Hewlett Packard Enterprise

HPE 3PAR StoreServ Management Console 3.4 管理者ガイド

摘要

本書は、HPE 3PAR StoreServ Management Console（SSMC）について説明します。本書の対象読者には、HPE 3PAR StoreServ ストレージシステムのシステム構成とリソース割り当てを監視および管理するストレージ管理者が含まれます。

部品番号: QL226-99903
発行: 2018 年 9 月
版数: 1

ご注意

本書の内容は、将来予告なしに変更されることがあります。Hewlett Packard Enterprise 製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、 その保有、使用、または複製には、Hewlett Packard Enterprise から使用許諾を得る必要があります。 FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェアドキュメンテーション、および商業用製品の技術データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

他社の Web サイトへのリンクは、Hewlett Packard Enterprise の Web サイトの外に移動します。Hewlett Packard Enterprise は、Hewlett Packard Enterprise の Web サイト以外の情報を管理する権限を持たず、また責任を負いません。

商標

Microsoft®および Windows®は、米国および/またはその他の国における Microsoft Corporation の登録商標または商標です。

Java®および Oracle®は、Oracle および/またはその関連会社の登録商標です。

VMware®、VMware® vCenter Server®、および VMware vSphere® Web Client は、米国および/またはその他の国および地域での VMware, Inc.の登録商標または商標です。

目次

HPE 3PAR StoreServ Management Console（SSMC）

SSMC はアプライアンスとしてデプロイされます。SSMC は、Main Console や Administrator Console を含む、最新のブラウザーベースのインターフェイスを提供します。

- **Main Console**—ご使用のストレージを監視および管理するための情報とチュートリアルへリンクしています。含まれている機能は次のとおりです。
  - 全般
  - Block Persona
  - File Persona
  - Storage Optimization
  - データ保護
  - ストレージシステム
  - 連携
  - System Reporter
  - セキュリティ
  - VMware
- **Administrator Console**—証明書の追加、管理、HPE 3PAR StoreServ システムの切断、削除、およびアップグレードを行います。

以下のドキュメントを含む、追加のドキュメントについては、HPE Storage Information Library を参照してください。

HPE 3PAR StoreServ Management Console リリースノート
HPE 3PAR StoreServ Management Console ユーザーガイド
HPE 3PAR StoreServ Management Console オンラインヘルプ

詳しくは

SSMC Main Console の機能(7 ページ)
SSMC および MC によるストレージシステム管理(22 ページ)
HPE Storage Information Library

SSMC Main Console の機能

以下の表およびリストでは、Main Console からの SSMC アクセスの概要が示されます。詳細およびこれらの機能の使用方法についての情報は、HPE 3PAR StoreServ Management Console ユーザーガイドを参照してください。

ヒント: SSMC の一部の機能は、特定のバージョンの HPE 3PAR OS を必要とします。OS への依存についての詳細は、HPE 3PAR StoreServ Management Console リリースノートを参照してください。

- **一般** – ダッシュボード、アクティビティ、スケジュール、および設定の画面が含まれます。

- **ダッシュボード画面** – 標準のパネル、オプションのパネル、およびユーザー作成のパネルを使用して、接続されているストレージシステムの主なプロパティとヘルスが表示されます。既存のダッシュボードの構成を使用するか、独自の構成をカスタマイズします。
- **アクティビティ画面** – 接続されているストレージシステムの、すべてのユーザーおよびシステム生成のアクティビティが表示されます。アクティビティをマークし、承認します。
- **スケジュール画面** – スケジュールされたタスクの表示されたリストを示します。スケジュールされたタスクを選択し、その詳細を表示したり、タスクを編集、削除、再開、または一時停止します。ビューを作成、編集、削除、および管理します。
- **設定画面** – 容量の形式（PiB、TiB、GiB、MiB、および小数）、メインメニューのコンパクションビュー（メニュー項目のカスタマイズ）、System Reporter（サーバーの詳細、スケジューリング、および電子メールの設定）、SMTP（サーバーの詳細、デフォルトの電子メール受信者）、他の形式（日付と時刻、WWN）、優先設定（音声、表示設定、ポートオプション、タイムアウト設定を含む）、データテーブル（サイズおよび外観）、ダイアログウィンドウのデフォルト表示（Block Persona 項目のデフォルトビューのカスタマイズ）、アプリケーション（SSMC のバージョン情報）、HPE InfoSight（HPE InfoSight と接続）を含むグローバル設定を編集します。

- **Block Persona** – ホスト（およびセット）、仮想ボリューム（およびセット）、共通プロビジョニンググループ（CPG）、ポリシー、および復元ポイント（スナップショット）を管理します。カテゴリごとのビューとアクションを以下に示します。

  ホスト

  概要
  ホスト詳細
  エクスポート
  パフォーマンス
  アクティビティ
  マップ

  ホストセット

  概要
  エクスポート
  パフォーマンス
  アクティビティ
  マップ

  仮想ボリューム

  概要
  容量
  設定
  コピー
  エクスポート
  パフォーマンス
  復元ポイント
  アクティビティ
  マップ

  仮想ボリュームセット

  概要
  容量
  エクスポート
  パフォーマンス

アクティビティ
マップ

共通プロビジョニンググループ（CPG）

概要
設定
アクティビティ
マップ

ポリシー

概要
アクティビティ

表 1: Block Persona 用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	ホスト/ホストセット	仮想ボリューム	仮想ボリュームセット	共通プロビジョニンググループ（CPG）	ポリシー
仮想ボリュームセットに追加		X			
コンパクション				X	
変換		X			
作成および編集	X	X	X	X	X
クローンの作成		X			
類似の作成		X			
スナップショットの作成		X	X		
削除	X	X	X	X	X
圧縮セービングの推定		X			
重複排除セービングの推定		X			
エクスポートおよびアンエクスポート	X	X	X		
スナップショット名パターンとスケジュールの管理					X

表は続く

機能/ 使用可能なアクション	ホスト/ホストセット	仮想ボリューム	仮想ボリュームセット	共通プロビジョニンググループ（CPG）	ポリシー
クローンのプロモート		X			
スナップショットのプロモート		X			
容量効率の更新				X	
チューニングの再起動		X			
クローンを再同期		X			
チューニングのロールバック		X			
ポリシーとして保存		X			
Peer Motion の開始	X		X		
クローンの停止		X			
チューニング		X			

- **File Persona** – ファイル共有、ファイルストア、仮想ファイルサーバー、ファイルプロビジョニンググループ（FPG）、および File Persona 構成に関連したアクティビティを管理します。カテゴリごとのビューとアクションを以下に示します。ビューの選択肢は、プロトコル（FTP、オブジェクト、SMB、NFS）に基づいて異なります。

  ファイル共有

  概要
  NFS エクスポート設定
  NFS 監査イベント
  アクティビティ
  マップ

  ファイルストア

  概要
  ファイルスナップショット
  ウイルス対策（AV）
  データ保持
  アクティビティ
  マップ

仮想ファイルサーバー

概要
クォータ
ウイルス対策（AV）設定
ファイルスナップショット
回収タスク
データ保持
ファイルアクセス監査の設定
admin パス監査ログ
アクティビティ
マップ

ファイルプロビジョニンググループ

概要
回収タスク
アクティビティ
マップ

File Persona 構成

概要
認証設定
ウイルス対策（AV）設定
ネットワーク設定
File Persona ルートの設定
プロトコル設定
ユーザーマッピング
コンプライアンス要求
アクティビティ
マップ

表 2: File Persona 用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	ファイル共有	ファイルストア	仮想ファイルサーバー	ファイルプロビジョニンググループ	File Persona 構成
有効化				X	
File Persona の構成					X
ウイルス対策（AV）スキャンの作成		X	X		
作成、編集、および削除	X	X	X	X	
ファイル共有の作成	X	X	X		

表は続く

機能/ 使用可能なアクション	ファイル共有	ファイルストア	仮想ファイルサーバー	ファイルプロビジョニンググループ	File Persona 構成
ファイルスナップショットの作成		X	X		
ファイルストアの作成		X	X		
ローカルグループの構成					X
ローカルユーザーの構成					X
仮想ファイルサーバーの作成			X	X	X
無効化				X	
File Persona ノードペアの削除					X
ファイルスナップショットの削除		X			
LDAP 構成の削除					X
ユーザーマッピングの編集					X
ユーザーマッピングのエクスポート					X
プロトコル設定の編集					X
Remote Copy グループのフェイルオーバー				X	
サイズの増加			X	X	
Active Directory の終了					X
ウィルス対策（AV）隔離の管理		X	X		
データ保持ファイルの管理	X	X			

表は続く

機能/ 使用可能なアクション	ファイル共有	ファイルストア	仮想ファイルサーバー	ファイルプロビジョニンググループ	File Persona 構成
データ保持スキャンの管理		X			
既存のウィルス対策（AV）スキャンの管理		X	X		
ファイルアクセス監査ログの管理			X		
ファイルスナップショットの回収タスクの管理				X	
クォータの管理			X		
ウイルス対策ポリシーの編集			X		
ノードのフェイルオーバー				X	
File Persona ノードの一時停止					X
再割り当て				X	
ファイルスナップショットのスペースの回収			X	X	
回復				X	
ファイルプロビジョニンググループの回復					X
Remote Copy グループの復元				X	
File Persona ノードの再開					X
データ保持スキャンのスケジュール	X	X			
アンマウント				X	

表は続く

機能/ 使用可能なアクション	ファイル共有	ファイルストア	仮想ファイルサーバー	ファイルプロビジョニンググループ	File Persona 構成
オンディスクバージョンのアップグレード				X	
ウイルス定義のアップデート					X

- **Storage Optimization** – カテゴリごとのビューとアクションを以下に示します。

Adaptive Flash Cache

概要
アクティビティ

Adaptive Optimization

概要
アクティビティ
マップ

Priority Optimization

概要
アクティビティ
マップ

表 3: Storage Optimization 用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	Adaptive Flash Cache	Adaptive Optimization	Priority Optimization
作成		X	X
削除		X	X
無効	X		X
編集	X	X	X
有効			X
ボリュームセットで有効	X		
スケジュール		X	X

- **データ保護** – Remote Copy の構成およびグループを管理します。カテゴリごとのビューとアクションを以下に示します。

Remote Copy 構成

概要
ターゲット
リンク
グループ
アクティビティ

Remote Copy グループ

概要
ボリュームペア
ソースボリューム
ターゲットボリューム
アクティビティ
マップ

RMC 認証情報

概要

復元ポイント

概要
エクスポート

表 4: データ保護用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	Remote Copy 構成	Remote Copy グループ	RMC 認証情報	復元ポイント
追加			X	
リンクの追加	X			
接続（アタッチ）				X
Quorum Witness の構成	X			
作成	X	X		
削除		X		X
切断（デタッチ）				X
編集	X	X	X	
ターゲットの編集	X			
フェイルオーバー		X		

表は続く

機能/ 使用可能なアクション	Remote Copy 構成	Remote Copy グループ	RMC 認証情報	復元ポイント
回復		X		
リンクの削除	X			
Quorum Witness の削除	X			
ターゲットの削除	X			
復元（フェイルバック）		X		X
フェイルオーバーの切り戻し		X		
開始		X		
Peer Motion の開始		X		
停止		X		
フェイルオーバーの切り替え		X		
スイッチオーバー		X		
同期		X		

- **ストレージシステム** – システム、コントローラーノード、ポート、ドライブエンクロージャー、および物理ドライブを管理するためのオプションが含まれています。カテゴリごとのビューとアクションを以下に示します。

システム

概要
構成
容量
容量セービング
容量予測
暗号化
System Reporter
設定
サービス
ソフトウェア
ファブリック
ライセンス

- レイアウト
- 分析
- パフォーマンス
- アクティビティ
- マップ

コントローラーノード

- 概要
- 概略図
- アダプターカード
- 電源
- マイクロコントローラー
- システムファン
- 内蔵ドライブ
- バッテリ
- パフォーマンス
- アクティビティ
- マップ

ポート

- 概要
- 概略図
- 設定
- ホスト
- セッション
- パフォーマンス
- アクティビティ
- マップ

ドライブエンクロージャー

- 概要
- 概略図
- マガジン
- インターフェイスカード
- 電源
- 冷却ファン
- 物理ドライブ
- SFP
- アクティビティ
- マップ

物理ドライブ

- 概要
- 概略図
- パフォーマンス
- アクティビティ
- マップ

表 5: Storage Systems 用の SSMC Main Console で使用可能なアクション

アクション	システム	コントローラーノード	ポート	ドライブエンクロージャー	物理ドライブ
ライセンスの追加	X				
EKM サーバーの確認	X				
クリア			X		
無効			X		
編集	X		X	X	
ラベルの編集			X		
有効			X		
暗号化の有効	X				
バックアップファイルのエクスポート	X				
初期化			X		
位置確認	X	X	X [1]	X	X
Ping			X		
スナップショット効率性の更新	X				
暗号化のキーの変更	X				
ファームウェアの再読み込み			X		
バッテリテストのログのリセット		X			
バックアップファイルの復元	X				
EKM サーバーの設定	X				
バッテリテストのログの表示		X			

表は続く

アクション	システム	コントローラーノード	ポート	ドライブエンクロージャー	物理ドライブ
ネームサーバーとの同期			X		
チューニング	X				

[1] システム/ポート機能によって異なります。

- **連携** – 連携構成と Peer Motion を管理します。カテゴリごとのビューとアクションを以下に示します。

連携構成

概要
ピアリンク
推奨されるゾーン
アクティビティ
マップ

Peer Motion

概要
仮想ボリューム
仮想ボリュームセット
アクティビティ

表 6: 連携用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	連携構成	Peer Motion
中断		X
移行ソースの追加	X	
優先度の変更		X
作成	X	
削除	X	X
編集	X	
移行ソースの編集	X	
構成のインポート	X	
外部システムの更新	X	
移行ソースの削除	X	

表は続く

機能/ 使用可能なアクション	連携構成	Peer Motion
再開		X
再試行		X
Peer Motion の開始	X	
連携の同期	X	
テイクオーバー		X
アップグレード	X	

- **System Reporter** – レポートとしきい値アラートを管理します。カテゴリごとのビューとアクションを以下に示します。

レポート

チャート
スケジュール
概要
アクティビティ

しきい値アラート

概要
アクティビティ

詳細分析

詳細分析の概要

表 7: System Reporter 用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	レポート	しきい値アラート
作成	X	X
複数レポートの作成	X	
削除	X	X
編集	X	X
電子メール通知の有効化		X
しきい値アラートの有効化		X
CSV へのエクスポート	X	

表は続く

機能/ 使用可能なアクション	レポート	しきい値アラート
PDF へのエクスポート	X	
レポートのエクスポート	X	
レポートのインポート	X	
プライベートへ変更	X	
パブリックへ変更	X	
ズームをリセット	X	

重要: System Reporter の一部の機能は、特定の 3PAR OS バージョンを実行しているシステムでのみ使用できます。最適なパフォーマンスを実現するために、Hewlett Packard Enterprise では、最新の 3PAR OS バージョンにアップグレードすることをお勧めします。

- **セキュリティ** – ユーザー、LDAP、ロール、接続、およびドメインを管理します。カテゴリごとのビューとアクションを以下に示します。

ユーザー

現在のユーザー、システム、およびドメインの概要

LDAP

概要
承認
アクティビティ

ロール

システム名、ロール、および簡単な説明の概要

接続

現在接続されているユーザーの概要

ドメイン

概要
アクティビティ
マップ

表 8: セキュリティ用の SSMC Main Console で使用可能なアクション

機能/ 使用可能なアクション	ユーザー	LDAP	ロール	接続	ドメイン
LDAP 構成のコピー		X			
作成	X	X			X
削除	X	X		X	X
編集		X			X
認証の編集	X	X			
パスワードの編集	X				
接続のテスト		X			

- **VMWARE** – VMware ストレージコンテナーの作成および削除、および SSMC で使用するために構成された VMware 仮想マシンの参照を行います。

  ストレージコンテナ

  概要
  仮想マシン
  VMware VVol
  アクティビティ
  パフォーマンス
  マップ

  仮想マシン

  概要
  VMware VVol
  パフォーマンス
  マップ

各項目に対応するウィンドウについての詳細情報は、HPE 3PAR StoreServ Management Console ユーザーガイドの Main Console のクイックツアーを参照してください。これらの機能の使用方法については、HPE 3PAR StoreServ Management Console オンラインヘルプを参照してください。

詳しくは

HPE Storage Information Library

SSMC および MC によるストレージシステム管理

HPE 3PAR オペレーティングシステム 3.2.2 のリリースにより、SSMC は、3PAR OS 3.2.2 およびそれ以降のバージョンをサポートする 3PAR アレイのデフォルトの管理ツールとなりました。HPE 3PAR Management Console（MC）の最後のメジャーリリースは 4.7 です。MC およびその機能についての詳細は、各バージョンの MC ユーザーガイドを参照してください。

3PAR CLI についての詳細は、最新版の HPE 3PAR OS Command Line Interface Reference および HPE 3PAR OS コマンドラインインターフェイス管理者ガイドを参照してください。

最新のドキュメントは、HPE Storage Information Library で参照できます。

詳しくは

SSMC でサポートされている機能（カテゴリ別）(23 ページ)

HPE Storage Information Library

SSMC でサポートされている機能（カテゴリ別）

カテゴリ	機能	SSMC 3.4 でのサポート
VMware VVol 管理	ストレージコンテナー管理 仮想マシンのマッピング	あり
ハードウェア管理	DAR 暗号化	あり
	FIPS 140-2 のサポート（EKM 用）	表示のみ
	ポートでの iSCSI VLAN タグのサポートの構成および表示	あり
ヘルス管理	イベント	なし（CLI でサポート）
	アラート	あり
	タスク	あり
オンラインインポート	従来の 3PAR および非 3PAR ソースからの Peer Motion	あり
連携（Peer Motion）	3PAR システム間での双方向 Peer Motion	あり
	Smart SAN	あり
プロビジョニング	Adaptive Optimization	あり
	Adaptive Flash Cache	あり （3PAR OS 3.2.1 以降）
	Dynamic Optimization	あり
	重複排除	あり （3PAR OS 3.2.1 MU2 以降）
	圧縮	あり
	CPG のコンパクション	あり
	ポリシー（テンプレート）	あり（仮想ボリュームのみ）

表は続く

カテゴリ	機能	SSMC 3.4 でのサポート
	物理的コピー（クローン）	あり
	仮想ボリュームの変換	あり
	Smart SAN	あり
	仮想ボリュームの圧縮	あり （3PAR OS 3.2.1 以降）
Remote Copy	RC 構成の作成	あり
	RC 構成の編集（新しいシステムを追加）	あり
	ターゲットの削除	あり
	ターゲットの編集	あり
	ターゲットへのリンクの追加	あり
	ターゲットからのリンクの削除	あり
	RC ポートの構成	あり
	RC グループの作成	あり
	RC グループの起動	あり
	RC グループの編集	あり
	RC グループの削除	あり
	RC グループの停止	あり
	RC グループの同期	あり
	フェイルオーバー	あり
	フェイルオーバーの取り消し	あり
	回復	あり
	復元	あり
	Peer Persistence	あり
	3 データセンター（3DC）の Peer Persistence	あり
セキュリティとドメイン	ドメイン管理	あり

表は続く

カテゴリ	機能		SSMC 3.4 でのサポート
	LDAP		あり
	Federal Information Processing Standard（連邦情報処理規格）（FIPS）		あり
	Two-Factor 認証（2FA）		あり
パフォーマンスとレポート	AO 構成	領域 IO 密度	あり
		累積領域 IO 密度	あり
		スペース移動	あり
	CPG	領域 IO 密度	あり
		累積領域 IO 密度	あり
		スペース	あり
	物理ドライブ	PD 使用 - 総 IOPS	あり
		I/O 時間とサイズの分散	あり
		スペース	あり
		パフォーマンス統計	あり
	ポート（データ）	ディスク - 総スループット	あり
		ホスト - 総スループット	あり
		Peer - 総スループット	あり
		RCFC - 総スループット	あり
		RCIP - 総スループット	あり
		I/O 時間とサイズの分散	あり
		パフォーマンス統計	あり
	VLUN	I/O 時間とサイズの分散	あり

表は続く

カテゴリ	機能		SSMC 3.4 でのサポート
		パフォーマンス統計	あり
	仮想ボリューム	スペース	あり
	仮想ボリュームセット	QoS	あり
	ドメイン	QoS	あり
	コントローラーノード	CPU パフォーマンス	あり
		キャッシュパフォーマンス	あり
	論理ドライブ	I/O 時間とサイズの分散	なし
		スペース	なし
		パフォーマンス統計	いいえ
詳細分析			
カスタムチャート	物理ドライブ		あり
	論理ドライブ		なし
	仮想ボリューム		あり
	VLUN		あり
	ポート（データ）		あり
	ポート（コントロール）		あり
	iSCSI		あり
	iSCSI セッション		あり
	CMP ノード		あり
	仮想ボリュームのキャッシュ（以前は CMP VV）		あり
	CPU		あり
	Remote Copy リンク		あり
	Remote Copy VV		あり
	FCoE		あり

表は続く

カテゴリ	機能	SSMC 3.4 でのサポート
	QoS	あり
	ノードのリンク	あり

詳しくは

SSMC の互換性および相互運用性(28 ページ)

SSMC の互換性および相互運用性

サポートされているブラウザー、サーバーモデル、ファームウェア、およびオペレーティングシステムについての最新の詳細情報は、**SSMC の情報への SPOCK でのアクセス**を参照してください。

SSMC の情報への SPOCK でのアクセス

手順

1. ブラウザーから SPOCK（**https://h20272.www2.hpe.com/spock/**）へログインします。
2. SPOCK ホームページの左ナビゲーションペインを表示し、Software 見出しまで下にスクロールします。
3. **Array SW: 3PAR** をクリックします。
4. 3PAR Array Software ウィンドウを表示し、HPE 3PAR Operating System Software: Array Software 見出しまで下にスクロールします。
5. HPE 3PAR StoreServ Management Console の下の **HPE 3PAR SSMC** をクリックします。

システム要件

最小システム要件は以下のとおりです。

- SSMC 仮想アプライアンスでは、HPE は、（オペレーティングシステムではなく）ハイパーバイザーのみへの SSMC のデプロイをサポートしています。以下のハイパーバイザーがサポートされます。
  - VMware ESXi バージョン 6.0、6.5、6.7
  - Microsoft Hyper-V Server 2012 R2、Microsoft Hyper-V Server 2016
- サーバーサイジングについては、**サーバーサイジング情報**を参照してください。
- 連携のメンバーシップおよび互換性には、以下の要件があります。
  - 3PAR オペレーティングシステム 3.2.2 以降
  - Peer Motion、ストレージ連携、および Online Import ライセンス
  - ケーブル接続およびポート構成の要件（**HPE Storage Information Library** を参照）。

