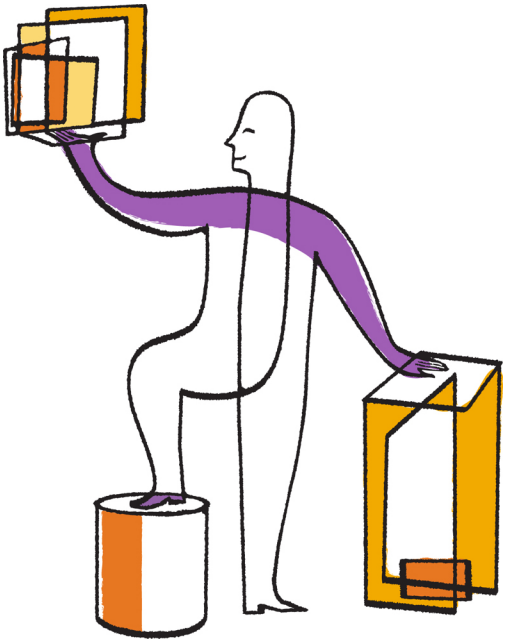
8.3.1用に更新

clustered Data ONTAP® 8.3

システム アドミニストレーション ガイド



ネットアップ株式会社
www.netapp.com/jp

部品番号: 215-10709_A0
作成日: 2015年6月

目次

クラスタ管理者とSVM管理者の違い 10
Data ONTAP管理インターフェイスの基本 11
CLIを使用したクラスタへのアクセス 11
シリアル ポートによるクラスタへのアクセス 11
SSHを使用したクラスタへのアクセス 11
クラスタへのTelnetアクセスまたはRSHアクセスの有効化 13
Telnetを使用したクラスタへのアクセス 14
RSHを使用したクラスタへのアクセス 15
Data ONTAPコマンドライン インターフェイスの使用 16
CLIコマンド用のシェルの種類について 17
CLIコマンド ディレクトリの移動方法 18
CLIで値を指定する際のルール 19
コマンド履歴の表示方法とコマンドの再発行方法 20
CLIコマンドを編集するためのキーボード ショートカット 20
管理権限レベルの使用 21
CLIでの権限レベルの設定 22
CLIでの表示環境設定 22
クエリ演算子の使用方法 23
拡張クエリの使用方法 24
フィールドを使用したshowコマンド出力のカスタマイズ方法 24
位置指定パラメータの概要 25
Data ONTAPマニュアル ページへのアクセス方法 26
CLIセッションの管理 27
CLIセッションのレコードの管理 27
CLIセッションの自動タイムアウト時間の管理 28
OnCommand System Managerのブラウザベースのグラフィカル インターフェイスを使用したクラスタへのアクセス 28
OnCommand System Managerの概要 29
OnCommand System Managerへのアクセス管理方法 29
クラスタ管理の基礎（クラスタ管理者のみ） 31
クラスタとは 31
シングルノード クラスタに関する考慮事項 32
クラスタ管理サーバとは 32
クォーラムとイプシロンについて 33
クラスタ レプリケーション リングとは 34
クラスタ内のノードに関する情報の表示 34
クラスタ属性を表示する 35
クラスタ属性の変更 35
クラスタ レプリケーション リングのステータス表示 36
ノードの管理 37
ノード属性の表示 37

ノード属性の変更 37
ノード名の変更 38
クラスタへのノードの追加 38
クラスタからのノードの削除 40
Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、および MIBファイルへのアクセス 42
ノードのシステム コンソールへのアクセス 43
ノードのルート ボリュームとルート アグリゲートに関するルール 44
ノードのルート ボリュームのスペースの解放 45
ノードの起動または停止 46
システム プロンプトでのノードのリブート 46
ブート環境のプロンプトからのData ONTAPのブート 47
ノードのシャットダウン 48
ブート メニューによるノード管理 49
サービス プロセッサを使用したリモートからのノードの管理 50
SPの概要 50
SPネットワークの設定 52
SPファームウェアの更新の管理方法 57
SPへのアクセス 59
SP CLIでのオンライン ヘルプの使用 63
ノードのリモート管理用コマンド 63
Data ONTAPからのSPの管理用コマンド 71
SVMの管理 76
SVMとは 76
SVMルート ボリュームがデータ アクセスに使用される仕組み 78
SVMの種類 78
SVMの使用目的 78
クラスタ内のSVM数 79
SVMのセットアップ 80
SVMの作成計画 80
SVMの作成に関するガイドライン 83
FlexVolを備えたSVMの作成 86
Infinite Volumeを備えたSVMの作成 90
SVMの設定 92
SVM管理者用のユーザ アカウントの作成 92
SVM管理者用のローカル ユーザ アカウントの作成 93
SVM管理者用のNISまたはLDAPユーザ アカウントへのアクセスの許可 93
SVM管理者用のActive Directoryユーザまたはグループへのアクセスの許可 94
SVM管理者への管理の委譲 95
SVMの変更 97
SVMのアグリゲートの変更 98
SVMのプロトコルの変更 99
SVM属性の変更用コマンド 100

SVMに関する情報の表示 100
SVMの名前の変更 102
SVMの削除 102
SVMの起動 103
SVMの停止 104
SVMコンテキストからのSVMの管理 105
SVMのルート ボリュームのリストア 106
負荷共有ミラー コピーの昇格 107
データ保護ミラー コピーの昇格 108
新しいFlexVolの昇格 108
Infinite Volumeを備えたSVM上への新しいルート ボリュームの作成 109
ストレージQoSを使用したSVMへのI/Oパフォーマンスの制御および監視 110
SVMの管理 112
SVMのアクセス方式と認証方式 113
SVMへのログイン 114
ログイン パスワードの変更 115
SVMに関する情報の表示 115
ネットワーク設定に関する情報の表示 116
SVMの管理に関する詳細情報の参照先 117
クラスタへのアクセスの管理 119
ユーザ アカウントの管理 119
ユーザ アカウントへのアクセス方法 120
ユーザ アカウントの認証方式 120
ADユーザとグループに対するクラスタおよびSVMへのアクセスの許可 121
NISまたはLDAPユーザに対するクラスタへのアクセスの許可 123
ユーザ アカウントの管理用コマンド 125
アクセス制御ロールの管理 126
クラスタ管理者の事前定義されたロール 127
SVM管理者の事前定義されたロール 127
アクセス制御ロールのカスタマイズに関する考慮事項 129
アクセス制御ロールのカスタマイズによる特定コマンドへのユーザ アクセスの制限 132
アクセス制御ロールでのユーザ名およびパスワードのルール設定の管理 133
パスワード ルールの設定に関する考慮事項 134
アクセス制御ロールの管理用コマンド 135
SSHセキュリティ設定の管理 137
SSHセキュリティ設定の管理用コマンド 139
公開鍵の管理 139
公開鍵の管理用コマンド 140
サーバまたはクライアント認証用のデジタル証明書の管理 140
クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール 141

クラスタまたはSVMのSSLクライアントを認証するためのクライアントCAまたはルートCA証明書のインストール 144
クラスタまたはSVMがクライアントであるSSLサーバを認証するためのサーバCA証明書のインストール 147
クラスタまたはSVMをSSLクライアントとして認証するためのクライアント証明書のインストール 148
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール 150
期限切れのデジタル証明書の交換 152
デジタル証明書の管理用コマンド 153
Webサービスへのアクセスの管理 154
Webプロトコル エンジンの管理 155
Webサービスの管理 156
SSLの管理 158
Webサービスへのアクセスの設定 159
管理アクティビティの監査設定の管理 162
コマンド履歴ログの転送 163
管理アクティビティの監査設定の管理用コマンド 165
クラスタ時間の管理 166
クラスタ時間の管理用コマンド 167
バナーとMOTDの管理 168
バナーの作成 169
バナーの管理 171
MOTDの作成 172
MOTDの管理 173
ライセンスの管理 176
ライセンス タイプとライセンス方式 177
ライセンスの管理用コマンド 178
ジョブおよびスケジュールの管理 180
ジョブのカテゴリ 180
ジョブの管理用コマンド 180
ジョブ スケジュールの管理用コマンド 181
クラスタ構成のバックアップおよびリストア 183
構成バックアップ ファイルとは 183
構成バックアップの管理 183
ノードおよびクラスタ構成を自動的にバックアップする方法 183
構成バックアップ スケジュールの管理用コマンド 184
構成バックアップ ファイルの管理用コマンド 184
ノード構成のリカバリ 185
ノードのリカバリに使用する構成バックアップ ファイルの検索 185
構成バックアップ ファイルを使用したノード構成のリストア 186
クラスタ構成のリカバリ 187
クラスタのリカバリに使用する構成の検索 187
既存の構成からのクラスタ構成のリストア 188
ノードのクラスタとの同期 190

コア ダンプの管理 191
コア ダンプ ファイルの分割方法 191
コア ダンプの管理用コマンド 192
コア分割の管理用コマンド 193
ストレージ システムの監視 195
イベント メッセージの管理 195
イベント管理システムのセットアップ 196
イベントの管理用コマンド 197
AutoSupportの管理 198
AutoSupportメッセージが送信されるタイミングおよび場所 199
AutoSupportによるイベントトリガー型メッセージの作成および送信 201
AutoSupportメッセージとそのコンテンツのタイプ 202
AutoSupportサブシステムとは 203
AutoSupportのサイズ割当量と時間割当量 203
イベントトリガー型AutoSupportメッセージで送信されるファイル 205
AutoSupportメッセージで送信されるログ ファイル 205
週単位のAutoSupportメッセージで送信されるファイル 206
AutoSupportがテクニカル サポートから送信指示を取得する仕組み 206
Eメールで送信したAutoSupportメッセージの構造 207
AutoSupportの重大度のタイプ 208
AutoSupportの使用要件 208
AutoSupportの設定 210
コア ダンプ ファイルのアップロード 212
パフォーマンス アーカイブ ファイルのアップロード 213
AutoSupportメッセージの説明の取得 214
AutoSupportの管理用コマンド 214
AutoSupportマニフェストに含まれる情報 216
My AutoSupportとは 216
AutoSupportのトラブルシューティング 216
システム ヘルスの監視 221
ヘルスモニタの動作 221
使用可能なクラスタ ヘルスモニタ 223
システム ヘルス アラートの自動受信 224
デグレードしたシステム ヘルスへの対応 225
クラスタと管理ネットワーク スイッチの検出の設定 226
クラスタおよび管理ネットワーク スイッチの監視の確認 227
システムの健全性の監視用コマンド 228
ダッシュボードを使用した重要なシステム情報の表示 231
ダッシュボード アラームの通知 231
ダッシュボードの管理用コマンド 232
クラスタのパフォーマンスの監視 233
オブジェクト、インスタンス、カウンタとは 234
パフォーマンス プリセットによる収集データの定義 234
オブジェクトのパフォーマンス データの収集と表示 235
統計のフィルタリング 236

統計のソート 237
パフォーマンス プリセット設定のインポート（クラスタ管理者のみ） 238
高度な方法を使用したクラスタのパフォーマンスの監視 238
クラスタのパフォーマンスの監視用コマンド 241
環境情報の表示 244
システム パフォーマンスの管理 245
ストレージQoSを使用したワークロード パフォーマンスの管理 245
ストレージQoSの仕組み 246
ワークロード パフォーマンスの制御と監視 250
例：ワークロードの分離 252
例：非クリティカルなワークロードに制限をプロアクティブに設定する 253
例：共有ストレージ インフラのワークロードに制限をプロアクティブに設定する 254
ワークロードの制御および監視用コマンド 255
RAVEを使用したヒストグラムベースの予測 257
WAFLキャッシュ メモリの増加 258
Flash PoolアグリゲートとFlash Cacheの比較 258
WAFL外部キャッシュの有効化と無効化 259
標準ユーザ データ ブロックのキャッシング 260
優先度が低いユーザ データ ブロックのキャッシング 261
システム メタデータのみのキャッシング 261
ランダム ライト ワークロード ブロックのキャッシュの有効化と無効化 262
先読みデータのキャッシュの有効化と無効化 262
WAFL外部キャッシュ設定の表示 262
WAFL外部キャッシュの利用率およびアクセスに関する情報の表示 263
モジュールのFlash Cacheファミリーでのキャッシュの保持 263
読み取りパフォーマンスの向上 266
読み取り再配置とは 266
読み取り再配置の管理用コマンド 267
書き込みパフォーマンスの向上 267
空きスペースの再配置による空きスペースの最適化方法 267
空きスペースの再配置を有効化する状況 268
他の再配置機能と合わせて空きスペースの再配置を使用する状況 268
空きスペースの再配置によって最適化が可能または不可能なアグリゲートのタイプ 269
空きスペース再配置の管理用コマンド 269
データ バックアップおよびリカバリのためのピア関係の管理 270
クラスタ ピア関係の管理 270
クラスタ ピアとは 270
クラスタ ピア関係の管理用コマンド 270
認証パスフレーズを使用したクラスタ ピアのセキュリティ 272
クラスタのピア関係での相互接続 272
クラスタ ピア関係の変更 291
クラスタ ピアリング関係の削除 292
SVMピア関係の管理 292

SVMピア関係とは 293
SVMピア関係の状態 294
SVMピア関係の作成 294
SVMピア関係の承認 297
SVMピア関係の拒否 298
SVMピア関係に対するピアリング アプリケーションの変更 299
SVMピア関係の削除 300
SVMピア関係の中断 301
SVMピア関係の再開 301
SVMピア関係に関する情報の表示 302
用語集 304
著作権に関する情報 312
商標に関する情報 313
マニュアルの更新について 314
索引 315

クラスタ管理者とSVM管理者の違い

クラスタ管理者は、クラスタ全体と、そのクラスタに含まれるStorage Virtual Machine（SVM、旧Vserver）を管理します。SVM管理者は、自身が担当するデータSVMだけを管理します。

クラスタ管理者は、クラスタ全体とクラスタのリソースを管理できます。また、データSVMをセットアップし、SVMの管理をSVM管理者に委譲することもできます。クラスタ管理者固有の権限は、それぞれのアクセス制御ロールによって異なります。デフォルトでは、「admin」アカウント名またはロール名を持つクラスタ管理者は、クラスタとSVMを管理するためのあらゆる権限を持っています。

SVM管理者は、ボリューム、プロトコル、LIF、サービスなど、自身が担当するSVMのストレージおよびネットワーク リソースだけを管理できます。SVM管理者固有の権限は、クラスタ管理者によって割り当てられた、それぞれのアクセス制御ロールによって異なります。

注: Data ONTAPのコマンドライン インターフェイス（CLI）では、コマンドやパラメータ名が`vserver`のまま変更されておらず、出力にもこれまでどおり*Vserver*と表示されます。

関連コンセプト

SVMの管理（クラスタ管理者のみ）（76ページ）
クラスタ管理者の事前定義されたロール（127ページ）
SVM管理者の事前定義されたロール（127ページ）

Data ONTAP管理インターフェイスの基本

クラスタは、Data ONTAP Command-Line Interface（CLI;コマンドライン インターフェイス）またはWebインターフェイスを使用して管理できます。CLIは、UNIXのtcshシェルに類似するコマンドベースのメカニズムを提供します。Webインターフェイスでは、Webブラウザを使用してクラスタを管理できます。

関連コンセプト

クラスタとは（31ページ）
CLIコマンド用のシェルの種類について（クラスタ管理者のみ）（17ページ）

CLIを使用したクラスタへのアクセス（クラスタ管理者のみ）

クラスタには、シリアル コンソール、SSH、Telnet、またはRSHを使用してアクセスできます。これらのプロトコルを使用することで、クラスタにアクセスしてCLIコマンドを実行できます。

シリアル ポートによるクラスタへのアクセス

クラスタには、ノードのシリアル ポートに接続されているコンソールから直接アクセスできます。

手順

1. コンソールでEnterキーを押します。

   ログイン プロンプトが表示されます。

2. ログイン プロンプトで次のいずれかを実行します。

クラスタにアクセスするアカウント	入力するアカウント名
デフォルトのクラスタ アカウント	**admin**
別の管理ユーザ アカウント	*username*

   パスワード プロンプトが表示されます。

3. adminまたは管理ユーザ アカウントのパスワードを入力し、Enterキーを押します。

SSHを使用したクラスタへのアクセス

クラスタにSSH要求を発行することで、管理タスクを実行できます。SSHはデフォルトでは有効になっています。

開始する前に

- アクセス方法として**ssh**を使用するように設定されたユーザ アカウントを持っている必要があります。
  `security login`コマンドの`-application`パラメータで、ユーザ アカウントのアクセス方法を指定します。詳細については、`security login`のマニュアル ページを参照してください。
- Active Directory（AD）のドメイン ユーザ アカウントを使用してクラスタにアクセスする場合は、CIFS対応のStorage Virtual Machine（SVM）でクラスタの認証トンネルが設定されている必要があり、さらにADのドメイン ユーザ アカウントがアクセス方法として**ssh**を、および認証方式として**domain**を用い、クラスタに追加されている必要があります。

- IPv6接続を使用する場合は、クラスタ上でIPv6が設定されて有効化され、さらにファイアウォール ポリシーにIPv6アドレスが設定されている必要があります。
  IPv6が有効になっているかどうかは、`network options ipv6 show`コマンドで表示できます。ファイアウォール ポリシーを表示するには、`system services firewall policy show`コマンドを使用します。

タスク概要

- Data ONTAPでは、OpenSSHクライアント バージョン5.4p1とOpenSSHサーバ バージョン5.4p1がサポートされています。
  サポートされているプロトコルはSSH v2だけです。SSH v1はサポートされていません。
- Data ONTAPでは、1つのノードについて同時に最大64のSSHセッションがサポートされています。
  クラスタ管理LIFがノード上に存在する場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。
  着信接続が1秒あたり10件を超えると、サービスは一時的に60秒間無効になります。
- Data ONTAPでは、SSHに対してAESおよび3DES暗号化アルゴリズム（*暗号*とも呼ばれる）のみがサポートされています。
  AESでは、128ビット、192ビット、256ビットのキーの長さがサポートされます。3DESのキーの長さはDES同様に56ビットですが、3回繰り返されます。
- Data ONTAP CLIにWindowsホストからアクセスする場合は、PuTTYなどのサードパーティのユーティリティを使用できます。
- Windows Active Directory（AD）ユーザ名を使用してData ONTAPにログインする場合、Data ONTAPでADユーザ名とドメイン名が作成されたときと同じように大文字と小文字を区別する必要があります。
  ADのユーザ名とドメイン名では、大文字と小文字は区別されませんが、Data ONTAPではユーザ名の大文字と小文字が区別されます。Data ONTAPで作成されたユーザ名と、ADで作成されたユーザ名の大文字小文字表記が違うと、ログインに失敗します。

手順

1. 管理ホストで、次のいずれかの形式で`ssh`コマンドを入力します。
   - **`ssh` *`username@hostname_or_IP`* `[`*`command`*`]`**
   - **`ssh -l` *`username hostname_or_IP`* `[`*`command`*`]`**

   ADのドメイン ユーザ アカウントを使用している場合は、*`username`*を*`domainname`*`\\`*`AD_accountname`*（ドメイン名のあとにバックスラッシュ2つ）または*`"domainname\AD_accountname"`*（二重引用符で囲み、ドメイン名のあとにバックスラッシュ1つ）の形式で指定する必要があります。

   *`hostname_or_IP`*は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4またはIPv6アドレスを使用できます。

   SSHインタラクティブ セッションの場合、*`command`*は必要ありません。

SSH要求の例

次の例は、「joe」という名前のユーザ アカウントでSSH要求を発行し、クラスタ管理LIFが10.72.137.28のクラスタにアクセスする方法を示しています。

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
```

```
node1                  true    true
node2                  true    true
2 entries were displayed.

cluster1::>
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

$
```

次の例は、「DOMAIN1」という名前のドメインの「john」という名前のユーザ アカウントでSSH要求を発行し、クラスタ管理LIFが10.72.137.28のクラスタにアクセスする方法を示しています。

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

cluster1::>
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

$
```

クラスタへのTelnetアクセスまたはRSHアクセスの有効化

TelnetとRSHは、事前定義されている管理ファイアウォール ポリシー（**mgmt**）では無効になっています。クラスタがTelnet要求またはRSH要求を受け入れることができるようにするには、TelnetまたはRSHを有効にした新しい管理ファイアウォール ポリシーを作成し、その新しいポリシーをクラスタ管理LIFに関連付ける必要があります。

タスク概要

Data ONTAPでは、事前定義されているファイアウォール ポリシーは変更できませんが、事前定義された**mgmt**管理ファイアウォール ポリシーをコピーし、コピーしたポリシーでTelnetまたはRSHを有効化することで新しいポリシーを作成できます。ただし、TelnetおよびRSHはセキュアなプロトコルではないため、SSHを使用してクラスタにアクセスすることを検討してください。SSHは、セキュリティ保護されたリモート シェルおよび双方向ネットワーク セッションを実現します。

手順

1. `system services firewall policy clone`コマンドを使用し、**`mgmt`**管理ファイアウォール ポリシーをベースにした新しい管理ファイアウォール ポリシーを作成します。
2. `system services firewall policy create`コマンドを使用し、作成した新しい管理ファイアウォール ポリシーでTelnetまたはRSHを有効にします。
3. `network interface modify`コマンドを使用して、新しいポリシーをクラスタ管理LIFに関連付けます。

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ：system services firewall policy clone - Clone an existing firewall policy

clustered Data ONTAP 8.3.1マニュアル ページ：system services firewall policy create - Create a firewall policy entry for a network service

clustered Data ONTAP 8.3.1マニュアル ページ：network interface modify - Modify a logical interface

Telnetを使用したクラスタへのアクセス

管理タスクを実行するために、クラスタに対してTelnet要求を発行できます。デフォルトでは、Telnetは無効です。

開始する前に

Telnetを使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- アクセス方法としてTelnetを使用するように設定されたクラスタ ローカル ユーザ アカウントを持っている必要があります。
  `security login`コマンドの`-application`パラメータで、ユーザ アカウントのアクセス方法を指定します。詳細については、`security login`のマニュアル ページを参照してください。
- Telnet要求がファイアウォールを通過できるように、クラスタ管理LIFまたはノード管理LIFによって使用される管理ファイアウォール ポリシーでTelnetが有効になっている必要があります。
  デフォルトではTelnetは無効になっています。`-service telnet`パラメータを指定して`system services firewall policy show`コマンドを実行すると、ファイアウォール ポリシーでTelnetが有効になっているかどうかが表示されます。詳細については、`system services firewall policy`のマニュアル ページを参照してください。
- IPv6接続を使用する場合は、クラスタ上でIPv6が設定されて有効化され、さらにファイアウォール ポリシーにIPv6アドレスが設定されている必要があります。
  IPv6が有効になっているかどうかは、`network options ipv6 show`コマンドで表示できます。ファイアウォール ポリシーを表示するには、`system services firewall policy show`コマンドを使用します。

タスク概要

- Telnetはセキュアなプロトコルではありません。
  クラスタにアクセスする場合は、SSHを使用することを検討してください。SSHは、セキュリティ保護されたリモート シェルおよび双方向ネットワーク セッションを実現します。
- Data ONTAPでは、1つのノードについて同時に最大50のTelnetセッションがサポートされています。
  クラスタ管理LIFがノード上に存在する場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。
  着信接続数が1秒あたりで10を超えると、サービスは一時的に60秒間無効になります。

- Data ONTAP CLIにWindowsホストからアクセスする場合は、PuTTYなどのサードパーティのユーティリティを使用できます。

手順

1. 管理ホストで次のコマンドを入力します。

   telnet
   hostname_or_IP

   *hostname_or_IP*は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4またはIPv6アドレスを使用できます。

Telnet要求の例

次の例は、Telnetアクセスを使用するように設定された「joe」というユーザが、クラスタ管理LIFが10.72.137.28であるクラスタにアクセスするTelnet要求を発行する方法を示しています。

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

関連コンセプト

ユーザ アカウントへのアクセス方法（120ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

RSHを使用したクラスタへのアクセス

クラスタにRSH要求を発行することで、管理タスクを実行できます。RSHはセキュアなプロトコルではなく、デフォルトでは無効になっています。

開始する前に

RSHを使用してクラスタにアクセスするには、次の条件を満たしている必要があります。

- アクセス方法としてRSHを使用するように設定された、クラスタのローカル ユーザ アカウントを持っている必要があります。
  `security login`コマンドの`-application`パラメータで、ユーザ アカウントのアクセス方法を指定します。詳細については、`security login`のマニュアル ページを参照してください。
- RSH要求がファイアウォールを通過できるように、クラスタ管理LIFまたはノード管理LIFによって使用される管理ファイアウォール ポリシーでRSHが有効になっている必要があります。
  デフォルトでは、RSHは無効です。`-service rsh`パラメータを指定して`system services firewall policy show`コマンドを実行すると、ファイアウォール ポリシーでRSHが有効になっているかどうかが表示されます。詳細については、`system services firewall policy`のマニュアル ページを参照してください。
- IPv6接続を使用する場合は、クラスタ上でIPv6が設定されて有効化され、さらにファイアウォール ポリシーにIPv6アドレスが設定されている必要があります。

IPv6が有効になっているかどうかは、`network options ipv6 show`コマンドで表示できます。ファイアウォール ポリシーを表示するには、`system services firewall policy show`コマンドを使用します。

タスク概要

- RSHはセキュアなプロトコルではありません。
  クラスタにアクセスする場合は、SSHを使用することを検討してください。SSHは、セキュリティ保護されたリモート シェルおよび双方向ネットワーク セッションを実現します。
- Data ONTAPでは、1つのノードについて同時に最大50のRSHセッションがサポートされています。
  クラスタ管理LIFがノード上に存在する場合、クラスタ管理LIFはこの制限をノード管理LIFと共有します。
  着信接続数が1秒あたりで10を超えると、サービスは一時的に60秒間無効になります。

手順

1. 管理ホストから、次のコマンドを入力します。

   `rsh` *`hostname_or_IP`* `-l` *`username`*`:`*`password command`*

   *`hostname_or_IP`*は、クラスタ管理LIFまたはノード管理LIFのホスト名またはIPアドレスです。クラスタ管理LIFを使用することを推奨します。IPv4またはIPv6アドレスを使用できます。

   *`command`*は、RSHを介して実行するコマンドです。

RSH要求の例

次の例は、RSHアクセスを使用するように設定された「joe」というユーザが、`cluster show`コマンドを実行するRSH要求を発行する方法を示しています。

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

Data ONTAPコマンドライン インターフェイスの使用

Data ONTAP Command-Line Interface（CLI;コマンドライン インターフェイス）は、管理インターフェイスのコマンド ベースのビューを提供します。ストレージ システム プロンプトでコマンドを入力すると、コマンドの結果がテキストで表示されます。

CLIのコマンド プロンプトは *`cluster_name`*`::>`で表されます。

権限レベル（`set`コマンドの`-privilege`パラメータ）を**advanced**に設定すると、たとえば *`cluster_name`*`::*>`のように、プロンプトにアスタリスク（`*`）が含められます。

CLIコマンド用のシェルの種類について（クラスタ管理者のみ）

クラスタには、CLIコマンド用に*クラスタシェル*、*ノードシェル*、*システムシェル*の3種類のシェルがあります。各シェルの用途は異なり、それぞれに異なるコマンド セットがあります。

- クラスタシェルは、クラスタにログインすると自動的に開始されるネイティブ シェルです。
  クラスタシェルには、クラスタの設定と管理に必要なすべてのコマンドが含まれています。クラスタシェルのCLIヘルプ（クラスタシェルのプロンプトで「?」を入力するとトリガーされる）には、使用可能なクラスタシェル コマンドが表示されます。クラスタシェルの`man` *`command_name`*コマンドは、指定されたクラスタシェル コマンドのマニュアル ページを表示します。

- ノードシェルは、ノード レベルでのみ有効なコマンドのための特別なシェルです。
  ノードシェルには、`system node run`コマンドを使用してアクセスできます。
  ノードシェルのCLIヘルプ（ノードシェルのプロンプトで「?」または`help`と入力するとトリガーされる）には、使用可能なノードシェル コマンドが表示されます。ノードシェルの`man` *`command_name`*コマンドは、指定されたノードシェル コマンドのマニュアル ページを表示します。
  よく使用されるノードシェル コマンドとオプションの多くは、クラスタシェルにトンネリングまたはエイリアスされ、クラスタシェルから実行することもできます。

- システムシェルは、診断とトラブルシューティングの目的に限って使用する低レベルのシェルです。
  システムシェルおよび関連する「diag」アカウントは、下位レベルの診断用です。アクセスにはdiagnostic権限が必要で、テクニカル サポートがトラブルシューティング タスクを実行するために予約されています。

クラスタシェル内でのノードシェル コマンドおよびオプションへのアクセス

ノードシェルのコマンドとオプションには、ノードシェル（`system node run –node` *`nodename`*）を使用してアクセスできます。よく使用されるノードシェル コマンドとオプションの多くは、クラスタシェルにトンネリングまたはエイリアスされ、クラスタシェルから実行することもできます。

クラスタシェルでサポートされているノードシェル オプションには、`vserver options`クラスタシェル コマンドを使用してアクセスできます。これらのオプションを表示するには、次のいずれかを実行します。

- `vserver options -vserver` *`nodename_or_clustername`* `-option-name ?`を使用してクラスタシェルCLIを照会する

- `man vserver options`を使用してクラスタシェルCLIの`vserver options`のマニュアル ページにアクセスする

クラスタシェルでノードシェルまたはレガシーのコマンドまたはオプションを入力した場合、そのコマンドまたはオプションに相当するクラスタシェル コマンドがある場合には該当するクラスタシェル コマンドを使用するように通知されます。

クラスタシェルでノードシェルまたはレガシーのコマンドまたはオプションを入力した場合、そのコマンドまたはオプションについて「not supported」というステータスが通知されます。

関連タスク

利用可能なノードシェル コマンドの表示（18ページ）

利用可能なノードシェル コマンドの表示

ノードシェルからCLIヘルプを使用すると、利用可能なノードシェル コマンドのリストを取得できます。

手順

1. ノードシェルにアクセスするには、クラスタシェルのシステム プロンプトで次のコマンドを入力します。

   `system node run -node {`*`nodename`*`|local}`

   `local`は、クラスタにアクセスするために使用するノードです。

   注: `system node run`コマンドには、`run`というエイリアス コマンドがあります。

2. 利用可能なノードシェル コマンドのリストを表示するには、ノードシェルで次のコマンドを入力します。

   `[`*`commandname`*`] help`

   *`commandname`*は、そのリストを表示する対象のコマンドの名前です。*`commandname`*を含めない場合は、CLIは利用可能なすべてのノードシェル コマンドを表示します。

   クラスタシェルCLIに戻るには、「`exit`」と入力するかCtrl+Dを使用します。

利用可能なノードシェル コマンドを表示する例

次の例では、node2という名前のノードのノードシェルにアクセスし、ノードシェル コマンド`environment`に関する情報を表示しています。

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-
battery-3]]
```

関連コンセプト

クラスタシェル内でのノードシェル コマンドおよびオプションへのアクセス（17ページ）

CLIコマンド ディレクトリの移動方法

CLIのコマンドをコマンド ディレクトリ別の階層に整理できます。完全なコマンド パスを入力するか、ディレクトリ構造を移動することによって、階層内のコマンドを実行できます。

CLIを使用するときは、プロンプトにディレクトリの名前を入力し、Enter キーを押すと、コマンド ディレクトリに直接アクセスできます。この場合は、ディレクトリ名がプロンプト テキストに表示され、適切なコマンド ディレクトリとやり取りしていることが示されます。コマンド階層のより下層に移動するには、コマンド サブディレクトリの名前を入力し、Enterキーを押します。これにより、サブディレクトリ名がプロンプト テキストに表示され、コンテキストがそのサブディレクトリに移動します。

コマンド全体を入力すると、複数のコマンド ディレクトリを移動できます。たとえば、ディスク デバイスについての情報を表示するには、プロンプトで`storage disk show`コマンドを入力します。ま

た、次の例に示すように、一度に1つのコマンド ディレクトリを移動して、コマンドを実行することもできます。

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

コマンドに最小文字数を入力してコマンドをカレント ディレクトリに対して一意にすると、コマンドを省略できます。たとえば、前述の例のコマンドを省略するには、`st d sh`と入力します。また、Tabキーを使用して省略したコマンドを展開し、デフォルトのパラメータ値を含め、そのコマンドのパラメータを表示することもできます。

コマンド階層の最上部に移動するには、`top`を使用します。`up`コマンドまたは`..` コマンドを使用すると、コマンド階層の1つ上のレベルに移動します。

注: CLIでアスタリスク(`*`)を付けたコマンドまたはコマンド オプションは、advanced権限以上のレベルでのみ実行できます。

CLIで値を指定する際のルール

ほとんどのコマンドには、1つ以上の必須またはオプションのパラメータがあります。多くのパラメータは、値を指定する必要があります。CLIで値を指定する際には、いくつかのルールがあります。

- 値は数値、ブール指定子、事前に定義された値リストから選択した値、またはテキスト文字列です。
  一部のパラメータでは、2つ以上の値をカンマで区切って指定できます。値のカンマ区切りのリストは引用符(`" "`)で囲む必要はありません。テキスト、スペース、またはクエリ文字(クエリを意図していない場合、または小なり記号または大なり記号で始まるテキスト)を指定する場合は、必ず値全体を引用符で囲む必要があります。
- CLIは、疑問符(「?」)をコマンドとして解釈し、特定のコマンドのヘルプ情報を表示します。
- コマンド名、パラメータ、特定の値などのCLIに入力するテキストの一部では、大文字と小文字が区別されません。
  たとえば、`vserver cifs`コマンドのパラメータ値を入力した場合、大文字と小文字の使い分けは無視されます。ただし、ノード、Storage Virtual Machine(SVM)、アグリゲート、ボリューム、論理インターフェイスの名前などのほとんどのパラメータ値は大文字と小文字が区別されます。
- 文字列またはリストをとるパラメータの値をクリアする場合は、空の一組の引用符(`""`)またはダッシュ(`"-"`)を指定します。
- ハッシュ記号(「#」)はシャープ記号とも呼ばれ、コマンドライン入力のコメントを表します。使用する場合は、コマンドラインの最後のパラメータのあとに配置する必要があります。
  CLIでは、「#」から行末までのテキストは無視されます。

次の例では、テキスト コメント付きでSVMが作成されます。次に、SVMが変更されてコメントが削除されます。

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is-repository
false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

次の例では、「#」に続くコメントでコマンドの内容を説明しています。

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-admin
-application ssh -authmethod password #This command creates a new user account
```

コマンド履歴の表示方法とコマンドの再発行方法

各CLIセッションで発行されたすべてのコマンドの履歴は、それぞれのセッションで保管されます。現在のセッションのコマンド履歴を表示できます。また、コマンドの再発行もできます。

コマンド履歴を表示するには、`history`コマンドを使用します。

コマンドを再発行するには、次の引数のいずれかを使用して`redo`コマンドを実行します。

- 前回のコマンドの一部と一致する文字列
  たとえば、実行した唯一の`volume`コマンドが`volume show`の場合、そのコマンドを再実行するには`redo volume`コマンドを使用します。
- `history`コマンドによって一覧表示された前回のコマンドの数値ID
  たとえば、履歴リストの4番目のコマンドを再発行するには、**`redo 4`**コマンドを使用します。
- 履歴リストの末尾からの負のオフセット
  たとえば、2つ前に実行したコマンドを再発行するには、**`redo -2`**コマンドを実行します。

たとえば、コマンド履歴の末尾から3番目のコマンドを再実行するには、次のコマンドを入力します。

```
cluster1::> redo -3
```

CLIコマンドを編集するためのキーボード ショートカット

コマンド プロンプトに表示されているコマンドが、アクティブなコマンドです。キーボード ショートカットを使用して、アクティブなコマンドを簡単に編集できます。UNIXのtcshシェルやEmacsエディタのショートカットに類似したショートカットを使用できます。

次の表に、CLIコマンドを編集するためのキーボード ショートカットを記載します。「Ctrl-」とある場合、Ctrlキーを押しながらそのあとの文字を入力します。「Esc-」とある場合、Escキーを押して離してから、そのあとの文字を入力します。

目的	キーボード ショートカット
カーソルを1文字左に移動する	Ctrl-B
	左矢印
カーソルを1文字右に移動する	Ctrl-F
	右矢印
カーソルを1単語分左に移動する	Esc-B
カーソルを1単語分右に移動する	Esc-F
カーソルを行頭へ移動する	Ctrl-A
カーソルを行末へ移動する	Ctrl-E
行頭からカーソルまでの入力内容を切り取ってバッファに保存する この切り取りバッファは、一部のプログラムの*クリップボード*と同様に一時メモリのように機能します。	Ctrl-U
カーソルから行末までの入力内容を切り取ってバッファに保存する	Ctrl-K
カーソルから次の単語の末尾までを切り取ってバッファに保存する	Esc-D
カーソルの左側の単語を切り取ってバッファに保存する	Ctrl-W
切り取りバッファの内容をカーソル位置に挿入する	Ctrl-Y

目的	キーボード ショートカット
カーソルの左側の文字を削除する	Ctrl-H
	Backspace
カーソル位置の文字を削除する	Ctrl-D
行をクリアする	Ctrl-C
画面をクリアする	Ctrl-L
コマンドライン上の現在の内容を、履歴リストの前のエントリに置き換える このキーボード ショートカットを押すたびに履歴カーソルが1つ前のエントリに移動します。	Ctrl-P
	Esc-P
	上矢印
コマンドライン上の現在の内容を、履歴リストの次のエントリに置き換える このキーボード ショートカットを押すたびに履歴カーソルが1つ先のエントリに移動します。	Ctrl-N
	Esc-N
	下矢印
カーソルの編集位置から、途中まで入力したコマンドを補完する、または有効な入力のリストを表示する	Tab
	Ctrl-I
状況に応じたヘルプの表示	?
疑問符（「?」）のマッピングをエスケープする たとえば、コマンドの引数に疑問符を入力するには、Escキーを押してから「?」を押します。	Esc-?
TTY出力を開始する	Ctrl-Q
TTY出力を停止する	Ctrl-S

管理権限レベルの使用

Data ONTAPのコマンドとパラメータは、*admin*、*advanced*、*diagnostic*の3つの権限レベルで定義されます。権限レベルは、タスクの実行に必要なスキルレベルに対応しています。

admin

このレベルではほとんどのコマンドとパラメータを使用できます。このレベルのコマンドとパラメータは、一般的なタスクまたはルーチン タスクで使用します。

advanced

このレベルのコマンドとパラメータは高度な知識を必要とし、あまり使用することはありません。適切に使用しないと、問題の原因になる可能性があります。

高度なコマンドまたはパラメータを使用する場合は、必ずサポート担当者のアドバイスを受けてください。

diagnostic

診断コマンドおよびパラメータは、システム停止の原因になる可能性があります。サポート担当者が問題の診断と修正を行う場合にのみ使用します。

CLIでの権限レベルの設定

CLIで権限レベルを設定するには、setコマンドを使用します。権限レベルの設定の変更は、現在のセッションにのみ適用されます。これらは、セッションをまたいで持続することはありません。

手順

1. CLIで権限レベルを設定するには、setコマンドと-privilegeパラメータを使用します。

権限レベルの設定の例

次の例では、権限レベルをadvancedに設定してから、adminに設定します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
them only when directed to do so by technical support.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

関連参照情報

管理権限レベルの使用（21ページ）

CLIでの表示環境設定

CLIセッションの表示環境を設定するには、setコマンドおよびrowsコマンドを使用します。設定する環境設定は、実行中のセッションのみに適用されます。これらは、セッションをまたいで持続することはありません。

タスク概要

次のCLI表示環境を設定できます。

- コマンド セッションの権限レベル
- システムを停止させる可能性のあるコマンドについては確認を発行するかどうか
- コマンドshowですべてのフィールドを表示するかどうか
- フィールド区切り文字として使用する文字
- データ サイズを報告する際のデフォルトの単位
- 現在のCLIセッションで画面に表示する行数 - この行数を超えると出力は一時停止する
  行数を指定しない場合、端末の実際の高さに基づいて自動的に調整されます。実際の高さが定義されていない場合、デフォルトで24行になります。
- デフォルトのStorage Virtual Machine（SVM）またはノード
- エラーが発生した場合に続行中のコマンドを停止するかどうか

手順

1. CLI表示環境を設定するには、setコマンドを使用します。

   現在のCLIセッションで画面に表示する行数を設定するには、rowsコマンドも使用できます。

   詳細については、setコマンドおよびrowsコマンドのマニュアル ページを参照してください。

CLIでの表示環境設定の例

次の例は、フィールド区切り文字としてカンマを設定し、**GB**をデフォルトのデータ サイズ単位として設定し、現在のCLI セッションで画面に表示する行数を50に設定します。

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

クエリ演算子の使用方法

管理インターフェイスでは、クエリとUNIX形式のパターンおよびワイルドカードがサポートされており、コマンド パラメータ引数の複数の値を照合できます。

次の表に、サポートされているクエリ演算子を示します。

演算子	説明
*	すべてのエントリに一致するワイルドカード。 たとえば、`volume show -volume *tmp*`というコマンドを実行すると、名前に文字列`tmp`が含まれるすべてのボリュームのリストが表示されます。
!	NOT演算子。 一致させない値を示します。たとえば、**`!vs0`**は値`vs0`に一致しないことを示します。
|	OR演算子。 比較する2つの値を区切ります。たとえば、**`vs0 | vs2`**はvs0またはvs2のいずれかに一致します。複数のOR文を指定できます。たとえば、**`a | b* | *c*`**はエントリa、またはbで始まるエントリ、またはcを含むエントリに一致します。
..	範囲演算子。 たとえば、**`5..10`**は値5から10までの値に一致します。
<	less-than演算子。 たとえば、**`<20`**は20よりも小さい値に一致します。
>	greater-than演算子。 たとえば、**`>5`**は5よりも大きい値に一致します。
<=	less-than-or-equal-to演算子。 たとえば、**`<=5`**は5以下の値に一致します。
>=	greater-than-or-equal-to演算子。 たとえば、**`>=5`**は5以上の値に一致します。
{*query*}	拡張クエリ。 拡張クエリは、コマンド名のあとで、別のパラメータの前の最初の引数として指定する必要があります。 たとえば、`volume modify {-volume *tmp*} -state offline`というコマンドを実行すると、名前に文字列`tmp`が含まれるすべてのボリュームがオフラインに設定されます。

クエリ文字をリテラルとして解析する場合、正しい結果が返されるようにするには、二重引用符（""）で文字列を囲む必要があります（「^」、「.」、「*」、「$」などの文字）。

1つのコマンドラインに複数のクエリ演算子を使用できます。たとえば、`volume show -size >1GB -percent-used <50 -vserver !vs1`というコマンドを実行すると、サイズが1GBより大きく、利用率が50%未満で、「vs1」という名前のStorage Virtual Machine（SVM）上にないすべてのボリュームが表示されます。

拡張クエリの使用方法

拡張クエリを使用して、指定した値を持つオブジェクトに対して操作を照合し、実行することができます。

拡張クエリは、中括弧（{}）でそのクエリを囲んで指定します。拡張クエリは、コマンド名のあとで、別のパラメータの前の最初の引数として指定する必要があります。たとえば、文字列`tmp`を含む名前のすべてのボリュームをオフラインに設定するには、次の例のコマンドを実行します。

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

一般に、拡張クエリは`modify`コマンドと`delete`コマンドでのみ役立ちます。`create`コマンドまたは`show`コマンドでは意味がありません。

クエリと変更操作の組み合わせはツールとして便利です。ただし、混乱を招く可能性があり、正しく実装しないとエラーとなります。たとえば、`system node image modify`コマンドを使用してノードのデフォルト ソフトウェア イメージを自動的に設定すると、他のソフトウェア イメージがデフォルトとならないように設定されます。 次の例のコマンドは、実質的には無効な操作です。

```
cluster1::> system node image modify {-isdefault true} -isdefault false
```

このコマンドは、現在のデフォルトのイメージをデフォルト以外のイメージとして設定してから、新しいデフォルトのイメージ（以前のデフォルト以外のイメージ）をデフォルト以外のイメージに設定します。その結果、元のデフォルトの設定が保持されます。正しく操作を実行するには、次の例のコマンドを使用します。

```
cluster1::> system node image modify {-iscurrent false} -isdefault true
```

フィールドを使用したshowコマンド出力のカスタマイズ方法

`-instance`パラメータを`show`コマンドに指定して詳細を表示すると、その出力が長くなり、不要な情報が含まれる可能性があります。`show`コマンドの`-fields`パラメータを使用すると、指定した情報のみを表示できます。

たとえば、`volume show -instance`を実行すると、複数の画面に情報が表示される可能性があります。（常に表示されるデフォルトのフィールド以外に）指定したフィールドのみが含まれるように出力をカスタマイズするには、`volume show -fields` *`fieldname[,fieldname...]`*を使用します。`-fields ?`を使用すると、`show`コマンドの有効なフィールドを表示できます。

