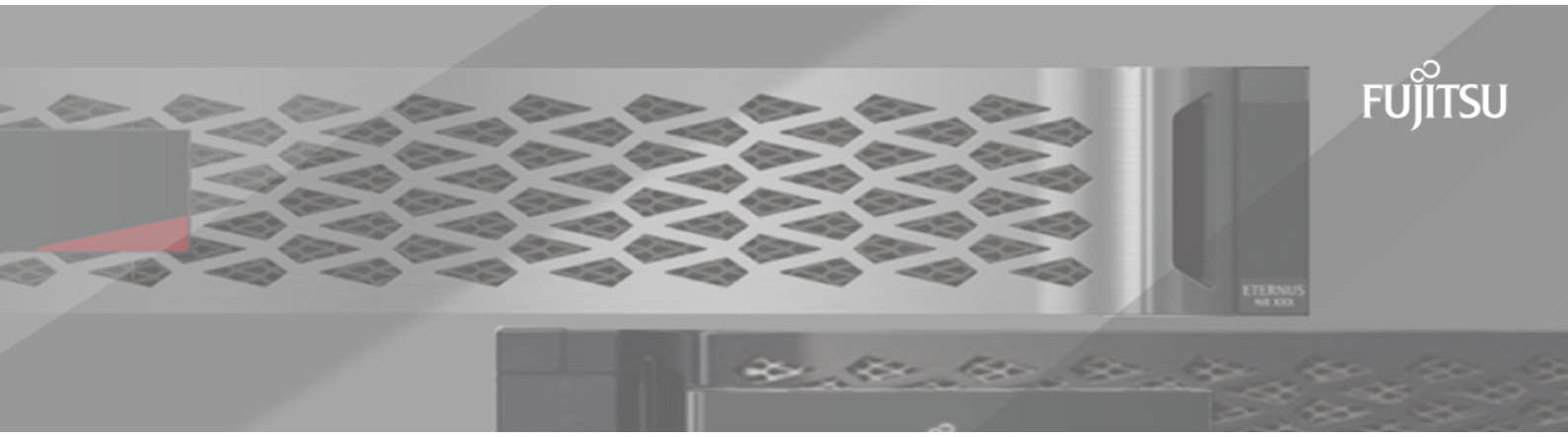
A3CA08733-A512-02



FUJITSU Storage ETERNUS AB/HB Series

SANtricity® Web Services Proxy

インストールと使用

目次

概要と要件 4
- Web Servicesの概要 4
- 互換性と制限事項 5
- APIの基本 6
- 用語と概念 9

Web Services Proxyのインストールと設定 10
- インストールの要件と考慮事項 10
- Web Services Proxyのインストール 11
  - Web Services Proxyファイルのダウンロード 11
  - WindowsサーバまたはLinuxサーバへのインストール 11
  - APIドキュメントとUnified Managerへのアクセス 14
- Web Services Proxyの設定 16
  - Webサーバの停止と再起動 16
  - ポートの競合の解決 16
  - ロードバランシング / ハイアベイラビリティの設定 17
  - Symbol HTTPSの無効化 18
  - Cross-Origin Resource Sharingの設定 18
- Web Services Proxyのアンインストール 19
  - グラフィカル モードでのアンインストール 19
  - コンソール モードでのアンインストール 19
  - サイレント モードでのアンインストール 19
  - RPMコマンドでのアンインストール（Linuxのみ） 19

ユーザ アクセスの管理 21
- アクセス管理の概要 21
- ユーザ アクセスの設定 22
  - パスワードへの暗号化の追加適用 22
  - ベーシック認証の設定 23
  - ロールベース アクセスの設定 23

セキュリティと証明書の管理 25
- セキュリティと証明書の設定 25
  - SSLの有効化 25
  - 証明書の検証の省略 25
  - ホスト管理証明書の生成とインポート 26

ストレージ システムの管理 28
- ストレージ システムを検出する 28
  - ストレージ システムの自動検出 28
  - APIエンドポイントを使用したストレージ システムの検出と追加 28
- 管理可能なストレージ システム数の引き上げ 31

統計の自動ポーリングの管理 32
- 統計の概要 32
- 統計機能 32
- ポーリング間隔の設定 33

AutoSupportの管理 34
- AutoSupport（ASUP）の概要 34
- AutoSupportを設定する 34
  - AutoSupportの有効化または無効化 34
  - AutoSupportの配信方法の設定 35

著作権に関する情報.....36
登録商標.....37
マニュアルの更新について..... 38

概要と要件

このガイドでは、SANtricity Unified Managerインターフェイスを含むSANtricity Web Services Proxyのインストールおよび設定方法について説明します。Web Services ProxyはRESTful APIサーバで、ホスト システムに別途インストールして、数百台規模の新旧のFujitsu ETERNUS AB/HBシリーズ ストレージ システムを管理します。Unified Managerは、同様の機能を提供するWebベースのインターフェイスです。

Web Servicesの概要

インストールと設定を開始する前に、Web ServicesとSANtricity Unified Managerの概要について説明します。

Web Services

Web Servicesは、富士通のETERNUS AB/HBシリーズのストレージ システムを設定、管理、監視するためのアプリケーション プログラミング インターフェイス（API）です。API要求を発行することで、ETERNUS AB/HBシリーズ ストレージ システムの設定、プロビジョニング、パフォーマンス監視などのワークフローを実行できます。

Web Services APIを使用してストレージ システムを管理するには、次の知識が必要になります。

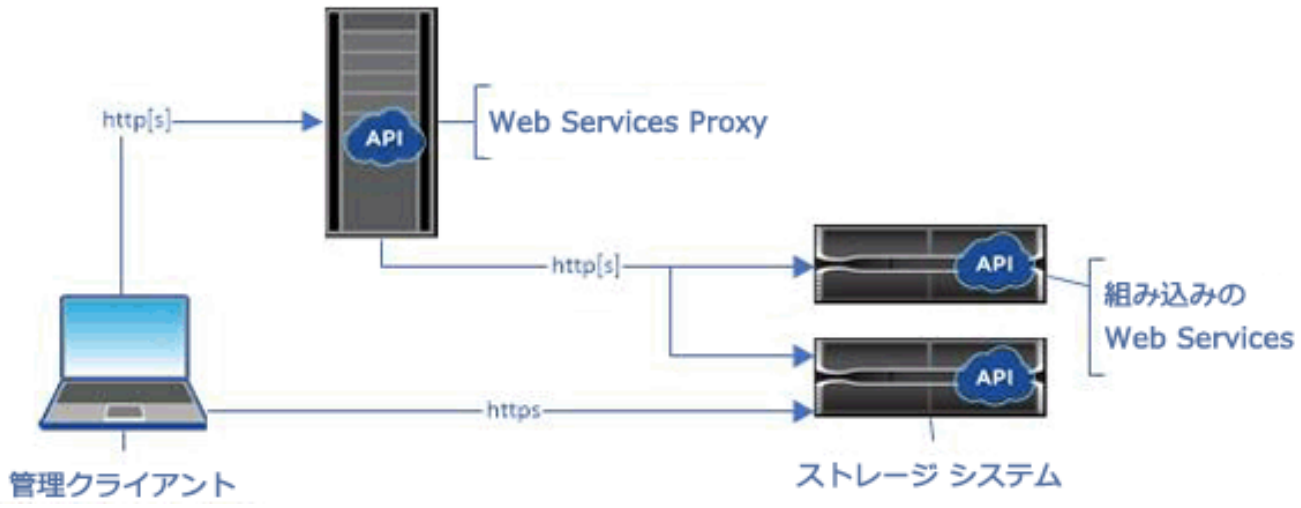
- JavaScript Object Notation（JSON）：Web ServicesのデータはJSONでエンコードされているため、JSONのプログラミング概念を理解しておく必要があります。詳細については、http://www.json.org/を参照してください。
- Representational State Transfer（REST）：Web Servicesは実質的にすべてのSANtricity管理機能へのアクセスを提供するRESTful APIであるため、RESTの概念を理解しておく必要があります。詳細については、http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htmを参照してください。
- プログラミング言語の概念：Web Services APIで使用される最も一般的なプログラミング言語はJavaとPythonですが、HTTP要求を行うことができれば他のプログラミング言語も使用できます。

実装

Web Servicesには2種類の実装があります。

- 組み込み： Fujitsu SANtricity 11.60 以降のバージョンを実行する HB2100/HB2200/HB2300 / AB2100 ストレージシステム、 SANtricity 11.60 以降のバージョンを実行する HB5100/HB5200 / AB5100 ストレージシステム、および SANtricity 11.60 以降のバージョンを実行する AB3100 または AB6100 ストレージシステムには、各コントローラに RESTful API サーバが組み込まれています。インストールは不要です。
- プロキシ：SANtricity Web Services Proxyは、WindowsサーバまたはLinuxサーバに別途インストールするRESTful APIサーバです。このホストベースのアプリケーションでは、数百台規模の新旧のFujitsu ETERNUS AB/HBシリーズ ストレージ システムを管理できます。一般に、ストレージ システムが10台を超えるネットワークではプロキシを使用します。プロキシは、多数の要求を組み込みのAPIよりも効率的に処理できます。

中核となるAPIはどちらの実装でも使用できます。



次の表は、プロキシ バージョンと組み込みバージョンの比較です。

表 1 :

