Fsas Technologies

C140-0128-02Z3

ETERNUS AX series オールフラッシュアレイ，ETERNUS AC series オールフラッシュアレイ，ETERNUS HX series ハイブリッドアレイ

Active IQ Unified Manager セキュリティ強化ガイド

目次

図目次

表目次

はじめに

本書では、Active IQ Unified Manager のガイダンスと設定について説明し、情報システムの機密性、整合性、および可用性に関する規定のセキュリティ目標を組織が達成できるように補助します。

第 2 版
2025 年 3 月

登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/
本書では、本文中の™、® などの記号は省略しています。

本書の読み方

対象読者

本書は、ETERNUS AX/AC/HX series の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

関連マニュアル

ETERNUS AX/AC/HX series に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

本書の表記について

本文中の記号

本文中では、以下の記号を使用しています。

注意	お使いになるときに注意していただきたいことを記述しています。必ずお読みください。
備考	本文を補足する内容や、参考情報を記述しています。

1. 本製品について

現在の脅威の様相が変化すると、最も重要な資産であるデータと情報を保護するための固有の課題に直面することになります。私たちが目の当たりにしている高度でダイナミックな脅威や脆弱性は、ますます複雑化していきます。システム管理者は、難読化の有効性および潜在的な侵入者側の偵察技術の向上と相まって、積極的な方法でデータと情報のセキュリティに対処する必要があります。本書では、ソリューションに不可欠な機密性、整合性、可用性について、そのタスクの運用担当者と管理者を支援します。

1.1 Active IQ Unified Manager インストールパッケージの整合性の確認

Active IQ Unified Manager インストールパッケージの整合性を確認するには、2 つの方法があります。インストールパッケージのチェックサムと署名から整合性を確認することができます。

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、FTI (Fsas Technologies Inc.) のダウンロードサイトで提供されているチェックサムと照合する必要があります。

1.1.1 Windows での署名の確認

FTI ダウンロードサイトから Windows アプリケーションパッケージの実行可能ファイル (.exe) をダウンロードした後は、署名を必ず確認してください。これを行うには、.exe ファイルを右クリックし、[プロパティ] を開きます。[プロパティ] ダイアログボックスで、[デジタル署名] を選択します。署名者名に Fsas Technologies Inc. が表示されていることを確認してください (図 1.1 を参照)。

図 1.1 Windows での署名の確認

1.1.2 Red Hat Enterprise Linux での署名の確認

Red Hat Enterprise Linux (RHEL) の製品 zip とともに、製品のダウンロードページにコード署名証明書があります。コード署名証明書から、ユーザーは以下のように公開鍵を抽出できます。

