択して有効または無効に

できます。APIの詳細については、『Active IQ Unified Manager API開発者ガイド』を参照してください。

5. Unified Managerで管理するクラスタを追加し、[次へ]をクリックします。管理対象の各クラスタについて、ホスト名またはクラスタ管理IPアドレス（IPv4またはIPv6）とユーザ名およびパスワードを入力する必要があります。このユーザにはadminロールが必要です。

   この手順はオプションです。クラスタはWeb UIの[ストレージ管理] > [クラスタ セットアップ]を使用してあとで追加することができます。

6. [サマリ]ページで、すべての設定が正しいことを確認して[終了]をクリックします。

[はじめに]ページが閉じ、Unified Managerのが表示されます。

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。

必要なもの

- 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。
  - 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。

  - クラスタでONTAPバージョン9.7以降が実行されている必要があります。
  - 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。

  - HTTPSプロトコルを使用してクラスタに接続するポート番号（通常はポート443）
  - 必要な証明書を用意しておきます。次の2種類の証明書が必要です。

    サーバ証明書: 登録に使用します。クラスタを追加するには有効な証明書が必要です。サーバ証明書の有効期限が切れた場合は、証明書を再生成する必要があります。その後Unified Managerを再起動すると、サービスが自動で再登録されます。

クライアント証明書認証に使用されます。クラスタを追加するには有効な証明書が必要です。有効期限が切れた証明書でUnified Managerにクラスタを追加することはできません。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。ただし、追加済みのクラスタに対して証明書の有効期限が切れ、その証明書がUnified Managerで使用されている場合、EMSメッセージは引き続き機能します。クライアント証明書を再生成する必要はありません。

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。

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 、 **Storage Management** > **Cluster Setup** の順にクリックします。
2. クラスタセットアップページで 、追加をクリック します。
3. [Add Cluster]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、ポート番号など、必要な値を指定します。

   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. [Submit]をクリックします。
5. [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。
6. [Yes]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。

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）。

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。

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、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ないかを確認してください。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。

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。

必要なもの

アプリケーション管理者のロールが必要です。

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. イベント通知の設定

   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. リモート認証の有効化

   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. 認証サーバの設定のテスト

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 アクセスの管理

   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. アラートの追加

   通知を送信するEメール　アドレスの追加、通知を受信する設定タスクと管理タスクの実行、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。

必要なもの

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。

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 、 **[全般]** 、 **[通知]** の順にクリックします。
2. [Notifications]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。

必要なもの

アプリケーション管理者のロールが必要です。

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。

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場合、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。

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. 左側のナビゲーションペインで、［全般］ > ［リモート認証］ をクリックします。
2. [リモート認証を有効化]チェックボックスをオンにします。
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 ...	次の情報を入力 ...
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 ◦ Bind Distinguished Name（適切なLDAP表記を使用） • 管理者パスワード • 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[Use Secure Connection]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. [Save]をクリックします。

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。

必要なもの

- アプリケーション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。

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. 左側のナビゲーションペインで、［全般］ > ［リモート認証］ をクリックします。
2. [ネストされたグループの検索を無効化]チェックボックスをオンにします。
3. [Save]をクリックします。

認証サービスのセットアップ

認証サービスを使用すると、Unified Managerへのアクセスを許可する前に、リモートユーザまたはリモート　グループを認証サーバで認証できます。事前定義された認証サービス（Active DirectoryやOpenLDAPなど）を使用するか、または独自の認証メカニズムを設定してユーザを認証できます。

必要なもの

- リモート認証を有効にしておく必要があります。
- アプリケーション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、［全般］ > ［リモート認証］ をクリックします。
2. 次のいずれかの認証サービスを選択します。

選択内容	こうする
Active Directory	a. 管理者の名前とパスワードを入力します。 b. 認証サーバのベース識別名を指定します。 たとえば、認証サーバのドメイン名がou@domain.comである場合のベース識別名は、cn=ou,dc=domain,dc=comです。
OpenLDAP	a. バインド識別名とバインド　パスワードを入力します。 b. 認証サーバのベース識別名を指定します。 たとえば、認証サーバのドメイン名がou@domain.comである場合のベース識別名は、cn=ou,dc=domain,dc=comです。

選択内容	こうする
その他	a. バインド識別名とバインド　パスワードを入力します。 b. 認証サーバのベース識別名を指定します。 たとえば、認証サーバのドメイン名がou@domain.comである場合のベース識別名は、cn=ou,dc=domain,dc=comです。 c. 認証サーバでサポートされているLDAPプロトコルのバージョンを指定します。 d. ユーザ名、グループ　メンバーシップ、ユーザ グループ、およびメンバーの属性を入力します。

認証サービスを変更する場合は、既存の認証サーバを削除してから新しい認証サーバを追加する必要があります。

3. [Save]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。

必要なもの

- 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。
- アプリケーション管理者のロールが必要です。

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. 左側のナビゲーションペインで、［全般］ > ［リモート認証］ をクリックします。

2. [セキュアな接続を使用]オプションを有効または無効にします。

実行する処理	こうする
有効にする	a. [セキュアな接続を使用]オプションをオンにします。 b. [Authentication Servers] 領域で、 [Add]をクリックします。 c. Add Authentication Server ダイアログボックスで、サーバの認証名または IP アドレス（IPv4 または IPv6）を入力します。 d. [ホストの認証] ダイアログボックスで、 [証明書の表示] をクリックします。 e. 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. [ホストの許可] ダイアログボックスで、 [はい] をクリックします。 [セキュアな接続を使用]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。

実行する処理	こうする
無効にする	a. [セキュアな接続を使用]オプションをオフにします。 b. [Authentication Servers] 領域で、**[Add]** 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。

3. 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。

必要なもの

- リモート ユーザまたはリモート グループをUnified Manager server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。
- アプリケーション管理者のロールが必要です。

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. 左側のナビゲーションペインで、［全般］ > ［リモート認証］ をクリックします。
2. [Test Connection]をクリックします。
3. [テストユーザー] ダイアログボックスで、リモートユーザーのユーザー名とパスワード、またはリモートグループのユーザー名を指定し、 [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。

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。

必要なもの

- 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、[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。
  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。

アラートは、ここで説明するように、 Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

手順

1. 左側のナビゲーションペインで、**Storage Management** > **Alert Setup** の順にクリックします。
2. [Alert Setup] ページで、**[Add]** 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、アラートの名前と概要を入力します。
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。

   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。

   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. [Save]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。

- アラート名ヘルステスト
- 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

[Add Alert] ダイアログボックスで、次の手順を実行します。

手順

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. **<<Available　Resources**　領域で「**abc**」という名前のボリューム**>>**　をすべて選択し、　Selected Resources 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「*」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. [Matching Events] 領域から [All Critical Events] を選択し、 [Selected Events] 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「xyz」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. [Select Script to Execute]メニューで、[Test]スクリプトを選択します。

8. [Save]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。

必要なもの

ローカル ユーザとしてログインする必要があります。

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メンテナンス コンソールの使用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. Change Password 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. [Save]をクリックします。

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。

アクティブでないセッションのタイムアウト設定

Unified　Managerに非アクティブ時のタイムアウト値を指定して、一定の時間が経過したらセッションを自動的に終了するように設定できます。デフォルトでは、タイムアウトは4,320分（72時間）に設定されています。

必要なもの

アプリケーション管理者のロールが必要です。

この設定は、ログインしているすべてのユーザ セッションに適用されます。

> このオプションは、Security Assertion Markup Language（SAML）認証を有効にしている場合は使用できません。

手順

1. 左側のナビゲーションペインで 、 [一般]>[機能設定] をクリックします。

2. [機能設定]ページで、次のいずれかを実行して非アクティブ時のタイムアウトを指定します。

実行する処理	操作
タイムアウトを設定しない（セッションを自動的に閉じない）	[非アクティブ時のタイムアウト]パネルで、スライダ ボタンを左（オフ）に動かして[適用]をクリックします。
タイムアウト値（分）を設定する	[非アクティブ時のタイムアウト]パネルで、スライダ ボタンを右（オン）に動かし、非アクティブ時のタイムアウト値（分）を指定して[適用]をクリックします。

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。

必要なもの

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、アプリケーション管理者ロールが割り当てられている必要があります。