次の例に、`-instance`パラメータと`-fields`パラメータの出力の違いを示します。

```
cluster1::> volume show -instance

                                    Vserver Name: cluster1-1
                                     Volume Name: vol0
                                  Aggregate Name: aggr0
                                     Volume Size: 348.3GB
                            Volume Data Set ID: -
                     Volume Master Data Set ID: -
                                   Volume State: online
                                    Volume Type: RW
                                   Volume Style: flex
                                            ...
                         Space Guarantee Style: volume
                     Space Guarantee in Effect: true
                                            ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>
```

```
cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- -----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

位置指定パラメータの概要

Data ONTAP CLIの位置指定パラメータ機能を活用して、効率的にコマンドを入力することができます。あるコマンドの位置指定パラメータは、そのコマンドのヘルプで特定できます。

位置指定パラメータとは

- 位置指定パラメータは、値を指定する前にパラメータ名を指定する必要のないパラメータです。
- コマンド入力には、位置指定パラメータとそれ以外のパラメータを組み合わせて指定できます。ただし、コマンド内の他の位置指定パラメータとの相対的な順序が、***command_name ?***の出力に従っている場合に かぎります。
- 位置指定パラメータは、必須パラメータの場合とオプション パラメータの場合があります。
- あるパラメータが1つのコマンドでは位置指定パラメータで、別のコマンドでは位置指定パラメータでない場合もあります。

注意: 位置指定パラメータ機能をスクリプトで使用することは、特に位置指定パラメータがオプション パラメータである場合や、位置指定パラメータの前にオプション パラメータを指定する場合には推奨されません。

位置指定パラメータを特定する方法

位置指定パラメータは、***command_name ?*** コマンドの出力で特定できます。位置指定パラメータは、次のどちらかの形式で、パラメータ名が角かっこで囲まれています。

- [*-parameter_name*] *parameter_value*は、必須の位置指定パラメータです。
- [[*-parameter_name*] *parameter_value*]は、オプションの位置指定パラメータです。

たとえば、次の***command_name ?*** の出力では、パラメータは該当するコマンドの位置指定パラメータです。

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

しかし次の出力では、パラメータは該当するコマンドの位置指定パラメータではありません。

- `-lif <lif-name>`
- `[-lif <lif-name>]`

位置指定パラメータの使用例

次の例に示す**volume create ?** の出力から、このコマンドの3つのパラメータ(`-volume`、`-aggregate`、`-size`)が位置指定パラメータであることがわかります。

```
cluster1::> volume create ?
   -vserver <vserver name>                                Vserver Name
   [-volume] <volume name>                                Volume Name
   [-aggregate] <aggregate name>                          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]                   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                                    Volume Type (default: RW)
  [ -policy <text> ]                                      Export Policy
  [ -user <user name> ]                                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]                   Space Guarantee Style (default: volume)
  [ -percent-snapshot-space <percent> ]                   Space Reserved for Snapshot Copies
  ...
```

次の例では、位置指定パラメータ機能を使用せずにvolume createコマンドを指定しています。

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

次の例では、位置指定パラメータ機能を使用して効率的にコマンドを入力しています。位置指定パラメータとそれ以外のパラメータの両方を使用してvolume createコマンドを入力し、位置指定パラメータの値はパラメータ名なしで指定されています。位置指定パラメータは、**volume create ?**の出力に示された順序で指定されており、-volumeの値は-aggregateの値の前に指定され、そのあとに-sizeの値が続いています。

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0

cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1 -nvfail off 1g
-space-guarantee none
```

Data ONTAPマニュアル ページへのアクセス方法

Data ONTAPマニュアル（man）ページでは、Data ONTAPコマンドの使用方法が説明されています。これらのマニュアル ページはコマンドライン、およびネットアップ サポート サイトで参照できます。

man *command_name*コマンドは、指定されたコマンドのマニュアル ページを表示します。コマンド名を指定しなかった場合は、マニュアル ページのインデックスが表示されます。man manコマンドを使用すると、manコマンド自体についての情報を表示できます。マニュアル ページを終了するには、「**q**」を入力します。

*『Clustered Data ONTAP Commands: Manual Page Reference』*には、管理者レベルおよび拡張レベルのData ONTAPコマンドのマニュアル ページがまとめられています。このリファレンスは、ネットアップ サポート サイトで参照できます。

関連情報

ネットアップ サポート サイト：mysupport.netapp.com

CLIセッションの管理（クラスタ管理者のみ）

CLIセッションにログを作成して指定したアップロード先にアップロードし、レコードとして保管できます。さらに、CLIセッションの自動タイムアウト時間を指定し、タイムアウト値で指定した分数が経過したあとにセッションを自動的に切断することもできます。

CLIセッションのレコードの管理

指定した名前とサイズの上限を使用してCLIセッションをファイルに記録し、そのファイルをFTPまたはHTTPのアップロード先にアップロードできます。また、以前に記録したCLIセッションのファイルを表示または削除することもできます。

CLI セッションのレコードを停止する、CLIセッションを終了する、あるいはファイルが指定されたサイズの上限に到達したときにCLIセッションの記録が終了します。デフォルトのファイル サイズの上限は1MBです。最大ファイル サイズの上限は2GBです。

CLIセッションを記録しておくと、たとえば、問題をトラブルシューティングして詳細情報を保存したり、特定の時点でのスペース使用量の永続レコードを作成する場合に便利です。

CLIセッションの記録

CLIセッションを記録するには、`system script start`コマンドと`system script stop`コマンドを使用します。

手順

1. 現在のCLIセッションのファイルへの記録を開始するには、`system script start`コマンドを使用します。

   `system script start`コマンドの使用の詳細については、マニュアル ページを参照してください。

   Data ONTAPは指定したファイルへのCLIセッションの記録を開始します。

2. CLIセッションを続行します。

3. セッションの記録を停止するには、`system script stop`コマンドを使用します。

   `system script stop`コマンドの使用の詳細については、マニュアル ページを参照してください。

   Data ONTAPはCLIセッションの記録を停止します。

CLIセッションのレコードの管理用コマンド

CLIセッションのレコードを管理するには、`system script`コマンドを使用します。

状況	使用するコマンド
指定したファイルで現在のCLIセッションの記録を開始する	*system script start*
現在のCLIセッションの記録を停止する	*system script stop*
CLIセッションのレコードに関する情報を表示する	*system script show*
CLIセッションのレコードをFTPまたはHTTPのデスティネーションにアップロードする	*system script upload*
CLIセッションのレコードを削除する	*system script delete*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

CLIセッションの自動タイムアウト時間の管理

タイムアウト値は、自動的にCLIセッションが終了するまでアイドル状態を維持できる時間を指定します。CLIタイムアウト値は、クラスタ全体が対象です。つまり、クラスタ内のどのノードも同じCLIタイムアウト値を使用します。

デフォルトでは、CLIセッションの自動タイムアウト時間は30分です。

CLIセッションのタイムアウト値を管理するには、`system timeout`コマンドを使用します。

CLIセッションの自動タイムアウト時間の管理用コマンド

CLIセッションの自動タイムアウト時間を管理するには、`system timeout`コマンドを使用します。

状況	使用するコマンド
CLIセッションの自動タイムアウト時間を表示する	*`system timeout show`*
CLIセッションの自動タイムアウト時間を変更する	*`system timeout modify`*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

OnCommand System Managerのブラウザベースのグラフィカル インターフェイスを使用したクラスタへのアクセス

コマンドライン インターフェイス（CLI）ではなくグラフィカル インターフェイスを使用してクラスタにアクセスして管理するには、OnCommand System Managerを使用します。OnCommand System ManagerはData ONTAPに搭載されているWebサービスでデフォルトで有効になっており、ブラウザを使用してアクセスできます。

開始する前に

`admin`ロール、および**`http`**、**`ontapi`**、**`console`**の各アプリケーション タイプが設定されたクラスタ ユーザ アカウントが必要です。

手順

1. Webブラウザで、クラスタ管理LIFを次のいずれかの形式で指定してアクセスします。
   - **`https://`*`cluster-mgmt-LIF`***（IPv4を使用している場合）
   - **`https://[`*`cluster-mgmt-LIF`*`]`**（IPv6を使用している場合）

   *`cluster-mgmt-LIF`*には、クラスタ管理LIFのIPアドレスを指定します。

   OnCommand System Managerのブラウザ アクセスでサポートされるのはHTTPSのみです。

   自己署名のデジタル証明書がクラスタで使用されている場合、信頼されていない証明書であることを伝える警告がブラウザ画面に表示されることがあります。危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をクラスタにインストールしてサーバを認証します。
2. クラスタ管理者のクレデンシャルを使用してOnCommand System Managerにログインします。

関連コンセプト

Webサービスへのアクセスの管理(154ページ)

関連タスク

Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、およびMIBファイルへのアクセス(42ページ)
クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール(141ページ)

OnCommand System Managerの概要

System Managerは、グラフィカルな管理インターフェイスで、ストレージ システムおよびストレージ オブジェクト(ディスク、ボリューム、アグリゲートなど)の管理やストレージ システムに関連する一般的な管理作業をWebブラウザから実行できます。クラスタ管理者は、クラスタとそのリソースをSystem Managerですべて管理できます。

重要: System Managerは実行ファイルとしては提供されなくなりました。WebサービスとしてData ONTAPに搭載されており、デフォルトで有効になっていて、ブラウザからアクセスできます。

System Managerでは、次のような多くの一般的な作業を実行できます。

- ディスク、アグリゲート、ボリューム、qtree、およびクォータなどのストレージ オブジェクトを構成し、管理する
- CIFSおよびNFSなどのプロトコルを設定し、ファイル共有をプロビジョニングする
- FC、FCoE、iSCSIなどのプロトコルをブロック アクセス用に設定する
- サブネット、ブロードキャスト ドメイン、データ / 管理インターフェイス、インターフェイス グループなどのネットワーク コンポーネントを作成および設定する
- ミラーリング関係とバックアップ関係をセットアップおよび管理する
- クラスタ管理、ストレージ ノード管理、およびStorage Virtual Machine(SVM、旧Vserver)管理の操作を実行する
- SVMの作成と設定、SVMに関連付けられたストレージ オブジェクトの管理、およびSVMサービスの管理を行う
- クラスタでHA構成を監視および管理する
- サービス プロセッサを設定して、ノードに対してその状態に関係なくログイン、管理、および監視を実行する

System Managerの詳細については、ネットアップ サポート サイトを参照してください。

関連情報

ネットアップ サポート サイト:mysupport.netapp.com

OnCommand System Managerへのアクセス管理方法

WebブラウザからOnCommand System Managerへのアクセスを有効または無効にすることができます。System Managerのログを表示することもできます。

WebブラウザからSystem Managerへのアクセスは、`vserver services web modify -name` **`sysmgr`** `-vserver` *`cluster_name`* `-enabled` [**`true`**|**`false`**]を使用して制御できます。

System Managerのログは、System Managerがアクセスされたときにクラスタ管理LIFをホストしているノードの`/mroot/etc/log/mlog/sysmgr.log`ファイルに記録されます。このログ ファイルは、

ブラウザを使用して表示できます。System Managerのログは、AutoSupportメッセージにも使用されます。

クラスタ管理の基礎（クラスタ管理者のみ）

クラスタ管理者は、System Setupを使用して新しいクラスタを設定できます。クラスタが作成されると、クラスタ管理者は、クラスタのステータスと属性を表示したり、クラスタの名前を変更したり、クラスタ内の別のノードにイプシロンを割り当てたりすることができます。

関連情報

ネットアップのマニュアル：System Setup（最新リリース）

クラスタとは

クラスタは、グループにまとめられた1つ以上のノードで構成され（HAペア）、拡張可能です。クラスタを作成すると、ノードでリソースをプールし、作業をクラスタに分散しながら、管理者に管理対象の1つのエンティティとして表示します。また、個々のノードがオフラインになった場合でも、エンドユーザに対する継続的なサービスが可能になります。

- 1つのクラスタ内の最大ノード数は、プラットフォーム モデルおよびライセンス プロトコルによって異なります。
- クラスタ内の各ノードでは、クラスタ内の他のノードと同じボリュームを表示および管理できます。
  ファイルシステム全体のネームスペースは、すべてのボリュームとそれらの結果のパスで構成され、クラスタ全体にまたがります。
- クラスタ内のノードは、物理的に分離されたセキュアな専用イーサネット ネットワークを介して通信を行います。
  クラスタ内の各ノード上のクラスタのLogical Interface（LIF;論理インターフェイス）は、同じサブネット上にある必要があります。
- クラスタに新しいノードを追加したときに、新しいノードを指すようにクライアントを更新する必要はありません。
  新しいノードの追加は、クライアントに対して透過的です。
- 2ノード クラスタ（単一のHAペア）がある場合は、クラスタ ハイアベイラビリティ（HA）を構成する必要があります。
- スタンドアロン ノードにクラスタを作成できます（シングルノード クラスタと呼ばれます）。
  この構成ではクラスタ ネットワークは必要なく、クラスタ ポートを使用してデータ トラフィックを処理できます。ただし、シングルノード クラスタでは、ノンストップ オペレーションはサポートされていません。

関連コンセプト

クォーラムとイプシロンについて（33ページ）
クラスタ管理サーバとは（32ページ）
シングルノード クラスタに関する考慮事項（32ページ）

関連情報

NetApp Hardware Universe
clustered Data ONTAP 8.3 ハイアベイラビリティ構成ガイド
clustered Data ONTAP 8.3 ネットワーク管理ガイド

シングルノード クラスタに関する考慮事項

シングルノード クラスタは、スタンドアロン ノード上でクラスタを実行する特殊な実装です。ワークロードに必要なノードが1つだけで、ノンストップ オペレーションが不要な場合に導入できます。

たとえば、リモート オフィス用のデータ保護を提供するためにシングルノード クラスタを導入できます。この場合、シングルノード クラスタがSnapMirrorとSnapVaultを使用して、サイトのデータをプライマリ データセンターにレプリケートします。

シングルノード クラスタでは、HAモードを**non_HA**に設定します。これにより、ノード上で不揮発性メモリ（NVRAM）カードのNVRAMメモリがすべて、そのノードで使用されるようになります。さらに、シングルノード クラスタは、クラスタ ネットワークを使用しません。データLIFをホストできるデータ ポートとして、クラスタ ポートを使用できます。

通常、シングルノード クラスタはクラスタのセットアップ時に設定します。ただし、既存のクラスタからノードを削除してシングルノード クラスタを作成することもできます。

シングルノード クラスタでは、次の機能や処理はサポートされていません。

- ストレージ フェイルオーバーおよびクラスタHA
  シングルノード クラスタは、スタンドアロンHAモードで動作します。ノードがオフラインになると、クライアントは、そのクラスタに格納されているデータにアクセスできなくなります。
- 複数のノードを必要とする処理
  たとえば、ボリュームの移動やほとんどのコピー処理は実行できません。
- Infinite Volume
  Infinite Volumeには、少なくとも2つのアグリゲートを含める必要があります。
- クラスタへのクラスタ構成バックアップの格納
  デフォルトでは、構成バックアップ スケジュールによってクラスタ構成のバックアップが作成され、クラスタ全体の異なるノードに格納されます。クラスタをシングルノードで構成した場合、ノードにアクセスできなくなる障害が発生すると、クラスタ構成バックアップ ファイルをリモートURLに格納しておかないかぎり、クラスタをリカバリできません。

関連タスク

クラスタへのノードの追加（38ページ）
クラスタからのノードの削除（40ページ）

関連参照情報

構成バックアップ スケジュールの管理用コマンド（184ページ）

関連情報

ネットアップのマニュアル：System Setup（最新リリース）

クラスタ管理サーバとは

クラスタ管理サーバは*管理*SVMとも呼ばれる、クラスタを1つの管理可能なエンティティとして扱う特別なStorage Virtual Machine（SVM）です。クラスタ管理サーバは最上位の管理ドメインとして機能するとともに、データSVMに論理的に属さないリソースを所有します。

クラスタ管理サーバは、クラスタ上で常に使用可能です。クラスタ管理サーバには、コンソールまたはクラスタ管理LIFからアクセスできます。

ホーム ネットワーク ポートに障害が発生すると、クラスタ管理LIFがクラスタ内の別のノードに自動的にフェイルオーバーします。使用している管理プロトコルの接続特性に応じて、ユーザがフェイルオーバーを認識できる場合とできない場合があります。コネクションレス型プロトコル（SNMPなど）を使用している場合、または接続が限定されている場合（HTTPなど）には、フェイルオーバーを認識する可能性は低くなります。ただし、長期的な接続（SSHなど）を使用している場合は、フェイルオーバー後にクラスタ管理サーバに再接続する必要があります。

クラスタを作成した場合は、IPアドレス、ネットマスク、ゲートウェイ、ポートなど、クラスタ管理LIFのすべての特性を設定します。

データSVMやノードSVMとは異なり、クラスタ管理サーバにはルート ボリュームまたはホスト ユーザ ボリュームがありません（システム ボリュームをホストすることは可能）。さらに、クラスタ管理サーバで使用できるのはクラスタ管理タイプのLIFだけです。

`vserver show`コマンドを実行すると、コマンドの出力リストにクラスタ管理サーバが表示されます。

関連コンセプト

SVMの種類（78ページ）

クォーラムとイプシロンについて

クォーラムとイプシロンは、クラスタの健常性と機能を判断するための重要な基準で、通信および接続に関する潜在的な問題へのクラスタの対応を決定します。

*クォーラム*は、クラスタが完全に機能するための前提条件です。クラスタがクォーラムを構成している場合は、過半数のノードが正常で、相互に通信可能です。クォーラムが失われると、クラスタは通常のクラスタ処理を実行できなくなります。すべてのノードが1つのまとまりとしてデータの単一のビューを共有するため、任意の時点において1つのノードの集まりだけがクォーラムを構成することができます。つまり、通信が確立されていない2つのノードが異なる方法でデータを変更できる場合には、データを1つのデータ ビューに表示できなくなります。

クラスタ内の各ノードはノード マスターを選出する投票プロトコルに属しており、マスター以外の各ノードは *セカンダリ*となります。マスター ノードは、クラスタ内に情報を同期する役割を担います。形成されたクォーラムは継続的な投票によって維持されます。マスター ノードがオフラインになった場合、クラスタでクォーラムが維持されていれば、オンラインのノードの投票によって新しいマスターが選出されます。

ノード数が偶数のクラスタの場合は同票となる可能性があるため、*イプシロン*と呼ばれる追加の投票荷重が設定されたノードが1つあります。大規模なクラスタの同じ数のノード間で接続障害が発生した場合、すべてのノードが正常であることを条件に、イプシロンが設定されたノードのグループがクォーラムを維持します。たとえば、次の図では、4ノード クラスタの2つのノードで障害が発生しています。ただし、残りのノードの1つにイプシロンが設定されているため、正常なノードが過半数に満たなくてもクォーラムが維持されます。

クラスタが作成されると、自動的に最初のノードにイプシロンが割り当てられます。イプシロンを保持しているノードで障害が発生したり、ハイアベイラビリティ パートナーをテイクオーバーしたり、ハイアベイラビリティ パートナーにテイクオーバーされた場合、イプシロンは別のHAペアの正常なノードに自動的に割り当てられます。

ノードをオフラインにすると、クラスタがクォーラムを維持できるかどうかに影響することがあります。そのため、クラスタのクォーラムが失われたり、あと1つのノード障害によってクォーラムが失われるような処理を実行しようとすると、警告メッセージが表示されます。クォーラムに関する警告メッセージを無効にするには、advanced権限レベルで`cluster quorum-service options modify`コマンドを使用します。

一般的に、クラスタのノード間に信頼性のある接続が確立されている場合には、小規模のクラスタよりも大規模のクラスタの方が安定します。ノードの半数にイプシロンを加えた過半数のクォーラムの要件は、2ノードのクラスタよりも24ノードのクラスタの方が簡単に維持できます。

2ノードのクラスタでは、クォーラムの維持に独特な課題が存在します。2ノード クラスタでは*クラスタHA*が使用され、どちらのノードにもイプシロンは設定されません。代わりに、両方のノードが継続的にポーリングされ、1つのノードに障害が発生した場合には、もう一方のノードが、論理インターフェイスと管理機能へのアクセスに加えてデータへの完全な読み取り / 書き込みアクセスを提供します。

関連情報

clustered Data ONTAP 8.3 ハイアベイラビリティ構成ガイド

クラスタ レプリケーション リングとは

*レプリケーション リング*は、クラスタ内のすべてのノードで実行される一連の同一プロセスです。

クラスタリングの基礎になるのはレプリケートされたデータベース（RDB）です。クラスタ内の各ノードにはRDBのインスタンスが保持されています。クラスタ全体でデータの一貫性を確保するために、いくつかのプロセスでRDBが使用されています。該当するプロセスとしては、管理アプリケーション（**mgmt**）、ボリューム ロケーション データベース（**vldb**）、仮想インターフェイス マネージャ（**vifmgr**）、SAN管理デーモン（**bcomd**）、設定レプリケーション サービス（**crs**）などがあります。

たとえば、あるクラスタの**vldb**レプリケーション リングは、クラスタ内で実行中の**vldb**のすべてのインスタンスで構成されています。

RDBレプリケーションでは、クラスタ内のすべてのノード間のクラスタ リンクが正常であることが要求されます。クラスタ ネットワークの全体または一部に障害が発生すると、ファイル サービスを利用できなくなる場合があります。advanced権限レベルの`cluster ring show`コマンドを実行すると、レプリケーション リングのステータスが表示され、トラブルシューティングに役立ちます。

クラスタ内のノードに関する情報の表示

ノード名、ノードが正常に機能しているかどうか、ノードがクラスタへの参加条件を満たしているかどうかを表示できます。advanced権限レベルでは、ノードにイプシロンが設定されているかどうかも表示できます。

手順

1. クラスタ内のノードに関する情報を表示するには、`cluster show`コマンドを使用します。

   ノードにイプシロンが設定されているかどうかを表示するには、このコマンドをadvanced権限レベルで実行します。

クラスタ内のノードの表示例

次の例では、4ノード クラスタ内のすべてのノードに関する情報が表示されています。

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
```

```
node1                  true    true
node2                  true    true
node3                  true    true
node4                  true    true
```

次の例では、advanced権限レベルで、「node1」という名前のノードに関する情報が表示されています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when
directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

クラスタ属性を表示する

クラスタの一意の識別子（UUID）、名前、シリアル番号、場所、連絡先情報を表示できます。

手順

1. クラスタの属性を表示するには、`cluster identity show`コマンドを使用します。

クラスタ属性を表示する例

次の例では、クラスタの名前、シリアル番号、場所、連絡先情報が表示されています。

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

クラスタ属性の変更

クラスタ名、場所、および連絡先情報などのクラスタ属性を必要に応じて変更できます。

タスク概要

クラスタの作成時に設定されたクラスタのUUIDは変更できません。

手順

1. クラスタの属性を変更するには、`cluster identity modify`コマンドを使用します。

   `-name`パラメータにはクラスタの名前を指定します。`cluster identity modify`のマニュアルページに、クラスタ名の指定方法に関するルールが説明されています。

   `-location`パラメータにはクラスタの場所を指定します。

`-contact`パラメータには、名前やEメール アドレスなどの連絡先情報を指定します。

クラスタ名変更の例

次の例では、現在のクラスタ名（「cluster1」）を「cluster2」に変更します。

```
cluster1::> cluster identity modify -name cluster2
```

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ：cluster identity modify - Modify the cluster's attributes

クラスタ レプリケーション リングのステータス表示

クラスタ レプリケーション リングのステータスを表示して、クラスタ全体の問題の診断に役立てることができます。クラスタに問題がある場合は、トラブルシューティングに役立てるために、サポート担当者からこのタスクを実行するように依頼される場合があります。

手順

1. クラスタ レプリケーション リングのステータスを表示するには、advanced権限レベルで`cluster ring show`コマンドを使用します。

クラスタ リングレプリケーション ステータスの表示例

次の例では、node0という名前のノードのVLDBレプリケーション リングのステータスが表示されています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
them only when
         directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
           Node: node0
      Unit Name: vldb
         Status: master
          Epoch: 5
    Master Node: node0
     Local Node: node0
       DB Epoch: 5
DB Transaction: 56
 Number Online: 4
       RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

ノードの管理（クラスタ管理者のみ）

*ノード*とは、クラスタ内のコントローラのことです。ノードについての情報を表示したり、ノード属性を設定したり、ノード名を変更したり、ノードを追加または削除したり、ノードを起動または停止したりできます。Service Processor（SP;サービス プロセッサ）を使用して、ノードをリモートから管理することもできます。

ノードは、クラスタ ネットワークを介してクラスタ内の他のノードに接続されます。また、Data ONTAPシステムの物理ストレージを提供するディスク シェルフや、Data ONTAPで使用するアレイLUNを提供するストレージ アレイにも接続されます。クラスタではなくノードで制御されるサービスやコンポーネントは、`system node`コマンドを使用して管理できます。

ノードSVMは、クラスタ内のノードを表します。`vserver show`コマンドを実行すると、出力のリストにノードSVMが含まれます。

ノード属性の表示

クラスタ内の1つ以上のノードの属性（名前、所有者、場所、モデル番号、シリアル番号、ノードの稼働時間、ヘルス、クラスタへの参加資格など）を表示できます。

手順

1. クラスタ内の特定のノードまたはすべてのノードの属性を表示するには、`system node show`コマンドを使用します。

ノードに関する情報の表示例

次の例では、node1に関する詳細な情報が表示されています。

```
cluster1::> system node show -node node1
              Node: node1
             Owner: Eng IT
          Location: Lab 5
             Model: model_number
     Serial Number: 12345678
         Asset Tag: -
            Uptime: 23 days 04:42
   NVRAM System ID: 118051205
         System ID: 0118051205
         Vendor: NetApp
            Health: true
       Eligibility: true
```

ノード属性の変更

必要に応じて、ノードの属性を変更できます。変更できる属性は、ノードの所有者情報、場所情報、資産タグ、クラスタへの参加資格です。

タスク概要

ノードのクラスタへの参加資格は、advanced権限レベルで、`system node modify`コマンドまたは`cluster modify`コマンドに`-eligibility`パラメータ指定して変更します。このパラメータを**`false`**に設定すると、そのノードはクラスタ内で非アクティブになります。

注意: ノード設定をリストアする場合やノードのメンテナンスが長引いている場合などを除いて、**false**には設定しないでください。クラスタ参加資格を無効に設定すると、参加資格を再設定してリブートするまで、そのノードはSANデータを提供しなくなります。ノードにクラスタ参加資格がないと、そのノードへのNASデータ アクセスも影響を受ける可能性があります。

手順

1. `system node modify`コマンドを使用して、ノードの属性を変更します。

ノード属性の変更の例

次のコマンドを実行すると、「node1」というノードの属性が変更されます。このノードの所有者は「Joe Smith」に設定され、その資産タグは「js1234」に設定されています。

```
cluster1::> system node modify -node node1 -owner "Joe Smith"
-assettag js1234
```

ノード名の変更

ノード名は必要に応じて変更できます。

手順

1. ノード名を変更するには、`system node rename`コマンドを使用します。

   `-newname`パラメータに、ノードの新しい名前を指定します。`system node rename`のマニュアル ページに、ノード名の指定方法に関するルールが記載されています。

   クラスタ内の複数のノードの名前を変更する場合、各ノードに対してこのコマンドを実行する必要があります。

ノード名の変更例

次のコマンドでノード名を「node1」から「node1a」に変更します。

```
cluster1::> system node rename -node node1 -newname node1a
```

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ:system node rename - Rename a node

クラスタへのノードの追加

クラスタを作成したあと、ノードをクラスタに追加して、クラスタを拡張できます。一度に追加できるノードは1つだけです。

開始する前に

- 複数ノード クラスタにノードを追加する場合は、クラスタ内の既存ノードのうち半数を上回るノードが正常である必要があります(`cluster show`で確認可能)。
- 2ノードのスイッチレス クラスタにノードを追加する場合は、ノードの追加前に、クラスタ管理スイッチとインターコネクト スイッチをインストールして設定しておく必要があります。
  スイッチレス クラスタ機能は、2ノード クラスタでのみサポートされます。

クラスタHAは、クラスタのノードが3つ以上のときは不要であるため、3つ以上で構成する場合や3つ以上に増えた場合は自動的に無効になります。

- シングルノード クラスタに2つ目のノードを追加する場合は、その2つ目のノードがインストールされていて、クラスタ ネットワークが構成されている必要があります。
- クラスタでSPの自動設定が有効になっている場合、SP用に指定されたサブネットに、参加するノードで使用可能なソースが必要です。
  クラスタに参加するノードは、指定されたサブネットを使用して、SPの自動設定を実行します。
- 新しいノードのノード管理LIFについて、次の情報を収集しておく必要があります。
  - ポート
  - IPアドレス
  - ネットマスク
  - デフォルト ゲートウェイ

タスク概要

ノードは、HAペアを形成できるように偶数である必要があります。クラスタへのノードの追加を開始したら、その処理を完了する必要があります。先に追加したノードがクラスタに参加するまでは、別のノードの追加を開始することはできません。

手順

1. クラスタに追加するノードに電源を入れます。

   ノードがブートし、ノードのセットアップ ウィザードがコンソール上で起動されます。

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
     Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.



Enter the node management interface port [e0c]:
```

2. ノードのセットアップ ウィザードを終了します。

   exit

   ノードのセットアップ ウィザードが終了し、セットアップ タスクが完了していないという警告がログイン プロンプトに表示されます。

3. ユーザ名adminを使用してadminアカウントにログインします。

4. クラスタ セットアップ ウィザードを開始します。

   cluster setup

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
```

```
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.


Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

5. クラスタにノードを追加します。

   join

6. プロンプトに従ってノードをセットアップし、クラスタに追加します。
   - プロンプトでデフォルト値を受け入れるには、Enterキーを押します。
   - プロンプトで独自の値を入力するには、値を入力してEnterキーを押します。
7. 追加するノードごとに前述の手順を繰り返します。

終了後の操作

ノードをクラスタに追加したあと、HAペアごとにストレージ フェイルオーバーを有効にする必要があります。

関連コンセプト

SPネットワーク設定に関する考慮事項(52ページ)

関連情報

clustered Data ONTAP 8.3 ハイアベイラビリティ構成ガイド
Clustered Data ONTAP: Adding a second controller module to create an HA pair
Clustered Data ONTAP Switch Setup Guide for Cisco Switches

クラスタからのノードの削除

クラスタから不要なノードを削除できます。一度に削除できるノードは1つのみです。ノードを削除した場合は、フェイルオーバー パートナーも削除する必要があります。ノードを削除すると、そのノードのデータはアクセスできなくなるか、消去されます。

開始する前に

クラスタ内のノードのうち半数を上回るノードが正常である必要があります(`cluster show`で確認可能)。

削除するノード内のすべてのデータを退避しておく必要があります。

タスク概要

注意: クラスタからノードを削除する(`cluster unjoin`)と、ユーザは、そのノードに接続されたディスクのすべてのシステム データとユーザ データにアクセスできなくなります。クラスタからノードを削除したあとでそのノードを同じクラスタに戻す必要が生じた場合、データのリストア方法をテクニカル サポートに問い合わせる必要があります。

手順

1. クラスタでストレージ暗号化を有効にし、自己暗号化ディスク（SED）をFederal Information Processing Standard（FIPS）準拠モードで運用している場合は、ノードに接続されているディスクをノードの削除後に完全消去して転用できるように、FIPS準拠モードを無効にします。

   a. `storage encryption disk show`コマンドで`-fips`パラメータを指定して、現在FIPS準拠モードになっているSEDを表示します。

   b. advanced権限レベルの`storage encryption disk modify`コマンドで`-disk` *`disk_path_name`*パラメータと`-fips-key-id 0x0`パラメータを指定して、FIPS準拠モードを無効にします。

   c. `storage encryption disk show`コマンドで`-fips`パラメータを指定して、SEDをもう一度表示し、変更したSEDがFIPS準拠モードになっていないことを確認します。

2. 削除するノードが現在のマスター ノードである場合は、クラスタの別のノードでマスター ノードとして選出できるように、`system node reboot`コマンドを使用してノードをリブートします。

   マスター ノードとは、**`mgmt`**、**`vldb`**、**`vifmgr`**、**`bcomd`**、**`crs`**などのプロセスを保持しているノードです。advanced権限レベルの`cluster ring show`コマンドを使用すると、現在のマスター ノードが表示されます。

3. クラスタの別のノードからadvanced権限レベルの`cluster unjoin`コマンドを使用して、クラスタからノードを削除します。

   次の内容のメッセージが表示されます。

   - ノードのフェイルオーバー パートナーをクラスタから削除する必要があること。
   - ノード削除後で、クラスタに再追加する前に、ブート メニュー オプション**[(4) Clean configuration and initialize all disks]**を使用して、ノードの設定を消去し、すべてのディスクを初期化する必要があること。

   ノードを削除する前に対処が必要な条件がある場合は、エラー メッセージが表示されます。メッセージの内容は、たとえば、ノードに削除が必要な共有リソースがある、あるいはノードのクラスタHA構成またはストレージ フェイルオーバー構成を無効にする必要があるなどの場合があります。

   ノードがクォーラム マスターの場合、クラスタのクォーラムがいったん失われて、すぐに戻ります。クォーラムが失われるのは一時的であり、データの操作には影響しません。

4. エラー メッセージにエラー状態が示された場合は、その状態に対処し、`cluster unjoin`コマンドを再実行します。

   クラスタからノードが正常に削除されると、そのノードは自動的にリブートします。

5. ノードを転用する場合は、ノードがリブートしたあとに次の手順を実行します。

   a. ブート プロセス時に、プロンプトに応じてCtrl+Cキーを押してブート メニューを表示します。

   b. ブート メニュー オプションの**[(4) Clean configuration and initialize all disks]**を選択し、ノードの設定を消去してすべてのディスクを初期化します。

6. クラスタからフェイルオーバー パートナーを削除するには、前述の手順を繰り返します。

終了後の操作

シングルノード クラスタにするためにノードを削除した場合は、データ トラフィックを処理するようにクラスタ ポートを変更します。それには、クラスタ ポートがデータ ポートになるように変更し、そのデータ ポートにデータLIFを作成します。

関連タスク

システム プロンプトでのノードのリブート（46ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、およびMIBファイルへのアクセス

Service Processor Infrastructure（**spi**）Webサービスは、Webブラウザがクラスタのログ ファイル、コア ダンプ ファイル、およびMIBファイルにアクセスできるよう、デフォルトで有効になっています。ノードが停止した場合でも、パートナーにテイクオーバーされていれば、これらのファイルにアクセスできます。

開始する前に

- クラスタ管理LIFが起動している必要があります。
  クラスタまたはノードの管理LIFを使用して**spi** Webサービスにアクセスできます。ただし、クラスタ管理LIFを使用することを推奨します。
  `network interface show`コマンドを実行すると、クラスタ内のすべてのLIFのステータスが表示されます。
- ユーザ アカウントに「admin」ロール（**spi** Webサービスへのアクセスがデフォルトで付与されたロール）がない場合、アクセス制御ロールに**spi** Webサービスへのアクセスを許可する必要があります。
  `vserver services web access show`コマンドを実行すると、どのロールにどのWebサービスに対するアクセスが許可されているかが表示されます。
- 「admin」ユーザ アカウント（デフォルトで**http**アクセスが含まれる）を使用していない場合、**http**アクセス方式でユーザ アカウントをセットアップする必要があります。
  `security login show`コマンドを実行すると、ユーザ アカウントのアクセス方法、ログイン方法、およびアクセス制御ロールが表示されます。
- HTTPSを使用してセキュアなWebアクセスを確保するには、SSLを有効にしてデジタル証明書をインストールする必要があります。
  `system services web show`コマンドを実行すると、クラスタ レベルのWebプロトコル エンジンの設定が表示されます。

タスク概要

spi はデフォルトで有効になっていますが、手動で無効にすることができます（`vserver services web modify -vserver * -name spi -enabled false`）。

「admin」ロールには**spi** Webサービスへのアクセスがデフォルトで許可されますが、手動で無効にすることができます（`services web access delete -vserver cluster_name -name spi -role admin`）。

手順

1. 次のいずれかの**spi** WebサービスURLをWebブラウザに指定します。
   - `http://cluster-mgmt-LIF/spi/`
   - `https://cluster-mgmt-LIF/spi/`

   *cluster-mgmt-LIF*は、クラスタ管理LIFのIPアドレスです。

2. 入力画面が表示されたら、ユーザ アカウントとパスワードを入力します。

   アカウントが認証されると、クラスタの各ノードの`/mroot/etc/log/`ディレクトリ、`/mroot/etc/crash/`ディレクトリ、および`/mroot/etc/mib/`ディレクトリへのリンクがブラウザに表示されます。

関連コンセプト

Webプロトコル エンジンの管理（155ページ）
Webサービスの管理（156ページ）
Webサービスへのアクセスの管理（154ページ）
ユーザ アカウントへのアクセス方法（120ページ）
SSLの管理（158ページ）
管理アクティビティの監査設定の管理（162ページ）
コア ダンプの管理（クラスタ管理者のみ）（191ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

ノードのシステム コンソールへのアクセス

ブート メニューまたはブート環境のプロンプトでハングしているノードには、システム コンソール（*シリアル コンソール*とも呼ばれる）を介してのみアクセスできます ノードのシステム コンソールには、ノードのSPまたはクラスタへのSSH接続からアクセスできます。

タスク概要

SPとData ONTAPはどちらもシステム コンソールにアクセスするためのコマンドを提供しています。ただし、SPからはそのノードのシステム コンソールにしかアクセスできませんが、クラスタからはクラスタ内のすべてのノードのシステム コンソールにアクセスできます。

手順

1. 次のように、ノードのシステム コンソールにアクセスします。

使用する環境	入力するコマンド
ノードのSP CLI	`system console`
Data ONTAP CLI	`system node run-console`

2. プロンプトが表示されたら、システム コンソールにログインします。
3. システム コンソールを終了するには、Ctrl+Dを押します。

システム コンソールへのアクセスの例

次の例に、「SP node2」プロントで`system console`コマンドを入力した結果を示します。システム コンソールに、node2がブート環境のプロンプトでハングしていることが表示されます。コンソールで`boot_ontap`コマンドを入力してノードをData ONTAPでブートし、続いてCtrl+Dを押してコンソールを終了してSPに戻ります。

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
```

```
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
...
```

システム コンソールを終了するには、Ctrl+Dを押します。

```
Connection to 123.12.123.12 closed.
SP node2>
```

次の例に、node2（ブート環境プロンプトでハングしているノード）のシステム コンソールにアクセスするため、Data ONTAPからsystem node run-consoleコマンドを入力した結果を示します。コンソールでboot_ontapコマンドを入力してnode2をData ONTAPでブートし、続いてCtrl+Dを押してコンソールを終了してData ONTAPに戻ります。

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you
might open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
...
```

システム コンソールを終了するには、Ctrl+Dを押します。

```
Connection to 123.12.123.12 closed.
cluster1::>
```

関連コンセプト

SP CLIセッション、SPコンソール セッション、システム コンソール セッションの関係（61ページ）

関連タスク

SSHを使用したクラスタへのアクセス（11ページ）
管理ホストからのSPへのアクセス（59ページ）
ブート環境のプロンプトからのData ONTAPのブート（47ページ）

ノードのルート ボリュームとルート アグリゲートに関するルール

ノードのルート ボリュームには、そのノードの特別なディレクトリとファイルが格納されています。ルート ボリュームはルート アグリゲートに含まれています。ノードのルート ボリュームとルート アグリゲートには、いくつかのルールが適用されます。

ノードのルート ボリュームは、工場出荷時またはセットアップ ソフトウェアによってインストールされたFlexVolです。ルート ボリュームは、システム ファイル、ログ ファイル、およびコア ファイル用に

予約されています。ディレクトリ名は/mrootで、テクニカル サポートの指示に従って、システムシェルからのみアクセスできます。ノードのルート ボリュームの最小サイズは、プラットフォーム モデルによって異なります。

- ノードのルート ボリュームには次のルールが適用されます。
  - テクニカル サポートから指示がないかぎり、ルート ボリュームの構成またはコンテンツを変更しないでください。
  - ユーザ データはルート ボリュームに格納しないでください。
    ユーザ データをルート ボリュームに格納すると、HAペアのノード間でのストレージのギブバックに時間がかかります。
  - 別のボリュームを新しいルート ボリュームに指定するか、ルート ボリュームを別のアグリゲートに移動する必要がある場合は、テクニカル サポートにお問い合わせください。
- ルート アグリゲートは、ノードのルート ボリューム専用になります。
  ルート以外のボリュームをルート アグリゲートに作成することはできません。

関連情報

NetApp Hardware Universe

ノードのルート ボリュームのスペースの解放

ノードのルート ボリュームがいっぱいか、ほぼいっぱいになると、警告メッセージが表示されます。ルート ボリュームがいっぱいになると、ノードは正しく動作できません。コア ダンプ ファイル、パケット トレース ファイル、およびルート ボリュームのSnapshotコピーを削除することにより、ノードのルート ボリュームのスペースを解放できます。

手順

1. system node coredump showコマンドを使用して、ノードのコア ダンプ ファイルおよびその名前を表示します。
2. 不要なコア ダンプ ファイルは、system node coredump deleteコマンドを使用して、ノードから削除します。
3. 次のコマンドを入力して、ノードシェルにアクセスします。

   system node run -node *nodename*

   *nodename*は、ルート ボリュームのスペースを解放したいノードの名前です。
4. ノードシェルに次のコマンドを入力して、ノードシェルのadvanced特権レベルに切り替えます。

   priv set advanced
5. ノードのパケット トレース ファイルは、次のようにノードシェルから表示、削除を行います。
   a. 次のコマンドを入力して、ノードのルート ボリュームにあるすべてのファイルを表示します。

      ls /etc/

   b. ノードのルート ボリュームにいずれかのパケット トレース ファイル（*.trc）がある場合は、次のコマンドを入力して個別に削除します。

      rm /etc/*file_name*.trc
6. ノードのルート ボリュームのSnapshotコピーは、次のようにノードシェルから特定、および削除を行います。
   a. 次のコマンドを入力してルート ボリューム名を特定します。

      vol status

ルート ボリュームは、`vol status`コマンドの出力で「Options」列に「root」として表記されます。

例

次の例で、ルート ボリュームは`vol0`です。

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

b. 次のコマンドを入力してルート ボリュームのSnapshotコピーを表示します。

`snap list root_vol_name`

c. 次のコマンドを入力して不要なルート ボリュームのSnapshotコピーを削除します。

`snap delete root_vol_name snapshot_name`

7. 次のコマンドを入力してノードシェルを終了し、クラスタシェルに戻ります。

`exit`

ノードの起動または停止

メンテナンスまたはトラブルシューティングの目的で、ノードの起動または停止が必要になる場合があります。ノードの起動または停止は、Data ONTAP CLI、ブート環境プロンプト、またはSP CLIから実行できます。

SP CLIコマンドの`system power off`または`system power cycle`を使用してノードの電源をオフにしたり、電源を再投入すると、ノードが誤ってシャットダウンされる（*ダーティー シャットダウン*）場合があります。この方法は、Data ONTAPの`system node halt`コマンドを使用した正常なシャットダウンの代わりにはなりません。

関連コンセプト

サービス プロセッサを使用したリモートからのノードの管理（50ページ）

関連情報

clustered Data ONTAP 8.3 ハイアベイラビリティ構成ガイド

システム プロンプトでのノードのリブート

ノードは、システム プロンプトから通常モードでリブートできます。ノードは、PC CompactFlashカードなどのブート デバイスからブートするように構成されています。

手順

1. クラスタのノード数が4つ以上の場合は、リブートするノードにイプシロンが設定されていないことを確認します。

   a. 権限レベルをadvancedに設定します。

   `set -privilege advanced`

   b. イプシロンが設定されているノードを特定します。

   `cluster show`

例

次の例では、「node1」にイプシロンが設定されています。

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

c. リブートするノードにイプシロンが設定されている場合は、そのノードからイプシロンを削除します。

   `cluster modify -node node_name -epsilon false`

d. 稼働したままにする別のノードにイプシロンを割り当てます。

   `cluster modify -node node_name -epsilon true`

e. admin権限レベルに戻ります。

   `set -privilege admin`

2. `system node reboot`コマンドを使用して、ノードをリブートします。

   `-skip-lif-migration`パラメータを指定しなかった場合は、リブートの前に、別のノードへのデータおよびクラスタ管理LIFの同期的移行が試行されます。LIFの移行が失敗した場合、またはタイム アウトになった場合、リブート プロセスは中止され、LIFの移行の失敗を示すエラーがData ONTAPに表示されます。

   例

   ```
   cluster1::> system node reboot -node node1 -reason "software upgrade"
   ```

   ノードのリブート プロセスが開始されます。Data ONTAPログイン プロンプトが表示され、リブート プロセスが完了したことが示されます。

ブート環境のプロンプトからのData ONTAPのブート

ノードのブート環境のプロンプトから、Data ONTAPの現在のリリースまたはバックアップ リリースをブートできます。

手順

1. ストレージ システム プロンプトから、`system node halt`コマンドを使用してブート環境のプロンプトにアクセスします。

   ストレージ システム コンソールに、ブート環境のプロンプトが表示されます。

2. ブート環境のプロンプトに、次のコマンドのいずれかを入力します。

ブート対象	コマンド
Data ONTAPの現在のリリース	`boot_ontap`
ブート デバイスのData ONTAPプライマリ イメージ	`boot_primary`
ブート デバイスのData ONTAPバックアップ イメージ	`boot_backup`

