テクニカル レポート

# NetApp Active IQ Unified Manager セキュリティ強化ガイド

NetApp
ONTAP TME Team
2023年2月| TR-4943

## 概要

このテクニカルレポートでは、組織が情報システムの機密性、整合性、可用性に関して規定されたセキュリティ目標を達成できるよう、NetApp® Active IQ® Unified Managerのガイダンスと構成設定について説明します。

目次

**はじめに ..... 3**

Active IQ Unified Managerインストールパッケージの整合性の検証 ..... 3

ポートとプロトコル ..... 5

ロールとユーザ ..... 8

Mutual Transport Layer Security（証明書ベースの認証） ..... 10

Active IQ Unified Manager HTTPS証明書 ..... 11

ログインバナー ..... 12

非アクティブ時のタイムアウト ..... 12

APIゲートウェイ ..... 13

スクリプトアップロード ..... 13

ユーザーあたりの最大同時セッション数 ..... 14

レート制限 ..... 14

暗号化設定 ..... 15

証明書ベースのSSHおよびRDPからActive IQ Unified Managerシステムへ ..... 15

SSHフィンガープリントの再生成 ..... 15

ネットワークタイムプロトコルの設定 ..... 15

**追加情報の入手方法 ..... 16**

**バージョン履歴 ..... 16**

表一覧

表1）Active IQ Unified Managerに必要なインバウンドポート ..... 5

表2）Active IQ Unified Managerに必要なアウトバウンドポート ..... 6

表3）アプリケーションユーザのタイプ ..... 8

表4）事前定義されたロールのタイプ ..... 9

図一覧

図1）Windowsでの署名の確認 ..... 3

図2）vAppでの署名の確認 ..... 5

図3）証明書ベースの認証ステータス ..... 10

図4）[Add cluster]ダイアログ ..... 11

図5）ログインバナーの設定 ..... 12

図6）非アクティブ時のタイムアウトの変更 ..... 13

図7）APIゲートウェイ機能の無効化 ..... 13

図8）スクリプトアップロードの無効化 ..... 14

# はじめに

現在、進化を続ける脅威から最も価値のある資産であるデータと情報を保護するため、組織は今までに経験したことのない課題に直面しています。日々進化する脅威や脆弱性はますます洗練され、難読化やスパイ技術も巧妙化しているため、システム管理者にはデータや情報のセキュリティにプロアクティブに対処することが求められています。このガイドは、セキュリティ部門のオペレータや管理者に対し、NetAppソリューションの中核をなす機密性、整合性、可用性を活用した支援を提供することを目的としています。

## Active IQ Unified Managerインストールパッケージの整合性の検証

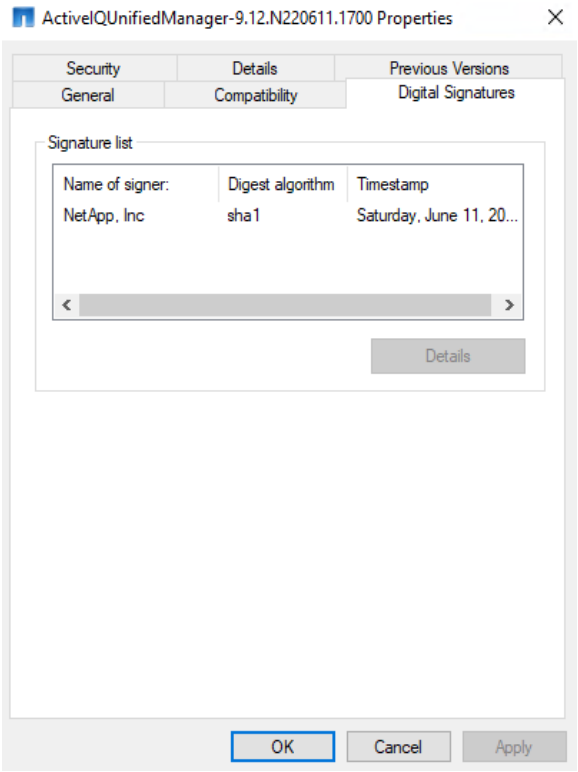
お客様は、2つの方法を使用してActive IQ Unified Managerインストールパッケージの整合性を検証できます。インストールパッケージのチェックサムと署名を確認できます。

チェックサムはActive IQ Unified Managerのダウンロードページにあります。ユーザーは 、ダウンロードしたパッケージのチェックサムを、Active IQ Unified Managerダウンロードページで提供されたチェックサムと照合する必要があります。

### Windowsでの署名の確認

ユーザーは、NetApp Support SiteからダウンロードしたWindowsアプリケーションパッケージの実行可能ファイル（.exe）の署名を必ず確認する必要があります。これを行うには `.exe` 、ファイルを右クリックして**[プロパティ]を開きます。[Open Properties]** ダイアログボックスで **[Digital Signatures]を選択**します。図1に示すように、署名者の名前がNetApp Incとして表示されます。

**図1）Windowsで署名を確認する**



## Red Hat Enterprise Linuxでのシグネチャの確認

コード署名証明書は、Red Hat Enterprise Linux（RHEL）の製品zipと一緒に製品ダウンロードページにあります。コード署名証明書から、ユーザーは次のように公開鍵を抽出できます。

```
#> openssl x509 -pubkey -noout -in netapp_cert.pem > pubkey.pem
```