  重要: 1 つのストレージ連携を管理できるのは、1 つの SSMC インスタンスのみです。
- HPE Recovery Manager Central（RMC）の HPE 3PAR SSMC との互換性には、次の前提条件を満たしている必要があります。
  - HPE 3PAR オペレーティングシステム 3.2.2 以降をインストールします。
  - 同じ HPE StoreServ ストレージシステムに SSMC と RMC を構成します。
  - SSMC が HTTP を使用して RMC に接続できることを確認します。
  - RMC で保護ポリシーを作成します。

注記:

- HPE 3PAR SSMC の **RMC 認証情報**によって、最大 4 つの HPE RMC インスタンスを追加できます。
- 現在 SSMC は RMC 5.x.x 以降のバージョンをサポートしています。

詳細については、HPE Storage Information Library の HPE Recover Manager Central（RMC）のドキュメントを参照してください。

サーバーサイジング情報

SSMC をデプロイする際の必要なサーバーサイジングの考慮事項を以下に示します。

デプロイの構成	管理対象アレイの数	管理対象オブジェクトの数	管理対象 vCPU の数	システムメモリ
小	8	128 K	4	16 GB
中	16	256 K	8	32 GB
大	32	500 K	16	48 GB

SSMC でサポートされているブラウザー

HPE 3PAR StoreServ Management Console（64 ビット推奨）に接続する場合、以下のブラウザーがサポートされています。

- Microsoft Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

最新バージョンについての情報は、**SSMC の情報への SPOCK でのアクセス**を参照してください。

注記: HPE では、SSMC の操作性とパフォーマンスの向上のため、Google Chrome の使用をお勧めしています。

SSMC でサポートされている HPE 3PAR StoreServ ストレージアレイ

- HPE 3PAR StoreServ 7000 ストレージシリーズ
- HPE 3PAR StoreServ 8000 ストレージシリーズ
- HPE 3PAR StoreServ 9000 ストレージシリーズ
- HPE 3PAR StoreServ 10000 ストレージシリーズ
- HPE 3PAR StoreServ 20000 ストレージシリーズ

SSMC 2.2 以降では、最大 32 台の 3PAR StoreServ ストレージアレイを接続および管理できます。

最新の情報にアクセスするには、**SSMC の情報への SPOCK でのアクセス**を参照してください。

SSMC でサポートされている HPE 3PAR オペレーティングシステム

- HPE 3PAR OS 3.2.1 およびすべての MU（HPE 3PAR StoreServ 7000 および 10000 ストレージアレイ）
- HPE 3PAR OS 3.2.2 およびすべての MU（HPE 3PAR StoreServ 7000、8000、10000、および 20000 ストレージアレイ）
- HPE 3PAR OS 3.3.1 およびすべての MU（HPE 3PAR StoreServ 7000、8000、9000、10000、および 20000 ストレージアレイ）

最新の情報にアクセスするには、SSMC の情報への SPOCK でのアクセスを参照してください。

SSMC でサポートされているプロキシ設定

インターネットに接続されている場合、SSMC は HTTPS v1.2 のみでプロキシをサポートしています。SSMC では、Socket Secure（SOCKS）プロキシはサポートされていません。

SSMC のデプロイ情報

SSMC はサーバーベースであり、SSMC サーバーは、ストレージアレイを監視するために継続的に動作します。ユーザーは、SSMC サーバーに Web ブラウザーでログインし、管理データを参照します。

複数ネットワークセッション

SSMC などの、3PAR StoreServ アレイ用の管理ツールは、アクティビティを監視し、管理機能を提供するために、アレイとのネットワークセッションを開く必要があります。SSMC は、管理サーバーの各インスタンスから、管理対象の各アレイへのネットワークセッションを複数開きます。ユーザーがブラウザーセッションを閉じた後も、SSMC サーバーはアレイを監視し続けます。これは、SSMC サーバーがデータを収集するため、アレイへの接続を保持することを意味します。

サーバーのインストール

SSMC のインストールは、VMware や Hyper-V などの仮想化環境でサポートされています。HPE では、VMware Workstation プレーヤーのような Type 2 ハイパーバイザーではなく Type 1 ハイパーバイザーに SSMC をインストールすることをお勧めします。

通信

SSMC サーバーと通信するためのデフォルトの URL は、`https://<IP_address_or_DNS_name>:8443` です。

SSMC には、アレイへの接続をユーザーが管理できる**接続**画面もあります。ユーザーは、SSMC の**セキュリティ**メニューからこの画面にアクセスできます。

HPE 3PAR StoreServ Management Console ユーザーガイドを参照してください。

SSMC の連携要件

SSMC で使用される連携システムおよび移行ソースは、以下の要件を満たす必要があります。

- 連携システムには、以下の要件があります。
  - Peer モードで構成されているポートが 2 つあること（パートナーノードに接続している必要がありますが、スロット番号とポート番号が同じである必要はありません）。システム間通信およびデータ転送用に排他的に使用され、ホスト I/O に使用することはできません。
  - ポートがファブリックスイッチへケーブル接続されていて、レディ状態であること（3PAR OS 3.2.2 以降が必要）。

- 連携の移行ソースには、以下の要件があります。
  - ホストモードで構成されているかまたは空きのポートが 2 つあること（パートナーノードに接続している必要がありますが、スロット番号とポート番号が同じである必要はありません）。
  - ポートがファブリックスイッチへケーブル接続されていて、レディ状態であること。
  - Smart SAN による Target-driven ゾーニングであること。
  - 連携構成のゾーニングの自動作成を有効にするには、Smart SAN をサポートするファイバーチャネルスイッチがあること。
  - 連携の同期化アクションまたは構成のインポートアクションを使用しているときにゾーニングを自動作成するには、スイッチに Brocade Fabric OS v8 以降が必要（HPE Storage Information Library で入手できる HPE 3PAR Storage Federation を参照してください）。

詳しくは

HPE Storage Information Library

SSMC のセキュリティ設定

認証機関、Two-Factor 認証、FIPS について詳しくは、HPE 3PAR StoreServ Management Console 管理者ガイドおよび HPE 3PAR StoreServ Management Console ユーザーガイドを参照してください。

SSMC の LDAP 設定

LDAP サーバーは、3PAR StoreServ ストレージシステムアレイへの接続に使用される認証方法です。HPE 3PAR SSMC を使用して、StoreServ アレイに LDAP 認証を構成できます。

SSMC は、LDAP サーバーの情報を使用して、LDAP ユーザーの認証および承認を行います。複数のストレージシステムが同じ LDAP サーバーを使用している場合、承認されたユーザーは、同じ LDAP 構成のすべてのサーバーにアクセスするために同じ認証情報を使用できます。

HPE 3PAR OS には、ストレージシステムユーザーの認証および承認に LDAP サーバーを使用するように構成できる LDAP クライアントが含まれています。

SSMC の LDAP 設定を構成するには、HPE 3PAR StoreServ Management Console ユーザーガイドを参照してください。

SSMC の証明書

SSMC は、ブラウザー証明書、アレイ証明書、および Two-Factor 認証証明書の 3 タイプの証明書を使用します。

ブラウザー証明書 – SSMC と企業ネットワーク間の接続を検証します。デフォルトでは自己署名証明書が SSMC で使用され、それによりブラウザーでセキュリティ警告が表示されます。SSMC の自己署名証明書を CA 署名証明書で置き換えると、ブラウザーの警告が表示されなくなります。

アレイ証明書 – SSMC サーバーと 3PAR アレイ間の接続を検証します。各アレイには、それぞれ証明書があり、個別に管理する必要があります。ただし、共通の CA 証明書チェーンが証明書にある場合は、すべてのアレイに対してその証明書チェーンを 1 回で SSMC にインポートすることができます。証明書チェーンについての詳細は、Oracle の **keytool** の Web サイトまたは **openssl** の Web サイトを参照してください。

CA 証明書の管理に利用できる方法は多数ありますが、Hewlett Packard Enterprise では、Java の `keytool` および `openssl` のみを対象とします。

Two-Factor 認証証明書 – Two-Factor 認証のみを備えた環境で使用されます。SSMC がストレージアレイに対して固有情報を証明できるようにします。クライアント用途のフラグを設定する必要があります。

警告: SSMC の以前のバージョンからの移行により、ターゲットアプライアンスで構成されている CA 証明済み証明書が置き換えられます。HPE では、移行後にのみ、アプライアンスの CA 署名済み証明書を構成することをお勧めします。移行前にアプライアンスの CA 署名済み証明書を構成する場合は、もう一度アプライアンスを構成しなければならない場合があります。

詳しくは

SSMC 用の CA 署名付き証明書の管理(33 ページ)
FIPS のキーストアエントリーの変更(45 ページ)
SSMC 用の CA 署名アレイ証明書の管理(38 ページ)
SSMC での Two-Factor 認証の処理(40 ページ)

SSMC 用の CA 署名付き証明書の管理

前提条件

証明書に関連付けられているテキストファイルを編集する前に、以下のベストプラクティスおよびドキュメントを参照してください。

- **Keytool - Key and certificate management tool** を参照します
- **Jetty how to for configuring SSL** を参照します
- **Jetty how to for secure passwords** を参照します

クライアントの Web ブラウザーへのルート証明書および中間 CA 証明書のインポート

1. Microsoft Internet Explorer で、**ツール** > **インターネット オプション** > **コンテンツ** > **証明書**の順に移動します。
2. **インポート**をクリックし、ウィザードを使用して、信頼されたルート証明機関ストアにルート証明書をインポートします。
3. **インポート**をクリックし、ウィザードを使用して、中間証明機関ストアに中間証明書をインポートします。

SSMC 用の CA 署名ブラウザー証明書の作成

デフォルトでは自己署名証明書が SSMC で使用され、それによりブラウザーでセキュリティ警告が表示されます。SSMC の自己署名証明書を CA 署名証明書で置き換えると、ブラウザーの警告が表示されなくなります。

Java の keytool による、SSMC CA 署名済みブラウザー証明書の作成

前提条件

- 以下の手順では、Java の keytool を使用して、公開鍵と秘密鍵を管理します。**keytool** は`/opt/hpe/ssmc/ssmcbase/fips/jre/bin` にあります。このディレクトリをパスに追加するか、または以下の手順で使用されている keytool コマンドにこのパスをプリペンドしてください。

  詳しくは、**http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html** を参照してください。
- サイトで CA 署名済み証明書を取得するために必要な適切な証明書情報を収集します。これには、DNS、組織名、組織単位、および市、都道府県、国を使用してアクセス可能な、SSMC アプライアンスの完全修飾ドメイン名（FQDN）が含まれます。
- 組織の認証局と、認証局要求を送信する場所を把握してください。
- 企業の Web サイトから、PEM エンコードされたルート証明書および中間 CA 証明書をダウンロードしてください。
- ルート証明書および中間 CA 証明書を、クライアントの Web ブラウザーにインポートしてください（**クライアントの Web ブラウザーへのルート証明書および中間 CA 証明書のインポート**を参照してください）。
- FIPS を有効にした後（推奨しません）、このキーストアを作成している場合、キーストアに追加の変更を行う必要があります。

手順

1. `ssmcadmin` として SSMC アプライアンスにログインし、TUI から **X** を押してシェルにエスケープします。
2. バックアップを保存するデフォルトのキーストアの名前を変更します。
   `ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ mv keystore keystore.orig`
3. keytool を使用して、新しいキーストアファイルに新しい公開鍵/秘密鍵のペアを作成します。
   `keytool -genkeypair -keystore keystore -alias jetty -keyalg RSA`

   a. プロンプトで、キーストアのパスワードを入力します。キーストアを新たに作成している場合は、適切なパスワードを設定し、それをキーストアのパスワードとして書き留めておきます。
   b. 前提条件の一部として収集した証明書情報を入力します。組織の正しい情報を入力してください。以下のような出力が得られます。
      `CN=<FQDN.com>, OU=<unit_name>, O=<company_name>, L=<city>, ST=<state>, C=<country>`
   c. セキュリティ情報を正しく入力したことを確認します。**はい**をクリックして続行するか、または**いいえ**をクリックして、提供された情報を編集します。
   d. プロンプトで、キーの新しいパスワードを入力するか、**Enter** キーを押して、キーのパスワードとして既存のキーストアのパスワードを使用します。このパスワードを `KeyManager` のパスワードとして書き留めておきます。

4. 証明書署名要求（CSR）を生成します。
   `keytool -certreq -keystore keystore -alias jetty -file <certificate.request.txt>`
5. 特定のファイルに応答出力をリダイレクトし、`cat` コマンドを使用して画面上に内容を表示します。
   `cat <certificate.request.txt>`
6. ファイルの内容（BEGIN および END 行を含む）を、切り取り/貼り付けバッファーにコピーします。
   ファイルは、以下のような内容になります。

```
-----BEGIN NEW CERTIFICATE REQUEST-----

MIIDAzCCAesCAQAwgY0xCzAJBgNVBAYTAlVTTREwDwYDVQQIEwhDb2xvcmFkbzEZMBcGA1UEBxM
Q

Q29sb3JhZG8gU3ByaW5nczEYMBYGA1UEChMPSGV3bGV0dC1QYWNrYXJkMQ0wCwYDVQQLEwRTU01
D

MScwJQYDVQQDEx5ib3VsZGluYjQuYW1lcmljYXMuaHBxY29ycC5uZXQwggEiMA0GCSqGSIb3DQE
B
    . . .
    jksX/6ml5BHOwjjJuYoNtMcKk0p+wkgMusGTN0oWK3qTZsGBtKiOb
+Q0u12fVOhp6wIX3BXubl0D
    9Rj6irOLSuA7FpB0EJFaSXk4uDtzjM7AYhmkidJgPb5OudpnrN5Ftwom7CcKHyia
+RITB9NqeYZ9
    F9avjhMaJVfUfLP25B4zZPeEjO3XfgFp9SqUyC/
WubeuawoWFgyT6rx6ybdyJTKkP0VY3F39YlMY
    P8wAklZlhagi84SkC369DN5xE08CkLtSg+4A1/
dqaRkobZXmc1UIefPX1amdAgMBAAGgMDAuBgkq
    hkiG9w0BCQ4xITAfMB0GA1UdDgQWBBQSCOpXLIzpy21zVkM1n4/
BOShU6TANBgkqhkiG9w0BAQsF
    . . .
    diE9nfpu2J4z9/8Hi+wKOm6h/ania17hGJ2X+rPaSdoHuDN0YuPKLoGv+lj/Nen
+kLN5dVwydAsf
```

```
    E84/8X+LZiqlH0dlt2w+7Lo8nRdQOMfgxgdsoJLB6HISEfdG19fYGJavmraz
+2tkIKjgdgdG3ipq

6ppzN3Cn2lGpAEW74+YNhSTJamrFtB4REt1PO5S0xzhtx5qYTyukzJTMBxm19N7r92htvv6hApN
P
    B0XlyGdnCwsSterAsKYUyxg2kIRSvXPT+SPUIeC/VZHMtw==
    -----END NEW CERTIFICATE REQUEST-----
```

7. 企業のセキュリティサイトに移動し、コピーされているファイル情報を使用して、CA 署名済み証明書を要求します。

   CA 署名済み証明書が PEM エンコーディングの X.509 証明書形式に準拠していることを確認します。

8. CA 署名済み証明書を、結果の電子メールまたは Web サイトから取得します。これは、以下のような内容になります。

```
-----BEGIN CERTIFICATE-----
    MIIGoTCCBYmgAwIBAgIQL6hBGubWdXYmFXBoILHAaDANBgkqhkiG9w0BAQUFADCB
    njEPMA0GA1UEChMGaHAuY29tMRowGAYDVQQLExFJVCBJbmZyYXN0cnVjdHVyZTEL
    MAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQtUGFja2FyZCBDb21wYW55MUAw
    PgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0ZSBDbGFzcyAyIENlcnRpZmlj
    YXRpb24gQXV0aG9yaXR5MB4XDTE1MDIyODAwMDAwMFoXDTE2MDIyODIzNTk1OVow
    XTEgMB4GA1UEChQXSGV3bGV0dC1QYWNrYXJkIENvbXBhbnkxEDAOBgNVBAsUB1Nl
    cnZlcnMxJzAlBgNVBAMTHmJvdWxkaW5iNC5hbWVyaWNhcy5ocHFjb3JwLm5ldDCC
    ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJZDjTcTlCFPnAbKh9GCCNey
    sqd0JvPOJgJhVNdXMSWxaAKX3i/X8o6OSxf/qaXkEc7COMm5ig20xwqTSn7CSAy6
    wZM3ShYrepNmwYG0qI5v5DS7XZ9U6GnrAhfcFe5uXQP1GPqKs4tK4DsWkHQQkVpJ
    eTi4O3OMzsBiGaSJ0mA9vk652mes3kW3CibsJxQfKJr5EhMH02p5hn0X1q+OExol
    V9R8s/bkHjNk94SM7dd+AWn1KpTIL9a5t65rChYWDJPqvHrJt3IlMqQ/RVjcXf1i
    . . .
    b25zaXRlY3JsLnZlcmlzaWduLmNvbS9IZXdsZXR0UGFja2FyZENvbXBhbnlIUElU
    RzIvTGF0ZXN0Q1JMLmNybIaBuWxkYXA6Ly9sZGFwLmhwLmNvbS9DTj1IZXdsZXR0
    LVBhY2thcmQlMjBQcml2YXRlJTIwQ2xhc3MlMjAyJTIwQ2VydGlmaWNhdGlvbiUy
    MEF1dGhvcml0eSxPPUhld2xldHRtUGFja2FyZCUyMENvbXBhbnksQz1VUyxPVT1J
    VCUyMEluZnJhc3RydWN0dXJlLE89aHAuY29tP2NlcnRpZmljYXRlcmV2b2NhdGlv
    bmxpc3Q7YmluYXJ5MCoGA1UdJQEB/wQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYI
    KwYBBQUHAwQwewYDVR0gBHQwcjBwBgorBgEEAQsEAwUBMGIwKQYIKwYBBQUHAgEW
    HWh0dHA6Ly9kaWdpdGFsYmFkZ2UuaHAuY29tL2NwMDUGCCsGAQUFBwICMCkaJ1Ro
    aXMgYXV0aG9yaXR5IGlzIGZvciBIUCBidXNpbmVzcyBvbmx5LjCB6QYIKwYBBQUH
    AQEEgdwwgdkwJgYIKwYBBQUHMAGGGmh0dHA6Ly9ocC1vY3NwLnN5bWF1dGguY29t
    MIGuBggrBgEFBQcwAqSBoTCBnjEPMA0GA1UEChMGbHAuY29tMRowGAYDVQQLExFJ
    VCBJbmZyYXN0cnVjdHVyZTELMAkGA1UEBhMCVVMxIDAeBgNVBAoTF0hld2xldHQt
    UGFja2FyZCBDb21wYW55MUAwPgYDVQQDEzdIZXdsZXR0LVBhY2thcmQgUHJpdmF0
    ZSBDbGFzcyAyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MA0GCSqGSIb3DQEBBQUA
    A4IBAQA1PaoebXz9gJ9O2+LG2upBVR1VrrUgPcbPOVA3Eiv+L1ZH1jTgOSqSvQ2B
    yTtq8pKuHr5LMybXpUWGtKlsirIazeka3Do8Nu7pnZH8yTc7x6ECYWAwYGi0Xr2w
    o/pJzDWU/UmmUZBZ2TuVNe5oEn6bXoeVC/v3LsHVkmKHWdI039SdRskVhfcrNaL5
    . . .
    Dm6NmvrhHeR8NSbvpDmD/raoCyZZenD0JtiMnuYMF3Vd7DtwEjSZ27BvQbs8skp+
    c6LVqo9nbzpnwrHFQIuk1W2saNxu
    -----END CERTIFICATE-----
```

   証明書を調べ、keytool ユーティリティが読み取れることを確認します。これにより、キーストアに追加する前に証明書が正しい形式（PEM）になります。

   ```
   /opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -printcert -v -file <filename>
   ```

9. CA ルート証明書、中間証明書（存在する場合）、および CA 署名済みマシン証明書を、キーストア内に置きます。すべての証明書を、この順序で同じキーストアに追加します。

   a. CA ルート証明書（ここでは、別名は `jetty` ではなく `root` です）：

```
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ /opt/hpe/ssmc/ssmcbase/
fips/jre/bin/keytool -import -alias root -keystore keystore -
trustcacerts -file <RootCA.cer>
```

```
キーストアのパスワードを入力してください:
.
.
.
この証明書を信頼しますか。[いいえ]: yes
証明書がキーストアに追加されました
```

b. 中間証明書（ - alias がないこと以外は先のコマンドと同じです）:

```
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ /opt/hpe/ssmc/ssmcbase/
fips/jre/bin/keytool -import -keystore keystore -trustcacerts -file
<IntermediateCA.cer>
```

c. CA 署名証明書（ここでは、別名は jetty です）:

```
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ /opt/hpe/ssmc/ssmcbase/
fips/jre/bin/keytool -import -alias jetty -keystore keystore -
trustcacerts -file <SignedByCA.cer>
```

すべての証明書が、同じキーストアに存在する必要があります。

10. /opt/hpe/ssmc/ssmcbase/etc/の jetty-ssl-context.xml ファイルを、新しいキーストアが使用するパスワードで更新します。

- 全体としてデフォルトパスワードをキーストアに変更した場合は、新しいパスワード（キーストアのパスワードとして書き留めたパスワード）を反映するように KeyStorePassword エントリーを更新します。
- キーストア内でパスワードを秘密鍵に変更した場合は、新しいパスワード（KeyManager のパスワードとして書き留めたパスワード）を反映するように KeyManagerPassword を更新します。
- クリアテキストパスワードを追加することも、次のコマンドを使用して新しいパスワードに難読化文字列を生成することもできます。

  ```
  /opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-
  <version>.jar org.eclipse.jetty.util.security.Password <new password>
  ```

注記: バージョンを確認するには、以下のコマンドを使用します。ls -l /opt/hpe/ssmc/jetty/lib/jetty-util-*.jar

---

11. 以下の例は、パスワードの指示がある jetty-ssl-context.xml ファイル構成を示しています。詳しくは、**Jetty HowTo** を参照してください。

```
<Set name="KeyStorePassword"><Property
name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password"
default="OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v"/></Set>
<Set name="KeyStoreType"><Property
name="jetty.sslContext.keyStoreType"
default="JKS"/></Set>
<Set name="KeyStoreProvider:><Property
name="jetty.sslContext.keyStoreProvider"/></Set>
<Set name="KeyManagerPassword"><Property
name="jetty.sslContext.keyManagerPassword"
```

```
deprecated="jetty.keymanagerpassword"
default="OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1"/></Set>
```

12. config_appliance コマンドを使用して TUI に戻ります。
13. **TUI** メニューオプション 2 を使用して、3PAR StoreServ Management Console Server サービスを再起動します。
14. FQDN（完全修飾ドメイン名）を使用してブラウザーを起動し、セッションがこの証明書を使用することを確認します。
15. FIPS を有効にした後にこの手順を完了している場合は、キーストアへの必要な FIPS の変更を完了していることを確認してください。