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の生成

   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仮想マシンの再起動

   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

Active IQ Unified Managerを初めてインストールすると、デフォルトのHTTPS証明書がインストールされます。新しいHTTPSセキュリティ証明書を生成して、既存の証明書を置き換えることができます。

必要なもの

アプリケーション管理者のロールが必要です。

証明書を再生成する理由はいくつもあります。たとえば、識別名（DN）をより適切な値に変更する場合、キーのサイズを大きくする場合、有効期限を延長する場合、現在の証明書の有効期限が切れた場合などです。

Unified Manager Web UIにアクセスできない場合は、を使用して同じ値でHTTPS証明書を再生成できます。証明書を再生成する際に、キーのサイズと有効期間を定義できます。メンテナンス　コンソールの[Reset Server Certificate]オプションを使用した場合、新しいHTTPS証明書の有効期間は397日間に設定されます。また、RSAキーのサイズは2048ビットに設定されます。

手順

1. 左側のナビゲーションペインで 、**General** > **HTTPS Certificate** の順にクリックします。

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。

実行する処理	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。

実行する処理	操作
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。共通名はホストのFQDNに設定する必要があります。それ以外のフィールドの値は必須ではありませんが、必要に応じて[E　メール]、[会社]、[部門]、[市町村]、[都道府県]、[国]などの値を入力し、証明書に表示することができます。[キー　サイズ]（キー　アルゴリズムはRSA）と[有効期間]も選択できます。 • キー　サイズに指定できる値は、　2048、3072、 4096 です。 • 有効期間は1日～36500日です。 ただし、推奨される有効期間は397日（13カ月）以内です。397日を超える有効期間を選択しても、CSRをエクスポートして既知のCAから署名を受ける場合にCAからは有効期間が397日に削減され署名済み証明書が返されます。 • 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。

HTTPS証明書を表示して新しい証明書の情報を確認します。

Unified Manager仮想マシンの再起動

仮想マシンは、Unified　Managerの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。

必要なもの

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。

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。

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 Unified Managerサーバを識別しやすくなります。

必要なもの

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。

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. 次のコマンドを入力して、Data Center 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。

   ```
   systemctl stop ocieau ocie mysqld
   ```

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
   ```

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

4. サーバのHTTPS証明書を再生成します。

   ```
   /opt/fujitsu/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
   ```

   ```
   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、次のコマンドを入力してData Center Managerを再起動します。

   ```
   systemctl start mysqld ocie ocieau
   ```

ポリシーベースのストレージ管理の有効化 / 無効化

Unified Manager 9.7以降では、ONTAPクラスタにストレージ ワークロード（ボリュームとLUN）をプロビジョニングし、割り当てられたパフォーマンス サービス レベルに基づいてワークロードを管理できます。この機能はONTAP System Managerでワークロードを作成してQoSポリシーを適用する処理に相当しますが、Unified Managerを使用して適用した場合は、Unified Managerインスタンスで監視しているすべてのクラスタのワークロードをプロビジョニングおよび管理できます。

アプリケーション管理者のロールが必要です。

このオプションはデフォルトで有効になっていますが、Unified Managerを使用してワークロードをプロビ

ジョニングおよび管理しない場合は無効にできます。

このオプションを有効にすると、ユーザ インターフェイスに新しい項目がいくつか追加されます。

新しいコンテンツ	場所
新しいワークロードのプロビジョニング ページ	［ 共通タスク ］ >［ プロビジョニング ］ から使用できます
パフォーマンス サービス レベル ポリシーの作成ページ	設定 > ポリシー > パフォーマンスサービスレベルから選択できます
パフォーマンス ストレージ効率ポリシーの作成ページ	**[**設定] > **[**ポリシー**]** > **[**ストレージ効率化**]** から選択できます
現在のワークロード パフォーマンスとワークロードIOPSを表示するパネル	ダッシュボードで確認できます

これらのページおよびこの機能の詳細については、製品のオンライン ヘルプ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 、[一般]>[機能設定] をクリックします。
2. [機能設定]ページで、次のいずれかを実行してポリシーベースのストレージ管理を有効または無効にします。

実行する処理	こうする
ポリシーベースのストレージ管理を無効にする	[ポリシーベースのストレージ管理]パネルで、スライダ ボタンを左に動かします。
ポリシーベースのストレージ管理を有効にする	[ポリシーベースのストレージ管理]パネルで、スライダ ボタンを右に動かします。

Unified Managerのバックアップの設定

Unified　Managerのバックアップ機能を設定するには、ホスト　システムのメンテナンス コンソールで一連の設定手順を実行します。

設定手順については、Active IQ Unified Manager 9.11.1 クラスタ ヘルスの監視および管理のバックアップおよびリストア処理の管理を参照してください。

機能設定の管理

[機能設定] ページでは、 Active IQ Unified Manager の特定の機能を有効または無効にできます。ポリシーに基づいたストレージオブジェクトの作成と管理、 API ゲートウェイとログインバナーの有効化、アラート管理用スクリプトのアップロード、非アクティブ時間に基づく Web UI セッションのタイムアウト、 Active IQ プラットフォームイベントの受信停止などが含まれます。

[機能の設定] ページは、アプリケーション管理者ロールを持つユーザーのみが使用できます。

スクリプトアップロードについては、リンクスクリプトアップロードの有効化 / 無効化を参照してください。

ポリシーベースのストレージ管理の有効化

[ポリシーベースのストレージ管理]オプションを使用すると、サービス　レベル目標（SLO）に基づいてストレージを管理できます。このオプションはデフォルトで有効になっています。

この機能をアクティブ化すると、Active IQ Unified Managerインスタンスに追加されるONTAPクラスタのストレージ　ワークロードをプロビジョニングし、割り当てられたとに基づいてワークロードを管理できます。

この機能をアクティブ化または非アクティブ化するには、 General > Feature Settings > Policy-Based Storage Management　を選択します。この機能をアクティブ化すると、次のページを使用して操作と監視を行うことができます。

- [プロビジョニング]ページ（ストレージ ワークロードのプロビジョニング）
- ポリシー > パフォーマンスサービスレベル
- [ポリシー] >[ストレージ効率化]の順にクリックします
- [クラスタ セットアップ]ページの[パフォーマンス サービス レベルで管理されるワークロード]列
- [ダッシュボード]の[ワークロード パフォーマンス]パネル

画面を使用して、パフォーマンスサービスレベルとストレージ効率化ポリシーを作成したり、ストレージ ワークロードをプロビジョニングしたりできます。また、割り当てられたに準拠したストレージ ワークロードと準拠しないストレージ ワークロードを監視することもできます。さらに、[ワークロード パフォーマンス] / [ワークロードIOPS]パネルで、プロビジョニングされたストレージ ワークロードに基づいて、デ

ータセンター内のクラスタの合計容量、使用可能容量、使用済み容量、およびパフォーマンス（IOPS）を評価することもできます。

この機能をアクティブ化したら、 Unified Manager REST API を実行して、メニューバー > ヘルプボタン> API ドキュメント > ストレージプロバイダカテゴリからこれらの機能の一部を実行できます。また、ホスト名またはIPアドレスとURLを+の形式で入力してREST APIページにアクセスすることもできます。

API ゲートウェイの有効化

APIゲートウェイ機能を使用すると、それぞれのONTAPクラスタに個別にログインしなくても、単一のコントロール　プレーンであるActive　IQ　Unified　Managerから複数のONTAPクラスタを一元的に管理できます。

この機能は、Unified　Managerに最初にログインしたときに表示される設定ページから有効にできます。または、 **General** > **Feature Settings** > API Gateway からこの機能を有効または無効にすることもできます。

Unified Manager REST APIとONTAP REST APIは別のものであり、Unified Manager REST APIを使用してONTAP REST APIのすべての機能を利用できるわけではありません。ただし、Unified Managerでは提供されていない特定の機能を管理するためにONTAP　APIにアクセスする必要がある場合は、APIゲートウェイ機能を有効にしてONTAP　APIを実行できます。ゲートウェイは、ヘッダーと本文の形式をONTAP　APIと同じにすることで、API要求をトンネリングするプロキシとして機能します。Unified Managerのクレデンシャルを使用して特定のAPIを実行することで、個々のクラスタのクレデンシャルを渡すことなくONTAPクラスタにアクセスして管理することができます。UnifiedManagerは単一の管理ポイントとして機能し、個々のUnified Managerインスタンスで管理されるONTAPクラスタに対してまとめてAPIを実行することができます。APIから返される応答は、対応するONTAP REST APIをONTAPから直接実行した場合と同じです。

