認証を管理する
Active IQ Unified Manager

NetApp
November 13, 2026

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

目次

認証を管理する . . . 1
- Active IQ Unified Manager で認証サーバーを編集する . . . 1
- Active IQ Unified Manager で認証サーバーを削除する . . . 1
- Active IQ Unified Manager で Active Directory または OpenLDAP を使用して認証する . . . 1
- 監査ログ . . . 2
  - Active IQ Unified Manager の監査ログについて . . . 2
  - Active IQ Unified Manager 監査ログの設定 . . . 3
  - Active IQ Unified Manager で監査ログのリモートロギングを有効にする . . . 3
- Active IQ Unified Manager のリモート認証ページを使用する . . . 4
  - [認証サーバ]領域 . . . 7

認証を管理する

Active IQ Unified Manager で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検索を無効にする」チェックボックスをオンにします。
3. 「Authentication Servers」エリアで、編集する認証サーバーを選択し、「Edit」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。

Active IQ Unified Manager で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. 削除リクエストを確定するには、「はい」をクリックしてください。

   「セキュア接続を使用する」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た証明書は、認証サーバーとともに削除されます。

Active IQ Unified Manager で Active Directory または OpenLDAP を使用して認証する

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構成することで、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、適切な認証サーバーを追加することで、認証サーバー上のリモートユーザーがUnified Manager にアクセスできるようになります。リモートユーザーまたはグループの認証情報は、認証サーバーによって管理されます。管理サーバーは、構成済みの認証サーバー内でリモートユーザーを認証するために、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保持します。管理サーバーが認証を実行し、認証にActive DirectoryやOpenLDAPは使用しません。

監査ログ

Active IQ Unified Manager の監査ログについて

監査ログを使用することで、監査ログが侵害されているかどうかを検出できます。ユーザーが実行したすべてのアクティビティは監視され、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および公開されている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：ファイルビューでは、ファイルは作成日順に一覧表示されます。このビューには、システムへのインストールまたはアップグレードから現在までに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で何らかの操作を行うと、その情報が更新され、ログに記録されます。各ログファイルの状態は、「`File Integrity Status\`」属性を使用して取得され、ログファイルの改ざんや削除を検出するために積極的に監視されます。監査ログがシステム内で利用可能な場合、監査ログは次のいずれかの状態になります：

状態	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）。
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

*DELETE*ボタンを使用すると、Audit Logsビューに表示されている任意の監査ログを削除できます。監査ログを削除する際、必要に応じてファイルの削除理由を指定できます。これは、将来的に正当な削除であるかを判断するのに役立ちます。REASON列には、削除操作を実行したユーザー名とともに、その理由が表示されます。

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。

Active IQ Unified Managerの監査ログセクションにある*DOWNLOAD*ボタンを使用して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 `.gzip`形式でダウンロードされます。

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。

Active IQ Unified Manager 監査ログの設定

監査ログセクションの*設定*ボタンを使用すると、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グ記録を有効にしたりできます。

システムに保管したいデータの量と頻度に応じて、最大ファイルサイズ*と*監査ログ保持日数*の値を設定できます。*監査ログ合計サイズ*フィールドの値は、システムに存在する監査ログデータの合計サイズを示します。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*監査ログ合計サイズ*のフィールドの値によって決定されます。監査ログのバックアップサイズが*監査ログ合計サイズ*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。これは、最も古いファイルが削除されることを意味します。しかし、そのファイルエントリはデータベース内に残っており、「Rollover Delete」とマークされます。*監査ログ保持日数*の値は、監査ログファイルが保持される日数を表します。このフィールドに設定された値よりも古いファイルはすべて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*に値を入力してください。

   リモートログを有効にするには、*リモートログを有効にする*を選択します。

Active IQ Unified Manager で監査ログのリモートロギングを有効にする

リモート監査ログを有効にするには、「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選択します。この機能を使用すると、監査ログをリモートSyslogサーバに転送できます。これにより、容量に制約がある場合でも

監査ログを管理できるようになります。

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選択します。

   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、対象サーバーの公開証明書を選択します。

   証明書は `.pem`形式でアップロードする必要があります。この証明書は対象の`Syslog`サーバから取得する必要があり、有効期限が切れていないものでなければなりません。証明書には、選択した「`hostname」が `SubjectAltName`（SAN）属性の一部として含まれている必要があります。

4. 以下のフィールドに値を入力してください：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   ミリ秒単位の値を指定してください。

5. **FORMAT** および **PROTOCOL** フィールドで、必要なSyslogフォーマットとTLSプロトコル バージョンを選択します。
6. 対象のSyslogサーバが証明書ベースの認証を必要とする場合は、*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を作成する必要があります。

   例：syslog-ng では、コマンド `openssl x509 -noout -hash -in cert.pem`を使用して証明書の<hash>を作成する必要があります。その後、クライアント認証証明書を<hash> .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. *Save*をクリックしてサーバとの接続を設定し、リモートログ記録を有効にします。

   [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*の値は設定に影響を与える可能性があります。設定応答時間が規定値よりも長くなると、接続エラーにより設定が失敗する可能性があります。接続を正常に確立するには、*接続タイムアウト*の値を増やして、再度設定を試してください。

Active IQ Unified Manager のリモート認証ページを使用する

[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。

  - **Active Directory**
    - 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

      認証サーバーにおけるリモートユーザーの場所を指定します。例えば、認証サーバーのドメイン名が ou@domain.com の場合、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

      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

      認証サーバーにおけるリモートユーザーの場所を指定します。例えば、認証サーバーのドメイン名が ou@domain.com の場合、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

      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

  認証サーバーにおけるリモートユーザーの場所を指定します。例えば、認証サーバーのドメイン名が ou@domain.com の場合、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 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構成で追加し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。

  - Edit

    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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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