詳しくは

FIPS を有効にするためのキーストアの変更(45 ページ)

非 keytool 方式による、SSMC CA 署名付きブラウザー証明書の作成

openssl など、keytool 以外の方法を使用している環境では、以下の手順を使用してください。

1. ご使用中のセキュリティ環境で適切なツールおよびオプションを使用して、秘密鍵および公開証明書を作成します。たとえば、
   a. openssl genrsa –out private.key 2048
   b. openssl req –new –sha256 –key private.key –out csr.txt
   c. csr.txt を CA に送信し、署名されるようにします。

   期待される結果は、フレーズ-----BEGIN CERTIFICATE-----が入った公開証明書を含むファイルです。このファイルには、以下のものが含まれます。

   - private.key のような名前のファイル内の秘密鍵。
   - public.cer のような名前のファイル内の公開証明書（秘密鍵を使用して構築されたもの）。

2. private.key および public.cer ファイルを、以下の手順でキーストアにインポートします。
   a. 既存の SSMC キーストアファイル/opt/hpe/ssmc/ssmcbase/etc/keystore（使用しません）を削除します。
   b. プロンプトで、以下の各コマンドを入力します。

      ```
      openssl pkcs12 -inkey private.key -in public.cer -export -out jetty.pkcs12
      keytool -list -keystore jetty.pkcs12 -storetype PKCS12
      ```

      別名（多くの場合「1」）のあるエントリーを探します。
   c. 次のコマンドを入力します。前の手順で作成したエイリアスを使用します。

      ```
      /opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -importkeystore -srckeystore
      jetty.pkcs12 -srcstoretype PKCS12 -destkeystore /opt/hpe/ssmc/
      ssmcbase/etc/keystore -destalias jetty -srcalias 1
      ```

SSMC 用の CA 署名アレイ証明書の管理

この証明書の目的は、HPE 3PAR OS の固有情報を SSMC に対して証明することです。この証明書は、目的フラグとして SSL Client が設定されていれば、内部の CA 要件を満たすどのような方法でも作成できま

す。詳細は、**Hewlett Packard Enterprise Storage Information Library** で入手できる HPE 3PAR OS Command Line Interface Reference の `createcert` を参照してください。

SSMC で使用するための証明書情報のコピー

手順

1. SSMC に追加する証明書情報が含まれる 3PAR ストレージシステムにアクセスします。
2. 次のコマンドを入力して、3PAR アレイにインストールされている証明書のリストを表示します。
   `showcert`
3. SSL 証明書が CLI サービスに使用できる場合、この証明書をエクスポートするか、さもなければ `unified-server` で使用できる証明書をこの順序でエクスポートします（`<SSL_service>`の代わりに使用）。
4. アレイに CA 署名済み証明書がインストールされている場合は、次のコマンドを入力して、ルート CA 証明書をエクスポートします。
   `showcert -service <SSL_service> -type rootca -pem`

   その後手順 6 に進みます。

   注記: SSMC にルート CA 証明書だけをインポートすることが、PKI にとっての業界のベストプラクティスになります。アレイは TLS ハンドシェイクの一部として、信頼済みチェーンのあらゆる中間（下位 CA）証明書とともにプライマリアレイ証明書を送信します。
5. アレイに自己署名証明書がインストールされている場合は、次のコマンドを入力して、自己署名証明書をエクスポートします。
   `showcert -service <SSL_service> -type cert -pem`
6. 次のテキストの間にある証明書情報を次のテキストも含めてコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   -----END CERTIFICATE-----
   ```

   注記: `showcert` CLI コマンドで出力した証明書テキストは、PEM エンコーディングの x509 規格に準拠しています。検証とインポートが正しく機能するには、SSMC へのインポート中にまったく同じテキストの内容を保持することが重要です。
7. 証明書情報をテキストファイルに格納し、SSMC に追加できるように（**SSMC への SSMC アレイ証明書の追加**を参照）そのファイルをアクセス可能な場所に保管します。

SSMC への SSMC アレイ証明書の追加

前提条件

アレイ証明書から証明書テキストをコピーします（**SSMC で使用するための証明書情報のコピー**を参照してください）。

手順

1. SSMC の Administrator Console にログインします。
2. **アクション**を選択してから、**証明書の管理**をクリックします。
3. **証明書の追加**をクリックしてから、証明書テキストをボックスに貼り付けます。
4. **検証**をクリックしてから、**OK** をクリックします。

SSMC CA 署名済みアレイ証明書の受諾

CA 署名証明書を持つストレージシステムに最初に接続しようとするとき（または、最後のログイン以降にその証明書が CA 署名証明書に変更されているとき）、システムは、ユーザーが証明書を受け入れることを要求します。

重要: 証明書を受け入れることができるのは、ロールが **SUPER**、**BROWSE**、または **EDIT** のユーザーだけです。

手順

1. SSMC の Administrator Console にログインします。
2. 証明書の受け入れを必要とするストレージシステムを選択します。
3. **アクション→証明書の承諾**の順に選択します。
4. （オプション）証明書の詳細を表示するには、サブジェクト名の横にある矢印をクリックします。
5. **承諾とキャッシュ**をクリックし、**OK** をクリックします。

   証明書の期限が切れている場合、ストレージシステムへ接続するには、証明書を更新する必要があります。

ストレージシステムへの接続

手順

1. SSMC の Administrator Console にログインします。
2. 接続していないシステムを選択します。
3. **アクション**をクリックしてから、**接続**をクリックします。

SSMC での Two-Factor 認証の処理

SSMC X.509 の Two-Factor 認証ソリューションでは、以下のユーザー認証の手順を行います。

1. SSMC は、Two-Factor 認証用に構成されている場合、クライアント証明書をブラウザーに要求します。
2. SSMC のアクセスに使用された Web ブラウザーは、クライアント証明書を SSMC に提示します。
3. SSMC は、ブラウザーのクライアント証明書の発行者の信頼性を検証します。
4. ブラウザーの証明書の発行者を信頼した場合、SSMC は、クライアント証明書のユーザー識別子を解析します。
5. SSMC は、ブラウザーのクライアント証明書から解析したユーザー識別子に加え、自分のクライアント証明書をストレージアレイに提示します。
6. ストレージアレイ上の 3PAR OS は、SSMC のクライアント証明書の発行者の信頼性を検証します。
7. ストレージアレイは、SSMC の証明書の発行者を信頼した場合、サービスアカウントユーザーを使用して、構成されている LDAP サーバーにバインドします。
8. 3PAR OS は、SSMC が提供したユーザー識別子と一致する LDAP エントリーを検索します。

9. 3PAR OS は、一致する LDAP ユーザーを見つけた場合、ユーザーロールを決定するために、LDAP グループのメンバーシップを検証します。
10. ユーザーは、決定された識別子およびロールで、SSMC にログインします。

重要: SSMC 管理コンソールで、Two-Factor 認証がすべてのシステムで正しく構成されていることを確認します。構成が 1 つ誤っているだけでも、SSO ログインの機能に影響を与える可能性があります。

SSMC の X.509 の Two-Factor 認証ソリューションに必要な LDAP 設定

LDAP 構成の共通の要件に加えて、Two-Factor には、追加の LDAP 設定が必要です。これらの設定は、SSMC Main Console の **LDAP 構成の作成**画面および **LDAP 構成の編集**画面の**詳細オプション**にあります。詳細は、HPE 3PAR StoreServ Management Console オンラインヘルプを参照してください。

- **サービスアカウントの設定** – サービスアカウントユーザーのユーザー名およびパスワードを指定します。Two-Factor 認証には、LDAP ユーザーの認証および権限付与を行うための、サービスアカウントというプロキシユーザーが必要です。サービスアカウントの LDAP ユーザー名は、フルバインド DN です。必要な権限には、ユーザーおよびグループのサブツリーの読み取り権限が含まれます。
- **X509 認証** – 証明書フィールドおよび LDAP 属性を指定します。
  - 証明書フィールドは、システムがユーザー ID として使用する証明書フィールドを指定します。指定できるのは、`subject` または `subjectAlt` です。
    - `subject` フィールドは、サブジェクト属性を使用します。たとえば、証明書の `DN E=user@example.com,OU=Engineering,O=Example Corp` というサブジェクトは、`subject:E*`または `subject:E*,OU,O` のいずれかの値が、電子メールアドレスフィールドをユーザー識別子として使用することを示します。
    - `subjectAlt` フィールドは、デフォルトが `rfc822Name` の、エンコードタイプを使用します。このエンコードタイプは、メールアドレスを指しています。

      エンコードタイプが `otherName` の場合、プリンシパル名（OID 1.3.6.1.4.1.311.20.2.3）値が想定されます。
  - `LDAP attribute` フィールドは、ユーザー識別子に一致させる、LDAP エントリーの属性を指定します。使用される属性は、LDAP スキーマ全体およびユースケースによって異なります。たとえば、ldap-2FA-cert-field 属性に `subject:E*`が設定されている場合、ユーザー識別子は電子メールアドレスで、対応する LDAP 属性は `mail` です。

SSMC の Two-Factor 認証の有効化

構成ファイルの以下の設定を変更します。

手順

1. クライアント証明書を有効にします。
   a. `/opt/hpe/ssmc/ssmcbase/etc/`ディレクトリで `jetty-ssl-context.xml` を見つけます。
   b. テキストエディターで `jetty-ssl-context.xml` を開きます。
   c. このファイル内で `Set name="WantClientAuth"`行を見つけ、設定を `true` に変更します（デフォルトは `false` になっています）。

```
<Set name="WantClientAuth">
<Property name="jetty.sslContext.wantClientAuth" deprecated="jetty.ssl.wantClientAuth" default="true"/>
</Set>
```

SSMC は、クライアントのブラウザーにクライアント証明書を要求します。

2. Two-Factor 処理を有効にします。

   a. `/opt/hpe/ssmc/ssmcbase/resources/`ディレクトリで `ssmc.properties` ファイルを見つけます。

   b. テキストエディターで `ssmc.properties` を開きます。

   c. ファイルに以下の行を追加します。
   `security.twofactor.enabled = true`

   この設定を有効にすることで、SSMC ホストのリモートにあるホストからログインするユーザーに対して、Two-Factor 認証の使用が強制されます。

SSMC の証明書および X.509 の Two-Factor 認証

SSMC では、2 つのクライアント証明書および 2 つのサーバー証明書が使用されます。これらの証明書は一般的に、同じルート CA と中間 CA のセットにより署名されます。SSMC の X.509 の Two-Factor 認証ソリューションは、これらの証明書のいくつかを認証目的で使用します。

重要: SSMC で FIPS をすでに有効にしており、ここで Two-Factor 認証を有効にする場合は、必ず**FIPS のキーストアエントリーの変更**の説明に従って適切な変更をしてください。

- **証明書 A** – SSMC に対してブラウザーの身元を証明するクライアント証明書です。

  この証明書は、SSMC にログインするユーザーを示しています。この詳細は、証明書使用モデル（スマートカード、仮想スマートカード、ソフトウェアトークン）によって異なります。CAC（Common Access Card）の場合、証明書は、物理スマートカード上に存在します。仮想スマートカードの場合、証明書には、クライアントコンピューター上の物理 TPM（Trusted Platform Module）チップに格納された秘密鍵があります。ソフトウェアトークンの場合、証明書全体が、オペレーティングシステムまたはブラウザーに存在します。

  X.509 の証明書を管理するためのガイドラインを、以下に示します。

  - Java の keytool を使用して、Java のトラストストア`/opt/hpe/ssmc/ssmcbase/etc/truststore` に、クライアント証明書の信頼性をインストールします。

    例：`/opt/hpe/ssmc/jre/bin/keytool -keystore truststore -import -trustcacerts -alias <alias> -file <certificate file>`

  - トラストストアのデフォルトのパスワードは、**BuyMore3PAR!**です。このパスワードを変更すると、`/opt/hpe/ssmc/ssmcbase/etc/jetty-ssl-context.xml` に構成の変更を行う必要があります。

  - 次のファイルを使用して新しいパスワードの難読化文字列を生成します。

    ```
    /opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-<version>.jar
    org.eclipse.jetty.util.security.Password <new password>
    ```

  - `/opt/hpe/ssmc/ssmcbase/etc/jetty-ssl-context.xml` にある `TrustStorePassword` プロパティの、トラストストアの既存パスワードの難読化文字列を置き換えます。

- **証明書 B** – ブラウザーに対して SSMC の身元を証明するサーバー証明書です（厳密には、Two-Factor 認証には必要ありません）。

この証明書は、SSMC のインストール時に、自己署名サーバー証明書として自動的に作成されます。この証明書は、CA によって署名された証明書で置き換えることができます。

この証明書は、Java のキーストア `/opt/hpe/ssmc/ssmcbase/etc/keystore` に存在します。証明書 B を、Java の keytool で管理することができます（**SSMC 用の CA 署名ブラウザー証明書の作成**を参照してください）。

- **証明書 C** – ストレージアレイに対して SSMC の身元を証明するクライアント証明書です。

  この証明書は、デフォルトでは存在しません。IT ポリシーに応じてこの証明書を生成し、目的フラグに SSL Client を設定してください。

  X.509 の証明書を管理するためのガイドラインを、以下に示します。

  - 生成されると、この証明書は`/opt/hpe/ssmc/ssmcbase/data/StoreServMC/security/TPDServerKeyStore` に存在するようになります。Java の keytool を使用して、この証明書を管理できます。たとえば、`keytool -destkeystore TPDServerKeyStore -importkeystore -alias <alias in p12 file> -srcstoretype pkcs12 -srckeystore <p12 file with client key and certificate>`です。

    重要: Two-Factor 認証を使用する場合、同じエイリアス情報を含むように `ssmc.properties` ファイルを編集する必要があります。次の形式になります。

    `tpd.server.key.alias = <alias in p12 file>`

  - Java の keytool を使用して、Java のトラストストア`/opt/hpe/ssmc/ssmcbase/etc/truststore` に、クライアント証明書の信頼性をインストールします。

    例：`keytool -keystore TPDServerKeyStore -import -trustcacerts -alias <alias> -file <certificate file>`

  - トラストストアのデフォルトのパスワードは、**BuyMore3PAR!**です。このパスワードを変更する場合は、新しい情報を`/opt/hpe/ssmc/ssmcbase/resources/ssmc.properties` に追加します。

    重要: キーストアのパスワードとキーマネージャーのパスワードが異なる場合、両方のパスワードを `ssmc.properties` に追加する必要があります。これは、Two-Factor 認証を有効にする場合に特に重要です。以下の構文を使用します。

    `tpd.server.keystore.password = <keystore password>`

    `tpd.server.keymanager.password = <keymanager password>`

  - クリアテキストパスワードを追加することも、次のコマンドを使用して新しいパスワードに難読化文字列を生成することもできます。

    ```
    /opt/hpe/ssmc/jre/bin/java -cp /opt/hpe/ssmc/jetty/lib/jetty-util-<version>.jar org.eclipse.jetty.util.security.Password <new password>
    ```

    .

  - `tpd.server.keystore.password` プロパティを、クリアテキストのパスワードの値か、または `OBF:` を前に付けた難読化パスワードとともに、`/opt/hpe/ssmc/ssmcbase/resources/ssmc.properties` ファイルに追加します。たとえば、`OBF:18rk1siq1pyv1k701l8b1vnw1vn61l4z1k761pvr1sgs18pq` です。

- **証明書 D** – SSMC に対して 3PAR ストレージアレイの身元を証明するサーバー証明書です。

  3PAR ストレージアレイは、この証明書を自己署名サーバー証明書として自動的に作成します。この証明書は、3PAR ストレージアレイの CLI `createcert unified-server -csr -CN`

storagearray1.example.com を使用して証明書署名要求を生成することにより、置き換えることができます。

X.509 の証明書を管理するためのガイドラインを、以下に示します。

- CA 公開証明書と中間 CA 公開証明書を、PEM テキスト形式で 1 つのファイルに結合します。証明書 D の発行者と同じでなければ、cat int_ca.pem root_ca.pem > ca_bundle.pem を使用して、SSMC のクライアント証明書 C の発行者を含めます。
- 新しいサーバー証明書と CA バンドルを、importcert unified-server cert.pem ca_bundle.pem を使用してインストールします。
- 証明書 D のトラストチェーンを、PEM テキスト形式で 1 つのファイルにエクスポートします。このファイルを、SSMC ホスト上のパス /opt/hpe/ssmc/ssmcbase/data/StoreServMC/security にコピーします。これにより SSMC は、Admin Console に接続されている新しいサーバー証明書をストレージアレイが信頼することを認識および許可することができます。

詳しくは

FIPS のキーストアエントリーの変更(45 ページ)

SSMC 管理者ログインの保護

必要に応じて管理者ログインを選択的に有効にすることにより、SSMC 管理者認証情報を保護できます。SSMC が使用されていない場合は、管理者ログインを無効にします。管理者ログインを有効にするには、以下の手順を実行します。

1. ssmcadmin として SSMC アプライアンスにログインします。
2. パスワードを入力します。
3. アプライアンスターミナルユーザーインターフェイス（TUI）に移動します。
4. Main Menu を選択します。
5. Advanced Features を選択します。
6. Disable Administrator Console Login を選択します。
7. Y を選択します。

注記: デフォルトでは、SSMC 管理コンソールのログインは有効です。デフォルト設定を編集すると、SSMC が再起動します。短いダウンタイムが予想されるので、適切に計画してください。

SSMC における Federal Information Processing Standard（連邦情報処理規格）（FIPS）

Federal Information Processing Standards（FIPS）は、暗号化モジュールを承認するための、米国連邦政府標準です。SSMC は、FIPS 140-2 レベル 1 で検証された暗号化モジュールを使用できます。FIPS モードが有効になっている場合、これらのモジュールは検証基準に適合した動作を行います。

SSMC での FIPS の有効化

前提条件

1. **SSMC 用の CA 署名付きブラウザー証明書の作成**
2. **SSMC 証明書での Two-Factor 認証のチェック**

重要: FIPS モードが有効な SSMC は、HPE 3PAR OS 3.2.2 MU5 以前の SSMC 管理アレイをサポートしていません。ただし、ソース HPE 3PAR アレイが OS 3.1.2 または 3.1.3 で稼働している場合は、SSMC の Online Import Utility（OIU）機能を使用して移行を実行できます。その他のすべての 3PAR OS バージョンからの移行には Peer Motion Manager（PMM）を使用します。

手順

- すべての暗号モジュールに対して、SSMC で FIPS 140-2 モードを有効または無効にできます。Main Console から、設定ページのアプリケーションセクションで FIPS 設定を切り替えます（オンまたはオフ）。この設定を変更した場合、変更を有効にするために SSMC を再起動する必要があります。
- **3PAR SSMC Main Console** > **設定** > **アプリケーション**に移動して、SSMC での FIPS ステータスを表示します。

  詳しくは、HPE 3PAR StoreServ Management Console ユーザーガイドを参照してください。

FIPS のキーストアエントリーの変更

SSMC で FIPS を有効または無効にするには、CA 署名済みブラウザー証明書に対して作成されたキーストアに変更を加える必要があります。FIPS を有効にする前にブラウザー証明書を作成する場合、必要なキーストアの変更は、FIPS を有効にするときに自動的に証明書に対して行われます。

ただし、SSMC のブラウザー証明書を作成する前に FIPS を有効にする場合、キーストアに手動で変更する必要があります。Hewlett Packard Enterprise では、最初に標準の暗号化のキーストアを作成し、続いて FIPS を有効にすることを強くお勧めします。

前提条件

Java の keytool による、SSMC CA 署名ブラウザー証明書の作成

詳しくは

SSMC の証明書(33 ページ)

FIPS を有効にするためのキーストアの変更

SSMC の手順に従ってブラウザーの証明書を作成する前に FIPS を有効にしていた場合は、この手順を使用してキーストアファイルを変更します。

手順

1. 非 FIPS インストールに簡単に戻すことができるように、SSMC をインストールしたシステムから、デフォルトのキーストアの名前を変更します。

```
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ pwd
/opt/hpe/ssmc/ssmcbase/etc
ssmcadmin@server2:/opt/hpe/ssmc/ssmcbase/etc$ mv keystore keystore.nofps
```

2. `/opt/hpe/ssmc/ssmcbase/fips/jre/bin` に移動して、次のコマンドを実行します。

