# 認証の管理

## Active IQ Unified Manager 9.13

NetApp
December 18, 2023

# 目次

# 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 でアラート通知を送信するための設定」の前のセクションを参照してください。

## 認証サーバを編集しています

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、 * 一般 * > * 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にする *] ボックスをオンにします。
3. [* 認証サーバ * ] 領域で、編集する認証サーバを選択し、 [ * 編集 ] 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. [ 保存（ Save ） ] をクリックします。

## 認証サーバを削除しています

Unified Manager サーバが認証サーバと通信できないようにするには、認証サーバを削除します。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は、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または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、 * 一般 * > * リモート認証 * をクリックします。
2. 削除する認証サーバーを 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する *] 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ている証明書は認証サーバとともに削除されます。

# 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 の略

  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。

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てアクセスするには、*監査ログ：ファイルビュー*を使用します。監査ログ：ファイルビュー内のファイルは、作成日に基づいて一覧表示されます。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、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る「 File Integrity Status 」属性を使用して取得されます。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。

| 状態 | 説明 |
| --- | --- |
| アクティブ | ログが現在ログに記録されているファイル。 |
| 正常 | 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。 |

| 状態 | 説明 |
| --- | --- |
| 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

**delete** ボタンを使用すると、 Audit Logs ビューに表示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 * download * 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。「normal」または「Tampered」とマークされたファイルは、圧縮された形式でダウンロードされます `.gzip` の形式で入力し

監査ログファイルは定期的にアーカイブされ、参照用にデータベースに保存されます。アーカイブの前に、監査ログはセキュリティと整合性を維持するためにデジタル署名されます。

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。

## 監査ログを設定しています

### 監査ログセクションの *Configure * 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。

システムに保存するデータの量と頻度に応じて、 * 最大ファイルサイズ * 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 * 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 * 」フィールドの値によって決まります。監査ログのバックアップのサイズが、監査ログの合計サイズ * で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。しかし、ファイルエントリはデータベースで引き続き使用でき、「ロールオーバー削除」とマークされます。監査ログの保持日数 * 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 **>] > [** 構成 *] 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 * 、監査ログの保持日数 * の値を入力します。

リモート・ロギングを有効にする場合は、 * リモート・ロギングを有効にする * 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

監査ログの設定ダイアログ・ボックスのリモート・ログを有効にするチェックボックスをオンにすると ' リモート監査ログを有効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. [ 監査ログの設定 *] ダイアログボックスで、 [ リモートログを有効にする *] 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 * hostname * と * port * 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。

   証明書はにアップロードする必要があります `.pem` の形式で入力しこの証明書は、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。証明書には、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 `SubjectAltName` （SAN）属性。

4. 次のフィールドの値を入力します。 * 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. [**format**] フィールドと [**protocol**] フィールドで、必要な syslog 形式と TLS プロトコルのバージョンを選択します。
6. ターゲット Syslog サーバーで証明書ベースの認証が必要な場合は、 * クライアント認証を有効にする * チェックボックスを選択します。

   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：syslog-ngには、コマンドを使用して証明書の<hash>が作成されている必要があります `openssl x509 -noout -hash -in cert.pem`をクリックし、クライアント認証証明書を<hash>.0のあとのファイルにシンボリックリンクする必要があります。

7. サーバとの接続を設定し、リモートロギングを有効にするには、 * Save * をクリックします。

   [ 監査ログ ] ページに移動します。

の値は、設定に影響する可能性があります。設定が定義された値よりも応答に時間がかかると、接続エラーが原因で設定に失敗する可能性があります。正常な接続を確立するには、[接続タイムアウト]*の値を増やして、設定をやり直してください。

# Remote Authentication ページの略

Remote Authentication 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。

  - * Active Directory *
    - 管理者の名前

      認証サーバの管理者名を指定します。

    - 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、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します

      認証サーバとの通信に使用す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、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します

  LDAP認証サーバとの通信にSecure LDAPを使用することを指定します。

◦ * その他 *

- 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、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。プロトコルのバージョンを自動的に検出するか、バージョン 2 または 3 に設定するかを指定できます。

- ユーザー名属性

  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。

  *Member*,*User Object Class*,_GroupオブジェクトClass_attributesに入力する値は、Active Directory、OpenLDAP、およびLDAPの設定に追加する値と同じである必要があります。そうしないと、認証が失敗する可能性があります。

- セキュアな接続を使用します

  認証サーバとの通信に使用す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 *

  認証サーバを追加、編集、または削除できます。

  - 追加（ 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、いずれかの認証サーバにアクセスできない場合でも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。

- * ポート *

  認証サーバのポート番号が表示されます。

- * 認証のテスト *

  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。

## 著作権に関する情報



## 商標に関する情報