この機能を有効にすると、メニュー　バー[ヘルプ]ボタン[APIドキュメント]　>　[gateway]カテゴリからUnified　Manager　REST　APIを実行できます。また、ホスト名またはIPアドレスとURLを `https://<hostname>/docs/api/` の形式で入力してREST APIページにアクセスすることもできます。

非アクティブ時のタイムアウトの指定

Active IQ Unified Managerに対して非アクティブ時のタイムアウト値を指定できます。操作がない状態で指定した時間が経過すると、アプリケーションから自動的にログアウトされます。このオプションはデフォルトで有効になっています。

この機能を非アクティブ化するか、 [一般（General）]>[フィーチャー設定（Feature Settings）]>[非アクティブタイムアウト（Inactivity Timeout）] から時間を変更できますこの機能をアクティブにした場合、操作

がない場合に自動的にログアウトするまでの時間（分）を[ログアウトまでの時間]フィールドで指定します。デフォルト値は分（72時間）です。

このオプションは、Security Assertion Markup Language（SAML）認証を有効にしている場合は使用できません。

Active IQ ポータル イベントの有効化

Active IQポータル イベントを有効にするか無効にするかを指定できます。有効にすると、Active IQポータルでシステム構成やケーブル配線などに関する追加のイベントが検出されて表示されます。このオプションはデフォルトで有効になっています。

この機能を有効にすると、Active IQポータルで検出されたイベントがActive IQ Unified Managerに表示されます。イベントはすべての監視対象ストレージ システムから生成されたAutoSupportメッセージに対して一連のルールを実行することによって作成されます。これらのイベントは、Unified Managerの他のイベントと違い、システム構成、ケーブル配線、ベストプラクティス、および可用性の問題に関連するインシデントやリスクを特定します。

この機能は、[全般] > [機能設定] > [Active IQポータル イベント]からアクティブ化または非アクティブ化できます。外部ネットワークへのアクセスがないサイトでは、[ストレージ管理] > [イベント セットアップ] > [ルールをアップロード]からルールを手動でアップロードする必要があります。

この機能はデフォルトで有効になっています。この機能を無効にすると、Active IQイベントがUnified Managerで検出または表示されなくなります。この機能を無効にしたあとに有効にした場合、Unified Managerは、クラスタに対するActive IQイベントを00:15（クラスタのタイムゾーン）に受信します。

準拠のためのセキュリティ設定の有効化と無効化

Features Settings ページの Security Dashboard パネルにある Customize ボタンを使用して、 Unified Manager で準拠監視のセキュリティパラメータを有効または無効にできます。

このページで有効または無効になる設定によって、 Unified Manager でのクラスタと Storage VM の全体的な準拠ステータスが制御されます。選択し **: All Clusters** view of the Clusters inventory page and the **Security:** た項目に基づいて、対応する列が Storage VM インベントリページの Security All Storage VM ビューに表示されます。

これらの設定を編集できるのは、管理者ロールのユーザだけです。

ONTAP クラスタ、Storage VM、およびボリュームのセキュリティ条件は、ONTAP 9 セキュリティ設定ガイドに定義されている推奨事項に照らして評価されます。ダッシュボードおよびセキュリティページのセキュリティパネルには、クラスタ、 Storage VM 、およびボリュームのデフォルトのセキュリティコンプライアンスステータスが表示されます。また、セキュリティイベントが生成され、セキュリティ違反があるクラスタと Storage VM に対して有効になる管理操作も実行されます。

セキュリティ設定のカスタマイズ

ONTAP 環境に応じて準拠監視の設定をカスタマイズするには、次の手順を実行します。

手順

1. **[一般]>[機能設定]>[セキュリティダッシュボード]>[カスタマイズ]**の順にクリックします。**Customize Security Dashboard Settings** （セキュリティダッシュボード設定のカスタマイズ）ポップアップが表示されます。

   有効または無効にしたセキュリティコンプライアンスパラメータは、クラスタおよび Storage VM 画面のデフォルトのセキュリティビュー、レポート、およびスケジュールされたレポートに直接影響します。セキュリティパラメータを変更する前に、これらの画面から Excel レポートをアップロードした場合、ダウンロードした Excel レポートに問題がある可能性があります。

2. ONTAPクラスタのカスタム設定を有効または無効にするには、クラスタで必要な一般設定を選択します。クラスタコンプライアンスをカスタマイズするためのオプションについては、Active IQ Unified Manager 9.11.1 クラスタ ヘルスの監視および管理を参照してください
3. Storage VM のカスタム設定を有効または無効にするには、 Storage VM で必要な一般設定を選択します。StorageVMコンプライアンスをカスタマイズActive IQ Unified Manager 9.11.1クラスタ ヘルスの監視および管理を参照してください。

AutoSupport および認証設定のカスタマイズ

AutoSupport 設定 セクションでは、 ONTAP からの AutoSupport メッセージの送信に HTTPS 転送を使用するかどうかを指定できます。

認証設定 セクションでは、デフォルトの ONTAP 管理者ユーザに対して Unified Manager のアラートを生成するように設定できます。

スクリプトアップロードの有効化 / 無効化

スクリプトをUnified　Managerにアップロードして実行する機能は、デフォルトで有効になっています。セキュリティ上の理由からこの操作を禁止したい場合は、この機能を無効にすることができます。

必要なもの

アプリケーション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 、[一般]>[機能設定] をクリックします。
2. [機能設定]ページで、次のいずれかを実行してスクリプトを無効または有効にします。

実行する処理	こうする
スクリプトを無効にする	[スクリプト　アップロード]パネルで、スライダボタンを左に動かします。
スクリプトを有効にする	[スクリプト　アップロード]パネルで、スライダボタンを右に動かします。

ログインバナーを追加しています

ログインバナーを追加すると、システムへのアクセスを許可されているユーザ、ログインおよびログアウト時の使用条件などの情報を組織で表示できます。

このログインバナーのポップアップは、ストレージオペレータや管理者など、ログイン、ログアウト、セッションタイムアウトの際に表示されます。

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。

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
- 富士通の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

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でアプリケーション管理者のロールを割り当てられ、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。

診断ユーザの権限

診断アクセスの目的は、富士通の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、富士通の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、富士通の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。

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。

必要なもの

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

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。

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	これらの手順に従ってください
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	これらの手順に従ってください
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。

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

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。

必要なもの

- maintenance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。

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。

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。

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。

- IPアドレス設定の表示

  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）。

- IPアドレス設定の変更

  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。

- 静的ルートの表示

  現在の静的ネットワーク ルートが表示されます。

- 静的ルートの変更

  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。

  - 戻る

    [Main Menu]に戻ります。

  - 終了

    メンテナンス コンソールを終了します。

- ネットワーク インターフェイスの無効化

  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。

- 変更内容のコミット

  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。

- ホストへのpingの実行

  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。

- 背面

  [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）。

LinuxまたはMicrosoft Windowsシステムに Unified Managerをインストールしている場合、このメニューにはRestore from a Unified Manager Backupオプションのみが表示されます。

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、富士通の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。

- **<logged in user>** ユーザパスワードを変更します

  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。

- タイム ゾーンの変更

  タイムゾーンを現在の場所に変更します。

- NTPサーバの変更

  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）。

- NTPサービスの変更

  `ntp` と `systemd-timesyncd` サービスを切り替えます。

- 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。

- 背面

  [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、トラブルシューティングのサポートを受ける際に富士通のサポートに送信するサポート バンドルを生成できます。

表示されるメニュー オプションは次のとおりです。

- Generate Light Support Bundle

  30日分のログと構成データベース レコードのみを含む軽量なサポート バンドル（パフォーマンス データ、取得記録ファイル、サーバ ヒープ ダンプは含まれません）を作成できます。

- サポート バンドルの生成

  ユーザのホーム ディレクトリに、診断情報を含む完全なサポート バンドル（7-Zipファイル）を作成できます。システムがインターネットに接続されている場合は、サポート バンドルを富士通にアップロードすることもできます。

  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メッセージや軽量なサポート バンドル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 の GUI で サーバ証明書を再生成するには、 General > HTTPS Certificates > Regenerate HTTPS Certificate をクリックします。