```
./keytool -provider
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
providerpath ../../../bcFipsJars/bc-fips-1.0.1.jar -importkeystore -
```

srckeystore /opt/hpe/ssmc/ssmcbase/etc/keystore.nofps -destkeystore /opt/hpe/ssmc/ssmcbase/etc/keystore -srcstoretype JKS -deststoretype BCFKS -srcstorepass {store password} -deststorepass {store password} -srckeypass {key password} -destkeypass {key password} -alias jetty

3. /opt/hpe/ssmc/ssmcbase/etc の jetty-ssl-context.xml ファイルを、新しいキーストアが使用するパスワードで更新します。
   - デフォルトのパスワードを全体的にキーストアに変更した場合は、**KeyStorePassword** エントリーを変更します。
   - パスワードをキーストア**内の**秘密鍵に変更した場合は、**KeyManagerPassword** を変更します。
   - jetty-util-<version>.jar ファイルは/opt/hpe/ssmc/jetty/lib にあります。

SSMC でのクライアント IP フィルタリングのサポート

SSMC は、IP アドレスによるリモートブラウザークライアントのホワイトリスト化およびブラックリスト化に、クライアント IP フィルタリングのサポート（Jetty で提供されるものなど）を使用します。管理者は、IP アドレスとサブネットをテンプレートファイル/opt/hpe/ssmc/ssmcbase/etc/jetty-ipaccess.xml に追加することにより、IP フィルタリングを構成できます。このファイルのフォーマットについて詳しくは、**https://www.eclipse.org/jetty/documentation/9.4.x/ipaccess-handler.html** にある Jetty のドキュメントを参照してください。

IP フィルタリングに対するすべての変更を有効にするには、SSMC サーバーを再起動します。

IP アドレスのブラックリスト化またはホワイトリスト化を行う前に、次の結果を検討してください。

- jetty ipaccess.xml ファイルを編集するときには注意してください。不適切に編集すると、SSMC が起動できなくなったり、SSMC が異常な動作を行う場合があります。
- IPv4 と IPv6 は、同じホストからの別々の接続として扱われます。両方のプロトコルで稼働している SSMC サーバーでは、100%のブラックリスト化またはホワイトリスト化を実現するには、IPv4 と IPv6 の両方のアドレスで IP フィルタリングを有効にしている必要があります。
- インクルードリストに 1 つ以上の IP アドレスが含まれる場合は、その他の許可される IP アドレスをすべて、インクルードリストに明示的に追加します。インクルードリストに追加されない IP アドレスは、SSMC へのアクセスが許可されません。

  △ **注意:** インクルードリストに 1 つ以上の IP アドレスが含まれる場合は、ループバック IP アドレスを 127.0.0.1 として追加します。ループバック IP アドレスがない場合、SSMC アプライアンスは不安定な状態（再起動の繰り返し）に陥る可能性があります。

- 明示的な IP アドレスをインクルードリストに追加した場合、エクスクルードリストのアドレス範囲全体を上書きします。含められた IP サブネットに関連付けられたすべての IP アドレスが除外されます。リストされた 1 つの IP アドレスだけがホワイトリスト化されます。
- 明示的な IP アドレスをエクスクルードリストに追加したときも、同様の状況が起こります。IP サブネットに含まれたすべての IP アドレスがインクルードリストにリストされている場合でも、除外された IP アドレスがこれらの IP アドレスよりも優先され、これらを除外します。

SSMC でのリモート Syslog 監査の構成

前提条件

- SSMC ホストシステムの `ssmcbase/resources/` ディレクトリに置かれた `log4j2.json` のバックアップコピーを作成します。
- JSON 対応の構文チェック機能を備えたテキストエディターを使用して、エラーを回避してください。大カッコやカンマの欠落などの `log4j2.json` ファイル内の構文エラーは、すべてのロギングの失敗を引き起こす可能性があります。
- ホストの IP アドレス、ポート番号、およびプロトコルの値を Syslog ホストシステムから収集します。
- Syslog ホストシステムで SSL を使用している場合は、Syslog ホストの信頼済みの証明書を格納しているトラストストアのパスワードが必要です。Syslog ホストの新しい信頼済みの証明書を生成するには、以下を参照してください。

  SSMC リモート Syslog appender の新しいトラストストアの生成。

手順

1. SSMC ホストシステムで、`ssmcbase/resources/log4j2.json` ファイルを探します。
2. 必要に応じて復元できるように、`log4j2.json` ファイルを変更する前にこのファイルのバックアップコピーを作成します。
3. ファイル内で **appenders** ブロックを探します。
4. `"newline"`を`"true"`に変更します。
5. 下に示した例の `host`、`port`、および `protocol` の値をご使用の Syslog ホストの値に換えたエントリーを挿入します。

   プロトコルエントリーには `tcp` または `udp` の値を含める必要があります。

   > **重要:** SSMC FIPS モードをオンに切り替えると、`"type"`エントリーは自動的に`"JKS"`から`"BCFKS"`に変更されます。FIPS には、`"BCFKS"`の`"type"`設定が必要です。

```
 "appenders" : {
     "Syslog" : {
           "host" : "192.168.1.1",
           "port" : "6514",
           "protocol" : "tcp",
           "newLine" : "false",
           "appName" : "ssmcaudit",
           "includeMDC" : "true",
           "name" : "RemoteSyslog",
           "format" : "RFC5424",
           "mdcID" : "ssmcaudit",
           "messageId" : "Audit",
           "facility" : "AUTH",
           "SSL" : {
                 "protocol" : "SSL",
                 "TrustStore" : {
                       "password" : "password here",
                       "location" : "resources/syslog-truststore",
                       "type" : "JKS"
                 }
           }
     },
```

6. ファイル内の SSL 情報を確認します。

   Syslog サーバーで SSL を使用していない場合は、SSL ブロックを省略できます。

   Syslog サーバーで SSL を使用している場合は、Syslog サーバーの信頼済みの証明書を格納したトラストストアのパスワードを入力します。

7. `log4j2.json` ファイルで `loggers` ブロックを探します。

8. `asynclogger` リストの次のエントリーのように、ファイルを編集します。

```
"loggers" : {
      "asynclogger" : [
      {
          "name" : "RemoteAudit",
          "level" : "debug",
          "additivity" : "false",
          "appender-ref" : {
              "ref" : "RemoteSyslog"
           }
      },
```

9. 変更されたファイルを `SSMC/ssmcbase/resources` フォルダーに保存します。

   新しいロギング構成はすぐに有効になります。変更が成功した場合は、リモート Syslog サーバーに、次のような監査エントリーが表示されます。

```
Oct 20 14:26:21 ssmc-host.example.com ssmcaudit "192.168.1.2",
"unknown","unknown","unknown","CREATE","foundation action","SUCCESS",
"https://192.168.1.3:8443/foundation/REST/sessionservice/sessions",
"unknown","unknown","SUCCESS"
```

SSMC リモート Syslog appender の新しいトラストストアの生成

手順

1. SSMC ホストシステムの `ssmcbase/resources` ディレクトリから、次のいずれかの Java keytool コマンドを使用して、SSMC リモート Syslog appender の新しいトラストストアを生成します。

   非 FIPS モード

```
keytool -import -trustcacerts -file ca-cert.pem -alias syslog-CA -keystore
syslog-truststore
```

   FIPS モード

```
keytool -import -trustcacerts -file ca-cert.pem -alias syslog-CA -keystore
syslog-truststore -deststoretype BCFKS -providerpath ../bcFipsJars/bc-
fips-1.0.0.jar -provider
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

2. 結果生成されるトラストストアファイルを `ssmcbase/resources` ディレクトリに置いておきます。

3. Syslog appender エントリでの SSL のパスワード値としてこのトラストストアに対して選択したパスワードを使用します（**SSMC でのリモート Syslog 監査の構成**を参照してください）。

FPG からの 3PAR アレイ全体のプッシュボタンフェイルオーバーおよびフェイルバックに対する SSMC によるサポート

HPE 3PAR OS 3.3.1 MU2 のディザスタリカバリ管理が、File Persona バージョン 1.5 によるファイルプロビジョニングまで拡張されます。ユーザーは、ファイルプロビジョニンググループ（FPG）へのフェイルオーバー、復元、リストア操作を実行できます。

フェイルオーバー中、ソースシステムの FPG はマウント解除され、ターゲットシステムにマウントされます。ソースからターゲットシステムへのファイルシステムのリカバリは最小限の実行でシームレスに行われます。

復元時も同様に、FPG はターゲットシステムからマウント解除されてソースシステムにマウントされ、Remote Copy グループを復元します。その結果、ユーザーは、ターゲットまたはソース上のファイルシステムに最小のダウンタイムでアクセスし続けられます。

フェイルオーバーではなく Remote Copy グループのパス管理を有効にした場合、内部でスイッチオーバーが行われます。ソースストレージシステムの役割とターゲットストレージシステムの役割が自動的に入れ替えられます。自動同期モードでは、システムは自動的にすべてのボリュームを回復してターゲットストレージシステムと同期させ、スイッチオーバーも実行します。Remote Copy グループは、自動同期モード中やパス管理を有効にしているときに、**正常**状態のまま保たれます。

コンプライアンス WORM

super と edit の役割を持つ 3PAR アレイユーザーは、仮想ファイルサーバーとファイルストアの両方のレベルで、コンプライアンスモードでデータ保持ポリシーを設定できます。コンプライアンスモードを有効にすると、保持属性を変更する要求はすべて、承認のためにコンプライアンス責任者（CO）に送られます。CO が要求を承認すると、ユーザーは**コンプライアンス要求の管理**キューから元の要求を実行できます。要求には、有効期限の変更、リーガルホールドの設定または削除、CO ユーザーの作成、コンプライアンス要求のキューサイズの変更などがあります。SSMC ユーザーは、現在のキューサイズやグローバルコンプライアンス承認ステータスを表示でき、グローバルオプションで変更を要求できます。

CO ユーザーは、キューのすべての要求を表示および編集（承認、拒否、または削除）できます。CO ユーザーもキューのサイズを変更できます。

SSMC アプライアンスのアップグレードに関する注意事項

1. アップグレードにより SSMC サービスが再起動します。HPE では、慎重にダウンタイムを計画するようにお勧めします。
2. ダウングレードはサポート対象外です。
3. SSMC アプライアンスのアップグレードは、SSMC 3.4 以降のリリースでサポートされます。たとえば、SSMC 3.4 から 3.4.x 以降にアップグレードできます。

前提条件

アップグレードが失敗した場合に備えて SSMC アプライアンスのバックアップを取ります。このバックアップは、データの破損やデータの損失時の SSMC インスタンスの復元に役立ちます。

SSMC アプライアンスをアップグレードするには、以下の手順に従ってください。

1. SSMC の Administrator Console にログインします。
2. **アクション** > **アップグレード**をクリックします。
3. StoreServ 管理コンソールのアップグレードウィンドウが開き、**ファイルを選択**をクリックします。
4. アップグレード対象の SSMC パッケージ（`.star` ファイル）を選択します。

5. **アップロード**をクリックします。
6. **アップグレードします**をクリックします。

注記: 次のように移動して、HPE 3PAR StoreServ Management Console のバージョンを確認できます。

- **HPE 3PAR StoreServ Management Console** > **設定** > **アプリケーション**または
- バージョンは **HPE 3PAR StoreServ Management Console** の右下に表示されます。

SSMC でのプロキシ設定の構成

手順

1. SSMC Main Console にログインします。
2. **設定** > **アプリケーション**に移動します。
3. **アプリケーション**フィールドを編集します。
4. **プロキシアドレス**を入力します。この手順はオプションです。
5. **プロキシポート**を入力します。
6. **プロキシユーザー**と**プロキシパスワード**を入力します。これらの入力はオプションです。
7. **OK** をクリックします。

仮想アプライアンスとしての SSMC のデプロイ

SSMC 3.4 リリース以降、SSMC は仮想アプライアンスにのみ使用できます。

SSMC アプライアンスは、Debian オペレーティングシステムで実行する事前構成済み仮想マシンです。SSMC アプライアンスは、1 つの仮想アプライアンスに詳細分析やエラスティック検索などの複数の SSMC サービスをパッケージ化し、お客様のデプロイの複雑さを軽減します。SSMC デプロイアーキテクチャーでは、ハイパーバイザーで提供される高可用性機能を利用し、デプロイの複雑さを軽減します。

SSMC アプライアンスは、様々な環境をサポートすることを過度に重視していません。たとえば、Microsoft Windows、Linux、パッチ、ウィルス対策、堅牢化などです。

SSMC 仮想アプライアンスソフトウェアは、VMware vSphere Hypervisor 用の Open Virtual Format（OVF）形式、および Microsoft Hyper-V 用の自己解凍型仮想ハードディスク（VHD）形式で提供されます。SSMC アプライアンスは、Microsoft Hyper-V（Windows Server 2012 R2 または 2016）および VMware vSphere Hypervisor（VMware ESXi 6.0 または 6.5 または 6.7）でサポートされます。

SSMC のデプロイについては次の表を参照してください。

VMware vCenter または ESXi のバージョン	デプロイの経由
VMware vCenter Server 6.0 または VMware ESXi 6.0	VMware vSphere Client
VMware vCenter Server 6.5 または VMware ESXi 6.5	VMware vSphere Web Client
VMware vCenter Server 6.7 または VMware ESXi 6.7	VMware vSphere Web Client

SSMC をデプロイするための前提条件

前提条件

- ご使用のシステムが、SSMC をデプロイするための**システム要件**を満たしていることを確認します。
- すべての連携システムおよび移行ソースが、**SSMC の連携要件**を満たしていることを確認します。
- シックプロビジョニングディスクの場合、利用可能な空きスペースが 500GB あることを確認してください。

ISO イメージファイル

`HPESSMC-<build number>.iso` イメージをドライブにマウントします。ISO イメージの内容を以下に示します。

フォルダー名	サブフォルダー	サブフォルダー内のファイル	説明
HPE_SSMC_<build number>_HyperV_Image	HPESSMC-<build number>.HyperV_Appliance.zip	SsmcAppliance-<build number>-disk1.vhd.zip	
		SSMC-Hyper-V-Installer.ps1	Windows PowerShell スクリプト。
HPE_SSMC_<build number>_Migration_Tools	HPESSMC-<build number>.WinMigrationTool.exe		Windows 環境の移行ツール。
	HPESSMC-<build number>.RhelMigrationTool.zip		RHEL 環境の移行ツール。
HPE_SSMC_<build number>_VMware_Image	HPESSMC-<build number>.VMware_Appliance.zip	SsmcAppliance-disk1.vmdk	Virtual Machine Disk Format。
		SsmcAppliance-ESXi.ovf	VMware ESXi 用の Open Virtualization Format。
		SsmcAppliance-ESXi_ja.ovf	日本語 Open Virtualization Format。
		SsmcAppliance-ESXi_zh-CN.ovf	簡体字中国語 Open Virtualization Format。
		SsmcAppliance-VC.ovf	vCenter サーバー用の Open Virtualization Format。
		SsmcAppliance-VC_ja.ovf	日本語 vCenter サーバー用の Open Virtualization Format。
		SsmcAppliance-VC_zh-CN.ovf	簡体字中国語 vCenter サーバー用の Open Virtualization Format。

必ずすべてのファイルを同じフォルダーに抽出します。

SSMC でのアプライアンス証明書のダウンロード

手順

1. https://<appliance-ip>:8443 を開きます。
2. Internet Explorer を使用している場合は、**セキュリティレポート**をクリックします。Google Chrome を使用している場合は、**サイト情報の表示**をクリックします。
3. **詳細** > **ファイルにコピー**を選択します。

4. **証明書のエクスポートウィザード**で**次へ**をクリックします。
5. **Base-64 encoded X.509 (.CER)**を選択します。
6. エクスポートするファイルの名前を指定します。
7. **次へ**をクリックします。
8. **終了**をクリックします。

ヒント: ダウンロードした SSMC アプライアンス証明書を保存します。

SSMC アプライアンスのデプロイ手順

SSMC は、次の方法でデプロイできます。

- **VMware vCenter Server を通じた SSMC アプライアンスのデプロイ**
- **VMware ESXi を通じた SSMC アプライアンスのデプロイ**
- **Hyper-V を通じた SSMC アプライアンスのデプロイ**

VMware vCenter Server を通じた SSMC アプライアンス OVF テンプレートのデプロイ

前提条件

- OVF ファイルをインポートする前に、VMware vSphere Client 以降のバージョンがマシンにインストールされている必要があります。**ここをクリックして、VMware vSphere ソフトウェアをダウンロードします**。

  注記: 上記の Web リンク先は、HPE 以外の Web サイトです。これらのサイトの情報について、HPE は一切責任を負いかねますのでご了承ください。

  注記: OVF（Open Virtualization Format）は、仮想マシンまたはソフトウェアのパッケージ化と配布に関するオープン標準です。

- SSMC では、VMware vCenter バージョン 6.0、6.5、および 6.7 をサポートしています。VMware 環境の具体的なサポートについては、VMware 社の Web サイトの VMware 互換性マトリックスを参照してください。

手順

1. `HPESSMC-<build number>.iso` イメージを開きます。
2. ISO イメージから `HPESSMC-<build number>-VMware_Appliance.zip` をコピーします。
3. ローカルフォルダーにファイルを解凍します。
4. `HPE_SSMC_Appliance-<build number>-VC.ovf` を展開します。VMware vSphere Client または Web Client を開き、VMware vCenter Server に接続します。以下の手順に従って、OVF テンプレートをデプロイします。

a. VMware vSphere Client の場合、**ファイル** > **OVF テンプレートのデプロイ**に移動します。**OVF テンプレートのデプロイ**ウィザードが表示されます。

b. Web クライアントの左のナビゲーターパネルの下で**ホストおよびクラスタ** > **アクション** > **OVF テンプレートのデプロイ**をクリックします。

5. ソースページで、**参照**をクリックして OVF のインポート元を指定し、**次へ**をクリックします。
6. OVF テンプレートの詳細ページで、OVF テンプレートを確認し、**次へ**をクリックします。

注記: vSphere Web Client からのデプロイ中に `.ovf` と `.vmdk` の両方のファイルを選択します。

7. 使用許諾契約ページで、**承諾** > **次へ**をクリックします。
8. 名前と場所ページで、SSMC アプライアンスの名前を入力して、**次へ**をクリックします。
9. デプロイの構成ページで、サポートされるデプロイ構成のいずれかを選択し、**次へ**をクリックします。

注記:

小規模、中規模、または大規模として構成を選択した場合、デプロイの構成ページに表示される構成の詳細を確認します。

デプロイオプション	構成の詳細
小規模	小規模デプロイでは、最大 8 つのアレイと 128,000 のオブジェクトを管理します。このデプロイには、4 つの vCPU と 16GB のメモリが必要です。
中規模	中規模デプロイでは、最大 16 のアレイと 256,000 のオブジェクトを管理します。このデプロイには、8 つの vCPU と 32GB のメモリが必要です。
大規模	大規模デプロイでは、最大 32 のアレイと 500,000 のオブジェクトを管理します。このデプロイには、16 の vCPU と 48GB のメモリが必要です。

10. 特定のホストの指定ページで、特定のホストを選択し、**次へ**をクリックします。
11. ストレージページで、デプロイするストレージを選択し、**次へ**をクリックします。
12. ディスクのフォーマットページで、**シンプロビジョニング**を選択し、**次へ**をクリックします。

注記: シックプロビジョニングディスクの場合、利用可能な空きスペースが 500GB あることを確認してください。

13. ネットワークのマッピングページで、アプライアンスをインベントリ内のネットワークにマッピングし、**次へ**をクリックします。
14. プロパティページで、システム全体の構成と IP 設定の詳細を入力します。

a. ホスト名を入力します。

b. ssmcadmin ユーザーのパスワードを入力します。

注記: アプライアンスの SSMC ログイン認証情報と SSMC コンソールの SSMC ログイン認証情報は異なります。

c. パスワードの確認を入力します。

d. タイムゾーンを入力します。

e. IP バージョンを入力します。

f. IP タイプを入力します。

注記: 2 つのオプションを使用できます。

- **Static**：選択した場合、IP アドレスを指定します。
- **DHCP**：選択した場合、IP アドレスは自動的に提供されます。

g. IP アドレス（静的な設定にのみ適用可能）を入力します。

h. サブネットマスク（静的な設定にのみ適用可能）を入力します。

i. デフォルトゲートウェイを入力します。

注記: VMware vCenter Server では、プロパティページで作成したエントリーを検証できません。

15. 終了準備の完了ページで、デプロイの設定を確認し、**デプロイ後にパワーオン**チェックボックスをオンにして、**終了**をクリックします。

16. 数分後にデプロイが正常に完了しましたというメッセージが表示されます。**OK** をクリックします。

注記: 追加の設定を行い、SSMC アプライアンスを再構成するには、**テキストベースのユーザーインターフェイス（TUI）**を使用します。

VMware ESXi を通じた SSMC アプライアンスのデプロイ

前提条件

- OVF ファイルをインポートする前に、VMware vSphere 5.0 Client 以降のバージョンがマシンにインストールされている必要があります。

  ここをクリックして、VMware vSphere ソフトウェアをダウンロードします。

  注記: 上記の Web リンク先は、HPE 以外の Web サイトです。これらのサイトの情報について、HPE は一切責任を負いかねますのでご了承ください。

  注記: OVF（Open Virtualization Format）は、仮想マシンまたはソフトウェアのパッケージ化と配布に関するオープン標準です。

- SSMC では、VMware ESXi バージョン 6.0、6.5、および 6.7 をサポートしています。VMware 環境の具体的なサポートについては、VMware 社の Web サイトの VMware 互換性マトリックスを参照してください。

手順

1. ISO イメージから `HPESSMC-<build number>.iso` イメージを開きます。
2. ISO イメージから `HPESSMC-<build number>-VMware_Appliance.zip` ファイルをコピーします。
3. ローカルフォルダーにファイルを解凍します。
4. `HPE_SSMC_Appliance-<build number>-ESXi.ovf` を展開します。VMware vSphere Client または Web Client を開き、VMware vCenter Server に接続します。以下の手順に従って、OVF テンプレートをデプロイします。

   a. VMware vSphere Client の場合、**ファイル** > **OVF テンプレートのデプロイ**に移動します。**OVF テンプレートのデプロイ**ウィザードが表示されます。

   b. Web クライアントの左のナビゲーターパネルの下で**ホスト** > **仮想マシン** > **VM の作成/登録** > **OVF ファイルまたは OVA ファイルから仮想マシンをデプロイ**をクリックします。

5. ソースページで、**参照**をクリックして OVF のインポート元を指定し、**次へ**をクリックします。
6. OVF テンプレートの詳細ページで、OVF テンプレートを確認し、**次へ**をクリックします。

   注記: vSphere Web Client からのデプロイ中に `.ovf` と `.vmdk` の両方のファイルを選択します。

7. 使用許諾契約ページで、**承諾** > **次へ**をクリックします。
8. 名前と場所ページで、SSMC アプライアンスの名前を入力して、**次へ**をクリックします。
9. デプロイの構成ページで、サポートされるデプロイ構成のいずれかを選択し、**次へ**をクリックします。

   注記:

   - 選択した VMware ESXi が選択した構成をサポートしていることを確認します。サポートしていない場合、デプロイ後、SSMC アプライアンスは起動しません。
   - 小規模、中規模、または大規模として構成を選択した場合、デプロイの構成ページに表示される構成の詳細を確認します。

デプロイオプション	構成の詳細
小規模	小規模デプロイでは、最大 8 つのアレイと 128,000 のオブジェクトを管理します。このデプロイには、4 つの vCPU と 16GB のメモリが必要です。
中規模	中規模デプロイでは、最大 16 のアレイと 256,000 のオブジェクトを管理します。このデプロイには、8 つの vCPU と 32GB のメモリが必要です。
大規模	大規模デプロイでは、最大 32 のアレイと 500,000 のオブジェクトを管理します。このデプロイには、16 の vCPU と 48GB のメモリが必要です。

10. ストレージページで、デプロイするストレージを選択し、**次へ**をクリックします。
11. ディスクのフォーマットページで、**シンプロビジョニング**を選択し、**次へ**をクリックします。

    注記: シックプロビジョニングディスクの場合、利用可能な空きスペースが 500GB あることを確認してください。

12. ネットワークのマッピングページで、仮想マシンをインベントリ内のネットワークにマッピングし、**次へ**をクリックします。
13. 終了準備の完了ページで、デプロイの設定を確認し、**デプロイ後にパワーオン**チェックボックスをオンにして、**終了**をクリックします。
14. 数分後にデプロイが正常に完了しましたというメッセージが表示されます。**OK** をクリックします。
15. VM コンソールを使用して SSMC アプライアンスにログインします。
16. SSMC ログイン下で `ssmcadmin` を入力します。
17. パスワードを入力します。

    注記:

    - ESXi サーバーでのデプロイ後に、必ずデフォルトのパスワードを変更してください。
    - パスワードの入力には、米国英語キーボードレイアウトだけを使用してください。
    - アプライアンスの SSMC ログイン認証情報と SSMC コンソールの SSMC ログイン認証情報は異なります。