次に、公開キーを使用して、次のようにRPM製品zipの署名を検証します。

```
#> openssl dgst -sha256 -verify <public key> -signature <signature file> <Binary>
example:
#> openssl dgst -sha256 -verify AIQUM-RHEL-public.key -signature ActiveIQUnifiedManager-
9.12.N220730.0329-el8.zip.sig ActiveIQUnifiedManager-9.12.N220730.0329-el8.zip
Verified OK => response
```

## vAppでの署名の確認

vAppインストールパッケージは、`gzipped` tarファイルの形式で提供されます。このtarファイルには、仮想アプライアンスのルート証明書と中間証明書、READMEファイル、およびOpen Virtualization Appliance（OVA）パッケージが含まれています。OVAファイルを使用してvAppを導入するときは、[Review Details]ページでvAppパッケージのデジタル署名を確認できます。

- ダウンロードしたvAppパッケージが改ざんされていない場合は、**[パブリッシャ]** 列に**[信頼された証明書]と表示されます**。
- ダウンロードしたvAppパッケージが改ざんされている場合は、**[パブリッシャ]** 列に **[無効な証明書]と表示されます**。

指定したルート証明書と中間証明書をVMware vCenterバージョン7.0U3E以降にアップロードする必要があります。vCenterのバージョン7.0.1から7.0.U3Eの場合、証明書を検証する機能はVMwareでサポートされていません。vCenterバージョン6.xの場合、証明書をアップロードする必要はありません。

### 信頼されたルート証明書のvCenterへのアップロード

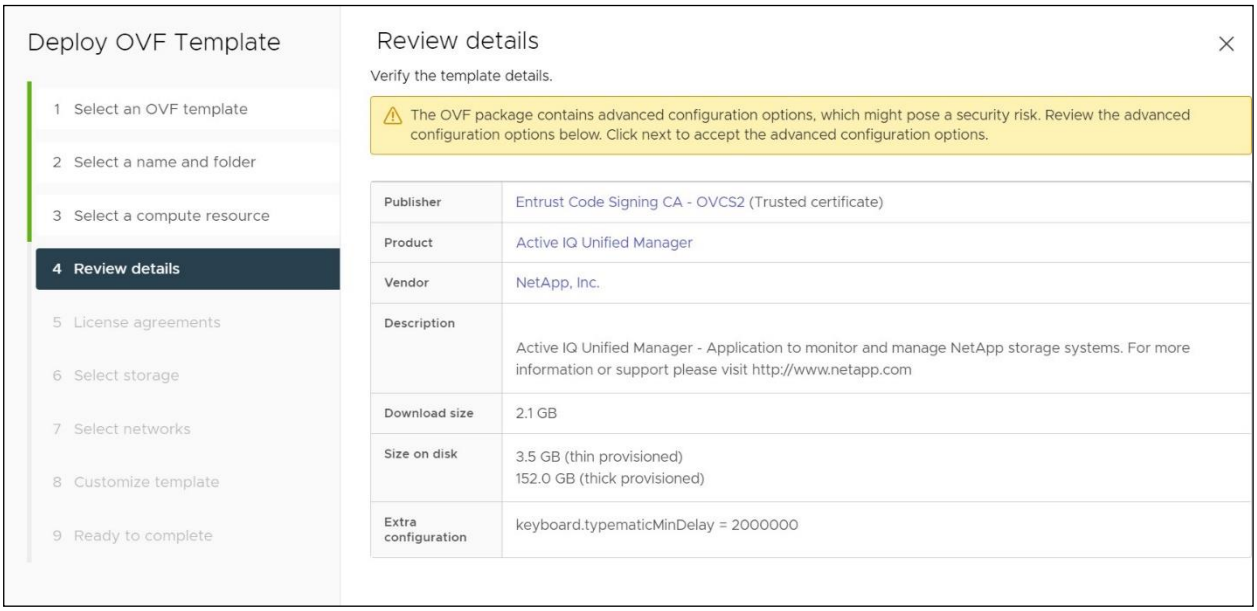
1. VMware vSphere ClientでvCenter Serverにログインします。
2. administrator@vsphere.localまたはvCenter Single Sign-On Administratorsグループの別のメンバーのユーザ名とパスワードを指定します。インストール時に別のドメインを指定した場合は、administrator@mydomainとしてログインします。
3. 証明書管理ユーザーインターフェイスに移動します。
   a. [ホーム]メニューから **[管理]を選択します**。
   b. **[証明書]で、 [証明書管理]をクリックします**。
4. プロンプトが表示されたら、vCenter Serverのクレデンシャルを入力します。
5. **[信頼されたルート証明書]で、 [追加]をクリックし**ます。
6. [browse]をクリックし、証明書 `.pem` ファイルの場所を選択します（`AIQUM-VAPP-INTER-ROOT- CERT.pem`）。
7. **[追加]**をクリックします。

証明書がストアに追加されます。

詳細については、「信頼されたルート証明書を証明書ストアに追加する」を参照してください。

（OVAファイルを使用して）vAppを導入する際に、[Review details]ページでvAppパッケージのデジタル署名を確認できます。ダウンロードしたvAppパッケージが正規のものである場合は、図2に示すように、[パブリッシャ]列に[信頼された証明書]と表示されます。

**図2）vAppでの署名の確認**




# ポートとプロトコル

必要なポートとプロトコルを使用して、クライアントとActive IQ Unified Managerサーバの間、およびActive IQ Unified Managerと管理対象のストレージシステム、サーバ、その他のコンポーネントの間の通信を行うことができます。

## Active IQ Unified Managerに必要なインバウンドポートとアウトバウンドポート

表1 に、Active IQ Unified Managerに必要なインバウンドポートとアウトバウンドポートを示します。表1 および 表2 にリストされているポートだけが、リモートマシンからの接続用に開いている必要があります。他のすべてのポートは、リモートマシンからの接続に対して無効にする必要があります。