考慮事項	プロキシ	組み込み
インストール	ホスト システム（Linuxまたはwindows）が必要です。	インストールや有効化は必要ありません。
セキュリティ	デフォルトで最小限のセキュリティ設定が適用されます。 セキュリティ設定が低いため、開発者はAPIをすばやく簡単に使用できます。必要に応じて、組み込みバージョンと同じセキュリティ プロファイルを適用できます。	デフォルトで高いセキュリティ設定が適用されます。 セキュリティ設定が高くなっているのは、APIがコントローラ上で直接実行されるためです。たとえば、HTTPアクセスは許可されないほか、HTTPSについてもSSLや古いTLSの暗号化プロトコルはすべて無効です。
一元管理	1台のサーバからすべてのストレージ システムを管理します。	組み込み先のコントローラのみを管理します。

Unified Manager

プロキシインストールパッケージには、HB2100/HB2200/HB2300、HB5100/HB5200、AB3100、AB6100などのETERNUS AB/HB シリーズの新しいストレージシステムの設定が可能な、Webベースのインターフェイスである Unified Managerが含まれています。

Unified Managerでは次のバッチ処理を実行できます。

- 複数のストレージ システムのステータスをまとめて表示
- ネットワーク内の複数のストレージ システムを検出
- 1つのストレージ システムから複数のシステムに設定をインポート
- 複数のストレージ システムのファームウェアをアップグレード

互換性と制限事項

Web Services Proxyをインストールして使用する前に、互換性と制限事項について確認しておく必要があります。

Web Services Proxyの使用に関する互換性と制限事項を以下に記載します。

表 2 :

考慮事項	互換性または制限事項
HTTPのサポート	Web Services ProxyではHTTPまたはHTTPSを使用できます（組み込み版のWeb Servicesにはセキュリティ上の理由からHTTPSが必要です）。
ストレージ システムとファームウェア	Web Services Proxy ではすべての ETERNUS AB/HB シリーズストレージシステムを管理でき、古いシステムと最新のHB2100/HB2200/HB2300、AB2100、HB5100/HB5200、AB5100、AB3100、AB6100シリーズシステムを混在させることもできます。
IPのサポート	Web Services Proxyでは、IPv4プロトコルまたはIPv6プロトコルがサポートされます。 **注 :** IPv6プロトコルは、Web Services Proxyがコントローラの設定から管理アドレスを自動検出しようとしたときに失敗することがあります。原因としては、IPアドレスの転送時の問題のほか、ストレージ システムでIPv6が有効になっているがサーバでは有効になっていない場合などが考えられます。
NVSRAMファイル名の制約	Web Services Proxyは、NVSRAMファイル名を使用してバージョン情報を正確に識別します。そのため、Web Services Proxyで使用されているNVSRAMファイルの名前は変更できません。NVSRAMファイルの名前が変更された場合、Web Services Proxyで有効なファームウェア ファイルとして認識されない可能性があります。
Symbol Web	Symbol WebはREST API内のURLです。ほぼすべてのsymbol呼び出しへのアクセスを提供します。symbol関数は次のURLの一部です。 `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` **注 :** Symbolが無効なストレージ システムは、Web Services Proxyを介してサポートされます。

APIの基本

Web Services APIのHTTP通信は、要求と応答のサイクルで構成されます。

使用するプログラミング言語やツールに関係なく、Web Services APIの各呼び出しは、URL、HTTP動詞、およびAcceptヘッダーを含む同様の構造を持ちます。

要求のURL要素

すべての要求には次のようなURLが含まれ、以下の表に示す要素で構成されます。

```
https://webservices.name.com:8443/devmgr/v2/storage-systems
```

表 3 :

要素	説明
HTTP転送プロトコル `https://`	Web Services ProxyではHTTPまたはHTTPSを使用できます。 組み込み版のWeb Servicesにはセキュリティ上の理由からHTTPSが必要です。
ベースURLとポート `webservices.name.com:8443`	各要求がWeb Servicesのアクティブなインスタンスに正しくルーティングされるように、 インスタンスの完全修飾ドメイン名（FQDN）またはIPアドレス、およびリスニング ポートが必要です。デフォルトでは、Web Servicesの通信にはポート8080（HTTP）とポート8443（HTTPS）が使用されます。 Web Services Proxyでは、どちらのポートもインストール時または`wsconfig.xml`ファイルで変更可能です。さまざまな管理アプリケーションを実行するデータセンター ホストでは、ポートの競合は珍しくありません。 組み込みのWeb Servicesでは、コントローラ上のポートは変更できず、デフォルトのポート8443を使用してセキュアな接続が確立されます。
APIパス `devmgr/v2/storage-systems`	要求はWeb Services API内の特定のRESTリソース（エンドポイント）に対して実行されます。ほとんどのエンドポイントは次の形式です。 `devmgr/v2/<resource>/[id]` APIパスは次の3つの部分で構成されます。 • `devmgr` （Device Manager）は、Web Services APIのネームスペースです。 • `v2` は、アクセスするAPIのバージョンです。`utils`を使用してログイン エンドポイントにアクセスすることもできます。 • `storage-systems` は、ドキュメント内のカテゴリです。

サポートされるHTTP動詞

サポートされるHTTP動詞には、GET、POST、およびDELETEがあります。

- GET要求は読み取り専用要求に使用されます。
- POST要求はオブジェクトの作成と更新に使用されます。また、セキュリティに影響する可能性のある読み取り要求にも使用されます。
- DELETE要求は、一般にオブジェクトを管理対象から削除したり、オブジェクトを完全に削除したり、オブジェクトの状態をリセットしたりするために使用されます。

注 : 現在のところ、Web Services APIではPUTおよびPATCHはサポートしていません。代わりに、POSTを使用してこれらの動詞の代表的な機能を実行できます。

Acceptヘッダー

特に指定がないかぎり、Web Servicesは要求の本文をJSON形式で返します。一部のクライアントは、デフォルトで「text/html」などを要求します。この場合、APIは要求された形式でデータを提供できない

ことを示すHTTPコード406で応答します。ベストプラクティスとして、応答にJSON形式が必要なケースのためにAcceptヘッダーを「application/json」と定義することを推奨します。応答本文が返されないそれ以外のケース（DELETEなど）では、Acceptヘッダーを指定しても意図しない結果が生じることはありません。

応答

APIに要求を送信すると、次の2つの重要な情報が応答として返されます。

- HTTPステータス コード：要求が成功したかどうかを示します。
- 応答本文（オプション）：通常は、リソースの状態を示すJSON本文、または失敗の詳しい状況を示す本文が返されます。

ステータス コードとcontent-typeヘッダーから、応答本文の内容を判断する必要があります。HTTPステータス コードが200～203および422の場合、Web Servicesは応答でJSON本文を返します。それ以外のHTTPステータス コードの場合、Web Servicesは一般にJSON本文を返しません。これは、仕様で許可されていない（204）か、ステータスが説明を必要としないためです。次の表に、一般的なHTTPステータス コードとその定義を示します。また、各HTTPコードに関連付けられた情報がJSON本文で返されるかどうかも示します。

表 4 :

HTTPステータス コード	説明	JSON本文
200 OK	処理に成功したことを示します。	○
201 Created	オブジェクトが作成されたことを示します。このコードは、ステータス200の代わりにごくまれに使用されます。	○
202 Accepted	要求は非同期要求としての処理を承認されましたが、実際の結果を取得するためには再度要求が必要です。	○
203 Non-Authoritative Information	200と同様ですが、Web Servicesはデータが最新であることを保証できません（その時点でキャッシュ データしか使用できない場合など）。	○
204 No Content	処理には成功しましたが、応答本文はありません。	×
400 Bad Request	要求のJSON本文が有効でないことを示します。	×
401 Unauthorized	認証に失敗したことを示します。クレデンシャルが指定されていないか、ユーザ名またはパスワードが無効です。	×
403 Forbidden	認証に失敗したことを示します。認証されたユーザに要求したエンドポイントにアクセスする権限がありません。	×
404 Not Found	要求されたリソースが見つからなかったことを示します。このコードは、識別子で要求されたAPIやリソースが存在しない場合に使用されます。	×
422 Unprocessable Entity	要求の形式には問題はありませんが、入力パラメータが無効であるか、ストレージ システムの状態が原因でWeb Servicesが要求を実行できません。	○
424 Failed Dependency	Web Services Proxyでは、要求されたストレージ システムに現在アクセスできないことを示すために使用されます。したがって、Web Servicesは要求を実行できません。	×
429 Too Many Requests	要求の上限を超えたため、あとで再試行する必要があります。	×

サンプル スクリプト

GitHubに、Fujitsu SANtricity Web Services APIの使用方法を示すサンプル スクリプトをまとめたリポジトリが用意されています。

関連タスク

Web Services APIへのログイン（14ページ）

用語と概念

Web Services Proxyに関連する用語を以下に記載します。

表 5 :