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

続いて、以下のように公開鍵を使用して 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
```

1.1.3 vApp での署名の確認

vApp インストールパッケージは、gzip 形式で圧縮された tar ファイルとして提供されます。この tar ファイルには、README ファイルおよびオープン仮想アプライアンス (OVA) パッケージとともに、仮想アプライアンスのルート / 中間証明書が含まれています。OVA ファイルを使用して vApp を展開するときに、vApp パッケージのデジタル署名を「Review details」ページで確認することができます。

- ダウンロードした vApp パッケージに改ざんがなければ、[Publisher] 列に [Trusted certificate] 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、[Publisher] 列に [Invalid certificate] と表示されます。

提供されたルート / 中間証明書を VMware vCenter のバージョン 7.0 Update 3e 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 Update 1 から 7.0 Update 3e 未満では、証明書を確認する機能が VMware でサポートされていません。なお、vCenter のバージョン 6.x では、証明書をアップロードする必要はありません。

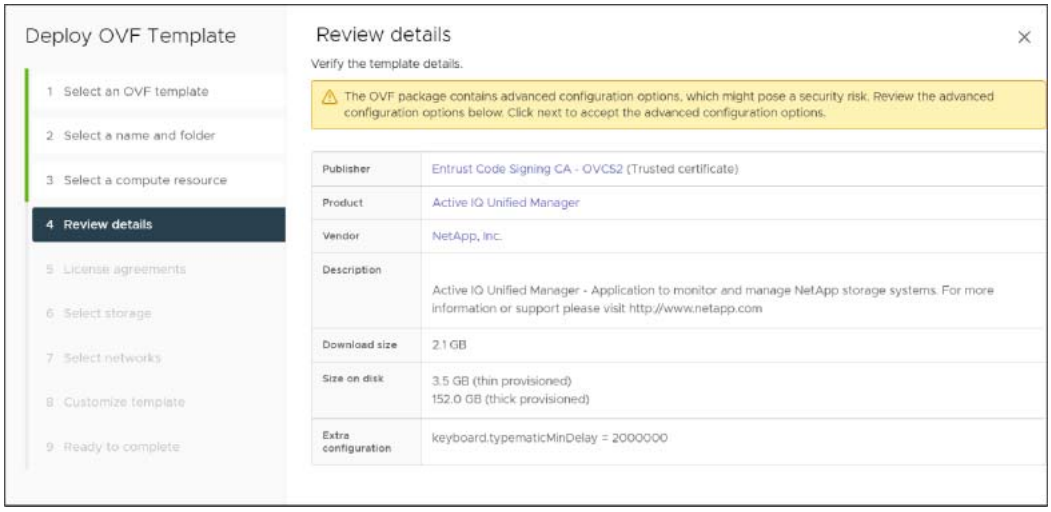
信頼されたルート証明書の vCenter へのアップロード

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 管理者グループの別メンバーのユーザー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. [証明書の管理] ユーザーインターフェイスに移動します。
   - 3-1 [ホーム] メニューから [管理] を選択します。
   - 3-2 [証明書] で、[証明書の管理] をクリックします。
4. プロンプトが表示されたら、vCenter Server の認証情報を入力します。
5. [信頼できるルート証明書] で、[追加] をクリックします。
6. [参照] をクリックし、証明書の .pem ファイル (AIQUM-VAPP-INTER-ROOT-CERT.pem) の場所を選択します。
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。

詳細は、「証明書ストアへの信頼できるルート証明書の追加」を参照してください。

OVA ファイルを使用した vApp の展開時に、vApp パッケージのデジタル署名を [Review details] ページで確認することができます。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、[Publisher] 列に [Trusted certificate] と表示されます (図 1.2 を参照)。

図 1.2 vApp での署名の確認



1.2 ポートとプロトコル

必須ポートとプロトコルにより、クライアントと Active IQ Unified Manager サーバ間、および Active IQ Unified Manager と管理対象ストレージシステム、サーバ、その他のコンポーネント間の通信が可能になります。

1.2.1 Active IQ Unified Manager に必要なインバウンドポートおよびアウトバウンドポート

表 1.1 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 1.1 および表 1.2 に記載のポートのみ、リモート装置からの接続を有効にしてください。それ以外のすべてのポートは、リモート装置からの接続を無効にする必要があります。

表 1.1 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 ユーザーインターフェイス	HTTP	80 (*1)
API を使用した Unified Manager ユーザーインターフェイスとプログラム	HTTPS	443 (*1)
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 (*2)

*1: デフォルトのポートは、インストール後に変更できます。

*2: デフォルトでは、MySQL ポート 3306 は localhost からの接続のみ有効になっています。Active IQ Unified Manager を OnCommand Workflow Automation (WFA) と統合する場合、またはデータベースへのリモート接続が必要な場合にのみ、リモート装置からの接続に対してポート 3306 を有効にするようにしてください。表 1.2 に、Active IQ Unified Manager に必要なアウトバウンドポートを示します。

表 1.2　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

1.2.2　HTTP および HTTPS ポートの変更

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 80 と HTTPS ポート 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 (ポート番号が 1024 より大きいポート) で実行することを推奨します。HTTP および HTTPS ポートは、メンテナンスコンソールから以下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
```

1.2.3 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。Active IQ Unified Manager を WFA と統合する場合、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、リモート接続に対して MySQL ポートを有効にする必要があります。

