アラート通知を送信するように**Unified Manager**を構成する

Active IQ Unified Manager

NetApp
October 15, 2025

目次

アラート通知を送信するようにUnified Managerを構成する

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。

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. "イベント通知を設定"。

   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. "リモート認証を有効にする"。

   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. "認証サーバを追加する"。

   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. "ユーザーを追加する"。

   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. "アラートを追加する"。

   通知を送信するEメール アドレスの追加、通知を受信するユーザの追加、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。

イベント通知を設定

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。

開始する前に

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

  送信されたアラート通知の「From」フィールドに電子メール アドレスが表示されます。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] をクリックします。
2. [通知]ページで、該当する項目を設定します。

   注記:

   - 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は、すべての電子メール通知が正常に配信されるように、実際に機能する電子メール 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。
3. *保存*をクリックします。
4. **STARTTLS** を使用する または **SSL** を使用する オプションを選択した場合は、保存 ボタンをクリックすると証明書ページが表示されます。証明書の詳細を確認し、証明書を受け入れて通知設定を保存します。

   証明書の詳細を表示するには、[証明書の詳細を表示] ボタンをクリックしてください。既存の証明書の有効期限が切れている場合は、[**STARTTLS** を使用する] または [**SSL** を使用する] ボックスのチェックを外し、通知設定を保存し、[**STARTTLS** を使用する] または [**SSL** を使用する] ボックスを再度チェックして新しい証明書を表示します。

リモート認証を有効にする

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。

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。

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にする…*のボックスをチェックします。
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。

認証タイプの場合...	次の情報を入力してください...
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） • 管理者のパスワード • ベース識別名（適切なLDAP表記を使用）
オープンLDAP	• バインド識別名（適切なLDAP表記を使用） • パスワードをバインドする • 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[セキュアな接続を使用]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: 認証サーバーを追加し、認証をテストします。
5. *保存*をクリックします。

リモート認証からネストされたグループを無効にする

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。

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。

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にする*のボックスをチェックします。
3. *保存*をクリックします。

認証サービスを設定する

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。

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、[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。

選択した場合...	操作
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。

選択した場合...	操作
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。
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。 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. *保存*をクリックします。

認証サーバを追加する

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。

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。

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. *安全な接続を使用する*オプションを有効または無効にします。

状況	操作
有効にする	a. *安全な接続を使用する*オプションを選択します。 b. 認証サーバー領域で、[追加] 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. [ホストの承認]ダイアログ ボックスで、[証明書を表示]をクリックします。 e. [証明書の表示] ダイアログ ボックスで証明書情報を確認し、[閉じる] をクリックします。 f. [ホストの承認] ダイアログ ボックスで、[はい] をクリックします。 *セキュア接続認証を使用する*オプションを有効にすると、Unified Manager は認証サーバと通信し、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。
無効にする	a. *安全な接続を使用する*オプションをオフにします。 b. 認証サーバー領域で、[追加] 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。

認証サーバーの構成をテストする

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。

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. *認証テスト*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。

アラートを追加する

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。

開始する前に

- 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、ここで説明する手順に従って[アラート セットアップ]ページで作成できるほか、イベントを受け取ったあとに[イベントの詳細]ページで直接作成することもできます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > アラート設定 をクリックします。
2. アラート設定ページで、[追加]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、アラートの名前と説明を入力します。
4. *リソース*をクリックし、アラートに含めるまたはアラートから除外するリソースを選択します。

   *名前に含まれる*フィールドにテキスト文字列を指定してフィルターを設定し、リソースのグループを選択できます。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名またはイベント重大度タイプに基づいてイベントを選択します。

   

   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. アクション をクリックし、通知するユーザーを選択し、通知頻度を選択し、トラップ受信者に SNMP トラップを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[ユーザ]ページで変更した場合、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. *保存*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: HealthTest
- リソース: 名前に「`abc`」が含まれるすべてのボリュームが含まれ、名前に「`xyz`」が含まれるすべてのボリュームが除外されます
- 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
- アクション: 「sample@domain.com」と「`Test`」スクリプトが含まれており、ユーザーに15分ごとに通知する必要があります。

[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「`abc`」が含まれるボリュームを表示するには、「名前を含む」フィールドに **abc** と入力します。

b. を選択**<<All Volumes whose name contains 'abc'>>** を [使用可能なリソース] 領域から選択し、[選択したリソース] 領域に移動します。

c. *除外*をクリックし、*名前に含まれる*フィールドに*xyz*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から*重大*を選択します。
4. [一致するイベント] 領域から すべての重要なイベント を選択し、[選択したイベント] 領域に移動します。
5. アクション*をクリックし、**[**これらのユーザーに警告**]** フィールドに ***sample@domain.com** と入力します。
6. ユーザーに 15 分ごとに通知するには、[**15** 分ごとに通知] を選択します。

   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. [実行するスクリプトの選択] メニューで、[テスト スクリプト] を選択します。
8. *保存*をクリックします。

著作権に関する情報

商標に関する情報