**表1）Active IQ Unified Managerに必要なインバウンドポート**

| インターフェイス | プロトコル | ポート |
|---|---|---|
| Unified Managerユーザインターフェイス | HTTP | 80 * |
| APIを使用するUnified Managerユーザインターフェイスとプログラム | HTTPS | 443 * |
| メンテナンス コンソール | セキュアシェル（SSH）/ SFTP | 22 |
| Linuxコマンドライン | SSH / SFTP | 22 |
| syslog | UDP | 514 |
| MySQLデータベース | MySQL | 3306 ** |

*デフォルトのポートはインストール後に変更できます。

**デフォルトでは、MySQLポート3306はlocalhostからの接続に対してのみ開かれています。Active IQ Unified ManagerとOnCommand Workflow Automation（WFA）を統合する場合やデータベースへのリモート接続を行う場合は、リモートマシンからの接続用にポート3306を開いておく必要があります。表2 に、Active IQ Unified Managerが必要とするアウトバウンドポートを示します。

**表2）Active IQ Unified Managerに必要なアウトバウンドポート**

| デスティネーション | プロトコル | ポート |
|---|---|---|
| ストレージ システム | HTTPS | 443 / TCP |
| ストレージ システム | NDMP | 10000 / TCP |
| AutoSupportサーバ | HTTPS | 443 |
| 認証サーバ | LDAP | 389 |
| 認証サーバ | LDAPS | 636 |
| メール サーバ | SMTP | 25 |

## HTTPオヨヒHTTPSホオトノヘンコウ

デフォルトでは、Active IQ Unified Managerサービスはデフォルトの**HTTP**ポートと**HTTPS**ポート**80**と**443**をそれぞれ使用します。

**ベスト プラクティス**

これらのサービスは、デフォルト以外のポートおよび非特権ポート（**1024**より大きいポート番号）で実行することを推奨します。**HTTP**ポートと**HTTPS**ポートは、メンテナンスコンソールから次のように変更できます。

```
 [root@server bin]# maintenance_console
Active IQ Unified Manager Maintenance Console
Version: 9.12.N220531.1701-2205311701
System ID: dc006e8a-9273-4d61-870e-b76982afcb37
Status: Running
Main Menu

1 ) Support/Diagnostics
2 ) Reset Server Certificate
3 ) Backup Restore
4 ) External Data Provider
5 ) Performance Polling Interval Configuration
6 ) Disable SAML authentication
7 ) View/Change Application Ports
8 ) Debug Log Configuration
9 ) Control access to MySQL port 3306
x ) Exit
Enter your choice: 7
Maintenance console requires username & password to perform this
operation, enter administrator username & password when prompted.

Enter username: umadmin
Enter password:
Below are the application ports that can be changed, and their current values:
HTTP communication: 80
HTTPS communication: 443
Do you want to change the ports? (y/n): y
HTTP Port (Not specifying anything will set it to default 80): 7777
HTTPS Port (Not specifying anything will set it to default 443): 9999
This action will restart Active IQ Unified Manager.
Are you sure you want to change the application ports and restart Active IQ Unified Manager now?
(y/n): y
Stopping service 'Active IQ Unified Manager acquisition unit'
Stopped 'Active IQ Unified Manager acquisition unit' successfully
Stopping service 'Active IQ Unified Manager'
Stopped 'Active IQ Unified Manager' successfully
Starting service 'Active IQ Unified Manager'
Started 'Active IQ Unified Manager' successfully
Starting service 'Active IQ Unified Manager acquisition unit'
Started 'Active IQ Unified Manager acquisition unit' successfully
Active IQ Unified Manager service restart succeeded
```

```
The application ports have been changed successfully
Exit out of the maintenance console and then log back in
Press any key to continue.
Active IQ Unified Manager Maintenance Console
Version: 9.12.N220531.1701-2205311701
System ID: dc006e8a-9273-4d61-870e-b76982afcb37
Status: Running
```

## MySQLポート3306へのリモートアクセスの制御

デフォルトでは、MySQLポート3306にはlocalhostからのみアクセスできます。MySQLポートは、Active IQ Unified ManagerとWFAを統合する場合、またはActive IQ Unified Managerデータベースにリモートでアクセスする必要がある場合にのみ、リモート接続用に開いておく必要があります。

### ベスト プラクティス

リモート接続用にMySQLポートを閉じておくことは、セキュリティ上のベストプラクティスです。
RHELおよびvAppでは、メンテナンスコンソールから次のように変更できます。

```
[root@aiqum ~]# /opt/netapp/ocum/bin/maintenance_console
Active IQ Unified Manager Maintenance Console
Version : 9.12.N220531.1701-2205311701
System ID : dc006e8a-9273-4d61-870e-b76982afcb37
Status : Running
Main Menu
```

```
1 ) Support/Diagnostics
```

```
2 ) Reset Server Certificate
3 ) Backup Restore
4 ) External Data Provider
5 ) Performance Polling Interval Configuration
6 ) Disable SAML authentication
7 ) View/Change Application Ports
8 ) Debug Log Configuration
9 ) Control access to MySQL port 3306
x ) Exit
Enter your choice: 9
Maintenance console requires username & password to perform this
operation, enter administrator username & password when prompted.

Enter username: umadmin
Enter password:
The MySQL port 3306 is currently accessible only by localhost.
Do you wish to enable access to everyone? (y/n): y

The MySQL port 3306 is now accessible by everyone.
Active IQ Unified Manager Maintenance Console
Version : 9.12.N220531.1701-2205311701
System ID : dc006e8a-9273-4d61-870e-b76982afcb37
Status : Running
Main Menu
```

```
1 ) Support/Diagnostics
```

```
2 ) Reset Server Certificate
3 ) Backup Restore
4 ) External Data Provider
5 ) Performance Polling Interval Configuration
6 ) Disable SAML authentication
7 ) View/Change Application Ports
8 ) Debug Log Configuration
9 ) Control access to MySQL port 3306
x ) Exit
Enter your choice: x
[root@aiqum ~]#
```

