認証を管理する
Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-916/config/task_edit_authentication_servers.html on October 15, 2025. Always check docs.netapp.com for the latest.

目次

認証を管理する 1
認証サーバーを編集する 1
認証サーバーを削除する 1
Active DirectoryまたはOpenLDAPによる認証 2
監査ログ 2
監査ログを構成する 3
監査ログのリモートログを有効にする 4
[リモート認証]ページ 5
[認証サーバ]領域 7

認証を管理する

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、認証サービスの設定、認証サーバーの追加については、前のセクションの「**Unified Manager** を設定してアラート通知を送信する」を参照してください。

認証サーバーを編集する

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。

開始する前に

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にする*ボックスをチェックします。
3. *認証サーバー*領域で、編集する認証サーバーを選択し、*編集*をクリックします。
4. 認証サーバーの編集 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*をクリックします。

認証サーバーを削除する

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。

開始する前に

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ーを 1 つ以上選択し、[削除] をクリックします。
3. 削除要求を確認するには、[はい] をクリックします。

   安全な接続を使用する オプションが有効になっている場合、認証サーバーに関連付けられている証明書は認証サーバーとともに削除されます。

Active DirectoryまたはOpenLDAPによる認証

管理サーバーでリモート認証を有効にし、管理サーバーが認証サーバーと通信するように設定して、認証サーバー内のユーザーが Unified Manager にアクセスできるようにすることができます。

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、認証サーバ内のリモート ユーザーが Unified Manager にアクセスできるようにすることができます。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 ユーザーの場合、管理サーバーはユーザー名とパスワードの独自のデータベースを維持します。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]を使用して、監査ログが侵害されていないかどうかを検出できます。ユーザが実行するアクティビティはすべて監視され、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 を使用すると、 Active IQ Unified Managerで使用可能なすべての監査ログ ファイルを表示およびアクセスできます。監査ログ: ファイル ビュー内のファイルは、作成日に基づいてリストされます。このビューには、インストールまたはアップグレードされてから現在までにシステムで取得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、そのたびに情報が更新されて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`」属性を使用してキャプチャされ、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。システムで使用可能な監査ログは、次のいずれかのステータスになります。

州	説明
ACTIVE	ログを記録中のファイル。
NORMAL	圧縮されてシステムに格納されている、アクティブでないファイル。
TAMPERED	侵害されたファイル（権限のないユーザによって手動で編集された）。

州	説明
MANUALL_DELETE	権限のあるユーザ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ロールオフで削除されたファイル。
UNEXPECTED_DELETE	不明な理由で削除されたファイル。

[監査ログ]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。監査ログを削除する際、あとで適切な削除だったことがわかるように、必要に応じてファイルの削除理由を指定することができます。この理由は、削除処理を実行したユーザの名前とともに[理由]列に表示されます。

> ログ ファイルを削除すると、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 セクションの ダウンロード ボタンを使用してActive IQ Unified Managerから監査ログをダウンロードし、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`形式。

監査ログ ファイルは定期的にアーカイブされ、参照できるようにデータベースに保存されます。セキュリティと整合性を維持するために、アーカイブ前に監査ログはデジタル署名されます。

完全なAutoSupport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。一方、軽量なサポート バンドルには、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。

監査ログを構成する

監査ログ セクションの 構成 ボタンを使用して、監査ログ ファイルのローリング ポリシーを構成し、監査ログのリモート ログ記録を有効にすることもできます。

システムに保存するデータの希望量と頻度に応じて、最大ファイル サイズ と 監査ログ保持日数 の値を設定できます。フィールド **TOTAL AUDIT LOG SIZE** の値は、システム内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 **TOTAL AUDIT LOG SIZE** 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。ただし、ファイル エントリはデータベース内で引き続き使用可能であり、「`Rollover Delete`」としてマークされます。 **AUDIT LOG RETENTION DAYS** の値は、監査ログ ファイルが保存される日数です。このフィールドで設定された値よりも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、および*監査ログの保持日数*に値を入力します。

   リモート ログを有効にする場合は、[リモート ログを有効にする] を選択する必要があります。 /// 2025-6-11、OTHERDOC-133

監査ログのリモートログを有効にする

監査ログの構成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すると、リモート監査ログを有効にすることができます。この機能を使用して、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のバックアップとしても機能します。

手順

1. *監査ログの構成*ダイアログボックスで、*リモートログの有効化*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フィールドが表示されます。

2. 接続するリモート サーバーの **HOSTNAME** と **PORT** を入力します。
3. **SERVER CA CERTIFICATE** フィールドで、**BROWSE** をクリックして、対象サーバーの公開証明書を選択します。

   証明書は、 `.pem`形式。ターゲットの`syslog`サーバから取得した、有効期限内の証明書を使用してください。証明書には、選択した「`hostname`」が `SubjectAltName`(SAN) 属性。

4. 次のフィールドに値を入力します: **CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   ミリ秒単位の値を指定してください。

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 バージョンを選択します。
6. 対象の 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を作成する必要があります。

   例: syslog-ngでは、コマンドを使用して証明書の<ハッシュ>を作成する必要があります。 `openssl x509 -noout -hash -in cert.pem`次に、クライアント認証証明書を <ハッシュ> .0 という名前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. 保存 をクリックして、サーバーとの接続を構成し、リモート ログを有効にします。

   [監査ログ]ページにリダイレクトされます。

接続タイムアウト*の値は構成に影響する可能性があります。定義された値よりも応答に時間がかかると、接続エラーが発生して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、構成を再度試してください。

[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化する]チェックボックスをオンにすると、認証サーバを使用したリモート認証を有効にすることができます。

- 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。

  - アクティブディレクトリ
    - 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、認証サーバーのドメイン名がou@domain.com の場合、基本識別名は **cn=ou,dc=domain,dc=com** になります。

    - 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。

    - 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。

  - オープン**LDAP**
    - 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、認証サーバーのドメイン名がou@domain.com の場合、基本識別名は **cn=ou,dc=domain,dc=com** になります。

- セキュアな接続を使用

  LDAP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。

◦ 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、認証サーバーのドメイン名がou@domain.com の場合、基本識別名は **cn=ou,dc=domain,dc=com** になります。

- 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。

> *Member*、*User Object Class*、および *Group Object Class* 属性に入力する値は、Active Directory、OpenLDAP、および LDAP 構成に追加された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

  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。

[認証サーバ]領域

[認証サーバ]領域には、管理サーバがリモート ユーザの検出と認証を行う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。

  - 追加

    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。

- ポート

  認証サーバのポート番号が表示されます。

- テスト認証

  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

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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