18. 新しいパスワードを再入力します。
19. **テキストベースのユーザーインターフェイス（TUI）**を使用して、SSMC アプライアンスを構成します。

PowerShell インストーラースクリプトを使用した Microsoft Hyper-V からの SSMC アプライアンスのデプロイ

前提条件

- Hyper-V サーバーに SSMC アプライアンスをインストールするには、管理者特権があることを確認します。
- Hyper-V サーバー上で、ネットワークスイッチと適切なアダプターが構成されていることを確認します。
- Hyper-V ホストに、以下の 2017 年 4 月の Microsoft ホットフィックスまたはその他の最新のロールアップをインストールします。
  - Windows Server 2016 - KB4015217
  - Windows Server 2012 R2 - KB4015550
- HPE では、Windows システムを使用する前に、Windows の最新の必須および重要パッチをインストールすることをお勧めします。Windows Update について詳しくは、**Microsoft サポート**を参照してください。インストールを進める前に、必ずパッチのリビジョンを確認してください。

手順

1. ISO イメージから `HPE_SSMC_<build number>_HyperV_Image` フォルダーを開きます。
2. Hyper-V サーバーに `HPESSMC-<build number>-HyperV_Appliance.zip` ファイルの内容を抽出します。
   次のファイルが `HPESSMC-<build number>-HyperV_Appliance.zip` に用意されていることを確認します。
   - `SSMCAppliance-<build number>-disk1.vhd.zip`
   - `SSMC-Hyper-V-Installer.ps1`
3. SSMC VHD ZIP ファイルがある場所へのディレクトリパスを指定します。
4. 指定のディレクトリから `.\SSMC-Hyper-V Installer.ps1` コマンドを使用して、PowerShell スクリプトを実行します。

   重要: 「信頼された発行者」に関連したエラーメッセージが表示されたら、`Always run` を選択します。`Always run` オプションによって HPE が信頼された発行者として追加され、中断せずに実行が続行します。
5. ライセンス契約に同意するには、`a` と入力します。
6. SSMC アプライアンスを作成するディレクトリのパスを指定します。

   注記: サーバー上に指定したディレクトリがないことを確認します。デプロイスクリプトは、指定した名前のディレクトリを作成し、SSMC システムディスクの VHD ファイルをコピーして、SSMC アプライアンスを作成します。
7. SSMC アプライアンスの名前を指定します。
8. 使用できる構成から SSMC の仮想ハードウェア構成テンプレートを選択します。

   注記:

   小規模、中規模、または大規模として構成を選択した場合、デプロイの構成ページに表示される構成の詳細を確認します。

デプロイオプション	構成の詳細
小規模	小規模デプロイでは、最大 8 つのアレイと 128,000 のオブジェクトを管理します。このデプロイには、4 つの vCPU と 16GB のメモリが必要です。
中規模	中規模デプロイでは、最大 16 のアレイと 256,000 のオブジェクトを管理します。このデプロイには、8 つの vCPU と 32GB のメモリが必要です。
大規模	大規模デプロイでは、最大 32 のアレイと 500,000 のオブジェクトを管理します。このデプロイには、16 の vCPU と 48GB のメモリが必要です。

9. ネットワークインターフェイスを構成する VM スイッチを選択します。

   注記: 構成されている VM スイッチが 1 つだけ存在する場合は、このスイッチがデフォルトで選択されます。

   - 構成の概要が表示されます。
   - 新しい SSMC アプライアンスが Hyper-V マネージャー上に作成されます。

10. `Y` と入力して、SSMC アプライアンスの電源をオンにします。
11. Hyper-V マネージャー上の SSMC アプライアンスを右クリックして、**接続**を選択します。
12. SSMC アプライアンスコンソールにログインし、ユーザー名を `ssmcadmin` に、パスワードを `ssmcadmin` に設定します。

    注記: Hyper-V サーバーでの SSMC のデプロイ後に、必ずデフォルトのパスワードを変更してください。

    アプライアンスの SSMC ログイン認証情報と SSMC コンソールの SSMC ログイン認証情報は異なります。

13. **テキストベースのユーザーインターフェイス（TUI）**を使用して、SSMC アプライアンスを構成します。

Microsoft クラスターを使用した SSMC アプライアンスの高可用性（HA）

Hyper-V 用の SSMC アプライアンスは、顧客のユースケースに応じて以下の方法でデプロイできます。ユーザーは、アプライアンスのデプロイ前に以下のオプションを比較検討できます。ユースケースは、クラスター統合環境と非クラスター化環境に大きく分類されます。

Microsoft フェイルオーバークラスターを使用した SSMC アプライアンスの高可用性（HA）

このシナリオでは、SSMC アプライアンスは共有ストレージ（3PAR）上に作成されます。アプライアンスの高可用性は、Microsoft フェイルオーバークラスターで提供されます。ここでは、アプライアンスをホストしているノードが停止した場合に、フェイルオーバークラスターが別の使用可能なノードへのアプライアンスの移動を処理して、アプライアンスはオンラインに戻りユーザーにサービスを提供します。

アプライアンスは、シングルサイトクラスターかマルチサイトクラスターのどちらかで、フェイルオーバークラスター内の VM としてデプロイできます。要件に応じて CSV ディスクか CSV 以外のディスクのいずれかにアプライアンスをデプロイできます。

シングルクラスターサイト：

- すべてのフェイルオーバークラスターノードが 1 つのサイトにあり、すべてのクラスターノードが共有ストレージ用の 1 つの 3PAR アレイに接続しています。
- CSV ボリュームと CSV 以外のボリュームのどちらでも、アプライアンス VM を配置できます。アプライアンスのデプロイを開始する前に、CSV ボリュームと CSV 以外のボリュームを構成します。
- すべてのファイルオーバークラスターノードの仮想スイッチ名（Hyper-V マネージャーの GUI から構成できます）が同じであることを確認します。同じでない場合、別のノードへのアプライアンスのフェイルオーバーが失敗します。
- アプライアンスのデプロイを開始します。VM のデプロイ中、アプライアンスを置く CSV ディスク上の場所または CSV 以外のディスク上の場所を選択します。
- アプライアンスウィザードの手順に従ってください。

- アプライアンスはローカルノード上に作成されますが、HA VM としてではありません。HA として VM を作成するには、以下の手順に従います。
  - 実行している場合は、VM を停止します。
  - 次の PowerShell コマンドを実行します。`Add-ClusterVirtualMachineRole--VirtualMachine <VM name> -Name <VM name>`.
  - アプライアンスのクラスター化された VM（HA VM）が作成され、これにより VM はノードの障害でも利用できるようになります。
- 欠点：このタイプの構成では、ノードの障害に HA をもたらしますが、3PAR に災害が発生した場合は、HA を実現できません。この問題を解決するには、マルチサイトクラスターを検討してください。

マルチサイトクラスター：代表的なマルチサイトクラスターは、2 つのサイトにまたがり、サイト全体の災害時に HA をもたらします。すべてのフェイルオーバークラスターノードは、3PAR アレイベースのレプリケーションを使用して 2 つのサイトに分散されます。複数のサイトを持つことで、真のディザスタリカバリソリューションをユーザーの業務アプリケーションにもたらします。

データは、アレイベースのレプリケーションを使用して別のサイトアレイにレプリケートされます。通常、マルチサイトアレイでは、一方の側にボリュームへの読み取り/書き込みアクセスが行われ、もう一方の側には読み取りアクセスだけが行われます。したがって、災害時には、アプライアンスは他方のサイトに移動します。「**Cluster Extension for Windows**」などの製品は、災害中にシームレスにストレージフェイルオーバーを実行し、HA ソリューションを実現します。

この構成では、サイト全体のシャットダウンというシナリオ中でも、ユーザーがアプライアンスを使用できます。

フェイルオーバークラスターを使用しない SSMC アプライアンスの高可用性

Hyper-V レプリカの使用：Hyper-V は、ユーザーがある Hyper-V ホストから別の Hyper-V ホストへの VM（アプライアンス）のライブ移行を実行できるメカニズムを提供します。Hyper-V レプリカ機能を構成します。詳しくは、**https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/set-up-hyper-v-replica** を参照してください。

この構成を完了したら、SSMC アプライアンスをデプロイします。ある Hyper-V ホストから別の Hyper-V ホストにアプライアンスを移動するには、**移動 > 仮想マシンを移動する**を選択します。

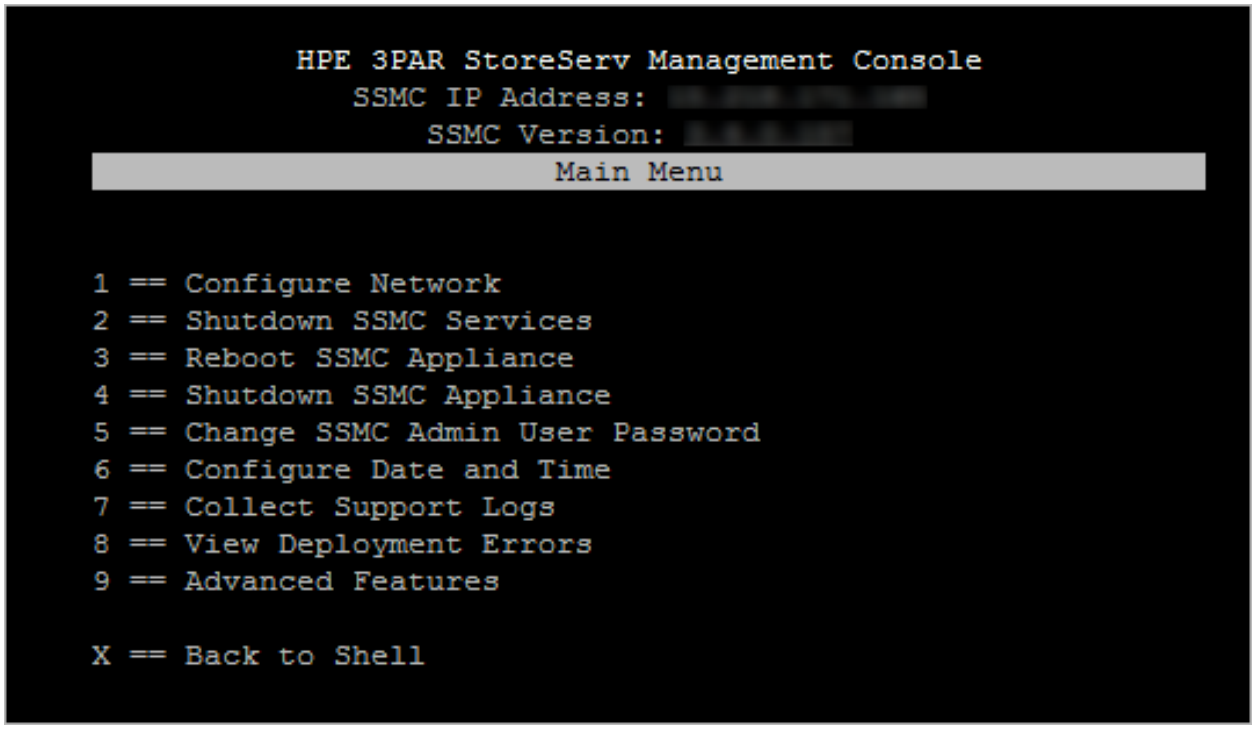
テキストベースのユーザーインターフェイス（TUI）

テキストベースのユーザーインターフェイス（TUI）は、SSMC アプライアンスの構成と管理を可能にする SSMC アプライアンスのユーティリティです。

`ssmcadmin` として SSMC アプライアンスにログインすると、自動的に TUI が起動します。

上/下矢印キーを使用して項目を選択します。現在選択されているオプションが強調表示されます。**Enter** キーを押すと、強調表示されているオプションが実行されます。

Linux bash シェルにエスケープするには、メインメニューで **X** キーを押します。シェルから TUI に戻るには、コマンド `config_appliance` を入力します。



テキストベースのユーザーインターフェイス（TUI）のタスク

TUI には、メインメニューに以下のオプションがあります。

1. ネットワークの構成
2. SSMC サービスのシャットダウン/開始
3. SSMC アプライアンスの再起動
4. SSMC アプライアンスのシャットダウン
5. SSMC 管理者ユーザーのパスワードの変更
6. 日付と時刻の構成
7. サポートログの収集

8. デプロイエラーの表示
9. 拡張機能

ネットワークの構成

手順

1. メインメニューから、**Configure Network** を選択します。
2. **Configure Network** 画面が表示されたら、ネットワーク設定が構成されていない SSMC に対して **Enter** キーを押します。
3. ネットワークの設定がすでに構成されている場合、設定を変更できることを示すメッセージが表示されます。（必要である場合を除き、推奨できません）。設定を変更する場合は、**Enter** キーを押します。変更しない場合は、**X** キーを押してメインメニューに戻ります。
4. SSMC アプライアンスのホスト名とキー入力して、**Enter** キーを押します。
5. ネットワークデバイスを選択して、**Enter** キーを押します。
6. インターネットプロトコルバージョンを選択します。

注記: 以下のインターネットプロトコル構成が SSMC アプライアンスでサポートされています。

構成	接続
単一の仮想ネットワークインターフェイスカード（NIC）	IPv4 アドレスか、IPv6 アドレス（混在モード）のいずれかを構成します。ただし、IPv4 アドレスと IPv6 アドレスは両方一緒にはサポートされません。
2 つの仮想ネットワークインターフェイスカード（NIC）	以下の構成がサポートされます。 ・ IPv4、IPv6 ・ IPv4、IPv4 ・ IPv6、IPv6

注記: マルチホーミング要件のため、SSMC アプライアンスに 2 つのネットワークインターフェイスを構成してください。

7. インターネットプロトコルタイプを選択します。

   Static：選択した場合、IP アドレスを指定します。

   DHCP：選択した場合、IP アドレスは自動的に提供されます。
8. **Y** または **N** を入力して設定を確認します。
9. **Network configuration successful** というメッセージが表示されたら、**X** を入力してメインメニューに戻ります。

SSMC サービスのシャットダウン/開始

TUI のメインメニューから、**Shutdown SSMC Services** または **Start SSMC Services** を選択します。

SSMC サービスのシャットダウンを選択すると、ご使用の Web ブラウザーから SSMC の GUI にアクセスできなくなります。SSMC サービスを開始すると、ご使用の Web ブラウザーから SSMC の GUI にアクセスできます。

SSMC アプライアンスの再起動

TUI メインメニューから、**Reboot SSMC Appliance** を選択します。

このオプションは、SSMC アプライアンスを再起動します。TUI にアクセスするには、コンソールに `ssmcadmin` として再度ログインする必要があります。

注記: 再起動すると、SSMC サーバーおよび SSMC アプライアンスへの接続が一時的に失われます。

SSMC アプライアンスのシャットダウン

TUI メインメニューから、**Shutdown SSMC Appliance** を選択します。

このオプションを選択して、SSMC アプライアンス VM をシャットダウンできます。

SSMC 管理者のユーザーパスワードの変更

TUI メインメニューから、**Change SSMC Admin User Password** を選択します。

これは、SSMC 管理者のユーザーパスワードの変更に役立ちます（`ssmcadmin`）。

日付と時刻の構成

手順

1. TUI メインメニューから、**Configure Date and Time** を選択します。
2. タイムゾーンを変更するには、**Change Time Zone** を選択します。
   a. お住まいの地域を入力して、**Enter** キーを押します。
   b. タイムゾーンに対応する都市または地域を入力して、**Enter** キーを押します。

   入力したデータに応じてタイムゾーンが設定されます。
3. **Configure Date and Time** を選択して、**Enter** キーを押します。
   a. コンソールで指定された形式で日付を入力します。
   b. コンソールで指定された形式で時刻を入力します。
   c. **Y** キーを押して、日付と時刻の変更を確認します。
4. **Date and Time configuration successful** というメッセージが表示されたら、**X** を入力してメインメニューに戻ります。

サポートログの収集

手順

1. TUI メインメニューから、**Collect Support Logs** を選択します。
2. サポートログを収集する場合は、**Y** と入力します。
3. サポートログの名前と位置がコンソールに表示されます。ログへのアクセスを確認します。メインメニューに戻るには、**X** を押します。

デプロイエラーの表示

手順

1. TUI メインメニューから、**View Deployment Errors** を選択します。
2. デプロイエラーが存在する場合は、コンソールに表示されます。
3. メインメニューに戻るには、**X** を押します。

拡張機能

手順

1. TUI メインメニューから、**Advanced Features** を選択します。
2. 次のいずれかのオプションを選択します。
   a. **Disable Administrator Console Login**
   b. **Clear Administrator Credential**
3. 画面に表示される指示に従います。

管理者コンソールログインの無効化

手順

1. TUI メインメニューから、**Advanced Features** を選択します。
2. **Disable Administrator Console Login** を選択します。
3. 管理者ログインを無効にするには、**Y** を選択するか、**N** を選択してキャンセルします。Disable Administrator Console Login アクションにより SSMC サービスが再起動します。

注記: このオプションは、CAC または Two-Factor 認証が有効でアクティブであるときに、ネットワークから管理者コンソールアクセス（ログインに管理者認証情報が必要）をロックする場合に役立ちます。

管理者認証情報のクリア

手順

1. TUI メインメニューから、**Advanced Features** を選択します。
2. **Clear Administrator Credential** を選択します。
3. 管理者認証情報をクリアするには、**Y** を選択するか、**N** を選択してキャンセルします。管理者認証情報のクリア操作は SSMC サービスを再起動します。

注記: このオプションは、管理コンソールユーザーのパスワードのクリアに役立ちます。

DNS サーバーと NTP サーバーの構成

DNS サーバーの構成

DNS サーバーを構成するには、コマンド `sudo/ssmc/sbin/ConfigDNS.py-d domainserver.com-s < DNS IP >`を使用します。

NTP サーバーの構成

NTP サーバーを初めて構成するには、以下の手順を実行します。

1. NTP サーバーを構成するには、`sudo /usr/sbin/ntpdate <ntp server>`コマンドを実行します。
2. NTP サービスを起動するには、`sudo systemctl start ntp` コマンドを使用します。

NTP サーバーを変更するには、次の手順に従います。

1. 現在の NTP サービスを停止するには、コマンド `sudo systemctl stop ntp` を使用します。
2. NTP を更新するには、`sudo /usr/sbin/ntpdate <ntp server>`を実行します。
3. NTP サービスを起動するには、`sudo systemctl start ntp` コマンドを使用します。

デフォルトで、アプライアンス上の NTP サービスは、再起動のたびに停止します。再起動するたびに NTP を構成し起動するには、`sudo systemctl enable ntp` コマンドを使用します。

インストーラーベースの SSMC デプロイから SSMC アプライアンスへの移行

SSMC 3.4 リリース以降、SSMC は仮想アプライアンスにのみ使用できます。以前の SSMC デプロイから移行する予定の場合は（SSMC 3.2 から 3.3.1）、HPE 3PAR SSMC 移行ツールを使用します。

HPE 3PAR SSMC 移行ツールは、Windows および Linux 環境で使用できる個別のインストーラーです。以前の SSMC インスタンスをホストしているマシンまたは VM から移行ツールをインストールして実行します。

ブラウザーからのインバウンド通信を許可するために、SSMC はインバウンドポート 8443（デフォルト）を使用します。

注意:

- 移行前に SSMC アプライアンスで管理者認証情報などの認証情報を一切設定しないでください。管理者の認証情報を設定した場合、移行は失敗します。移行サービスは常に、SSMC で認証情報または設定を確認します。構成が事前に存在する場合は、移行が失敗します。移行エラーステータスは、ユーザーに通知されます。
- 移行ツールから求められたら、SSMC アプライアンスのデプロイ中に ssmcadmin ユーザーに提供したものと同じパスワードを使用します。
- カスタムパスに保存されている SR レポートは、ディレクトリ`/var/opt/hpe/ssmc/data/persist/scheduledreports/users/`に格納されます。
- すでに定義されている管理者認証情報をクリアした場合、およびもう一度移行を実行する場合は、アプライアンスでの設定が変更されます。

次の表は、HPE 3PAR SSMC 移行ツールを使用して移行されるコンポーネントと移行されないコンポーネントを示しています。

移行されるコンポーネント	移行されないコンポーネント
SSMC の管理者認証情報	ログ
SSMC 構成済みアレイとその認証情報	SSMC ポートの構成（アプライアンスで常に 8443）
SR レポート	SR レポートカスタムパス
HPE 3PAR RMC 構成	
CA 署名済み証明書	
FIPS モードの構成	

警告: 移行の結果、ターゲットアプライアンスで構成されている CA 署名済み証明書が置き換わることがあります。アプライアンスでの CA 証明書の構成は、移行後のみに行うことをお勧めします。移行前にアプライアンスの CA 署名済み証明書を構成する場合は、もう一度 CA 証明書を構成する必要が生じることがあります。

SSMC の CA 署名済み証明書を構成するには、**SSMC 用の CA 署名付き証明書の管理**を参照してください。

HPE 3PAR SSMC 移行は、2 段階のプロセスです。最初の手順では、SSMC 構成が移行され、ターゲットアプライアンスは、以前に生成された SR レポートを表示する機能を除き使用可能です。2 番目の手順では、ユーザーは SR レポートを移行するように求められます。ユーザーが SR 移行を選択すると、SR レポート移行が開始されます。

注記: レポートの累積サイズに応じて、SR レポート移行には時間がかかる場合があります。ネットワークの中断や再起動のためにこの移行が失敗した場合は、移行ツールを再実行してください。SR レポート移行は、障害のために移行されなかったレポートに対して再開します。

FIPS モードが有効な SSMC 3.3 または 3.3.1 を移行する場合、移行中に移行ツールからアプライアンス証明書の入力が求められます。

HPE 3PAR SSMC 移行ツールは、Windows 環境と Linux 環境で使用でき、移行のための個別の手順が含まれます。

- **新しい SSMC アプライアンスへの Windows ベース SSMC デプロイの移行**
- **新しい SSMC アプライアンスへの RHEL ベース SSMC デプロイの移行**

前提条件

- 管理者または root ユーザーのみが移行を開始できます。
- アプライアンスがソース SSMC マシンから到達可能であることを確認します。
- SSMC 3.2 および 3.3 から SSMC 3.4 への移行だけが許可されます。SSMC 3.2 以前のバージョンからの移行は実行できません。SSMC が必要な最低限のバージョンでない場合は、移行前に SSMC をアップグレードする必要があります。
- SSMC アプライアンスに移行する前に、ssmcadmin ユーザー認証情報が設定されていることを確認します。

新しい SSMC アプライアンスへの Windows ベース SSMC デプロイの移行

次の Windows オペレーティングシステムが SSMC アプライアンスでサポートされています。

- Microsoft Windows Server 2016 Datacenter オペレーティングシステム
- Microsoft Windows Server 2012 R2 Datacenter オペレーティングシステム
- Microsoft Windows Server 2008 R2 Enterprise オペレーティングシステム
- Microsoft Windows 10 オペレーティングシステム
- Microsoft Windows 7 オペレーティングシステム
- Microsoft Windows Server 2012 Standard
- Hyper-V 2012 コア