使用するイメージがわからない場合、まずboot_ontapを使用してください。

関連タスク

ノードのシステム コンソールへのアクセス（43ページ）

ノードのシャットダウン

ノードが応答しなくなった場合や、サポート担当者からトラブルシューティング対応の一環として実行するように指示された場合は、ノードをシャットダウンできます。

手順

1. クラスタのノード数が4つ以上の場合は、シャットダウンするノードにイプシロンが設定されていないことを確認します。

   a. 権限レベルをadvancedに設定します。

   set -privilege advanced

   b. イプシロンが設定されているノードを特定します。

   cluster show

   例

   次の例では、「node1」にイプシロンが設定されています。

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

   c. シャットダウンするノードにイプシロンが設定されている場合は、そのノードからイプシロンを削除します。

   cluster modify -node *node_name* -epsilon false

   d. 稼働したままにする別のノードにイプシロンを割り当てます。

   cluster modify -node *node_name* -epsilon true

   e. admin権限レベルに戻ります。

   set -privilege admin

2. system node haltコマンドを使用して、ノードをシャットダウンします。

   -skip-lif-migrationパラメータを指定しなかった場合は、シャットダウンの前に、別のノードへのデータおよびクラスタ管理LIFの同期的移行が試行されます。LIFの移行が失敗した、またはタイム アウトになった場合、シャットダウン プロセスは中止され、LIFの移行の失敗を示すエラーがData ONTAPに表示されます。

   -dumpパラメータを使用すれば、シャットダウン時にコア ダンプを手動でトリガーすることができます。

   例

   次の例では、「node1」という名前のノードをハードウェア保守のためにシャットダウンします。

```
cluster1::> system node halt -node node1 -reason 'hardware
maintenance'
```

ブート メニューによるノード管理

ブート メニューを使用して、ノードの構成エラーの修正、管理パスワードのリセット、ディスクの初期化、ノード構成のリセット、ブート デバイスへのノード構成情報のリストアを実行できます。

手順

1. システム プロンプトで`system node reboot`コマンドを使用してノードをリブートし、ブート メニューにアクセスします。

   ノードのリブート プロセスが開始されます。

2. リブート プロセス時にブート メニューを表示するよう求められた場合、Ctrl+Cキーを押してこれを実行します。

   ノードに次のブート メニュー オプションが表示されます。

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
Selection (1-8)?
```

   注: ブート メニュー オプション**[(2) Boot without /etc/rc]**は廃止されており、選択しても何も実施されません。

3. 対応する番号を入力して、次のオプションのいずれかを選択します。

目的	選択するオプション
通常のモードでノードをブートする	**1) Normal Boot**
ノードのパスワード（「admin」アカウントのパスワードと同じ）を変更する	**3) Change Password**
ノードのディスクを初期化し、そのノードのルート ボリュームを作成する	**4) Clean configuration and initialize all disks** **注意:** このメニュー オプションを選択すると、ノードのディスク上のすべてのデータが消去され、ノード構成が工場出荷時のデフォルトの設定にリセットされます。 このメニュー オプションは、ノードをクラスタから分離して別のクラスタに追加するまでの間に選択します。このメニュー オプションでは、ディスクを初期化する前にノードがリブートされます。 アレイを使用するノードの場合、アレイLUNではなくディスク シェルフ上のディスクのみが初期化されます。ディスク シェルフがないノードの場合は、ストレージ アレイ上のルート ボリュームが初期化されます。 初期化しようとするノードに、ルート データの分割用にパーティショニングされたディスクがある場合、ノードを初期化する前にディスクのパーティションを削除しておく必要があります。

目的	選択するオプション
アグリゲート処理およびディスク保守処理を実行し、アグリゲートおよびディスクに関する詳細情報を取得する	**5) Maintenance mode boot** 保守モードは`halt`コマンドで終了します。
ノードのルート ボリュームからPC CompactFlashカードなどのブート デバイスに構成情報をリストアする	**6) Update flash from backup config** Data ONTAPは、一部のノード構成情報をブート デバイスに格納します。ノードがリブートすると、ブート デバイス上の情報がノードのルート ボリュームに自動的にバックアップされます。ブート デバイスが壊れたり、交換が必要になった場合は、このメニュー オプションを使用して構成情報をノードのルート ボリュームからブート デバイスにリストアすることができます。
ノードに新しいソフトウェアをインストールする	**7) Install new software first** ブート デバイス上のData ONTAPソフトウェアにルート ボリュームに使用するストレージ アレイのサポートが含まれない場合は、このメニュー オプションを使用して、ストレージ アレイをサポートするソフトウェアのバージョンを取得してノードにインストールします。 このメニュー オプションは、Data ONTAPソフトウェアの新しいバージョンを、ルート ボリュームがインストールされていないノードにインストールするときにのみ使用します。Data ONTAPのアップグレードには使用*しない*でください。
ノードをリブートする	**8) Reboot node**

関連タスク

ノードのシステム コンソールへのアクセス（43ページ）

関連情報

clustered Data ONTAP 8.3 物理ストレージ管理ガイド

サービス プロセッサを使用したリモートからのノードの管理

Service Processor（SP;サービス プロセッサ）はサポート対象のすべてのプラットフォーム モデルに含まれるリモート管理デバイスです。SPを使用してノードをリモートから管理できます。SPは、ノードの動作状態に関係なく、継続して機能します。

Data ONTAP-vプラットフォーム（Data ONTAP Edgeなど）にはSPは搭載されていません。Data ONTAP-vプラットフォームのリモート管理には、Data ONTAP-v管理ツール（dvadmin）を使用します。

SPの概要

SPは、ノードに対するアクセス、監視、およびトラブルシューティングをリモートから行うことができるリモート管理デバイスです。

SPの主な機能は次のとおりです。

- SPを使用すると、ノード コントローラの状態に関係なく、ノードにリモートからアクセスして、ノードの診断、シャットダウン、電源の再投入、リブートを実行できます。
  SPはスタンバイ電圧で動作するため、少なくとも1つのノード電源装置に電力が供給されていれば使用可能です。
  SPにログインするには、管理ホストからSecure Shellクライアント アプリケーションを使用します。ログインすると、SP CLIを使用して、リモートからノードの監視とトラブルシューティングを行

うことができます。さらに、SPを使用してシリアル コンソールにアクセスし、リモートからData ONTAPコマンドを実行できます。

SPにはシリアル コンソールからアクセスでき、またSPからシリアル コンソールにアクセスすることもできます。SPでは、SP CLIセッションと別のコンソール セッションを両方同時に開くことができます。

たとえば、温度センサーで異常な高温または低温が検知されると、Data ONTAPのトリガーによって、SPがマザーボードを正常にシャットダウンします。シリアル コンソールが応答しなくなりますが、コンソールでCtrl+Gを押してSP CLIにアクセスすることができます。アクセスすると、SPから`system power on`または`system power cycle`コマンドを使用して、ノードの電源投入または再投入ができます。

- SPによって環境センサーが監視され、イベントがログに記録されるため、タイムリーで効果的な保守操作を行うことができます。

  SPはノードの温度、電圧、電流、ファン速度などの環境センサーを監視します。環境センサーが異常を検知すると、SPが異常な測定値をログに記録し、Data ONTAPに問題を通知します。またSPはノードがAutoSupportメッセージを送信できるかどうかにかかわらず、必要に応じてAutoSupportメッセージによってアラートと「down system」（システム停止）通知を送信します。

  さらに、ブートの進行、Field Replaceable Unit（FRU;フィールド交換可能ユニット）の交換、Data ONTAPが生成するイベント、SPのコマンド履歴といったイベントについてもログに記録します。AutoSupportメッセージを手動で起動し、指定したノードから収集されたSPログ ファイルを含めることができます。

  SPは、停止したノードの代わりにこれらのメッセージを生成し、AutoSupportメッセージに追加の診断情報を添付する以外には、AutoSupport機能には影響を及ぼしません。AutoSupportの設定値やメッセージ内容は、Data ONTAPから継承されます。

  注: SPは、通知を送信するときに、`system node autosupport modify`コマンドの`-transport`パラメータ設定に依存しません。SPはSimple Mail Transfer Protocol（SMTP;簡易メール転送プロトコル）のみを使用し、メール ホストの情報を含めるためにホストのAutoSupport設定を必要とします。

  SNMPが有効になっている場合、SPはSNMPトラップを生成して、すべての「down system」イベントに対するトラップ ホストを設定します。

- SPには、System Event Log（SEL;システム イベント ログ）に最大4,000のイベントを格納できる不揮発性メモリ バッファがあるため、問題の診断に役立ちます。

  SELには、各監査ログ エントリが監査イベントとして格納されます。SELはSPのオンボード フラッシュ メモリに格納されています。SELのイベント リストは、SPによって、指定された受信者にAutoSupportメッセージを通じて自動的に送信されます。

  SELには次の情報が含まれています。

  - SPが検出したハードウェア イベント。たとえば、電源装置、電圧、またはその他のコンポーネントに関するセンサーのステータスなど
  - SPが検出したエラー。たとえば、通信障害、ファンの故障、メモリまたはCPUのエラーなど
  - ノードがSPに送信した重大なソフトウェア イベント。たとえば、パニック、通信障害、ブート障害、あるいはSPの`system reset`または`system power cycle`コマンド実行の結果として生じたユーザ起因の「down system」（システム停止）など

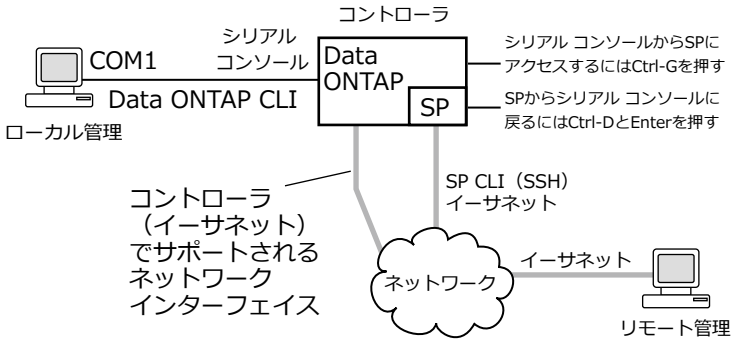
- SPは、管理者によるコンソール ログインまたはコンソール接続の有無にかかわらず、シリアル コンソールを監視します。

  コンソールにメッセージが送信されると、SPはメッセージをコンソール ログに格納します。ノードのいずれかの電源装置からSPに給電されていれば、コンソール ログの機能は維持されます。SPはスタンバイ電源で動作するので、ノードの電源再投入時または電源オフ時にも使用可能です。

- SPが設定されている場合、ハードウェア アシスト テイクオーバーが可能です。

- SP APIサービスは、Data ONTAPがネットワークを介してSPと通信できるようにします。
  このサービスは、SPファームウェアの更新にネットワーク インターフェイスを使用する、ノードが別のノードのSP機能やシステム コンソールにアクセスできるようにする、別のノードからSPログをアップロードする、などのネットワークベースの機能をサポートすることで、Data ONTAPによるSPの管理を強化します。
  SP APIサービスの設定は変更でき、サービスが使用するポートを変更したり、サービスが内部通信に使用するSSL証明書およびSSH証明書を更新したり、サービス全体を無効化したりすることができます。

次の図は、Data ONTAPおよびノードのSPへのアクセスを示しています。SPインターフェイスは、イーサネット ポート（シャーシ背面にあるレンチ マークの付いたポート）経由でアクセスされます。



関連情報

clustered Data ONTAP 8.3 ハイアベイラビリティ構成ガイド

SPネットワークの設定

SPネットワークを設定すると、IPアドレスを使用してSPにアクセスできるようになります。クラスタ レベルでSPの自動ネットワーク設定を設定するか（推奨）または個々のノードのSPネットワークを手動で設定できます。また、Data ONTAPでネットワーク経由でのSPへのアクセスに使用するSP APIサービスを変更することもできます。

SPネットワーク設定に関する考慮事項

SPに対する自動ネットワーク設定をクラスタレベルで有効にできます（推奨）。SPの自動ネットワーク設定を無効なままにし（デフォルト）、SPネットワーク設定をノード レベルで手動で管理することもできます。どちらの場合にも、いくつかの考慮事項があります。

SPの自動ネットワーク設定を有効にすると、指定したサブネットのアドレス リソース（IPアドレス、サブネット マスク、ゲートウェイ アドレスなど）を使用してネットワークが自動的に設定されます。SPの自動ネットワーク設定を使用すると、各ノードのSPにIPアドレスを手動で割り当てる必要がありません。SPの自動ネットワーク設定を有効にするには、まず設定に使用するサブネットが先にクラスタに定義されている必要があるため、デフォルトでは、自動ネットワーク設定は無効になっています。

SPの自動ネットワーク設定を有効にした場合、次のシナリオと考慮事項が該当します。

- これまでに一度もSPが設定されていない場合、SPネットワークは、SPの自動ネットワーク設定に指定したサブネットに基づいて自動的に設定されます。
- 以前にSPが手動で設定されている場合、または別のサブネットに基づく既存のSPネットワーク設定がある場合、クラスタ内のすべてのノードのSPネットワークが、自動ネットワーク設定に指定したサブネットに基づいて再設定されます。
  再設定によってSPに別のアドレスが割り当てられると、DNS設定に影響し、SPのホスト名を解決できなくなる可能性があります。その場合、DNS設定の更新が必要になります。

- クラスタに参加するノードには、指定したサブネットを使用してSPネットワークが自動的に設定されます。
- `system service-processor network modify`コマンドを使用して、SP IPアドレスを変更することはできません。
  SP自動ネットワーク設定が有効になっている場合、このコマンドで実行できるのはSPネットワーク インターフェイスの有効化または無効化のみです。
  - SPの自動ネットワーク設定が以前に有効にされている場合、SPネットワーク インターフェイスを無効にすると、割り当てられたアドレス リソースは解放されてサブネットに戻されます。
  - SPネットワーク インターフェイスを無効にし、その後再度有効にすると、SPは別のアドレスで再設定されることがあります。

SPの自動ネットワーク設定を無効にした場合（デフォルト）、次のシナリオと考慮事項が該当します。

- これまでに一度もSPが設定されていない場合、SP IPv4ネットワーク設定は、IPv4 DHCPを使用するデフォルトの設定になり、IPv6は無効になります。
  クラスタに参加するノードのSPネットワーク設定も、デフォルトでIPv4 DHCPに設定されます。
- `system service-processor network modify`コマンドを使用して、ノードのSP IPアドレスを設定できます。
  あるサブネットに割り当てられているアドレスを使用してSPネットワークを手動で設定しようとすると、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、重複するアドレスが割り当てられる可能性があります。

一度有効にしたSPの自動ネットワーク設定を無効にした場合、次のシナリオと考慮事項が該当します。

- SPの自動ネットワーク設定でIPv4アドレス ファミリーが無効になっている場合、SP IPv4ネットワークはDHCPを使用するデフォルトの設定になります。また、`system service-processor network modify`コマンドを使用し、個々のノードのSP IPv4設定を変更できます。
- SPの自動ネットワーク設定でIPv6アドレス ファミリーが無効になっていいる場合、SP IPv6ネットワークも無効になります。また、`system service-processor network modify`コマンドを使用して、個々のノードのSP IPv6設定を有効にし、変更することができます。

関連タスク

SP自動ネットワーク設定の有効化（53ページ）
SPネットワークの手動設定（54ページ）

SP自動ネットワーク設定の有効化

SPネットワークを手動で設定するよりも、自動ネットワーク設定を使用するようにSPを設定することを推奨します。SP自動ネットワーク設定はクラスタ全体の設定であるため、個々のノードでSPネットワークを手動で管理する必要がありません。

開始する前に

- SP自動ネットワーク設定には、クラスタ内に定義済みで、SPネットワーク インターフェイスとリソースが競合しないサブネットを使用する必要があります。
  `network subnet show`コマンドを実行すると、クラスタのサブネット情報が表示されます。
  サブネットの関連付けを強制するパラメータ（`network subnet`コマンドの`-force-update-lif-associations`パラメータ）は、ネットワークLIFでのみサポートされ、SPネットワーク インターフェイスではサポートされません。
- SPにIPv6接続を設定する場合、Data ONTAPに対してIPv6が設定済みで、有効になっている必要があります。

`network options ipv6 show`コマンドを使用すると、Data ONTAPの現在のIPv6設定が表示されます。

手順

1. `system service-processor network auto-configuration enable`コマンドを使用して、SPで使用するサブネットのIPv4またはIPv6アドレス ファミリーと名前を指定します。
2. `system service-processor network auto-configuration show`コマンドを使用して、SPの自動ネットワーク設定を表示します。
3. その後クォーラム内のすべてのノードに対してSP IPv4またはIPv6ネットワーク インターフェイスを無効または有効にする場合は、`system service-processor network modify`コマンドに`-address-family` [**`IPv4`**|**`IPv6`**]パラメータおよび`-enable` [**`true`**|**`false`**]パラメータを指定して使用します。

   SP自動ネットワーク設定が有効になっている場合、クォーラム内のノードのSP IPアドレスを変更することはできません。実行できるのは、SP IPv4またはIPv6ネットワーク インターフェイスの有効化または無効化だけです。

   ノードがクォーラム外にある場合、ノードから`system service-processor network modify`を実行し、そのノードのSP自動ネットワーク設定をオーバーライドすることを確認して、SPのIPアドレスを含むノードのSPネットワーク設定を変更できます。ただし、ノードがクォーラムに参加すると、指定したサブネットに基づいて、ノードに対してSPの自動再設定が実行されます。

関連コンセプト

SPネットワーク設定に関する考慮事項（52ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

SPネットワークの手動設定

SPに自動ネットワーク設定が設定されていない場合、IPアドレスを使用してSPにアクセスできるように、ノードのSPネットワークを手動で設定する必要があります。

開始する前に

SPにIPv6接続を設定する場合、Data ONTAPに対してIPv6が設定済みで、有効になっている必要があります。`network options ipv6`コマンドを使用すると、Data ONTAPのIPv6設定を管理できます。

タスク概要

SPは、IPv4、IPv6、またはその両方を使用するように設定できます。SPのIPv4設定では静的アドレス指定とDHCPアドレス指定をサポートし、SPのIPv6設定では静的アドレス指定のみをサポートしています。

SPの自動ネットワーク設定が設定されている場合、ノードごとにSPネットワークを手動で設定する必要はなく、`system service-processor network modify`コマンドを使用して実行できるのは、SPネットワーク インターフェイスの有効化または無効化だけです。

手順

1. `system service-processor network modify`コマンドを使用して、ノードのSPネットワークを設定します。

- `-address-family`パラメータには、SPのIPv4とIPv6のどちらの設定を変更するかを指定します。
- `-enable`パラメータは、指定したIPアドレス ファミリーのネットワーク インターフェイスを有効にします。
- `-dhcp`パラメータでは、DHCPサーバのネットワーク設定と、指定のネットワーク アドレスのどちらを使用するかを指定します。
  IPv4を使用している場合にのみ、DHCPを（`-dhcp`を**v4**に設定することで）有効にできます。IPv6設定の場合、DHCPを有効にできません。
- `-ip-address`パラメータには、SPのパブリックIPアドレスを指定します。
  あるサブネットに割り当てられているアドレスを使用してSPネットワークを手動で設定しようとすると、警告メッセージが表示されます。警告を無視して手動でのアドレス割り当てを続行すると、重複するアドレスが割り当てられる可能性があります。
- `-netmask`パラメータでは、SPのネットマスクを指定します（IPv4を使用している場合）。
- `-prefix-length`パラメータでは、SPのサブネット マスクのネットワーク プレフィックス長を指定します（IPv6を使用している場合）。
- `-gateway`パラメータには、SPのゲートウェイIPアドレスを指定します。

2. クラスタ内の各ノードについて、手順*1*を繰り返してSPネットワークを設定します。
3. `system service-processor network show`コマンドに`-instance`パラメータまたは`-fields` **`setup-status`**パラメータを指定して使用し、SPネットワーク設定を表示してSPのセットアップ ステータスを確認します。

   ノードのSPのセットアップ ステータスは、次のいずれかになります。

   - **`not-setup`**–未設定
   - **`succeeded`**–設定済み
   - **`in-progress`**–設定中
   - **`failed`**–設定に失敗

SPネットワークの設定例

次の例では、IPv4を使用するようにノードのSPを設定し、SPを有効化し、最後にSPネットワーク設定を表示して設定内容を確認します。

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                                Node: node1
                        Address Type: IPv4
                   Interface Enabled: true
                      Type of Device: SP
                              Status: online
                         Link Status: up
                         DHCP Status: none
                          IP Address: 192.168.123.98
                         MAC Address: ab:cd:ef:fe:ed:02
                             Netmask: 255.255.255.0
        Prefix Length of Subnet Mask: -
          Router Assigned IP Address: -
                Link Local IP Address: -
                   Gateway IP Address: 192.168.123.1
                    Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                          Subnet Name: -
Enable IPv6 Router Assigned Address: -
```

```
             SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

                                Node: node1
                        Address Type: IPv6
                   Interface Enabled: false
                      Type of Device: SP
                              Status: online
                         Link Status: disabled
                         DHCP Status: none
                          IP Address: -
                         MAC Address: ab:cd:ef:fe:ed:02
                             Netmask: -
        Prefix Length of Subnet Mask: -
          Router Assigned IP Address: -
                Link Local IP Address: -
                   Gateway IP Address: -
                    Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                         Subnet Name: -
Enable IPv6 Router Assigned Address: -
             SP Network Setup Status: not-setup
    SP Network Setup Failure Reason: -

2 entries were displayed.

cluster1::>
```

関連コンセプト

SPネットワーク設定に関する考慮事項（52ページ）

関連タスク

SP自動ネットワーク設定の有効化（53ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

SP APIサービス設定の変更

SP APIは、Data ONTAPがネットワークを介してSPと通信できるようにするセキュアなネットワークAPIです。SP APIサービスが使用するポートを変更したり、サービスの内部通信に使用される証明書を更新したり、またはサービス全体を無効にすることができます。この設定の変更が必要になることはほとんどありません。

タスク概要

- SP APIサービスは、デフォルトでポート**50000**を使用します。
  この値は、ポート**50000**が別のネットワーク アプリケーションの通信に使用されているネットワーク環境の場合や、他のアプリケーションからのトラフィックとSP APIサービスが生成するトラフィックを分離する場合などに変更できます。
- SP APIサービスが使用するSSL証明書およびSSH証明書は、クラスタ内専用であり、外部に配布されることはありません。
  証明書のセキュリティが侵害されることはほとんどありませんが、侵害された場合には証明書を更新できます。
- SP APIサービスは、デフォルトで有効になっています。
  SP APIサービスは、SPが設定または使用されていないプライベートLANでこのサービスを無効にしたい場合など、例外的な場合にのみ無効にする必要があります。
  SP APIサービスを無効にすると、APIは着信接続をいっさい受け入れません。さらに、ネットワークベースのSPファームウェアの更新や「down system」ログ収集などの機能は使用できなくなります。システムはシリアル インターフェイスの使用に切り替わります。

手順

1. `set -privilege` **`advanced`**コマンドを使用して、advanced権限レベルに切り替えます。
2. SP APIサービス設定を次のように変更します。

目的	使用するコマンド
SP APIサービスで使用されるポートの変更	`system service-processor api-service modify`（`-port` {**`49152`**..**`65535`**}パラメータを指定）
SP APIサービスの内部通信に使用されるSSL証明書およびSSH証明書の更新	`system service-processor api-service renew-certificates` パラメータを指定しない場合、ホスト証明書（クライアント証明書およびサーバ証明書を含む）のみが更新されます。 `-renew-all` **`true`**パラメータを指定すると、ホスト証明書とルートCA証明書の両方が更新されます。
SP APIサービスの無効化または再有効化	`system service-processor api-service modify`（`-is-enabled` {**`true`**|**`false`**}パラメータを指定）

3. `system service-processor api-service show`コマンドを使用してSP APIサービス設定を表示します。

SPファームウェアの更新の管理方法

Data ONTAPには、*ベースライン イメージ*と呼ばれるSPファームウェア イメージが含まれています。新しいバージョンのSPファームウェアがリリースされた、そのファームウェアをダウンロードしてSPファームウェアを更新できます。Data ONTAPのバージョンをアップグレードする必要はありません。

Data ONTAPでは、次の方法でSPファームウェアの更新を管理できます。

- SP自動更新機能がデフォルトで有効になっており、次のシナリオでSPファームウェアを自動的に更新できます。
  - 新しいバージョンのData ONTAPにアップグレードする場合。
    Data ONTAPにバンドルされているSPファームウェアのバージョンがノードで実行されているSPファームウェアのバージョンよりも新しい場合、Data ONTAPのアップグレード プロセスには、SPファームウェアの更新が自動的に含まれます。

    注: Data ONTAPは、失敗したSP自動更新を検出し、修正アクションをトリガーして、SP自動更新を最大3回試行します。3回の試行がすべて失敗した場合は、テクニカル サポートにお問い合わせください。
  - ネットアップ サポート サイトからダウンロードしたSPファームウェアのバージョンが、現在実行しているSPファームウェアのバージョンよりも新しい場合。
  - Data ONTAPを以前のバージョンにダウングレードまたはリバートする場合。
    SPファームウェアは、ダウングレードまたはリバート後のData ONTAPバージョンでサポートされる最新バージョンに自動的に更新されます。SPファームウェアの手動更新は必要ありません。

  `system service-processor image modify`コマンドを使用して、SP自動更新機能を無効にできます。ただし、この機能は有効にしておくことを推奨します。この機能を無効にすると、Data ONTAPのイメージとSPファームウェアのイメージが、未認定の最適ではない組み合わせとなります。

- Data ONTAPでは、SPの更新を手動でトリガーできます。`system service-processor image update`コマンドを使用して、SP更新の実行方法を指定できます。
  次のいずれかのオプションを指定します。

- 使用するSPファームウェア パッケージ（**-package**）
  パッケージ ファイル名を指定することによって、ダウンロードするSPファームウェアを更新できます。`system image package show`コマンドは、ノード上で使用可能なすべてのパッケージ ファイルを表示します（SPファームウェア パッケージのファイルを含む）。
- SP更新用のベースラインSPファームウェア パッケージを使用するかどうか（**-baseline**）
  SPファームウェアを、現在実行しているバージョンのData ONTAPに付属しているベースラインのバージョンに更新できます。
- ネットワーク インターフェイスまたはシリアル インターフェイスを使用して、ファームウェア イメージ全体を更新するか、変更部分のみを更新するか（**-update-type**）
- ファームウェア イメージ全体を更新する場合、ログ設定を工場出荷時のデフォルトにリセットし、イベント ログ、IPMIログ、およびフォレンジック ログを含めてSPに保存されているすべてのログの内容を消去するかどうか（**-clear-logs**）

- `system service-processor image update-progress show`コマンドを使用すると、Data ONTAPから実行された最新のSPファームウェア更新のステータスを表示できます。

SPへの既存の接続は、SPファームウェアを更新するときに切断されます。これは、SPファームウェア更新が自動的にまたは手動で開始される場合に該当します。

関連情報

ネットアップのダウンロード：システム ファームウェアおよび診断
Clustered Data ONTAP 8.3 Commands: Manual Page Reference

ネットワーク インターフェイスを使用したSPファームウェアの更新

バージョン1.5、2.5、3.1以降のSPを実行しているData ONTAPからトリガーされるSPファームウェア更新では、SPネットワーク インターフェイス経由でのIPベースのファイル転送メカニズムがサポートされます。

ネットワーク インターフェイス経由のSPファームウェア更新は、シリアル インターフェイス経由の更新よりも高速です。そのため、SPファームウェアを更新中のメンテナンス時間が短縮され、さらにData ONTAPの処理が停止されることもありません。この機能をサポートするSPバージョンは、Data ONTAP 8.3以降に搭載されています。ネットアップ サポート サイトからも入手でき、互換性があるバージョンのData ONTAPが実行されているコントローラにインストールできます。

SPバージョン1.5、2.5、3.1以降を実行している場合、ファームウェア更新は次のように実施されます。

- Data ONTAPによって*自動的*にトリガーされたSPファームウェア更新では、デフォルトでネットワーク インターフェイスが使用されます。ただし、次のいずれかの条件に該当する場合、SP自動更新はシリアル インターフェイス経由に切り替わります。
  - SPネットワーク インターフェイスが設定されていないか、使用できない。
  - IPベースのファイル転送に失敗する。
  - SP APIサービスが無効になっている。
- Data ONTAPから*手動*でトリガーされたSPファームウェア更新（`system service-processor image update`を使用）では、`-update-type`パラメータが**network-full**に設定されている場合のみネットワーク インターフェイスが使用されます。
  それ以外の値に設定されている場合は、シリアル インターフェイスが使用されます。

SP CLIからトリガーされるSPファームウェア更新では、実行しているSPのバージョンにかかわらず、常にSPネットワーク インターフェイスが使用されます。

関連情報

ネットアップのダウンロード：システム ファームウェアおよび診断

SPへのアクセス

service-processorアプリケーション タイプで設定されたクラスタ ユーザ アカウントは、管理ホストからSSH接続を使用して、またはシリアル コンソールからSPにアクセスできます。Data ONTAPでは、特定のIPアドレスを持つ管理ホストのみにSPのSSHアクセスを制限できます。

`system timeout`コマンドを使用すると、SPへのコンソール接続およびSSH接続などのCLIセッションの自動タイムアウト時間の設定を管理できます。

関連コンセプト

CLIセッションの自動タイムアウト時間の管理（28ページ）

SPにアクセスできるアカウント

SPにアクセスする際には、クレデンシャルを求められます。アプリケーション タイプ**service-processor**で作成されたクラスタ ユーザ アカウントは、クラスタの任意のノード上のSP CLIにアクセスできます。SPユーザ アカウントは、Data ONTAPから管理され、パスワードによって認証されます。

SPにアクセスするためのユーザ アカウントは、SP CLIではなくData ONTAPで管理します。ロールに関わりなくクラスタ ユーザ アカウントは、`security login create`コマンドの`-application`パラメータを**service-processor**に設定し、`-authmethod`パラメータを**password**に設定して作成された場合にSPへのアクセスが可能になります。SPではパスワード認証のみサポートされます。

「admin」という名前のクラスタ ユーザ アカウントには、デフォルトで**service-processor**アプリケーション タイプが含まれており、SPへのアクセス権があります。

Data ONTAPでは、システム用に予約されている名前（「root」や「naroot」など）を使用したユーザ アカウントを作成できないようになっています。システム用に予約されている名前を使用してクラスタまたはSPにアクセスすることはできません。

現在のSPユーザ アカウントを表示するには、`security login show`コマンドの`-application` **service-processor**パラメータを使用します。

管理ホストからのSPへのアクセス

管理ホストからノードのSPにログインして、ノードの管理タスクをリモートから実行できます。

開始する前に

次の条件を満たす必要があります。

- SPへのアクセスに使用する管理ホストではSSHv2がサポートされている必要がある。
- SPへのアクセス用にユーザ アカウントがすでにセットアップされている必要がある。
  SPにアクセスするには、`security login create`コマンドの`-application`パラメータを**service-processor**に、`-authmethod`パラメータを**password**に指定してユーザ アカウントを作成しておく必要があります。

タスク概要

SPがIPv4またはIPv6アドレスを使用するように設定されており、ホストからのSSHログイン試行が10分以内に連続5回失敗した場合には、SPはSSHログイン要求を拒否し、ホストのIPアドレスとの通信を15分間中断します。通信は15分後に再開され、SPへのログインを再度試行できるようになります。

Data ONTAPでは、システム用に予約されている名前（「root」や「naroot」など）をクラスタまたはSPにアクセスする目的で作成または使用することはできません。

手順

1. 管理ホストから、SPにログインします。

   ssh *sername@SP_IP_address*

2. プロンプトが表示されたら、*username*のパスワードを入力します。

   SPプロンプトが表示されると、SP CLIにアクセスしていることになります。

管理ホストからSPにアクセスする例

次の例は、SPへのアクセスのために設定されているjoeというユーザ アカウントを使用してSPにログインする方法を示しています。

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

次の例は、IPv6グローバル アドレスまたはIPv6ルータ通知アドレスを使用して、IPv6に対してSSHが設定されかつSPが構成されているノードのSPにログインする方法を示しています。

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

関連コンセプト

SP CLIセッション、SPコンソール セッション、システム コンソール セッションの関係（61ページ）

関連タスク

ノードのシステム コンソールへのアクセス（43ページ）

システム コンソールからSPへのアクセス

システム コンソール（*シリアル コンソール*とも呼ばれる）からSPにアクセスし、タスクを監視したり、トラブルシューティングしたりできます。

手順

1. システム コンソールからSP CLIにアクセスするには、プロンプトでCtrl+Gを押します。
2. プロンプトが表示されたら、SP CLIにログインします。

   SPプロンプトが表示されると、SP CLIにアクセスしていることになります。

3. SP CLIを終了してシステム コンソールに戻るには、Ctrl+Dを押すか「exit」と入力してEnterキーを押します。

システム コンソールからSP CLIへのアクセスの例

次の例に、Ctrl+Gを押してシステム コンソールからSP CLIにアクセスした結果を示します。SPプロンプトにhelp system powerコマンドを入力し、次にCtrl+DとEnterキーを押してシステム コンソールに戻ります。

```
cluster1::>
```

（Ctrl+Gを押してSP CLIにアクセスします。）

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

（Ctrl+DとEnterキーを押してシステム コンソールに戻ります。）

```
cluster1::>
```

SP CLIセッション、SPコンソール セッション、システム コンソール セッションの関係

SP CLIセッションを開いてノードをリモートから管理したり、別のSPコンソール セッションを開いてノードのコンソールにアクセスしたりすることができます。SPコンソール セッションは、同時システム コンソール セッションに表示される出力をミラーリングします。SPとシステム コンソールには独立したシェル環境があり、独立したログイン認証が行われます。

SP CLIセッション、SPコンソール セッション、システム コンソール セッションの関係を理解しておくと、ノードをリモートから管理する際に役に立ちます。これらのセッションの関係を次に示します。

- SP CLIセッションには一度に1人の管理者しかログインできません。ただしSPでは、SP CLIセッションと別のSPコンソール セッションを同時に開くことができます。

  SP CLIはSPプロンプト（SP>）で表されます。SP CLIセッションでは、SP system consoleコマンドでSPコンソール セッションを開始できます。同時に、SSHを介して別のSP CLIセッションを開始することもできます。Ctrl+Dキーを押してSPコンソール セッションを終了すると、自動的にSP CLIセッションに戻ります。SP CLIセッションがすでに存在する場合は、既存のSP CLIセッションを終了するかどうかを尋ねるメッセージが表示されます。「Y」キーを押すと、既存のSP CLIセッションが終了し、SPコンソールからSP CLIに戻ることができます。このアクションは、SPのイベント ログに記録されます。

  SSH経由で接続されたData ONTAP CLIセッションでは、別のノードからData ONTAPのsystem node run-consoleコマンドを実行して、ノードのシステム コンソールに切り替えることができます。

- セキュリティ上の理由から、SP CLIセッションとシステム コンソール セッションには独立したログイン認証機能があります。

  SP CLIから（SP system consoleコマンドを使用して）SPコンソール セッションを開始すると、システム コンソールのクレデンシャルを入力するように求められます。システム コンソール セッションから（Ctrl+Gキーで）SP CLIにアクセスすると、SP CLIのクレデンシャルを入力するように求められます。

- SPコンソール セッションとシステム コンソール セッションには独立したシェル環境があります。

SPコンソール セッションは、同時システム コンソール セッションに表示される出力をミラーリングします。ただし、同時システム コンソール セッションでは、SPコンソール セッションをミラーリングしません。
また、SPコンソール セッションは、同時SSHセッションの出力をミラーリングしません。

SPにアクセスできるIPアドレスの管理

デフォルトでは、SPはあらゆるIPアドレスの管理ホストからのSSH接続要求を受け付けます。指定するIPアドレスを持つ管理ホストのみからのSSH接続要求を受け付けるようにSPを設定できます。実施する変更内容は、クラスタ内の任意のノードのSPへのSSHアクセスに適用されます。

手順

1. 指定するIPアドレスのみにSPアクセスを付与するには、`system service-processor ssh add-allowed-addresses`コマンドに`-allowed-addresses`パラメータを指定して使用します。

   - `-allowed-addresses`パラメータの値は、*address*/*netmask*の形式で指定する必要があり、複数の*address*/*netmask*のペアはカンマで区切る必要があります。例として、**`10.98.150.10/24, fd20:8b1e:b255:c09b::/64`**のようになります。
     `-allowed-addresses`パラメータを**`0.0.0.0/0, ::/0`**に設定すると、すべてのIPアドレスがSPにアクセスできるようになります（デフォルト）。
   - 指定したIPアドレスのみにSPアクセスを制限することでデフォルトの設定を変更すると、指定したIPアドレスで「allow all」のデフォルト設定（**`0.0.0.0/0, ::/0`**）を置き換えることの確認を求めるプロンプトが表示されます。
   - `system service-processor ssh show`コマンドを使用すると、SPにアクセスできるIPアドレスが表示されます。

2. 指定したIPアドレスをSPへのアクセスからブロックする場合、`system service-processor ssh remove-allowed-addresses`コマンドに`-allowed-addresses`パラメータを指定して使用します。

   すべてのIPアドレスをSPへのアクセスからブロックする場合、SPはすべての管理ホストからアクセス不能になります。

SPにアクセスできるIPアドレスの管理の例

次の例は、SPへのSSHアクセスのためのデフォルト設定を示しています。ここでは、指定したIPアドレスのみにSPアクセスを制限することで、デフォルトの設定を変更し、指定したIPアドレスをアクセス リストから削除し、すべてのIPアドレスに対するSPアクセスをリストアします。

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed-addresses
192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed-addresses
192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list, all IP
         addresses will be denied access. To restore the "allow all" default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed-addresses
```

```
0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

SP CLIでのオンライン ヘルプの使用

SPプロンプトで疑問符（?）またはhelpと入力すると、SPオンライン ヘルプによってSP CLIコマンドとオプションが表示されます。

手順

1. SPコマンドのヘルプ情報を表示するには、SPプロンプトで次のいずれかを入力します。
   - `help`
   - ?

   例

   次に、SP CLIオンライン ヘルプの例を示します。

   ```
   SP> help
   date - print date and time
   exit - exit from the SP command line interface
   events - print system events and event information
   help - print command help
   priv - show and set user mode
   sp - commands to control the SP
   system - commands to control the system
   version - print SP version
   ```

2. SPコマンドのオプションのヘルプ情報を表示するには、SPプロンプトで次のコマンドを入力します。

   help *SP_command*

   例

   次に、SP eventsコマンドのSP CLIオンライン ヘルプの例を示します。

   ```
   SP> help events
   events all - print all system events
   events info - print system event log information
   events newest - print newest system events
   events oldest - print oldest system events
   events search - search for and print system events
   ```

ノードのリモート管理用コマンド

ノードをリモートで管理するには、ノードのSPにアクセスし、SP CLIコマンドを実行してノード管理タスクを実行します。よく実行されるいくつかのリモート ノード管理タスクについては、クラスタ内の別のノードからData ONTAPコマンドを使用することもできます。一部のSPコマンドはプラットフォーム固有であるため、使用しているプラットフォームでは使用できない場合があります。

状況	使用するSPコマンド	またはData ONTAPコマンド
使用できるSPコマンド、または指定したSPコマンドのサブコマンドを表示する	help [*command*]	

状況	使用するSPコマンド	またはData ONTAPコマンド
SP CLIの現在の権限レベルを表示する	`priv show`	
SP CLIについて指定されたモードにアクセスするための権限レベルを設定する	`priv set {`**`admin`**`|`**`advanced`**`|`**`diag`**`}`	
システムの日付と時間を表示する	`date`	`date`
SPによって記録されるイベントを表示する	`events {`**`all`**`|`**`info`**`|`**`newest`** *`number`*`|`**`oldest`** *`number`*`|`**`search`** *`keyword`*`}`	
SPのステータスとネットワーク設定情報を表示する	`sp status [-v | -d]` `-v`オプションを指定すると、SP統計情報が詳細形式で表示されます。`-d`オプションを指定すると、SPデバッグ ログが表示に追加されます。	*`system service-processor show`*
SPが稼働している時間、および過去1分、5分、15分間に実行キューに入れられたジョブの平均数を表示する	`sp uptime`	
システム コンソール ログを表示する	`system log`	
SPログ アーカイブ、またはアーカイブ内のファイルを表示する	`sp log history show [-archive {`**`latest`**`|`**`all`**`|`*`archive-name`*`}] [-dump {`**`all`**`|`*`file-name`*`}]`	
ノードのコントローラの電源ステータスを表示する	`system power status`	*`system node power show`*
バッテリ情報を表示する	`system battery show`	
ACP情報またはエクスパンダセンサーのステータスを表示する	`system acp [`**`show`**`|`**`sensors show`**`]`	
すべてのシステムFRUとそのIDをリストする	`system fru list`	
指定したFRUの製品情報を表示する	`system fru show` *`fru_id`*	
FRUのデータ履歴ログを表示する	`system fru log show` （advanced権限レベル）	

状況	使用するSPコマンド	またはData ONTAPコマンド
状態や現在の値など、環境センサーのステータスを表示する	`system sensors`または`system sensors show`	*`system node environment sensors show`*
指定したセンサーのステータスと詳細を表示する	`system sensors get` *`sensor_name`* *`sensor_name`*は、`system sensors`または`system sensors show`コマンドを使用して取得できます。	
SPファームウェアのバージョン情報を表示する	`version`	*`system service-processor image show`*
SPコマンド履歴を表示する	`sp log audit` （advanced権限レベル）	
SPデバッグ情報を表示する	`sp log debug` （advanced権限レベル）	
SPメッセージ ファイルを表示する	`sp log messages` （advanced権限レベル）	
watchdogリセット イベントでシステムの詳細情報を収集する設定を表示するか、watchdogリセット イベント中に収集されたシステムの詳細情報を表示するか、収集されたシステム詳細情報をクリアする	`system forensics` [**`show`** | **`log dump`** | **`log clear`**]	
システム コンソールにログインする	`system console`	`system node run-console`
	システム コンソール セッションを終了するには、Ctrl-Dを使用します。	
ノードをオンまたはオフにするか、電源の再投入を行う（電源をオフにして再度オンにする）	`system power` **`on`**	*`system node power on`* （advanced権限レベル）
	`system power` **`off`**	
	`system power` **`cycle`**	
	スタンバイ電源は、SPが中断されることなく実行されるように、常に稼働しています。電源再投入の場合は、電源は一時的に停止したあと、再度オンになります。 **注意:** これらのコマンドを使用してノードの電源をオフにするか再投入すると、ノードが誤ってシャットダウンされる（*ダーティー シャットダウン*）場合があります。この方法は、Data ONTAPの`system node halt`コマンドを使用した正常なシャットダウンの代わりにはなりません。	

状況	使用するSPコマンド	またはData ONTAPコマンド
コア ダンプを作成してノードをリセットする	`system core [-f]` `-f`オプションを使用すると、強制的にコア ダンプが作成され、ノードがリセットがされます。	*`system node coredump trigger`* （advanced権限レベル）
	このコマンドの機能は、ノードでNon-maskable Interrupt（NMI）ボタンを押した場合と同じです。ノードがダーティー シャットダウンされ、ノードを停止する際にコア ファイルが強制的にダンプされます。これらのコマンドは、ノード上のData ONTAPがハングし、`system node shutdown`などのコマンドに応答しないときに役立ちます。生成されたコア ダンプ ファイルは、`system node coredump show`コマンドの出力に表示されます。SPは、ノードへの給電が遮断されないかぎり、継続して機能します。	
ノードのブート デバイスのイメージが壊れたなどの問題からリカバリするために、BIOSファームウェア イメージ（primary、backup、またはcurrent）をオプションで指定してノードをリブートする	`system reset {`**`primary`**`|`**`backup`**`|`**`current`**`}`	`system node reset -firmware {`**`primary`**`|`**`backup`**`|`**`current`**`}`パラメータを指定 （advanced権限レベル）
	注意: この処理を実行すると、ノードがダーティー シャットダウンされます。 BIOSファームウェア イメージを指定しない場合、最新のイメージを使用してリブートされます。SPは、ノードへの給電が遮断されないかぎり、継続して機能します。	
バッテリ ファームウェアの自動更新のステータスを表示するか、次回のSPブート時のバッテリ ファームウェアの自動更新を有効または無効にする	`system battery auto_update [`**`status`**`|`**`enable`**`|`**`disable`**`]` （advanced権限レベル）	
現在のバッテリ ファームウェアのイメージと指定したファームウェア イメージを比較する	`system battery verify [`*`image_URL`*`]` （advanced権限レベル） *`image_URL`*が指定されていない場合、比較にはデフォルトのバッテリ ファームウェア イメージが使用されます。	
指定した場所でイメージからバッテリ ファームウェアを更新する	`system battery flash` *`image_URL`* （advanced権限レベル） 何らかの理由でバッテリ ファームウェアの自動アップグレード プロセスに失敗した場合は、このコマンドを使用します。	
指定した場所でイメージを使用してSPファームウェアを更新する	`sp update` *`image_URL`* *`image_URL`*は200文字以内にする必要があります。	*`system service-processor image update`*