用語	定義
API	アプリケーション プログラミング インターフェイス（API）は、開発者がデバイスとの通信に使用する一連のプロトコルとメソッドです。Web Services APIは、ETERNUS AB/HBシリーズ ストレージ システムとの通信に使用されます。
ASUP	AutoSupport（ASUP）は、データを収集してカスタマー サポート バンドルとして保存し、リモートでのトラブルシューティングや問題分析用にメッセージ ファイルを富士通のサポートに自動的に送信する機能です。
エンドポイント	エンドポイントはAPIで使用できる関数です。エンドポイントには、HTTP動詞とURIパスが含まれます。Web Servicesでは、エンドポイントを使用してストレージ システムの検出やボリュームの作成などのタスクを実行できます。
HTTP動詞	HTTP動詞は、データの取得や作成など、エンドポイントで実行するアクションです。Web Servicesでは、POST、GET、およびDELETEのHTTP動詞がサポートされます。
JSON	JavaScript Object Notation（JSON）はXMLとほぼ同じ構造化データ形式で、最小限の判読可能な形式を使用します。Web Services内のデータはJSONでエンコードされています。
REST / RESTful	Representational State Transfer（REST）は、APIのアーキテクチャ スタイルを定義する大まかな仕様です。ほとんどのREST APIは仕様に完全には準拠していないため、「RESTful」または「REST-like」と称されます。一般に「RESTful」APIはプログラミング言語に依存せず、次のような特徴があります。 • HTTPベース（プロトコルの一般的なセマンティクスに従う） • 構造化データ（JSONやXMLなど）のプロデューサとコンシューマ • オブジェクト指向（処理指向でない） Web Servicesは、実質的にすべてのSANtricity管理機能へのアクセスを提供するRESTful APIです。
ストレージ システム	ストレージ システムは、シェルフ、コントローラ、ドライブ、ソフトウェア、およびファームウェアを含むETERNUS AB/HBシリーズ アレイです。
Symbol API	Symbolは、ETERNUS AB/HBシリーズ ストレージ システムを管理するためのレガシーAPIです。Web Services APIの基盤となる実装で使用されています。
Web Services	Web Servicesは、ETERNUS AB/HBシリーズ ストレージ システムの管理用に開発者向けに設計された富士通独自のAPIです。Web Servicesには2つの実装があります。1つはコントローラに組み込まれており、もう1つはプロキシとしてLinuxまたはWindowsに別途インストールできます。

Web Services Proxyのインストールと設定

Web Services ProxyはWindowsまたはLinuxのホスト システムにインストールして設定できます。

インストールの要件と考慮事項

インストールの要件とアップグレード時の考慮事項を確認しておく必要があります。

インストールの要件

Web Services Proxyのインストールには次の要件があります。

表 6 :

要件	説明
ホスト名の制限	Web Services Proxyをインストールするサーバのホスト名に、ASCII文字、数字、ハイフン（-）以外の文字が含まれていないことを確認してください。この要件は、サーバの自己署名証明書の生成に使用されるJava Keytoolの制限によるものです。サーバのホスト名にアンダースコア（_）などの他の文字が含まれていると、インストール後にWebサーバを起動できません。
オペレーティング システム	Web Services Proxyは次のオペレーティング システムにインストールできます。 • Linux • Windows 互換性があるオペレーティング システムとファームウェアの一覧については、サポート組み合わせ表を参照してください。
Linux：その他の考慮事項	Webサーバが適切に機能するためには、Linux Standard Base libraries（init-functions）が必要です。オペレーティング システムに応じたlsb/insservパッケージをインストールする必要があります。詳細については、Readmeファイルの「Additional packages required」セクションを参照してください。
複数のインスタンス	Web Services Proxyのインスタンスはサーバごとに1つしかインストールできませんが、ネットワーク内の複数のサーバにインストールすることができます。
キャパシティ プランニング	Web Services Proxyでは、ロギング用に十分なスペースが必要です。使用可能なディスク スペースについて、システムが次の要件を満たしていることを確認してください。 • インストールに必要なスペース：275MB • ロギング用の最小スペース：200MB • システム メモリ：2GB（デフォルトではヒープ スペースに1GBを使用） ディスクスペース監視ツールを使用して、永続的ストレージとロギングに使用可能なディスク ドライブ スペースを確認できます。

要件	説明
ライセンス	Web Services Proxyは、ライセンス キーを必要としない無料のスタンドアロン製品です。ただし、該当する著作権とサービス利用規約が適用されます。グラフィカル モードまたはコンソール モードでプロキシをインストールする場合は、エンド ユーザ ライセンス契約（EULA）に同意する必要があります。

アップグレード時の考慮事項

以前のバージョンからアップグレードする場合は、保持される項目と削除される項目があることに注意してください。

- Web Services Proxyについては、以前の設定が保持されます。これには、ユーザ パスワード、検出されたすべてのストレージ システム、サーバ証明書、信頼された証明書、サーバのランタイム設定などが含まれます。
- Unified Managerについては、リポジトリにロードされていたすべてのSANtricity OSファイルがアップグレード時に削除されます。

Web Services Proxyのインストール

インストールを実施するには、ファイルをダウンロードし、LinuxサーバまたはWindowsサーバにプロキシ パッケージをインストールします。インストール後、APIドキュメントまたはUnified Managerにアクセスして、ストレージ システムの管理を開始できます。

Web Services Proxyファイルのダウンロード

製品添付のDVDから、インストール ファイルとreadmeファイルをダウンロードできます。

このタスクについて

ダウンロード パッケージには、Web Services ProxyとUnified Managerインターフェイスが含まれています。

WindowsサーバまたはLinuxサーバへのインストール

Web Services ProxyとUnified Managerは、3つのモード（グラフィカル、コンソール、サイレント）のいずれかを使用するか、RPMファイル（Linuxのみ）を使用してインストールできます。

グラフィカル モードでのインストール

グラフィカル モードでのインストールは、WindowsとLinuxのどちらでも実行できます。グラフィカル モードでは、Windows形式のインターフェイスにプロンプトが表示されます。

始める前に

- システム要件とアップグレード時の考慮事項を確認しておきます。
- プロキシとUnified Managerをインストールするサーバに正しいインストール ファイル（Windowsの場合はEXE、Linuxの場合はBIN）をダウンロードしておきます。

手順

1. インストール ファイルをダウンロードしたフォルダにアクセスします。
2. WindowsまたはLinuxのインストールを起動します。
   - Windows：インストール ファイルをダブルクリックします。`santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`
   - Linux：次のコマンドを実行します。`santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

注： 上記ファイル名の「*nn.nn.nn.nnnn*」はバージョン番号です。

インストール プロセスが開始され、Fujitsu SANtricity Web Services ProxyおよびUnified Managerのスプラッシュ画面が表示されます。

3. 画面の指示に従います。
   インストールでは、複数の機能を有効にし、複数の設定パラメータを入力します。選択した内容は、必要に応じてあとで構成ファイルで変更できます。
4. 「Webserver Started」というメッセージが表示されたら、**[OK]**をクリックしてインストールを完了します。
   [Install Complete]ダイアログ ボックスが表示されます。
5. Unified Managerまたは対話型のAPIドキュメントを起動する場合は該当するチェック ボックスをオンにし、**[Done]**をクリックします。

関連概念

インストールの要件と考慮事項（10ページ）

関連タスク

Web Services Proxyファイルのダウンロード（11ページ）
Web Services APIへのログイン（14ページ）
Unified Managerへのログイン（15ページ）

コンソール モードでのインストール

コンソール モードでのインストールは、WindowsとLinuxのどちらでも実行できます。コンソール モードでは、ターミナル ウィンドウにプロンプトが表示されます。

始める前に

- システム要件とアップグレード時の考慮事項を確認しておきます。
- プロキシとUnified Managerをインストールするサーバに正しいインストール ファイル（Windowsの場合はEXE、Linuxの場合はBIN）をダウンロードしておきます。

手順

1. 次のコマンドを実行します。`<install filename> -i console`
   上記コマンドの*<install filename>*は、ダウンロードしたプロキシ インストール ファイルの名前です（例：`santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`）。

   注： インストール プロセス中にコマンド プロンプトで「`QUIT`」と入力すると、いつでもインストールをキャンセルできます。

   インストール プロセスが開始され、「Launching Installer - Introduction」というメッセージが表示されます。
2. 画面の指示に従います。
   インストールでは、複数の機能を有効にし、複数の設定パラメータを入力します。選択した内容は、必要に応じてあとで構成ファイルで変更できます。
3. インストールが完了したら、**Enter**キーを押してインストーラを終了します。

関連概念

インストールの要件と考慮事項（10ページ）

関連タスク

Web Services Proxyファイルのダウンロード（11ページ）
Web Services APIへのログイン（14ページ）
Unified Managerへのログイン（15ページ）

サイレント モードでのインストール

サイレント モードでのインストールは、WindowsとLinuxのどちらでも実行できます。サイレント モードでは、メッセージやスクリプトはターミナル ウィンドウに表示されません。

始める前に

- システム要件とアップグレード時の考慮事項を確認しておきます。
- プロキシとUnified Managerをインストールするサーバに正しいインストール ファイル（Windowsの場合はEXE、Linuxの場合はBIN）をダウンロードしておきます。

手順

1. 次のコマンドを実行します。`<install filename> -i silent`

   上記コマンドの*<install filename>*は、ダウンロードしたプロキシ インストール ファイルの名前です（例：`santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`）。
2. **Enter**キーを押します。

   インストール処理が完了するまでに数分かかることがあります。インストールが完了すると、ターミナル ウィンドウにコマンド プロンプトが表示されます。

関連概念

インストールの要件と考慮事項（10ページ）

関連タスク

Web Services Proxyファイルのダウンロード（11ページ）
Web Services APIへのログイン（14ページ）
Unified Managerへのログイン（15ページ）