- **ベストプラクティス**

  リモート接続に対して MySQL ポートを無効にすることが、セキュリティ上のベストプラクティスとなります。RHEL および vApp では、メンテナンスコンソールから以下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 ~]#
```

備考

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) を有効にします。

1.3 ロールとユーザー

Active IQ Unified Manager のインストールでは、以下の 3 種類のユーザーが作成および使用されます。

- システムユーザー
- ローカルユーザーなどのアプリケーションユーザー
- MySQL ユーザーまたはデータベースユーザー

1.3.1 システムユーザー

システムユーザーとは、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たユーザーです。

- デフォルトのシステムユーザーである umadmin は、Active IQ Unified Manager のインストールに伴って RHEL または CentOS 上に作成されます。このユーザーはメンテナンスユーザーであり、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。
- 同様のシステムユーザーが vApp 上に作成されます。このユーザーの認証情報は、vApp を展開するユーザーによって入力されます。メンテナンスユーザーであり、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。
- Active IQ Unified Manager サービスを実行するために、システムユーザーである jboss が RHEL および vApp 上に作成されます。jboss ユーザーには、Active IQ Unified Manager サービスを実行するための RHEL および vApp の制限された権限があります。
- RHEL または CentOS および vApp のメンテナンスユーザーと jboss ユーザーには、root としていくつかのスクリプトを実行する権限があります。メンテナンスユーザーと jboss ユーザーのこれらのアクセス権限は、/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。
- /etc/sudoers.d/ocum_sudoers ファイルと /etc/sudoers.d/ocie_sudoers ファイルは、Active IQ Unified Manager のインストール中に作成されます。これらのファイルは root が所有し、root ユーザーにのみ読み取り権限があります。これらのファイルのアクセス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ー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 上で最高の権限を持ちます。

備考

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ーを作成してください。

1.3.2 アプリケーションユーザー

Active IQ Unified Manager では、アプリケーションユーザーはローカルユーザーとして指定されます。アプリケーションユーザーは、Active IQ Unified Manager アプリケーションで作成されたユーザーです。表 1.3 に、アプリケーションユーザーの種類を示します。

表 1.3 アプリケーションユーザーの種類

ユーザー	説明
メンテナンスユーザー	Unified Manager の初期設定時に作成されます。その後、メンテナンスユーザーは追加のユーザーを作成し、ロールを割り当てます。Unified Manager は、RHEL または CentOS システムにインストールされています。メンテナンスユーザーには、umadmin というユーザー名とデフォルトのパスワードが付与されます。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ーです。
ローカルユーザー	メンテナンスユーザーまたはアプリケーション管理者ロールを持つユーザーによって指定されたロールに基づいて機能を実行します。