- SAML 認証の無効化

  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の現在の接続設定と構成設定を表示します
  - サーバー接続の追加　/　変更：部データプロバイダの新しい接続設定を入力したり、既存の設定を変更したりできます。
  - Modify Server Configuration：外部データプロバイダの新しい設定を入力したり ' 既存の設定を変更したりできます
  - サーバー接続の削除-- 外部データプロバイダへ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。

- View/Change Application Ports

  Data Center 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。

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。

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。

必要なもの

- 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。

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。

必要なもの

Unified Managerサーバの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。

> 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。

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。

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 メンテナンスコンソールの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。

この変更が完了したら、Unified　Manager　Web　UI　にアクセスするために、ユーザは新しいポート番号をURLに追加する必要があります。たとえば、https://host.company.com:1234、https://2001:db8:0:1:2123、https://12.13.14.15:1122のようになります。

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。

必要なもの

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。

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 コンソールのメインメニューで 、 **System Configuration** > **Reboot Operating System** の順に選択 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。

   [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。

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常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95%に達すると警告イベントが生成され、95%に達すると重大イベントが生成されます。

ディレクトリの容量の95%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/fujitsu/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。

必要なもの

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。

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。

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 現在の /opt/fujitsu/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/fujitsu/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 -arp /opt/fujitsu/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/fujitsu/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/Fujitsu/data | awk{print $4} | 'awk -F ：{print $3} | " 頭部 -1`

      次のような情報が返されます。

```
echo $se_type
mysqld_db_t
```

b. 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/fujitsu/data ディレクトリの内容を削除します。
   a. cd /opt/fujitsu/data
   b. 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/fujitsu/data ディレクトリのサイズを150GB以上に拡張します。

ディスクから /opt/fujitsu/data を作成した場合は、 /opt/fujitsu/data をNFS共有またはCIFS共有としてマウントしないでください。マウントした場合、ディスク スペースを拡張しようとしたときに一部のLVMコマンド（resizeやextendなど）が想定どおりに機能しないことがあります。

8. /opt/fujitsu/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 /opt/fujitsu/ | grep 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/fujitsu/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。
   a. touch /opt/fujitsu/data/abc
   b. ls -Z /opt/fujitsu/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/fujitsu/data/abc
```

10. ファイルを削除して、この無駄なファイルがデータベース エラーの原因にならないようにします。
11. 拡張したディレクトリに /opt/fujitsu/data の内容をコピーします。

    cp -arp /backup-data/* /opt/fujitsu/data/

12. SE Linuxが有効になっている場合は、次のコマンドを実行します。