RPMコマンドでのインストール（Linuxのみ）

RPMパッケージ管理システムと互換性があるLinuxシステムでは、オプションのRPMファイルを使用してWeb Services Proxyをインストールできます。

始める前に

- システム要件とアップグレード時の考慮事項を確認しておきます。
- プロキシとUnified Managerをインストールするサーバにに RPMファイルをダウンロードしておきます。

手順

1. ターミナル ウィンドウを開きます。
2. 次のコマンドを入力します。`rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm`

   注： 上記コマンドの「*nn.nn.nn.nnnn*」はバージョン番号です。

   インストール処理が完了するまでに数分かかることがあります。インストールが完了すると、ターミナル ウィンドウにコマンド プロンプトが表示されます。

関連概念

インストールの要件と考慮事項（10ページ）

関連タスク

Web Services Proxyファイルのダウンロード（11ページ）
Web Services APIへのログイン（14ページ）
Unified Managerへのログイン（15ページ）

APIドキュメントとUnified Managerへのアクセス

Web Servicesには、REST APIと直接やり取りできるAPIドキュメントが含まれています。また、複数のETERNUS AB/HBシリーズ ストレージ システムを管理するためのブラウザベースのインターフェイスであるUnified Managerも含まれています。

Web Services APIへのログイン

Web Services Proxyをインストールしたら、ブラウザから対話型のAPIドキュメントにアクセスできます。

始める前に

- Web Services ProxyをWindowsサーバまたはLinuxサーバにインストールしておきます。

このタスクについて

APIドキュメントはWeb Servicesの各インスタンスと一緒に実行されるほか、富士通のサポート サイトからPDF版を入手することもできます。対話型のバージョンにアクセスするには、ブラウザを開き、Web Servicesの場所（組み込みバージョンの場合はコントローラ、プロキシの場合はサーバ）を示すURLを入力します。

注： Web Services APIはOpenAPI仕様（旧称Swagger仕様）を実装しています。

初回ログイン時は「admin」クレデンシャルを使用します。「admin」は、すべての機能とロールにアクセスできるスーパー管理者とみなされます。

手順

1. ブラウザを開きます。
2. 組み込み実装またはプロキシ実装のURLを入力します。
   - 組み込み：`https://<controller>:<port>/devmgr/docs/`

     注： このURLで、`<controller>`はコントローラのIPアドレスまたはFQDN、`<port>`はコントローラの管理ポート番号（デフォルトは8443）です。
   - プロキシ：`http[s]://<server>:<port>/devmgr/docs/`

     注： このURLで、`<server>`はプロキシがインストールされているサーバのIPアドレスまたはFQDN、`<port>`はリスニング ポート番号（デフォルトはHTTPが8080、HTTPSが8443）です。

   注： リスニング ポートがすでに使用されている場合は競合が検出され、別のリスニング ポートを選択するように求められます。

   ブラウザでAPIドキュメントが開きます。
3. 対話型のAPIドキュメントを開いたら、ページ右上のドロップダウン メニューから**[utils]**を選択します。
4. **[Login]**カテゴリをクリックし、使用可能なエンドポイントを表示します。
5. **[POST: /login]**エンドポイントをクリックし、**[Try it out]**をクリックします。
6. 初めてのログインの場合は、ユーザ名とパスワードに「`admin`」と入力します。
7. **[Execute]**をクリックします。
8. ストレージ管理用のエンドポイントにアクセスするには、右上のドロップダウン メニューから**[v2]**を選択します。
   エンドポイントの上位レベルのカテゴリが表示されます。APIドキュメントのナビゲート方法を以下に示します。

表 7 :

要素	説明
ドロップダウン メニュー	ページ右上にあるドロップダウン メニューで、APIドキュメントのバージョン2（V2）、Symbolインターフェイス（Symbol V2）、ログイン用のAPIユーティリティ（utils）を切り替えることができます。 **注 :** APIドキュメントのバージョン1はプレリリース版であり、一般には提供されていないため、V1はドロップダウン メニューに含まれていません。
カテゴリ	APIドキュメントは、上位レベルのカテゴリ（AdministrationやConfigurationなど）別に編成されています。カテゴリをクリックすると、関連するエンドポイントが表示されます。
エンドポイント	エンドポイントを選択すると、そのエンドポイントのURLパス、必須パラメータ、応答本文、およびURLから返される可能性があるステータス コードが表示されます。
Try It Out	エンドポイントを直接操作するには、**[Try it out]**をクリックします。このボタンは、エンドポイント用の各ビューにあります。 このボタンをクリックすると、パラメータを入力するためのフィールドが表示されます（該当する場合）。値を入力し、**[Execute]**をクリックします。 対話型ドキュメントでは、JavaScriptを使用して直接APIに要求が送信されます。テスト要求ではありません。

関連概念

APIの基本（6ページ）

Unified Managerへのログイン

Web Services Proxyをインストールしたら、Unified ManagerにアクセスしてWebベースのインターフェイスで複数のストレージ システムを管理できます。

始める前に

- Unified Managerを含むWeb Services ProxyをWindowsサーバまたはLinuxサーバにインストールしておきます。

このタスクについて

Unified Managerにアクセスするには、ブラウザを開き、プロキシがインストールされている場所のURLを入力します。サポートされるブラウザとバージョンを次に示します。

表 8 :

ブラウザ	最小バージョン
Google Chrome	47
Microsoft Internet Explorer	11
Microsoft Edge	EdgeHTML 12
Mozilla Firefox	31

ブラウザ	最小バージョン
Safari	9

手順

1. ブラウザを開き、次の URL を入力します。 `http[s]://<server>:<port>/um`

   このURLで、*<server>*はWeb Services Proxyがインストールされているサーバの IPアドレスまたはFQDN、*<port>*はリスニング ポート番号（デフォルトはHTTPが8080、HTTPSが8443）です。

   Unified Managerのログイン ページが開きます。
2. 初めてログインする場合、ユーザ名に`admin`と入力し、adminユーザのパスワードを設定して確認します。

   パスワードに指定できる文字数は最大30文字です。ユーザとパスワードの詳細については、Unified Managerオンライン ヘルプのアクセス管理に関するセクションを参照してください。

Web Services Proxyの設定

Web Services Proxyの設定は、環境独自の運用やパフォーマンスの要件に合わせて変更することができます。

Webサーバの停止と再起動

Webサーバ サービスはインストール時に開始され、バックグラウンドで実行されます。一部の設定タスクでは、Webサーバ サービスの停止や再起動が必要になる場合があります。

手順

次のいずれかを実行します。

- Windowsの場合、**[スタート]**メニューから**[管理ツール]** > **[サービス]**を選択し、「Fujitsu SANtricity Web Services」を見つけて**[停止]**または**[再起動]**を選択します。
- Linuxの場合、オペレーティング システムのバージョンに応じてWebサーバを停止および再起動する方法を選択します。どのデーモンが起動されたかは、インストール中にポップアップ ダイアログに表示されます。次に例を示します。

  ```
  web_services_proxy webserver installed and started. You can interact with
  it using systemctl start|stop|restart|status web_services_proxy.service
  ```

  サービスの操作に使用される最も一般的な方法は**systemctl**コマンドです。

ポートの競合の解決

定義されたアドレスまたはポートを別のアプリケーションも使用しているときにWeb Services Proxyを実行する場合、`wsconfig.xml`ファイルでポートの競合を解決できます。

手順

1. `wsconfig.xml`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows） – `C:\Program Files\Fujitsu\SANtricity Web Services Proxy`
   - （Linux） – `/opt/fujitsu/santricity_web_services_proxy`
2. `wsconfig.xml`ファイルに次の行を追加します。nはポート番号です。

   ```
   <sslport clientauth="request">n</sslport>
   <port>n</port>
   ```

   次の表に、HTTPポートとHTTPSポートを制御する属性を示します。

表 9 :

名前	説明	親ノード	属性	必須
config	設定のルートノード	Null	Version：設定スキーマの現在のバージョンは1.0です。	○
sslport	SSL要求をリスンするTCPポート。デフォルトは8443です。	config	Clientauth	×
port	HTTP要求をリスンするTCPポート。デフォルトは8080です。	config	-	×

3. ファイルを保存して、閉じます。
4. Webサーバ サービスを再起動して変更を反映させます。

関連タスク

Webサーバの停止と再起動（16ページ）

ロードバランシング / ハイアベイラビリティの設定

ハイアベイラビリティ（HA）構成でWeb Services Proxyを使用するには、ロード バランシングを設定します。一般にHA構成では、1つのノードですべての要求を受信して他のノードはスタンバイにするか、すべてのノード間で要求の負荷を分散するかのどちらかになります。

このタスクについて

Web Services Proxyはハイアベイラビリティ（HA）環境で利用することができ、ほとんどのAPIは要求を受信するノードに関係なく正しく動作します。メタデータ タグとフォルダの2つは例外で、これらはローカル データベースに格納され、Web Services Proxyインスタンス間で共有されません。

ただし、ごく一部の要求でタイミングの問題が発生することがわかっています。具体的には、プロキシのインスタンス間で新しいデータの取得に時間差が発生することがあります。Web Services Proxyには、この問題を解決するための特別な設定が含まれています。このオプションは、有効にするとデータの整合性を保つために要求の処理にかかる時間が長くなることから、デフォルトでは有効になっていません。このオプションを有効にするには、.INIファイル（Windows）または.SHファイル（Linux）にプロパティを追加する必要があります。