リモートグループ	認証サーバに保存されている認証情報を使用して、Unified Manager ユーザーインターフェイスにアクセスするユーザーのグループです。リモートグループ内のすべてのユーザーは、個々のユーザー認証情報を使用して Unified Manager ユーザーインターフェイスにアクセスすることができます。
リモートユーザー	認証サーバに保存されている認証情報を使用して、Unified Manager ユーザー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ー	Unified Manager データベース内のデータへの読み取り専用アクセス権を持ち、Unified Manager ユーザーインターフェイスまたはメンテナンスコンソールにはアクセスできず、API コールを実行することができません。データベースユーザーには、以下の 2 つのロールが割り当てられています。 • Integration Schema • Report Schema

ローカルユーザー (アプリケーションユーザー) には、ロールが割り当てられています。表 1.4 に、ローカルユーザーに対して使用可能な Active IQ Unified Manager のロールを示します。

1.3.3 ロール

ロールベースアクセスコントロール (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誰がアクセスできるかを管理できます。Active IQ Unified Manager の RBAC ソリューションは、ユーザーの管理アクセスを、定義されたロールに付与されたレベルに制限します。これにより、管理者は割り当てられたロールによってローカルユーザーを管理できます。ローカルユーザーアカウントは固定のため、割り当てられたロールは変更できません。表 1.4 に、Active IQ Unified Manager で事前に定義されているロールを示します。

表 1.4 事前に定義されたロールの種類

ユーザー	説明
Operator	履歴や容量の傾向など、Unified Manager によって収集されたストレージシステム情報およびその他のデータを表示します。このロールにより、ストレージの使用者はイベントの表示、割り当て、確認、解決、およびノートの追加が可能です。
Storage administrator	Unified Manager 内のストレージ管理操作を設定します。このロールにより、ストレージ管理者は閾値の構成や、アラートやその他のストレージ管理固有のオプションやポリシーの作成が可能です。
Application administrator	ストレージ管理に関連しない設定を構成します。このロールにより、ユーザー、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、ネットワーキング、AutoSupport など) の管理が可能になります。
Integration schema	このロールにより、Unified Manager を OnCommand Workflow Automation (WFA) に統合するための Unified Manager データベースビューへの読み取り専用アクセスが可能になります。このロールを持つユーザーは MySQL データベースで作成されるため、データベースユーザーになります。

1.3.4 ユーザータイプ

ユーザータイプは、Active IQ Unified Manager にあ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、管理者ロールを持つユーザーによって割り当てられます。Active IQ Unified Manager のローカルユーザーには、Application Administrator、Storage Administrator、および Operator の 3 つのロールが設定可能です。表 1.4 で、これらのロールについて説明しています。

- **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は、最小権限の原則を使用してユーザーのロールを選択することです。

Integration Schema および Report Schema ロールを持つユーザーは、MySQL データベース内に作成されます。データベースユーザーと呼ばれます。MySQL ポートがリモートマシンからの接続に対して有効になっている場合、これらのユーザーはリモートマシンから MySQL データベースに接続できます。通常、これらのユーザー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。