**注：** Windowsプラットフォームで、ファイアウォールを有効にしてMySQLポート3306へのアクセスを制限します。ネットワーク環境に応じて、適切なファイアウォールとネットワーク設定（パブリック、プライベート、またはネットワーク）をオンにします。

## ロールとユーザ

Active IQ Unified Managerインストールでは、次の3種類のユーザが作成され、使用されます。

- システムユーザ
- アプリケーションユーザ（ローカルユーザなど）
- MySQLユーザまたはデータベースユーザ

### システムユーザ

システムユーザとは、基盤となるオペレーティングシステムにActive IQ Unified Managerをインストールすることで作成されるユーザです。

- `umadmin` RHELまたはCentOSでは、Active IQ Unified Managerのインストールによってデフォルトのシステムユーザが作成されます。このユーザはメンテナンスユーザで、メンテナンスコンソールスクリプトを実行するために作成されます。
- vAppでも同様のシステムユーザが作成されます。このユーザのクレデンシャルは、vAppを導入するユーザが入力します。メンテナンスユーザで、メンテナンスコンソールスクリプトを実行するために作成されます。
- `jboss` Active IQ Unified Managerサービスを実行するために、RHELおよびvAppでシステムユーザを作成します。この `jboss` ユーザには、Active IQ Unified Managerサービスを実行するためのRHELおよびvAppに対する権限が制限されています。
- `jboss` RHEL、CentOS、vAppのメンテナンスユーザとメンテナンスユーザには、いくつかのスクリプトをrootとして実行する権限があります。メンテナンスユーザと `jboss` ユーザのこれらの権限は `/etc/sudoers.d/ocum_sudoers`、ファイルと `/etc/sudoers.d/ocie_sudoers` ファイルで定義されます。
- ファイル`/etc/sudoers.d/ocum_sudoers` とは `/etc/sudoers.d/ocie_sudoers`、Active IQ Unified Managerのインストール時に作成されます。これらのファイルはrootによって所有され、rootユーザに対する読み取り権限のみを持ちます。これらのファイルの権限は変更しないでください。
- Windowsでは、Active IQ Unified Managerのインストールによってシステムユーザが作成されることはありません。Windows上のActive IQ Unified Managerサービスは、ローカルシステムアカウントとして実行されます。ローカルシステムアカウントは、Windows OSで最も高い権限を持ちます。

  **注：** Windowsシステムでは、Unified Managerをインストールする前に管理者権限を持つ新しいユーザを作成してください。

### アプリケーションユーザ

Active IQ Unified Managerでは、アプリケーションユーザの名前はローカルユーザです。これらは、Active IQ Unified Managerアプリケーションで作成されたユーザです。表3 に、アプリケーションユーザのタイプを示します。

**表3）アプリケーションユーザのタイプ**

| ユーザ | 説明 |
|---|---|
| メンテナンス ユーザ | Unified Managerの初期設定時に作成されます。メンテナンスユーザは、追加のユーザを作成してロールを割り当てます。Unified ManagerはRHELシステムまたはCentOSシステムにインストールします。maintenanceユーザにはユーザ名 `umadmin` が割り当てられ、デフォルトのパスワードが設定されます。 ユーザは、Active IQ Unified Managerの使用を開始する前にこのパスワードを変更する必要があります。これは、デフォルトで作成される唯一のアプリケーションユーザです。 |
| ローカル ユーザ | メンテナンスユーザまたはアプリケーション管理者ロールを持つユーザから割り当てられたロールに基づいて機能を実行します。 |

| ユーザ | 説明 |
| --- | --- |
| リモート グループ | 認証サーバに保存されているクレデンシャルを使用してUnified Managerのユーザインターフェイスにアクセスするユーザのグループ。リモートグループのユーザは、各自のユーザクレデンシャルを使用してUnified Managerのユーザインターフェイスにアクセスできます。 |
| リモート ユーザ | 認証サーバに保存されているクレデンシャルを使用してUnified Managerのユーザインターフェイスにアクセスします。 |
| データベース ユーザ | Unified Managerデータベースのデータへの読み取り専用アクセスが許可されます。Unified Managerのユーザインターフェイスやメンテナンスコンソールにはアクセスできず、API呼び出しも実行できません。データベースユーザには、次の2つのロールが関連付けられています。<br>• 統合スキーマ<br>• レポート スキーマ |

ローカルユーザ（アプリケーションユーザ）には、ロールが関連付けられています。表4 に、Active IQ Unified Managerでローカルユーザに使用できるロールを示します。

### ロール

ロールベースアクセス制御（RBAC）を使用すると、Active IQ Unified Managerのさまざまな機能やリソースにアクセスするユーザを制御できます。Active IQ Unified ManagerのRBAC解決策では、ユーザの管理アクセスが、定義されたロールに許可されたレベルに制限されます。これにより、管理者は、割り当てられたロールでローカルユーザを管理できます。ローカルユーザアカウントは静的であり、割り当てられているロールを変更することはできません。表4 に、Active IQ Unified Managerの事前定義されたロールを示します。