手順

1. 次のいずれかを実行します。
   - Windows：`appserver64.ini`ファイルを開き、`Dload-balance.enabled=true`プロパティを追加します。

     例：`vmarg.7=-Dload-balance.enabled=true`
   - Linux：`webserver.sh`ファイルを開き、`Dload-balance.enabled=true`プロパティを追加します。

     例：`DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`
2. 変更を保存します。
3. Webサーバ サービスを再起動して変更を反映させます。

関連タスク

Webサーバの停止と再起動（16ページ）

Symbol HTTPSの無効化

Symbolコマンド（デフォルト設定）を無効にして、代わりにリモート プロシージャ コール（RPC）でコマンドを送信することができます。この設定は`wsconfig.xml` ファイルで変更できます。

このタスクについて

デフォルトでは、Web Services ProxyはSANtricity OSバージョン08.60以降を実行するHB2100/HB2200/HB2300シリーズおよびHB5100/HB5200シリーズのすべてのストレージ システムにHTTPS経由でSymbolコマンドを送信します。HTTPS経由で送信されたSymbolコマンドは、ストレージ システムに対して認証されます。必要な場合はHTTPS Symbolのサポートを無効にし、RPC経由でコマンドを送信することができます。RPC経由のSymbolが設定されている場合、ストレージ システムへのすべてのパッシブ コマンドが認証なしで有効になります。

注： RPC経由のSymbolが使用された場合、Web Services ProxyはSymbol管理ポートが無効になっているシステムに接続できません。

手順

1. `wsconfig.xml`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy`
   - （Linux）－`/opt/fujitsu/santricity_web_services_proxy`
2. `devicemgt.symbolclientstrategy`エントリの値を`httpsPreferred`から`rpcOnly`に変更します。

   例：`<env key="devicemgt.symbolclientstrategy">rpcOnly</env>`
3. ファイルを保存します。

Cross-Origin Resource Sharingの設定

Cross-Origin Resource Sharing（CORS）を設定できます。CORSは、追加のHTTPヘッダーを使用して、あるオリジン（ドメイン）で実行されているWebアプリケーションに別のオリジンにあるサーバのリソースへのアクセスを許可するメカニズムです。

このタスクについて

CORSは`working`ディレクトリにある`cors.cfg`ファイルで制御されます。デフォルトではCORSは無制限に許可され、クロス ドメイン アクセスは制限されません。

構成ファイルがない場合、CORSは無制限に許可されます。`cors.cfg`ファイルがある場合は、その設定が使用されます。`cors.cfg`ファイルが空の場合は、CORS要求は実行できません。

手順

1. `cors.cfg`ファイルを開きます。このファイルは`working`ディレクトリにあります。
2. 必要な行をファイルに追加します。

   CORS構成ファイルの各行は、照合する正規表現のパターンで構成されます。originヘッダーが`cors.cfg`ファイルの各行と照合され、 いずれかの行のパターンと一致すると要求が許可されます。ホスト要素だけでなく、完全なオリジンが比較されます。
3. ファイルを保存します。

タスクの結果

要求は次のようにプロトコルに基づいてホストと照合されます。

- 任意のプロトコルのlocalhostに対応：*localhost*
- HTTPSのみのlocalhostに対応：https://localhost*

Web Services Proxyのアンインストール

Web Services ProxyとUnified Managerを削除する際は、インストール時に使用した方法に関係なく、任意のモード（グラフィカル、コンソール、サイレント、またはRPMファイル）を使用できます。

グラフィカル モードでのアンインストール

グラフィカル モードでのアンインストールは、WindowsとLinuxのどちらでも実行できます。グラフィカル モードでは、Windows形式のインターフェイスにプロンプトが表示されます。

手順

1. WindowsまたはLinuxのアンインストールを起動します。
   - Windows：`uninstall_web_services_proxy`アンインストール ファイルが格納されているディレクトリに移動します。このディレクトリのデフォルトの場所は`C:/Program Files/Fujitsu/SANtricity Web Services Proxy/`です。`uninstall_web_services_proxy.exe`をダブルクリックします。

     注：[コントロール パネル] > **[プログラム]** > **[プログラムのアンインストール]**に移動して、[Fujitsu SANtricity Web Services Proxy]を選択することもできます。
   - Linux：Web Services Proxyアンインストール ファイルが格納されているディレクトリに移動します。このディレクトリのデフォルトの場所は`/opt/fujitsu/santricity_web_services_proxy/uninstall_web_services_proxy`です。次のコマンドを実行します。`uninstall_web_services_proxy -i gui`

   SANtricity Web Services Proxyのスプラッシュ画面が表示されます。
2. [Uninstall]ダイアログ ボックスで、**[Uninstall]**をクリックします。
   アンインストールの進捗状況が表示されます。
3. 「Uninstall Complete」というメッセージが表示されたら、**[Done]**をクリックします。

コンソール モードでのアンインストール

コンソール モードでのアンインストールは、WindowsとLinuxのどちらでも実行できます。コンソール モードでは、ターミナル ウィンドウにプロンプトが表示されます。

手順

1. `uninstall_web_services_proxy`ディレクトリに移動します。
2. 次のコマンドを実行します。`uninstall_web_services_proxy -i console`
   アンインストール プロセスが開始されます。
3. アンインストールが完了したら、**Enter**キーを押してインストーラを終了します。

サイレント モードでのアンインストール

サイレント モードでのアンインストールは、WindowsとLinuxのどちらでも実行できます。サイレント モードでは、メッセージやスクリプトはターミナル ウィンドウに表示されません。

手順

1. `uninstall_web_services_proxy`ディレクトリに移動します。
2. 次のコマンドを実行します。`uninstall_web_services_proxy -i silent`
   アンインストール プロセスが実行されますが、メッセージやスクリプトはターミナル ウィンドウに表示されません。Web Services Proxyのアンインストールが完了すると、ターミナル ウィンドウにコマンド プロンプトが表示されます。

RPMコマンドでのアンインストール（Linuxのみ）

RPMコマンドを使用して、LinuxシステムからWeb Services Proxyをアンインストールできます。

手順

1. ターミナル ウィンドウを開きます。
2. コマンドラインで次のコマンドを入力します。`rpm -e santricity_webservices`

   注 : アンインストール プロセスでは、元のインストールに含まれていなかったファイルが残ることがあります。Web Services Proxyを完全に削除するには、それらのファイルを手動で削除してください。

ユーザ アクセスの管理

セキュリティ対策として、Web Services APIとUnified Managerへのユーザ アクセスを管理することができます。

アクセス管理の概要

アクセス管理には、ロールベース ログイン、パスワード暗号化、ベーシック認証、LDAP統合が含まれます。

ロールベース アクセス制御

ロールベース アクセス制御（RBAC）は、事前定義されたユーザにロールを関連付けます。各ロールは特定レベルの機能に対する権限を付与します。

次の表は各ロールとその説明です。

表 10 :

ロール	説明
security.admin	SSLおよび証明書の管理。
storage.admin	ストレージ システム設定への読み取り / 書き込みのフル アクセス。
storage.monitor	ストレージ システム データを表示するための読み取り専用アクセス。
support.admin	ストレージ システムのすべてのハードウェア リソースとAutoSupport（ASUP）の取得などのサポート処理に対するアクセス。

デフォルトのユーザ アカウントは`users.properties`ファイルに定義されています。ユーザ アカウントは、`users.properties`ファイルを直接編集するか、Unified Managerのアクセス管理機能を使用して変更できます。

次の表は、Web Services Proxyで使用可能なユーザ アカウントの一覧です。

表 11 :

事前定義のユーザ アカウント	説明
admin	すべての機能にアクセスできるスーパー管理者。すべてのロールが含まれています。Unified Managerの場合は、初回ログイン時にパスワードを設定する必要があります。
storage	すべてのストレージ プロビジョニングを担当する管理者。このユーザには、`storage.admin`、`support.admin`、`storage.monitor`の各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
security	セキュリティ設定を担当するユーザ。このユーザには、`security.admin`と`storage.monitor`の各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
support	ハードウェア リソース、障害データ、ファームウェア アップグレードを担当するユーザ。このユーザには、`support.admin`と`storage.monitor`の各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。

事前定義のユーザ アカウント	説明
monitor	システムへの読み取り専用アクセスを付与されたユーザ。このユーザには、storage.monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効です。
rw	rw（読み取り / 書き込み）ユーザには、storage.admin、support.admin、storage.monitorの各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
ro	ro（読み取り専用）ユーザには、storage.monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効です。

パスワード暗号化

それぞれのパスワードに対して、既存のSHA256パスワード エンコーディングを使用して暗号化プロセスを追加で適用できます。この追加の暗号化プロセスは、各SHA256ハッシュ暗号化の各パスワードにランダムなバイト セット（ソルト）を適用します。ソルトが付加されたSHA256暗号化は、新しく作成されるすべてのパスワードに適用されます。

注： Web Services Proxy 3.0よりも前のリリースでは、パスワードはSHA256ハッシュのみで暗号化されていました。SHA256ハッシュのみで暗号化された既存のパスワードではこのエンコーディングが維持され、users.propertiesファイルで引き続き有効です。ただし、SHA256ハッシュのみで暗号化されたパスワードは、ソルトが付加されたSHA256暗号化を使用したパスワードほど安全ではありません。