1.3.5 Active IQ Unified Manager アプリケーションユーザーのロックおよびロック解除

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。非アクティブアカウントは、悪意のある人物がリソースにアクセスする機会をもたらします。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、ロックするようにしてください。アプリケーション管理者のロールを持つユーザーは、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、左側のペインから [設定]> [全般] > [ユーザー] を選択します。ユーザーページには、ユーザーアカウントをロックまたはロック解除するオプションがあります。

1.4 相互トランスポート層セキュリティ (証明書ベースの認証)

ONTAP 9.12 以降、Active IQ Unified Manager は、ONTAP 9.12 で追加された新しいクラスタの ONTAP との通信に相互トランスポート層セキュリティ (TLS) を使用します。Active IQ Unified Manager の以前のバージョンからアップグレードした場合は、クラスタプロパティを編集して相互 TLS を有効にできます。

図 1.3 に示すように、Cluster Setup のページには、各クラスタに設定された相互トランスポート層セキュリティ (mTLS) のステータスが表示されます。

図 1.3 証明書ベース認証のステータス

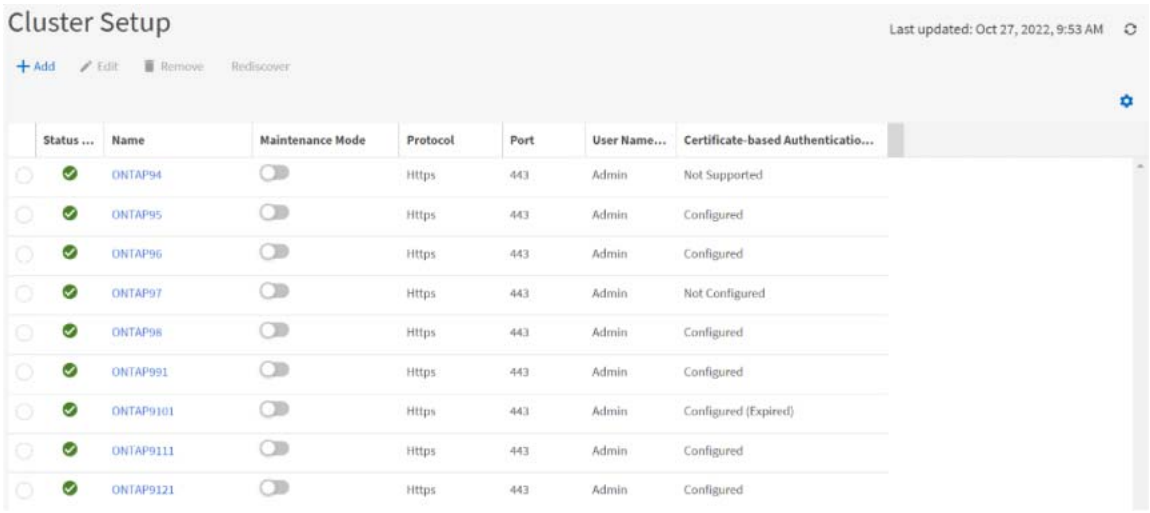


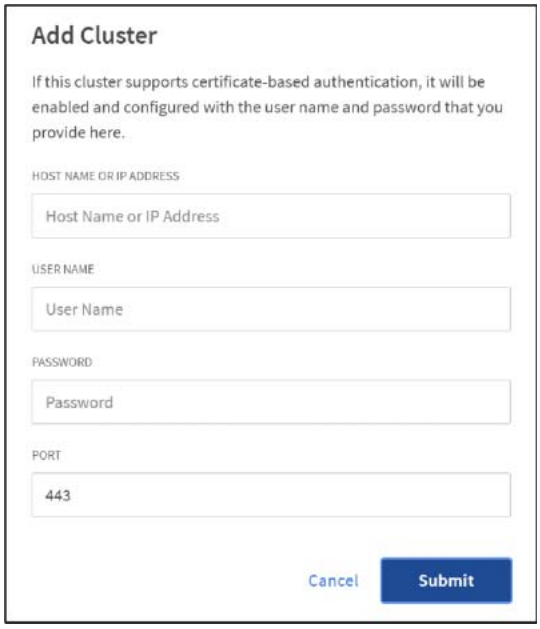
図 1.3 に、証明書ベースの認証の 4 つのステータスを示します。

- **Configured**
  mTLS が設定され、Active IQ Unified Manager と ONTAP 間の認証に使用されています。
- **Not Configured**
  ユーザーが Active IQ Unified Manager を以前のバージョンからアップグレードしており、mTLS がこのクラスタに対してまだ設定されていない場合です。クラスタプロパティを編集することによって構成できます。
- **Not Supported**
  ONTAP のバージョンが 9.5 以前です。mTLS をサポートしていません。
- **Configured (Expired)**
  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。
そのため、設定は必要ありません。図 1.4 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 1.4 [Add Cluster] ダイアログ



クラスタ編集

クラスタの編集中に、3 種類の画面が表示される場合があります。これは、mTLS が有効になっているかどうか、または ONTAP クラスタでサポートされているかどうかによって異なります。

- **mTLS がサポートされ有効の場合**
  [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。
- **mTLS はサポートされているが無効の場合**
  この場合、[Submit] ボタンをクリックすると、mTLS が有効になります。
- **mTLS がサポートされていない場合**
  [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。

1.5 Active IQ Unified Manager の HTTPS 証明書

デフォルトでは、Active IQ Unified Manager は、インストール中に自動的に作成された自己署名証明書を使用して、ユーザーインターフェイスへの HTTPS アクセスを保護します。Active IQ Unified Manager は、以下の機能を提供します。

- 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