**表4）事前定義されたロールのタイプ**

| ロール | 説明 |
| --- | --- |
| 演算子 | ストレージシステムの情報やUnified Managerで収集されたその他のデータ（履歴や容量のトレンドなど）を表示できます。このロールでは、ストレージオペレータはイベントの表示、割り当て、確認応答、解決、メモの追加を行うことができます。 |
| ストレージ管理者 | Unified Managerでのストレージ管理処理を設定します。このロールにより、ストレージ管理者はしきい値を設定したり、アラートやその他のストレージ管理に固有のオプションやポリシーを作成したりできます。 |
| アプリケーション管理者 | ストレージ管理とは関係のない設定を行います。ユーザ、セキュリティ証明書、データベースアクセス、および管理オプション（認証、 SMTP、ネットワーク、およびAutoSupport。 |
| 統合スキーマ | Unified ManagerとOnCommand Workflow Automation（WFA）の統合用にUnified Managerのデータベース ビューにアクセスするための読み取り専用アクセスが許可されます。このロールのユーザはMySQLデータベース内に作成されるため、データベースユーザになります。 |

## ユーザタイプ

ユーザタイプは、ユーザがActive IQ Unified Managerに持っているアカウントの種類を指定します。これらのタイプにはそれぞれ独自のロールがあり、Administratorロールを持つユーザによって割り当てられます。Active IQ Unified Managerローカルユーザには、アプリケーション管理者、ストレージ管理者、オペレータの3つのロールがあります。表4 に、これらのロールの説明を示します。

**ベスト プラクティス**

セキュリティのベストプラクティスとして、最小権限の原則を使用してユーザのロールを選択することを推奨します。

統合スキーマロールとレポートスキーマロールを持つユーザは、MySQLデータベースに作成されます。これらのユーザはデータベースユーザと呼ばれます。これらのユーザーは、リモートマシンからの接続用に

MySQLポートが開いている場合、リモートマシンからMySQLデータベースに接続できます。これらのユーザを作成する必要はありません。必要な場合にのみ作成してください。

## Active IQ Unified Managerアプリケーションユーザのロックとロック解除

非アクティブなユーザーアカウントは、組織にセキュリティリスクをもたらします。非アクティブなアカウントは、悪意のある攻撃者がリソースにアクセスする機会を提供します。Active IQ Unified Managerには、ユーザーアカウントをロックまたはロック解除する機能があります。非アクティブなユーザーアカウントはロックする必要があります。アプリケーション管理者ロールを持つユーザは、アカウントをロックまたはロック解除できます。

ユーザーアカウントをロックまたはロック解除するには、 左側のメニューで「設定」>「一般」を開き、**「ユーザー」を選択します**。[Users]ページには、ユーザアカウントをロックまたはロック解除するオプションがあります。

## Mutual Transport Layer Security（証明書ベースの認証）

ONTAP ONTAP 9.12以降では、Active IQ Unified Manager 9.12で追加された新しいクラスタのONTAPとの通信に相互のTransport Layer Security（TLS）が使用されます。以前のバージョンのActive IQ Unified Managerからアップグレードした場合は、クラスタのプロパティを編集して相互TLSを有効にできます。

図3 に示すように、[Cluster Setup]ページには、各クラスタに設定されているMutual Transport Layer Security（MTLS；相互トランスポートレイヤセキュリティ）のステータスが表示されます。