ベーシック認証

ベーシック認証はデフォルトで有効になっており、サーバからベーシック認証チャレンジが返されます。この設定はwsconfig.xmlファイルで変更できます。

LDAP

Lightweight Directory Access Protocol（LDAP）は、分散型のディレクトリ情報サービスへのアクセスと管理に使用されるアプリケーション プロトコルで、Web Services Proxyで有効になっています。LDAPとの統合により、ユーザ認証とグループへのロールの割り当てが可能になります。

LDAP機能の設定については、Unified Managerインターフェイスの設定オプション、または対話型のAPIドキュメントのLDAPのセクションを参照してください。

関連タスク

パスワードへの暗号化の追加適用（22ページ）
ベーシック認証の設定（23ページ）
ロールベース アクセスの設定（23ページ）

ユーザ アクセスの設定

ユーザ アクセスを管理するには、パスワードを暗号化したり、ベーシック認証を設定したり、ロールベース アクセスを定義したりします。

パスワードへの暗号化の追加適用

最高レベルのセキュリティを実現するために、既存のSHA256パスワード エンコーディングを使用して、パスワードに暗号化を追加で適用できます。

このタスクについて

この追加の暗号化プロセスは、各SHA256ハッシュ暗号化の各パスワードにランダムなバイト セット（ソルト）を適用します。ソルトが付加されたSHA256暗号化は、新しく作成されるすべてのパスワードに適用されます。

手順

1. `users.properties`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy\data\config`
   - （Linux）－`/opt/fujitsu/santricity_web_services_proxy/data/config`
2. 暗号化されたパスワードをプレーン テキストで再入力します。
3. **securepasswds**コマンドライン ユーティリティを実行してパスワードを再暗号化するか、Web Services Proxyを再起動します。このユーティリティは、Web Services Proxyのルート インストール ディレクトリにインストールされています。

   注： また、Unified Managerでパスワードが編集されるたびに、ローカル ユーザのパスワードにソルトを付加してハッシュ化することもできます。

関連概念

アクセス管理の概要（21ページ）

ベーシック認証の設定

ベーシック認証はデフォルトで有効になっており、サーバからベーシック認証チャレンジが返されます。この設定は、必要に応じて`wsconfig.xml`ファイルで変更できます。

手順

1. `wsconfig.xml`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy`
   - （Linux）－`/opt/fujitsu/santricity_web_services_proxy`
2. ファイルの次の行を編集して、`false`（無効）または`true`（有効）を指定します。

   例：`<env key="enable-basic-auth">true</env>`
3. ファイルを保存します。
4. Webサーバ サービスを再起動して変更を反映させます。

関連概念

アクセス管理の概要（21ページ）

ロールベース アクセスの設定

ユーザ アクセスを特定の機能に制限するには、各ユーザ アカウントに指定するロールを変更します。

このタスクについて

Web Services Proxyにはロールベース アクセス制御（RBAC）が含まれており、事前定義されたユーザにロールが関連付けられています。各ロールは特定レベルの機能に対する権限を付与します。ユーザ アカウントに割り当てられているロールは、`users.properties`ファイルを直接編集することで変更できます。

注： Unified Managerのアクセス管理を使用してユーザ アカウントを変更することもできます。詳細については、Unified Managerのオンライン ヘルプを参照してください。

手順

1. `users.properties`ファイルを開きます。このファイルは次の場所にあります。

- （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy\data\config`
- （Linux）－`/opt/fujitsu/santricity_web_services_proxy/data/config`

2. 変更するユーザ アカウント（storage、security、monitor、support、rw、ro）の行を見つけます。

   注： adminユーザは変更しないでください。adminユーザはすべての機能にアクセスできるスーパーユーザです。

3. 指定されているロールを必要に応じて追加または削除します。

   次のロールがあります。

   - security.admin：SSLおよび証明書の管理。
   - storage.admin：ストレージ システム設定への読み取り / 書き込みのフル アクセス。
   - storage.monitor：ストレージ システム データを表示するための読み取り専用アクセス。
   - support.admin：ストレージ システムのすべてのハードウェア リソースとAutoSupport（ASUP）の取得などのサポート処理に対するアクセス。

   注： storage.monitorロールは、管理者を含むすべてのユーザに必要です。

4. ファイルを保存します。

関連概念

アクセス管理の概要（21ページ）

セキュリティと証明書の管理

証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。証明書は、Web Services Proxy構成ファイル、APIコマンド、またはUnified Managerインターフェイスを使用して管理できます。

セキュリティと証明書の設定

セキュリティ対策として、SSLポートを指定し、証明書を管理することができます。

SSLの有効化

Web Services ProxyはセキュリティSecure Sockets Layer（SSL）を使用しており、インストール時にSSLが有効化されます。SSLポートの指定は`wsconfig.xml`ファイルで変更できます。

手順

1. `wsconfig.xml`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy`
   - （Linux）－`/opt/fujitsu/santricity_web_services_proxy`
2. 次の例のように、SSLポート番号を追加または変更します。

```
<sslport clientauth=”request”>8443</sslport>
```

タスクの結果

SSLが設定された状態でサーバを起動すると、サーバはキーストア ファイルと信頼ストア ファイルを探します。

- キーストアが見つからない場合、サーバは最初に検出された非ループバックIPv4アドレスのIPアドレスを使用してキーストアを生成し、自己署名証明書をキーストアに追加します。
- 信頼ストアが見つからないか指定されていない場合、サーバはキーストアを信頼ストアとして使用します。

証明書の検証の省略

セキュアな接続をサポートするために、Web Services Proxyはストレージ システムの証明書を独自の信頼された証明書と照合して検証します。必要に応じて、ストレージ システムへの接続時にこの検証を省略するように指定できます。

始める前に

- ストレージ システムへの接続がすべてセキュアである必要があります。

手順

1. `wsconfig.xml`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy`
   - （Linux）－`/opt/fujitsu/santricity_web_services_proxy`
2. 次の例に示すように、`trust.all.arrays`エントリに「`true`」と入力します。

```
<env key="trust.all.arrays">true</env>
```

3. ファイルを保存します。

ホスト管理証明書の生成とインポート

証明書は、クライアントとサーバの間にセキュアな接続を確立するためにWebサイトの所有者を識別します。Web Services Proxyがインストールされているホスト システムの認証局（CA）証明書を生成してインポートするには、APIエンドポイントを使用します。

始める前に

- 対話型のAPIドキュメントにログインしておきます。

このタスクについて

ホスト システムの証明書を管理するには、APIを使用して次のタスクを実行します。

- ホスト システムの証明書署名要求（CSR）を作成します。
- CSRファイルをCAに送信し、証明書ファイルが送られてくるのを待ちます。
- 署名済み証明書をホスト システムにインポートします。

注 : 証明書はUnified Managerインターフェイスでも管理できます。詳細については、Unified Managerのオンライン ヘルプを参照してください。

手順

1. 対話型のAPIドキュメントで、右上のドロップダウン メニューから**[v2]**を選択します。
2. **[Administration]**リンクを展開し、下にスクロールして**[/certificates]**エンドポイントまで移動します。
3. CSRファイルを生成します。
   a) **[POST:/certificates]**を選択し、**[Try it out]**を選択します。
   Webサーバで自己署名証明書が再生成されます。各フィールドに情報を入力して、CSRの生成に使用する共通名、組織、組織単位、代替IDなどの情報を定義できます。
   b) **[Example values]**ペインに必要な情報を追加して有効なCA証明書を生成し、コマンドを実行します。

   注 : CSRの再生成が必要になるため、**POST:/certificates**と**POST:/certificates/reset**は繰り返し呼び出さないでください。**POST:/certificates**または**POST:/certificates/reset**を呼び出すと、そのたびに新しい秘密鍵を使用して新しい自己署名証明書が生成されます。サーバで秘密鍵がリセットされる前に生成されたCSRを送信した場合、新しいセキュリティ証明書は機能しません。CSRを生成し直して新しいCA証明書を要求する必要があります。
   c) **GET:/certificates/server**エンドポイントを実行して、現在の証明書が**POST:/certificates**コマンドで追加した情報を含む自己署名証明書であることを確認します。

   サーバ証明書（「jetty」という別名で表示）は、この時点ではまだ自己署名証明書です。
   d) **[POST:/certificates/export]**エンドポイントを展開し、**[Try it out]**を選択してCSRファイルのファイル名を入力し、**[Execute]**をクリックします。
4. `fileUrl`をブラウザの新しいタブにコピーしてCSRファイルをダウンロードし、そのCSRファイルを有効なCAに送信して新しいWebサーバ証明書チェーンを要求します。
5. CAから新しい証明書チェーンが発行されたら、証明書管理ツールを使用してルート証明書、中間証明書、およびWebサーバ証明書に分割し、それらの証明書をWeb Services Proxyサーバにインポートします。
   a) **[POST:/sslconfig/server]**エンドポイントを展開し、**[Try it out]**を選択します。
   b) [`alias`]フィールドにCAルート証明書の名前を入力します。
   c) [`replaceMainServerCertificate`]フィールドで**[false]**を選択します。
   d) 新しいCAルート証明書を参照して選択します。
   e) **[Execute]**をクリックします。
   f) 証明書のアップロードが成功したことを確認します。
   g) CA中間証明書について、CA証明書のアップロード手順を繰り返します。

h) 新しいWebサーバ セキュリティ証明書ファイルについて、証明書のアップロード手順を繰り返します。ただし、[`replaceMainServerCertificate`]ドロップダウンでは**[true]**を選択します。

i) Webサーバ セキュリティ証明書のインポートが成功したことを確認します。

j) キーストアに新しいルート証明書、中間証明書、およびWebサーバ証明書があることを確認するために、**GET:/certificates/server**を実行します。