状況	使用するSPコマンド	またはData ONTAPコマンド
SPをリブートする	`sp reboot`	*`system service-processor reboot-sp`*
	注意: SPをバックアップ イメージからブートすることは避けてください。バックアップ イメージからのブートは、トラブルシューティングとリカバリの目的でのみ使用します。この場合、SPの自動ファームウェア更新の無効化が必要になることがあるため、推奨される設定ではありません。SPをバックアップ イメージからブートする前に、テクニカル サポートにお問い合わせください。	
NVRAMフラッシュ コンテンツを消去する	`system nvram flash clear` （advanced権限レベル） このコマンドは、コントローラの電源がオフのとき（`system power off`）には実行できません。	
SP CLIを終了する	`exit`	

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

しきい値ベースのSPセンサーの読み取り値とsystem sensorsコマンドのステータス値について

しきい値ベースのセンサーは、さまざまなシステム コンポーネントを定期的に計測します。SPは、しきい値ベースのセンサーの読み取り値と、事前に設定された制限値（コンポーネントで許容される動作状態を定義）を比較します。SPは、センサーの読み取り値に基づいてセンサーの状態を表示し、管理者はこの情報を使用してコンポーネントを監視することができます。

しきい値ベースのセンサーには、システム温度、電圧、電流、ファン速度のセンサーなどがあります。しきい値ベースのセンサーのリストは、プラットフォームによって異なります。

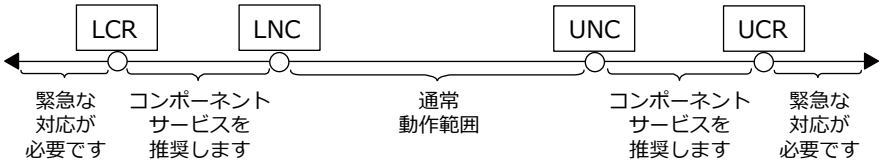
しきい値ベースのセンサーには次のしきい値があり、これらはSPの`system sensors`コマンドの出力に表示されます。

- 重大-下限（LCR）
- 異常-下限（LNC）
- 異常-上限（UNC）
- 重大-上限（UCR）

センサー読み取り値がLNCとLCRの間、またはUNCとUCRの間の場合は、コンポーネントが問題の兆候を示しており、その結果、システムに障害が発生する可能性があることを示しています。したがって、コンポーネントの保守をすぐに計画する必要があります。

センサーの読み取り値がLCR以下、またはUCR以上の場合は、コンポーネントが誤動作しており、システム障害が発生しつつあることを意味します。したがって、コンポーネントに対して緊急な対応が必要です。

次の図に、各しきい値と対応する重大度の範囲を示します。



しきい値ベースのセンサーの読み取り値は、system sensorsコマンド出力の[Current]列に表示されます。system sensors get *sensor_name*コマンドを使用すると、指定したセンサーに関するその他の情報が表示されます。読み取り値が正常および異常のしきい値を超えると、センサーは重大度が上昇していることを報告します。読み取り値が各しきい値を超えると、しきい値のレベルに応じてsystem sensorsコマンド出力に表示されるセンサーのステータスが、okからnc（異常）またはcr（重要）に変わり、SELイベント ログにイベント メッセージが記録されます。

しきい値ベースのセンサーには、4つのしきい値レベルが全部揃っていないものもあります。しきい値がない場合、system sensorsコマンド出力のしきい値欄にはnaと表示されます。この値は、そのセンサーに該当するしきい値または重大度が設定されていないことを意味し、SPはそのしきい値についてセンサーを監視しません。

system sensorsコマンド出力の例

次の例に、SP CLIのsystem sensorsコマンドで表示される情報を示します。

```
SP node1> system sensors

Sensor Name      | Current    | Unit       | Status| LCR        | LNC        | UNC        | UCR
-----------------+------------+------------+-------+------------+------------+------------+-----------
CPU0_Temp_Margin | -55.000    | degrees C  | ok    | na         | na         | -5.000     | 0.000
CPU1_Temp_Margin | -56.000    | degrees C  | ok    | na         | na         | -5.000     | 0.000
In_Flow_Temp     | 32.000     | degrees C  | ok    | 0.000      | 10.000     | 42.000     | 52.000
Out_Flow_Temp    | 38.000     | degrees C  | ok    | 0.000      | 10.000     | 59.000     | 68.000
PCI_Slot_Temp    | 40.000     | degrees C  | ok    | 0.000      | 10.000     | 56.000     | 65.000
NVMEM_Bat_Temp   | 32.000     | degrees C  | ok    | 0.000      | 10.000     | 55.000     | 64.000
LM56_Temp        | 38.000     | degrees C  | ok    | na         | na         | 49.000     | 58.000
CPU0_Error       | 0x0        | discrete   | 0x0180| na         | na         | na         | na
CPU0_Therm_Trip  | 0x0        | discrete   | 0x0180| na         | na         | na         | na
CPU0_Hot         | 0x0        | discrete   | 0x0180| na         | na         | na         | na
CPU1_Error       | 0x0        | discrete   | 0x0180| na         | na         | na         | na
CPU1_Therm_Trip  | 0x0        | discrete   | 0x0180| na         | na         | na         | na
CPU1_Hot         | 0x0        | discrete   | 0x0180| na         | na         | na         | na
IO_Mid1_Temp     | 30.000     | degrees C  | ok    | 0.000      | 10.000     | 55.000     | 64.000
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000      | 10.000     | 55.000     | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028      | 1.048      | 1.154      | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834      | 0.844      | 1.348      | 1.368
CPU1_VCC         | 1.086      | Volts      | ok    | 0.834      | 0.844      | 1.348      | 1.368
1.0V             | 0.989      | Volts      | ok    | 0.941      | 0.951      | 1.057      | 1.067
1.05V            | 1.048      | Volts      | ok    | 0.980      | 0.999      | 1.106      | 1.125
1.1V             | 1.096      | Volts      | ok    | 1.028      | 1.038      | 1.154      | 1.174
1.2V             | 1.203      | Volts      | ok    | 1.125      | 1.135      | 1.261      | 1.280
1.5V             | 1.513      | Volts      | ok    | 1.436      | 1.455      | 1.571      | 1.591
1.8V             | 1.754      | Volts      | ok    | 1.664      | 1.703      | 1.896      | 1.935
2.5V             | 2.543      | Volts      | ok    | 2.309      | 2.356      | 2.621      | 2.699
3.3V             | 3.323      | Volts      | ok    | 3.053      | 3.116      | 3.466      | 3.546
5V               | 5.002      | Volts      | ok    | 4.368      | 4.465      | 5.490      | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678      | 1.707      | 1.892      | 1.911
…
```

しきい値ベースのセンサーのsystem sensors get *sensor_name*コマンド出力の例

次の例に、しきい値ベースのセンサー5VについてSP CLIにsystem sensors get *sensor_name*コマンドを入力した結果を示します。

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID               : 5V (0x13)
 Entity ID              : 7.97
 Sensor Type (Analog)   : Voltage
 Sensor Reading         : 5.002 (+/- 0) Volts
 Status                 : ok
 Lower Non-Recoverable  : na
 Lower Critical         : 4.246
 Lower Non-Critical     : 4.490
 Upper Non-Critical     : 5.490
```

```
  Upper Critical        : 5.758
  Upper Non-Recoverable : na
  Assertion Events      :
  Assertions Enabled    : lnc- lcr- ucr+
  Deassertions Enabled  : lnc- lcr- ucr+
```

システム センサー コマンド出力でのディスクリートSPセンサーのステータス値について

ディスクリート センサーにはしきい値がありません。その値（SP CLIのsystem sensorsコマンド出力の[Current]列の下に表示）は、現実的な意味を持たないため、SPでは無視されます。system sensorsコマンド出力の[Status]列に、ディスクリート センサーのステータス値が16進形式で表示されます。

ディスクリート センサーには、ファン、Power Supply Unit（PSU;電源装置ユニット）エラー、システムエラー用のセンサーなどがあります。実際のディスクリート センサーは、プラットフォームによって異なります。

SP CLIのsystem sensors get *sensor_name*コマンドを使用すると、ほとんどのディスクリート センサーのステータス値を解釈できます。次の例に、ディスクリート センサーCPU0_ErrorおよびIO_Slot1_PresentにSystem sensors get *sensor_name*を実行した結果を示します。

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID              : CPU0_Error (0x67)
 Entity ID             : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted       : Digital State
                         [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                        [Device Present]
```

コマンドsystem sensors get *sensor_name*にはほとんどのディスクリート センサーのステータス情報が表示されますが、System_FW_Status、System_Watchdog、PSU1_Input_Type、およびPSU2_Input_Typeディスクリート センサーのステータス情報は表示されません。これらのセンサーのステータス情報は、次の情報を使用して解釈できます。

System_FW_Status

System_FW_Statusセンサーの状態は、0x*AABB*の形式で表示されます。センサーの状態を特定するには、*AA*と*BB*の情報を組み合わせます。

*AA*の値は次のいずれかです。

01

システム ファームウェアのエラー

02

システム ファームウェアのハング

04

システム ファームウェア進行中

*BB*の値は次のいずれかです。

00

システム ソフトウェアが正常にシャットダウンされました

01

メモリを初期化しています

02

NVMEMを初期化しています（NVMEMがある場合）

04

メモリ コントローラのハブ（MCH）値をリストアしています（NVMEMがある場合）

05

ユーザがセットアップに入りました

13

オペレーティング システムまたはLOADERを起動しています

1F

BIOSを起動しています

20

LOADERを実行しています

21

LOADERがプライマリBIOSファームウェアをプログラミングしています。システムの電源を切らないでください。

22

LOADERが代替BIOSファームウェアをプログラミングしています。システムの電源を切らないでください。

2F

Data ONTAPを実行しています

60

SPによってシステムの電源が切断されました

61

SPによってシステムに電源が入りました

62

SPによってシステムがリセットされました

63

SP watchdog電源サイクル

64

SP watchdogコールド リセット

たとえば、System_FW_Statusセンサーのステータス0x042Fは、「システム ファームウェアが進行中（04）で、Data ONTAPが実行中（2F）」という意味です。

System_Watchdog

System_Watchdogセンサーは、次の状態のいずれかです。

0x0080

このセンサーの状態は変更されていません

0x0081

タイマー割り込み

0x0180

タイマー期限切れ

0x0280

ハード リセット

0x0480

電源が切れています

0x0880

電源サイクル

たとえば、System_Watchdogセンサーのステータス0x0880は、watchdogタイムアウトが発生したことを意味し、システムの再投入につながります。

PSU1_Input_TypeおよびPSU2_Input_Type

直流（DC）電源の場合、PSU1_Input_TypeおよびPSU2_Input_Typeセンサーは適用されません。交流（AC）電源の場合、センサーのステータスは次の値のいずれかです。

0x01*xx*

220V PSUタイプ

0x02*xx*

110V PSUタイプ

たとえば、PSU1_Input_Typeセンサーのステータス0x0280は、PSUタイプが110Vであるとセンサーが報告していることを意味します。

Data ONTAPからのSPの管理用コマンド

Data ONTAPには、SPネットワーク設定、SPファームウェア イメージ、SPへのSSHアクセス、一般的なSPの管理など、SPを管理するためのコマンドが用意されています。

SPネットワーク設定の管理用コマンド

状況	使用するData ONTAPコマンド
SPの自動ネットワーク設定を有効にして、指定されたサブネットのIPv4またはIPv6アドレス ファミリーを使用する	*system service-processor network auto-configuration enable*
指定されたサブネットのIPv4またはIPv6アドレス ファミリーを使用する、SPの自動ネットワーク設定を無効にする	*system service-processor network auto-configuration disable*
SPの自動ネットワーク設定を表示する	*system service-processor network auto-configuration show*

状況	使用するData ONTAPコマンド
ノードのSPネットワークに対して、次の項目を手動で設定する • IPアドレス ファミリー（IPv4またはIPv6） • 指定したIPアドレス ファミリーのネットワーク インターフェイスを有効にするかどうか • IPv4を使用している場合、DHCPサーバからのネットワーク設定と、指定のネットワーク アドレスのどちらを使用するか • SPのパブリックIPアドレス • SPのネットマスク（IPv4を使用している場合） • SPのサブネット マスクのネットワーク プレフィックス長（IPv6を使用している場合） • SPのゲートウェイIPアドレス	*system service-processor network modify*
次のようなSPネットワーク設定を表示する • 設定されているアドレス ファミリー（IPv4またはIPv6）、およびそれが有効かどうか • リモート管理デバイスのタイプ • 現在のSPのステータスとリンクのステータス • ネットワーク設定（IPアドレス、MACアドレス、ネットマスク、サブネット マスクのプレフィックス長、ルータが割り当てたIPアドレス、リンクのローカルIPアドレス、ゲートウェイIPアドレスなど） • 前回SPが更新された時刻 • SPの自動設定に使用されるサブネットの名前 • ルータが割り当てたIPv6 IPアドレスが有効かどうか • SPネットワークのセットアップ ステータス • SPネットワークのセットアップ エラーの原因	*system service-processor network show* SPネットワークの詳細をすべて表示するには、`-instance`パラメータを指定します。
次のSP APIサービス設定を変更する • SP APIサービスで使用されるポートの変更 • SP APIサービスの有効化または無効化	*system service-processor api-service modify* （advanced権限レベル）
SP APIサービス設定を表示する	*system service-processor api-service show* （advanced権限レベル）

状況	使用するData ONTAPコマンド
SP APIサービスの内部通信に使用されるSSL証明書およびSSH証明書を更新する	*system service-processor api-service renew-certificates* （advanced権限レベル）

SPファームウェア イメージの管理用コマンド

状況	使用するData ONTAPコマンド
現在インストールされているSPファームウェア イメージの次の詳細を表示する • リモート管理デバイスのタイプ • SPがブートされるイメージ（primaryまたはbackup）とそのステータス、およびファームウェア バージョン • ファームウェアの自動更新が有効かどうかと、最新の更新ステータス	*system service-processor image show* `-is-current`パラメータは、インストールされているファームウェアのバージョンが最新かどうかではなく、SPが現在ブートされているイメージ（primaryまたはbackup）を示します。
SPの自動ファームウェア更新を有効または無効にする	*system service-processor image modify* デフォルトでは、SPファームウェアは、Data ONTAPの更新時、またはSPファームウェアの新しいバージョンを手動でダウンロードしたときに、自動で更新されます。自動更新を無効にすると、Data ONTAPイメージとSPファームウェア イメージの組み合わせが最適でなくなる、または無効になる場合があるため、無効にしないことを推奨します。
ノードにSPファームウェア イメージを手動でダウンロードする	*system node image get* SPファームウェア イメージはData ONTAPに同梱されています。Data ONTAPに同梱されているSPファームウェアとは異なるバージョンを使用する場合を除き、SPファームウェアを手動でダウンロードする必要はありません。

状況	使用するData ONTAPコマンド
次の項目を指定して、SPファームウェアを手動で更新する • 使用するSPファームウェア パッケージ パッケージ ファイル名を指定すると、SPで特定のSPファームウェア パッケージを使用できます。`system node image package show`コマンドは、ノード上で使用可能なすべてのパッケージ ファイルを表示します（SPファームウェア パッケージのファイルを含む）。 • インストールのベースライン SPファームウェアを、現在実行しているバージョンのData ONTAPに付属しているベースラインのバージョンに更新できます。 • ネットワーク インターフェイスまたはシリアル インターフェイスを使用して、ファームウェア イメージ全体を更新するか、変更部分のみを更新するか • ファームウェア イメージ全体を更新する場合は、ログ設定も工場出荷時のデフォルトにリセットし、イベント ログ、IPMIログ、フォレンジック ログなど、SPで保持されているすべてのログの内容を消去するかどうか	*system service-processor image update*
Data ONTAPからトリガーされた最新のSPファームウェア更新に関し、以下を含むステータスを表示する • 最新のSPファームウェア更新の開始時刻と終了時刻 • 更新が進行中かどうかと、進行状況（%）	*system service-processor image update-progress show*

SPへのSSHアクセスの管理用コマンド

状況	使用するData ONTAPコマンド
指定したIPアドレスにのみSPへのアクセス権を付与する	*system service-processor ssh add-allowed-addresses*
指定したIPアドレスにSPへのアクセスを禁止する	*system service-processor ssh remove-allowed-addresses*
SPにアクセスできるIPアドレスを表示する	*system service-processor ssh show*

一般的なSP管理コマンド

状況	使用するData ONTAPコマンド
次のようなSPの一般情報を表示する • リモート管理デバイスのタイプ • 現在のSPのステータス • SPネットワークが設定されているかどうか • パブリックIPアドレスやMACアドレスなどのネットワーク情報 • SPファームウェアのバージョンとIntelligent Platform Management Interface（IPMI）のバージョン • SPファームウェアの自動更新が有効かどうか	*system service-processor show* SPの情報をすべて表示するには、-instance パラメータを指定します。
ノードでSPをリブートし、使用するSPファームウェア イメージ（プライマリまたはバックアップ）を必要に応じて指定する	*system service-processor reboot-sp* **注意:** SPをバックアップ イメージからブートすることは避けてください。バックアップ イメージからのブートは、トラブルシューティングとリカバリの目的でのみ使用します。この場合、SPの自動ファームウェア更新の無効化が必要になることがあるため、推奨される設定ではありません。SPをバックアップ イメージからブートする前に、テクニカル サポートにお問い合わせください。
指定したノードから収集されたSPログ ファイルを含むAutoSupportメッセージを生成して送信する	*system node autosupport invoke-splog*
クラスタ内で収集されたSPログ ファイルの割り当てマップを表示する（収集する各ノードに格納されているSPログ ファイルのシーケンス番号を含む）	*system service-processor log show-allocations*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

SVMの管理（クラスタ管理者のみ）

クラスタ管理者は、クラスタ内のStorage Virtual Machine（SVM、旧Vserver）を管理できます。クラスタがクライアントにデータを提供するためには、少なくとも1つのSVMが必要です。したがって、クラスタ管理者はSVMを作成して管理する必要があります。

クラスタ管理者は、SVM運用管理タスクとSVM管理タスクの両方を行うか、それともSVMの管理はSVM管理者に委譲するかを選択できます。

SVMを管理するには、SVMとは何か、無停止運用や拡張性などの利点、および関連付けられた管理タスクを理解する必要があります。

クラスタ管理者は、次のSVM管理タスクを実行できます。

- SVMの作成
- SVMの変更
- SVMの削除
- SVMの名前変更
- SVMコンテキストからのSVMの管理
- SVMの起動と停止

注: クラスタ管理者とSVM管理者の両方が、SVMについての情報を表示できます。

注: Data ONTAPのコマンドライン インターフェイス（CLI）では、コマンドやパラメータ名が`vserver`のまま変更されておらず、出力にもこれまでどおり*Vserver*と表示されます。

関連コンセプト

SVMの管理（112ページ）

SVMとは

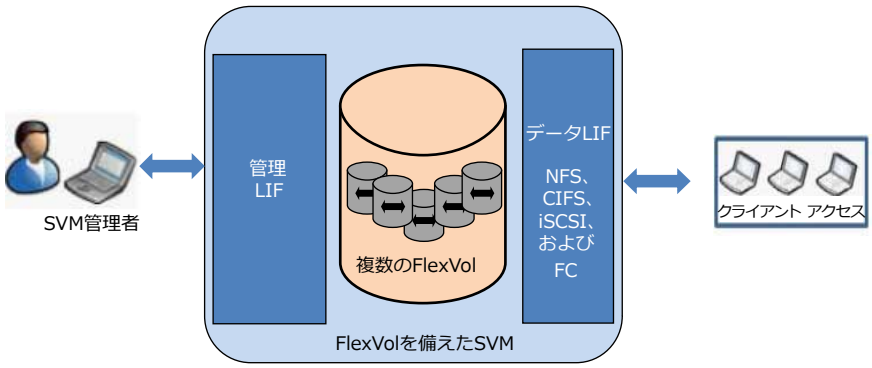
Storage Virtual Machine（SVM、旧Vserver）には、複数のデータ ボリュームと、クライアントへのデータの提供に使用するLIFが1つ以上含まれます。clustered Data ONTAP 8.1.1以降のSVMには、1つ以上のFlexVol、または1つのInfinite Volumeを含めることができます。

SVMは共有されている仮想データ ストレージおよびネットワークを安全に分離し、クライアントにはそれぞれのSVMが単一の専用サーバとして認識されます。各SVMには独立した管理者認証ドメインがあり、SVM管理者による個別管理が可能です。

クラスタでは、SVMがデータ アクセスを提供します。データをやり取りするために、クラスタでは少なくとも1つのSVMが必要です。SVMは、クラスタのストレージおよびネットワーク リソースを使用します。ただし、ボリュームとLIFはSVM専用です。1つのクラスタ内に複数のSVMが共存でき、クラスタ内のどのノードにバインドされることもありません。ただし、所属している物理クラスタには紐付けられます。

各クラスタには、FlexVolを備えたSVMとInfinite Volumeを備えたSVMを1つ以上配置できます。

FlexVolを備えたSVM

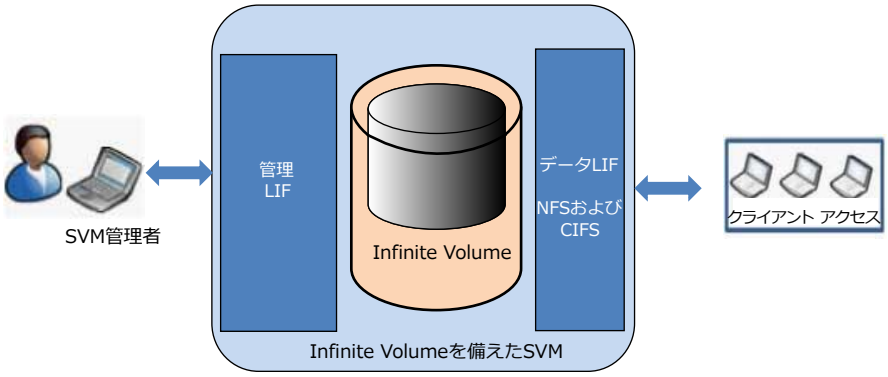


NAS環境内のFlexVolを備えたSVMは、それぞれが1つのディレクトリ階層として表示され、一意のネームスペースが割り当てられます。ネームスペースを使用することで、NASクライアントはデータの物理的な場所を指定することなくデータにアクセスできます。また、クラスタおよびSVMの管理者は、分散されたデータ ストレージを、複数の階層からなる単一のディレクトリとして管理できます。

NASの各SVM内のボリュームはジャンクションによって相互に関連付けられ、ジャンクション パスにマウントされます。これらのジャンクションは、各ボリューム内のファイルシステムを表します。SVMのルート ボリュームはネームスペース階層の最上位に位置するFlexVolで、その他のボリュームはSVMのルート ボリュームにマウントされてネームスペースを拡張します。SVMにボリュームが作成されると、SVMのルート ボリュームにジャンクション パスが追加されます。

FlexVolを備えたSVMには、ファイルとLUNを含めることができます。このSVMは、NASクライアントにはNFSプロトコルとCIFSプロトコルを使用してファイルレベルのデータ アクセスを提供し、SANホストにはiSCSIプロトコルとFibre Channel（FC;ファイバチャネル）プロトコル（FCoEが含まれる）を使用してブロックレベルのデータ アクセスを提供します。

Infinite Volumeを備えたSVM



Infinite Volumeを備えたSVMには、データを提供するInfinite Volumeを1つだけ含めることができます。Infinite Volumeを備えたSVMに含まれるジャンクション パスは1つで、デフォルト値は/NSです。このジャンクションは、Infinite Volumeを備えたSVMが提供する大規模なネームスペースに対して単一のマウント ポイントを提供します。Infinite Volumeを備えたSVMにジャンクションを追加することはできません。ただし、Infinite Volumeのサイズを拡張することはできます。

Infinite Volumeを備えたSVMが格納できるのはファイルだけです。このタイプのSVMは、NFSプロトコルとCIFSプロトコルを使用してファイルレベルのデータ アクセスを提供します。Infinite Volumeを備えたSVMにLUNを含めることはできず、ブロックレベルのデータ アクセスは提供されません。

注: Data ONTAPのコマンドライン インターフェイス（CLI）では、コマンドやパラメータ名が `vserver`のまま変更されておらず、出力にもこれまでどおり*Vserver*と表示されます。

SVMルート ボリュームがデータ アクセスに使用される仕組み

すべてのStorage Virtual Machine（SVM）には、データ ボリュームがネームスペースに結合されるパスを含むルート ボリュームがあります。NASクライアントのデータ アクセスは、ネームスペース内のルート ボリュームの健常性に依存しますが、SANクライアントのデータ アクセスは、ネームスペース内のルート ボリュームの健常性に依存しません。

ルート ボリュームは、SVMによって提供されるネームスペースへのエントリ ポイントとして機能します。SVMのルート ボリュームはネームスペース階層の最上位に位置するFlexVolで、マウント ポイントとして使用されるディレクトリと、データ ボリュームがネームスペースに結合されるパスが含まれています。

SVMネームスペースのルート ボリュームが万一使用できない場合、NASクライアントは、ネームスペース階層にアクセスできないためネームスペース内のデータにアクセスできません。このため、ノードに障害やフェイルオーバーが発生したときに引き続きネームスペース ディレクトリ情報を使用できるようにするために、クラスタの各ノード上にルート ボリュームの負荷共有ミラー コピーを作成することを推奨します。

ユーザ データはSVMのルート ボリュームに格納しないでください。SVMのルート ボリュームはジャンクション パスに使用し、ユーザ データはSVMのルート以外のボリュームに格納する必要があります。

SVMの種類

クラスタは、クラスタとそのリソースの管理、およびクライアントとアプリケーションへのデータ アクセスを支援する3種類のSVMで構成されます。

クラスタには、次の種類のSVMが含まれます。

- 管理SVM
  クラスタのセットアップ プロセスでは、クラスタ用の管理SVMが自動的に作成されます。管理SVMはクラスタを表します。
- ノードSVM
  ノードSVMは、ノードがクラスタに追加されると作成され、ノードSVMはクラスタの個別のノードを表します。
- システムSVM（アドバンスト）
  システムSVMは、クラスタレベルの通信用にIPspace内に自動的に作成されます。
- データSVM
  データSVMは、データを提供するSVMを表します。クラスタのセットアップ後、クラスタ管理者はデータSVMを作成し、作成したSVMにボリュームを追加して、クラスタからのデータ アクセスを可能にする必要があります。
  クラスタがクライアントにデータを提供するためには、少なくとも1つのデータSVMが必要です。

注: 特に指定がないかぎり、SVMという用語はデータ（データ提供用）SVMを指します。これは、FlexVolを備えたSVMとInfinite Volumeを備えたSVMの両方に適用されます。

CLIでは、SVMはVserverと表示されます。

SVMの使用目的

Storage Virtual Machine（SVM、旧Vserver）は、他のあらゆるストレージ システムと同様に、物理ストレージかコントローラかにかかわらず、クライアントにデータ アクセスを提供します。SVMには、ノ

ンストップ オペレーション、優れた拡張性、セキュリティ、ユニファイド ストレージなどの利点があります。

SVMには次の利点があります。

- マルチテナンシー
  SVMは、セキュア マルチテナンシーの基本ユニットであり、ストレージ インフラをパーティショニングすることで、複数の独立したストレージ システムが存在するように見せることができます。これらのパーティションでは、データと管理が分離されます。
- ノンストップ オペレーション
  SVMは、必要なかぎり継続的に無停止で稼働できます。SVMを使用すると、ソフトウェアとハードウェアのアップグレード、ノードの追加と削除、およびすべての管理操作中もクラスタを継続的に稼働できるようになります。
- 優れた拡張性
  SVMは、オンデマンド データ スループットなどのストレージ要件を満たします。
- セキュリティ
  SVMはそれぞれ単一の独立したサーバとみなされるため、複数のSVMを相互にデータフローがない状態でクラスタ内に共存させることができます。
- ユニファイド ストレージ
  SVMは、複数のデータ アクセス プロトコルを使用して同時にデータをやり取りできます。SVMは、CIFSやNFSなどのNASプロトコルでファイルレベルのデータ アクセスを提供し、iSCSIやFC（FCoEを含む）などのSANプロトコルでブロックレベルのデータ アクセスを提供します。SVMは、SANクライアントとNASクライアントそれぞれに同時にデータを提供できます。

  注: Infinite Volumeを備えたSVMで使用できるのは、NFSおよびCIFSプロトコルのみです。

- 管理の委譲
  SVMには、それぞれにユーザおよび管理者認証を設定できます。SVM管理者は、自身がアクセス権を付与されているSVMを管理できます。ただしSVM管理者には、クラスタ管理者によって割り当てられた権限があります。
- 大規模なデータセットの管理が簡単
  Infinite Volumeを備えたSVMを使用すると、SVM管理者がデータ コンテナを複数ではなく1つだけ管理すれば済むため、大規模な非構造化データの管理が簡単になります。

クラスタ内のSVM数

クラスタ内に作成できるSVMの数は、ノード数、およびLIFがクラスタでどのように設定され、使用されているかによって異なります。

1つのクラスタ内の最大ノード数は、プラットフォーム モデルおよびライセンス プロトコルによって異なります。クラスタ内のノード数の詳細については、*Hardware Universe*（*hwu.netapp.com*）を参照してください。

設定されているLIFの数に基づいた、クラスタの推奨SVM数を次の表に示します。

SVMのプロトコル種類	クラスタあたりのノード数						SVM設定
	1	2	4	6	8	10-24	
NFS / CIFSプロトコルのSVM：データ用および管理用の単一のLIF	125	250	500	750	1000	1000	各SVMがデータ用および管理用にアクティブなIP LIFを1つ、フェイルオーバー用に予約されたIP LIFを1つ持つ

SVMのプロトコル種類	クラスタあたりのノード数						SVM設定
	1	2	4	6	8	10-24	
FC / FCoEプロトコルのSVM:データ用LIF 1つ、管理用LIF 1つ	125	250	250	250	250	N/A	各SVMがクラスタのノードごとにFC / FCoE LIFを2つ、管理専用IP LIFを1つ持つ
iSCSIプロトコルのSVM:データ用LIF 1つ、管理用LIF 1つ	125	125	165	190	200	N/A	各SVMがクラスタのノードごとにiSCSI LIFを1つ、管理専用IP LIFを1つ持つ

SANが設定されたSVMがクラスタに含まれている場合、Infinite Volumeを備えたSVMを作成することはできません。

Infinite Volumeを備えたSVMは、NASクラスタ内の10を超えるノードにまたがることはできません。

注: プロトコルが異なるSVMの組み合わせがクラスタに存在する場合は、クラスタ内のSVMの数が同じにならないことがあります。

SVMのセットアップ

SVMの各サブタイプは、データ アクセス、災害からのデータ保護、およびデータの高可用性を提供します。クラスタごとに少なくとも1つのデータ アクセスSVMを設定する必要があります。そのためにはセットアップの計画、要件の把握、セットアップ ワークシートの作成、およびSVMの作成と設定が必要です。

SVMの作成計画

SVMのさまざまな側面を理解することが、SVMのセットアップ プロセスを計画するうえで必要になります。また、SVMを作成する目的を理解し、SVMに格納する必要があるボリュームの種類、データ アクセス環境、ネットワーク分離などの詳細を把握する必要もあります。

データ アクセス用のSVM

クラスタからデータを提供するためには、SVMを作成する必要があります。SVMには、クライアントにデータを提供するためのFlexVolを1つ以上、またはInfinite Volumeを1つ含めることができます。

OnCommand System Managerを使用して、FlexVolを備えたSVMおよびInfinite Volumeを備えたSVMを作成および設定することもできます。

clustered Data ONTAP 8.3 OnCommand System Managerを使用したクラスタ管理

データ アクセス用にFlexVolを備えたSVMを作成する際には、SVMの次の属性を理解しておく必要があります。

SVM属性	有効値	説明
SVMサブタイプ	default	データ アクセス用に作成するデータSVMは、`subtype`オプションを**`default`**に設定する必要があります。
ボリューム	FlexVol	`-is-repository`オプションは**`false`**(デフォルト値)に設定する必要があります。
プロトコル	NFS、CIFS、iSCSI、FC	データSVMは、データをNASクライアントとSANホストに同時に提供できます。

SVM属性	有効値	説明
ルート ボリュームのセキュリティ形式	• NFSおよびCIFS：mix • CIFS：ntfs • NFS、iSCSI、FC：unix	SVMルート ボリュームには、クライアントに応じたセキュリティ形式を選択します。
IPspace	任意のIPspace	IPspaceは、各SVMに対するセキュアな専用ネットワーク パスを定義します。 SVMの作成時にIPspaceを割り当てることで、SVM用のネットワークを分離できます。

データ アクセス用にInfinite Volumeを備えたSVMを作成する際には、SVMの次の属性を理解しておく必要があります。

SVM属性	有効値	説明
SVMサブタイプ	default	データ アクセス用に作成するデータSVMは、`subtype`オプションを**`default`**に設定する必要があります。
ボリューム	Infinite Volume	`-is-repository`オプションは**`true`**に設定する必要があります。デフォルト値は**`false`**です。
プロトコル	• NFS NFSv3、pNFS、NFSv4.1がサポートされています。 • CIFS SMB 1.0がサポートされています。	データSVMは、NASクライアントのみにデータを提供できます。
ルート ボリュームのセキュリティ形式	• NFSおよびCIFS：mix • CIFS：ntfs • NFS：unix	SVMルート ボリュームには、クライアントに応じたセキュリティ形式を選択します。
IPspace	任意のIPspace	IPspaceは、各SVMに対するセキュアな専用ネットワーク パスを定義します。 SVMの作成時にIPspaceを割り当てることで、SVM用のネットワークを分離できます。

ディザスタ リカバリのデスティネーションSVM

SVMをディザスタ リカバリのデスティネーションとして作成し、ソース（データ アクセス）SVMのデータおよび設定情報をレプリケートできます。

注: ディザスタ リカバリでサポートされるのは、FlexVolを備えたSVMだけです。

ディザスタ リカバリ用にSVMを作成する際には、SVMの次の属性を理解しておく必要があります。

SVM属性	有効値	説明
SVMサブタイプ	dp-destination	ディザスタ リカバリ用に作成するデスティネーションSVMは、subtypeオプションを**dp-destination**に設定する必要があります。
ボリューム	FlexVol	デフォルト値は**false**であるため、-is-repositoryオプションを指定する必要はありません。
プロトコル	NFS、CIFS、iSCSI、FC	ディザスタ リカバリ用に設定されたSVMでは、ソースSVMに設定されたプロトコルがサポートされます。
ルート ボリュームのセキュリティ形式	• NFSおよびCIFS：mix • CIFS：ntfs • NFS、iSCSI、FC：unix	デスティネーションSVMの作成時には、ルート ボリュームは設定されません。初回のベースライン転送で、ソースSVMのルート ボリュームが、ルート ボリュームのセキュリティ形式と一緒にデスティネーションSVMにレプリケートされます。
IPspace	任意のIPspace	IPspaceは、各SVMに対するセキュアな専用ネットワーク パスを定義します。 SVMの作成時にIPspaceを割り当てることで、SVM用のネットワークを分離できます。 デスティネーションSVMには、ソースSVMのIPspaceに関係なく、使用可能な任意のIPspaceまたはデフォルトIPspaceを設定できます。

MetroCluster構成用のSVM

MetroCluster構成用のソースおよびデスティネーションStorage Virtual Machine（SVM）を作成して、データの同期ディザスタ リカバリおよび高可用性を実現できます。

注: MetroCluster構成でサポートされるのは、FlexVolを備えたSVMだけです。

MetroCluster構成用にSVMを作成する際には、SVMの次の属性を理解しておく必要があります。

SVM属性	有効値	説明
SVMサブタイプ	sync-sourceおよびsync-destination	MetroCluster構成のために作成されるソースおよびデスティネーションSVMは、subtypeオプションをそれぞれ**sync-source**または**sync-destination**に設定する必要があります。
ボリューム	FlexVol	デフォルト値は**false**であるため、-is-repositoryオプションを指定する必要はありません。
プロトコル	NFS、CIFS、iSCSI、FC	ソースおよびデスティネーションSVMはすべてのプロトコルをサポートします。

SVM属性	有効値	説明
ルート ボリュームのセキュリティ形式	• NFSおよびCIFS：mix • CIFS：ntfs • NFS、iSCSI、FC：unix	ソースとデスティネーションSVMのルート ボリュームは、同じセキュリティ形式にする必要があります。
IPspace	任意のIPspace	IPspaceは、各SVMに対するセキュアな専用ネットワーク パスを定義します。 SVMの作成時にIPspaceを割り当てることで、SVM用のネットワークを分離できます。 ソースおよびデスティネーションSVMは、同じ名前のIPspaceに属している必要があります。

SVMの作成に関するガイドライン

SVMを作成する際には、命名に関するガイドラインと、言語およびIPspaceに関する考慮事項を理解しておく必要があります。

SVMの命名ガイドライン

- SVM名は、クラスタ間で一意である必要があります。
  SVMの完全修飾ドメイン名（FQDN）を使用するか、クラスタ間でSVM名を一意にするためのその他の命名規則を使用してください。
- SVM名の最大文字数は47文字です。
  ただし、MetroCluster構成のSVMの場合は、最大41文字です。
- SVM名では大文字と小文字が区別され、英数字を使用できます。
  SVM名にはピリオド（.）、ハイフン（-）、アンダースコア（_）を使用できますが、1文字目をハイフン、ピリオド、または数字にすることはできません。

言語に関する考慮事項

デフォルトの言語設定は**C.UTF-8**（**POSIX.UTF-8**）で、すべてのボリュームにこの設定が継承されます。ボリュームの作成時に別の言語を指定できます。

SVMの言語を変更すると、デフォルトの言語設定が変更されますが、既存のボリュームの言語設定は変更されません。

言語のエンコード値には.UTF-8を付加してください。たとえば、en_USを指定する場合、推奨される形式はen_US.UTF-8です。

注: Infinite Volumeを備えたSVMの言語をあとから変更することはできません。

IPspaceに関する考慮事項

SVMの作成時には、IPspaceをSVMに割り当てる必要があります。SVMのIPspaceはあとから変更または削除できません。

言語オプション一覧

Storage Virtual Machine（SVM）の作成時にSVMの言語を設定します。SVMの言語により、そのSVMのボリュームのデフォルト言語設定が決定されます。SVMの言語は変更できます。

ボリュームの作成時にボリュームの言語を指定し、SVMの言語とは異なる言語にすることができます。ボリュームの言語を指定しなかった場合は、SVMの言語設定が継承されます。ボリュームを作成したあとで、ボリュームの言語を変更することはできません。したがって、利用可能な言語オプションを確認しておく必要があります。

次の表に、さまざまな利用可能言語オプションを示します。この表を利用すれば、SVMまたはボリュームの作成時に正しい値を選択して入力することが容易になります。

言語の値	言語
c	POSIX
C.UTF-8	POSIX（UTF-8）
ar	アラビア語
ar.UTF-8	アラビア語（UTF-8）
cs	チェコ語
cs.UTF-8	チェコ語（UTF-8）
da	デンマーク語
da.UTF-8	デンマーク語（UTF-8）
de	ドイツ語
de.UTF-8	ドイツ語（UTF-8）
en	英語
en.UTF-8	英語（UTF-8）
en_us	英語（US）
en_US.UTF-8	英語（US）（UTF-8）
es	スペイン語
es.UTF-8	スペイン語（UTF-8）
fi	フィンランド語
fi.UTF-8	フィンランド語（UTF-8）
fr	フランス語
fr.UTF-8	フランス語（UTF-8）
he	ヘブライ語
he.UTF-8	ヘブライ語（UTF-8）
hr	クロアチア語
hr.UTF-8	クロアチア語（UTF-8）
hu	ハンガリー語
hu.UTF-8	ハンガリー語（UTF-8）
it	イタリア語

言語の値	言語
it.UTF-8	イタリア語（UTF-8）
ja_v1	日本語（euc-j）
ja_v1.UTF-8	日本語（euc-j）（UTF-8）
ja_jp.pck_v2	日本語PCK（sjis）
ja_JP.PCK_v2.UTF-8	日本語PCK（sjis）（UTF-8）
ko	韓国語
ko.UTF-8	韓国語（UTF-8）
no	ノルウェー語
no.UTF-8	ノルウェー語（UTF-8）
nl	オランダ語
nl.UTF-8	オランダ語（UTF-8）
pl	ポーランド語
pl.UTF-8	ポーランド語（UTF-8）
pt	ポルトガル語
pt.UTF-8	ポルトガル語（UTF-8）
ro	ルーマニア語
ro.UTF-8	ルーマニア語（UTF-8）
ru	ロシア語
ru.UTF-8	ロシア語（UTF-8）
sk	スロバキア語
sk.UTF-8	スロバキア語（UTF-8）
sl	スロベニア語
sl.UTF-8	スロベニア語（UTF-8）
sv	スウェーデン語
sv.UTF-8	スウェーデン語（UTF-8）
tr	トルコ語
tr.UTF-8	トルコ語（UTF-8）
zh	簡体字中国語
zh.UTF-8	簡体字中国語（UTF-8）
zh.GBK	簡体字中国語（GBK）
zh.GBK.UTF-8	簡体字中国語（GBK）（UTF-8）
zh_TW	繁体字中国語（euc-tw）
zh_TW.UTF-8	繁体字中国語（euc-tw）（UTF-8）
zh_TW.BIG5	繁体字中国語（Big 5）
zh_TW.BIG5.UTF-8	繁体字中国語（Big 5）（UTF-8）

言語設定

ファイル名が正しく表示されるためには、Storage Virtual Machine（SVM）またはボリュームの言語設定とクライアントの言語設定が一致している必要があります。言語設定が一致していないと、ファイル名に間違った文字が含まれる可能性があります。

次の表に、各種クライアントについて、エンコードの種類に応じた言語設定を記載します。

クライアントのプロトコル	クライアントのエンコードの種類	言語設定
Win95 / 98 / MEで実行されているCIFS	ISO 8859-1	Non-UTF-8クライアント ロケールに一致させます。「en_US」のUTF-8は追加しません。
WinNT 3.1以降で実行されているCIFS	UCS-2	他のクライアントでNon-UTF-8ロケールが使用されない場合は、UTF-8クライアント ロケールに一致させます。「en_US.UTF-8」のUTF-8を追加します。 他のクライアントでNon-UTF-8ロケールが使用される場合は、Non-UTF-8クライアント ロケールに一致させます。「en_US」のUTF-8は追加しません。
NFSv2 / 3	Non-UTF-8クライアント ロケール	Non-UTF-8クライアント ロケールに一致させます。「en_US」のUTF-8は追加しません。
NFSv4	UTF-8	他のクライアントでNon-UTF-8ロケールが使用されない場合は、UTF-8クライアント ロケールに一致させます。「en_US.UTF-8」のUTF-8を追加します。 他のクライアントでNon-UTF-8ロケールが使用される場合は、Non-UTF-8クライアント ロケールに一致させます。「en_US」のUTF-8は追加しません。
FCまたはiSCSI		UTF-8を推奨します。C / POSIXも許容されます。

注: SVMのデフォルトの言語設定はC.UTF-8です。

FlexVolを備えたSVMの作成

クラスタがデータ アクセスを提供するためには、クラスタにSVMが少なくとも1つ必要です。FlexVolを備えたSVMを作成して、NASクライアントおよびSANホストにデータ アクセスを提供できます。デ

ィザスタ リカバリおよび高可用性を提供するためにFlexVolを備えたSVMを作成することもできます。

開始する前に

事前に計画要件を確認し、ガイドラインを理解しておく必要があります。

- *SVMの作成計画*
- *SVMの作成に関するガイドライン*

次の要件が満たされていることを確認します。

- 十分なスペースがある、ルートではないアグリゲートが、少なくとも1つクラスタに含まれている必要があります。
- SVMのルート ボリュームのアグリゲートに、1GB以上のスペースが必要です。
- CIFSの作成および認証エラーが起きないよう、NTPを設定および有効にしてクラスタを同期しておく必要があります。
- IPspaceを割り当てる場合、IPspaceを作成しておく必要があります。
- MetroCluster構成の場合、ローカル サイトとリモート サイトが設定されている必要があります。

タスク概要

異なるSSHセッションを使用するか、スクリプトを使用することで、複数のSVMを同時に作成できます。

注: パフォーマンスの低下を避けるため、同時に作成するSVMは5個以下にすることを推奨します。

選択肢

- データ アクセス用のFlexVolを備えたSVMの作成（87ページ）
- ディザスタ リカバリのデスティネーションSVMの作成（88ページ）
- MetroCluster構成用SVMの作成（89ページ）

