



## 認証の管理

### Active IQ Unified Manager 9.9

NetApp  
December 15, 2023

This PDF was generated from <https://docs.netapp.com/ja-jp/active-iq-unified-manager-99/online-help/task-enabling-remote-authentication.html> on December 15, 2023. Always check docs.netapp.com for the latest.

# 目次

認証の管理 .....	1
リモート認証の有効化 .....	1
リモート認証でのネストされたグループの無効化 .....	2
認証サービスをセットアップしています .....	3
認証サーバを追加しています .....	4
認証サーバの設定をテストする .....	5
認証サーバを編集しています .....	6
認証サーバを削除しています .....	6
Active Directory または OpenLDAP による認証 .....	7
SAML 認証の有効化 .....	7
アイデンティティプロバイダの要件 .....	9
SAML 認証に使用するアイデンティティプロバイダを変更する .....	10
SAML 認証を無効にします .....	11
監査ログ .....	12
認証ウィンドウとダイアログボックスの概要 .....	14

# 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。

また、SAML認証を有効にして、Unified Manager Web UIにログイン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）で認証するようにすることができます。

## 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。

### 作業を開始する前に

アプリケーション管理者のロールが必要です。



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。

### このタスクについて

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

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



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、\* 一般 \* > \* リモート認証 \* をクリックします。
2. [Enable remote authentication...\*] チェックボックスをオンにします。
3. [Authentication Service] フィールドで、サービスのタイプを選択し、認証サービスを設定します。

認証タイプ	入力する情報
Active Directory	<ul style="list-style-type: none"> <li>• 認証サーバの管理者名。次のいずれかの形式で指定します。 <ul style="list-style-type: none"> <li>◦ domainname \ username</li> <li>◦ username @ domainname</li> <li>◦ Bind Distinguished Name（適切なLDAP表記を使用）</li> </ul> </li> <li>• 管理者パスワード</li> <li>• ベース識別名（適切な LDAP 表記を使用）</li> </ul>
LDAP を開きます	<ul style="list-style-type: none"> <li>• バインド識別名（適切な LDAP 表記を使用）</li> <li>• バインドパスワード</li> <li>• ベース識別名</li> </ul>

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。

認証サーバに Secure Connection オプションを使用する場合、Unified Manager は Secure Sockets Layer（SSL）プロトコルを使用して認証サーバと通信します。

1. 認証サーバを追加し、認証をテストします。
2. [ 保存（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。

### 作業を開始する前に

- アプリケーション管理者のロールが必要です。
- 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

### このタスクについて

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、\* 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 \* ] チェックボックスをオンにします。
3. [ 保存 ( Save ) ] をクリックします。

## 認証サービスをセットアップしています

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。

### 作業を開始する前に

- 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、\* 一般 \* > \* 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。

を選択した場合は	操作
Active Directory	<ol style="list-style-type: none"><li>1. 管理者の名前とパスワードを入力します。</li><li>2. 認証サーバのベース識別名を指定します。</li></ol> <p>たとえば、認証サーバのドメイン名がou@domain.comの場合、ベース識別名はになります cn=ou,dc=domain,dc=com。</p>
OpenLDAP	<ol style="list-style-type: none"><li>1. バインド識別名とバインドパスワードを入力します。</li><li>2. 認証サーバのベース識別名を指定します。</li></ol> <p>たとえば、認証サーバのドメイン名がou@domain.comの場合、ベース識別名はになります cn=ou,dc=domain,dc=com。</p>

を選択した場合は	操作
その他	<ol style="list-style-type: none"> <li>1. バインド識別名とバインドパスワードを入力します。</li> <li>2. 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の場合、ベース識別名はになります cn=ou,dc=domain,dc=com。</li> <li>3. 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。</li> <li>4. 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。</li> </ol>



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。

1. [ 保存 ( Save ) ] をクリックします。

## 認証サーバを追加しています

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。

### 作業を開始する前に


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

### このタスクについて

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、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。