これらのオプションには、左側のペインから [設定] > [全般] > [HTTPS 証明書] を選択してアクセスできます。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。証明書が CA によって署名された後、[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 サーバに証明書をインストールすることができます。[HTTPS 証明書再生成] オプションを使用すると、インストール時に生成された自己署名証明書を変更できます。この操作は、証明書署名要求を作成する前に行うこともできます。

ベストプラクティス

Active IQ Unified Manager サーバには、CA 署名付き証明書を使用することを推奨します。

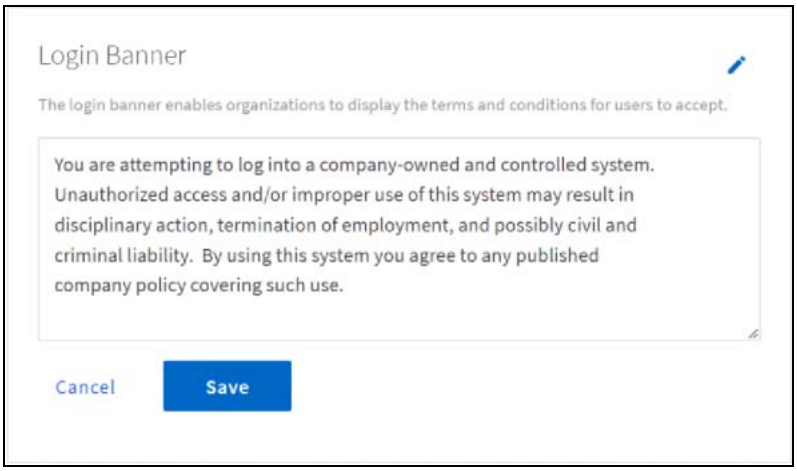
1.6 ログインバナー

ログインバナーは、Active IQ Unified Manager のユーザー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、組織はユーザーの契約条件を表示できます。

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ます。セキュリティ上のベストプラクティスは、ログインバナーを設定することです。ログインバナーを設定するには、[設定] > [全般] > [機能設定] > [ログインバナー] に移動します (図 1.5 を参照)。

図 1.5 ログインバナーの設定



1.7 非アクティブタイムアウト

Unified Manager のユーザーインターフェイスには、指定された非アクティブ時間の経過後にユーザーをログアウトしてセッションを閉じるタイムアウトがあります。このオプションは、デフォルトで有効になっています。

- **ベストプラクティス**

  Active IQ Unified Manager のユーザーインターフェイスのデフォルトの非アクティブタイムアウトは 3 日です。セキュリティ上のベストプラクティスは、非アクティブタイムアウトの時間を 30 分以下に短縮することです。

  非アクティブタイムアウトを変更するには、[設定] > [全般] > [機能設定] を選択し、非アクティブ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 1.6 非アクティブタイムアウトの変更

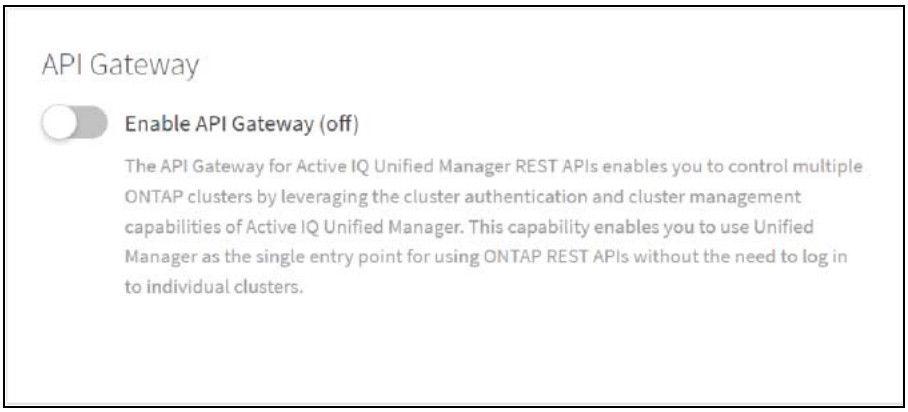
1.8 API ゲートウェイ

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することなく、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 に保存された認証情報を使用して API 要求を ONTAP クラスタに転送します。

- **ベストプラクティス**

  API ゲートウェイ機能を Active IQ Unified Manager で使用しない場合は、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 1.7 API ゲートウェイ機能の無効化



1.9 スクリプトのアップロード

Active IQ Unified Manager では、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**

  スクリプトのアップロード機能が使用されていない場合は、[設定] > [全般] > [機能設定] に移動して、スクリプトのアップロード機能を無効にします (図 1.8 を参照)。

  図 1.8 スクリプトアップロードの無効化

1.10 ユーザーあたりの最大同時セッション数

デフォルトでは、ユーザーあたりの最大同時セッション数は 100 です。Active IQ Unified Manager でアプリケーション管理者ロールを持つユーザーは、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は、最大同時セッション数を低く抑えることです。値を高くすると、DOS 攻撃または分散型サービス妨害 (DDoS) 攻撃の機構に使われることがあります。

以下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
```