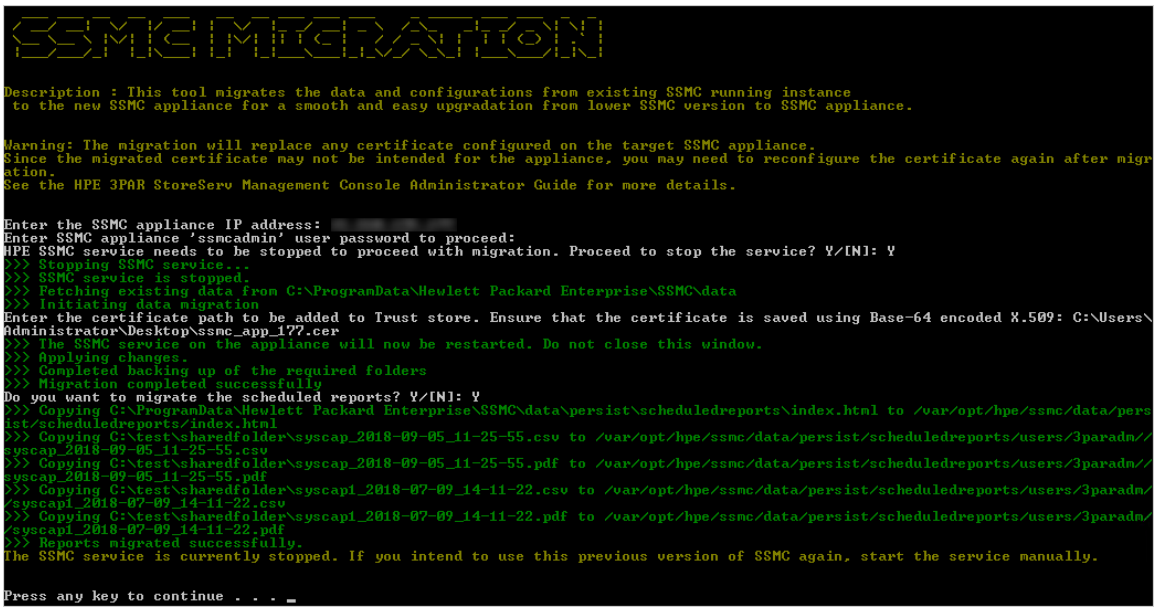
重要: Windows Server 2016 Datacenter オペレーティングシステムを使用している場合は、HPE では、**Windows SmartScreen 設定**をオフにすることをお勧めします。`.exe` SSMC 移行ファイルを実行する場合は、必ず **Windows SmartScreen 設定**を無効にしてください。

HPE 3PAR SSMC 移行ツールは.exe ファイルとして Windows で使用できます。このファイルは、**SSMC ISO image** > **HPE_SSMC_<build number>_Migration_Tools** で入手できます。

手順

1. **HPESSMC-<build number>.WinMigrationTool.exe** ファイルを開きます。
2. HPE 3PAR SSMC 移行ツール - InstallShield ウィザードで**次へ**をクリックします。
3. ライセンス契約を受け入れた後、**次へ**をクリックします。
4. **インストール**をクリックします。

   `HPE 3PAR SSMC migration tool.bat` ショートカットファイルがデスクトップ上に作成されます。
5. `.bat` ファイルを起動します。



6. SSMC 移行ツールで、以下の詳細を指定します。

入力名	説明
Enter SSMC appliance IP address.	構成の移行先の SSMC アプライアンスの IP アドレス。
Enter SSMC appliance '`ssmcadmin`' user password to proceed.	初めてアプライアンスをデプロイしたときに作成された `ssmcadmin` ユーザーのパスワード。
HPE SSMC service needs to be stopped to proceed with migration. Proceed to stop the service? Y/[N]	アプライアンスの移行を進めるため、ソース SSMC 上で SSMC サービスを停止することを確認します。このオプションは、SSMC サービスが実行されている場合にのみ表示されます。
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509.	FIPS モードがソース上で有効になっている場合に、移行に必要になる SSMC アプライアンス証明書を入力します。

表は続く

入力名	説明
Do you want to migrate the scheduled reports? Y/[N].	スケジュールされたレポートを移行することを確認します。
Do you want to download the SSMC appliance logs, that can be shared with HPE support? Y/[N].	何らかの理由で移行が失敗した場合、エラーログをダウンロードすることを確認します。

新しい SSMC アプライアンスへの RHEL ベース SSMC デプロイの移行

HPE 3PAR SSMC 移行ツールは.zip ファイルとして Linux で使用できます。このファイルは、**SSMC ISO image** > **HPESSMC-<build number>.RhelMigrationTool.zip** で入手できます。

手順

1. **HPESSMC-<build number>.RhelMigrationTool.zip** フォルダーを解凍します。コマンドラインインターフェイス（CLI）を使用している場合は、コマンド `unzip <file_name>`を使用して移行フォルダーを解凍します。

   注記: 以下のファイルが **HPESSMC-<build number>.RhelMigrationTool.zip** フォルダーで使用できることを確認します。

   - `DataMigrationTool_lib`
   - `DataMigrationTool.jar`
   - `ssmc_migration_tool.sh`
   - `log4j2.properties`

2. `chmod +x` コマンドを `ssmc_migration_tool.sh` で実行します。
3. コマンド`./ssmc_migration_tool.sh` を使用して実行を開始します。

```
[root@HPERMCF487D16F55 test]# ./ssmc_migration_tool.sh
 ___ ___ __  __  ___   __  __ ___ ___ ___ ___ _____ ___ ___  _  _
/ __/ __|  \/  |/ __| |  \/  |_ _/ __| _ \  /_\_   _|_ _/ _ \| \| |
\__ \__ \ |\/| | (__  | |\/| || | (_ |   / / _ \| |  | | (_) | .` |
|___/___/_|  |_|\___| |_|  |_|___\___|_|_\/_/ \_\_| |___\___/|_|\_|


Description : This tool migrates the data and configurations from existing SSMC running instance
 to the new SSMC appliance for a smooth and easy upgradation from lower SSMC version to SSMC appliance.


Warning: The migration will replace any certificate configured on the target SSMC appliance.
Since the migrated certificate may not be intended for the appliance, you may need to reconfigure the certificate again after migration.
See the HPE 3PAR StoreServ Management Console Administrator Guide for more details.


Enter the SSMC appliance IP address:
Enter SSMC appliance 'ssmcadmin' user password to proceed:
HPE SSMC service needs to be stopped to proceed with migration. Proceed to stop the service? Y/[N]: Y
>>> Fetching existing data from /var/opt/hpe/ssmc/data
>>> Initiating data migration
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509: /home/ssmc_app_177.cer
>>> The SSMC service on the appliance will now be restarted. Do not close this window.
>>> Applying changes.
>>> Completed backing up of the required folders
>>> Migration completed successfully
Do you want to migrate the scheduled reports? Y/[N]: Y
>>> Copying /var/opt/hpe/ssmc/data/persist/scheduledreports/index.html to /var/opt/hpe/ssmc/data/persist/scheduledreports/index.html
>>> Reports migrated successfully.
The SSMC service is currently stopped. If you intend to use this previous version of SSMC again, start the service manually.
```

4. SSMC 移行ツールで、以下の詳細を指定します。

入力名	説明
Enter SSMC appliance IP address.	構成の移行先の SSMC アプライアンスの IP アドレス。
Enter SSMC appliance '`ssmcadmin`' user password to proceed.	初めてアプライアンスをデプロイしたときに作成された `ssmcadmin` ユーザーのパスワード。
HPE SSMC service needs to be stopped to proceed with migration. Proceed to stop the service? Y/[N].	アプライアンスの移行を進めるため、ソース SSMC 上で SSMC サービスを停止することを確認します。このオプションは、SSMC サービスが実行されている場合にのみ表示されます。
Enter the certificate path to be added to Trust store. Ensure that the certificate is saved using Base-64 encoded X.509.	FIPS モードがソース上で有効になっている場合に、移行に必要になる SSMC アプライアンス証明書を入力します。
Do you want to migrate the scheduled reports? Y/[N].	スケジュールされたレポートを移行することを確認します。
Do you want to download the SSMC appliance logs, that can be shared with HPE support? Y/[N].	何らかの理由で移行が失敗した場合、エラーログをダウンロードすることを確認します。

移行後の注意事項

ソース SSMC に CA 証明書が構成されている場合があり、移行によりこの証明書はアプライアンスに転送されます。CA 証明書はソース SSMC の FQDN とともに埋め込まれているため、望ましい構成にならないことがあります。この状況を修正するため、次のオプションのいずれかを検討してください。

- CA 証明書で参照される情報に基づいて、ソース SSMC FQDN またはソース SSMC IP、あるいはその両方を新しいアプライアンスに割り当てます。
- 正しい FQDN（または IP）で新しいアプライアンス IP またはホストの新しい証明書を生成します。新しいアプライアンスでこの新しい CA 証明書を構成します。

SSMC の構成

重要: このセクションは、SSMC の新規セットアップに適用されます。すでに既存の SSMC デプロイがあり、新しくデプロイする SSMC アプライアンスに設定または構成をコピーする場合は、**新しい SSMC アプライアンスへの移行**を参照してください。

プロセスの概要：

1. **SSMC へのアクセス**
2. **SSMC 管理者認証情報の設定**
3. **SSMC へのストレージシステムの追加**
4. **Administrator Console からの SSMC 管理対象システムへの接続**

詳しくは

SSMC の証明書(33 ページ)

SSMC へのアクセス

リモートシステムから SSMC にアクセスするには、次の方法を使用します。

リモートシステムから SSMC にアクセスするには、サポートされているブラウザーを開き、次の URL を入力します。

```
https://<server name or IP>:<port_number>
```

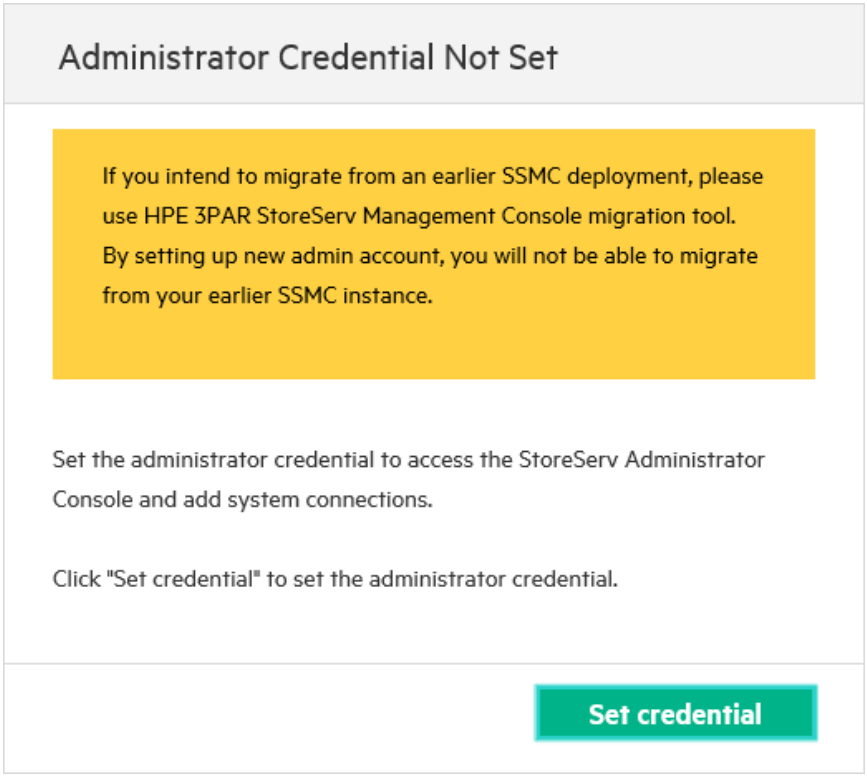
ヒント: Web サイトのセキュリティ証明書の問題を示すメッセージがブラウザーに表示された場合でも、その Web サイトを安全に続行できます。この Windows メッセージを削除するには、**SSMC の CA 証明書**を参照してください。

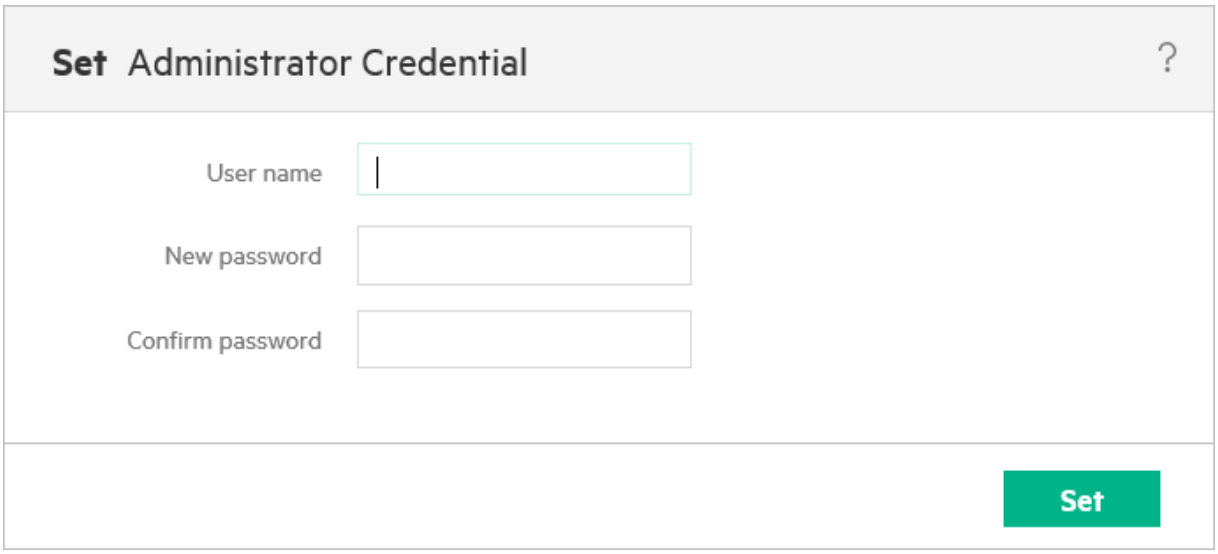
SSMC 管理者認証情報の設定

インストール後に初めて SSMC を開くときは、システムが SSMC の管理者アカウントのユーザー名およびパスワードを設定するよう要求します。このアカウントは、SSMC の Administrator Console だけをアクセスできます。

手順

1. 新しくインストールされた SSMC にアクセスします（**SSMC へのアクセス**を参照してください）。
2. システムプロンプトで、**認証情報を設定**をクリックします。



3. 管理者認証情報の設定ダイアログで、管理者アカウントのユーザー名を入力します。ユーザー名は、スペースを含まない 2 文字以上の文字列である必要があります。UTF-8 を含み、いかなる文字も使用できます。
4. 

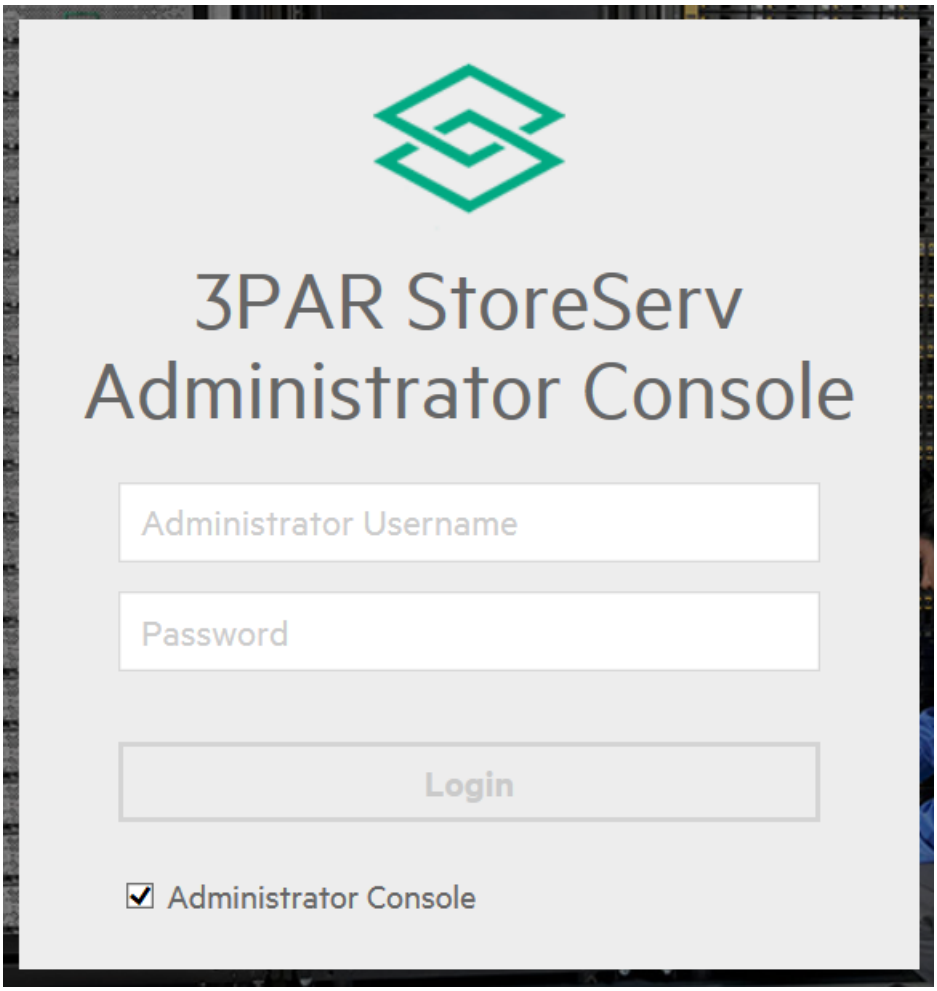
5. このアカウントのパスワードを入力します。パスワードは 8～32 文字で、少なくとも大文字が 1 文字、小文字が 1 文字、数字が 1 文字、および英数字以外の文字が 1 文字含まれている必要があります。
6. 確認のため、パスワードを再度入力します。
7. **設定**をクリックします。

管理者認証情報を設定した後、Administrator Console にログインし、まず 3PAR StoreServ ストレージシステムを追加する必要があります。

Administrator Console へのログイン

手順

1. SSMC にログインします（**SSMC へのアクセス**を参照してください）。
   a. SSMC へ初めてログインした場合は、表示されたダイアログボックスで **Administrator Console** を選択します。
   b. Administrator Console への以降のログインでは、SSMC のログイン画面の **Administrator Console** チェックボックスを選択します。
   c. Main Console への以降のログインでは、**Administrator Console** のチェックボックスがチェックされていないことを確認します。
2. SSMC 管理者ユーザー名とパスワードを入力します。



3. **Login** をクリックします。
   - Administrator Console が、新しいブラウザーウィンドウに表示されます。
   - 最初に Administrator Console を表示しようとしたとき、ホスト（SSMC サーバー）からのポップアップウィンドウが許可されていないという警告がブラウザーから出力されることがあります。多くの場合、警告アイコンをクリックすることで、ポップアップウィンドウを有効にできます。

SSMC へのストレージシステムの追加

手順

1. SSMC の Administrator Console にログインします。
2. **アクション**を選択し、**追加**をクリックします。
3. 追加するサーバーの DNS 名または IP アドレスを入力します。

   カンマかスペースのどちらかで区切ることで、複数のサーバーを追加できます。それぞれのサーバーを別々の行に記すこともできます。

   同時に複数のサーバーを追加する場合、それぞれのサーバーが同じログインおよびパスワード情報を使用していることが必要です。

   SSMC は、**システムへ接続**を選択解除しない限り、システムへ接続します。
4. **追加**をクリックします。

   システムは、メインの管理者コンソール画面に戻り、自動的にサーバーに接続します。

   接続の状態が未接続であり、状態説明に、有効な CA 証明書をインストールする必要があることが示されている場合は、**SSMC 用の CA 署名アレイ証明書の管理**を参照してください。

Administrator Console からの SSMC 管理対象システムへの接続

手順

1. SSMC サーバー上の SSMC Administrator Console にログインし、接続するストレージシステムを選択します。
2. **アクション→接続**の順に選択します。
3. **接続**ダイアログで**接続**をクリックします。

ストレージシステムへの接続が確立されると、接続の状態カラムに**接続済み**というテキストが、**状態説明**カラムに**接続が完了しました**というテキストが表示されます。

SSMC でのセッション制限

SSMC で、認証された各ログインは、別のユーザーによるログインか、同じユーザーによるログインかに関わらず、セッションとしてカウントされます。許可されたセッションの総数は、`ssmcbase/resources/ssmc.properties` の `security.max.active.ui.sessions` ディレクティブを使用して制御できます。この番号は、SSMC をインストールした後いつでも編集できます。

SSMC の高可用性を維持するための管理上のヒント

HPE では、SSMC の構成を変更した後は毎回、定期的なバックアップを取ることをお勧めしています。SSMC での SSMC 構成の変更のリストを以下に示します。

- システム認証情報の追加または編集。
- RMC 認証情報の追加または編集。

- グローバル設定への変更。
- システムレポートのカスタム設定。

定期的なバックアップは、システムクラッシュからのデータの保護に役立ちます。

HPE InfoSight 用の SSMC 構成

HPE InfoSight は、ストレージシステムから（サービスプロセッサー経由で）送信されるコールホームデータを分析し、機械学習アルゴリズムを実行して、有益なデータの情報をマイニングします。これらの有益な情報は、アラートとして SSMC に戻されます。

HPE InfoSight への SSMC の接続を有効にすると、SSMC はユーザーにシステムのヘルスについてのプロアクティブ通知を表示できます。さらに、アラートはストレージシステムのパフォーマンス、データが利用できなくなる可能性、データ損失の問題などの様々な問題を軽減するために役立つ適切なアクションも提案します。

HPE InfoSight アラートは、定期的に SSMC からフェッチされます。

SSMC での HPE InfoSight の前提条件

1. アラートを表示するシステム（アレイ）は、3PAR サービスプロセッサーからホームを呼び出すように構成する必要があります。
2. SSMC がインターネット（したがって HPE InfoSight）と通信できるように、適用可能な場合は、**プロキシサーバー情報**をセットアップします。
3. SSMC でアラートを受信する HPE InfoSight の構成：
   a. サインアップ手順に従って、Infosight.hpe.com で HPE パスポートのユーザーアカウントを作成します。
   b. HPE パスポートのアカウントは、HPE InfoSight のシステムグループに関連付ける必要があります。
   c. ストレージシステムは、システムグループに登録する必要があります。

SSMC での HPE InfoSight アカウントの追加

前提条件

HPE InfoSight アカウントの作成について詳しくは、HPE 3PAR StoreServ Management Console ユーザーガイドを参照してください。