### 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. [ セキュアな接続を使用する \* ] オプションを有効または無効にします。

状況	操作
有効にします	<ol style="list-style-type: none"> <li>1. [セキュアな接続を使用（ Use Secure Connection * ） ] オプションを選択します。</li> <li>2. [Authentication Servers] 領域で、 <b>[Add]</b> をクリックします。</li> <li>3. 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。</li> <li>4. [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。</li> <li>5. [ 証明書の表示 ] 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。</li> <li>6. [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。</li> </ol> <div>  <p>Secure Connection authentication * 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。</p> </div>
無効にします	<ol style="list-style-type: none"> <li>1. [セキュアな接続を使用する *] オプションをオフにします。</li> <li>2. [Authentication Servers] 領域で、 <b>[Add]</b> をクリックします。</li> <li>3. [Add Authentication Server] 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 ）、およびポートの詳細を指定します。</li> <li>4. [ 追加（ Add ） ] をクリックします。</li> </ol>

追加した認証サーバが Servers 領域に表示されます。

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

## 認証サーバの設定をテストする

認証サーバの設定を検証して、管理サーバが認証サーバと通信できるかどうかを確認できます。設定を検証するには、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、設定済みの設定を使用して認証します。

## 作業を開始する前に

- リモートユーザまたはリモートグループを Unified Manager サーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- 認証サーバから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。

## このタスクについて

認証サービスが Active Directory に設定されている場合に、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、\* 一般 \* > \* リモート認証 \* をクリックします。
2. [ \* 認証のテスト \* ] をクリックします。
3. [ユーザーのテスト\*]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。

## 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。

## 作業を開始する前に

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、\* 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。



## 作業を開始する前に

アプリケーション管理者のロールが必要です。

## このタスクについて

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。

## 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。

## 作業を開始する前に

- リモート認証を設定し、正常に実行され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。

## このタスクについて

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、両方の接続を完了できるように準備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 \* をクリックします。
2. Enable SAML authentication \* チェックボックスをオンにします。

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 メタデータの取得」ボタンをクリックすると、IdP のメタデータフィールドに自動的に値が入力されます。

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. [ 保存（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 \* ] をクリックすると、Unified Manager が再起動します。

## 結果

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

## 完了後

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



アイデンティティプロバイダに ADFS を使用している場合は、Unified Manager GUI で ADFS のタイムアウトが考慮されず、Unified Manager のセッションタイムアウトに達するまでセッションが継続されます。GUI セッションのタイムアウトを変更するには、\* General \* > \* Feature Settings \* > \* Inactivity Timeout \* をクリックします。

## 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。

### サポートされている暗号化標準

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

### 検証済みのアイデンティティプロバイダ

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

## ADFS の設定要件

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

要求規則	価値
Sam - アカウント名	名前 ID
Sam - アカウント名	urn : OID : 0.9.2342.19200300.100.1.1

要求規則	価値
トークングループ — 修飾されていない名前	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、Unified Manager からログアウトするときにユーザ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 [Authentication Policies] フォルダをクリックします
  - c. 右の [アクション] 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트라ネット認証方式をデフォルトの「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。この問題を解決する方法は 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 サーバでの失効チェックを無効にします。

["証明書利用者信頼ごとの失効チェックを無効にします"](#)

- 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 認証に使用するアイデンティティプロバイダを変更する

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。

### 作業を開始する前に

- 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。

### このタスクについて

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 \* をクリックします。
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。

Unified Manager サーバから IdP に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

「タデータの取得」ボタンをクリックすると、IdP のメタデータフィールドに自動的に値が入力されます。

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. [ 構成の保存 \* ] 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。

## 完了後

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。

## SAML 認証を無効にします

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がサインオン認証を実行します。

### このタスクについて

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 Unified Manager メンテナンスコンソール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 \* をクリックします。
2. [SAML 認証を有効にする \*] チェックボックスをオフにします。
3. [ 保存（ 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 \* ] をクリックすると、Unified Manager が再起動します。

## 結果

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。

## 完了後

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。

## 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たり、アクセスしたりできます。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。
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

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。

### このタスクについて

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。

### このタスクについて

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。

## 認証ウィンドウとダイアログボックスの概要

LDAP認証は、Setup/Authenticationページから有効にできます。

### 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ーを設定するか、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の場合、ベース識別名はになります cn=ou,dc=domain,dc=com。

- 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の場合、ベース識別名はになります cn=ou,dc=domain,dc=com。

- セキュアな接続を使用します

- 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。

◦ \* 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` の場合、ベース識別名はになります `cn=ou,dc=domain,dc=com`。

▪ 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。

- 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。

## SAML Authentication ページ

SAML 認証ページを使用して、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、「\* IdP メタデータの取得方法 \*」ボタンをクリックしてこのフィールドに値を入力できます。

- \* 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 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

## 著作権に関する情報

Copyright © 2023 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权を有し、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权については、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。