1.11 レート制限

レート制限は、DOS 攻撃および DDOS 攻撃に対抗する機構を提供します。OS ファイアウォール経由の新しい接続について、ソース IP アドレスごとにレート制限を設定できます。これにより、悪意のある攻撃の影響を軽減できます。

1.11.1 RHEL

RHEL では、iptables コマンドを使用してレート制限を設定できます。以下のコマンドを使用して、1 秒あたり「n」件の要求で新規接続をレート制限します。

```
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

システムでは、1 つのソース IP に対して、平均で毎秒 10 件の要求が許可されます。最初に 5 件の要求がバーストされます。閾値を超える要求はドロップされます。

1.11.2 vApp

vApp のデフォルトでは、レート制限付きの IP テーブルは、要求数が 1 秒につき 10 件にあらかじめ設定されています。変更が必要な場合は、診断シェルを使用して vApp にログインします。

備考

診断シェルは 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された場合にのみ使用してください。

1.11.3 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。ソース IP ごとにレート制限を設定するには、サードパーティー製のツールをインストールする必要があります。

1.12 暗号化設定

Active IQ Unified Manager で使用される一部のデフォルトの暗号を無効にできます。これを行うには、Active IQ Unified Manager インターフェイスで [設定] > [全般] > [HTTPs 暗号化スイートの管理] を選択します。ただし、すべてのブラウザで最適なユーザーインターフェイスをサポートするために、すべてのデフォルトの暗号をサポートすることを推奨します。

1.13 Active IQ Unified Manager システムへの証明書ベースの SSH および RDP

Active IQ Unified Manager がインストールされている装置には、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**
  Active IQ Unified Manager を Windows にインストールしている場合は、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。Microsoft の Using certificates in Remote Desktop Services に従い、証明書ベースの RDP を Windows マシンに設定します。
- **vApp**
  Active IQ Unified Manager のメンテナンスユーザーは、SSH 経由で vApp にログインすることができます。Active IQ Unified Manager の vApp への証明書ベースの SSH を設定して、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、DIAG シェルにログインする必要があります。DIAG シェル上のすべてのコマンドは、sudo を使用して実行する必要があります。sudo を仕様しない場合、許可拒否の問題が発生します。vApp で証明書ベースの SSH を設定するには、Debian のマニュアルに従ってください。

  vApp の場合のみ、1 人のユーザー (メンテナンスユーザー) が SSH でログインできます。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場合があります。
- **RHEL/CentOS**
  ルートおよびその他のシステムユーザーは、Active IQ Unified Manager 関連の操作を実行したり、通常のシステムメンテナンスおよび操作を実行したりするために、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 のマニュアル「OpenSSH 証明書認証の使用」に従い、証明書ベースの SSH を RHEL に設定します。

1.14 SSH フィンガープリントの再生成

証明書は有効期間が過ぎると期限切れになりますが、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の再生成方法については、Debian、RHEL、および CentOS のマニュアルを参照してください。

1.15 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) との同期が取れていないネットワーク時間が原因で、セキュリティ上の問題が発生することがあります。

1.15.1 vApp

NTP サーバは、vApp の `maintenance_console` 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。これは旧環境のサービスであるため、場合によっては仮想マシンでうまく動作しません。NTP 用の `systemd-timesyncd` サービスに切り替えることができます。

`systemd-timesyncd` は、NTP のクライアントに特化した軽量版です。メンテナンスコンソールから [System Config] > [Change NTP Service] オプションを選択して、`systemd-timesyncd` に切り替えることができます。

1.15.2 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 サービスよりも多くの機能が向上します。

ETERNUS AX series オールフラッシュアレイ , ETERNUS AC series オールフラッシュアレイ ,
ETERNUS HX series ハイブリッドアレイ Active IQ Unified Manager セキュリティ強化ガイド

C140-0128-02Z3

発行年月　2025 年 3 月
発行責任　エフサステクノロジーズ株式会社

Fsas Technologies