**図3）証明書ベースの認証ステータス**

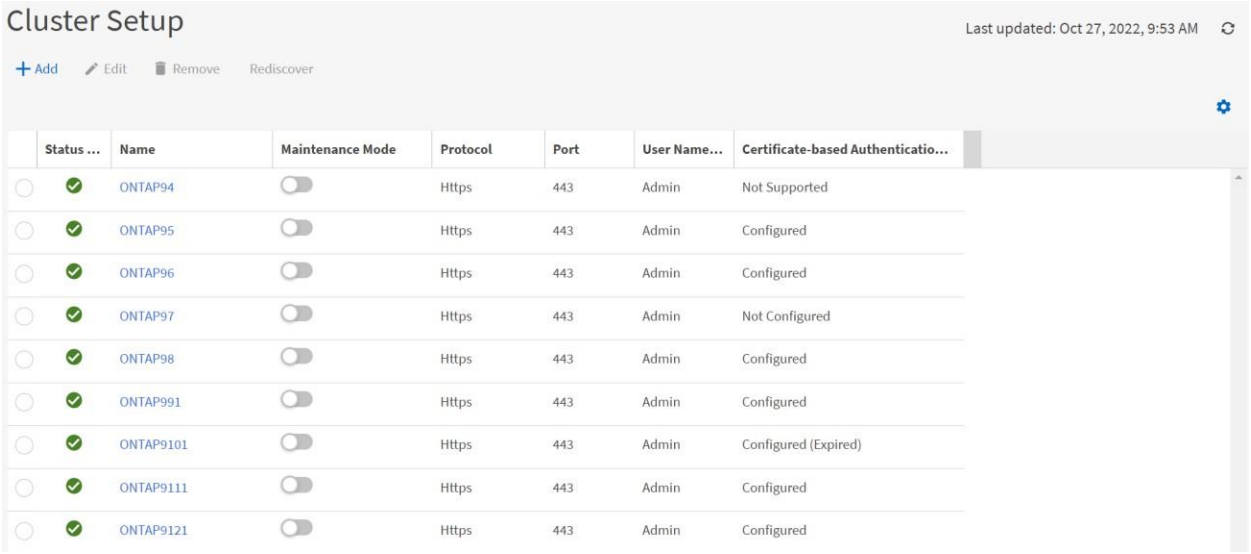


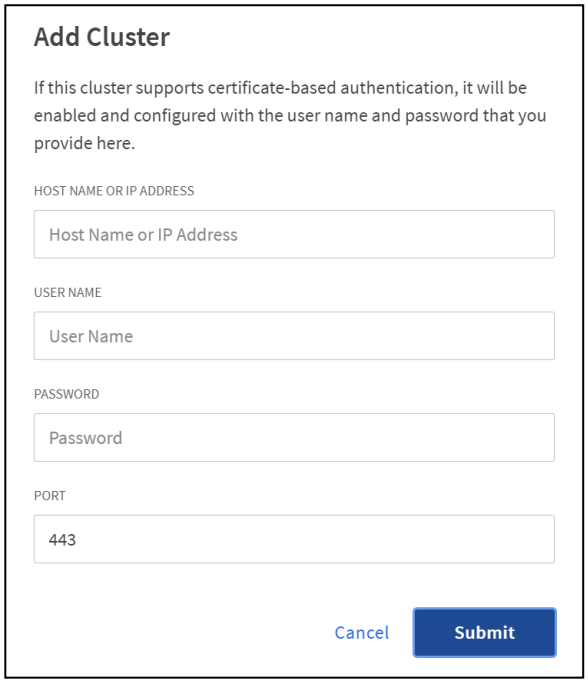

図3 は、証明書ベースの認証の4つの異なるステータスを示しています。

- **設定済み。**MTLSが設定され、Active IQ Unified ManagerとONTAP間の認証に使用されます。
- **設定されていません。**これは、ユーザが以前のバージョンのActive IQ Unified Managerからアップグレードし、このクラスタにMTLSが設定されていない場合に発生します。これは、クラスタのプロパティを編集することで設定できます。
- **サポート対象外**ONTAP 9.5より前のバージョンで、MTLSはサポートされません。
- **設定済み（期限切れ）。**MTLSの証明書の有効期限が切れています。

### クラスタの追加

クラスタ追加ワークフローで、追加するクラスタがMTLSをサポートしている場合、MTLSはデフォルトで設定されます。設定は必要ありません。図4 は、クラスタ追加オプションのスクリーンショットです。

**図4）[Add cluster]ダイアログ**




## クラスタの編集

クラスタ編集処理中に、3種類の画面が表示されることがあります。これは、MTLSが有効になっているか、ONTAPクラスタでサポートされているかによって異なります。

- **MTLSがサポートされ、有効になります。**送信ボタンをクリックしても、MTLSの変更は必要ありません。
- **MTLSはサポートされていますが、イネーブル**この場合、送信ボタンをクリックすると、MTLSがイネーブルになります。
- **MTLSはサポートされていません。**[Submit]ボタンをクリックしても、MTLSを変更する必要はありません。

## Active IQ Unified Manager HTTPS証明書

デフォルトでは、Active IQ Unified Managerは、ユーザインターフェイスへのHTTPSアクセスを保護するために、インストール時に自動的に作成される自己署名証明書を使用します。Active IQ Unified Managerには次の機能があります。

- HTTPS証明書署名要求のダウンロード
- HTTPS証明書のインストール
- HTTPS証明書の再生成

前のオプションにアクセスするには、左側のペインで **[Settings] > [General]>[HTTPS Certificate]**の順に選択します。これらの機能を使用すると、HTTPS証明書署名要求をダウンロードできます。CAによって署名された証明書は、**[HTTPS証明書のインストール ]**オプションを使用してActive IQ Unified Managerサーバにインストールできます。インストール時に生成された自己署名証明書を変更するには、[HTTPS証明書の再生成]オプションを使用します。これは、証明書署名要求を作成する前にも実行できます。

**ベスト プラクティス**

セキュリティに関するベストプラクティスとして、Active IQ Unified ManagerサーバにはCA署名証明書を使用することが推奨されます。必要な手順については、「Active IQ Unified Manager用の署名済み証明書を生成して変換する方法」を参照してください。

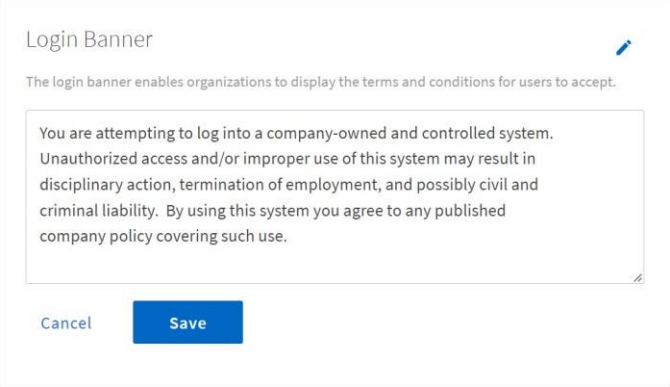
## ログインバナー

ログインバナーは、Active IQ Unified Managerユーザインターフェイスにログインすると表示されます。ログインバナーを使用すると、組織はユーザーの利用規約を表示できます。

**ベスト プラクティス**

デフォルトでは、ログインバナーは空に設定されています。セキュリティに関するベストプラクティスとして、ログインバナーを設定することを推奨します。ログインバナーを設定するには、図5に示すように、[Settings]>[General]>[Feature Settings]と[Log-in Banner]の順に選択します。