関連コンセプト

クラスタ時間の管理（クラスタ管理者のみ）（166ページ）

関連タスク

SVM管理者への管理の委譲（95ページ）
SVMに関する情報の表示（100ページ）

データ アクセス用のFlexVolを備えたSVMの作成

クライアントにデータ アクセスを提供するには、クラスタ内に少なくとも1つSVMを作成する必要があります。

手順

1. サブタイプを**`default`**に指定し、`is-repository`パラメータを**`false`**に指定して、`vserver create`コマンドを実行します。

例

次のコマンドを実行すると、データ アクセス用のFlexVolを備えたSVMがIPspace ipspaceA内に作成されます。

```
cluster1::>vserver create -vserver vs0.example.com -subtype default -
rootvolume root_vs0 -aggregate
aggr1 -rootvolume-security-style unix -language C.UTF-8 -is-
repository false -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

2. `vserver show`コマンドを使用して、新しく作成したSVMのステータスを確認します。

例

```
cluster1::> vserver show
                               Admin      Operational   Root
Vserver          Type    Subtype    State      State         Volume     Aggregate
-------          -----   -------    -------   --------     ----------- ----------
cluster1         admin     -         -           -             -           -
cluster1-01      node      -         -           -             -           -
vs0.example.com  data    default    running   running       root_vs0      aggr1
```

SVMの作成がルート ボリュームの作成などの中間処理が原因で失敗した場合、SVMは`initializing`状態になります。その場合、SVMを削除して再度作成する必要があります。

タスクの結果

SVMが1GBのルート ボリュームで作成され、自動的に起動して`running`状態になります。デフォルトでは、vsadminユーザ アカウントが作成され、`locked`状態になります。vsadminロールがデフォルトのvsadminユーザ アカウントに割り当てられます。

終了後の操作

データ提供用SVMにデータ アクセスを設定する必要があります。

関連タスク

SVMの設定(92ページ)

ディザスタ リカバリのデスティネーションSVMの作成

デスティネーションSVMを作成すると、データと設定情報をデスティネーションSVMにレプリケートすることによって、データを提供しているSVMを保護できます。

開始する前に

十分なスペースがある、ルートではないアグリゲートが、少なくとも1つクラスタに含まれている必要があります。

手順

1. サブタイプに**`dp-destination`**を指定して`vserver create`コマンドを実行します。

例

次のコマンドを実行すると、ディザスタ リカバリのデスティネーションSVMがデフォルトのIPspace内に作成されます。

```
cluster2::>vserver create -vserver dvs0.example.com -subtype dp-
destination

[Job 3220] Job succeeded:
Vserver creation completed
```

2. `vserver show`コマンドを使用して、新しく作成したSVMのステータスを確認します。

   注: SVMの作成がルート ボリュームの作成などの中間処理が原因で失敗した場合、SVMは`initializing`状態になります。その場合、SVMを削除して再度作成する必要があります。

   例

```
cluster2::> vserver show
                                                Admin    Operational   Root
Vserver           Type    Subtype              State    State         Volume     Aggregate
-------           -----   -------             -------   --------     ----------- ----------
cluster1          admin     -                    -          -           -           -
cluster1-01       node      -                    -          -           -           -
dvs0.example.com  data    dp-destination      running   stopped         -           -
```

タスクの結果

ルート ボリュームなしでデスティネーションSVMが作成され、`stopped`状態になります。

終了後の操作

デスティネーションSVMをディザスタ リカバリ用に設定する必要があります。

MetroCluster構成用SVMの作成

MetroCluster構成用のSVMを作成して、MetroCluster構成用に設定されたクラスタのデータに対して同期ディザスタ リカバリおよび高可用性を提供できます。

開始する前に

- 2つのクラスタがMetroCluster構成になっている必要があります。
- 両方のクラスタ内でアグリゲートが利用可能でオンラインになっている必要があります。
- 必要に応じて、両方のクラスタに同じ名前のIPspaceを作成しておく必要があります。

タスク概要

MetroCluster構成のどちらかのクラスタにSVMを作成すると、SVMはソースSVMとして作成され、ソースSVM名にサフィックス「-mc」を追加した名前のパートナーSVMがパートナー クラスタに自動的に作成されます。

MetroCluster構成では、1つのクラスタに64個のSVMを作成できます。したがって、MetroCluster構成は最大128個のSVMをサポートします。

手順

1. `is-repository`パラメータを**`false`**に設定して`vserver create`コマンドを使用します。

   例

   次のコマンドでは、ローカル サイトに**`sync-source`**サブタイプでSVMが作成され、パートナー サイトに**`sync-destination`**サブタイプでSVMが作成されます。

```
cluster_A::>vserver create -vserver vs4 -rootvolume vs4_root -
aggregate aggr1
-rootvolume-security-style mixed -is-repository false
[Job 196] Job succeeded:
Vserver creation completed
```

ローカル サイトにSVM **vs4**が作成され、パートナー サイトに**vs4-mc**が作成されます。

2. 作成したSVMを表示します。

   - ローカル クラスタで、`metrocluster vserver show`コマンドを使用してSVMを確認します。
     次のコマンドは、パートナーSVMとその設定内容を表示します。

     ```
     cluster_A::> metrocluster vserver show

                          Partner    Configuration
     Cluster     Vserver   Vserver    State
     ---------  --------  --------- -----------------
     cluster_A   vs4       vs4-mc     healthy
     cluster_B   vs1       vs1-mc     healthy
     ```

   - ローカル クラスタおよびパートナー クラスタから`vserver show`コマンドを使用して、新しく設定したSVMの状態を確認します。
     次のコマンドは、SVMの管理状態と運用状態を表示します。

     ```
     cluster_A::> vserver show

                                  Admin   Operational Root
     Vserver Type  Subtype        State   State       Volume     Aggregate
     ------- ----- -------       ------- --------    ----------- ----------
     vs4     data  sync-source   running   running    vs4_root   aggr1

     cluster_B::> vserver show

                                     Admin   Operational  Root
     Vserver Type  Subtype          State   State        Volume      Aggregate
     ------- ----- -------          ------  ---------    ----------- ----------
     vs4-mc  data  sync-destination running stopped      vs4_root    aggr1
     ```

   SVMの作成がルート ボリュームの作成などの中間処理が原因で失敗した場合、SVMは`initializing`状態になります。その場合、SVMを削除して再度作成する必要があります。

タスクの結果

MetroCluster構成用のSVMが、1GBのルート ボリュームで作成されます。sync-source SVMの状態は`running`、sync-destination SVMの状態は`stopped`です。

Infinite Volumeを備えたSVMの作成

データ アクセスを提供するためには、クラスタにSVMが少なくとも1つ必要です。Infinite Volumeを備えたSVMを作成して、NAS環境内の大規模データへのアクセスを提供できます。

開始する前に

事前に計画要件を確認し、ガイドラインを理解しておく必要があります。

- *SVMの作成計画*
- *SVMの作成に関するガイドライン*

次の要件が満たされていることを確認します。

- 十分なスペースがある、ルートではないアグリゲートが、少なくとも1つクラスタに含まれている必要があります。

- SVMのルート ボリュームのアグリゲートに、1GB以上のスペースが必要です。
- CIFSの作成および認証エラーが起きないよう、NTPを設定および有効にしてクラスタを同期しておく必要があります。
- IPspaceを割り当てる場合、IPspaceを作成しておく必要があります。

タスク概要

異なるSSHセッションを使用するか、スクリプトを使用することで、最大5個のSVMを同時に作成できます。

注: パフォーマンスの低下を避けるため、同時に作成するSVMは5個以下にすることを推奨します。

Infinite Volumeを備えたSVMの言語を変更することはできません。

手順

1. `is-repository`パラメータを**`true`**に設定して`vserver create`コマンドを使用します。

   例

   次のコマンドは、vs0.example.comという名前の、Infinite Volumeを備えたStorage Virtual Machine（SVM、旧Vserver）を作成します。

   ```
   cluster1::>vserver create -vserver vs1.example.com -rootvolume
   root_vs0 -aggregate
   aggr1 -rootvolume-security-style unix -language C.UTF-8 -snapshot-
   policy default -is-repository true

   [Job 2061] Job succeeded:
   Vserver creation completed
   ```

2. `vserver show`コマンドを使用して、新しく作成したSVMのステータスを確認します。

   例

   ```
   cluster1::> vserver show
                                    Admin      Operational   Root
   Vserver          Type    Subtype    State      State         Volume     Aggregate
   -------          -----   -------    -------   --------     ----------- ----------
   cluster1         admin     -         -           -             -           -
   cluster1-01      node      -         -           -             -           -
   vs1.example.com  data    default    running   running       root_vs0      aggr1
   ```

   SVMの作成がルート ボリュームの作成などの中間処理が原因で失敗した場合、SVMは`initializing`状態になります。その場合、SVMを削除して再度作成する必要があります。

タスクの結果

SVMが1GBのルート ボリュームで作成され、自動的に起動して`running`状態になります。デフォルトでは、vsadminユーザ アカウントが作成され、`locked`状態になります。vsadminロールがデフォルトのvsadminユーザ アカウントに割り当てられます。

関連コンセプト

クラスタ時間の管理（クラスタ管理者のみ）（166ページ）

関連タスク

SVM管理者への管理の委譲（95ページ）
SVMに関する情報の表示（100ページ）

SVMの設定

SVMを作成したら、クライアントにデータ アクセスを提供できるように、ストレージをプロビジョニングし、ネットワーク、サービス、およびプロトコルを設定する必要があります。

タスク概要

以下は、SVMの作成後に実行する必要がある設定タスクの概要とその順序を示しています。設定タスクに関する詳細は、clustered Data ONTAPの他のドキュメントに記載されています。

ネットアップのマニュアル：Data ONTAP 8（現在のリリース）

手順

1. アグリゲート名が必要なボリューム関連のすべての処理に、SVMのアグリゲートを指定します。
2. パスワードを設定してvsadminユーザ アカウントのロックを解除し、SVMの管理を委譲します。
3. 次の手順を実行し、SVMへのデータ アクセスを提供します。
   a. ネットワーク インターフェイスを設定します（LIFやルートの作成など）。
   b. ボリュームを作成してストレージをプロビジョニングします。
   c. LDAP、NIS、およびDNSなどのサービスを設定します。
   d. NFS、CIFS、iSCSI、FCなどのプロトコルを設定します。
4. ノードに障害やフェイルオーバーが発生したときに引き続きネームスペース ディレクトリ情報を使用できるようにするために、クラスタの各ノード上にルート ボリュームの負荷共有ミラー コピーを作成します。

関連タスク

SVM管理者への管理の委譲（95ページ）
SVMのアグリゲートの変更（98ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド
clustered Data ONTAP 8.3 論理ストレージ管理ガイド
clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（CIFS）
clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）
clustered Data ONTAP 8.3 SANアドミニストレーション ガイド
clustered Data ONTAP 8.3 SVMルート ボリューム保護エクスプレス ガイド

SVM管理者用のユーザ アカウントの作成

任意のSVM事前定義ロールまたはカスタマイズされたロールからSVMの管理をSVM管理者に委任するには、ローカル ユーザに対してSVMユーザ アカウントを作成するか、またはNISユーザとLDAPユーザ、およびActive Directory（AD）ユーザまたはグループへのアクセスを提供する必要があります。

選択肢

- ローカル ユーザ アカウントの作成（93ページ）

- NISまたはLDAPユーザ アカウントへのアクセスの許可（93ページ）
- Active Directoryユーザまたはグループへのアクセスの許可（94ページ）

ローカル ユーザ アカウントの作成

SVM管理者用のローカル ユーザ アカウントを作成し、ユーザ パスワード、SSH公開鍵、SSL証明書の各認証方式を使用してSVMにアクセスできます。

開始する前に

- SSH公開鍵認証を使用する場合、公開鍵と秘密鍵のキー ペアをクライアントに作成しておく必要があります。

  `security login publickey create`コマンドを使用して、クラスタに公開鍵を設定しておく必要があります。

- SSL証明書認証を使用する場合、自己署名デジタル証明書を作成してインストールしておく必要があります。

タスク概要

アプリケーション、認証方式、および定義済みのロールまたはカスタマイズされたロールをSVMローカル ユーザ アカウント用に選択できます。

手順

1. `security login create`コマンドを使用して、任意のSVMロール用にSVMローカル ユーザ アカウントを作成します。

   例

   次のコマンドを実行すると、認証方式としてパスワードを使用するSVMロールが作成されます。

   ```
   cluster1::>security login create -user-or-group-name user1 -application ssh  -authmethod
   password  -role vsadmin-backup -vserver vs1.example.com
   ```

   次のコマンドを実行すると、認証方式として公開鍵を使用するSVMロールが作成されます。

   ```
   cluster1::>security login create -user-or-group-name user2 -application ssh  -authmethod
   publickey  -role vsadmin-backup -vserver vs2.example.com
   ```

   次のコマンドを実行すると、認証方式として証明書を使用するSVMロールが作成されます。

   ```
   cluster1::>security login create -user-or-group-name user3 -application ontapi  -
   authmethod cert -role vsadmin-backup -vserver vs3.example.com
   ```

NISまたはLDAPユーザ アカウントへのアクセスの許可

SVM管理者がLDAPまたはNISの認証方式を使用してSVMにアクセスできるようにするため、LDAPまたはNISユーザ アカウントにアクセスを許可できます。

開始する前に

- NISまたはLDAPユーザ アカウントを、NISまたはLDAPサーバ上に作成しておく必要があります。
- NISまたはLDAPサーバを検索するようにSVMが設定されている必要があります。

タスク概要

SVMユーザ アカウントのアプリケーションとロールを選択できます。

SVMユーザ アカウントは、LDAPまたはNISディレクトリ内に直接作成するか、SVMのローカル管理リポジトリ内にローカル ユーザとして作成することができます。SVMユーザ アカウントをどこに作成したかに応じて、ネーム サービス スイッチ（`ns-switch`）の設定時に関連するネーム サービス ソースを含める必要があります。

手順

1. `security login create`コマンドを使用して、任意のSVMロール用にSVMユーザ アカウントを作成します。

   例

   次のコマンドを実行すると、認証方式がnsswitchに設定されたSVMユーザ アカウントが作成されます。

   ```
   cluster1::>security login create -user-or-group-name user1 -application ssh  -authmethod
   nsswitch -role vsadmin-backup -vserver vs1.example.com
   ```

2. `vserver services name-service`コマンドを使用して、**`ldap`**、**`nis`**、**`files`**をSVM認証のネーム サービス ソースとして追加します。

   ネーム サービスに**`files`**を追加すると、LDAPサーバまたはNISサーバでユーザが見つからなかった場合、SVMローカル管理リポジトリを使用してSVMユーザ アカウントを認証できるようになります。

   例

   次のコマンドは、SVM用ネーム サービス ソースを追加します。

   ```
   cluster1::> vserver services name-service ns-switch create -vserver vs1.example.com -
   sources ldap,nis,files -database password -enabled true
   ```

関連情報

clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）

Active Directoryユーザまたはグループへのアクセスの許可

SVM管理者がWindows Active Directoryの認証方式を使用してSVMにアクセスできるようにするため、Active Directory（AD）ユーザまたはグループのアカウントにアクセスを許可できます。

開始する前に

- ADサーバにADユーザまたはグループを作成しておく必要があります。
- SVM用のADコンピュータ アカウントを作成しておく必要があります。

タスク概要

ADグループはユーザ アカウントの権限レベルを一元的に管理するためのもので、サポートされるアクセス方式はSSHとData ONTAP APIのみです。ADグループに属するすべてのユーザは、グループに割り当てられたロールを使用してSVMにアクセスできます。

手順

1. `security login create`コマンドを使用して、ADユーザまたはグループにアクセスを許可します。
   - ADユーザ アカウント

次のコマンドは、SVM vs0用に、ユーザ名＝guest、アプリケーション＝ssh、認証方式＝domain、アクセス制御ロール＝vsadminのアカウントをDOMAIN1に作成します。

```
cluster1::> security login create -user-or-group-name DOMAIN1\guest -application ssh -
authmethod domain -role vsadmin -vserver vs0.example.com
```

- ADグループ アカウント
  次のコマンドは、SVM vs1用に、ADグループ名＝adgroup、アプリケーション＝ssh、認証方式＝domain、アクセス制御ロール＝vsadminのアカウントをDOMAIN1に作成します。

```
 cluster1::> security login create -user-or-group-name DOMAIN1\adgroup -application
ssh -authmethod domain -role vsadmin -vserver vs1.example.com
```

SVM管理者への管理の委譲

Storage Virtual Machine（SVM）を基本的なネットワーク設定で最終的な運用状態までセットアップしたら、必要に応じてそのSVMの管理をSVM管理者に委譲できます。SVMの管理を委譲するには、事前に定義されたロールまたはカスタマイズしたロールを指定したユーザ アカウントを作成して割り当てます。

開始する前に

カスタマイズしたロールを使用してSVMの管理を委譲する場合は、`security login role create`コマンドを使用して、カスタマイズしたロールを作成しておく必要があります。

手順

1. `vserver show -fields aggr-list`コマンドを使用して、SVMにアグリゲートが割り当てられているかどうかを確認します。

   注: SVMにアグリゲートが割り当てられていないと、SVM管理者はボリュームを作成できません。

2. SVMにアグリゲートが割り当てられていない場合は、`vserver add-aggregates`コマンドを使用して、SVMのアグリゲート リストにアグリゲートを指定します。

   注: SVMにルート アグリゲート「aggr0」を割り当てることはできません。

   例

   次のコマンドは、SVM vs1.example.comに対してaggr1アグリゲートを指定します。

```
cluster1::> vserver add-aggregates -vserver vs1.example.com -
aggregates aggr1
```

3. FlexVolを備えたSVMの管理をSVM管理者に委譲する場合、`vserver modify`コマンドに`max-volumes`オプションを指定して、SVM管理者がそのSVMに作成できる最大ボリューム数を指定します。

   例

   次のコマンドは、SVM vs1.example.comに対して最大ボリューム数を指定します。

```
cluster1::> vserver modify -vserver vs1.example.com -max-volumes 10
```

4. `vserver add-protocols`コマンドまたは`vserver remove-protocols`コマンドを使用して、SVMのプロトコルを指定します。

例

次のコマンドは、SVM vs1.example.comに対してCIFSプロトコルを指定します。

```
cluster1::> vserver add-protocols -vserver vs1.example.com -protocols
cifs
```

設定とデータ アクセスに使用できるのは、指定したプロトコルだけです。

5. SVM管理用に、新しいLIFを作成するか、いずれかのデータLIFを使用します。

   重要: SANプロトコル用に設定されているデータLIFをSVM管理に使用することはできません。

状況	操作

SVM管理用に新しいLIFを作成する	**a.** `vserver show`コマンドを使用して、SVMに割り当てられているIPspaceを特定します。
	`cluster1::> vserver show -vserver vs1.example.com -fields ipspace`
	`vserver ipspace`
	`---------- -------`
	`vs1.example.com ipspace1`
	
	b. `network port show`コマンドを使用して、SVMと同じIPspaceからポートを選択します。
	`cluster1::> network port show -ipspace ipspace1`
	`Node Port IPspace Broadcast Domain Link MTU Speed (Mbps) Admin/Oper`
	`------ ------- ---------- ---------- ----- ------- ----------`
	`cluster1-01 e0c ipspace1 192.0.2.120/24 up 1500 auto/1000`
	`....`
	`....`
	
	c. `network interface create`コマンドを使用して、LIFを作成します。
	次のコマンドは、SVM vs1.example.comのIPspace ipspace1に属するポートe0cにデータLIF lif3を作成します。
	`cluster1::> network interface create -vserver vs1.example.com -lif lif3 -data-protocol`
	`none -role data -home-node node1-01 -home-port e0c -address 192.0.2.129 -netmask 255.255.255.128`

同じLIFをNFS、CIFS、およびSVM管理に使用する	`network interface modify`コマンドを使用して、ファイアウォール ポリシーを**`mgmt`**に変更します。 次のコマンドは、SVM管理用に、SVM vs1.example.comのデータLIF lif1を変更します。 `cluster1::>network interface modify -vserver vs1.example.com -lif lif1 -firewall-policy mgmt`

6. SVM管理者のロールに応じて、該当する処理を実行します。

使用するロール	操作

vsadmin：SVMを作成したときに作成されてロックされている事前定義のロール	**a.** `security login password`コマンドを使用して、パスワードを設定します。
	i. ユーザ アカウントのパスワードを入力します。
	ii. パスワードを再入力して確認します。
	次のコマンドを使用すると、SVM vs1.example.comのvsadminユーザ アカウントにパスワードが設定されます。
	`cluster1::>security login password -username vsadmin -vserver vs1.example.com`
	`Please enter a password for user 'vsadmin':`
	`Please enter it again:`
	`cluster1::>`
	b. `security login unlock`コマンドを使用して、ユーザ アカウントのロックを解除します。
	次のコマンドを使用すると、SVM vs1.example.comのvsadminユーザ アカウントのロックが解除されます。
	`cluster1::> security login unlock -username vsadmin -vserver vs1.example.com`

vsadmin-volume、vsadmin-protocol、vsadmin-readonlyなど、カスタマイズされたロールまたは事前定義されたその他のロール	`security login create`コマンドを使用して、ロールを指定してユーザ アカウントを作成します。
	a. ユーザ アカウントのパスワードを入力します。
	b. パスワードを再入力して確認します。
	次のコマンドを使用すると、SVM vs1.example.comに対し、vsadmin-readonlyロールを持つuser1ユーザ アカウントが作成されます。
	`cluster1::> security login create -user-or-group-name user1 -application ssh -authmethod password -vserver vs1.example.com -role vsadmin-readonly`
	`Please enter a password for user 'user1':`
	`Please enter it again:`
	`cluster1::>`

タスクの結果

SVMをSVM管理者に割り当てたら、SVM管理者はユーザ名とパスワード、および管理IPアドレスを使用して、そのSVMにログインできます。

SVMの変更

Storage Virtual Machine（SVM）のアグリゲートを指定し、SVMのプロトコルを許可または禁止し、言語やポリシーなどのSVMのその他の属性を変更できます。

関連タスク

SVMに関する情報の表示（100ページ）

SVMのアグリゲートの変更

SVM管理者がアグリゲート名を必要とするプロビジョニング処理（ボリュームの作成など）を実行する際に、使用可能なアグリゲートのリストを表示できるよう、SVMにアグリゲートを指定する必要があります。アグリゲートを追加または削除して、SVMにアグリゲートを指定できます。

タスク概要

クラスタ管理者は、アグリゲート名を必要とするあらゆる処理を実行できます。SVMにアグリゲートを指定する際には、SVM管理者と同じプロビジョニング処理しか実行できませんが、複数のアグリゲートにまたがるボリュームの移動とコピーは実行できます。

手順

1. SVMに、次のようにアグリゲートを追加または削除します。
   - `vserver add-aggregates`コマンドを使用して、SVMのアグリゲート リストにアグリゲートを追加します。
     次のコマンドでは、SVM vs1.example.comのアグリゲート リストにアグリゲートaggr0およびaggr1が追加されます。

     ```
     cluster1::> vserver add-aggregates -vserver vs1.example.com -
     aggregates aggr0, aggr1
     ```

   - `vserver remove-aggregates`コマンドを使用して、SVMのアグリゲート リストからアグリゲートを削除します。
     次のコマンドでは、aggr0が、SVM vs1.example.comのアグリゲート リストから削除されます。

     ```
     cluster1::> vserver remove-aggregates -vserver vs1.example.com -
     aggregates aggr0
     ```

2. `vserver show -instance`コマンドを使用して、SVMに割り当てられたアグリゲートのリストを表示します。

   例

   次のコマンドでは、SVM vs1.example.comに割り当てられたアグリゲートのリストが表示されます。

   ```
   cluster1::> vserver show -instance -vserver vs1.example.com

                                        Vserver: vs1.example.com
                                   Vserver Type: data
                                Vserver Subtype: default
                                          ...
                                          ...
                   List of Aggregates Assigned: aggr1
                                          ...
                                          ...
   ```

タスクの結果

変更したアグリゲート リストを、SVMのプロビジョニング処理に使用できます。

SVMのプロトコルの変更

SVMの作成時には、そのSVMの設定ですべてのプロトコルが許可されています。プロトコルを追加または削除して、SVMの設定で許可されているプロトコルのリストを編集できます。

タスク概要

SVMにプロトコルを追加すると、追加したプロトコルを設定に使用できるようになります。

プロトコルを削除すると、そのプロトコルはSVMの設定に使用できなくなり、そのプロトコルを介したデータ アクセスは停止します。

手順

1. SVMに次のようにプロトコルを追加または削除します。
   - SVMにプロトコルを許可するには、`vserver add-protocols`コマンドを使用します。
     次のコマンドを使用すると、SVM vs1.example.comのアグリゲート リストにNFSプロトコルとCIFSプロトコルが追加されます。

     ```
     cluster1::> vserver add-protocols -vserver vs1.example.com -
     protocols nfs, cifs
     ```

   - SVMにプロトコルを禁止するには、`vserver remove-protocols`コマンドを使用します。
     次のコマンドを使用すると、SVM vs1.example.comのアグリゲート リストからNFSプロトコルが削除されます。

     ```
     cluster1::> vserver remove-protocols -vserver vs1.example.com -
     protocols nfs
     ```

2. SVMに許可されているプロトコルのリストを表示するには、`vserver show-protocols`コマンドを使用します。

   例

   次のコマンドを実行すると、すべてのSVMのプロトコルが表示されます。

   ```
   cluster1::> vserver show-protocols

   Vserver Name                Protocols
   ---------------       ---------------
   ...
   ...                         -
   vs2.example1.com            fcp
   vs1.example.com             cifs fcp, iscsi, ndmp
   ...
   ...
   ```

SVM属性の変更用コマンド

`vserver modify`コマンドを使用して、SVMの属性（言語、最大ボリューム数、Snapshotポリシー、クォータ ポリシーなど）を変更できます。

変更する項目	使用するコマンド	FlexVolを備えたSVMでの使用	Infinite Volumeを備えたSVMでの使用	メモ
言語	`vserver modify -language`	はい	いいえ	SVMの言語を変更しても、SVM内の既存ボリュームの言語設定は変更されません。
Snapshotポリシー	`vserver modify -snapshot-policy`	はい	はい	N/A
クォータ ポリシー	`vserver modify -quota-policy`	はい	いいえ	N/A
QoSポリシー グループ	`vserver modify -qos-policy-group`	はい	いいえ	N/A
最大ボリューム数	`vserver modify -max-volumes`	はい	いいえ	値がデフォルト値の **`unlimited`**に設定されている場合、その SVMには任意の数のボリュームを作成できます。 値を**`0`**に指定した場合は、その SVMにボリュームを作成できません。したがって、SVM管理者がボリュームを作成できるように値を指定する必要があります。

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

SVMに関する情報の表示

クラスタ管理者は、`vserver show`コマンドを使用して、Storage Virtual Machine（SVM、旧Vserver）に関する設定情報を表示できます。

手順

1. 該当するコマンドを入力し、SVMに関する情報を表示します。

状況	入力するコマンド
すべてのSVMに関する基本情報を表示する	**vserver show**
すべてのSVMに関する詳細情報を表示する	**vserver show -instance**
特定のSVMに関する情報を表示する	**vserver show -vserver *Vserver_name*** *Vserver_name*には、SVMの名前を指定します。

例

次のコマンドを実行すると、すべてのSVMに関する基本情報が表示されます。

```
cluster1::>vserver show

                                   Admin      Operational   Root
Vserver          Type    Subtype   State      State         Volume     Aggregate
-------          -----   -------   -------    --------     ----------- ----------
cluster1         admin     -         -          -            -           -
cluster1-01      node      -         -          -            -           -
cluster1-02      node      -         -          -            -           -
vs0.example.com  data    default   running   running       root_vs0      aggr1
vs2.example.com        data              default               running
running                            root_vol2     aggr1
```

次のコマンドを実行すると、すべてのSVMに関する詳細情報が表示されます。

```
cluster1::> vserver show -instance

                    Vserver: cluster1
                   Vserver Type: admin
                Vserver Subtype:
                   Vserver UUID: 00000000-0000-0000-0000-000000000000
                    Root Volume: -
                       Aggregate: -
                   .
                   .
   List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: -
           Vserver Admin State: -
     Vserver Operational State: -
Vserver Operational State Stopped Reason: -
                   .
                   .
                    Config Lock: false
                   IPspace Name: Default
          Is Vserver Protected: -

                    Vserver: vs0.example.com
                   Vserver Type: data
                Vserver Subtype: default

                   Vserver UUID: 49294a39-e762-11df-8768-123478563412
                    Root Volume: root_vs0
                       Aggregate: aggr1
                   .
                   .
   List of Aggregates Assigned: aggr0_2, aggr1
Limit on Maximum Number of Volumes allowed: 10
           Vserver Admin State: running
     Vserver Operational State: running
Vserver Operational State Stopped Reason: -
                   .
                   .
                    Config Lock: false
                   IPspace Name: Default
          Is Vserver Protected: false
```

次のコマンドを実行すると、SVM vs2.example.comに関する詳細情報が表示されます。

```
cluster1::> vserver show -vserver vs2.example.com

                         Vserver: vs2.example.com
                    Vserver Type: data
                 Vserver Subtype: default
                    Vserver UUID: ca34e6b2-ddec-11df-b066-123478563412
                     Root Volume: root_vol2
```

```
                    .
                    .
                     Config Lock: false
                   IPspace Name: Default
          Is Vserver Protected: false
```

SVMの名前の変更

Storage Virtual Machine（SVM）の名前は、`vserver rename`コマンドを使用して変更することができます。たとえば、SVMの名前を一意にする場合に、SVMの名前を変更できます。`vserver rename`コマンドを使用してノードまたはadmin SVMの名前を変更することはできません。

開始する前に

SVMピア関係にあるSVMの名前を変更することはできません。

手順

1. SVMの名前を変更するには、`vserver rename`コマンドを使用します。

   例

   SVMのvs1.example.comという名前をvs2.example.comに変更する方法を次の例で説明します。

   ```
   Cluster1::> vserver rename -vserver vs1.example.com -newname
   vs2.example.com
   ```

   このコマンドの詳細については、マニュアル ページを参照してください。

2. `vserver show`コマンドを使用して、SVMの名前が変更されたことを確認します。

SVMの削除

不要になったStorage Virtual Machine（SVM）は、`vserver delete`コマンドを使用してクラスタから削除できます。

開始する前に

1. SVMに関連付けられているSVMピア関係を削除する必要があります。
2. すべてのボリュームについて、Snapshotコピーと、DPおよびLSミラーを無効にする必要があります。
3. LUNを使用している場合は、LUNのマッピングを解除してオフラインにし、削除する必要があります。
4. SVMに属するすべてのigroupを手動で削除する必要があります。
5. SVM上のすべてのボリュームをアンマウントしてオフラインにし、SVMのルート ボリュームも含めて削除する必要があります。
6. CIFSサーバを削除する必要があります。
7. SVMに関連付けられている、カスタマイズされたユーザ アカウントとロールを削除する必要があります。
8. SVMを停止する必要があります。

タスク概要

SVMを削除すると、SVMに関連付けられている次のオブジェクトも自動的に削除されます。

- LIF、LIFフェイルオーバー グループ、およびLIFルーティング グループ
- エクスポート ポリシー
- Sisポリシー

SVMを削除したあとでそのSVM関連の情報をリカバリすることはできません。

Kerberosを使用するように設定されているSVMを削除したり、別のService Principal Name（SPN;サービス プリンシパル名）を使用するように SVMを変更したりした場合、SVMの元のサービス プリンシパル名はKerberos Realmから自動的に削除されず、また無効にもなりません。 元のプリンシパルは、手動で削除または無効にする必要があります。プリンシパルを削除または無効にするためには、Kerberos Realm管理者のユーザ名とパスワードが必要です。

最初のSVMを削除する前にそのSVMから2つ目のSVMへデータを移動する場合は、SnapMirrorコマンドを使用できます。SnapMirrorの詳細については、*『clustered Data ONTAP データ保護ガイド』*を参照してください。

手順

1. SVMを削除するには`vserver delete`コマンドを使用します。

   例

   次の例は、vs1.example.comという名前のSVMを削除する方法を示しています。

   ```
   cluster1::> vserver delete -vserver vs1.example.com
   ```

   このコマンドの詳細については、マニュアル ページを参照してください。

   注: 中間処理の失敗が原因で、SVMの削除処理に失敗する場合があります。この場合、SVMはdeleting状態になります。このようなSVMには他のSVM処理を実行できないため、SVMを削除することを推奨します。たとえば、削除中状態にあるSVMとのSVMピアリング関係は作成できません。

SVMの起動

Storage Virtual Machine（SVM）を起動することで、SVMからデータ アクセスを提供できます。SVMを起動するには、`vserver start`コマンドを使用できます。

タスク概要

SVMを起動すると、停止していたプロトコルがデータの提供を開始します。プロトコルは、`vserver fcp stop`などのコマンドで個別に停止される場合と、はSVMの停止に伴って停止される場合があります。

あるSVMのリソースがHAペアに含まれている場合は、Storage Failover（SFO;ストレージ フェイルオーバー）中にそのSVMを起動することはできません。

手順

1. `vserver start`コマンドを使用し、SVMを起動します。

   例

   次のコマンドは、SVM vs0.example.comを起動します。

```
cluster1::> vserver start -vserver vs0.example.com
[Job 21] Job succeeded: DONE
```

2. 内部エラー メッセージが表示されてSVMの起動処理が失敗した場合、次の手順を実行します。

   a. `vserver show`コマンドを使用して、SVMの管理状態を確認します。

   b. SVMの管理状態が**`starting`**の場合は、`vserver start`コマンドを再度実行します。

   例

   次のコマンドは、起動に失敗したSVMを再起動します。

```
cluster1::> vserver start vs1.example.com
[Job 43] Job is queued: Vserver Start.

Error: command failed: [Job 43] Job failed: Internal Error

cluster1::> vserver show
                                   Admin      Operational   Root
Vserver          Type    Subtype    State      State         Volume     Aggregate
-------          -----   -------    -------   --------     ----------- ----------
cluster1         admin     -         -           -             -           -
cluster1-01      node      -         -           -             -           -
vs0.example.com  data    default    running   running       root_vs0      aggr1
vs1.example.com  data    default    starting  stopped       root_vs1      aggr1

cluster1::> vserver start vs1.example.com
[Job 48] Job succeeded: DONE
```

タスクの結果

SVMは**`running`**状態になり、クライアントへのデータの提供を開始します。

Infinite Volumeを備えたSVMを起動すると、データ ポリシーが自動的に再インポートされ、JSON形式がチェックされます。

関連タスク

SVMに関する情報の表示（100ページ）

関連情報

Clustered Data ONTAP 8.3 Infinite Volumes Management Guide

SVMの停止

Storage Virtual Machine（SVM）のトラブルシューティングを実施するかSVMを削除する場合、またはSVMからのデータ アクセスを停止する場合、`vserver stop`コマンドを使用してSVMを停止できます。

開始する前に

SVMに接続されているすべてのクライアントを切断する必要があります。

注意: SVMの停止時にSVMにクライアントが接続されていると、データの損失が発生する可能性があります。

タスク概要

SVMのリソースがHAペアに含まれている場合、ストレージ フェイルオーバー（SFO）中にそのSVMを停止することはできません。

SVMを停止しても、SnapMirrorデータ転送などその他の処理は引き続きスケジュールどおりに実行されます。

SVMが**stopped**状態の間は、SVM管理者はSVMにログインできません。

手順

1. `vserver stop`コマンドを使用してSVMを停止します。

   例

   次のコマンドは、SVM vs0.example.comを停止します。

```
cluster1::> vserver stop -vserver vs0.example.com
[Job 41] Job succeeded: DONE
```

2. 内部エラー メッセージが表示されてSVMの停止処理が失敗した場合、次の手順を実行します。

   a. `vserver show`コマンドを使用して、SVMの管理状態を確認します。

   b. SVMの管理状態が**stopping**の場合は、`vserver stop`コマンドを再度実行します。

   例

   次のコマンドは、停止に失敗したSVMを停止します。

```
cluster1::> vserver stop -vserver vs1.example.com
[Job 45] Job is queued: Vserver Stop.

Error: command failed: [Job 45] Job failed: Internal Error


cluster1::> vserver show
                                   Admin      Operational   Root
Vserver           Type    Subtype    State      State         Volume     Aggregate
-------           -----   -------    -------   --------     ----------- ----------
cluster1          admin     -         -           -             -           -
cluster1-01       node      -         -           -             -           -
vs0.example.com   data    default    stopped   stopped       root_vs0      aggr1
vs1.example.com   data    default    stopping  running       root_vs1      aggr1

cluster1::> vserver stop -vserver vs1.example.com
[Job 49] Job succeeded: DONE
```

タスクの結果

SVMが**stopped**状態になり、クライアントへのデータの提供が停止します。

関連タスク

SVMに関する情報の表示（100ページ）

SVMコンテキストからのSVMの管理

Storage Virtual Machine（SVM）とそのリソースは、`vserver context`コマンドを使用してSVMのコンテキストから管理できます。

タスク概要

SVMコンテキストに切り替えたあとの権限は、SVM管理者と同じです。`vserver context`コマンドを実行中にユーザ名を指定しなかった場合は、デフォルトのSVM管理者（vsadmin）と同じ権限を持ちます。ユーザ名を指定した場合は、ユーザ名のロールと同じ権限を持ちます。

あるSVMから別のSVMに切り替える場合は、最初のSVMを終了する必要があります。

手順

1. SVMコンテキストに入るには、`vserver context`コマンドを使用します。

   例

   クラスタからSVM vs1.example.comにコンテキストを切り替える方法を次の例で説明します。

   ```
   cluster1::> vserver context -vserver vs1.example.com -username
   vsadmin-volume

   Info: Use 'exit' command to return.

   vs1.example.com::>
   ```

   `vserver context`コマンドの詳細については、マニュアル ページを参照してください。

   別のSVM管理者のロールを使用するには、`-username`オプションを指定します。

   これで、SVM vs1.example.comのコンテキストに切り替わりました。権限は、vsadmin-volumeロールと同じになります。

2. SVMコンテキストから実行するコマンドを入力します。

   例

   SVM vs1.example.comコンテキストからSVM vs1.example.comに所属するボリュームを表示する方法を次の例で説明します。

   ```
   vs1.example.com::> vol show
     (volume show)
   Vserver          Volume     Aggregate    State      Type  Size  Available Used%
   ---------        ---------- ------------ ---------- ---- ----- ---------- -----
   vs1.example.com   root_vol1  aggr3        online     RW   1GB    972.5MB    5%
   vs1.example.com   vol1       aggr1        online     RW   20MB   18.88MB    5%
   ```

3. SVMコンテキストを終了するには、SVMプロンプトで**`exit`**と入力します。

SVMのルート ボリュームのリストア

Storage Virtual Machine（SVM）のルート ボリュームが使用できなくなると、クライアントはネームスペースのルートをマウントできません。このような場合、クライアントにデータ アクセスを提供するために、別のボリュームを昇格するか、または新しいルート ボリュームを作成して、ルート ボリュームをリストアする必要があります。

開始する前に

SVMルート ボリュームは、負荷共有ミラー コピーまたはデータ保護コピーを使用して保護する必要があります。

タスク概要

他のボリュームがジャンクションされていない任意のボリュームを昇格できます。

新しいボリュームをSVMルート ボリュームに昇格すると、データ ボリュームは新しいSVMルート ボリュームに関連付けられます。

選択肢

- FlexVolを備えたSVMの場合、次のいずれかのボリュームを昇格して、ルート ボリュームをリストアします。

- 負荷共有ミラー コピー
  負荷共有ミラー コピーの昇格
- データ保護ミラー コピー
  データ保護ミラー コピーの昇格
- 新しいFlexVol
  新しいFlexVolの昇格

- Infinite Volumeを備えたSVMの場合、新しいルート ボリュームを作成します。

  Infinite Volumeを備えたSVM上への新しいルート ボリュームの作成

終了後の操作

`volume mount`コマンドを使用して新しいルート ボリュームをマウントする必要があります。

負荷共有ミラー コピーの昇格

負荷共有ミラー コピーを昇格して、Storage Virtual Machine（SVM）のルート ボリュームをリストアできます。

手順

1. `set -privilege advanced`コマンドを使用して、特権レベルをadvancedに設定します。
2. `snapmirror promote`コマンドを使用して、負荷共有ミラー コピーをルート ボリュームとして昇格します。
3. `vol show`コマンドを使用して、SVMの新しいルート ボリュームを確認します。
4. `vol rename`コマンドを使用して、ルート ボリュームとして昇格したボリュームの名前を変更します。

   これらのコマンドの詳細については、マニュアル ページを参照してください。

次の例は、vol_dstlsという負荷共有ミラー コピーを、vs1.example.comというSVMのルート ボリュームとして昇格する方法を示しています。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you want to continue? {y|n}: y

cluster1::*> snapmirror promote -destination-path vs1.example.com:vol_dstls

Warning: Promote will delete the read-write volume cluster1://
vs1.example.com/vol1 and replace it with cluster1://vs1.example.com/
vol_dstls.
Do you want to continue? {y|n}: y
[Job 489] Job succeeded: SnapMirror: done

cluster1::*> volume show -volume vol_dstls -instance

               Vserver Name: vs1.example.com
               Volume Name: vol_dstls
               .
               .
               Junction Path: /
               .
               Vserver Root Volume: true
               .
               .
```

データ保護ミラー コピーの昇格

データ保護ミラー コピーを使用して、Storage Virtual Machine（SVM）のルート ボリュームをリストアできます。

手順

1. `snapmirror break`コマンドを使用して、SnapMirror関係を解除します。
2. `set -privilege advanced`コマンドを使用して、特権レベルをadvancedに設定します。
3. `volume make-vsroot`コマンドを使用して、データ保護ミラー コピーをルート ボリュームとして昇格します。
4. `volume show`コマンドを使用して、SVMの新しいルート ボリュームを確認します。
5. `volume rename`コマンドを使用して、ルート ボリュームとして昇格したボリュームの名前を変更します。

   これらのコマンドの詳細については、マニュアル ページを参照してください。

次の例は、vol_dstdpというデータ保護ミラー コピーを、vs1.example.comというSVMのルート ボリュームとして昇格する方法を示しています。

```
cluster1::
> snapmirror break -destination-path vs1.example.com:vol_dstdp
[Job 521] Job succeeded: SnapMirror Break Succeeded

cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you want to continue? {y|n}: y

cluster1::*> volume make-vsroot -volume vol_dstdp -vserver vs1.example.com
[Job 522] Job succeeded: DONE

cluster1::*> volume show -volume vol_dstdp -instance

              Vserver Name: vs1.example.com
              Volume Name: vol_dstdp
              .
              .
              Junction Path: /
              .
              Vserver Root Volume: true
              .
              .
```

新しいFlexVolの昇格

新しいFlexVolを作成および使用して、Storage Virtual Machine（SVM）のルート ボリュームをリストアできます。

タスク概要

clustered Data ONTAP 8.2以降では、SVMのルート ボリュームへのボリュームのマウント時にスペースまたはinodeの不足により障害が発生するのを防ぐために、SVMのルート ボリュームは1GBのサイズで作成されます。したがって、新しいFlexVolを昇格する場合には、サイズが1GB以上である必要があります。

手順

1. `set -privilege advanced`コマンドを使用して、特権レベルをadvancedに設定します。
2. `volume create`コマンドを使用して、サイズが1GBの新しいFlexVolを作成します。
3. `volume make-vsroot`コマンドを使用して、FlexVolをルート ボリュームとして昇格します。
4. `volume show`コマンドを使用して、SVMの新しいルート ボリュームを確認します。
5. `volume rename`コマンドを使用して、ルート ボリュームとして昇格したボリュームの名前を変更します。

   これらのコマンドの詳細については、マニュアル ページを参照してください。

次のコマンドを使用すると、SVMであるvs1.example.comのルート ボリュームとして、FlexVol new_rootvolが昇格されます。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you want to continue? {y|n}:

cluster1::*> vol create -vserver vs3 -volume new_rootvol -aggregate aggr0 -
size 1GB
  (volume create)

cluster1::*> volume make-vsroot -vserver vs1.example.com -volume new_rootvol

cluster1::*> volume show -volume new_rootvol -instance

               Vserver Name: vs1.example.com
               Volume Name: new_rootvol
               .
               .
               Junction Path: /
               .
               Vserver Root Volume: true
               .
               .
```

Infinite Volumeを備えたSVM上への新しいルート ボリュームの作成

Infinite Volumeを備えたStorage Virtual Machine（SVM）のルート ボリュームが使用できなくなった場合、特定のアグリゲートに新しいルート ボリュームを作成して、使用できないルート ボリュームに置き換える必要があります。既存のボリュームをルート ボリュームに昇格することはできません。

タスク概要

Infinite Volumeを備えたSVMに対して新しいルート ボリュームを作成すると、使用できなくなったそれまでのルート ボリュームは自動的に削除されます。

新しいルート ボリュームは、Infinite Volumeを備えたSVMに適したサイズで自動的に作成されます。Infinite Volumeを備えたSVMでは、ルート ボリュームに1GBのサイズが必要とされることはありません。

手順

1. `set -privilege`コマンドを使用してadvanced権限を設定します。
2. SVMの新しいルート ボリュームを作成します。これには`volume make-vsroot`コマンドに`-aggregate`パラメータを指定して使用します。

新しいルート ボリュームが作成され、使用できなくなったそれまでのルート ボリュームが削除されます。

3. `volume mount`コマンドを使用してInfinite Volumeをマウントします。

次の例では、Infinite Volumeを備えたSVM vs0の新しいルート ボリュームを作成し、Infinite Volume repo_volをマウントする方法を示します。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you want to continue? {y|n}: y

cluster1::*> volume make-vsroot -vserver vs0 -volume vs0_root1 -
aggregate aggr1

Warning: Creating a new Vserver root volume will delete the old
Vserver root
volume "vs0_root".
Do you want to continue? {y|n}: y

cluster1::*> volume show -volume vs0_root1 -instance

                                      Vserver Name: vs0
                                       Volume Name: vs0_root1
                                                ...
                                     Junction Path: /
                                                ...
                               Vserver Root Volume: true
                                                ...

cluster1::*> volume mount -vserver vs0 -volume repo_vol -junction-
path /NS -active true -policy-override false
[Job 69] Job succeeded: Volume "repo_vol" on Vserver "vs0" is
mounted at "/NS".

cluster1::*> volume show -vserver vs0 -volume repo_vol -fields
state, junction-path
vserver volume   state  junction-path
------- -------- ------ -------------
vs0     repo_vol online /NS
```