6. **[POST:/certificates/reload]**エンドポイントを選択して展開し、**[Try it out]**を選択します。両方のコントローラを再起動するかどうかを確認するメッセージが表示されたら、**[false]**を選択します（trueはデュアル アレイ コントローラの場合にのみ選択）。**[Execute]**をクリックします。
通常、**/certificates/reload**エンドポイントは要求が成功したことを示すHTTP応答202を返します。ただし、Webサーバの信頼ストアとキーストアの証明書をリロードする際、APIのプロセスとWebサーバの証明書リロード プロセスの間でまれに競合が発生します。その場合、Webサーバ証明書のリロードがAPIの処理よりも優先されることがあり、 その場合はリロードが正常に完了していても失敗したように表示されます。この場合も次の手順にそのまま進んでください。実際にリロードに失敗していれば、次の手順も失敗します。

7. Web Services Proxyの現在のブラウザ セッションを閉じて新しいブラウザ セッションを開き、Web Services Proxyへの新しいセキュアなブラウザ接続を確立できることを確認します。
incognitoモードまたはin-privateモードのブラウズ セッションを使用すると、以前のブラウズ セッションで保存されたデータを使用せずにサーバへの接続を開くことができます。

関連概念

APIの基本（6ページ）

関連タスク

Web Services APIへのログイン（14ページ）

ストレージ システムの管理

ネットワーク内のストレージ システムを管理するためには、まずそれらを検出し、管理リストに追加する必要があります。

ストレージ システムを検出する

ストレージ システムは自動で検出されるように設定することも、手動で検出することもできます。

ストレージ システムの自動検出

wsconfig.xmlファイルの設定を変更することで、ネットワークのストレージ システムを自動的に検出するように指定できます。デフォルトでは、IPv6の自動検出は無効になっており、IPv4は有効になっています。

始める前に

- IPv6の検出設定を有効にする前に、接続の問題を軽減するために、ストレージ システムへのIPv6接続がインフラでサポートされていることを確認してください。

このタスクについて

管理IPアドレスまたはDNSアドレスを1つ指定するだけで、ストレージ システムを追加することができます。パスが設定されていない場合や設定されていてルーティング可能な場合、サーバはすべての管理パスを自動的に検出します。

注： 初回接続後に、IPv6プロトコルを使用してコントローラの設定からストレージ システムを自動的に検出しようとすると、検出に失敗することがあります。原因としては、IPアドレスの転送時の問題のほか、ストレージ システムでIPv6が有効になっているがサーバでは有効になっていない場合などが考えられます。

手順

1. wsconfig.xmlファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－C:\Program Files\Fujitsu\SANtricity Web Services Proxy
   - （Linux）－/opt/fujitsu/santricity_web_services_proxy
2. autodiscoverの設定を必要に応じて「true」から「false」に変更します。次の例を参照してください。

   ```
   <env key="autodiscover.ipv6.enable">true</env>
   ```

   注： パスが設定されていても、サーバからアドレスにルーティングできるように設定されていないと、断続的に接続エラーが発生します。ホストからルーティング可能なIPアドレスを設定できない場合は、自動検出をオフにしてください（設定を「false」に変更）。
3. ファイルを保存します。

APIエンドポイントを使用したストレージ システムの検出と追加

APIエンドポイントを使用してストレージ システムを検出し、管理リストに追加することができます。この手順はストレージ システムとAPIの間に管理接続を作成します。

始める前に

- 対話型のAPIドキュメントにログインしておく必要があります。

- SANtricityバージョン11.60以降のストレージ システムの場合は、SANtricity System Managerインターフェイスで Symbolの従来の管理インターフェイスを有効にしておく必要があります。そうしないと、Discoveryエンドポイントが失敗します。この設定を確認するには、System Managerを開き、**[Settings]** > **[System]** > **[Additional Settings]** > **[Change Management Interface]**の順に選択します。

このタスクについて

このタスクでは、検出したシステムを対話型のAPIドキュメントで管理できるように、REST APIを使用してストレージ システムを検出および追加する方法を説明します。ただし、ストレージ システムの管理には、使いやすいインターフェイスを搭載したUnified Managerを使用することもできます。詳細については、Unified Managerのオンライン ヘルプを参照してください。

手順

1. 次の手順に従ってストレージ システムを検出します。
   a) APIドキュメントのドロップダウンで**[V2]**が選択されていることを確認し、**[Storage-Systems]**カテゴリを展開します。
   b) **[POST: /discovery]**エンドポイントをクリックし、**[Try it out]**をクリックします。
   c) 次の表の説明に従ってパラメータを入力します。

   表 12 :

`startIP` `endIP`	`string`に、ネットワーク内の1つ以上のストレージ システムを表す開始と終了のIPアドレス範囲を指定します。
`useAgents`	次のいずれかの値に設定します。 • `true` = ネットワーク スキャンにインバンドのエージェントを使用する。 • `false` = ネットワーク スキャンにインバンドのエージェントを使用しない。
`connectionTimeout`	接続がタイムアウトするまでの最大スキャン時間（秒数）を入力します。
`maxPortsToUse`	ネットワーク スキャンに使用するポートの最大数を入力します。

   d) **[Execute]**をクリックします。

   注 : APIの操作はユーザへの確認なしで実行されます。

   検出プロセスがバックグラウンドで実行されます。
   e) コード202が返されることを確認します。
   f) **[Response Body]**で、`requestId`の戻り値を確認します。要求IDは次の手順で結果を表示する際に必要になります。
2. 次の手順に従って検出結果を確認します。
   a) **[GET: /discovery]**エンドポイントをクリックし、**[Try it out]**をクリックします。
   b) 前の手順で確認した要求IDを入力します。**[Request ID]**を空白にすると、最後に実行された要求IDが使用されます。
   c) **[Execute]**をクリックします。
   d) コード200が返されることを確認します。
   e) 応答の本文で、要求IDと`storageSystems`の内容を確認します。次の例のようになります。

```
"storageSystems": [
    {
      "serialNumber": "123456789",
```

```
        "wwn": "000A011000AF0000000000001A0C000E",
        "label": "AB5100_Array",
        "firmware": "08.41.10.01",
        "nvsram": "N5700-841834-001",
        "ipAddresses": [
          "10.xxx.xx.213",
          "10.xxx.xx.214"
        ],
```

f) wwn、label、およびipAddressesの値を書き留めます。これらは次の手順で必要になります。

3. 次の手順に従ってストレージ システムを追加します。
   a) **[POST: /storage-system]**エンドポイントをクリックし、**[Try it out]**をクリックします。
   b) 次の表の説明に従ってパラメータを入力します。

表 13 :

id	このストレージ システムの一意の名前を入力します。ラベル（GET: /discoveryの応答に表示）を入力することもできますが、任意の文字列を使用できます。このフィールドに値を指定しないと、自動的に一意の識別子が割り当てられます。
controllerAddresses	GET: /discoveryの応答に表示されたIPアドレスを入力します。デュアル コントローラの場合は、IPアドレスをカンマで区切って指定します。次に例を示します。 “IP address 1”,”IP address 2”
validate	trueを入力し、Web Servicesがストレージ システムに接続できるかどうかの確認を受け取ります。
password	ストレージ システムの管理パスワードを入力します。
wwn	ストレージ システムのWWN（GET: /discoveryの応答に表示）を入力します。

   c) 次の例のように、“enableTrace”: trueのあとの文字列をすべて削除します。

```
{
  "id": "AB5100_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

   d) **[Execute]**をクリックします。
   e) コードの応答がエンドポイントが正常に実行されたことを示す201であることを確認します。**Post: /storage-systems**エンドポイントがキューに登録されます。次の手順で、**GET: /storage-systems**エンドポイントを使用して結果を確認できます。

4. 次の手順に従ってリストへの追加を確認します。
   a) **[GET: /storage-system]**エンドポイントをクリックします。
      パラメータは必要ありません。
   b) **[Execute]**をクリックします。
   c) コードの応答がエンドポイントが正常に実行されたことを示す200であることを確認します。

d) 応答の本文で、ストレージ システムの詳細を確認します。管理対象アレイのリストに追加されていれば、戻り値は次のようになります。

```
[
  {
    "id": "AB5100_Array",
    "name": "AB5100_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```

関連概念

APIの基本（6ページ）

関連タスク

Web Services APIへのログイン（14ページ）

管理可能なストレージ システム数の引き上げ

デフォルトでは、最大100台のストレージ システムをAPIで管理できます。さらに多くのストレージ システムを管理する必要がある場合は、サーバのメモリ要件を増やす必要があります。

このタスクについて

サーバは512MBのメモリを使用するように設定されています。ネットワーク内のストレージ システムが100台増えるごとに、これに250MB追加します。搭載されている物理メモリよりも多くのメモリは追加しないでください。オペレーティング システムやその他のアプリケーション用に十分な量を確保しておく必要があります。

注： デフォルトのキャッシュ サイズは8,192イベントです。MELイベントのキャッシュのおおよそのデータ使用量は、8,192イベントごとに1MBです。したがって、デフォルトのままにした場合、ストレージ システムのキャッシュ使用量は約1MBになります。