```
chcon -R --type=mysqld_db_t /opt/fujitsu/data
```

13. MySQLサービスを開始します。

    ```
    systemctl start mysqld
    ```

14. 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。

    ```
    systemctl start ocie ocieau
    ```

15. 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Unified　Managerメンテナンス　コンソールを使用して容量を追加できます。

必要なもの

- 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。

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。

   まれに、Unified　Manager環境のデータ　ディスクにハードディスク3ではなくハードディスク2が使用されていることがあります。その場合は、大きい方のディスクのスペースを増やしてください。データ ディスクのスペースは、常に他のディスクより大きくなります。

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。

必要なもの

Windowsの管理者権限が必要です。

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。

Option	概要の順にクリックします
物理サーバで、Unified Manager server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
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

ユーザ アクセスの管理

選択したクラスタ オブジェクトへのユーザ アクセスを制御するために、ロールを作成し、機能を割り当てることができます。クラスタ内の選択したオブジェクトにアクセスするために必要な権限を持つユーザを特定できます。このようなユーザにのみ、クラスタ オブジェクトを管理するためのアクセス権が与えられます。

設定タスクと管理タスクの実行

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。

必要なもの

- アプリケーション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。

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. 左側のナビゲーションペインで 、 **[**全般]>[ユーザー] をクリックします。
2. [ユーザー] ページで 、 **[**追加] をクリックします。
3. [Add User]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。

データベース ユーザの作成

Workflow AutomationとUnified Managerの間の接続をサポートする場合や、データベース ビューにアクセスする場合は、まずUnified Manager Web UIで、統合スキーマ ロールまたはレポート スキーマ ロールを割り当てたデータベース ユーザを作成する必要があります。

必要なもの

アプリケーション管理者のロールが必要です。

データベース ユーザは、Workflow Automationとの統合およびレポート固有のデータベース ビューへのアクセスを行えます。データベース ユーザは、Unified Manager Web UIやメンテナンス コンソールにはアクセスできず、API呼び出しも実行できません。

手順

1. 左側のナビゲーションペインで 、 [全般]>[ユーザー] をクリックします。
2. [ユーザ]ペインで、[追加]をクリックします。
3. [ユーザーの追加] ダイアログボックスの [タイプ] ドロップダウンリストで [データベースユーザー] を選択します。
4. データベース ユーザの名前とパスワードを入力します。
5. [ロール]ドロップダウン リストで適切なロールを選択します。

現在のロール	選択してください
Unified ManagerをWorkflow Automationに接続する場合	統合スキーマ
レポートおよびその他のデータベース ビューにアクセスする場合	レポート スキーマ

6. [追加]をクリックします。

ユーザの設定の編集

各ユーザを指定する E メールアドレスやロールなどのユーザ設定を編集することがで

きます。たとえば、ストレージ オペレータのユーザのロールを変更して、そのユーザにストレージ管理者の権限を割り当てることができます。

必要なもの

アプリケーション管理者のロールが必要です。

ユーザに割り当てられているロールを変更した場合、次のいずれかの時点で変更内容が反映されます。

- ユーザがUnified Managerからログアウトして再度ログインしたとき
- セッションの開始から24時間が経過してタイムアウトしたとき

手順

1. 左側のナビゲーションペインで、 [全般]>[ユーザー]をクリックします。
2. [ユーザー]ページで、設定を編集するユーザを選択し、[編集]をクリックします。
3. [ユーザーの編集] ダイアログボックスで、ユーザーに指定されている適切な設定を編集します。
4. [Save]をクリックします。

ユーザの表示

では、Unified　Managerを使用してストレージ　オブジェクトとデータを管理するユーザのリストを表示できます。ユーザに関する詳細（ユーザ名、ユーザのタイプ、Eメール アドレス、ユーザに割り当てられているロールなど）を参照できます。

必要なもの

アプリケーション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 、 **[**全般]>[ユーザー] をクリックします。

ユーザまたはグループの削除

管理サーバ　　データベースから1人または複数のユーザを削除して、それらのユーザがUnified　Managerにアクセスできないようにすることができます。また、グループを削除すると、そのグループのすべてのユーザによる管理サーバへのアクセスを禁止できます。

必要なもの

- リモート　グループを削除するときは、リモート　グループのユーザに割り当てられているイベントを再割り当てしておく必要があります。

ローカル ユーザまたはリモート ユーザを削除する場合は、それらのユーザに割り当てられていたイベントの割り当てが自動的に解除されます。

- アプリケーション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、 [全般]>[ユーザー]をクリックします。
2. [ユーザー] ページで、削除するユーザーまたはグループを選択し、 [削除] をクリックします。
3. [はい]をクリックして削除を確定します。

RBACとは

Role-Based Access Control（RBAC;ロールベース アクセス制御）を使用すると、IQ ManagerサーバOnCommand Unified Managerサーバのさまざまな機能およびリソースにアクセスするユーザを制御できます。

ロールベース アクセス制御の機能

管理者は、ロールベース アクセス制御（RBAC）を使用してロールを定義することにより、ユーザのグループを管理できます。特定の機能のアクセスを選択した管理者に制限する必要がある場合は、その管理者用の管理者アカウントを設定してください。その管理者が表示できる情報と、実行できる処理を制限する場合は、作成した管理者アカウントにロールを適用する必要があります。

管理サーバでは、ユーザ ログインとロールの権限に対してRBACを使用します。管理サーバで管理ユーザアクセスのデフォルト設定を変更していない場合は、ログインして設定を表示する必要はありません。

特定の権限を必要とする処理を開始すると、管理サーバによってログインを求められます。 たとえば、管理者アカウントを作成するには、アプリケーション管理者アカウントのアクセス権でログインする必要があります。

ユーザ タイプの定義

ユーザは、アカウントの種類に基づいて、リモート ユーザ、リモート グループ、ローカル ユーザ、データベース ユーザ、およびメンテナンス ユーザの各タイプに分類されます。それぞれのタイプには、管理者ロールを持つユーザによって独自のロールが割り当てられます。

Unified Managerには次のユーザ タイプがあります。

- メンテナンス ユーザ

  Unified Managerの初期設定時に作成されます。メンテナンス ユーザは、他のユーザを作成してロールを割り当てます。メンテナンスコンソールにアクセスできる唯一のユーザでもあります。Unified ManagerをRed Hat Enterprise LinuxまたはCentOSシステムにインストールしている場合は、メンテナンス ユーザのユーザ名はumadminです。

- ローカル ユーザ

  Unified Manager UIにアクセスし、メンテナンス ユーザまたはOnCommand管理者ロールを持つユーザから割り当てられたロールに基づいて操作を実行します。

- リモート グループ

  認証サーバに保存されているクレデンシャルを使用してUnified Manager UIにアクセスするユーザのグループです。このグループの名前は、認証サーバに保存されているグループの名前と同じにする必要があります。リモート グループのユーザは、各自のユーザ クレデンシャルを使用してUnified Manager UIにアクセスできます。リモート グループに割り当てられたロールに基づいて操作を実行できます。

- リモート ユーザ

  認証サーバに保存されているクレデンシャルを使用してUnified Manager UIにアクセスします。リモート ユーザは、メンテナンス ユーザまたはアプリケーション管理者ロールを持つユーザから割り当てられたロールに基づいて操作を実行します。

- データベース ユーザ

  Unified Managerデータベースのデータへの読み取り専用アクセスが許可されます。Unified ManagerのWebインターフェイスやメンテナンス コンソールにはアクセスできず、API呼び出しも実行できません。

ユーザ ロールの定義

メンテナンス ユーザまたはアプリケーション管理者が、各ユーザにロールを割り当てます。ロールにはそれぞれ特定の権限が含まれています。Unified Managerで実行できる操作の範囲は、割り当てられたロールとその権限で決まります。

Unified Managerには、事前定義された次のユーザ ロールが用意されています。

- オペレータ

ストレージ　システムの情報やUnified　Managerで収集されたその他のデータ（履歴や容量の使用状況など）を参照できます。このロールを割り当てられたストレージ　オペレータは、イベントについて、表示、割り当て、応答、解決、メモの追加などの操作が可能です。

- ストレージ管理者

  Unified　Managerでのストレージ管理処理の設定を行います。このロールを割り当てられたストレージ管理者は、しきい値の設定、およびアラートなどのストレージ管理用のオプションやポリシーの作成が可能です。

- アプリケーション管理者

  ストレージ管理以外の設定を行います。ユーザ、セキュリティ証明書、データベース　アクセスのほか、認証、SMTP、ネットワーク、AutoSupportなどの管理オプションの設定が可能です。

  Unified ManagerをLinuxシステムにインストールした場合は、OnCommand管理者ロールが割り当てられた最初のユーザに自動的にumadminという名前が付けられます。

- 統合スキーマ

  Unified ManagerとOnCommand Workflow Automation（WFA）の統合用にUnified Managerのデータベースビューにアクセスするための読み取り専用アクセスが許可されます。

- レポート スキーマ

  レポートおよびその他のデータベース ビューにUnified Managerデータベースから直接アクセスするための読み取り専用アクセスが許可されます。表示できるデータベースは次のとおりです。

  - fujitsu_model_view
  - fujitsu_performance
  - OCUM
  - ocum_report
  - ocum_report_birt
  - OPM
  - scalemonitor

設定タスクと管理タスクの実行

Unified　Managerで実行できる操作は、割り当てられているユーザ　ロールに基づいて決まります。

次の表に、各ユーザ ロールで実行できる機能を示します。

機能	オペレータ	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
ストレージ　システムの情報の表示	•	•	•	•	•
その他のデータ（履歴や容量の使用状況）の表示	•	•	•	•	•
イベントの表示、割り当て、解決	•	•	•		
ストレージ　サービス　オブジェクト（SVMの関連付けやリソース　プールなど）の表示	•	•	•		
しきい値ポリシーの表示	•	•	•		
ストレージ　サービス　オブジェクト（SVMの関連付けやリソース　プールなど）の管理		•	•		
アラートの定義		•	•		

機能	オペレータ	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
ストレージ管理オプションの管理		•	•		
ストレージ管理ポリシーの管理		•	•		
ユーザの管理			•		
管理オプションの管理			•		
しきい値ポリシーの定義			•		
データベースアクセスの管理			•		
WFAとの統合の管理とデータベース　ビューへのアクセス				•	
レポートのスケジュール設定と保存		•	•		
“[管理”　アクション]　から　[修正]　操作を実行します		•	•		

機能	オペレータ	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
データベースビューへの読み取り専用アクセスの提供					•

SAML認証の設定の管理