ストレージQoSを使用したSVMへのI/Oパフォーマンスの制御および監視

FlexVolを備えたStorage Virtual Machine（SVM）への入出力（I/O）パフォーマンスは、SVMをストレージQoSポリシー グループに割り当てることによって制御できます。たとえば、I/Oパフォーマンスを制御して、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりすることができます。ストレージQoSは、最大8ノードまでのクラスタでサポートされます。

タスク概要

ポリシー グループは、最大スループット制限（100MB/sなど）を適用します。ただし、最大スループットを指定せずにポリシー グループを作成することもでき、ワークロードを制御せずにパフォーマンスだけを監視できます。

FlexVol、LUN、およびファイルをポリシー グループに割り当てることもできます。

SVMをポリシーグループに割り当てる際の要件は以下のとおりです。

- 割り当てるSVMは、ポリシー グループが属するSVMである必要があります。
  このSVMは、ポリシー グループを作成するときに指定します。
- ポリシー グループにSVMを割り当てる場合、そのSVMに含まれるストレージ オブジェクトをポリシー グループに割り当てることはできません。

手順

1. `qos policy-group create`コマンドを使用してポリシー グループを作成します。

   例

   次のコマンドでは、最大スループットが5,000 IOPSのポリシー グループpg-vs1が作成されます。

   ```
   cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
   throughput 5000iops
   ```

2. `-qos-policy-group`パラメータを指定して`vserver modify`コマンドを使用し、SVMをポリシー グループに割り当てます。

   例

   次のコマンドでは、SVM vs1をポリシー グループpg-vs1に割り当てます。

   ```
   cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
   ```

3. `qos statistics`コマンドを使用してパフォーマンス データを表示します。

   例

   次のコマンドでは、ポリシー グループのパフォーマンスが表示されます。

   ```
   cluster1::> qos statistics performance show
   Policy Group           IOPS      Throughput   Latency
   -------------------- -------- --------------- ----------
   -total-                 12316       47.76MB/s  1264.00us
   pg_app2                  7216       28.19MB/s   420.00us
   pg_vs1                   5008       19.56MB/s     2.45ms
   _System-Best-Effort        62       13.36KB/s     4.13ms
   _System-Background         30           0KB/s        0ms
   ```

4. 必要に応じて、`qos policy-group modify`コマンドを使用して、ポリシー グループの最大スループット制限を調整します。

   例

   次のコマンドを実行すると、ポリシー グループpg-vs1の最大スループットが4,500 IOPSに変更されます。

   ```
   cluster1::> qos policy-group modify pg-vs1 -max-throughput 4500iops
   ```

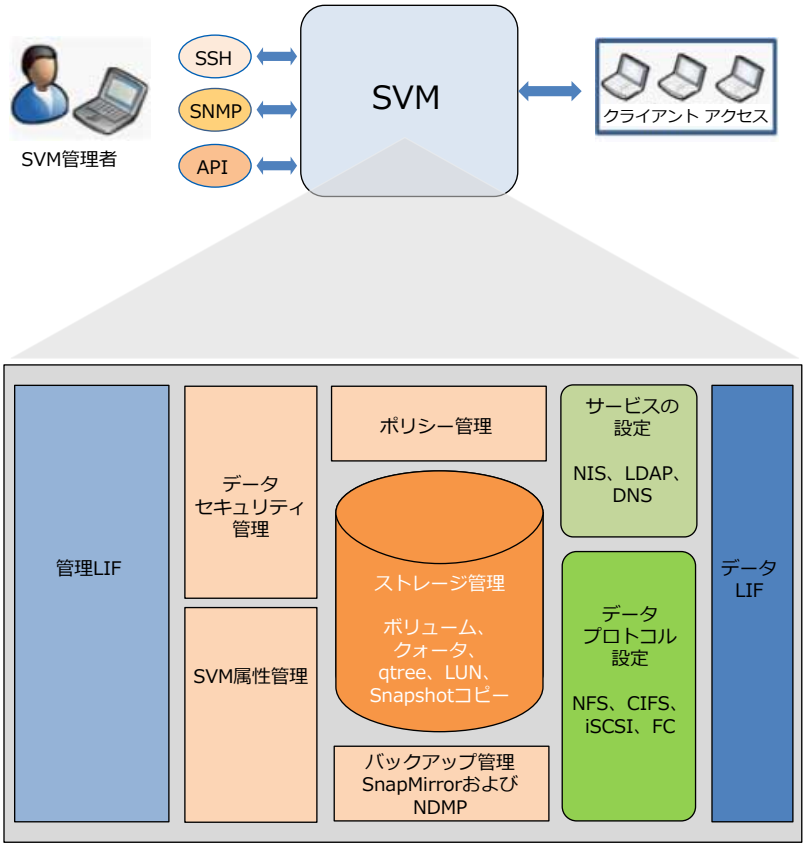
関連コンセプト

例：共有ストレージ インフラのワークロードに制限をプロアクティブに設定する（254ページ）
ストレージQoSを使用したワークロード パフォーマンスの管理（245ページ）

SVMの管理

SVM管理者は、クラスタ管理者によって割り当てられた権限に応じて、Storage Virtual Machine（SVM、旧Vserver）上のさまざまな管理タスクを実行できます。SVMにログインしたあと、SVM管理者は割り当てられている権限と、管理に使用できるコマンドを特定できます。

次の図は、SVMの管理コンポーネントを示しています。



SVM管理者には、次に示す管理機能のすべてまたは一部が与えられます。

- ジョブおよびスケジュールの管理
  SVMに関連するジョブとスケジュールを管理できます。
- データ アクセス プロトコルの設定
  NFS、CIFS、iSCSI、およびFibre Channel（FC;ファイバチャネル）のプロトコル（Fibre Channel over Ethernetを含む）などのデータ アクセス プロトコルを設定できます。
- ポリシー管理
  ポリシーを作成して管理することにより、SVMからのデータ アクセスを管理できます。
- データ アクセス セキュリティ管理
  クライアントを必要とすることなく、SVMのデータにセキュリティを設定できます。
- サービスの設定
  LDAP、NIS、DNSなどのサービスを設定できます。
- ストレージ管理
  ボリューム、クォータ、qtree、およびファイルを管理できます。

- LUNの管理
  SAN環境でLUNを管理できます。
- バックアップ管理
  SnapMirrorテクノロジとNDMPを使用して、SVMデータのバックアップと管理を行うことができます。
- SVMの監視
  パフォーマンス データ、ネットワーク接続、情報、SVMの健全性などを監視できます。

注: SVM設定のトラブルシューティングまたは変更に関しては、SVM管理者はクラスタ管理者に問い合わせる必要があります。

注: Data ONTAPのコマンドライン インターフェイス（CLI）では、コマンドやパラメータ名が`vserver`のまま変更されておらず、出力にもこれまでどおり*Vserver*と表示されます。

SVMのアクセス方式と認証方式

SVM管理者は、SVMユーザ アカウントでSVMにアクセスする際に使用するアクセス方式と認証方式を理解しておく必要があります。

ユーザ アカウントのアクセス方式

SVM管理者は、クラスタ管理者によるSVMユーザ アカウントのセットアップ方法に応じて、次のアクセス方式でSVMにアクセスして管理できます。

- SSH
- Data ONTAP API

  注: Data ONTAP APIアクセス方式はHTTPSを使用します。

- SNMP

ユーザ アカウントの認証方式

SVMユーザ アカウントの認証方式は、クラスタ管理者がSVMユーザ アカウントの作成に使用したアクセス方式によって異なります。

SVMユーザ アカウントの認証には、次に示す認証方式の1つを使用できます。

- Network Information Service（NIS）とLightweight Directory Access Protocol（LDAP;ライトウェイト ディレクトリ アクセス プロトコル）（**`nsswitch`**）

  注: clustered Data ONTAPは、SVMアカウントのLDAP認証ではRFC 2307スキーマのみサポートしています。他のスキーマ（Active Directory Identity Management for UNIX[AD-IDMU]やActive Directory Services for UNIX[AD-SFU]など）はサポートされません。

- Windows Active Directory（**`domain`**）
- ユーザ パスワード（**`password`**）
- SSH公開鍵認証（**`publickey`**）
- SNMPユーザベースのセキュリティ モデル（**`usm`**）
- SNMPコミュニティ ストリング（**`community`**）
- SSL証明書認証（**`cert`**）

SVMへのログイン

SVMリソースを管理するには、SVM管理者はクラスタ管理者から提供されたユーザ名とパスワードを使用してSVMにログインします。SVM管理者は、PuTTY（Windowsオペレーティング システム用）やOpenSSH（UNIXオペレーティング システム用）などの、該当するSecure Shellクライアント アプリケーションを使用できます。

開始する前に

SVMの管理IPアドレス、ユーザ名、パスワードが必要です。

タスク概要

ログイン後は、クラスタ管理者によりそのアカウントに割り当てられた権限に応じて、次のSVMリソースのすべてまたは一部を管理できます。

- NFS、CIFS、iSCSI、FC（FCoEを含む）などのデータ アクセス プロトコル
- NIS、LDAP、DNSなどのサービス
- ボリューム、qtree、クォータ、Snapshotコピー、およびファイル
- SnapMirrorとNDMPによるデータ バックアップ
- データ セキュリティとデータ ポリシー

このほか、ネットワーク接続、ネットワーク インターフェイス、LDAPクライアント設定、SVMの健全性も監視できます。

注: clustered Data ONTAPでサポートされる暗号化アルゴリズム（サイファとも言われます）は、SSH用のAESと3DESだけです。

手順

1. SSHアプリケーションを使用してSVMにログインするには、オペレーティング システムに応じて該当する操作を実行します。

ホストで使用されているOS	操作
Windowsオペレーティング システム	**a.** SSHアプリケーションでSVMの管理IPアドレスを入力します。 **b.** ログイン プロンプトでユーザ名とパスワードを入力します。
UNIXまたはLinuxオペレーティング システム	クライアント アプリケーションで次のコマンドを入力します。 **ssh *vserver_admin_name@vserver_ip_address*** *vserver_admin_name*はユーザ名です。 *vserver_ip_address*は、SVMの管理IPアドレスです。

注: 自分自身またはクラスタ管理者がユーザ アカウント用の公開鍵を作成済みの場合は、SVM管理者はSVMにログインするためにパスワードを必要としません。

ログイン パスワードの変更

クラスタ管理者から提供されたユーザ名とパスワードを使用してSVMにログインしたあと、SVM管理者はログイン パスワードを変更できます。

タスク概要

ログイン パスワードを変更する場合は、以下のデフォルト ルールに従う必要があります。

- パスワードにユーザ名を含めることはできません。
- 8文字以上である必要があります。
- 英文字と数字がそれぞれ1文字以上含まれている必要があります。
- 直近の6つのパスワードと同じパスワードは使用できません。

手順

1. `security login password`コマンドを使用してログイン パスワードを変更します。
2. 現在のパスワードを入力します。
3. 新しいパスワードを入力します。
4. 新しいパスワードをもう一度入力してパスワードを確認します。

タスクの結果

新しいパスワードでユーザ アカウントが更新されます。以降のログインではこの新しいパスワードを入力する必要があります。

次の例は、ユーザ パスワードを変更する方法を示しています。

```
vs1.example.com::> security login password
Please enter your current password:
Please enter a new password:
Please enter it again:
vs1.example.com::>
```

SVMに関する情報の表示

SVM管理者は、`vserver show`コマンドを使用して、自分に割り当てられたStorage Virtual Machine（SVM、旧Vserver）に関する詳細を表示できます。

手順

1. SVMの情報を表示します。
   - 基本情報を表示するには、**`vserver show`**コマンドを入力します。
   - 詳細情報を表示するには、**`vserver show -instance`**コマンドを入力します。

   例

   次のコマンドを実行すると、SVMに関する基本情報が表示されます。

```
vs2.example.com::> vserver show

                                   Admin      Operational   Root
Vserver          Type    Subtype   State      State         Volume     Aggregate
-------          -----   -------   -------    --------     ----------- ----------
vs2.example.com        data               default                running
running                            root_vol2     aggr1
```

次のコマンドを実行すると、SVMに関する詳細情報が表示されます。

```
vs2.example.com::> vserver show -instance


                   Vserver Type: data
                Vserver Subtype: default
                   Vserver UUID: ca34e6b2-ddec-11df-b066-123478563412
                    Root Volume: root_vol2
                   .
                   .
                    Config Lock: false
                   IPspace Name: Default
           Is Vserver Protected: false
```

ネットワーク設定に関する情報の表示

SVM管理者は、LIF、ルーティング グループ、ゾーンなどのネットワーク設定情報を表示して、SVMのネットワーク設定を監視できます。

タスク概要

SVMのネットワーク設定について、次の要素を表示できます。

- SVMのLIF、そのDNSゾーン名、およびそのルーティング グループ
- SVMのルーティング グループ
- アクティブなネットワーク接続とリスニング ネットワーク接続

手順

1. 表示する情報に応じて、該当するコマンドを実行します。

表示する項目	入力するコマンド
SVMのルーティング グループとサブネット	**network interface show-routing-group**
SVMのLIFのDNSゾーン名	**network interface show-zones**
静的ルート	**network routing-groups route show**
ルーティング グループ	**network routing-groups show**
アクティブなネットワーク接続とリスニング ネットワーク接続	**network connections active show** または **network connections listening show**
SVMのLIF	**network interface show**

例

次の例は、SVMのLIFを表示する方法を示しています。

```
vs1.example.com::> network interface show

                  Logical    Status     Network          Current     Current Is
Vserver           Interface  Admin/Oper Address/Mask     Node        Port    Home
-----------       --------- ---------- ---------------- ---------- ------- -----
vs1.example.com   lif1        up/up     192.0.2.65/126   node0       e1b     false
                  lif2        up/up     192.0.2.1/62     node1       e0d     false

2 entries were displayed.
```

SVMの管理に関する詳細情報の参照先

SVMの管理タスクの詳細については、clustered Data ONTAPの他のドキュメントで説明しています。

SVMで実行する管理タスクに応じて、該当するドキュメントを参照してください。

状況		参照するドキュメント
ジョブおよびスケジュールの管理		*ジョブおよびスケジュールの管理*（180ページ）
データ アクセス プロトコルの設定		• *clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）* • *clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（CIFS）* • *clustered Data ONTAP 8.3 SANアドミニストレーション ガイド*
ポリシーの管理	エクスポート ポリシー	*clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）*
	ファイル ポリシー	*clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（CIFS）* Infinite Volumeを備えたSVMはファイル ポリシーをサポートしません。
	クォータ ポリシー	*clustered Data ONTAP 8.3 論理ストレージ管理ガイド* Infinite Volumeを備えたSVMはクォータ ポリシーをサポートしません。
	SnapMirrorのポリシーとルール	*clustered Data ONTAP 8.3 データ保護ガイド*
	Snapshotコピーのポリシーとスケジュール	*clustered Data ONTAP 8.3 データ保護ガイド*
	Infinite Volumeを備えたSVM用のJSON形式のデータ ポリシー	*Clustered Data ONTAP 8.3 Infinite Volumes Management Guide*
データ アクセス セキュリティの管理		• *clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）* • *clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（CIFS）*

状況	参照するドキュメント
サービスの設定	• *clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）* • *clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（CIFS）*
ストレージの管理	*clustered Data ONTAP 8.3 論理ストレージ管理ガイド*
LUNの管理	*clustered Data ONTAP 8.3 SANアドミニストレーション ガイド*
データ保護とバックアップの管理	*clustered Data ONTAP 8.3 データ保護ガイド*
SVMのパフォーマンスの監視	*クラスタのパフォーマンスの監視*（233ページ）
SVM認証の管理	*クラスタへのアクセスの管理（クラスタ管理者のみ）*（119ページ）

クラスタへのアクセスの管理（クラスタ管理者のみ）

ユーザ アカウント、アクセス制御ロールとそれらのパスワード ルール、公開鍵、デジタル証明書、Webサービス、監査設定を管理することによって、クラスタへのアクセスを制御し、セキュリティを強化できます。

ユーザ アカウントの管理

クラスタまたはStorage Virtual Machine（SVM）のユーザ アカウントを作成、変更、ロック、ロック解除、または削除したり、ユーザのパスワードをリセットしたり、すべてのユーザ アカウントに関する情報を表示したりできます。

次の方法でクラスタまたはSVMのユーザ アカウントを管理できます。

- ユーザ アカウント名、関連付けられたSVM、アクセス方法、および認証方式を指定して、ユーザのログイン方法を作成する
  必要に応じて、ユーザに割り当てるアクセス制御ロールを指定し、ユーザ アカウントについてのコメントを追加できます。
  クラスタ ユーザ アカウントは100個まで作成できます。この数には、クラスタに追加されるActive Directoryドメイン ユーザ アカウントも含まれます。SVMに対して作成できるSVMユーザ アカウントの数に制限はありません。
- アカウント名、許可されたアクセス方法、認証方式、アクセス制御ロール、アカウント コメント、アカウント ステータスなど、ユーザのログイン情報を表示する
- 現在のコンソールまたはSSHセッションで、クラスタへのログインに使用されているユーザ アカウントを表示する
- アカウント名、関連付けられたSVM、認証方式、16進値でのエンジンID、認証プロトコル、プライバシー プロトコル、セキュリティ グループなどのSNMPユーザ情報を表示する
- ユーザのログイン方法に関連付けられているアクセス制御ロールを変更する
  1つのユーザ アカウントのすべてのアクセス方法および認証方式に対して、単一のロールを使用するのが理想的です。
- アクセス方法や認証方式など、ユーザのログイン方法を削除する
- ユーザ アカウントのパスワードを変更する
- ユーザがシステムにアクセスできないように、ユーザ アカウントをロックする
- ユーザが再びシステムにアクセスできるように、以前にロックしたユーザ アカウントのロックを解除する

ユーザ アカウントを管理するには、`security login`コマンドを使用します。SNMPユーザについての情報を表示するには、`security snmpusers`コマンドを使用します。これらのコマンドの詳細については、該当するマニュアル ページを参照してください。

注: システム用に予約されている名前（「root」や「naroot」など）を使用したユーザ アカウントを作成できないようになっています。システム用に予約されている名前を使用してクラスタ、1つのSVM、またはSPにアクセスすることはできません。

関連コンセプト

アクセス制御ロールでのユーザ名およびパスワードのルール設定の管理（133ページ）

関連タスク

アクセス制御ロールのカスタマイズによる特定コマンドへのユーザ アクセスの制限（132ページ）

ユーザ アカウントへのアクセス方法

Data ONTAPは、ユーザ アカウントがストレージ システムにアクセスする方法を指定するための、いくつかの方法を提供します。

`security login`コマンドの`-application`パラメータを使用して、ユーザがストレージ システムへのアクセスに使用できる方法を指定します。サポートされるアクセス方法は次のとおりです。

- システム コンソール（**`console`**）
- HTTPまたはHTTPS（**`http`**）
- Data ONTAP API（**`ontapi`**）
- RSH（**`rsh`**）
  デフォルトでは、RSHは無効です。
- サービス プロセッサ（**`service-processor`**）
- SNMP（**`snmp`**）
- SSH（**`ssh`**）
- Telnet（**`telnet`**）
  デフォルトでは、Telnetは無効です。

Storage Virtual Machine（SVM）ユーザ アカウントでは、アクセス方法として**`console`**、**`rsh`**、**`service-processor`**、**`telnet`**を使用することはできません。

ファイアウォールが有効になっている場合は、使用するアクセス方法もファイアウォール ポリシーに追加し、アクセス要求がファイアウォールを通過できるようにする必要があります。ファイアウォール ポリシーを表示するには、`system services firewall policy show`コマンドを使用します。

関連コンセプト

CLIを使用したクラスタへのアクセス（クラスタ管理者のみ）（11ページ）

関連参照情報

ユーザ アカウントの管理用コマンド（125ページ）

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ：system services firewall policy show - Show firewall policies

ユーザ アカウントの認証方式

Data ONTAPには、ユーザ アカウントの認証方式を指定するための複数の方法が用意されています。

ユーザ アカウントの認証方式を指定するには、`security login`コマンドの`-authmethod`パラメータを使用します。次の認証方式がサポートされています。

- SSL証明書認証（**`cert`**）
- SNMPコミュニティ ストリング（**`community`**）

- Windows Active Directory認証（**domain**）
  Windows Active Directory認証を使用する場合、Storage Virtual Machine（SVM）用にCIFSサーバを作成し、クラスタおよびSVMアクセスに対して`security login create`コマンドの`-authmethod`パラメータを**domain**に設定して、Windowsドメインのユーザまたはグループをアクセス制御ロールにマッピングする必要があります。
  さらに、Windows Active Directoryドメインのユーザまたはグループをクラスタ アクセスに対して認証するには、CIFS対応SVM経由のトンネルを設定する必要があります。

- LDAPまたはNIS認証（**nsswitch**）
  LDAPおよびNISの認証は、クラスタとSVMのユーザ アカウントでサポートされます。LDAPまたはNISを認証に使用するには、クラスタまたはSVMをLDAPまたはNIS用に設定し、`security login create`コマンドの`-authmethod`パラメータを**nsswitch**に設定してユーザをアクセス制御ロールにマッピングする必要があります。
  Data ONTAPは、SVMアカウントのLDAP認証ではRFC 2307スキーマのみサポートしています。他のスキーマ（Active Directory Identity Management for UNIX[AD-IDMU]やActive Directory Services for UNIX[AD-SFU]など）はサポートされません。また、ユーザ アカウントのLDAP認証でサポートされるパスワード暗号化メカニズムはMD5とDESのみです。

- ユーザ パスワード（**password**）

- SSH公開鍵認証（**publickey**）

- SNMPユーザベースのセキュリティ モデル（**usm**）

関連タスク

ADユーザとグループに対するクラスタおよびSVMへのアクセスの許可（121ページ）
NISまたはLDAPユーザに対するクラスタへのアクセスの許可（123ページ）

関連参照情報

ユーザ アカウントの管理用コマンド（125ページ）

認証方式に公開鍵とパスワードの両方が含まれる場合の認証動作

ユーザがSSHを使用してクラスタまたはStorage Virtual Machine（SVM）にアクセスし、ユーザ アカウントが**publickey**と**password**の両方の認証方式で設定されている場合（`security login`コマンドの`-authmethod`パラメータ）、ユーザは最初に公開鍵で認証されます。

公開鍵の認証に失敗した場合は、次の処理が実行されます。

- 認証用のパスワードを入力するようにメッセージが表示されます。

- パスワードの有効期限機能（`security login role config modify`コマンドの`-passwd-expiry-time`パラメータ）が有効になっており、かつユーザ パスワードが失効している場合は、アカウントへアクセスを許可する前に、パスワードを変更するようにメッセージが表示されます。

ADユーザとグループに対するクラスタおよびSVMへのアクセスの許可

Active Directory（AD）ドメイン ユーザおよびグループに対し、クラスタおよびSVMへのアクセスを許可することができます。ADグループにアクセスを許可すると、そのグループ内のすべてのADユーザがクラスタまたは指定したSVMにアクセスできるようになります。

開始する前に

- アクセスを許可するADユーザまたはグループが、ADサーバ上に存在する必要があります。

- ADドメインのユーザとグループがクラスタまたはSVMにアクセスできるようにするためには、（できれば同じNTPサーバを使用して）クラスタ時間とADドメイン コントローラの時間差を5分以内に維持する必要があります。

手順

1. クラスタ アクセス用にADユーザまたはグループを設定する場合は、次のいずれかの手順を実行します。
   - CIFSサーバが作成されているデータSVMがすでにクラスタにある場合は、`security login domain-tunnel create`コマンドの`-vserver`パラメータをそのデータSVMに設定することで、データSVMを認証トンネルとして使用できます。
     `security login domain-tunnel show`コマンドは、指定された認証トンネルを表示します。
   - CIFSサーバが作成されているデータSVMがクラスタにない場合は、クラスタ内の任意のデータSVMをドメインに追加することができます。そのためには、`vserver active-directory create`コマンドの`-vserver`パラメータをそのデータSVMに設定します。
     データSVMをドメインに追加してもCIFSサーバは作成されません（CIFSライセンスは必要ありません）。ただし、SVMまたはクラスタ レベルでのADユーザとグループの認証が可能になります。
2. `security login create`コマンドに`-authmethod`パラメータを**`domain`**に設定して使用し、ADユーザまたはグループにクラスタまたはSVMへのアクセスを許可します。

   `-user-or-group-name`パラメータの値は、*`domainname`**`username`*の形式で指定する必要があります。*`domainname`*はCIFSドメイン サーバの名前、*`username`*はアクセスを許可するADユーザまたはグループの名前です。

   ADユーザ認証とADグループ認証の場合、`-application`パラメータに指定できる値は**`ssh`**と**`ontapi`**のみです。

   認証トンネルを削除すると、クラスタはADログイン セッションを認証できなくなり、ADユーザとグループはクラスタにアクセスできません。認証トンネルを削除する前に認証されたオープンセッションは影響を受けません。

ADユーザまたはグループに対するクラスタまたはSVMへのアクセス許可例

次の例では、クラスタでADユーザまたはグループの認証に使用するトンネルとして「vs1」データSVMを指定してから、認証トンネルを表示します。

```
cluster1::> security login domain-tunnel create -vserver vs1

cluster1::> security login domain-tunnel show
    Tunnel Vserver: vs1
```

次のコマンドを実行すると、「DOMAIN1」ドメインの「Administrator」ADユーザが、SSHを使用してクラスタにアクセスできるようになります。

```
cluster1::> security login create -vserver cluster1
-user-or-group-name DOMAIN1\Administrator -application ssh
-authmethod domain
```

次のコマンドを実行すると、「DOMAIN1」ドメイン内の「group1」ADグループのすべてのユーザが、SSHを使用してクラスタにアクセスできるようになります。

```
cluster1::> security login create -vserver cluster1
-user-or-group-name DOMAIN1\group1 -application ssh
-authmethod domain
```

次のコマンドを実行すると、「DOMAIN1」ドメインの「Administrator」 ADユーザが、SSHを使用して「vs1」 SVMにアクセスできるようになります。

```
cluster1::> security login create -vserver vs1
-user-or-group-name DOMAIN1\Administrator -application ssh
-authmethod domain
```

次のコマンドを実行すると、「DOMAIN1」ドメイン内の「group1」 ADグループのすべてのユーザが、SSHを使用して「vs2」 SVMにアクセスできるようになります。

```
cluster1::> security login create -vserver vs2
-user-or-group-name DOMAIN1\group1 -application ssh
-authmethod domain
```

関連コンセプト

クラスタ時間の管理（クラスタ管理者のみ）（166ページ）

関連タスク

クラスタまたはSVMがクライアントであるSSLサーバを認証するためのサーバCA証明書のインストール（147ページ）

関連情報

clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（CIFS）

NISまたはLDAPユーザに対するクラスタへのアクセスの許可

LDAPまたはNISサーバにユーザ データベースを格納している場合、クラスタ（管理SVM）に対してLDAPまたはNISを設定し、ネーム サービス ソースにLDAPまたはNISを追加し、ユーザ アカウントに**nsswitch**認証方式を追加することで、データベース内のユーザがクラスタにアクセスできるようになります。

手順

1. クラスタにLDAPを設定します。

   a. `vserver services name-service ldap client create`コマンドの`-vserver`パラメータでクラスタ名を指定して、クラスタに対するLDAPクライアント設定を作成します。

      例

      次の例では、「cluster1」という名前のクラスタに対する「corp」という名前のLDAPクライアント設定を作成しています。このクライアント設定では、IPアドレスが「172.160.0.100」と「172.16.0.101」のLDAPサーバに匿名でバインドします。

      ```
      cluster1::> vserver services name-service ldap client create
      -vserver cluster1 -client-config corp -servers
      172.16.0.100,172.16.0.101
      ```

      `vserver services name-service ldap client show`コマンドを使用して、LDAPクライアント設定を表示できます。

   b. `vserver services name-service ldap create`コマンドで`-vserver` *`cluster_name`* パラメータと`-client-enabled true`パラメータを指定して、クラスタでLDAPを有効にします。

例

次の例では、LDAPクライアント設定「corp」をクラスタ「cluster1」に関連付け、クラスタでLDAPクライアントを有効にしています。

```
cluster1::> vserver services name-service ldap create
-vserver cluster1 -client-config corp -client-enabled true
```

`vserver services name-service ldap show`コマンドを使用して、LDAP設定を表示できます。

2. クラスタにNISドメインを設定するには、`vserver services name-service nis-domain create`コマンドで`-vserver` *`cluster_name`*パラメータを指定します。

例

次の例では、クラスタ「cluster1」に対するNISドメイン設定を作成しています。NISドメインの名前は「nisdomain」で、作成時にアクティブになり、IPアドレスが「192.0.2.180」のNISサーバを使用するように設定しています。

```
cluster1::> vserver services name-service nis-domain create
-vserver cluster1 -domain nisdomain -active true -servers 192.0.2.180
```

`vserver services name-service nis-domain show`コマンドを使用して、NISドメイン設定を表示できます。

3. 必要に応じて、`vserver services name-service ns-switch modify`コマンドで`-database passwd`、`-vserver` *`cluster_name`*、および`-sources`の各パラメータを指定して、ネーム サービス ソースの参照順序を変更します。

`passwd`データベースでは、有効なネーム サービス ソースとして**`files`**、**`ldap`**、および**`nis`**がサポートされます。これらのソースが`-sources`パラメータで指定した順序で参照されます。

例

次の例では、クラスタ「cluster1」の**`passwd`**データベースのネーム サービス ソースの順序を変更しています。クラスタのユーザ認証に使用するソースをローカル ファイル、LDAP、NISの順に参照するように設定しています。

```
cluster1::> vserver services name-service ns-switch modify
-vserver cluster1 -database passwd -sources files,ldap,nis
```

`vserver services name-service ns-switch show`コマンドを使用して、ネーム サービス スイッチ設定を表示できます。

4. `security login create`コマンドで`-authmethod nsswitch`パラメータと`-vserver` *`cluster_name`*パラメータを指定して、LDAPまたはNISのユーザ アカウントでクラスタにアクセスする際の認証方式を**`nsswitch`**に設定します。

例

次の例では、LDAPサーバまたはNISサーバの「john」という名前のユーザがクラスタ「cluster1」にSSHを使用してアクセスできるように設定しています。

```
cluster1::> security login create -vserver cluster1
-user-or-group-name john -application ssh -authmethod nsswitch
```

`security login show`コマンドを使用して、ユーザのログイン方法を表示できます。

関連情報

clustered Data ONTAP 8.3 ファイル アクセス管理ガイド（NFS）
clustered Data ONTAP 8.3.1マニュアル ページ：vserver services name-service ldap client create - Create an LDAP client configuration
clustered Data ONTAP 8.3.1マニュアル ページ：vserver services name-service ldap create - Create an LDAP configuration
clustered Data ONTAP 8.3.1マニュアル ページ：vserver services name-service nis-domain create - Create a NIS domain configuration
clustered Data ONTAP 8.3.1マニュアル ページ：vserver services name-service ns-switch modify - Change a Name Service Switch table entry
clustered Data ONTAP 8.3.1マニュアル ページ：security login create - Add a login method

ユーザ アカウントの管理用コマンド

ユーザ アカウントを管理するには、`security login`および`security snmpusers`コマンドを使用します。

状況	使用するコマンド
クラスタまたはSVMへのユーザ アクセスのログイン方法を、サポートされているアプリケーション タイプまたは認証方式で作成する	*`security login create`*
クラスタまたはSVMへのアクセス用に作成されたユーザ アカウントに関する情報を表示する	*`security login show`*
現在のコンソールまたはSSHセッションでクラスタへのログインに使用されているユーザ アカウントを表示する	*`security login whoami`*
SNMPユーザに関する情報を表示する	*`security snmpusers`*
クラスタまたはSVMへのアクセス用に作成されたユーザのログイン方法のアクセス制御ロールを変更する	*`security login modify`* **注:** 1つのユーザ アカウントのすべてのアクセス方法および認証方式に対して、単一のロールを使用するのが理想的です。
クラスタまたはSVMへのアクセス用に作成されたユーザ ログイン方法を削除する	*`security login delete`*
ユーザのパスワードを変更する	*`security login password`* **注:** 自分のユーザ アカウントのパスワードを変更する際には、最初に現在のパスワードの入力を求められます。現在のパスワードが不明な場合、「admin」ロールを持つ別のクラスタ管理者に、このコマンドを実行してパスワードをリセットしてもらってください。
ユーザ アカウントをロックする	*`security login lock`* **注:** Data ONTAPを使用するには、「admin」ロール権限があるクラスタ ユーザ アカウントが1つ以上存在し、**`console`**アプリケーション タイプのロックが解除されている必要があります。
ユーザ アカウントのロックを解除する	*`security login unlock`*

状況	使用するコマンド
Active Directoryドメイン ユーザのクラスタ アクセスを認証するためのトンネルとして使用する、CIFS対応のStorage Virtual Machine（SVM）を指定する	`security login domain-tunnel create`
Active Directoryドメイン ユーザの認証に使用するトンネルを変更する	`security login domain-tunnel modify`
Active Directoryドメイン ユーザの認証に使用するトンネルを表示する	`security login domain-tunnel show`
Active Directoryドメイン ユーザの認証に使用するトンネルを削除する	`security login domain-tunnel delete`

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

アクセス制御ロールの管理

Role-Based Access Control（RBAC;ロールベース アクセス制御）は、ユーザの管理アクセスをそのユーザのロールに付与されたレベルに制限します。管理者は、割り当てられたロールに基づいてユーザを管理できます。Data ONTAPには、複数の事前定義されたロールが用意されています。追加のアクセス制御ロールを作成したり、変更したり、削除したりできます。また、特定のロールのユーザに対してアカウント制限を指定することもできます。

アクセス制御ロールは、次の方法で管理できます。

- アクセス制御ロールを作成し、そのロールのユーザがアクセスできるコマンドまたはコマンド ディレクトリを指定する
- コマンドまたはコマンド ディレクトリに対するロールのアクセス レベルを制御し、コマンドまたはコマンド ディレクトリに適用されるクエリを指定する
- アクセス制御ロールのコマンドまたはコマンド ディレクトリへのアクセスを変更する
- ロール名、ロールがアクセスできるコマンドまたはコマンド ディレクトリ、アクセス レベル、クエリなど、アクセス制御ロールに関する情報を表示する
- アクセス制御ロールを削除する
- ユーザのアクセスを指定した一連のコマンドのみに制限する
- アクセス制御ロールのアカウントの制限とユーザ名およびパスワードの設定を変更する
- アクセス制御ロールまたはユーザ アカウントに関する制限の現在の設定を表示する
- Data ONTAP APIとそれに対応するCLIコマンドを表示する

Data ONTAPでは、事前定義されているロールは変更できません。

アクセス制御ルールを管理するには、`security login role`コマンドと`security login role config`コマンドを使用します。

クラスタ管理者の事前定義されたロール

Data ONTAPには、クラスタ ユーザ アカウント用に複数の事前定義されたロールがあります。追加のロールも作成できます。

次の表に、Data ONTAPの事前定義されたロールとコマンド ディレクトリへのアクセス レベルを示します。

ロール	アクセス レベル	コマンド ディレクトリまたはディレクトリ
admin	**all**	すべてのコマンド ディレクトリ（**デフォルト**）
autosupport	**all**	• `set` • `system node autosupport`
	none	その他のすべてのコマンド ディレクトリ（**デフォルト**）
backup	**all**	`vserver services ndmp`
	readonly	`volume`
	none	その他のすべてのコマンド ディレクトリ（**デフォルト**）
readonly	**all**	• `security login password` • `set`
	none	`security`
	readonly	その他のすべてのコマンド ディレクトリ（**デフォルト**）
none	**none**	すべてのコマンド ディレクトリ（**デフォルト**）

追加のロールを作成するには、`security login role create`コマンドを使用します。

注: 事前定義の**autosupport**ロールには事前定義の**autosupport**アカウントが含まれます。**autosupport**ロールと**autosupport**アカウントはAutoSupport OnDemandで使用されます。Data ONTAPでは、**autosupport**アカウントを変更または削除することはできません。また、**autosupport**ロールにユーザ アカウントを追加することもできません。

SVM管理者の事前定義されたロール

SVM管理者のロールとして、vsadmin、vsadmin-volume、vsadmin-protocol、vsadmin-backup、およびvsadmin-readonlyの5つのロールが事前に定義されています。これらの事前定義されたロールに加え、一連の権限を割り当ててカスタマイズしたSVM管理者ロールを作成できます。

SVMには、それぞれ独自のユーザおよび管理者認証ドメインを設定できます。SVMとユーザ アカウントを作成したあとに、SVMの管理をSVM管理者に委譲できます。

注: Infinite Volumeを備えたSVMではクォータ、qtree、およびLUNはサポートされません。したがって、SVM管理者はInfinite Volumeを備えたSVMでは、クォータ、qtree、およびLUNに関連するタスクを実行できません。

次の表に、SVM管理者の事前定義されたロールとその権限を示します。

SVM管理者のロール名	説明
vsadmin	このロールは、SVMのスーパーユーザ ロールであり、デフォルトで割り当てられます。このロールのSVM管理者には、次の権限があります。 • 自身のユーザ アカウントのローカル パスワードとキー情報の管理 • ボリューム、クォータ、qtree、Snapshotコピー、およびファイルの管理 • LUNの管理 • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健常性の監視 vsadminロールは、デフォルトで割り当てられています。
vsadmin-volume	このロールのSVM管理者には、次の権限があります。 • 自身のユーザ アカウントのローカル パスワードとキー情報の管理 • ボリューム、クォータ、qtree、Snapshotコピー、およびファイルの管理 • LUNの管理 • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • サービスの設定：DNS、LDAP、NIS • ネットワーク インターフェイスの監視 • SVMの健常性の監視
vsadmin-protocol	このロールのSVM管理者には、次の権限があります。 • 自身のユーザ アカウントのローカル パスワードとキー情報の管理 • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • サービスの設定：DNS、LDAP、NIS • LUNの管理 • ネットワーク インターフェイスの監視 • SVMの健常性の監視

SVM管理者のロール名	説明
vsadmin-backup	このロールのSVM管理者には、次の権限があります。 • 自身のユーザ アカウントのローカル パスワードとキー情報の管理 • NDMP処理の管理 • リストアしたボリュームの読み取り / 書き込み許可 • SnapMirror関係とSnapshotコピーの管理 • ボリュームとネットワーク情報の表示
vsadmin-readonly	このロールのSVM管理者には、次の権限があります。 • 自身のユーザ アカウントのローカル パスワードとキー情報の管理 • SVMの健常性の監視 • ネットワーク インターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

アクセス制御ロールのカスタマイズに関する考慮事項

Data ONTAPには、クラスタとStorage Virtual Machine（SVM）の管理者用に事前定義されたアクセス制御ロールがあります。クラスタまたはSVM用に追加のアクセス制御ロールを作成して、特定のコマンドまたはコマンド ディレクトリへのロールのアクセスをカスタマイズできます。特定のアクセス用のロールをカスタマイズするときは、いくつかの考慮事項があります。

構文に関する考慮事項

- アクセス制御ロールには、次の要素を含むルール（`security login role create`コマンドで指定）が1つ以上含まれている必要があります。
  - SVM名（`-vserver`）
    これは、ロールが属する管理SVM（クラスタ）またはデータSVMの名前です。
  - ロール名（`-role`）
  - 権限（`-cmddirname`）
    権限は、ロールのアクセス レベルを指定するコマンド（*組み込み*または*非組み込み*）またはコマンド ディレクトリです。
    ロールのカスタマイズに関しては、*組み込みコマンド*は末尾に`create`、`modify`、`delete`、または`show`があるすべてのコマンドのことです。他のコマンドはすべて*非組み込みコマンド*と呼ばれます。
  - アクセス レベル（`-access`）
    アクセス レベルには、**`all`**、**`readonly`**、または**`none`**を指定できます。
    アクセス レベルの指定方法は、付与する権限がコマンドとコマンド ディレクトリのどちらかであるかと、コマンドの場合はコマンドが組み込みと非組み込みのどちらであるかによって異なります。
- コマンド ディレクトリに対するロールのアクセスを指定する場合、デフォルトでは、そのアクセスはすべてのサブディレクトリと、ディレクトリおよびサブディレクトリ内のすべてのコマンドに適用されます。

ロールに付与する権限	指定するアクセス レベル	効果
コマンド ディレクトリ	**all**	ロールは、指定したディレクトリとそのサブディレクトリ（存在する場合）にアクセスでき、ディレクトリとサブディレクトリ内のすべてのコマンドを実行できます。
	readonly	ロールは、指定したディレクトリとそのサブディレクトリ（存在する場合）に読み取り専用でアクセスできます。 この組み合わせでは、ロールのアクセスは、指定したディレクトリとサブディレクトリ内の`show`コマンドのみに制限されます。ディレクトリ内の他のすべてのコマンドには、ロールはアクセスできません。
	none	ロールは、指定したディレクトリ、そのサブディレクトリ、およびコマンドにアクセスできません。

たとえば、次のコマンドでは、「vs1」SVMの「vol_role」ロールに、`volume`ディレクトリ、その全サブディレクトリ、およびディレクトリとサブディレクトリ内のコマンドへの**`all`**アクセスが付与されます。

```
security login role create -vserver vs1 -role vol_role -cmddirname "volume" -
access all
```

- サブディレクトリのアクセスが指定されている場合、親ディレクトリのアクセスよりも優先されます。
  親ディレクトリに特定のアクセス レベルが指定されていて、そのサブディレクトリに別のアクセス レベルが指定されている場合、サブディレクトリに指定されているアクセス レベルが親ディレクトリのアクセス レベルより優先されます。
  たとえば、次のコマンドでは、「vs1」SVMの「vol_role」ロールに、`volume`ディレクトリとそのサブディレクトリ内のコマンドへの**`all`**アクセスが付与されますが、`volume snapshot`サブディレクトリは例外であり、このサブディレクトリへのロールのアクセスは**`readonly`**に制限されます。

```
security login role create -vserver vs1 -role vol_role -cmddirname "volume" -
access all

security login role create -vserver vs1 -role vol_role -cmddirname "volume
snapshot" -access readonly
```

- コマンドに指定できるアクセス レベルは、コマンドが組み込みと非組み込みのどちらかによって異なります。

ロールに付与する権限	指定するアクセス レベル	効果
組み込みコマンド（末尾が`create`、`modify`、`delete`、または`show`のコマンド）	**all**	無効な組み合わせです。組み込みコマンドにはアクセス レベルを指定できません。アクセス レベルは、組み込みコマンドの *ディレクトリ*に指定する必要があります。
	readonly	
	none	

ロールに付与する権限	指定するアクセスレベル	効果
非組み込みコマンド	**all**	ロールは、指定したコマンドを実行できます。
	readonly	無効な組み合わせです。**readonly**アクセスは、コマンド レベルでは付与できません。*ディレクトリ*レベルで指定する必要があります。
	none	ロールは、指定したコマンドにはアクセスできません。

たとえば、次のコマンドでは、「vs1」SVMの「ssl_role」ロールがsecurity sslディレクトリ内のsecurity ssl showコマンドにアクセスできるようになりますが、このディレクトリ内の他のコマンドにはアクセスできません。

```
security login role create -vserver vs1 -role ssl_role -cmddirname "security
ssl" -access readonly
```

次の例では、最初の4つのコマンドは、コマンド ディレクトリを使用して「cluster1」クラスタの「login_role」ロールのアクセスをsecurity login show組み込みコマンドに制限し、最後の2つのコマンドは、ロールにsecurity login passwordおよびsecurity login role show-ontapi非組み込みコマンドへの追加のアクセスを付与しています。このロールは、security loginディレクトリ内の他のコマンドにはアクセスできません。

```
security login role create -vserver cluster1 -role login_role -cmddirname
"security login" -access readonly

security login role create -vserver cluster1 -role login_role -cmddirname
"security login domain-tunnel" -access none

security login role create -vserver cluster1 -role login_role -cmddirname
"security login publickey" -access none

security login role create -vserver cluster1 -role login_role -cmddirname
"security login role" -access none

security login role create -vserver cluster1 -role login_role -cmddirname
"security login password" -access all

security login role create -vserver cluster1 -role login_role -cmddirname
"security login role show-ontapi" -access all
```