注： メモリに加え、ストレージ システムごとにネットワーク ポートも必要です。LinuxとWindowsは、ネットワーク ポートをファイル ハンドルとみなします。ほとんどのオペレーティング システムでは、セキュリティ対策として、プロセスまたはユーザが一度に開くことができるファイル ハンドル数が制限されています。特にLinux環境では、開いているTCP接続がファイル ハンドルとみなされるため、Web Services Proxyを使用するとこの制限を簡単に超えてしまいます。対処方法はシステムによって異なるため、この制限を引き上げる方法については、使用しているオペレーティング システムのドキュメントを参照してください。

手順

1. 次のいずれかを実行します。
   - Windowsの場合は、`appserver64.init`ファイルを開き、 `vmarg.3=-Xmx512M`という行を探します。
   - Linuxの場合は、`webserver.sh`ファイルを開き、 `JAVA_OPTIONS="-Xmx512M"`という行を探します。
2. メモリを拡張するには、「512」を必要なメモリ（MB）に変更します。
3. ファイルを保存します。

統計の自動ポーリングの管理

検出されたストレージ システム上のすべてのディスクおよびボリュームの統計に対して、自動ポーリングを設定できます。

統計の概要

統計情報として、データ収集レートとストレージ システムのパフォーマンスに関する情報が提供されます。

Web Services Proxyでは、次のタイプの統計にアクセスできます。

- 統計の生データ：データ収集時点におけるデータ ポイントの合計カウンタ。読み取り処理の合計数や書き込み処理の合計数に使用できます。
- 統計の分析データ：特定の間隔について計算された情報。1秒あたりの読み取りI/O処理数（IOPS）や書き込みスループットなどがあります。

統計の生データは線形であり、通常、有用なデータを得るためには少なくとも2つの収集データ ポイントが必要になります。統計の分析データは統計の生データから導き出され、重要な指標を提供します。統計の生データから導出可能な多くの値が、わかりやすいポイントインタイム形式で統計の分析データに提示されます。

統計の生データは、自動ポーリングが有効になっているかどうかに関係なく取得できます。URLの末尾にクエリ文字列の`usecache=true`を追加すると、前回のポーリングからキャッシュされた統計を取得できます。キャッシュされた情報を使用すると、統計取得のパフォーマンスが大幅に向上します。ただし、設定されたポーリング間隔よりも短い期間に複数の呼び出しを行った場合は同じデータが返されます。

統計機能

Web Services Proxyは、サポートされているハードウェア モデルおよびソフトウェア バージョンからコントローラやインターフェイスの統計の生データと分析データを取得できるAPIエンドポイントを提供します。

統計の生データのAPI

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

統計の分析データのAPI

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

これらのURLは前回のポーリングから統計の分析データを取得するため、ポーリングが有効な場合にのみ使用できます。これらのURLには、次の入力出力データが含まれます。

- 1秒あたりの処理数
- スループット（MB/秒）
- 応答時間（ミリ秒）

これらのデータはストレージ パフォーマンスの最も一般的な指標で、統計の各ポーリング間の差異に基づいて計算されます。生データよりもこれらの分析された統計の方がよく使用されます。

注： システムの起動時は各種の指標の計算に使用する統計がまだ収集されていないため、統計の分析データを利用するには、起動後に少なくとも1回はポーリング サイクルが完了している必要があります。また、累積カウンタがリセットされた場合には次回のポーリング サイクルで予測できないデータが返されます。

ポーリング間隔の設定

統計を収集するポーリング間隔は、`wsconfig.xml`ファイルを編集して指定できます。

始める前に

- ストレージ システムがプロキシで検出されている必要があります。

このタスクについて

ポーリング間隔を設定するには、`wsconfig.xml`ファイルを編集してポーリング間隔（秒数）を指定します。

注： 統計はメモリにキャッシュされるため、ストレージ システムごとにメモリ使用量が1.5MBほど増えることがあります。

手順

1. `wsconfig.xml`ファイルを開きます。このファイルは次の場所にあります。
   - （Windows）－`C:\Program Files\Fujitsu\SANtricity Web Services Proxy`
   - （Linux）－`/opt/fujitsu/santricity_web_services_proxy`
2. `<env-entries>`タグ内に次の行を追加します。nはポーリング要求の間隔（秒数）です。

   ```
   <env key="stats.poll.interval">n</env>
   ```

   たとえば、60を入力した場合、60秒間隔でポーリングが開始されます。つまり、前のポーリング期間に関係なく、そのポーリング期間が終了してから60秒後にポーリングを開始するように要求されます。統計にはいずれも、取得時の正確な時刻がタイムスタンプとして記録されています。システムはそのタイムスタンプ（時間差）に基づいて60秒を計算します。
3. ファイルを保存します。

AutoSupportの管理

AutoSupport（ASUP）を設定すると、データを収集し、収集したデータをリモートでのトラブルシューティングや問題分析用に富士通のサポートに自動的に送信することができます。

AutoSupport（ASUP）の概要

AutoSupport（ASUP）は、手動およびスケジュールベースの基準に基づいて富士通にメッセージを自動的に送信します。

各AutoSupportメッセージには、ログ ファイル、設定データ、状態データ、パフォーマンス指標の情報が含まれています。デフォルトでは、次の表に示すファイルが週に一度富士通のサポート チームに送信されます。

表 14 :

ファイル名	説明
x-headers-data.txt	Xヘッダー情報を含む.txtファイル。
manifest.xml	メッセージの詳細な内容を含む.xmlファイル。
arraydata.xml	クライアントの永続データのリストを含む.xmlファイル。
appserver-config.txt	アプリケーション サーバの設定データを含む.txtファイル。
wsconfig.txt	Webサービスの設定データを含む.txtファイル。
host-info.txt	ホスト環境に関する情報を含む.txtファイル。
server-logs.7z	使用可能なすべてのWebサーバ ログ ファイルを含む.7zファイル。
client-info.txt	メソッドやWebページのヒット数など、アプリケーション固有のカウンタの任意のキーと値のペアを含む.txtファイル。
webservices-profile.json	これらのファイルには、Web Servicesのプロファイルデータと Jerseyの監視統計データが含まれています。デフォルトでは、Jerseyの監視統計は有効になっています。wsconfig.xmlファイルで、次のように有効と無効を切り替えることができます。 • 有効： <env key="enable.jersey.statistics">true</env> • 無効：<env key="enable.jersey.statistics">false</env>
jersey-monitoring-statistics.json	

AutoSupportを設定する

AutoSupportはインストール時にデフォルトで有効になりますが、この設定を変更したり、配信タイプを変更したりすることができます。

AutoSupportの有効化または無効化

AutoSupport機能はWeb Services Proxyの最初のインストール時に有効にするか無効にするかを指定しますが、この設定はASUPConfigファイルで変更することができます。

このタスクについて

AutoSupportは、以下の手順に従って`ASUPConfig.xml`ファイルで有効または無効にできます。また、APIを使用して有効または無効にすることもできます。APIを使用する場合は、**[Configuration]**と**[POST/asup]**を使用し、「true」または「false」を入力します。

手順

1. `ASUPConfig.xml`ファイルを開きます。このファイルは`working`ディレクトリにあります。
2. `<asupdata enabled="(Boolean)" timestamp="">`という行を探します。
3. 「`true`」（有効）または「`false`」（無効）と入力します。次に例を示します。

```
<asupdata enabled="false" timestamp="0">
```

注： タイムスタンプ エントリは必要ありません。

4. ファイルを保存します。

AutoSupportの配信方法の設定

AutoSupport機能でHTTPS、HTTP、またはSMTPのどの配信方法を使用するかを設定できます。デフォルトの配信方法はHTTPSです。

手順

1. `ASUPConfig.xml`ファイルにアクセスします。このファイルは`working`ディレクトリにあります。
2. `<delivery type="n">`という文字列に、次の表の説明に従って、1、2、または3のいずれかを入力します。

表 15：

値	説明
1	HTTPS（デフォルト） `<delivery type="1">`
2	HTTP `<delivery type="2">`

3	SMTP：AutoSupportの配信タイプをSMTPに設定する場合は、次の例に示すように、SMTPメール サーバのアドレス、および送信者と受信者のEメール アドレスも指定する必要があります。
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

著作権に関する情報

Copyright 2021 FUJITSU LIMITED. All rights reserved.

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。

富士通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、富士通によって「現状のまま」提供されています。富士通は明示的な保証、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。富士通は、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。

富士通は、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。富士通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、富士通は責任を負いません。この製品の使用または購入は、富士通の特許権、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。

登録商標

富士通、富士通ロゴ、ETERNUSは富士通の登録商標です。会社名、製品名等の固有名詞は、各社の商号、商標または登録商標です。

https://www.fujitsu.com/jp/products/computing/storage/trademark/

マニュアルの更新について

本書の最新版や本装置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/

必要に応じてご使用モデルのマニュアルを参照してください。

FUJITSU Storage ETERNUS AB/HB Series

SANtricity® Web Services Proxy インストールと使用

A3CA08733-A512-02

発行日: 2021 年 2 月

発行責任: 富士通株式会社

• 本書の内容は、改善のため事前連絡なしに変更することがあります。

• 本書の内容は、細心の注意を払って制作致しましたが、本書中の誤字、情報の抜け、本書情報の使用に起因する運用結果に関しましては、責任を負いかねますので予めご了承願います。

• 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。

• 無断転載を禁じます。