SSMC で HPE InfoSight アカウントを追加する手順に従ってください。

手順

1. SSMC Main Console にログインします。
2. **設定** > **HPE InfoSight** に移動します。
3. **HPE InfoSight** フィールドを編集します。
4. HPE InfoSight アカウントの**ユーザー名**を入力します。
5. HPE InfoSight アカウントの**パスワード**を入力します。
6. **OK** をクリックします。

SSMC での HPE InfoSight アラートの表示

HPE InfoSight と SSMC 間の接続が成功すると、SSMC で HPE Infosight アラートを表示できます。

HPE InfoSight アラートを受信するには、HPE InfoSight でストレージシステムを構成する必要があります。

注記: ストレージシステムが構成されていない場合は、SSMC に、対応するストレージシステムに関する警告メッセージが表示されます。

SSMC で HPE InfoSight アラートを表示する手順に従ってください。

手順

1. SSMC Main Console にログインします。
2. **ストレージシステム** > **システム**に移動します。
3. **概要**をクリックします。
4. ドロップダウンから**アクティビティ**を選択します。
5. 構成されているストレージシステムに関する HPE InfoSight アラートが表示されます。各アラートメッセージには、以下のフィールドがあります。

フィールド	説明
推奨アクション	HPE InfoSight の推奨事項を指定します。
全般	システム、シリアル番号、タイプ、メッセージコード、発生元などの 詳細を一覧表示します。
コンポーネント	コンポーネントの詳細を指定します。
頻度	このアラートの頻度を指定します。

SSMC での HPE InfoSight 証明書のダウンロード

手順

1. **https://infosight.hpe.com** を開きます。
2. Internet Explorer を使用している場合は、**セキュリティレポート**をクリックします。Google Chrome を使用している場合は、**サイト情報の表示**をクリックします。
3. **詳細** > **ファイルにコピー**を選択します。
4. **証明書のエクスポートウィザード**で**次へ**をクリックします。
5. **Base-64 encoded X.509 (.CER)**を選択します。
6. エクスポートするファイルの名前を指定します。
7. **次へ**をクリックします。
8. **終了**をクリックします。

ヒント: ダウンロードした HPE InfoSight 証明書を保存します。

SSMC での HPE InfoSight の無効化

手順

1. SSMC Main Console にログインします。
2. **設定** > **アプリケーション**に移動します。
3. **アプリケーション**を編集します。
4. **HPE InfoSight への接続の有効化**フィールドで、ドロップダウンから**いいえ**を選択します。

SSMC の System Reporter 用の HPE 3PAR Excel アドイン

3PAR Excel アドインを使用すると、HPE 3PAR StoreServ Management Console RESTful API のデータを、Microsoft Excel で抽出およびレポートすることができます。このアドインは、SSMC を使用してデータを抽出します。現在サポートされている Microsoft Excel のバージョンについては、**SSMC の情報への SPOCK でのアクセス**を参照してください。

SSMC HPE 3PAR Excel アドインのベストプラクティス

- SSMC 3.0 以降にアップグレードすると、レポートのサンプリング解像度が最適化され、パフォーマンスが向上します。たとえば、1 か月の**高解像度**レポートが、1 か月の**毎時**レポートに最適化されます。
- ポートのリアルタイムレポートは、IP ベースのポートをサポートしていません。
- スケーリングされた環境では、環境の規模によって、レポートの生成にさらに時間がかかる場合があります。

  Hewlett Packard Enterprise では、レポートの作成時に上記のような問題が発生しないように、可能な場合は**すべて**オプションを選択するのではなく、**オブジェクトでフィルター**、**ルールでフィルター**、または**上/下**オプションを使用することをお勧めします。また、Hewlett Packard Enterprise では、Chrome ブラウザーの使用をお勧めします。

SSMC 用 3PAR Excel アドインのインストール

前提条件

Microsoft .Net Framework 4.5 以降が必要です。

重要: ご使用のシステムに Microsoft .Net Framework がインストールされていない場合、3PAR Excel アドインでインストールします。このとき再起動が必要な場合があります。

3PAR Excel アドインのインストール後に Microsoft Excel を開くと、再起動が必要な内部構成をプログラムが実行することがあります。

Microsoft のアドインプログラムのインストールについて詳しくは、**Microsoft サポートの Web サイト**を参照してください。

手順

1. **Software Depot** で、**HPE 3PAR SSMC Excel client installer SW** を見つけます。

   指示に従ってインストーラーソフトウェアを CD ROM にコピーします。ISO mounter ソフトウェアを使用して、3PAR Excel アドインをインストールすることもできます。
2. Microsoft Excel のすべてのウィンドウを保存して閉じ、次にプログラムを閉じます。
3. クライアントシステムで `HPESSMCSRExcelAddin.exe` を実行し、説明に従います。

   3PAR Excel アドインは、デフォルトのパス `C:\Program Files\Hewlett Packard Enterprise\HPE3PARSRExcelAddin` または `C:\Program Files (x86)\Hewlett Packard Enterprise\HPE3PARSRExcelAddin` にインストールされます。

3PAR Excel アドインの使用方法

1. Microsoft Excel を起動します。
2. **System Reporter** タブを選択します。
3. SSMC サーバー名とポートを入力し、次にユーザー名とパスワード（3PAR StoreServ ストレージシステムの認証情報）を入力します。
4. **Connect to SSMC** をクリックします。

ヒント: パフォーマンスデータを生成した場合に CSV データを表示するには、Excel スプレッドシートの左最上部まで移動してください。

作成されたレポートの日付の形式

3PAR Excel アドインは、レポートをプロットする場合に以下の日付形式を使用します。

- 高解像度—`mm/dd/yyyy hh:mm`
- 毎時—`mm/dd/yyyy hh:mm`
- 日次—`mm/dd/yyyy`

タイムスタンプ列のこの日付形式は、Microsoft Excel のセルの書式設定を使用して変更することができます。

3PAR Excel アドインのアンインストール

1. Windows で、**プログラムと機能**に移動します。
2. インストールされているプログラムのリストから **HPE 3PAR SSMC System Reporter Excel Add-in** を選択し、**アンインストール**をクリックします。

3PAR Excel アドインのトラブルシューティング

Microsoft Excel にアドインへのリンクが表示されない

症状

3PAR Excel アドインのインストール後、Microsoft Excel にアドインが表示されない。

原因

Microsoft Excel の設定により、アドインが無効になっています。

アクション

Microsoft Excel のアドイン下に 3PAR Excel アドインが表示されない場合、以下の手順を使用してアドインを有効にします。

1. Microsoft Excel で、**ファイル**をクリックし、次に**オプション**をクリックします。
2. **アドイン**をクリックします。
3. ページ下部の管理ボックスで**使用できないアイテム**を選択してから、**設定**をクリックします。

4. **アドイン（SR Excel Addin）**を選択してから**有効にする**をクリックします。
5. **OK** をクリックし、次に、Excel を閉じてからもう一度開きます。

SSMC の使用

SSMC のパフォーマンスに対するベストプラクティス

- **一括操作を、一度に 100 オブジェクトに制限する。**

  SSMC では、複数のオブジェクトをテーブルから選択するか、またはダイアログ内で選択することで、複数のオブジェクトに対して同時に実行できる操作があります。多数のオブジェクトに対して同時にアクションを実行すると、SSMC はより多くのデータを収集し、ストレージアレイに対してより多くのコマンドを発行する必要があります。これにより、タイムアウトエラーまたは切断メッセージが発生することがあります。

- **ベストなパフォーマンスを得るために、Chrome または Firefox を使用する。**

  SSMC は Internet Explorer 11 と Microsoft Edge をサポートしていますが、これらのブラウザーを使用すると、大規模な構成では、許容できないパフォーマンスになることが時々あります。

- **テーブル内を移動するときは、キーボードの矢印キーではなく、マウスを使用する。**

  上または下の矢印キーを押すごとに、SSMC はテーブル内の新しい項目を選択し、その項目に対するプロパティをフルセット取得します。立て続けに何度も連続して矢印キーを押すと、対応する数のプロパティ要求が作成されます。大規模または負荷の高い構成では、これによりタイムアウトエラーが発生するか、または UI が切断されることがあります。

- **システムリストをフィルターして、使用しているシステムだけにする。**

  システムセレクターを使用してシステムリストをフィルターし、作業対象のシステムだけが表示されるようにします。大規模な環境では、これによってオブジェクト数が大幅に減り、SSMC の応答が早くなります。

- **システム要件の項に記載されているメモリおよび CPU のガイドラインに従う。**

  アプライアンスは、小規模、中規模、大規模の 3 つの規模にデプロイできます。関連付けられているメモリと CPU の要件について詳しくは、**SSMC の最小および推奨システム要件**を参照してください。

- **同時に実行されるスケジュール済みレポートの数を、50 に制限する。**

- **フィルターを使用する。**

  ボリューム関連（エクスポート済みボリューム、仮想ボリューム、または仮想ボリュームキャッシュ）のレポートを作成するときは、Hewlett Packard Enterprise では、**すべてのオブジェクト**オプションを選択するのではなく、フィルターを使用することをお勧めします。

SSMC 管理者アカウントパスワードの変更

手順

1. Administrator Console にログインします。
2. メインメニューにある**セッション**アイコンをクリックします。
3. **認証情報の変更**をクリックします。
4. 表示された名前に対応する、現在のパスワードを入力します。
5. 新しいパスワードを入力します。
6. 確認のため、パスワードを再度入力します。
7. **変更**をクリックします。

SSMC 管理者アカウントパスワードのリセット

SSMC 管理者アカウントパスワードをリセットするには、TUI を使用します。**TUI** で示される指示に従います。

SSMC の Administrator Console からのログアウト

手順

1. メインメニューの**セッション**アイコンをクリックしてから、**ログアウトして閉じる**をクリックします。
2. **ログアウト**確認ダイアログで、**はい**をクリックするか、またはウィンドウの右上にある **X** をクリックして、ログイン画面に戻ります。

SSMC の管理対象システムの切断

管理対象システムを切断すると、ネットワークへの接続が終了します。システムは、SSMC を介した管理対象システムのリストからは削除されません。システムを切断すると、そのシステムを追加し直さずに、接続を後で再確立することができます。管理対象システムの削除については、**SSMC の管理対象システムの削除**を参照してください。

手順

管理対象システムを切断するには、以下の手順に従います。

1. SSMC の Administrator Console から、切断するシステムを選択します。
2. **アクション**を選択し、**接続解除**をクリックします。
3. 接続解除ダイアログで**接続解除**をクリックします。
4. 接続解除確認ダイアログボックス内の**接続解除します**をクリックします。

システムが切断されると、接続の状態カラムには**接続されていません**というテキストが、状態説明カラムには**ユーザー接続が解除されました**というテキストが表示されます。

SSMC の管理対象システムの削除

管理対象システムを削除すると、そのシステムが切断された後、SSMC を介した管理対象システムのリストからシステムが削除されます。ストレージシステムを再度管理するには、ストレージシステムを追加する必要があります。

管理対象システムを削除するには、以下の手順に従います。

手順

1. SSMC の Administrator Console から、削除するストレージシステムを選択します。
2. **アクション**を選択し、**削除**をクリックします。
3. 削除ダイアログで**削除**をクリックします。
4. 削除確認ダイアログで**削除します**をクリックします。

ストレージシステムを削除すると、管理対象システムのリストには表示されなくなります。

詳しくは

SSMC へのストレージシステムの追加(75 ページ)

コンソール間の切り替え

Main Console から Administrator Console へのみ、切り替えを行うことができます。

手順

Main Console からの Administrator Console へのアクセス

1. Main Console へのログイン中に、メインメニューの**セッション**アイコンをクリックします。
2. **Administrator Console** をクリックします。
3. **Administrator Console** ログインダイアログボックスが、新しいブラウザーウィンドウに表示されます。
4. ログアウトしてウィンドウを閉じるには、**ログアウトして閉じる**をクリックします。
5. ログアウト確認が表示されたら、**はい**をクリックするか、またはウィンドウの右上にある **X** をクリックして、ログイン画面に戻ります。

SSMC の Main Console のダッシュボードとチュートリアルの使用

Main Console および利用可能なヘルプの機能について詳しくは、HPE 3PAR StoreServ Main Console ユーザーガイドを参照してください。

重要: ユーザーセッションがタイムアウトになった場合、Main Console のメニューとチュートリアルが異常な動作を示すことがあります。必ずセッションからログアウトしてください。

手順

1. SSMC のソフトウェアがインストールされているサーバーを参照します。

   `https://<IP address or FQDN>:<secure_port>`

   ログイン画面が開きます。
2. Main Console にログインします。

   a. SSMC のログイン画面で、3PAR アカウントのユーザー名とパスワードを入力します。

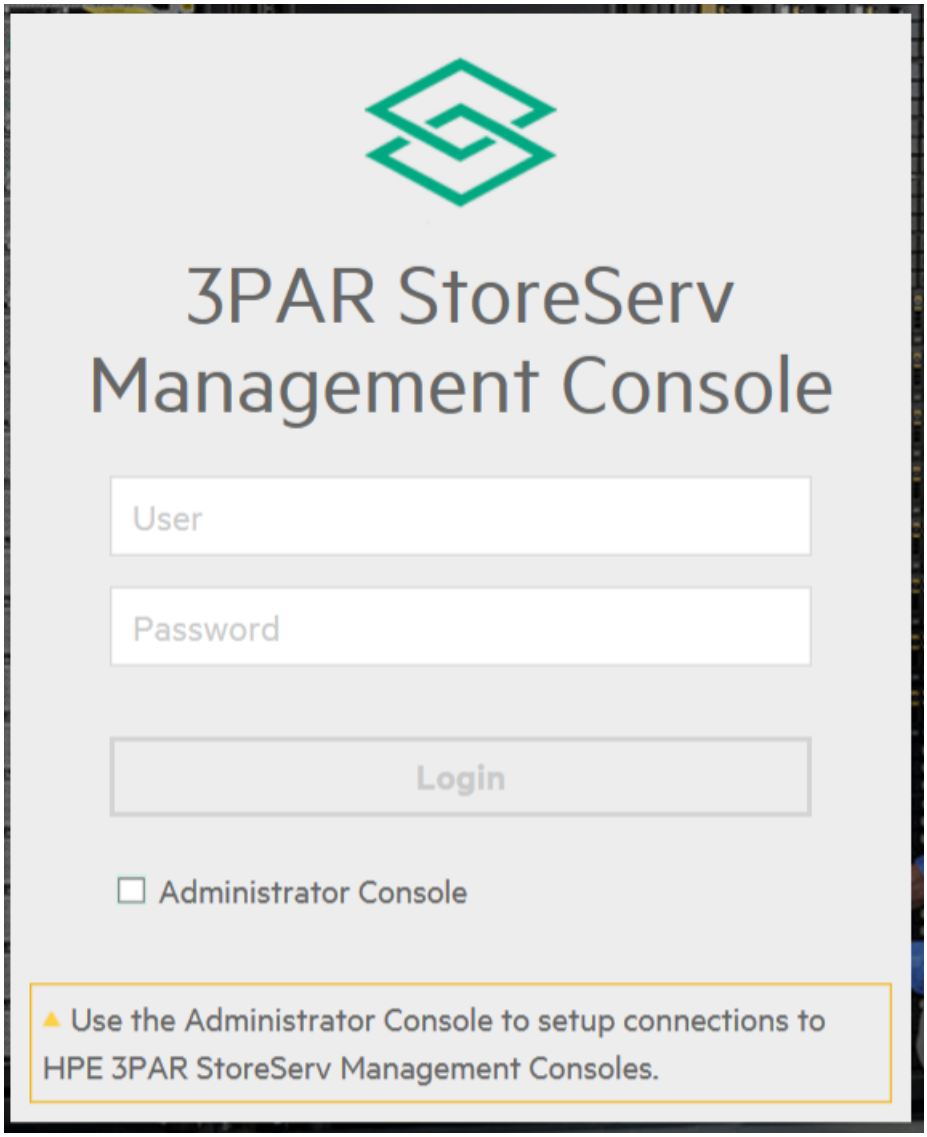


図 1: SSMC のログイン画面

b. Main Console にアクセスするために、Administrator Console の横のチェックボックスは**チェックを外してある**（デフォルト）ことを確認してください。

c. **ログイン**をクリックします。

ヒント: Main Console へ最初にログインした場合は、ナビゲーションチュートリアルが自動的に起動します。**次へ**をクリックして手動でチュートリアルを実行するか、**再生**をクリックして自動でチュートリアルを実行するか、または**閉じる**をクリックしてチュートリアルの参照を後に回すことができます。

3. Main Console 内の任意の場所で、ダッシュボードウィンドウの右上隅のクエスチョンマーク（**?**）をクリックすることで、ヘルプウィンドウが開きます。

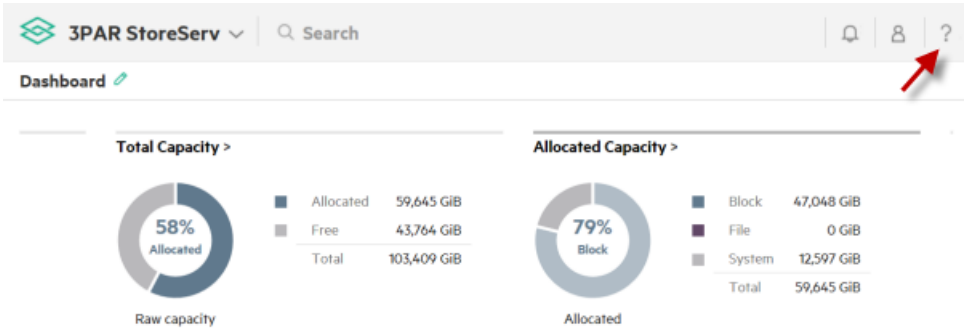


図 2: Main Console でヘルプにアクセスする

a. チュートリアルを実行するには、
ナビゲーションチュートリアルまたは**プロビジョニングチュートリアル**を実行します。

b. このページまたは任意のページのコンテキスト依存ヘルプは、**このページのヘルプ**をクリックします。

SSMC の構成のトラブルシューティング

SSMC へログインしているときには、アクティビティペインに、現在のセッションのアクティビティが表示されます。アクティビティの前の緑色のアイコンは、アクティビティが正常に完了したことを示します。アクティビティの前の黄色または赤色のアイコンは、エラーを示します。

SSMC の構成の問題

不正なオプション：?srckeystore

症状

FIPS のキーストアを変更した後、keytool により不正なオプション：`?srckeystore` エラーが返されました。

原因

Outlook や OneNote などのツールを使用して情報をコピーアンドペーストした場合、単純なダッシュ（-）をダッシュのように見えるがダッシュではないものに置き換えることがありました。

アクション

コピーアンドペーストではなくキーボードを使用して、ペーストしたダッシュを再入力してください。

FIPS モードの SSMC でサポートされていない HPE 3PAR オペレーティングシステムのバージョンの表示

症状

FIPS モードを有効にして SSMC を再起動した後、SSMC が一部のアレイに接続できなくなります。

原因

FIPS モード対応の SSMC は、サポートされている暗号を使用してのみアレイに接続できます。

アクション

SSMC で FIPS を必要とするすべての 3PAR StoreServ アレイを、HPE 3PAR オペレーティングシステム 3.2.2 MU6 以降にアップグレードしてください。

Google Chrome を使用して SSMC にログインした場合の、iPad での無効な証明書エラー

症状

Google Chrome を使用すると、iPAD から SSMC にログインできない。

原因

接続エラー `NET:ERR_CERT_INVALID` は、信頼できる証明書がインストールされていないことを示しています。

アクション

- SSMC サーバー上に、信頼できる証明書をインストールします。
- HPE 3PAR StoreServ Management Console 管理者ガイドを参照します。

利用可能なデータがテーブルにありません

症状

File Persona – ノードペアのエラーメッセージ。

原因

選択できるノードが表示されません。

アクション

- 3PAR CLI コマンド showlicense、showport、および showfs を実行して、システムに File Persona ライセンスと、File Persona をサポートしているノードがあることを確認します。
- システムに File Persona がインストールされている場合は、ノードに影響するほどシステムの状態が劣化している可能性を判断するために、システムの状態をチェックします。

Microsoft Internet Explorer を使用すると SSMC UI が読み込まれません

症状

SSMC UI はブラウザーから読み込まれず、応答しません。

原因

SSMC が自己署名証明書を必要とする場合、Microsoft Internet Explorer は SSMC が読み込まれないようにします。

アクション

- 接続が許可されるように、Windows Remote Manager で SSMC ホストを信頼できるホストとして設定します。
- **SSMC の証明書**を参照してください。

システム<*name*>には、利用可能な十分なポートがありません

症状

連携のエラーメッセージ。この連携にこのシステムを追加することはできない。

原因

このアクションを完了するために十分な数のポートがありません。

アクション

一部のポートをオフラインにして、連携に利用できるようにします。

ストレージアレイが容量履歴ダッシュボードパネルに表示されない

症状

容量履歴ダッシュボードパネルに、正しい数のストレージアレイがリストされません。

原因

オンノードの SR サービスが実行されていない場合は、容量履歴ダッシュボードパネルにストレージアレイが表示されません。

アクション

- 容量履歴ダッシュボードパネルに表示されているストレージアレイの数が予期したとおりでない場合は、不足しているアレイ上でオンノードの SR プロセスが実行されていない可能性があります。
- 対応策については、ご使用のシステムの特定のアレイレベルのドキュメントを参照してください。

SSMC にアクセスできない

症状

SSMC にアクセスするときに、`HTTP ERROR 403 - Forbidden` のエラーが表示されます。

原因

IP フィルタリングが実施されている可能性があります。

アクション

1. SSMC へのアクセスに使用しているシステムの IP アドレスを判別します。
2. **SSMC でのクライアント IP フィルタリングのサポート**を参照してください。

選択された 1 つ以上のシステムで利用できるデータがない場合でも、At Time ポップアップグラフにすべてのシステムのデータが示される

症状

利用できるデータがないシステムのデータポイントを選択すると、タイムスタンプデータが表示されます。

原因

これは、予期された動作です。特定の時点でのシステムのパフォーマンスデータが表示されます。その時点のデータが利用できない場合は、システムはその時点に最も近いタイムスタンプのデータを表示します。

アクション

対応は不要です。これは、予期された動作です。

サーバー[500] - Foundation.0060 からの HTTP エラー：ディレクトリパスにアクセスできない

症状

共有ディレクトリパスを含めるようにグローバル設定を編集した後で、システムから、ディレクトリパスにアクセスできないことを示すエラーが返されます。

原因

`java.policy`（セキュリティマネージャー）で許可を与えるまで、SSMC 3.3 のカスタム構成された共有ディレクトリパスにはアクセスできません。

アクション

System Reporter グローバル設定で共有ディレクトリパスを構成するときに、Java セキュリティマネージャー（`/opt/hpe/ssmc/jre/lib/security/java.policy`）でそのディレクトリ/パスの許可エントリーも追加する必要があります。この設定を変更した場合、有効にするために SSMC を再起動する必要があります。