- カスタマイズされたロールの場合、アクセス レベルを指定しないコマンドおよびコマンド ディレクトリはデフォルトのレベルである**none**になり、ロールは指定されていないコマンドやコマンド ディレクトリにはアクセスできません。

一般的な考慮事項

- Data ONTAPでは、事前定義されているロールは変更できません。
- カスタマイズされたロールには、security login passwordコマンドへの**all**アクセスを付与して、そのロールのユーザが自分のパスワードを変更できるようにすることを推奨します。
  たとえば、次のコマンドでは、「vs1」SVMの「guest_role」ロールに、アカウント パスワードを変更する権限が付与されます。

  ```
  security login role create -vserver vs1 -role guest_role -cmddirname "security
  login password" -access all
  ```

- SVMロールに、クラスタ管理者のみが使用できるコマンドやコマンド ディレクトリへのアクセスを付与することはできません。

たとえば、ライセンスを管理する権限があるのはクラスタ管理者のみであるため、SVMロールにsystem licenseディレクトリまたはこのディレクトリのコマンドへのアクセスを付与することはできません。あるコマンドにSVM管理者がアクセスできるかどうかは、マニュアル ページを参照してください。

関連タスク

アクセス制御ロールのカスタマイズによる特定コマンドへのユーザ アクセスの制限（132ページ）

アクセス制御ロールのカスタマイズによる特定コマンドへのユーザ アクセスの制限

クラスタ管理者は、指定したコマンドでアクセス制御ロールをカスタマイズし、ユーザ アカウントをそのロールにマッピングすることにより、ユーザが特定のコマンドにしかアクセスできないように制限できます。

手順

1. 指定されたコマンドのみに制限されるか、-cmddirnameパラメータを指定したsecurity login role createコマンドを使用して実行する、カスタマイズされたアクセス制御ロールを作成します。

   security login role showコマンドは、ロールがアクセスできるコマンドを表示します。

2. -roleパラメータを指定してsecurity login createコマンドを実行することにより、ユーザ アカウント用のログイン方法を作成し、カスタマイズされたロールにこのログイン方法をマッピングします。

アクセス制御ロールをカスタマイズしてユーザ アカウント アクセスを制限する例

次の例では、volume snapshotコマンドのみにアクセスが制限された「vol_snapshot」という名前のアクセス制御ロールと、「vol_snapshot」ロールが割り当てられた「snapshot_admin」という名前の「vs1」Storage Virtual Machine（SVM、旧Vserver）ユーザ アカウントを作成しています。このユーザには、このロールで定義されているように、volume snapshotコマンドに対するフル アクセス権限があります。このユーザは、SSHを使用してSVMと認証パスワードにアクセスできます。

```
cluster1::> security login role create -vserver vs1 -role vol_snapshot
-cmddirname "volume snapshot"

cluster1::> security login role show -vserver vs1 -role vol_snapshot
           Role          Command/                                Access
Vserver    Name          Directory                         Query Level
---------- ------------- --------- ---------------------------- --------
vs1        vol_snapshot  DEFAULT                                none
vs1        vol_snapshot  volume snapshot                        all
2 entries were displayed.

cluster1::> security login create -vserver vs1 -user-or-group-name snapshot_admin
-application ssh -authmethod password -role vol_snapshot

Please enter a password for user 'snapshot_admin':
Please enter it again:

cluster1::>
```

次の例では、アクセス制御ロール名「sec_login_readonly」を作成しています。このロールは、security loginディレクトリに対して読み取り専用のアクセス権限を持ちますが、security login domain-tunnel、security login publickey、およびsecurity login roleサブディレクトリにはアクセス権限を持たないようにカスタマイズされています。このため、このロールはsecurity login showコマンドにしかアクセスできません。続いて「new_admin」という名前のクラスタ ユーザ アカウントが作成され、「sec_login_readonly」ロールが割り当てられています。このユーザは、コンソールを使用してクラスタと認証パスワードにアクセスできます。

```
cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login" -access readonly

cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login domain-tunnel" -access none

cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login publickey" -access none

cluster1::> security login role create -vserver cluster1 -role sec_login_readonly
-cmddirname "security login role" -access none

cluster1::> security login role show -vserver cluster1 -role sec_login_readonly
  (security login role show)
           Role                 Command/                          Access
Vserver    Name                 Directory                   Query Level
---------- -------------------- --------- ---------------------- --------
cluster1   sec_login_readonly   DEFAULT                          none
cluster1   sec_login_readonly   security login                   readonly
cluster1   sec_login_readonly   security login domain-tunnel     none
cluster1   sec_login_readonly   security login publickey         none
cluster1   sec_login_readonly   security login role              none
5 entries were displayed.

cluster1::> security login create -vserver cluster1 -user-or-group-name new_admin
-application console -authmethod password -role sec_login_readonly

Please enter a password for user 'new_admin':
Please enter it again:

cluster1::>
```

関連コンセプト

ユーザ アカウントの管理（119ページ）
アクセス制御ロールのカスタマイズに関する考慮事項（129ページ）

関連参照情報

ユーザ アカウントの管理用コマンド（125ページ）
アクセス制御ロールの管理用コマンド（135ページ）

アクセス制御ロールでのユーザ名およびパスワードのルール設定の管理

ユーザ名およびパスワードのデフォルトのルールが、すべてのアクセス制御ロールのユーザに適用されます。特定のロールのユーザ名およびパスワードのルール設定を変更し、ユーザ アカウントのセキュリティを強化できます。

ユーザ名のデフォルトのルールは次のとおりです。

- ユーザ名は、3文字以上である必要があります。
- ユーザ名には、英数字と特殊文字、またはこれらの組み合わせを使用できます。
  ローカル ユーザ名（**password**または**publickey**認証方式で設定するユーザ名）の場合、特殊文字に関する次のルールが追加で適用されます。
  - 次の文字のみがサポートされます。

    _ . -
  - ユーザ名の1文字目をハイフン（-）にすることはできません。
- **password**認証方式で設定するユーザ名は16文字以下にする必要があります。
- **snmp**認証方式で設定するユーザ名は32文字以下にする必要があります。

パスワードのデフォルトのルールは次のとおりです。

- パスワードにユーザ名を含めることはできません。

- 8文字以上である必要があります。
- 英文字と数字がそれぞれ1文字以上含まれている必要があります。
- 直近の6つのパスワードと同じパスワードは使用できません。

ユーザ アカウントのセキュリティを強化するために、security login role config modifyコマンドのパラメータを使用して、アクセス制御ロールの次の設定を変更できます。

- ユーザ名のルール設定は次のとおりです。
  - ユーザ名の必須最小長（-username-minlength）
  - ユーザ名に英文字と数字を混在させる必要があるかどうか（-username-alphanum）
- パスワードのルール設定は次のとおりです。
  - パスワードの必須最小長（-passwd-minlength）
  - パスワードに英文字と数字を混在させる必要があるかどうか（-password-alphanum）
  - パスワード内の必須特殊文字数（-passwd-min-special-chars）
  - ユーザが初めてアカウントにログインしたときにパスワードを変更する必要があるかどうか（-require-initial-passwd-update）
    ユーザは、SSHまたはシリアル コンソール接続からのみ、初期パスワードを変更できます。
  - 再利用できない前のパスワードの数（-disallowed-reuse）
  - 前回のパスワード変更から次に変更するまでに必要な最小日数（-change-delay）
  - パスワードが期限切れになるまでの日数（-passwd-expiry-time）
- 初期ログイン試行についてのルール設定は次のとおりです。
  - アカウントの自動ロックをトリガーする無効なログイン試行の回数（-max-failed-login-attempts）
    ユーザによる無効なログイン試行の回数がこのパラメータで指定された値に達した場合、ユーザのアカウントは自動的にロックされます。
    ユーザ アカウントのロックを解除するには、security login unlockコマンドを使用します。
  - 無効なログイン試行が許容最大回数に到達した場合に、アカウントをロックする日数（-lockout-duration）

ルールの現在の設定は、security login role config showコマンドで表示できます。security login role configコマンドとデフォルト設定については、マニュアル ページを参照してください。

関連参照情報

アクセス制御ロールの管理用コマンド（135ページ）

パスワード ルールの設定に関する考慮事項

パスワード ルール設定の中には、ロールのユーザにパスワードの変更を求めるものがあります。ユーザがパスワードを変更できるようにするには、ユーザ アカウントに適切なアクセス方法を設定するとともに、パスワードのリセット コマンドを実行する権限をユーザのロールに与える必要があります。

次のいずれかの状況において、ロールのユーザはパスワードを変更する必要があります。

- ロールのパスワード設定により、ユーザは初めてアカウントにログインするときにパスワードの変更を求められます。
  この設定は、`security login role config modify`コマンドの`-require-initial-passwd-update`パラメータで定義します。
- ロールは、一定の間隔でユーザ パスワードの期限が切れるように設定されます。
  この設定は、`security login role config modify`コマンドの`-passwd-expiry-time`パラメータで定義します。

ユーザによるパスワード変更を可能にするには、以下の条件を満たす必要があります。

- ユーザに、SSHアクセス権またはコンソール アクセス権を与える必要があります。
  パスワードの変更は、そのアカウント ユーザにより、SSH接続またはコンソール接続を介してのみ可能です。
  指定されたアクセス方法をユーザに許可するには、`security login modify`コマンドの`-application`パラメータを使用します。

  注: Storage Virtual Machine（SVM）ユーザ アカウントには、コンソール アクセスはサポートされていません。

- ユーザのロールに、パスワードを変更するコマンド（`security login password`コマンド）の実行権限がある必要があります。
  コマンドまたはコマンド ディレクトリを実行する権限をロールに与えるには、`-cmddirname`パラメータを指定して`security login role modify`コマンドを実行します。

関連コンセプト

ユーザ アカウントへのアクセス方法（120ページ）

関連タスク

アクセス制御ロールのカスタマイズによる特定コマンドへのユーザ アクセスの制限（132ページ）

アクセス制御ロールの管理用コマンド

`security login role`コマンドは、特定のロールを持つユーザのシステムに対するアクセス レベルを制御します。`security login role config`コマンドを使用して、特定のロールに対するユーザ名とパスワードのルール設定を管理し、ユーザ アカウントのセキュリティを強化します。

状況	使用するコマンド
アクセス制御ロールを作成し、そのロールでアクセスできるコマンドまたはコマンド ディレクトリを指定する	*`security login role create`*
アクセス制御ロールがアクセスできるコマンドまたはコマンド ディレクトリを変更する	*`security login role modify`*
アクセス制御ロールに関する情報を表示する	*`security login role show`*
Data ONTAP APIとそれに対応するCLIコマンドを表示する	*`security login role show-ontapi`*
アクセス制御ロールを削除する	*`security login role delete`*

状況	使用するコマンド
特定のアクセス制御ロールに対する次のアカウント制限とルール設定を変更する • ユーザ名の必須最小長 • ユーザ名に英文字と数字を混在させる必要があるかどうか • パスワードの必須最小長 • パスワードに英文字と数字を混在させる必要があるかどうか • パスワードで要求される特殊文字の最小数 • ユーザが自分のアカウントに最初にログインする場合にパスワードを変更する必要があるか • 以前使用していた再利用できないパスワードの数 • 次回のパスワード変更までに経過する必要がある最小日数 • パスワードが期限切れになるまでの日数 • アカウントの自動ロックをトリガーする無効なログイン試行の回数 • 無効なログイン試行の最大回数に達してからアカウントがロックされる日数	`security login role config modify`
ユーザ アカウント制限とルール設定を表示する	`security login role config show`

状況	使用するコマンド
次の設定をデフォルト値にリセットする： • パスワードに必要な特殊文字数（`-passwd-min-special-chars` **0**） • ユーザが初めてアカウントにログインしたときにパスワードを変更する必要があるかどうか（`-require-initial-passwd-update` **disabled**） • パスワードが期限切れになるまでの日数（`-passwd-expiry-time` **unlimited**） • アカウントが自動でロックされる無効なログイン試行回数（`-max-failed-login-attempts` **0**） • 最大回数を超える無効なログインが試行された場合にアカウントがロックされる日数（`-lockout-duration` **0**） Data ONTAP 8.1.2以前にリバートすると、このコマンドの実行を求めるプロンプトが表示されます。	*`security login role config reset`* （advanced権限レベル）

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

SSHセキュリティ設定の管理

セキュリティ設定の管理には、SSHキー交換アルゴリズムおよびデータ暗号化アルゴリズム（*暗号*とも呼ばれる）の管理があります。Data ONTAPでは、それぞれのSSHセキュリティ要件に従って、クラスタまたはStorage Virtual Machine（SVM）の個々のSSHキー交換アルゴリズムおよび暗号を有効または無効にすることができます。

Data ONTAPでは、クラスタおよびSVMに関して次のSSHクライアントをサポートしています。

- 次のSSHキー交換アルゴリズムがサポートされ、デフォルトで有効になっています。
  - SHA-2の**`diffie-hellman-group-exchange-sha256`** SSHキー交換アルゴリズム
  - SHA-1の**`diffie-hellman-group-exchange-sha1`**、**`diffie-hellman-group14-sha1`**、および**`diffie-hellman-group1-sha1`** SSHキー交換アルゴリズム

  SHA-2アルゴリズムはSHA-1アルゴリズムより安全です。Data ONTAPは、SSHサーバとして機能し、クライアントに適した最も安全なSSHキー交換アルゴリズムを自動的に選択します。SSHのセキュリティをさらに強化するためには、SHA-1アルゴリズムを手動で無効にして、SHA-2アルゴリズムだけを有効にしておきます。

- 暗号については、AESおよび3DES対称鍵暗号の以下のカウンタ（CTR）モードおよび暗号ブロック チェーン（CBC）モードがサポートされており、デフォルトで有効になっています。
  - **`aes256-ctr`**
  - **`aes192-ctr`**
  - **`aes128-ctr`**

- **aes256-cbc**
- **aes192-cbc**
- **aes128-cbc**
- **3des-cbc**

CTRモードの暗号はCBCモードの暗号より安全です。同じモードの暗号間では、鍵サイズが大きいほど暗号の強度が増します。Data ONTAPでサポートされている暗号の中では、**aes256-ctr**が最も安全で、**3des-cbc**が最も弱い暗号です。

クラスタおよびSVMのSSHキー交換アルゴリズムと暗号は次の方法で管理できます。

- SSHキー交換アルゴリズムと暗号の現在の設定を表示する（`security ssh show`）。
  有効なSSHキー交換アルゴリズムが、セキュリティの強度が高い順に表示されます。
  有効なCTRモード暗号（より安全）は、CBCモード暗号（安全でない）の前に表示されます。同じモード の場合、鍵サイズが大きい暗号から表示されます。
- SSHキー交換アルゴリズムまたは暗号の現在の設定を、指定した設定で置き換える（`security ssh modify`）。
  クラスタのSSHキー交換アルゴリズムまたは暗号を変更した場合、以降作成されるすべてのSVMにも変更が適用されます。
- 現在の構成にSSHキー交換アルゴリズムまたは暗号を追加する（`security ssh add`）。
  追加したSSHキー交換アルゴリズムまたは暗号は有効になります。
  SSHキー交換アルゴリズムまたは暗号をクラスタ構成に追加した場合、以降作成されるすべてのSVMにも適用されます。
- 現在の構成からSSHキー交換アルゴリズムまたは暗号を削除する（`security ssh remove`）。
  削除したSSHキー交換アルゴリズムまたは暗号は無効になります。
  SSHキー交換アルゴリズムまたは暗号をクラスタ構成から削除した場合、以降作成されるすべてのSVMにも適用されます。
  クラスタまたはSVMからすべてのSSHキー交換アルゴリズムまたは暗号を削除することはできません。
- クラスタおよびすべてのSVMのSSHキー交換アルゴリズムと暗号の設定を、Data ONTAP 8.2.1より前で使用されていた設定にリストアする（`security ssh prepare-to-downgrade`、advanced権限レベル）。
  Data ONTAP 8.2.1より前のリリースにダウングレードまたはリバートすると、このコマンドを実行して、クラスタおよびすべてのSVMのSSHセキュリティ設定を以前のリリースのデフォルト設定（以下）にリセットするように求められます。
  - サポートされているすべてのSHA-1およびSHA-2 SSHキー交換アルゴリズムが、有効な状態にリセットされます。
  - データ暗号化アルゴリズムのすべての CTRおよびCBCモードが、有効な状態にリセットされます。

  注意: `security ssh prepare-to-downgrade`コマンドは、Data ONTAP 8.2.1より前のリリースにダウングレードまたはリバートする場合以外、実行しないでください。実行した場合、SSH設定機能が完全に無効になり、SSH設定を管理することができなくなります。

SSHセキュリティ設定の管理用コマンド

`security ssh`コマンドを使用すると、Storage Virtual Machine（SVM）のSSHセキュリティ設定を管理できます。これには、SSH鍵交換アルゴリズムおよびデータ暗号化アルゴリズム（暗号）の表示、交換、追加、削除、リストアが含まれます。

状況	使用するコマンド
クラスタおよびSVMSVMのSSH鍵交換アルゴリズムと暗号の現在の設定を表示する	*`security ssh show`*
クラスタまたはSVMSVMのSSH鍵交換アルゴリズムまたは暗号の現在の設定を、指定した設定で置き換える	*`security ssh modify`*
クラスタまたはSVMの現在の設定に、SSH鍵交換アルゴリズムまたは暗号を追加する	*`security ssh add`*
クラスタまたはSVMの現在の設定から、指定したSSH鍵交換アルゴリズムまたは暗号を削除する	*`security ssh remove`*
クラスタおよびすべてのSVMのSSH鍵交換アルゴリズムおよび暗号の設定を、Data ONTAP 8.2.1より前に使用していた設定にリストアする	*`security ssh prepare-to-downgrade`* （advanced権限レベル） Data ONTAP 8.2.1よりも前のリリースにダウングレードまたはリバートすると、このコマンドの実行を求めるプロンプトが表示されます。

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

公開鍵の管理

公開鍵を関連付けたり、変更したり、削除したりして、ユーザの認証を管理できます。

公開鍵は、次の方法で管理できます。

- 有効なOpenSSH形式の既存の公開鍵をユーザ アカウントに関連付けて公開鍵を追加する
  複数の公開鍵を1つのユーザ アカウントに指定可能
- FTPやHTTPなどのUniversal Resource Identifier（URI;ユニバーサル リソース識別子）から公開鍵をロードして、ユーザ アカウントに関連付ける
  また、既存の公開鍵をロードした公開鍵で上書きすることも可能
- 公開鍵についての情報を表示する
- 特定のユーザに関連付けられた公開鍵を変更する
- 特定のユーザに関連付けられた公開鍵を削除する

公開鍵を作成または変更する場合、あるいはURIから公開鍵をロードする場合は、**公開鍵**ログイン方法を使用してユーザ アカウントを設定する必要があります（`security login create`コマンドで`-authmethod`パラメータを**`publickey`**に設定）。

公開鍵を管理するには、`security login publickey`コマンドを使用します。これらのコマンドの詳細については、該当するマニュアル ページを参照してください。

公開鍵の管理用コマンド

公開鍵を管理するには、`security login publickey`コマンドを使用します。

状況	使用するコマンド
既存の公開鍵とユーザ アカウントを関連付ける	*security login publickey create*
URIから公開鍵をロードしてユーザに関連付ける	*security login publickey load-from-uri*
公開鍵に関する情報を表示する	*security login publickey show*
特定のユーザの公開鍵を変更する	*security login publickey modify*
特定のユーザの公開鍵を削除する	*security login publickey delete*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

サーバまたはクライアント認証用のデジタル証明書の管理

デジタル証明書は、通信が暗号化されること、および指定されたサーバに対してまたは認証されたクライアントからのみ、情報が非公開かつ変更されずに送信されることを保証します。証明書署名要求を生成し、サーバまたはクライアント認証用のデジタル証明書を生成、インストール、署名、表示、取り消し、削除することができます。

デジタル証明書（*公開鍵証明書*とも呼ばれる）は、公開鍵の所有者を確認する電子ドキュメントです。自己署名（所有者による）または認証局（CA）署名のいずれかの場合があります。クラスタまたはStorage Virtual Machine（SVM）がSSLサーバまたはクライアントである場合、デジタル証明書を使用してサーバまたはクライアント認証を提供できます。サーバ認証とクライアント認証の両方を提供する場合は相互認証（*双方向認証*とも呼ばれる）と呼ばれ、サーバとクライアントの両方が自身の証明書を相手に提示し、それぞれのIDを相互に検証します。

デジタル証明書は、次の方法で管理できます（`security certificate`コマンド ファミリー）。

- 自己署名デジタル証明書を作成してインストールする
- 署名のためにCAに送信するCertificate Signing Request（CSR;証明書署名要求）を生成する
- 自己署名したルートのCAを使用してデジタル証明書に署名する
- CA署名デジタル証明書およびルートCAの公開鍵証明書をインストールする
- 作成またはインストールされたデジタル証明書に関する情報を表示する
- クラスタまたはSVMによってCAとして署名されたデジタル証明書を表示する
- 証明書のセキュリティが侵害された場合、クラスタまたはSVMによってCAとして署名されたデジタル証明書を取り消す
- 不要になったデジタル証明書を削除する

適用される動作とデフォルトの設定は次のとおりです。

- クラスタまたはSVMを作成すると、Data ONTAPによってそのクラスタまたはSVMをサーバとして認証するための自己署名デジタル証明書が自動的に作成されます。
- デフォルトでは、Data ONTAPではSHA256暗号化ハッシュ関数を使用して、CSRまたはデジタル証明書に署名します。

- デフォルトでは、Data ONTAPで生成される秘密鍵は2,048ビットです。
- デフォルトでは、Data ONTAPで生成されるデジタル証明書の有効期限は365日間に設定されますが、デジタル証明書の作成時に、有効期限の設定を指定できます。
- デフォルトでは、SSLサーバ認証は有効になりますが、SSLクライアント認証は無効になります。
  `security ssl modify`コマンドは、SSLサーバとしてのクラスタまたはSVMおよびそのクライアントのSSL認証を有効または無効にします。`-server-enabled`パラメータのデフォルトは**true**であり、`-client-enabled`パラメータのデフォルトは**false**です。`-client-enabled`パラメータを**true**に設定すると、サーバ（クラスタまたはSVM）とそのクライアントの相互認証が有効になります。

デジタル証明書の管理では、次のタイプとサブタイプが適用されます。

- 証明書タイプ（`-type`パラメータ）は証明書の用途を指定します。
  証明書タイプは、次のいずれかになります。
  - **server**は、クラスタまたはSVMをSSLサーバとして認証する証明書です。
  - **client**は、クラスタまたはSVMをSSLクライアントとして認証する証明書です。
  - **server-ca**は、クラスタまたはSVMがクライアントであるSSLサーバのルート証明書です。
  - **client-ca**は、クラスタまたはSVMがサーバであるSSLクライアントのルート証明書です。
  - **root-ca**は、クラスタまたはSVMがCAとして機能できるようにする自己署名ルートCA証明書です。
    root-ca証明書を作成すると、**client-ca**証明書および**server-ca**証明書も自動的に作成されます。**root-ca**証明書を削除すると、対応する**client-ca**証明書および**server-ca**証明書も自動的に削除されます。
- Key Management Interoperability Protocol（KMIP）の証明書サブタイプ（`-subtype kmip-cert`パラメータ）は、**client**および**server-ca**のタイプと組み合わせて適用され、クラスタと外部キー管理ツール（KMIPサーバなど）の相互認証に使用される証明書であることを示します。
  KMIP証明書は、クラスタ レベルでサポートされ、データSVMレベルではサポートされません。クラスタ レベルでサポートされる操作はインストール、削除、および表示（`security certificate install`、`security certificate delete`、および`security certificate show`）で、作成（`security certificate create`）はサポートされません。

関連コンセプト

Webプロトコル エンジンの管理（155ページ）

関連タスク

Webサービスへのアクセスの設定（159ページ）

クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール

クラスタまたはStorage Virtual Machine（SVM）がSSLサーバとして認証されるようにするためには、**server**タイプのデジタル証明書をクラスタまたはSVMにインストールします。自己署名証明書またはCA署名証明書のいずれかをインストールできます。

タスク概要

クラスタまたはSVMを作成すると、そのクラスタまたはSVMの名前を共通名とする自己署名サーバ証明書が自動的に作成されます。対応するSSLサーバ認証が有効になり、同様にクラスタまたはSVMのデフォルトの共通名が使用されます。

クラスタまたはSVMに別の共通名を使用する場合、またはサーバ認証にCA署名証明書を使用する場合は、サーバ証明書を追加で作成またはインストールすることができます。また、指定したサーバ証明書を使用するようにSSL設定を変更することもできます。

手順

1. サーバ認証用の自己署名デジタル証明書を作成するには、`security certificate create`コマンドに`-type` **`server`**パラメータを指定して使用します。
2. サーバ認証にサードパーティのCA署名デジタル証明書を使用するには、次の手順を実行します。
   a. `security certificate generate-csr`コマンドを使用して、証明書署名要求（CSR）を生成します。

      CSR出力が表示されます。この出力には証明書要求と秘密鍵が含まれています。秘密鍵のコピーは保管しておいてください。

   b. CSR出力の証明書要求をデジタル形式（Eメールなど）で信頼できるサードパーティのCAに送信し、署名を求めます。

      要求が処理されると、署名済みのデジタル証明書がCAから返信されます。秘密鍵とCA署名デジタル証明書のコピーは保管する必要があります。

   c. `-type` **`server`**パラメータを指定した`security certificate install`コマンドを使用して、サードパーティのCA署名デジタル証明書をインストールします。
   d. プロンプトが表示されたら証明書と秘密鍵を入力し、Enterキーを押します。
   e. サーバ証明書の証明書チェーンを形成するCAルート証明書と中間証明書をインストールするかどうかを尋ねられたら、「Y」を入力します。
   f. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、Enterキーを押します。

      CAの証明書は、サーバ証明書の証明書チェーンを形成するためにインストールします。チェーンは、サーバ証明書を発行したCAの証明書から始まり、CAのルート証明書まで続く場合があります。中間証明書が不足していると、サーバ証明書のインストールに失敗します。

      CA証明書の入力後、証明書チェーンが**`server-chain`**として**`server`**証明書タイプでインストールされます。

3. サーバ認証に自己CA署名デジタル証明書を使用するには（クラスタまたはSVMがCAとして署名）、次の手順を実行します。
   a. `security certificate generate-csr`コマンドを使用して、CSRを生成します。

      CSR出力が表示されます。この出力には証明書要求と秘密鍵が含まれています。秘密鍵のコピーは保管しておいてください。

   b. `security certificate create`コマンドに`-type` **`root-ca`**パラメータを指定して実行し、クラスタまたはSVM用の自己署名ルートCA証明書を作成します。
   c. `security certificate show`コマンドに`-instance`パラメータおよび`-type` **`root-ca`**パラメータを指定して使用し、ルートCA証明書を表示します。

      CSRに署名するには、コマンド出力の次の情報が必要です。

      - 認証局（CA）
      - 証明書のシリアル番号

   d. `security certificate sign`コマンドを使用して、ルートCAでCSRに署名します。

e. プロンプトが表示されたら、CSRを入力してEnterキーを押します。

f. `-type` **`server`**パラメータを指定した`security certificate install`コマンドを使用して、自己CA署名デジタル証明書をインストールします。

g. プロンプトが表示されたら証明書と秘密鍵を入力し、Enterキーを押します。

h. サーバ証明書の証明書チェーンを形成するCAルート証明書と中間証明書をインストールするかどうかを尋ねられたら、「N」を入力します。

4. SSL設定を変更してサーバ認証用の証明書を指定する場合、`security ssl modify`コマンドに`-ca`パラメータおよび`-serial`パラメータを指定して使用します。

クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール例

次の例では、ある企業（カスタム共通名lab.companyname.com）で、「vs1」SVMに対して自己署名サーバ証明書が作成されます。この証明書は、「vs1」SVMをSSLサーバとして認証するためのものです。

```
cluster1::> security certificate create -vserver vs1 -common-name
lab.companyname.com -type server
```

次のコマンドでは、米国カリフォルニア州のサニーベールに所在する企業（カスタム共通名server1.companyname.com）のIT部門のソフトウェア グループが使用する、2,048ビット秘密鍵が設定されたCSRを作成します。SVMを管理する担当者のEメール アドレスは、web@companyname.comです。CSRと秘密鍵が出力に表示されます。

```
cluster1::> security certificate generate-csr -common-name
server1.companyname.com
-size 2048 -country US -state CA -locality Sunnyvale
-organization IT -unit Software -email-addr web@companyname.com

Certificate Signing Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQMwaTEQMA4GA1UEAxMHcnRwLmNvbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5DMQwwCgYDVQQHEwNSVFAxDTALBgNVBAoTBGNvcmUxDTALBgNVBAsT
BGNvcmUxDzANBgkqhkiG9w0BCQEWADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
...
-----END CERTIFICATE REQUEST-----


Private Key:
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
...
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your private key and certificate request for
future reference.
```

次のコマンドは、「vs1」SVMのCA署名サーバ証明書をインストールします。この証明書は、「vs1」SVMをSSLサーバとして認証するためのものです。

```
cluster1::> security certificate install -vserver vs1 -type server

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
...
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
...
-----END RSA PRIVATE KEY-----


Please enter certificates of Certification Authorities (CA) which form the
certificate chain of the server certificate. This starts with the issuing
CA certificate of the server certificate and can range up to the root CA
certificate.

Do you want to continue entering root and/or intermediate certificates {y|
n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
...
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate certificates {y|
n}: n

Note: You should keep a copy of your certificate and private key for future
reference.
If you revert to an earlier release, the certificate and private key are
deleted.
```

関連タスク

クラスタまたはSVMのSSLクライアントを認証するためのクライアントCAまたはルートCA証明書のインストール（144ページ）

クラスタまたはSVMのSSLクライアントを認証するためのクライアントCAまたはルートCA証明書のインストール

クラスタまたはStorage Virtual Machine（SVM）がアクセスを求めるクライアントを認証できるようにするには、クライアントの証明書署名要求（CSR）に署名したCAのルート証明書用に、**client-ca**タイプのデジタル証明書をクラスタまたはSVMにインストールします。**root-ca**タイプのルートCA証明書をクラスタまたはSVM上に作成し、クライアントのCSRに自己署名することもできます。

開始する前に

SSLクライアントの認証を有効にする場合、SSLサーバ認証も有効にする必要があります（デフォルト）。`security ssl show`コマンドを実行すると、設定が表示されます。

手順

1. クラスタまたはSVMがCAとしてクライアント証明書に署名し、クラスタまたはSVMの自己署名ルートCA証明書がまだない場合、`security certificate create`コマンドに`-type` **root-ca**パラメータを指定して実行し、自己署名ルートCA証明書を作成します。

   例

   次のコマンドを実行すると、「vs1」SVM（カスタム共通名lab.companyname.com）のルートCA証明書が作成されます。

   ```
   cluster1::> security certificate create -vserver vs1 -common-name
   lab.companyname.com -type root-ca
   ```

2. `-client-enabled`パラメータを**true**に設定して`security ssl modify`コマンドを実行し、クラスタまたはSVMでSSLクライアント認証を有効にします。

3. `security certificate generate-csr`コマンドを使用し、認証するクライアントのCSRを生成します。

   例

   次のコマンドでは、クライアント（カスタム共通名vs1admin）のCSRが生成されます。

```
cluster1::> security certificate generate-csr -common-name vs1admin

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwXTERMA8GA1UEAxMIdnMxYWRtaW4xCzAJBgNVBAYTAlVTMQkw
BwYDVQQIEwAxCTAHBgNVBAcTADEJMAcGA1UEChMAMQkwBwYDVQQLEwAxDzANBgkq
hkiG9w0BCQEWADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL6ohdT5
...
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvqiF1PmYy1Vtmkf6I8+mRXOy/m+3m/O1sEjUILbopzTlTu92
igqEzDY4W6q7KoRkcSa2x/Zn6IRlqxKrQbvUAJvAUDhcV7bn9NAzv9JE1j/6+0RY
IVR6Hr6QnCRSsjlLDxBnV3uZu8WNghpbIL98QP4oxwFu7G0HQsOleO3HMazOFyvW
...
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key
for future reference.
```

   証明書要求と秘密鍵が表示され、今後の参照用に出力をファイルにコピーするように求められます。

4. CSRに自己署名する場合は、次の手順を実行します。

   a. `security certificate show`コマンドに`-instance`パラメータおよび`-type` **root-ca**パラメータを指定して使用し、手順*1*で作成したルートCA証明書を表示します。

      CSRに署名するには、コマンド出力の次の情報が必要です。

      - 認証局（CA）
      - 証明書のシリアル番号

      例

```
cluster1::> security certificate show -instance -vserver vs1 -type
root-ca

                              Vserver: vs1
          FQDN or Custom Common Name: lab.companyname.com
        Serial Number of Certificate: 50F84392
               Certificate Authority: lab.companyname.com
                 Type of Certificate: root-ca
 Size of Requested Certificate(bits): 2048
              Certificate Start Date: Wed Jun 25 13:29:16 2014
         Certificate Expiration Date: Thu Jun 25 13:29:16 2015
              Public Key Certificate: -----BEGIN CERTIFICATE-----
                                      MIID
+zCCAuOgAwIBAgIEUPhDkjANBgkqhkiG9w0BAQsFADBbMQ8wDQYDVQQDEwZt
                                        .
                                        .
                                        .
```

b. `security certificate sign`コマンドを使用して、ルートCAでCSRに署名します。

署名済み証明書のデフォルトの形式（`-format`）はPEMです。形式をPKCS12に指定した場合は、`-destination`パラメータを使用して、署名済み証明書のアップロード先を指定することもできます。

c. プロンプトが表示されたら、CSRを入力してEnterキーを押します。

例

```
cluster1::> security certificate sign -vserver vs1 -ca
lab.companyname.com -ca-serial 50F84392

Please enter Certificate Signing Request (CSR): Press <enter> when
done

-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDEcMBoGA1UEAxMTQ1NSLlNpZ25pbmdUZXN0LmNvbTELMAkG
A1UEBhMCVVMxCTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNV
BAsTADEPMA0GCSqGSIb3DQEJARYAMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
...
-----END CERTIFICATE REQUEST-----


Signed Certificate: :
-----BEGIN CERTIFICATE-----
MIIDmzCCAoOgAwIBAgIEU9e2rzANBgkqhkiG9w0BAQsFADBoMRwwGgYDVQQDExNO
ZXcuQ29tcGFueU5hbWUuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYD
VQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcN
...
-----END CERTIFICATE-----
```

署名済み証明書が表示されます。証明書のコピーは保管しておいてください。

5. サードパーティのCAがCSRに署名する場合は、次の手順を実行します。

a. CSR出力から証明書要求（手順*3*）をコピーし、デジタル形式（Eメールなど）で信頼できるCAに送信して署名を求めます。

要求が処理されると、署名済みのデジタル証明書がCAから返信されます。秘密鍵とCA署名デジタル証明書のコピーは今後の参照用として保管しておいてください。

b. クラスタまたはSVMで、`security certificate install`コマンドに`-type client-ca`パラメータを指定して使用して、ルート証明書および証明書に署名したCAの各中間証明書をインストールします。

例

```
cluster1::> security certificate install -vserver vs1 -type client-
ca


Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDNjCCAp+gAwIBAgIQNhIilsXjOKUgodJfTNcJVDANBgkqhkiG9w0BAQUFADCB
zjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBUb3duMR0wGwYDVQQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCYGA1UE
...
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.
```

6. 自己署名証明書またはCA署名証明書をユーザに渡して、クライアントにインストールするよう依頼します。
7. 認証するクライアントごとに、手順*3*～*6*を繰り返します。
8. デジタル証明書で認証するユーザが設定されていない場合は、`security login create`コマンドと、**`cert`**に設定した`-authmethod`パラメータを使用して、ユーザを個別に追加します。

   クラスタ ユーザ アカウントの場合、デジタル証明書による認証は、**`http`**および**`ontapi`**アクセス方式（`-application`）でのみサポートされています。SVMユーザ アカウントの場合、デジタル証明書による認証は、**`ontapi`**アクセス方式でのみサポートされています。

   `security login show`コマンドを使用して、ユーザのログイン方法を表示できます。

関連タスク

クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール（141ページ）

クラスタまたはSVMがクライアントであるSSLサーバを認証するためのサーバCA証明書のインストール

クラスタまたはStorage Virtual Machine（SVM）が、別のSSLサーバ（たとえばLDAP over SSLをサポートするActive Directoryドメイン コントローラ）のクライアントであることがあります。この場合、サーバのルート証明書を**`server-ca`**タイプでクラスタまたはSVMにインストールして、クラスタまたはSVMがSSLサーバを認証できるようにします。

開始する前に

SSLサーバのルート証明書が必要です。サーバが自己署名したルート証明書、またはサーバ用にサードパーティCAが署名したルート証明書を使用できます。

手順

1. `security certificate install`コマンドに`-type` **`server-ca`**パラメータを指定して実行し、SSLサーバから提供されたルート証明書をインストールします。
2. プロンプトが表示されたら、証明書を入力してEnterキーを押します。

   今後の参照用として証明書のコピーを保管するように求められます。

SSLサーバのサーバCA証明書のインストール例

次の例では、SSLサーバのCA証明書が**`server-ca`**タイプでインストールされます。この証明書はサーバの認証用に使用され、クライアントである「vs1」SVMにインストールされます。

```
cluster1::> security certificate install -vserver vs1 -type server-
ca

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIDNjCCAp+gAwIBAgIQNhIilsXjOKUgodJfTNcJVDANBgkqhkiG9w0BAQUFADCB
zjELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJ
Q2FwZSBUb3duMR0wGwYDVQQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCYGA1UE
...
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.
```

関連タスク

クラスタまたはSVMをSSLクライアントとして認証するためのクライアント証明書のインストール（148ページ）

クラスタまたはSVMをSSLクライアントとして認証するためのクライアント証明書のインストール

SSLサーバでクラスタまたはStorage Virtual Machine（SVM）をSSLクライアントとして認証するためには、**client**タイプのデジタル証明書をクラスタまたはSVMにインストールします。次に、**client-ca**証明書をそのSSLサーバの管理者に渡してインストールしてもらいます。

開始する前に

SSLサーバのルート証明書を、クラスタまたはSVM上に**server-ca**証明書タイプでインストールしておく必要があります。

手順

1. クライアント認証に自己署名デジタル証明書を使用する場合は、`security certificate create`コマンドに`-type` **client**パラメータを指定して使用します。
2. クライアント認証にCA署名デジタル証明書を使用する場合は、次の手順を実行します。
   a. `security certificate generate-csr`コマンドを使用して、証明書署名要求（CSR）を生成します。

      証明書要求と秘密鍵を含むCSR出力が表示され、今後の参照用にファイルにコピーするよう求められます。

   b. CSR出力の証明書要求をデジタル形式（Eメールなど）で信頼できるCAに送信し、署名を求めます。

      要求が処理されると、署名済みのデジタル証明書がCAから返信されます。秘密鍵とCA署名証明書のコピーは今後の参照用として保管しておいてください。

   c. `security certificate install`コマンドに`-type` **client**パラメータを指定して使用し、CA署名証明書をインストールします。
   d. プロンプトが表示されたら証明書と秘密鍵を入力し、Enterキーを押します。
   e. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、Enterキーを押します。

      信頼できるルートCAから発行されたSSL証明書に至る証明書チェーンに中間証明書がない場合は、クラスタまたはSVMに中間証明書をインストールします。中間証明書は、エンドエンティティのサーバ証明書を発行する目的で信頼できるルートから発行される、副次的な証明書です。この結果、信頼できるルートCAから始まり、中間証明書を経て、発行されたSSL証明書で終わる証明書チェーンが形成されます。

3. クラスタまたはSVMの**client-ca**証明書をSSLサーバの管理者に渡してインストールしてもらいます。

   `security certificate show`コマンドに`-instance`パラメータおよび`-type` **client-ca**パラメータを指定して実行すると、**client-ca**証明書の情報が表示されます。

クラスタまたはSVMをSSLクライアントとして認証するためのクライアント証明書のインストール例

次の例では、ある企業（カスタム共通名lab.companyname.com）で、「vs1」SVMに対して自己署名クライアント証明書が作成されます。この証明書は、「vs1」SVMをSSLクライアントとして認証するためのものです。

```
cluster1::> security certificate create -vserver vs1 -common-name
lab.companyname.com -type client
```

次のコマンドでは、米国カリフォルニア州のサニーベールに所在する企業（カスタム共通名lab.companyname.com）のIT部門のソフトウェア グループが使用する、2,048ビット秘密鍵が設定されたCSRを作成します。SVMを管理する担当者のEメール アドレスは、web@companyname.comです。CSRと秘密鍵がコンソールに表示されます。

```
cluster1::> security certificate generate-csr -common-name
lab.companyname.com
-size 2048 -country US -state CA -locality Sunnyvale -organization IT
-unit Software -email-addr web@companyname.com

Certificate Signing Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQMwaTEQMA4GA1UEAxMHcnRwLmNvbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5DMQwwCgYDVQQHEwNSVFAxDTALBgNVBAoTBGNvcmUxDTALBgNVBAsT
BGNvcmUxDzANBgkqhkiG9w0BCQEWADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
...
-----END CERTIFICATE REQUEST-----


Private Key:
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
...
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your private key and certificate request for
future reference.
```

次のコマンドは、「vs1」SVMのCA署名クライアント証明書をインストールします。この証明書は、「vs1」SVMをSSLクライアントとして認証するためのものです。

```
cluster1::> security certificate install -vserver vs1 -type client

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
...
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
...
-----END RSA PRIVATE KEY-----


Please enter certificates of Certification Authorities (CA) which form the
certificate chain of the client certificate. This starts with the issuing
CA certificate of the client certificate and can range up to the root CA
certificate.

Do you want to continue entering root and/or intermediate certificates {y|
n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
...
-----END CERTIFICATE-----
```

```
Do you want to continue entering root and/or intermediate certificates {y|
n}: n

Note: You should keep a copy of your certificate and private key for future
reference.
If you revert to an earlier release, the certificate and private key are
deleted.
```

関連タスク

クラスタまたはSVMがクライアントであるSSLサーバを認証するためのサーバCA証明書のインストール（147ページ）

クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール

クラスタと外部キー管理ツール（Key Management Interoperability Protocol [KMIP]サーバなど）が相互認証することで、キー管理ツールがKMIPを使用してSSL経由でクラスタと通信できるようになります。この設定は、特定のアプリケーションや機能（Data ONTAP-vプラットフォームやストレージ暗号化機能など）で、データ アクセスの安全性を確保するためにセキュアなキーが必要とされる場合に使用します。

開始する前に

外部キー管理ツールからルート証明書を入手しておく必要があります。これはキー管理ツールをSSLサーバとして認証する証明書です。サーバが自己署名したルート証明書、またはサーバ用にサードパーティのCAが署名したルート証明書を使用できます。

タスク概要

最大4つのKMIPサーバと相互認証を行うようにクラスタを設定することができます。

手順

1. クラスタを外部KMIPサーバに対してSSLクライアントとして認証するKMIP証明書をインストールします。

   a. クラスタのKMIP認証に使用する署名付き証明書がない場合は、`security certificate generate-csr`コマンドを使用してデジタル証明書署名要求（CSR）を生成します。

      証明書要求と秘密鍵を含むCSR出力が表示され、今後の参照用にファイルにコピーするよう求められます。

   b. CSRをサードパーティのCAに送信して署名を求めるか、`security certificate sign`コマンドを使用してクラスタのルートCA証明書でCSRに署名します。

      クラスタのルートCA証明書を表示するには、`security certificate show`コマンドで`-instance`パラメータと`-type root-ca`パラメータを指定します。

      秘密鍵と署名付きデジタル証明書のコピーは今後の参照用として保管しておいてください。

   c. `security certificate install`コマンドで`-type client`パラメータと`-subtype kmip-cert`パラメータを指定して、クラスタの認証に使用する署名付きKMIP証明書をインストールします。

   d. プロンプトが表示されたら証明書と秘密鍵を入力し、Enterキーを押します。

   e. プロンプトが表示されたら追加のルート証明書または中間証明書を入力し、Enterキーを押します。

例

```
cluster1::> security certificate install -type client -subtype kmip-cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIFyjCCBLKgAwIBAgIQe1t1/RNlMt1xn+/KLgtvOzANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
...
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA1X+NLxxxtOJUM3dhpHOn3Z+76wGGax0jYOGzC5AQhigB8buL
Y2bfrs4Jtv6FeFVzfnpoWV9bZzgHiqzyRJkxv960YEVHPI3i5x+HDPDg3qRhWWRS
Zqfia35wJ8rxMydzydO7tvMtZyzVS8EpCl3rEMC+gMG+uVr0e4KJvamOoyAQ7c6z
...
-----END RSA PRIVATE KEY-----


Please enter certificates of Certification Authorities (CA) which form the
certificate chain of the client certificate. This starts with the issuing
CA certificate of the client certificate and can range up to the root CA
certificate.

Do you want to continue entering root and/or intermediate certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

cluster1::>
```