Unified Managerシステムでリモート認証を設定したあと、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またはAES-256
- Secure Hash Algorithm （SHA）：SHA-1 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。

請求規則	値
SAM-account-name	Name ID

請求規則	値
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。設定しないと、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。
  a. ADFS管理コンソールを開きます。
  b. 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。
  c. 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。
  d. [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。

    証明書利用者信頼ごとに失効確認を無効にする方法
  - 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。

SAML認証の有効化

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。

必要なもの

- 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。
- アプリケーション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。

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コマンド、ZAPIにアクセスするユーザには影響しません。

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. 左側のナビゲーションペインで、**General** > **SAML Authentication** の順にクリックします。
2. [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。
3. 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。
4. 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。
5. [Save]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。
6. [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。

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、次回から古いIdPのログイン ページではなく新しいIdPのログイン ページに変わります。

まだ完了していない場合は、IdPにアクセスし、Data Center 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。

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、Data Center Manager GUIでADFSのタイムアウトが考慮されず、Data Center 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。GUI セッションのタイムアウトは、**General** > **Feature Settings** > **Inactivity Timeout** の順にクリックして変更できます。

SAML認証に使用するアイデンティティ プロバイダの変更

Unified Managerでリモート ユーザの認証に使用するアイデンティティ プロバイダ（IdP）を変更することができます。

必要なもの

- IdPのURLとメタデータが必要です。
- IdPへのアクセスが必要です。

新しいIdPの設定は、Unified Managerの設定前にも設定後にも実行できます。

手順

1. 左側のナビゲーションペインで 、**General** > **SAML Authentication** の順にクリックします。
2. 新しい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にUnified Managerサーバから直接アクセスできる場合は、IdPのURL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。
3. Unified Managerのメタデータ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。
4. [設定の保存]をクリックします。

   設定を変更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。
5. [OK]をクリックします。

新しい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。

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、次回から古いIdPのログイン ページではなく新しいIdPのログイン ページに変わります。

Unified Managerセキュリティ証明書変更後のSAML認証設定の更新

Unified　Managerサーバにインストールされ ているHTTPSセキュリティ証明書が変更されたときは、SAML認証の設定を更新する必要があります。証明書が更新されるのは、ホスト　システムの名前を変更した場合、ホスト　システムに新しいIPアドレスを割り当てた場合、システムのセキュリティ証明書を手動で変更した場合です。

セキュリティ証明書が変更されたあとにUnified　Managerサーバが再起動されると、SAML認証は機能せず、ユーザはUnified　Managerのグラフィカル　インターフェイスにアクセスできなくなります。ユーザ　インターフェイスに再びアクセスできるようにするには、IdPサーバとUnified　Managerサーバの両方でSAML認証の設定を更新する必要があります。

手順

1. メンテナンス コンソールにログインします。
2. [Main Menu]で、[Disable SAML authentication]オプションの番号を入力します。

   SAML認証を無効にしてUnified Managerを再起動することの確認を求めるメッセージが表示されます。
3. 更新されたFQDNまたはIPアドレスを使用してUnified　Managerのユーザ　インターフェイスを起動し、更新されたサーバ証明書をブラウザで受け入れ、メンテナンス　ユーザのクレデンシャルを使用してログインします。
4. [セットアップ/認証]ページで、[SAML 認証]タブを選択し、IdP接続を設定します。
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。
6. [Save]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。
8. IdPサーバにアクセスし、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。

アイデンティティプロバイダ	設定手順
ADFS	a. ADFS管理GUIで、既存の証明書利用者信頼エントリを削除します。 b. `saml_sp_metadata.xml` を使用して、更新されたUnified Managerサーバから新しい証明書利用者信頼エントリを追加します。 c. Unified Managerがこの証明書利用者信頼エントリに対するADFS SAML応答を解析するために必要な3つの要求規則を定義します。 d. ADFS Windowsサービスを再開します。
Shibboleth	a. Unified Manager サーバの新しい FQDN をファイル`attribute-filter.xml`と`relying-party.xml`ファイルで更新します。 b. Apache Tomcat Web サーバを再起動し、ポート 8005 がオンラインになるまで待ちます。

9. Unified Manager にログインし、 IdP 経由で SAML 認証が想定どおりに機能することを確認します。

SAML認証の無効化

Unified Manager Web UIにログインするリモート ユーザのセキュアなアイデンティティ プロバイダ（IdP）による認証を中止する場合は、SAML認証を無効にします。SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダによるサインオン認証が行われます。

SAML認証を無効にすると、設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

SAML認証は、グラフィカル ユーザ インターフェイスにアクセスできない場合はを使用して無効にすることもできます。

SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. 左側のナビゲーションペインで 、**General** > **SAML Authentication** の順にクリックします。

2. [SAML認証を有効にする]チェック ボックスを選択解除します。
3. [Save]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。

4. [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。

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IdPのログイン ページではなくUnified Managerのログイン ページに変わります。

IdPにアクセスし、Unified ManagerサーバのURIとメタデータを削除します。

メンテナンス コンソールからのSAML認証の無効化

Unified Manager GUIにアクセスできない場合は、必要に応じてメンテナンス コンソールからSAML認証を無効にすることができます。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。

必要なもの

メンテナンスコンソールにメンテナンスユーザとしてアクセスできる必要があります。

SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダによるサインオン認証が行われます。設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

SAML認証は、UIのからも無効にできます。

SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. メンテナンス コンソールにログインします。
2. [Main Menu]で、[Disable SAML authentication]オプションの番号を入力します。

   SAML認証を無効にしてUnified Managerを再起動することの確認を求めるメッセージが表示されます。

3. 「y」と入力してEnterキーを押すと、Unified Managerが再起動します。

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IdPのログイン ページではなくUnified Managerのログイン ページに変わり

ます。

必要に応じて、IdPにアクセスしてUnified ManagerサーバのURIとメタデータを削除します。

[SAML 認証]ページ

では、Unified ManagerのWeb UIにログインするリモート ユーザをSAMLを使用して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Unified Managerを設定することができます。

- SAML設定を作成または変更するには、アプリケーション管理者ロールが必要です。
- リモート認証を設定しておく必要があります。
- 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つ設定しておく必要があります。

リモート認証とリモートユーザの設定が完了したら、 SAML 認証を有効にするチェックボックスをオンにして、セキュアなアイデンティティプロバイダを使用した認証を有効にすることができます。

- IdP URI

  Unified ManagerサーバからIdPにアクセスするためのURI。URIの例を次に示します。

  ADFSのURIの例：

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  ShibbolethのURIの例：

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- IdP メタデータ

  XML形式のIdPメタデータ。

  Unified ManagerサーバからIdPのURLにアクセスできる場合は、をクリックするとこのフィールドに値が入力されます。

- ホスト システム（FQDN）

  インストール時に定義されたUnified Managerホスト システムの完全修飾ドメイン名（FQDN）。この値は必要に応じて変更できます。

- ホスト URI

  IdPからUnified Managerホスト システムにアクセスするためのURI。

- ホスト メタデータ

  XML形式のホスト システム メタデータ

認証の管理

Unified Manager サーバで LDAP または Active Directory のいずれかを使用して認証を有効にし、サーバと連携してリモートユーザを認証するように設定することができます。