**図5）ログインバナーの設定**




## 非アクティブ時のタイムアウト

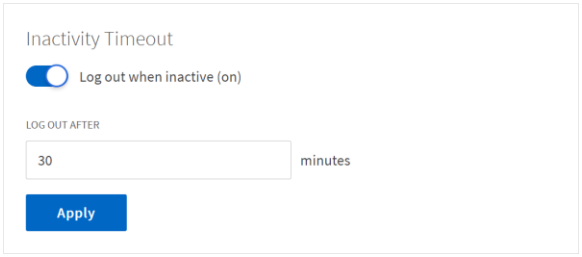
Unified Managerのユーザインターフェイスにはタイムアウトが設定され、指定した非アクティブな時間が経過した時点でログアウトしてセッションを閉じます。このオプションはデフォルトで有効になります。

**ベスト プラクティス**

Active IQ Unified Managerのユーザインターフェイスでの非アクティブ時のデフォルトのタイムアウトは3日間です。これを30分以下に短縮することは、セキュリティのベストプラクティスです。

非アクティブ時のタイムアウトを変更するには、**[設定] > [全般]>[機能設定]に移動し、**非アクティブ時のタイムアウトを分単位で変更して、**[適用]** ボタンをクリックします。

**図6）非アクティブ時のタイムアウトの変更**



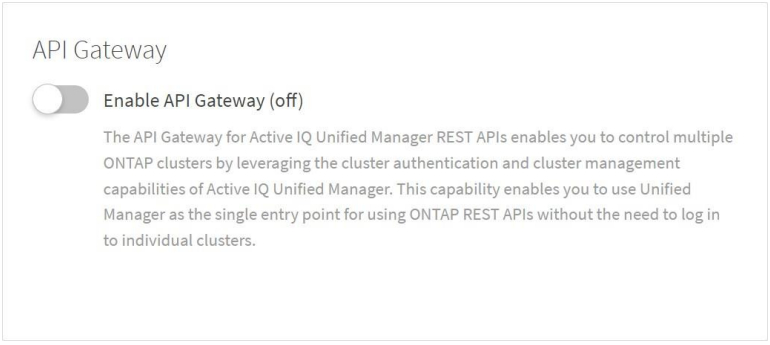

## API ゲートウェイ

Active IQ Unified ManagerのAPIゲートウェイ機能を使用すると、ONTAPクラスタに直接ログインせずにクラスタのONTAP REST APIを使用できます。代わりに、Unified Manager REST APIを使用して、Unified Managerに格納されているクレデンシャルを使用してONTAPクラスタにAPI要求を転送します。

**ベスト プラクティス**

Active IQ Unified ManagerでAPIゲートウェイ機能を使用しない場合は、無効にする必要があります。APIゲートウェイを無効にするには、**[設定] >[ 全般]> [機能設定]** に移動し、[APIゲートウェイの有効化]を **[オフ]に切り替え**ます。

**図7）APIゲートウェイ機能の無効化**



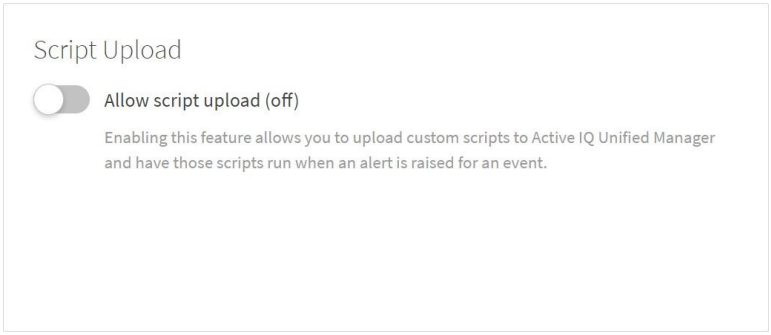

## スクリプトアップロード

Active IQ Unified Managerを使用すると、アラートアクションとしてカスタムスクリプトを実行できます。

**ベスト プラクティス**

セキュリティ上のベストプラクティスとして、スクリプトアップロード機能を使用していない場合は無効にして、**[設定] >[ 全般]> [機能設定]** に移動し、[スクリプトアップロード]をオフにしてください。図8を参照してください。

**図8）スクリプトアップロードの無効化**




## ユーザあたりの最大同時セッション数

デフォルトでは、ユーザあたりの最大同時セッション数は100です。Active IQ Unified Managerのアプリケーション管理者ロールを持つユーザは、環境の要件に応じてこの値を変更できます。

**ベストプラクティス**

セキュリティ上のベストプラクティスでは、最大同時セッション数を低くすることが推奨されます。これは、高い値を設定すると、DOS攻撃や分散型サービス拒否（DDoS）攻撃のメカニズムが提供されるためです。

次のコマンドを実行して、最大同時セッション数を変更します。

```
# um option list maximum.concurrent.user.session
Name Default Value Value Requires Restart
--------------------------------------------------------------------------------
maximum.concurrent.user.session 100 100 true
# um option set maximum.concurrent.user.session=500
Changed maximum.concurrent.user.session to 500.

# um option list maximum.concurrent.user.session
Name Default Value Value Requires Restart
--------------------------------------------------------------------------------
maximum.concurrent.user.session 100 500 true
```

## レート制限

レート制限は、DOSおよびDDoS攻撃に対するメカニズムを提供します。OSファイアウォールを介した新しい接続の送信元IPアドレスごとにレート制限を設定できるため、悪意のある攻撃の影響を軽減できます。

