Unified Manager でアラート通知を送信するための設定

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

目次

Unified Manager でアラート通知を送信するための設定 1
イベント通知を設定しています 1
リモート認証の有効化 2
リモート認証でのネストされたグループの無効化 4
認証サービスをセットアップしています 4
認証サーバを追加しています 5
認証サーバの設定をテストする 7
アラートの追加 7

Unified Manager でアラート通知を送信するための設定

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。

- 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。

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環境を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します"。

   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. "認証サーバを追加します"。

   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. "ユーザを追加します"。

   複数のタイプのローカルユーザまたは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割り当てます。

5. "アラートを追加します"。

   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しています

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 サーバを設定したり、さまざまな通知メカニズムを設定したりできます。たとえば、アラート通知を E メールや SNMP トラップとして送信できます。

- 必要なもの *

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

  メール・アドレスは ' 送信されたアラート通知の送信元フィールドに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は、この E メールアドレスが配信不能メールの受信者としても使用されます。

- SMTP サーバのホスト名、およびサーバにアクセスするためのユーザ名とパスワード
- 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

  複数のトラップ送信先を指定するには、各ホストをカンマで区切ります。この場合、バージョンやアウトバウンドトラップポートなど、他の SNMP 設定はすべてリスト内のすべてのホストで同じでなければなりません。

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、 * 一般 * > * 通知 * をクリックします。
2. 通知ページで、適切な設定を行います。
   - 注： *
     - 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、実際の作業用 E メールアドレスに変更して、すべての E メール通知が正常に配信されるようにしてください。
     - 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（ Save ）] をクリックします。
4. [*Use STARTTLS *]または[*Use SSL *]オプションを選択した場合は、[*Save]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ます。既存の証明書の有効期限が切れた場合は、「* STARTTLSを使用」または「* SSLを使用」チェックボックスをオフにし、通知設定を保存してから「* STARTTLSを使用*」または「SSLを使用*」チェックボックスを再度オンにして新しい証明書を表示します。

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。

- 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。

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	• 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。 ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` （適切なLDAP表記を使用） • 管理者パスワード • ベース識別名（適切な LDAP 表記を使用）
LDAP を開きます	• バインド識別名（適切な LDAP 表記を使用） • バインドパスワード • 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。

4. * オプション： * 認証サーバを追加し、認証をテストします。
5. [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。

- 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。
- 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、 * 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。

- 必要なもの *
- 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	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。

を選択した場合は	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。
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。 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（ 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。

- 必要なもの *
- 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、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	a. [セキュアな接続を使用（ Use Secure Connection * ）] オプションを選択します。 b. [Authentication Servers] 領域で、 [**Add**] をクリックします。 c. 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。 d. [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。 e. [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。 f. [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。 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。
無効にします	a. [セキュアな接続を使用する *] オプションをオフにします。 b. [Authentication Servers] 領域で、 [**Add**] をクリックします。 c. [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。 d. [追加（ Add ）] をクリックします。

追加した認証サーバが Servers 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。

- 必要なもの *
- 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。

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. Test User 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、 * Test * 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。

アラートの追加

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。

- 必要なもの *
- イベント生成時に 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、 Scripts 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、ここで説明するように、 Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [Alert Setup] ページで、 [**Add**] 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、アラートの名前と概要を入力します。
4. [* リソース] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

   [* 次を含む名前（ * Name Contains ）] フィールドでテキスト文字列を指定してフィルタを設定し、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使用可能なリソースのリストに表示されます。指定するテキスト文字列では、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. [*Events] 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の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. [*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、 SNMP トラップをトラップレシーバに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。

   ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとすると、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users 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（ Save ）] をクリックします。

アラートの追加例

この例は、次の要件を満たすアラートを作成する方法を示しています。

- 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を対象に含め、名前に「 xyz 」が含まれるすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを含みます
- アクション：「 + sample@domain.com + 」、「テスト」スクリプトを含み、 15 分ごとにユーザー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. 「 * Name Contains * 」フィールドに「 * abc 」と入力して、「 abc 」という名前のボリュームを表示します。
   b. 「 * + 」を選択します[All Volumes whose name contains 'abc']+* を使用可能なリソース領域から選択したリソース領域に移動します。
   c. [* 除外する *] をクリックし、 [* 名前に * が含まれる *] 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、 **[** イベントの重要度 **]** フィールドから **[** クリティカル *] を選択します。
4. [Matching Events] 領域から [*All Critical Events] を選択し、 [Selected Events] 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. 15 分ごとにユーザに通知するには、「 * 15 分ごとに通知する」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（ Save ）] をクリックします。