リモート認証の有効化、認証サービスのセットアップ、認証サーバの追加については、 Unified Managerでのアラート通知の送信の設定の前のセクションを参照してください。

認証サーバの編集

Unified Managerサーバが認証サーバとの通信に使用するポートを変更することができます。

必要なもの

アプリケーション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、［全般］ > ［リモート認証］ をクリックします。
2. [ネストされたグループの検索を無効化]チェックボックスをオンにします。
3. **[Authentication Servers]** 領域で、編集する認証サーバを選択し、 [Edit] をクリックします。
4. **Edit Authentication Server** ダイアログボックスで、ポートの詳細を編集します。
5. [Save]をクリックします。

認証サーバの削除

Unified Managerサーバと認証サーバの間の通信を中止する場合は、認証サーバを削除できます。たとえば、管理サーバが通信する認証サーバを変更する場合、認証サーバを削除して新しい認証サーバを追加できます。

必要なもの

アプリケーション管理者のロールが必要です。

認証サーバを削除すると、認証サーバのリモート ユーザとリモート グループはUnified Managerにアクセスできなくなります。

手順

1. 左側のナビゲーションペインで、［全般］ > ［リモート認証］ をクリックします。
2. 削除する認証サーバを1つ以上選択し、[削除]をクリックします。

3. [はい]をクリックして削除要求を確定します。

   [セキュアな接続を使用]オプションが有効になっている場合、認証サーバに関連付けられた証明書も認証サーバと一緒に削除されます。

Active DirectoryまたはOpenLDAPによる認証

管理サーバでリモート認証を有効にし、管理サーバが認証サーバと通信するように設定すると、認証サーバ内のユーザがUnified Managerにアクセスできるようになります。

事前定義された次の認証サービスのいずれかを使用するか、独自の認証サービスを指定できます。

- Microsoft Active Directory

  Microsoftのライトウェイト ディレクトリ サービスは使用できません。

- OpenLDAP

必要な認証サービスを選択し、適切な認証サーバを追加してその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します。リモートのユーザまたはグループのクレデンシャルは、認証サーバで管理されます。管理サーバでは、設定された認証サーバ内のリモート ユーザの認証にLightweight Directory Access Protocol（LDAP）を使用します。

Unified Managerで作成されたローカル ユーザについては、管理サーバのデータベースでユーザ名とパスワードが管理されます。管理サーバで認証が実行され、Active Directory認証またはOpenLDAP認証が使用されることはありません。

監査ログ

監査ログを使用すると、監査ログが侵害されたかどうかを検出できます。ユーザが実行するすべてのアクティビティが監視され、監査ログに記録されます。監査は`、Active IQ Unified Manager のすべてのユーザーインターフェイスと公開されている API の機能に対して実行されます。

監査ログ: ファイルビューを使用して、Active IQ Unified Managerで使用可能なすべての監査ログ ファイルを表示し、アクセスすることができます。Audit Log: ファイルビューファイルは、作成日に基づいてリストされます。このビューには、インストール時またはシステム内のにアップグレードされたときにキャプチャされたすべての監査ログの情報が表示されます。Unified Manager で何らかの操作を実行すると、情報が更新され、ログに記録されます。各ログファイルのステータスは、 File Integrity Status 属性を使用して

取得されます。この属性は、ログファイルの改ざんや削除を検出するためにアクティブに監視されます。システムで監査ログが使用可能になると、監査ログの状態は次のいずれかになります。

State	概要の略
ACTIVE	ログが現在ログに記録されているファイル。
NORMAL	非アクティブで圧縮され、システムに格納されているファイル。
改ざんされた	手動でファイルを編集したユーザーによって侵害されたファイル。
manual_delete_delete	許可されたユーザーによって削除されたファイル。
rollOver _ delete	ローリング設定ポリシーに基づいて移動したために削除されたファイル。
予期しない削除です	不明な理由で削除されたファイル。

Audit Log ページには、次のコマンドボタンがあります。

- 設定
- 削除
- ダウンロード

削除 ボタンを使用すると、監査ログビューにリストされている監査ログを削除できます。監査ログを削除したり、ファイルを削除する理由を指定したりできます。これにより、あとで有効な削除を確認するのに役立ちます。理由列には、削除操作を実行したユーザの名前と理由が表示されます。

ログファイルを削除すると、原因によってシステムからファイルが削除されますが、 DB テーブル内のエントリは削除されません。

監査ログは、監査ログセクションのダウンロードボタンを使用して Active IQ Unified Manager からダウンロードし、監査ログファイルをエクスポートできます。 “標準または” “改ざんとしてマークさ” `.gzip` れたファイルは、圧縮形式でダウンロードされます。

フル AutoSupport バンドルの生成時に、サポートバンドルにはアーカイブされた監査ログファイルとアクティブな監査ログファイルの両方が含まれます。ただし、簡易サポートバンドルが生成されると、アクティブな監査ログのみが含まれます。アーカイブされた監査ログは含まれません。

監査ログの設定

- 監査ログセクションの設定ボタンを使用して、監査ログファイルのローリングポリシーを設定したり、監査ログのリモートロギングを有効にしたりできます。

システム に格納するデータの量と頻度に応じて、 **MAX File** サイズと監査ログの保持日数の値を設定できます。フィールド **total audit log size** の値 は、システムに存在する監査ログデータの合計サイズです。ロールオーバーポリシーは、監査ログの保持日数、最大ファイルサイズ、および監査ログの合計サイズの値によって決まります。監査ログバックアップ　のサイズが監査ログの合計サイズに設定された値に達すると、最初にアーカイブされたファイルが削除されます。つまり、最も古いファイルが削除されます。ただし、ファイルエントリ **"``"**は引き続きデータベースで使用でき、ロールオーバー削除としてマークされます。監査ログの保持日　数の値は、監査ログファイルを保持する日数です。このフィールドに設定された値より古いファイルは、ロールオーバーされます。

手順

1. [監査ログ] > [設定] をクリックします。
2. 最大ファイルサイズ、監査ログの合計サイズ、および監査ログの保持日数を入力します。

   リモートロギングをイネーブルにする場合は、 [Enable Remote Logging] を選択する必要があります。

監査ログのリモートロギングを有効にする

Configure Audit Logs ダイアログボックスの Enable Remote Logging チェックボックスをオンにして、リモート監査ロギングをイネーブルにできます。この機能を使用すると、監査ログをリモートの syslog サーバに転送できます。これにより、スペースに制約がある場合でも監査ログを管理できます。

監査ログのリモートロギングは、 Active IQ Unified Manager サーバ上の監査ログファイルが改ざんされた場合に備えて、改ざんを防止するためのバックアップ機能を提供します。

手順

1. **Configure Audit Logs** ダイアログボックスで、**Enable Remote Logging** チェックボックスをオンにします。

   リモートロギングを設定するための追加フィールドが表示されます。

2. 接続先のリモートサーバのホスト名とポートを入力します。
3. サーバー **CA** 証明書 フィールドで、参照をクリックしてターゲットサーバーのパブリック証明書を選択します。

   証明書 `.pem` は、形式でアップロードする必要があります。この証明書は、ターゲットの syslog サーバから取得し、有効期限が切れていないことを確認する必要があります。証明書　`SubjectAltName` には、（SAN）属性の一部として選択したホスト名が含まれている必要があります。

4. 以下の変数に値を入力します。**CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   これらのフィールドの値はミリ秒単位で指定します。

5. 必要な syslog 形式と TLS プロトコルのバージョンを **format** フィールドと **protocol** フィールドで選択します。
6. ターゲット Syslog サーバで証明書ベースの認証が必要な場合は、 Enable Client Authentication チェックボックスをオンにします。

   監査ログ設定を保存する前に、クライアント認証証明書をダウンロードして Syslog サーバにアップロードする必要があります。そうしないと、接続が失敗します。syslog サーバのタイプによっては、クライアント認証証明書のハッシュの作成が必要になる場合があります。

   例 <hash> `openssl x509 -noout -hash -in cert.pem` <hash> ： syslog-ng にはコマンドを使用して証明書を作成する必要があり、クライアント認証証明書を .0 に続けてというファイルにシンボリックリンクする必要があります。

7. [保存] をクリックして、サーバーとの接続を設定し、リモートログを有効にします。

   [監査ログ] ページに移動します。

[リモート認証]ページ

[リモート認証]ページでは、Unified Manager Web UIにログインするリモート ユーザを認証できるように、Unified Managerと認証サーバの通信を設定することができます。

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。

[リモート認証を有効にする] チェックボックスをオンにすると、認証サーバーを使用してリモート認証を有効にできます。

- 認証サービス

  Active DirectoryやOpenLDAPなどのディレクトリ サービス プロバイダでユーザを認証するように管理サーバを設定するか、または独自の認証メカニズムを指定できます。認証サービスは、リモート認証を有効にした場合にのみ指定できます。

  - ActiveDirectory
    - 管理者名

      認証サーバの管理者の名前を指定します。

    - パスワード。

      認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

  認証サーバでのリモート　　ユーザの場所を指定します。たとえば、認証サーバのドメイン名がou@domain.comである場合のベース識別名は、cn=ou,dc=domain,dc=comです。

- ネストされたグループの検索を無効化

  ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active　Directoryを使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- セキュアな接続を使用

  認証サーバとの通信に使用される認証サービスを指定します。

◦ OpenLDAP

- バインド識別名

  認証サーバでリモート　ユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインド パスワード

  認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

  認証サーバでのリモート ユーザの場所を指定します。たとえば、認証サーバのドメイン名がou@domain.comである場合のベース識別名は、cn=ou,dc=domain,dc=comです。

- セキュアな接続を使用

  LDAPS認証サーバとの通信に使用されるセキュアなLDAPを指定します。

◦ others

- バインド識別名

  設定した認証サーバでリモート　ユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインド パスワード

  認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

  認証サーバでのリモート ユーザの場所を指定します。たとえば、認証サーバのドメイン名がou@domain.comである場合のベース識別名は、cn=ou,dc=domain,dc=comです。

- プロトコル バージョン

認証サーバでサポートされるLightweight Directory Access Protocol（LDAP）のバージョンを指定します。プロトコル　バージョンを自動検出するか、またはバージョン2か3に設定するかを指定できます。

- ユーザ名属性

  管理サーバによって認証されるユーザ　ログイン名を含む認証サーバ内の属性の名前を指定します。

- グループ メンバーシップ属性

  ユーザの認証サーバで指定されている属性と値に基づいて管理サーバのグループ　メンバーシップをリモート ユーザに割り当てる値を指定します。

- UGID

  リモート　ユーザがGroupOfUniqueNamesオブジェクトのメンバーとして認証サーバに含まれている場合は、このオプションを使用して、GroupOfUniqueNamesオブジェクトで指定されている属性を基に管理サーバのグループ　メンバーシップをリモート　ユーザに割り当てることができます。

- ネストされたグループの検索を無効化

  ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active　Directoryを使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- メンバー

  認証サーバがグループの個々のメンバーに関する情報を格納するために使用する属性の名前を指定します。

- ユーザ オブジェクト クラス

  リモート認証サーバ内のユーザのオブジェクト クラスを指定します。

- グループ オブジェクト クラス

  リモート認証サーバ内のすべてのグループのオブジェクト クラスを指定します。

- セキュアな接続を使用

  認証サーバとの通信に使用される認証サービスを指定します。

認証サービスを変更する場合は、既存の認証サーバをすべて削除してから新しい認証サーバを追加するようにしてください。

[Authentication Servers]領域

Authentication Servers 領域には、管理サーバがリモートユーザの検索および認証のために通信する認証サーバが表示されます。リモートのユーザまたはグループのクレデンシャルは、認証サーバで管理されます。

- コマンド ボタン

  認証サーバの追加、編集、削除を行うことができます。

  - Add:

    認証サーバを追加できます。

    追加する認証サーバがハイアベイラビリティ 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。

  - 編集：

    選択した認証サーバの設定を編集できます。

  - 削除

    選択した認証サーバを削除します。

- 名前または IP アドレス：

  管理サーバでユーザの認証に使用される認証サーバのホスト名またはIPアドレスが表示されます。

- port

  認証サーバのポート番号が表示されます。

- 認証をテスト

  このボタンでは、リモートのユーザまたはグループを認証することで認証サーバの設定を検証します。

  テストの際にユーザ名のみを指定すると、管理サーバは認証サーバでリモート ユーザを検索しますが、ユーザの認証は行いません。ユーザ名とパスワードを指定すると、管理サーバはリモート ユーザの検索と認証を行います。

  リモート認証が無効になっている場合は、認証をテストできません。

セキュリティ証明書の管理

Unified　ManagerサーバでHTTPSを設定することで、セキュアな接続を介してクラスタを監視および管理できるようになります。

HTTPSセキュリティ証明書の表示

HTTPS証明書の詳細をブラウザで取得した証明書と比較して、Unified　Managerに対するブラウザの暗号化された接続が妨害されていないことを確認できます。

必要なもの

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。

証明書を表示すると、再生成された証明書の内容を検証したり、Unified　Managerへのアクセスに使用できるURLの別名を確認したりできます。

手順

1. 左側のナビゲーションペインで 、**General** > **HTTPS Certificate** の順にクリックします。

   HTTPS証明書がページの上部に表示されます。

セキュリティ証明書について、の情報よりも詳しい情報を表示する必要がある場合は、ブラウザで接続証明書を表示できます。

HTTPS証明書署名要求のダウンロード

認証局にファイルを送信して署名を求めるために、現在のHTTPSセキュリティ証明書の証明書要求をダウンロードできます。CA署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

必要なもの

アプリケーション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 、**General** > **HTTPS Certificate** の順にクリックします。
2. [HTTPS 証明書署名要求のダウンロード]をクリックします。
3. `<hostname>.csr` ファイルを保存します。

認証局にファイルを送信して署名を求め、署名済み証明書をインストールできます。

CA 署名済みで返された HTTPS 証明書をインストールする

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。アップロードしてインストールするファイルは、既存の自己署名証明書の署名済みバージョンである必要があります。CA署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

必要なもの

次の操作を完了しておきます。

- 証明書署名要求ファイルをダウンロードし、認証局の署名を受けます。
- 証明書チェーンをPEM形式で保存します。
- すべての証明書（Unified　Managerサーバ証明書からルート署名証明書まで。存在する中間証明書もすべて含む）をチェーンに組み込みます。

アプリケーション管理者のロールが必要です。

CSR 作成の証明書の有効期間が 397 日を超える場合、証明書の署名と返却の前に CA によって有効期間が 397 日に短縮されます

手順

1. 左側のナビゲーションペインで 、**General** > **HTTPS Certificate** の順にクリックします。
2. [HTTPS 証明書のインストール]をクリックします。
3. 表示されたダイアログ　ボックスで、[ファイルを選択...]をクリックしてアップロードするファイルを探します。
4. ファイルを選択し、[インストール]をクリックしてファイルをインストールします。

外部ツールを使用して生成された HTTPS 証明書のインストール

証明書チェーンの例

証明書チェーン ファイルの内容の例を次に示します。

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

外部ツールを使用して生成された HTTPS 証明書のインストール

自己署名または CA 署名の証明書をインストールできます。証明書は、 OpenSSL 、 BoringSSL 、 LetsEncrypt などの外部ツールを使用して生成されます。

秘密鍵と証明書チェーンをロードするのは、外部で生成された公開鍵と秘密鍵のペアであるためです。使用できるキーペアアルゴリズム """"は RSA と EC です。［ **HTTPS** 証明書のインストール ］ オプションは、 ［ 全般 ］ セクションの ［ HTTPS 証明書 ］ ページで使用できます。アップロードするファイルは、次の入力形式である必要があります。

1. Active IQ UM ホストに属するサーバの秘密鍵
2. 秘密鍵と一致するサーバの証明書
3. ルートまでの CA の証明書（上記の証明書への署名に使用）

EC キーペアを含む証明書をロードするための形式

許可さ """"れる曲線は prime256v1 および secp384r1 です。外部で生成された EC ペアを含む証明書の例：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

RSA キーペアを含む証明書をロードするための形式

ホスト証明書に属する RSA キーペアで使用できるキーサイズは、 2048 、 3072 、および 4096 です **。

外部生成 RSA キーペアを含む証明書は、次のとおりです。

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

証明書をアップロードしたら、 Active IQ Unified Manager インスタンスを再起動して変更を有効にする必要があります。

外部で生成された証明書をアップロードする際にチェック

システムは、外部ツールを使用して生成された証明書をアップロードする際にチェックを実行します。い

ずれかのチェックに失敗すると、証明書は拒否されます。また、製品内の CSR から生成された証明書、および外部ツールを使用して生成された証明書の検証も含まれます。

- 入力された秘密鍵が、入力されたホスト証明書に照らして検証されます。
- ホスト証明書の Common Name （CN ；共通名）とホストの FQDN の照合が行われます。
- ホスト証明書の Common Name （CN ；共通名）を空または空白にしたり、 localhost に設定したりすることはできません。
- 有効開始日は将来の日付にすることはできません。また、証明書の有効期限は過去の日付にすることはできません。
- 中間 CA または CA が存在する場合、証明書の有効開始日を将来の日付にすることはできません。また、有効期限は過去の日付にすることはできません。

入力内の秘密鍵を暗号化しないでください。暗号化された秘密鍵がある場合、それらの秘密鍵はシステムで拒否されます。

例1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

例2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

例3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

証明書管理のページの説明

[HTTPS Certificate]ページでは、現在のセキュリティ証明書を表示し、新しいHTTPS証明書を生成することができます。

[HTTPS Certificate]ページ

[HTTPS Certificate]ページでは、現在のセキュリティ証明書の表示、証明書署名要求のダウンロード、新しいHTTPS証明書の生成、新しいHTTPS証明書のインストールを行うことができます。新しいHTTPS証明書を生成していない場合は、インストール時に生成された証明書がこのページに表示されます。

コマンド ボタン

各コマンド ボタンを使用して次の処理を実行できます。

- HTTPS 証明書署名要求のダウンロード

  現在インストールされているHTTPS証明書の署名要求をダウンロードします。署名を行う認証局に提出する<hostname>ファイルを保存するよう指示されます。

- HTTPS 証明書のインストール

  認証局の署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。新しい証明書は、管理サーバを再起動すると有効になります。

- HTTPS 証明書の再生成

  HTTPS証明書を生成して現在のセキュリティ証明書と置き換えることができます。新しい証明書は、Unified Managerを再起動すると有効になります。

[HTTPS 証明書の再生成]ダイアログ ボックス

[HTTPS 証明書の再生成]ダイアログ ボックスでは、セキュリティ情報をカスタマイズし、その情報を使用して新しいHTTPS証明書を生成することができます。

このページには現在の証明書の情報が表示されます。

現在の証明書属性を使用して再生成または現在の証明書属性を更新を選択して、現在の情報で証明書を再生成するか、新しい情報で証明書を生成することができます。

- 共通名

  必須。保護する対象の完全修飾ドメイン名（FQDN）。

  Unified Managerのハイアベイラビリティ構成では、仮想IPアドレスを使用します。

- Eメール

  任意。組織の連絡先のEメール アドレス。証明書の管理者またはIT部門のEメール アドレスが一般的です。

- 会社

  任意。通常は会社の法人名。

- 部門

  任意。社内の部署の名前。

- 市区町村

  任意。会社の所在地の市区町村。

- 状態

  任意。会社の所在地の都道府県。

- -country

  任意。会社の所在地の国。通常はISOの2文字の国コードです。

- 別名

  必須。既存のローカルホストやその他のネットワークアドレスに加えて、このサーバへのアクセスに使用できるプライマリ以外のドメイン名が追加されました。代行名はそれぞれカンマで区切ります。

  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。

- キーサイズ（キーアルゴリズム：RSA）

  キーアルゴリズムは rsa に設定されています。次のいずれかのキーサイズを選択できます。2048 、3072 、または 4096 ビット。デフォルトのキー・サイズは 2048 ビットに設定されています。

- 有効期間

  デフォルトの有効期間は 397 日です。以前のバージョンからアップグレードした場合は、以前の証明書の有効性が変更されていない可能性があります。

著作権に関する情報

富士通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、富士通によって「現状のまま」提供されています。富士通は明示的な保証、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。富士通は、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。

富士通は、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。富士通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、富士通は責任を負いません。この製品の使用または購入は、富士通の特許権、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。

登録商標

富士通、富士通ロゴ、ETERNUSは富士通の登録商標です。会社名、製品名等の固有名詞は、各社の商号、商標または登録商標です。
https://www.fujitsu.com/jp/products/computing/storage/trademark/

マニュアルの更新について

本書の最新版や本装置に関連する最新の情報は、以下のサイトで公開されています。

https://www.fujitsu.com/jp/products/computing/storage/manual/

必要に応じてご使用モデルのマニュアルを参照してください。

FUJITSU Storage ETERNUS AX/HX Series

Active IQ® Unified Manager 9.11.1 設定タスクと管理タスクの実行

CA08871-174-01

発行日: 2022 年 6 月

発行責任: 富士通株式会社