SSMC 推奨バージョンが FIPS モードで表示されない

症状

この問題は、SSMC に HPE InfoSight 証明書がインストールされていないために発生します。HPE InfoSight 証明書は、設定で HPE InfoSight を構成しているときに証明書を提供することによりインストールできます。ただし、ユーザーまたはアレイ管理者が HPE InfoSight 機能を使用しない場合もあり、この場合、HPE InfoSight は有効になっていません。ただし、管理者またはユーザーは推奨バージョン情報を確認できます。

解決方法 1

アクション

HPE InfoSight 構成で HPE InfoSight 証明書を提供します。HPE InfoSight 証明書をダウンロードします。HPE InfoSight 構成に対し SSMC でこの証明書を使用します。HPE InfoSight 証明書をダウンロードするには、次の手順に従ってください。

1. **HPE InfoSight 証明書をダウンロードします**。
2. SSMC と HPE InfoSight 間の接続を起動するには、次の手順に従ってください。
   a. **3PAR StoreServ Management Console** にログインします。
   b. **3PAR StoreServ** > **設定**に移動します。
   c. **HPE InfoSight** を編集します。

      注記: グローバル設定の編集ウィザードが開きます。

   d. 表示ドロップダウンから **HPE InfoSight** を選択します。

e. ユーザー名を入力します。

f. パスワードを入力します。

g. HPE InfoSight 証明書を証明書ボックスに入力します。

h. OK をクリックします。

推奨バージョンが 24 時間後に SSMC に表示されます。

解決方法 2

アクション

HPE InfoSight 証明書をアプライアンスに手動でインポートします。SSMC アプライアンスのいずれかのディレクトリ、たとえば<infosight cert location>に、ダウンロードした HPE InfoSight 証明書をコピーします。次のコマンドを使用して、手動で HPE InfoSight 証明書を構成します。

```
cd /opt/hpe/ssmc/ssmcbase/data/StoreServMC/infoSight
cp <infosight cert location> infosight.cer
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -genkey -keyalg RSA -alias infosight -keystore INFOSIGHT-MC-TrustStore -storepass
infosighttruststorepass -keypass infosighttruststorepass -dname "CN=hpe.com, OU=HPE, O=HPE, L=Palo Alto, S=CA, C=US"
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -import -alias infosight1 -file infosight.cer -keystore INFOSIGHT-MC-TrustStore
-storepass infosighttruststorepass -noprompt
/opt/hpe/ssmc/ssmcbase/fips/jre/bin/keytool -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
/opt/hpe/ssmc/ssmcbase/bcFipsJars/bc-fips-1.0.1.jar -importkeystore -srckeystore INFOSIGHT-MC-TrustStore -destkeystore
INFOSIGHT-MC-TrustStore.bcfks -srcstoretype JKS -deststoretype BCFKS -srcstorepass infosighttruststorepass
-deststorepass infosighttruststorepass -noprompt
rm INFOSIGHT-MC-TrustStore
mv INFOSIGHT-MC-TrustStore.bcfks INFOSIGHT-MC-TrustStore
rm infosight.cer
```

注記: HPE InfoSight 証明書をアプライアンスにコピーするには、SFTP ツールを使用します。

アプライアンスに ping を実行できない

症状

SSMC アプライアンスが最初にデプロイされ、デプロイ後にアプライアンス名が変更しました。SSMC アプライアンスにログインし、TUI からデプロイエラーを表示する場合は、**View deployment errors** を選択します。デプロイエラーを表示する代わりに、エラー **Unable to configure network 1 device** が表示されます。

アクション

このような場合は、`config_appliance` を使用し、TUI で示されるデフォルト値を再利用することでネットワークを再構成します。アプライアンスにアクセスするには、**再起動**が必要です。

SSMC のログファイル

SSMC には、深刻度が低いものから順に、以下の 4 種類の深刻度レベルがあります。

INFO

要求の進度を高度なレベルで表示する情報メッセージを示します。

WARN

潜在的に有害な状況、またはサーバーが対処可能なエラーを示します。

ERROR

システムの設計上発生してはならないエラーではあるものの、サーバーが動作を継続できるエラーを示します。

FATAL

サーバーが正常に起動できないような重大なエラー、またはすでに動作中であればサーバーがクラッシュするようなエラーを示します。

ログファイルとそのデフォルトの位置を、以下のリストに示します。

ログファイル名	ディレクトリ位置	内容
audit.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	Security Administrator モニターを補助し、セキュリティポリシーを実施します。保持/ロールオーバーポリシーは、それぞれ 1Mb の 10 ファイルです。audit.log には、以下のカラムがあります。 · **システム名** – 3PAR StoreServ Storage System アレイ名が利用可能な場合は、その名前です。それ以外の場合は IP アドレスです。 · **アクション** – CREATE、DELETE、UPDATE、LOGIN、READ、STARTUP、SHUTDOWN、ARRAY ACTION、または UNKNOWN のいずれかのアクションです。 · **結果** – SUCCESS、FAILURE、SOME_FAILURES、CANCELLED、KILLED、INFO、OPERATION、FORBIDDEN、UNAUTHORIZED、TASK CREATED、または UNKNOWN のいずれかの結果です。 · **深刻度** – INFO、WARNING、CRITICAL、または UNKNOWN のいずれかの分類です。
fatal.log		サーバーを正しく起動できない原因となったエラー、およびサーバーの予期しないシャットダウンの原因となったエラーをリストします。保持/ロールオーバーポリシーは、それぞれ 1Mb の 2 ファイルです。

表は続く

ログファイル名	ディレクトリ位置	内容
metrics.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	SSMC キャッシュ内のオブジェクトの数を示します。Metrics Cache stats の出力を使用して、SSMC が管理するオブジェクトの総数を計算します。それぞれが 10MB の、metrics.log.<1-3>という 3 つのログファイルが含まれています。
rest_history.log		GET、POST、PUT、および DELETE 要求の監査エントリーです。内部用、開発時のトラブルシューティング用です。
ssmc.log		アプリケーションの管理者にとって、製品のヘルスを測定する役に立ち、フィールドサポートとともにお客様の問題についてトラブルシューティングを行う助けとなります。保持/ロールオーバーポリシーは、それぞれ 100Mb の 2 ファイルです。
tclapi.audit	**論理的な位置：**/opt/hpe/SSMC/ssmcbase/data/InFormMC/log **物理的な位置：**/var/opt/hpe/SSMC/data/InForm/log	接続されている各 3PAR StoreServ ストレージシステムアレイに送信されたコマンドの監査エントリーです。
wrapper.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	このファイルには、YAJSW（Yet Another Java Service Wrapper）からのすべてのログ情報、および SSMC 製品からのすべてのコンソール出力が含まれます。このファイルは、ssmc.log のすべての内容をミラー化するとは限りません。SSMC の出力が、ログファイルのみに移動する場合、wrapper.log にはそのデータが含まれません。wrapper 情報には、YAJSW のバージョン、OS タイプ、JVM バージョン、作業ディレクトリ、サービス起動情報、起動されたアプリケーションの PID などがあります。アプリケーションのコンソール出力では、2 番目のフィールドの出力行に、「wrapper」の PID インスタントが含まれます。
archiveLogs		このファイルには、zip 圧縮形式で以前のファイルが含まれています。

表は続く

ログファイル名	ディレクトリ位置	内容
datapollers.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	このファイルには、アレイからデータをフェッチするためのすべてのポーリングジョブの開始と停止に関するログエントリーが含まれます。
diag.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	このファイルには JRE 関連の統計情報が含まれており、これは 1 分ごとに印刷されます。
events.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	このファイルには、SSMC サーバーが接続されているすべてのアレイから到達したすべてのイベントが記録されています。
eventsthrottle.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	このファイルには、生成されたすべての内部イベントと、アレイ応答の遅れのためにポーラースケジューラーに適用されるすべてのスロットル調整が記録されます。
vmvision.log	**論理的な位置：**/opt/hpe/ssmc/ssmcbase/data/logs **物理的な位置：**/var/opt/hpe/ssmc/data/logs	-

Web サイト

全般的な Web サイト

Hewlett Packard Enterprise Information Library

http://www.hpe.com/info/EIL

Single Point of Connectivity Knowledge（SPOCK）ストレージ互換性マトリックス

http://www.hpe.com/storage/spock

ストレージのホワイトペーパーおよび分析レポート

http://www.hpe.com/storage/whitepapers

その他の Web サイトについては、**サポートと他のリソース**を参照してください。

詳しくは

http://www.hpe.com/support/SSMCVideos

サポートと他のリソース

Hewlett Packard Enterprise サポートへのアクセス

- ライブアシスタンスについては、Contact Hewlett Packard Enterprise Worldwide の Web サイトにアクセスします。

  http://www.hpe.com/assistance

- ドキュメントとサポートサービスにアクセスするには、Hewlett Packard Enterprise サポートセンターの Web サイトにアクセスします。

  http://www.hpe.com/support/hpesc

ご用意いただく情報

- テクニカルサポートの登録番号（該当する場合）
- 製品名、モデルまたはバージョン、シリアル番号
- オペレーティングシステム名およびバージョン
- ファームウェアバージョン
- エラーメッセージ
- 製品固有のレポートおよびログ
- アドオン製品またはコンポーネント
- 他社製品またはコンポーネント

アップデートへのアクセス

- 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

  Hewlett Packard Enterprise サポートセンター

  http://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise サポートセンター：ソフトウェアのダウンロード

  http://www.hpe.com/support/downloads

  Software Depot

  http://www.hpe.com/support/softwaredepot

- eNewsletters およびアラートをサブスクライブするには、以下にアクセスします。

  http://www.hpe.com/support/e-updates-ja

- お客様の資格を表示したりアップデートしたり、契約や保証をお客様のプロファイルにリンクしたりするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページにアクセスします。

  http://www.hpe.com/support/AccessToSupportMaterials

重要: 一部のアップデートにアクセスするには、Hewlett Packard Enterprise サポートセンターからアクセスするときに製品資格が必要になる場合があります。関連する資格を使って HPE パスポートをセットアップしておく必要があります。

カスタマーセルフリペア（CSR）

Hewlett Packard Enterprise カスタマーセルフリペア（CSR）プログラムでは、ご使用の製品をお客様ご自身で修理することができます。CSR 部品を交換する必要がある場合、お客様のご都合のよいときに交換できるよう直接配送されます。一部の部品は CSR の対象になりません。Hewlett Packard Enterprise もしくはその正規保守代理店が、CSR によって修理可能かどうかを判断します。

リモートサポート（HPE 通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。リモートサポートは、インテリジェントなイベント診断を提供し、ハードウェアイベントを Hewlett Packard Enterprise に安全な方法で自動通知します。これにより、ご使用の製品のサービスレベルに基づいて、迅速かつ正確な解決が行われます。ご使用のデバイスをリモートサポートに登録することを強くおすすめします。

ご使用の製品にリモートサポートの追加詳細情報が含まれる場合は、検索を使用してその情報を見つけてください。

リモートサポートおよびプロアクティブケア情報

HPE 通報サービス

http://www.hpe.com/jp/hpalert

HPE プロアクティブケアサービス

http://www.hpe.com/services/proactivecare-ja

HPE プロアクティブケアサービス：サポートされている製品のリスト

http://www.hpe.com/services/proactivecaresupportedproducts

HPE プロアクティブケアアドバンストサービス：サポートされている製品のリスト

http://www.hpe.com/services/proactivecareadvancedsupportedproducts

保証情報

ご使用の製品の保証に関する情報を表示するには、以下のリンクを参照してください。

HPE ProLiant と IA-32 サーバーおよびオプション

http://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise および Cloudline サーバー

http://www.hpe.com/support/EnterpriseServers-Warranties

HPE ストレージ製品

http://www.hpe.com/support/Storage-Warranties

HPE ネットワーク製品

http://www.hpe.com/support/Networking-Warranties

規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterprise サポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

規定に関する追加情報

Hewlett Packard Enterprise は、REACH（欧州議会と欧州理事会の規則 EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

http://www.hpe.com/info/reach

RoHS、REACH を含む Hewlett Packard Enterprise 製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

http://www.hpe.com/info/ecodata

社内プログラム、製品のリサイクル、エネルギー効率などの Hewlett Packard Enterprise の環境に関する情報については、次を参照してください。

http://www.hpe.com/info/environment

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当（**docsfeedback@hpe.com**）へお寄せください。この電子メールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載ください。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。

用語集

AFC

Adaptive Flash Cache

AO

Adaptive Optimization

CA

認証局

CLI

コマンドラインインターフェイス

CPG

共通プロビジョニンググループ

DAR

保存データ

DIT

ディレクトリ情報ツリー

DN

識別名

DO

Dynamic Optimization

FIPS

連邦情報処理規格

FPG

ファイルプロビジョニンググループ

LDAP

Lightweight ディレクトリアクセスプロトコル

MC

HPE 3PAR Management Console

QoS

サービス品質

RC

Remote Copy

SLD

同期長距離

SSMC

HPE 3PAR StoreServ Management Console

シックプロビジョニング（Eager Zeroed）

フォールトトレランスなどのクラスタリング機能をサポートする、シック仮想ディスクのタイプです。仮想ディスクに必要な容量は、作成時に割り当てられます。フラットフォーマットと異なり、物理デバイスに残っているデータは、仮想ディスクの作成時にゼロで初期化されます。このフォーマットでディスクを作成する場合は、他のタイプで作成するよりも、大幅に時間がかかる場合があります。

シックプロビジョニング（Lazy Zeroed）

デフォルトのシックフォーマットで仮想ディスクを作成します。仮想ディスクに必要なスペースは、仮想ディスクを作成するときに割り当てられます。物理デバイス上に残っているデータは作成時に消去されませんが、後で必要に応じて、仮想マシンからの最初の書き込み時にゼロで消去されます。

シンプロビジョニング

ストレージ領域を節約します。シンディスクの場合、ユーザーがディスクサイズに入力する値に基づいて、ディスクが必要とするデータストア領域がプロビジョニングされます。ただし、シンディスクは最初に小さいサイズで開始され、ディスクが当初の操作に必要とするデータストア領域のみが使用されます。

オープンソースコード

次の表に、オープンソースコードのツールとライセンスの情報を示します。最新情報の一覧については、SSMC DVD ISO イメージのライセンスのディレクトリにある **thirdPartyManifest.pdf** を参照してください。

ツール名	バージョン	ライセンスの URL または場所
javax.activation の activation	1.1.1	**CDDL**
Apache James Mime4j	0.6	**Apache 2.0**
Apache Lucene	4.10.4	**Apache 2.0**
Avalon Framework	4.2.0	**Apache 2.0**
awaitility	2.0.0	**Apache 2.0**
Barcode4j	2.0	**Apache 2.0**
Bouncy Castle	1.52	**Bouncy Castle MIT**
org.codehaus.castor の castor	1.2	**Apache 2.0**
cglib	3.1	**Apache 2.0**
ColReorderWithResize	1.1.0 – dev2	**BSD-3 – Clause**
commons beanutils	1.9.2	**Apache 2.0**
commons-cli-1.2.jar	1.2	**Apache 2.0**
commons-codec-1.9.jar (master: commons-codec-1.6.jar)	1.9	**Apache 2.0**
commons-collections	3.2.2	**Apache 2.0**
commons-digester	2.1	**Apache 2.0**
commons-io	2.1	**Apache 2.0**
commons-lang	2.6	**Apache 2.0**
commons-lang3	3.4	**Apache 2.0**
commons-logging	1.1.3	**Apache 2.0**
commons-net	3.5	**Apache 2.0**
commons-pool	2.4.2	**Apache 2.0**

表は続く

ツール名	バージョン	ライセンスの URL または場所
commons-vfs2	2.0	Apache 2.0
commons-xml-apis	1.4.01	Apache 2.0
Dom4J	1.6.1	BSD-3 - Clause
Dynamic Reports	4.0.0	LGPL v3
org.eclipse.jdt.core.compiler の ecj	4.3.1	EPL 1.0
ECMA262-5.js	パブリックドメイン	ー
ElasticSearch Server	1.7.4	Apache 2.0
excanvas.js	なし/r3	Apache 2.0
ExpiringMap (JHalterman)	0.5.7	Apache 2.0
com.sun.xml.fastinfoset の FastInfoset	1.2.7	Apache 2.0
gentlyWEB	1.1	Apache 2.0
Globalize	0.1.1	MITJquery Globalize License
gson-2.3.1.jar	2.3.1	Apache 2.0
Guava	19.0	Apache 2.0
html5.js	2.1pre	MIT
org.apache.httpcomponents の httpclient	4.3.6	Apache 2.0
org.apache.httpcomponents の httpcore	4.3.3	Apache 2.0
ICU4j	2.6.1	ICU License
com.sun.istack の istack-commons-runtime	2.1.6	CDDL 1.0
com.itextpdf の itextpdf	5.5.0	LGPL 2.1
Jackson	1.9.13	Apache 2.0
com.fasterxml.jackson.core の jackson-annotations	2.8.0	Apache 2.0

表は続く

ツール名	バージョン	ライセンスの URL または場所
com.fasterxml.jackson.core の jackson-core	2.8.4	Apache 2.0
org.codehaus.jackson の jackson-core-asl	1.9.13	Apache 2.0
com.fasterxml.jackson.core の jackson-databind	2.8.4	Apache 2.0
com.fasterxml.jackson.datatype の jackson-datatype-guava	2.8.4	Apache 2.0
org.codehaus.jackson の jackson-jaxrs	1.9.12	Apache 2.0
org.codehaus.jackson の jackson-mapper-asl	1.9.13	Apache 2.0
org.codehaus.jackson の jackson-xc	1.9.12	Apache 2.0
net.sf.jasperreports の jasperreports	6.0.0	LGPL 2.1
Java Hamcrest	1.3	BSD-3 - Clause
Javassist	3.18.2 - GA	Apache 2.0
com.sun.mail の javax.mail	1.5.5	CDDL 1.0
javax.xml.bind の jaxb-api	2.2.7	CDDL 1.0
com.sun.xml.bind の jaxb-core	2.2.7	CDDL 1.0
com.sun.xml.bind の jaxb-impl	2.2.7	CDDL 1.0
Jaxen	1.1 - beta6	The Werken Company LicenseBSD 3 - Clause
org.jboss.spec.javax.annotation の jboss-annotations-api_1.2_spec	1.0.0 Final	CDDL 1.0
org.jboss.spec.javax.ws.rs の jboss-jaxrs-api_2.0_spec	1.0.0 Final	CDDL 1.0
org.jboss.logging の jboss-logging	3.1.4 GA	Apache 2.0
net.jcip の jcip-annotations	1	CCA 2.5
jfree の jcommon	1.0.15	LGPL 2.1
Jcraft Jsch	0.1.53	BSD-3 - Clause

表は続く

ツール名	バージョン	ライセンスの URL または場所
Jetty	9.3.12.v20160915	Apache 2.0
Jfreechart	1.0.13	LGPL v2.1
Joda Time	2.2	Apache 2.0
josql	2.2.0	Apache 2.0
jquery	1.8.3	MIT
jquery.ba-hashchange.js	1.3	MIT
jquery.browser.js	2.3	MIT
jquery.columnizer.js	1.6.0	Creative Commons Attribution 3.0
jquery.cookie.js	1.3.1	MIT
jquery.dataTables.js	1.9.4	MIT
jquery.dataTables.rowReordering.js	1.0.0	MIT
jquery.dateFormat.js	1.0（2011 年 6 月 15 日）	MIT
jquery.flot.categories.js	なし/1	MIT
jquery.flot.fillbetween.js	なし/0.8	MIT
jquery.flot.js	0.8.0	MIT
jquery.flot.pie.js	なし/0.7	MIT
jquery.flot.selection.js	なし/0.7	MIT
jquery.flot.time.js	なし/0.7	MIT
jquery.js	1.8.3	MIT
jquery.knob.js	1.2.0	MIT
jquery.mask.js	1.6.5	MIT
jquery.maskedinput-1.3.js	1.3	MIT
jquery.selectBox.js	1.0.7	MIT
jquery.sparkline.js	2.1	BSD-3 – Clause
jquery.ThreeDots.js	1.0.10	MIT

表は続く

ツール名	バージョン	ライセンスの URL または場所
jquery.timeago.js	1.4.1	MIT
jquery-ui.js	1.9.2	MIT
jquery-ui-sliderAccess.js	0.3	MIT
jquery-ui-timepicker-addon.js	1.1.2	MIT
jquery.validate.js	1.10.0	MIT
JSON	20080701	JSON License
Json.NET 6.0 Release 8	6.0、Rel 8	Codeplex MITOpenSource MIT
json2.js	なし/40597	ー
JSON-path	0.8.0	Apache 2.0
net.minidev の json-smart	1.1	Apache 2.0
JSR305	2.0.3	Apache 2.0
Junit	4.12	Eclipse Public License v1.0
krukow/clj-ds	0.0.4	Eclipse Public License v1.0
Log4J	1.2.17	Apache 2.0
Lucerne	4.6.1	Apache 2.0
Makeself	2.1.5	GNU GPL v2.txt
MapDB	1.0.9	Apache 2.0
org.apache.maven.scm の maven-scm-api	1.4	Apache 2.0
org.apache.maven.scm の maven-scm-provider-svn-commons	1.4	Apache 2.0
org.apache.maven.scm の maven-scm-provider-svnexe	1.4	Apache 2.0
modernizr.js	2.6.2	MIT
org.objenesis の objenesis	2.1	Apache 2.0
OpenCSV	2.3	Apache 2.0
org.codehaus.plexus の plexus-utils	1.5.6	Apache 2.0

表は続く

ツール名	バージョン	ライセンスの URL または場所
Reflections	0.9.9 – RC1	パブリックドメイン
regexp の regexp	1.3	Apache 2.0
require.js	2.1.4	MIT
RESTeasy	3.0.19.Final	Apache 2.0
sblim-cim-client	2.2.5	Eclipse Public License v1.0
shBrushCss.js	なし/3.0.83	MIT
shBrushJScript.js	なし/3.0.83	MIT
shBrushPlain.js	3.0.83	MIT
shBrushXml.js	なし/3.0.83	MIT
shCore.js	なし/3.0.83	MIT
SLF4J	1.7.10	MITSLF4J
org.yaml の snakeyaml	1.12	Apache 2.0
com.spatial4j の spatial4j	0.4.1	Apache 2.0
text.js	2.0.4	MIT
Touch Punch	0.2.3	MIT
Trove4J	3.0.3	MIT LGPL v2.1
use.js	0.3.0	MIT
xml-apis-1.4.01.jar	1.4.01	Apache 2.0
xregexp.js	1.5.1	MIT
Yet Another Java Service Wrapper (YAJSW)	11.11	LGPL v2.1
YourKit (yjpagent.dll)		https://www.yourkit.com/purchase/license.html
Zulu: Multi-platform Certified OpenJDK	1.8.0_45	GPL v2