### RHEL

RHELでは、iptablesコマンドを使用してレートリミッタを設定できます。次のコマンドは、1秒あたりの「n」要求で新しい接続をレート制限するために使用します。

```
iptables -A INPUT -m conntrack --ctstate NEW -m hashlimit --hashlimit-above 10/sec --hashlimit-
burst 5 --hashlimit-mode srcip --hashlimit-name conn-rate-limit -j DROP
```

### iptablesコマンドの使用

このシステムでは、一意の送信元IPに対して、1秒間に平均10個の要求が許可され、最初のバーストとして5個の要求が許可されます。しきい値を超える要求はドロップされます。

### vApp

vAppでは、レートリミッタが設定されたIPテーブルは、デフォルトで1秒あたり10リクエストに事前に設定されています。変更する必要がある場合は、診断シェルを使用してvAppにログインし、NetAppナレッジベースの記事「How to update rate limit in vApp of Active IQ Unified Manager」の手順に従います。

**注：** 診断シェルではOSレベルのコマンドを実行できます。テクニカルサポートから指示があった場合にのみ使用してください。

### Windows

Windowsでは、ファイアウォールのレート制限機能はサポートされていません。送信元IPごとにレートリミッタを設定するには、サードパーティ製ツールをインストールする必要があります。

## 暗号化設定

Active IQ Unified Managerで使用されるデフォルトの暗号の一部を無効にすることができます。これを行うには 、Active IQ Unified Managerインターフェイスで[Settings]>[General]>[Manage HTTPS cipher suites]に移動します。ただし、NetAppでは、すべてのブラウザでユーザインターフェイスを最適にサポートするために、すべてのデフォルト暗号をサポートすることを推奨しています。

## 証明書ベースのSSHおよびRDPからActive IQ Unified Managerシステムへ

Active IQ Unified Managerがインストールされているマシンには、証明書ベースのSSHまたはリモートデスクトッププロトコル（RDP）を使用してログインすることを推奨します。

- **[Windows]をクリックします。**Active IQ Unified ManagerをWindowsマシンにインストールした場合は、証明書ベースのRDPを使用してセキュリティを強化する必要があります。「リモートデスクトップサービスでの証明書の使用」のMicrosoftの指示に従って、証明書ベースのRDPをWindowsマシンに設定します。
- **vApp：**Active IQ Unified Managerメンテナンスユーザは、SSHを使用してvAppにログインできます。お客様は、証明書ベースのSSHをActive IQ Unified Manager vAppに設定してセキュリティを強化できます。証明書ベースのSSHを設定するには、「Active IQ Unified Manager仮想マシン（OVA）DIAGシェルへのアクセス方法」の手順に従ってDIAGシェルにログインする必要があります。DIAGシェルのコマンドはすべてsudoを使用して実行する必要があります。実行しないと、Permission-denied問題がヒットします。vAppで証明書ベースのSSHを設定するには、Debianのドキュメントに従ってください。

  vAppの場合、SSHを使用してログインできるユーザ（メンテナンスユーザ）は1人だけです。証明書ベースのSSHの設定には注意が必要です。SSHの設定を誤ると、vAppからロックアウトされる可能性があります。
- **RHEL / CentOS：**rootユーザやその他のシステムユーザは、Active IQ Unified Manager関連の処理や通常のシステムメンテナンスや運用を実行するためにRHELシステムにログインできます。Linuxマシンでは、証明書ベースのSSHを使用することを推奨します。RHELで証明書ベースのSSHを設定するには、OpenSSH証明書認証を使用したRHELのドキュメントに従ってください。

## SSHフィンガープリントの再生成

証明書は有効期限が切れますが、パスワードベースのSSHを使用している場合は、SSHフィンガープリントを定期的に再生成する必要があります。SSHフィンガープリントを再生成する方法については、Debian、RHEL、CentOSのドキュメントを参照してください。

## ネットワークタイムプロトコルの設定

ネットワークタイムプロトコル（NTP）のネットワーク時間が同期していないと、原因のセキュリティ上の問題が発生することがあります。

### vApp

NTPサーバは `maintenance_console`、vAppのから設定できます。

デフォルトでは、NTPのサービスはvAppのNTPDです。これはレガシーサービスであり、場合によっては仮想マシンでは適切に機能しません。`systemd-timesyncd` NTPのサービスに切り替えることができます。

`Systemd-timesyncd` は、NTPのクライアント専用軽量実装です。ユーザは `systemd-timesyncd`、メンテナンスコンソールから **[System Config]**、**[Change NTP Service]オプションの順に選択してに切り替えることができます。**

### RHELおよびWindows

OSの標準手順とベストプラクティスに従ってNTPサービスを設定します。

RHELでは、NTPサービスにchronyを使用できます。これにより、従来のNTPDサービスに比べて多くの点が改善されています。

# 詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- Active IQ Unified Managerのドキュメント
  https://docs.netapp.com/us-en/active-iq-unified-manager/
- Active IQ Unified Managerのリソース
  https://www.netapp.com/support-and-training/documentation/active-iq-unified-manager/

# バージョン履歴

| バージョン | 日付 | ドキュメントの改訂履歴 |
|---|---|---|
| バージョン1.0 | 2022年11月 | ドキュメント初版リリース |
| バージョン1.1 | 2023年1月 | インストール前に新しいWindowsユーザを追加するための新しい注意事項。 |
| バージョン1.2 | 2023年2月 | MySQLポート3306へのアクセスを制限するための注意を追加しました。 |

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

**機械翻訳に関する免責事項**

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

**著作権に関する情報**



**商標に関する情報**



TR-4943-0123-JP