2. KMIPサーバをクラスタに対してSSLサーバとして認証するKMIP証明書をインストールします。

   a. `security certificate install`コマンドで`-type server-ca`、`-subtype kmip-cert`、および`-kmip-server-ip` *`ip_address`*の各パラメータを指定して、KMIPサーバのKMIP証明書をインストールします。

      同じサブネットに属する複数のKMIPサーバを認証する場合は、`-kmip-server-ip`パラメータを使用してサブネットのアドレスを指定します。

      たとえば、`-kmip-server-ip 10.53.27.55`と指定すると、IPアドレスが**`10.53.27.55`**のKMIPサーバが認証され、`-kmip-server-ip 10.53.0.0`と指定すると、サブネット**`10.53.0.0`**に属するすべてのKMIPサーバが認証されます。

   b. プロンプトが表示されたら、証明書を入力してEnterキーを押します。

      今後の参照用として証明書のコピーを保管するように求められます。

例

```
cluster1::> security certificate install -type server-ca -subtype kmip-cert
-kmip-server-ip 10.53.0.0 -vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

3. `security certificate show`コマンドで`-subtype kmip-cert`パラメータを指定して、クラスタにインストールされたKMIP証明書を表示します。

例

```
cluster1::> security certificate show -subtype kmip-cert

Vserver    Serial Number   Common Name                Type
---------- --------------- -------------------------- ---------
cluster1
            7B5B75FD136532  cert.servername.com        server-ca
    Certificate Authority: Secure Server CA
          Expiration Date: Mon Oct 23 16:59:59 2017

cluster1
            050E37C2DB56E5  www.example.com            client
    Certificate Authority: www.example.com
          Expiration Date: Mon Apr 30 14:14:46 2018

2 entries were displayed.

cluster1::>
```

関連タスク

クラスタまたはSVMのSSLクライアントを認証するためのクライアントCAまたはルートCA証明書のインストール（144ページ）

期限切れのデジタル証明書の交換

作成またはインストールする証明書には、それぞれ有効期限があります。期限が切れた証明書は新しい証明書に交換し、対応するサーバまたはクライアント認証が中断しないようにする必要があります。

タスク概要

デフォルトでは、Data ONTAPで生成されるデジタル証明書の有効期限は365日間に設定されますが、デジタル証明書の作成時に、有効期限の設定（最長10年）を指定できます。

手順

1. `security certificate show`コマンドに`-fields expiration, expire-days`パラメータを指定して実行し、証明書の有効期限情報を表示します。

   期限切れの証明書を削除する際には、次の情報が必要です。

   - SVM名
   - その証明書に使用している共通名
   - シリアル番号
   - 認証局（CA）
   - 証明書のタイプまたはサブタイプ

2. `security certificate delete`コマンドを使用し、期限切れになった証明書を削除します。
3. 新しい証明書を同じ共通名で取得し、期限切れの証明書と交換します。

証明書のタイプ	実行する手順
serverタイプ	*クラスタまたはSVMをSSLサーバとして認証するサーバ証明書をインストールする*（141ページ）

証明書のタイプ	実行する手順
client-caタイプ	*クラスタまたはSVMのSSLクライアントを認証するためのクライアントCA証明書またはルートCA証明書のインストール*（144ページ）
server-caタイプ	*クラスタまたはSVMがクライアントであるSSLサーバを認証するためのサーバCA証明書のインストール*（147ページ）
clientタイプ	*クラスタまたはSVMをSSLクライアントとして認証するためのクライアント証明書のインストール*（148ページ）
kmip-certサブタイプ	*クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール*（150ページ）

デジタル証明書の管理用コマンド

クラスタまたはStorage Virtual Machine（SVM）のデジタル証明書を管理するには、`security certificate`コマンドを使用します。

状況	使用するコマンド
次のいずれかのタイプの自己署名デジタル証明書を作成およびインストールする • **server** • **root-ca** • **client**	*`security certificate create`*
署名のためにCAに送信するデジタル証明書署名要求を生成する	*`security certificate generate-csr`*
自己署名したルートのCAを使用してデジタル証明書に署名する	*`security certificate sign`*
次のいずれかのタイプのCA署名デジタル証明書およびルートCAの公開鍵証明書をインストールする、またはサブタイプが**kmip-cert**の**client**または**server-ca**の証明書をクラスタにインストールする • **server** • **client-ca** • **server-ca** • **client**	*`security certificate install`*
インストールされたデジタル証明書に関する情報を表示する	*`security certificate show`*
クラスタまたはSVMによってCAとして署名されたデジタル証明書を表示する	*`security certificate ca-issued show`*
クラスタまたはSVMによってCAとして署名された、侵害されたデジタル証明書を取り消す	*`security certificate ca-issued revoke`*
インストールされたデジタル証明書を削除する	*`security certificate delete`*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

Webサービスへのアクセスの管理

Webサービスは、HTTPまたはHTTPSを使用してユーザがアクセスできるアプリケーションです。クラスタ管理者はWebプロトコル エンジンをセットアップし、SSLを設定し、Webサービスを有効にし、ロールのユーザがWebサービスにアクセスできるようにします。

Data ONTAPは次のWebサービスをサポートします。

- Service Processor Infrastructure（**spi**）
  このサービスによって、ノードのログ ファイル、コア ダンプ ファイル、およびMIBファイルに、クラスタ管理LIFまたはノード管理LIFからHTTPまたはHTTPSでアクセスできるようになります。デフォルト設定は**enabled**です。
  ノードのログ ファイルまたはコア ダンプ ファイルへのアクセス要求を受け取ると、**spi** Webサービスは、あるノードからファイルが存在する別のノードのルート ボリュームへのマウント ポイントを自動的に作成します。マウント ポイントを手動で作成する必要はありません。

- Data ONTAP Classic（**compat**）
  このサービスは、**spi** Webサービスへの代替インターフェイスを提供します。デフォルト設定は**enabled**です。
  spi Webサービスと**compat** Webサービスの両方が有効になっている場合、ノードのログ ファイルとコア ダンプ ファイルにノードの管理LIFからHTTPまたはHTTPSでアクセスできます。

- Data ONTAP API（**ontapi**）
  このサービスでは、Data ONTAP APIを実行し、リモート プログラムで管理機能を実行できます。デフォルト設定は**enabled**です。
  一部の外部管理ツールにはこのサービスが必要です。たとえば、OnCommand System Managerを使用する場合、このサービスを有効にしておく必要があります。

- Data ONTAP Discovery（**disco**）
  このサービスは、外部の管理アプリケーションが、ネットワーク上のクラスタを検出できるようにします。デフォルト設定は**enabled**です。

- Support Diagnostics（**supdiag**）
  このサービスは、問題の分析および解決を支援するために、システム上の権限が設定された環境へのアクセスを制御します。デフォルト設定は**disabled**です。このサービスは、テクニカル サポートから指示があった場合にのみ有効にしてください。

- System Manager（**sysmgr**）
  このサービスは、Data ONTAPに組み込まれているOnCommand System Managerの可用性を管理します。デフォルト設定は**enabled**です。このサービスはクラスタでのみサポートされます。

関連コンセプト

OnCommand System Managerの概要（29ページ）

関連タスク

OnCommand System Managerのブラウザベースのグラフィカル インターフェイスを使用したクラスタへのアクセス（28ページ）
Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、およびMIBファイルへのアクセス（42ページ）

Webプロトコル エンジンの管理

クラスタ上でWebプロトコル エンジンを設定し、Webアクセスを許可するかどうか、およびどのSSLのバージョンが使用可能かを制御できます。また、Webプロトコル エンジンの構成設定を表示することもできます。

Webプロトコル エンジンは、次の方法でクラスタ レベルで管理できます。

- リモート クライアントがHTTPまたはHTTPSを使用してWebサービス コンテンツにアクセスできるかどうかを指定できます（`system services web modify`コマンドに`-external`パラメータを指定）。
- セキュアなWebアクセスに対してSSLv3を使用するかどうかを指定できます（`system services web modify`コマンドに`-sslv3-enabled`パラメータを指定）。

  デフォルトでは、SSLv3が有効です。Transport Layer Security 1.0（TLSv1.0）は有効になっており、無効にすることはできません。
- セキュアなWebサービス（HTTPS）に対してFederal Information Processing Standard（FIPS;連邦情報処理標準）140-2への準拠を有効にできます（`system services web modify`コマンドに`-ssl-fips-enabled`パラメータを指定）。また、FIPS 140-2準拠が有効でオンラインになっているかどうかを表示できます（`system services web show`）。

  デフォルトでは、FIPS 140-2への準拠は無効になっています。FIPS 140-2への準拠が有効な場合、SSLv3は無効になり、TLSv1のみが有効なままになります。Data ONTAPでは、FIPS 140-2への準拠が有効な場合、SSLv3を有効にすることはできません。

  FIPS 140-2を有効にし、その後無効にした場合、SSLv3は無効なままになりますが、TLSv1は常に有効です。
- Webプロトコルの設定を表示できます（`system services web show`）。

ファイアウォールが有効になっている場合は、Webサービスに使用する論理インターフェイス（LIF）のファイアウォール ポリシーを設定して、HTTPまたはHTTPSアクセスを許可する必要があります。

Webサービス アクセスにHTTPSを使用する場合は、Webサービスを提供するクラスタまたはStorage Virtual Machine（SVM）のSSLを有効にし、そのクラスタまたはSVMのデジタル証明書を提供する必要もあります。

MetroCluster構成では、クラスタ上のWebプロトコル エンジンの設定に対する変更内容は、パートナー クラスタにはレプリケートされません。

関連コンセプト

SSLの管理（158ページ）
Webサービスの管理（156ページ）

関連タスク

Webサービスへのアクセスの設定（159ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

Webプロトコル エンジンの管理用コマンド

Webプロトコル エンジンを管理するには、`system services web`コマンドを使用します。Webアクセス要求がファイアウォールを通過できるようにするには、`system services firewall policy create`および`network interface modify`コマンドを使用します。

状況	使用するコマンド
クラスタ レベルでWebプロトコル エンジンを次のように設定する • クラスタのWebプロトコル エンジンを有効または無効にする • クラスタのSSLv3を有効または無効にする • セキュアなWebサービス（HTTPS）に対するFIPS 140-2準拠を有効または無効にする	*`system services web modify`*
クラスタ レベルのWebプロトコル エンジンの設定を表示し、Webプロトコルがクラスタ全体で機能しているかどうかを判断し、FIPS 140-2準拠が有効でオンラインになっているかどうかを表示する	*`system services web show`*
ノード レベルのWebプロトコル エンジンの設定と、クラスタ内のノードに対するWebサービス処理のアクティビティを表示する	*`system services web node show`*
ファイアウォール ポリシーを作成するか、既存のファイアウォール ポリシーにHTTPまたはHTTPSプロトコル サービスを追加して、Webアクセス要求がファイアウォールを通過できるようにする	*`system services firewall policy create`* `-service`パラメータを**`http`**または**`https`**に設定すると、Webアクセス要求がファイアウォールを通過できるようになります。
ファイアウォール ポリシーをLIFと関連付ける	*`network interface modify`* `-firewall-policy`パラメータを使用すると、LIFのファイアウォール ポリシーを変更できます。

関連参照情報

SSLの管理用コマンド（159ページ）
デジタル証明書の管理用コマンド（153ページ）

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

Webサービスの管理

クラスタまたはStorage Virtual Machine（SVM）のWebサービスを有効または無効にしたり、Webサービスの設定を表示したり、あるロールのユーザがWebサービスにアクセスできるかどうかを管理したりできます。

クラスタまたはSVMのWebサービスは次の方法で管理できます。

- 特定のWebサービスを有効化または無効化する
- Webサービスへのアクセスを暗号化されたHTTP（SSL）のみに限定するかどうかを指定する

- Webサービスの可用性を表示する
- あるロールのユーザにWebサービスへのアクセスを許可または禁止する
- Webサービスへのアクセスが許可されているロールを表示する

Webサービスへアクセスするユーザは、次の条件のすべてを満たしている必要があります。

- 認証されたユーザであること。
  たとえば、Webサービスはユーザ名およびパスワードの入力を求めることがあります。ユーザの応答は有効なアカウントと一致する必要があります。
- ユーザが正しいアクセス方法で設定されていること。
  指定されたWebサービスの正しいアクセス方法が設定されたユーザのみが正常に認証されます。Data ONTAP API Webサービス（**ontapi**）の場合は、ユーザのアクセス方法が**ontapi**である必要があります。その他のすべてのWebサービスについては、ユーザのアクセス方法は**http**である必要があります。

  注: ユーザのアクセス方法および認証方法を管理するには、`security login`コマンドを使用します。

- Webサービスは、ユーザのアクセス制御ロールを許可するように設定する必要があります。

  注: ロールのWebサービスへのアクセスを制御するには、`vserver services web access`コマンドを使用します。

ファイアウォールが有効になっている場合は、Webサービスに使用するLIFのファイアウォール ポリシーを設定して、HTTPまたはHTTPSを許可する必要があります。

Webサービス アクセスにHTTPSを使用する場合は、Webサービスを提供するクラスタまたはSVMのSSLを有効にし、そのクラスタまたはSVMのデジタル証明書を提供する必要もあります。

関連コンセプト

Webプロトコル エンジンの管理（155ページ）
ユーザ アカウントの管理（119ページ）
ユーザ アカウントへのアクセス方法（120ページ）
SSLの管理（158ページ）

関連タスク

Webサービスへのアクセスの設定（159ページ）

Webサービスの管理用コマンド

クラスタまたはStorage Virtual Machine（SVM）でのWebサービスを使用を管理するには、`vserver services web`コマンドを使用します。ロールのWebサービスへのアクセスを制御するには、`vserver services web access`コマンドを使用します。

状況	使用するコマンド
クラスタまたはSVMのWebサービスを次のように設定する • Webサービスを有効または無効にする • Webサービスへのアクセスに HTTPSだけを許可するかどうかを指定する	*`vserver services web modify`*
クラスタまたはSVMのWebサービスの設定と可用性を表示する	*`vserver services web show`*

状況	使用するコマンド
特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを許可する	`vserver services web access create`
クラスタまたはSVMのWebサービスへのアクセスが許可されているロールを表示する	`vserver services web access show`
特定のロールに対して、SVMのWebサービスへのアクセスを禁止する	`vserver services web access delete`

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

ノード上のマウント ポイントの管理用コマンド

spi Webサービスでは、ノードのログ ファイルまたはコア ファイルに対するアクセス要求があると、1つのノードから別のノードのルート ボリュームに対してマウント ポイントが自動的に作成されます。マウント ポイントを手動で管理する必要はありませんが、`system node root-mount`コマンドを使用すれば手動でも管理できます。

状況	使用するコマンド
1つのノードから別のノードのルート ボリュームに対するマウント ポイントを手動で作成する	`system node root-mount create` 1つのノードから別のノードに対して作成できるマウント ポイントは1つだけです。
クラスタ内のノードにある既存のマウント ポイントを、マウント ポイントが作成された時刻と現在の状態を含めて表示する	`system node root-mount show`
1つのノードから別のノードのルート ボリュームに対するマウント ポイントを削除し、そのマウント ポイントに対する接続を強制的に終了する	`system node root-mount delete`

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

SSLの管理

SSLプロトコルは、デジタル証明書を使用してWebサーバとブラウザの間に暗号化された接続を確立することでWebアクセスのセキュリティを向上させます。

クラスタまたはStorage Virtual Machine（SVM）のSSLは次の方法で管理できます。

- SSLを有効化する
- デジタル証明書を生成してインストールし、クラスタまたはSVMと関連付ける
- SSL設定を表示してSSLが有効かどうかを確認し、可能な場合はSSL証明書名を表示する
- クラスタまたはSVMのファイアウォール ポリシーを設定し、Webアクセス要求が通過できるようにする
- 使用できるSSLのバージョンを定義する
- WebサービスのHTTPS要求のみにアクセスを制限する

関連コンセプト

Webプロトコル エンジンの管理（155ページ）
Webサービスの管理（156ページ）
サーバまたはクライアント認証用のデジタル証明書の管理（140ページ）

関連タスク

Webサービスへのアクセスの設定（159ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

SSLの管理用コマンド

クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理するには、`security ssl`コマンドを使用します。

状況	使用するコマンド
クラスタまたはSVMのSSLを有効にし、デジタル証明書と関連付ける	`security ssl modify`
クラスタまたはSVMのSSL設定と証明書名を表示する	`security ssl show`

関連参照情報

Webサービスの管理用コマンド（157ページ）
Webプロトコル エンジンの管理用コマンド（156ページ）
デジタル証明書の管理用コマンド（153ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド
Clustered Data ONTAP 8.3 Commands: Manual Page Reference

Webサービスへのアクセスの設定

Webサービスへのアクセスを設定することで、許可されたユーザが、HTTPまたはHTTPSを使用してクラスタまたはStorage Virtual Machine（SVM）のサービス コンテンツにアクセスできるようになります。

手順

1. ファイアウォールが有効になっている場合は、Webサービスで使用されるLIFのファイアウォール ポリシーでHTTPまたはHTTPSのアクセスがセットアップされていることを確認してください。

   注: ファイアウォールが有効になっているかどうかを確認するには、`system services firewall show`コマンドを使用します。

   a. ファイアウォール ポリシーでHTTPまたはHTTPSがセットアップされていることを確認するには、`system services firewall policy show`コマンドを使用します。

      ポリシーでWebアクセスをサポートするには、`system services firewall policy create`コマンドの`-service`パラメータを**`http`**または**`https`**に設定します。

b. HTTPまたはHTTPSをサポートしているファイアウォール ポリシーが、Webサービスを提供するLIFと関連付けられていることを確認するには、`-firewall-policy`パラメータを指定して`network interface show`コマンドを使用します。

   LIFに対してファイアウォール ポリシーを有効にするには、`-firewall-policy`パラメータを指定して`network interface modify`コマンドを使用します。

2. クラスタレベルのWebプロトコル エンジンを設定してWebサービスのコンテンツにアクセスできるようにするには、`system services web modify`コマンドを使用します。

3. セキュアなWebサービス（HTTPS）を使用する場合は、SSLを有効にし、`security ssl modify`コマンドを使用して、クラスタまたはSVMのデジタル証明書情報を入力します。

4. クラスタまたはSVMでWebサービスを有効にするには、`vserver services web modify`コマンドを使用します。

   この手順は、クラスタまたはSVMに対して有効にする各サービスについて繰り返す必要があります。

5. 特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを許可するには、`vserver services web access create`コマンドを使用します。

   アクセスを許可するロールはすでに存在している必要があります。既存のロールを表示するには`security login role show`コマンドを使用します。新しいロールを作成するには`security login role create`コマンドを使用します。

6. Webサービスへのアクセスが許可されているロールについては、`security login show`コマンドの出力で、ユーザにも正しいアクセス方法が設定されていることを確認してください。

   Data ONTAP API Webサービス（**`ontapi`**）にアクセスするには、ユーザのアクセス方法が**`ontapi`**に設定されている必要があります。その他すべてのWebサービスにアクセスするには、ユーザのアクセス方法が**`http`**に設定されている必要があります。

   注: ユーザのアクセス方法を追加するには、`security login create`コマンドを使用します。

関連コンセプト

SSLの管理（158ページ）
サーバまたはクライアント認証用のデジタル証明書の管理（140ページ）
Webプロトコル エンジンの管理（155ページ）
Webサービスの管理（156ページ）
アクセス制御ロールの管理（126ページ）
ユーザ アカウントへのアクセス方法（120ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

Webサービスへのアクセスに関する問題のトラブルシューティング

設定エラーは、Webサービスへのアクセスに関する問題が発生する原因になります。このエラーに対応するには、LIF、ファイアウォール ポリシー、Webプロトコル エンジン、Webサービス、デジタル証明書、およびユーザ アクセス許可がすべて正しく設定されていることを確認します。

次の表に、Webサービスの設定エラーを特定して対応する方法を示します。

アクセスに関する問題	原因となる設定エラー	エラーに対応する方法
Webサービスにアクセスを試みると、Webブラウザで`unable to connect`または`failure to establish a connection`エラーが返される	LIFが正しく設定されていない	Webサービスを配信するLIFにpingを送信できることを確認します。 **注:** LIFにpingを送信するには、`network ping`コマンドを使用します。ネットワーク設定の詳細については、*『clustered Data ONTAP ネットワーク管理ガイド』*を参照してください。
	ファイアウォールが正しく設定されていない	HTTPまたはHTTPSをサポートするようにファイアウォール ポリシーが設定されていて、ポリシーがWebサービスを配信するLIFに割り当てられていることを確認します。 **注:** ファイアウォール ポリシーを管理するには、`system services firewall policy`コマンドを使用します。ポリシーとLIFを関連付けるには、`network interface modify`コマンドと`-firewall-policy`パラメータを使用します。
	Webプロトコル エンジンが無効になっている可能性がある	Webプロトコル エンジンが有効になっていて、Webサービスがアクセス可能であることを確認します。 **注:** クラスタ用にWebプロトコル エンジンを管理するには、`system services web`コマンドを使用します。
Webサービスにアクセスを試みると、Webブラウザから`not found`エラーが返される	Webサービスが無効になっている可能性がある	アクセスを許可する個々のWebサービスが有効になっていることを確認します。 **注:** Webサービスへのアクセスを有効にするには、`vserver services web modify`コマンドを使用します。
Webブラウザで、特定のユーザのアカウント名とパスワードを使用してWebサービスにログインできない	ユーザが認証されない、アクセス方法が正しくない、またはユーザにそのWebサービスへのアクセスが許可されていない	ユーザ アカウントが存在し、正しいアクセス方法と認証方法が設定されていることを確認します。また、ユーザのロールにそのWebサービスへのアクセスが許可されていることを確認します。 **注:** ユーザ アカウントと、アクセス方法および認証方法を管理するには、`security login`コマンドを使用します。Data ONTAP API Webサービスにアクセスするには、**`ontapi`**アクセス方法が必要です。その他すべてのWebサービスにアクセスするには、**`http`**アクセス方法が必要です。Webサービスに対するロールのアクセスを管理するには、`vserver services web access`コマンドを使用します。

アクセスに関する問題	原因となる設定エラー	エラーに対応する方法
HTTPSを使用してWebサービスに接続すると、接続が遮断されたとWebブラウザに表示される	Webサービスを配信するクラスタまたはStorage Virtual Machine（SVM）でSSLが有効になっていない可能性がある	クラスタまたはSVMでSSLが有効になっていて、デジタル証明書が有効であることを確認します。 **注:** HTTPサーバのSSL設定を管理するには`security ssl`コマンドを使用し、デジタル証明書情報を表示するには`security certificate show`コマンドを使用します。
HTTPSを使用してWebサービスに接続すると、信頼されない接続であるとWebブラウザに表示される	自己署名デジタル証明書を使用している可能性がある	クラスタまたはSVMに関連付けられているデジタル証明書が、信頼されたCAによって署名されていることを確認します。 **注:** デジタル証明書署名要求を生成するには`security certificate generate-csr`コマンドを使用し、CA署名のデジタル証明書をインストールするには`security certificate install`コマンドを使用します。Webサービスを配信するクラスタまたはSVMのSSL設定を管理するには、`security ssl`コマンドを使用します。

関連コンセプト

Webプロトコル エンジンの管理（155ページ）
サーバまたはクライアント認証用のデジタル証明書の管理（140ページ）
Webサービスの管理（156ページ）
ユーザ アカウントの管理（119ページ）
アクセス制御ロールの管理（126ページ）
SSLの管理（158ページ）

関連タスク

クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール（141ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

管理アクティビティの監査設定の管理

監査ログを有効にすると、管理インターフェイスで実行された管理アクティビティのレコードが時間順に作成されます。コマンド履歴ログは指定した宛て先に転送できます。また、テクニカル サポート用の`mgwd.log`ファイルにどの要求を記録するかを制御することもできます。監査ログ ファイルは、Webブラウザを使用して表示できます。

Data ONTAPでは、クラスタで実行された管理アクティビティについて、発行された要求、要求を発行したユーザ、ユーザのアクセス方式、要求が発行された時間などの情報が記録されます。管理アクティビティには次のタイプがあります。

- set要求。通常は表示以外のコマンドや操作が該当します。

このタイプの要求は、たとえば、create、modify、deleteなどのコマンドを実行する際に発行されます。

- get要求。情報を取得して管理インターフェイスに表示する要求です。
  このタイプの要求は、たとえば、showコマンドを実行する際に発行されます。

管理アクティビティのログは、ノードの次のファイルに記録されます。

- /mroot/etc/log/mlog/command-history.logファイルには、set要求だけが記録されます。
  このファイルには、すべてのset要求が記録されますが、get要求は記録されません。この動作には、security audit modifyコマンドの設定は適用されません。
  このファイルは、AutoSupportによって指定の受信者に送信されます。また、最大10個の指定した宛て先（cluster log-forwarding createで指定）に内容を転送できます。たとえば、Splunkやsyslogサーバに転送し、監視や分析、バックアップなどの目的で使用できます。
- /mroot/etc/log/mlog/mgwd.logファイルには、デフォルトではset要求だけが記録されます。
  このファイルは、テクニカル サポートや診断に使用されます。デフォルトでは、すべてのset要求が記録され、get要求は記録されません。ただし、security audit modifyコマンドを使用して、このファイルに次の要求を記録するかどうかを制御できます。
  - Data ONTAP CLIから送信されたset要求（-cliset）
  - Data ONTAP APIから送信されたset要求（-ontapiset）
  - Data ONTAP CLIから送信されたget要求（-cliget）
  - Data ONTAP APIから送信されたget要求（-ontapiget）
- /mroot/etc/log/auditlogファイルには、ノードシェルのCLIコマンドが記録されます。
  このファイルには、ノードシェルで実行されたコマンドが記録されます。AutoSupportメッセージには、ノードとパートナー ノードのノードシェル監査ログ ファイルが含まれます。

command-history.logファイルとmgwd.logファイルは、1日単位でローテーションされます。また、サイズが100MBに達したときにもローテーションが実行されます。以前のファイルは34個まで保持されます（最大合計ファイル数はそれぞれ35ファイル）。

auditlogファイルは、週単位でローテーションされます。また、サイズが10MBに達したときにもローテーションが実行されます。auditlogファイルは最大で6個まで保持されます。

/mroot/etc/log/ディレクトリのコンテンツは、Webブラウザを使用して表示できます。

関連タスク

Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、およびMIBファイルへのアクセス（42ページ）

コマンド履歴ログの転送

最大10個の指定した宛て先にコマンド履歴ログ（/mroot/etc/log/mlog/command-history.logの内容）を転送できます。たとえば、Splunkやsyslogサーバにログを転送し、監視や分析、バックアップなどの目的で使用できます。

手順

1. cluster log-forwarding createコマンドを使用して、コマンド履歴ログを転送する各宛て先のIPアドレスまたはホスト名を指定します。

   このコマンドでは、指定した宛て先のレコードを作成する前に、宛て先のホストにpingを送信して接続が検証されます。pingに失敗した場合はエラーとなり、コマンドが失敗します。接続の

検証は-forceパラメータを使用して省略することもできますが、省略することは推奨されません。

cluster log-forwarding modifyコマンドを使用すると、以前に指定した宛て先を変更できます。

cluster log-forwarding deleteコマンドを使用すると、以前に指定した宛て先を削除できます。

例

```
cluster1::> cluster log-forwarding create -destination 192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination 192.168.123.98
-port 514 -facility user
```

2. cluster log-forwarding showコマンドを使用して、宛て先のレコードを表示します。

例

```
cluster1::> cluster log-forwarding show

                                    Syslog
Destination Host           Port    Facility
-------------------------- ------ --------
192.168.123.96             514     user
192.168.123.98             514     user
2 entries were displayed.

cluster1::>
```

関連タスク

Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、およびMIBファイルへのアクセス（42ページ）

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ：cluster log-forwarding create - Create a log forwarding destination

clustered Data ONTAP 8.3.1マニュアル ページ：cluster log-forwarding modify - Modify log forwarding destination settings

clustered Data ONTAP 8.3.1マニュアル ページ：cluster log-forwarding delete - Delete a log forwarding destination

clustered Data ONTAP 8.3.1マニュアル ページ：cluster log-forwarding show - Display log forwarding destinations

管理アクティビティの監査設定の管理用コマンド

どの管理アクティビティを`mgwd.log`ファイルに記録するかを管理するには、`security audit`コマンドを使用します。コマンド履歴ログを転送する宛て先の管理には、`cluster log-forwarding`コマンドを使用します。

状況	使用するコマンド
Data ONTAPのCLIまたはAPIから送信されたset要求またはget要求をテクニカル サポート用の`/mroot/etc/log/mlog/mgwd.log`ファイルに記録するかどうかを指定する	*`security audit modify`*
`/mroot/etc/log/mlog/mgwd.log`ファイルの設定を表示する	*`security audit show`*
コマンド履歴ログ（`/mroot/etc/log/mlog/command-history.log`）を転送する宛て先を指定する	*`cluster log-forwarding create`*
コマンド履歴ログの宛て先を変更する	*`cluster log-forwarding modify`*
コマンド履歴ログの宛て先を削除する	*`cluster log-forwarding delete`*
コマンド履歴ログの設定済みの宛て先を表示する	*`cluster log-forwarding show`*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

クラスタ時間の管理（クラスタ管理者のみ）

クラスタ時間が不正確だと問題が発生する可能性があります。Data ONTAPではクラスタのタイムゾーン、日付、時刻を手動で設定できますが、クラスタ時間を同期する場合はネットワーク タイム プロトコル（NTP）サーバを設定する必要があります。

NTPは常に有効です。ただし、NTPを有効にしただけでは、クラスタは外部の時間ソースと同期されません。Data ONTAPでは、次の方法でクラスタのNTP設定を管理できます。

- 最大10台の外部NTPサーバをクラスタに関連付けることができます（`cluster time-service ntp server create`）。
  - タイム サービスの冗長性と品質を高めるためには、最低3台の外部NTPサーバをクラスタに関連付ける必要があります。
  - NTPサーバはIPv4またはIPv6アドレス、あるいは完全修飾ホスト名で指定できます。
  - 使用するNTPバージョン（v3またはv4）を手動で指定できます。
    デフォルトでは、Data ONTAPは指定された外部NTPサーバでサポートされているNTPバージョンを自動的に選択します。
    指定したNTPバージョンがNTPサーバでサポートされていない場合は、時間を同期できません。
  - advanced権限レベルでは、クラスタに関連付けられている外部NTPサーバを、クラスタ時間を修正、調節するための主要時間ソースとして指定できます。
- クラスタに関連付けられているNTPサーバを表示できます（`cluster time-service ntp server show`）。
- クラスタのNTP設定を変更できます（`cluster time-service ntp server modify`）。
- クラスタと外部NTPサーバの関連付けを解除できます（`cluster time-service ntp server delete`）。
- advanced権限レベルでは、クラスタに関連付けられているすべての外部NTPサーバをクリアすることで、設定をリセットできます（`cluster time-service ntp server reset`）。

クラスタを統合しているノードは、自動的にクラスタのNTP設定を取り込みます。

Data ONTAPでは、NTPを使用できるだけでなく、クラスタ時間を手動で管理できます。この機能は、間違った時間を修正するときに便利です（ リブート後にノードの時間が著しくずれた場合など）。その場合は、NTPが外部の時間サーバと同期できるようになるまで、クラスタのおよその時間を指定します。手動で設定した時間は、クラスタ上のすべてのノードに反映されます。

クラスタ時間を手動で管理するには、次の方法があります。

- クラスタのタイムゾーン、日付、時刻を設定または変更できます（`cluster date modify`）。
- クラスタの現在のタイムゾーン、日付、時刻の設定を表示できます（`cluster date show`）。

注: 手動でのクラスタの日付や時刻変更は、ジョブ スケジュールには反映されません。ジョブは、ジョブが作成された時点または最後に実行された時点のクラスタの時刻に基づいて実行されます。そのため、クラスタの日付や時刻を手動で変更した場合は、`job show`コマンドおよび`job history show`コマンドを使用して、スケジュール済みのすべてのジョブが必要に応じて適切にキューに格納されているか完了していることを確認する必要があります。

関連情報

Network Time Protocol（NTP;ネットワーク タイム プロトコル）のサポート

クラスタ時間の管理用コマンド

クラスタのNTPサーバを管理するには、`cluster time-service ntp server`コマンドを使用します。クラスタ時間を手動で管理するには、`cluster date`コマンドを使用します。

次のコマンドによって、クラスタのNTPサーバを管理できます。

状況	使用するコマンド
クラスタを外部NTPサーバと関連付ける	*cluster time-service ntp server create*
クラスタに関連付けられたNTPサーバに関する情報を表示する	*cluster time-service ntp server show*
クラスタに関連付けられた外部NTPサーバの設定を変更する	*cluster time-service ntp server modify*
クラスタからNTPサーバへの関連付けを解除する	*cluster time-service ntp server delete*
すべての外部NTPサーバのクラスタとの関連付けを消去して設定をリセットする	*cluster time-service ntp server reset* **注:** このコマンドには、advanced権限レベルが必要です。

次のコマンドによって、手動でクラスタ時間を管理できます。

状況	使用するコマンド
タイム ゾーン、日付、および時刻を設定または変更する	*cluster date modify*
クラスタのタイム ゾーン、日付、および時刻の設定を表示する	*cluster date show*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

バナーとMOTDの管理

Data ONTAPでは、ログイン バナーまたはMessage Of The Day（MOTD）を設定して、クラスタまたはStorage Virtual Machine（SVM）のCLIユーザに管理情報を提供できます。

バナーは、ユーザにパスワードなどの認証を要求する前に、コンソール セッション（クラスタ アクセスのみ）またはSSHセッション（クラスタ アクセスまたはSVMアクセス）に表示されます。たとえば、バナーを使用して、システムへのログインを試行したユーザに次のような警告メッセージを表示することができます。

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been
logged.

Password:

cluster1::> _
```

MOTDは、ユーザの認証後、クラスタシェル プロンプトが表示される前に、コンソール セッション（クラスタ アクセスのみ）またはSSHセッション（クラスタ アクセスまたはSVMアクセス）に表示されます。たとえば、MOTDを使用して、認証されたユーザに次のような情報メッセージを表示することができます。

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running Data ONTAP Release 8.3.1.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.

cluster1::> _
```

バナーやMOTDの内容は、`security login banner modify`コマンドまたは`security login motd modify`コマンドを使用して作成または変更できます。

- CLIの対話型モードまたは非対話型モードを使用して、バナーまたはMOTDに使用するテキストを指定できます。
  対話型モードは、`-message`パラメータや`-uri`パラメータを指定せずにコマンドを実行すると起動されます。このモードでは、メッセージで改行（EOL）を使用することができます。
  非対話型モードでは、`-message`パラメータを使用してメッセージの文字列を指定します。このモードでは、改行はサポートされません。
- バナーまたはMOTDに使用する内容をFTPまたはHTTPからアップロードできます。
- 動的な内容を表示するようにMOTDを設定できます。
  MOTDには、たとえば次のような情報を動的に表示することができます。
  - クラスタ名、ノード名、SVM名
  - クラスタの日付や時刻
  - ログインしているユーザの名前
  - ユーザによるクラスタのノードへの前回のログイン
  - ログインしたデバイスの名前またはIPアドレス

- オペレーティング システムの名前
- ソフトウェア リリースのバージョン
- 有効なクラスタ バージョン文字列

`security login motd modify`のマニュアル ページに、動的に生成される内容をMOTDに表示するためのエスケープ シーケンスが記載されています。
バナーでは動的な内容はサポートされません。

バナーとMOTDはクラスタ レベルまたはSVMレベルで管理できます。

- バナーには次の特徴があります。
  - クラスタ用に設定したバナーは、バナー メッセージが定義されていないSVMに対しても表示されます。
  - SVMごとにSVMレベルのバナーを設定できます。
    このバナーが設定されたSVMでは、クラスタ レベルのバナーが設定されていても、SVMレベルのバナーだけが表示されます。
- MOTDには次の特徴があります。
  - クラスタ用に設定したMOTDは、デフォルトですべてのSVMに対しても有効になります。
  - それに加え、SVMごとにSVMレベルのMOTDを設定できます。
    この場合、SVMにログインしたユーザには、クラスタ レベルとSVMレベルの2つのMOTDが表示されます。
  - クラスタ レベルのMOTDを有効にするか無効にするかは、クラスタ管理者がSVM単位で設定できます。
    クラスタ管理者がSVMでクラスタ レベルのMOTDを無効にした場合、そのSVMにログインしたユーザにはクラスタ レベルのMOTDは表示されません。

バナーの作成

バナーを作成して、クラスタまたはSVMへのアクセスを試行したユーザにメッセージを表示することができます。バナーは、ユーザに認証を要求する前に、コンソール セッション（クラスタ アクセスのみ）またはSSHセッション（クラスタ アクセスまたはSVMアクセス）に表示されます。

手順

1. `security login banner modify`コマンドを使用して、クラスタまたはSVMのバナーを作成します。

状況	操作
1行のメッセージを指定する	`-message "text"`パラメータを使用してテキストを指定します。
メッセージで改行（EOL）を使用する	`-message`パラメータや`-uri`パラメータを指定せずにコマンドを実行して、対話型モードでバナーを編集します。
バナーに使用する内容を特定の場所からアップロードする	`-uri`パラメータを使用して、内容が格納されているFTPまたはHTTPの場所を指定します。

バナーの最大サイズは、改行も含めて2,048バイトまでです。

`-uri`パラメータを使用して作成したバナーには、静的な内容が表示されます。以降に元の内容が変更されても、自動では反映されません。

クラスタ用に作成したバナーは、既存のバナーがないSVMに対しても表示されます。以降にSVM用のバナーを作成すると、そのSVMに対しては、クラスタ レベルのバナーではなくそのバ

ナーが表示されます。SVMに対する-messageパラメータに二重引用符で囲んでハイフンを指定("-")すると、クラスタ レベルのバナーを使用するようにSVMがリセットされます。

2. security login banner showコマンドを使用して、作成したバナーが表示されることを確認します。

   -messageパラメータに空の文字列("")を指定すると、内容が空のバナーが表示されます。

   -messageパラメータに"-"を指定すると、バナーが設定されていないすべてのSVM(管理またはデータのいずれか)が表示されます。

バナーの作成例

次の例では、非対話型モードを使用してクラスタ「cluster1」用のバナーを作成しています。

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

次の例では、対話型モードを使用してSVM「svm1」用のバナーを作成しています。

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.
0        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

次の例では、作成したバナーを表示しています。

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------------
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------------
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

関連タスク

バナーの管理(171ページ)

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ:security login banner modify - Modify the login banner message

clustered Data ONTAP 8.3.1マニュアル ページ:security login banner show - Display the login banner message

バナーの管理

バナーはクラスタ レベルまたはSVMレベルで管理できます。クラスタ用に設定したバナーは、バナー メッセージが定義されていないSVMに対しても表示されます。以降にSVM用のバナーを作成すると、そのSVMに対しては、クラスタ用のバナーではなくそのバナーが表示されます。

選択肢

- クラスタ レベルのバナーの管理タスクを次に示します。

目的	操作
すべてのCLIログイン セッションに対して表示するバナーを作成する	クラスタ レベルのバナーを設定します。 **security login banner modify -vserver *cluster_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }**
すべてのログイン(クラスタとSVMの両方)に対するバナーを削除する	バナーを空の文字列("")に設定します。 **security login banner modify -vserver * -message ""**
SVM管理者が作成したバナーを変更する	SVMのバナー メッセージを変更します。 **security login banner modify -vserver *svm_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }**

- SVMレベルのバナーの管理タスクを次に示します。

  SVMのコンテキストでは、`-vserver svm_name`を指定する必要はありません。

目的	操作
クラスタ管理者が指定したバナーの代わりにSVM用の別のバナーを表示する	SVM用のバナーを作成します。 **security login banner modify -vserver *svm_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }**
クラスタ管理者が指定したバナーも含め、いずれのバナーもSVMに対して表示されないようにする	SVMに対するSVMのバナーを空の文字列に設定します。 **security login banner modify -vserver *svm_name* -message ""**
現在SVMレベルのバナーを使用しているSVMでクラスタレベルのバナーを使用する	SVMのバナーを"-"に設定します。 **security login banner modify -vserver *svm_name* -message "-"**

関連タスク

バナーの作成(169ページ)

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ:security login banner modify - Modify the login banner message

clustered Data ONTAP 8.3.1マニュアル ページ:security login banner show - Display the login banner message

MOTDの作成

Message Of The Day（MOTD）を作成して、認証されたCLIユーザに情報を提供することができます。MOTDは、ユーザの認証後、クラスタシェル プロンプトが表示される前に、コンソール セッション（クラスタ アクセスのみ）またはSSHセッション（クラスタ アクセスまたはSVMアクセス）に表示されます。

手順

1. `security login banner modify`コマンドを使用して、クラスタまたはSVMのMOTDを作成します。

状況	操作
1行のメッセージを指定する	`-message "text"`パラメータを使用してテキストを指定します。
改行（EOL）を使用する	`-message`パラメータや`-uri`パラメータを指定せずにコマンドを実行して、対話型モードでMOTDを編集します。
MOTDに使用する内容を特定の場所からアップロードする	`-uri`パラメータを使用して、内容が格納されているFTPまたはHTTPの場所を指定します。

MOTDの最大サイズは、改行も含めて2,048バイトまでです。

`security login motd modify`のマニュアル ページに、動的に生成される内容をMOTDに表示するためのエスケープ シーケンスが記載されています。

`-uri`パラメータを使用して作成したMOTDには、静的な内容が表示されます。以降に元の内容が変更されても、自動では反映されません。

クラスタ用に作成したMOTDは、デフォルトでは、各SVMに対して個別に作成したSVMレベルのMOTDと一緒に、すべてのSVMログインに対しても表示されます。SVMに対する`-is-cluster-message-enabled`パラメータを**`false`**に設定すると、そのSVMに対してはクラスタレベルのMOTDが表示されなくなります。

2. `security login motd show`コマンドを使用して、作成したMOTDが表示されることを確認します。

`-message`パラメータに空の文字列（`""`）を指定すると、未設定または内容が空のMOTDが表示されます。

MOTDの作成例

次の例では、非対話型モードを使用してクラスタ「cluster1」用のMOTDを作成しています。

```
cluster1::> security login motd modify -message "Greetings!"

cluster1::>
```

次の例では、対話型モードを使用してSVM「svm1」用のMOTDを作成しています。このMOTDでは、エスケープ シーケンスを使用して、動的に生成される内容を表示します。

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.
0        1         2         3         4         5         6         7         8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login was \L.

cluster1::>
```

次の例では、作成したMOTDを表示しています。

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------------
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------------
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login was \L.

2 entries were displayed.

cluster1::>
```

関連タスク

MOTDの管理（173ページ）

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ：security login motd modify - Modify the message of the day
clustered Data ONTAP 8.3.1マニュアル ページ：security login motd show - Display the message of the day

MOTDの管理

Message Of The Day（MOTD）はクラスタ レベルまたはSVMレベルで管理できます。それに加え、SVMごとにSVMレベルのMOTDを設定できます。クラスタ レベルのMOTDを有効にするか無効にするかは、クラスタ管理者がSVMごとに設定できます。

選択肢

- クラスタ レベルのMOTDの管理タスクを次に示します。

目的	操作
既存のMOTDがない場合にすべてのログインに対するMOTDを作成する	クラスタ レベルのMOTDを設定します。 **security login motd modify -vserver *cluster_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }**
SVMレベルのMOTDが設定されていない場合にすべてのログインに対するMOTDを変更する	クラスタ レベルのMOTDを変更します。 **security login motd modify -vserver *cluster_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }**
SVMレベルのMOTDが設定されていない場合にすべてのログインに対するMOTDを削除する	クラスタ レベルのMOTDを空の文字列（""）に設定します。 **security login motd modify -vserver *cluster_name* -message ""**

目的	操作
すべてのSVMで、SVMレベルのMOTDを使用する代わりに、クラスタレベルのMOTDを表示する	クラスタレベルのMOTDを設定してから、SVMレベルのすべてのMOTDを空の文字列に設定し、クラスタレベルのMOTDを有効にします。 1. **security login motd modify -vserver *cluster_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }** 2. **security login motd modify { -vserver !"*cluster_name*" } -message "" -is-cluster-message-enabled true**
クラスタレベルのMOTDを使用せずに、選択したSVMに対してのみMOTDを表示する	クラスタレベルのMOTDを空の文字列に設定し、選択したSVMに対するSVMレベルのMOTDを設定します。 1. **security login motd modify -vserver *cluster_name* -message ""** 2. **security login motd modify -vserver *svm_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] }** この手順は、必要に応じて、各SVMに対して繰り返し実行できます。
すべてのSVM（データと管理の両方）に対して同じSVMレベルのMOTDを使用する	同じMOTDを使用するようにクラスタとすべてのSVMを設定します。 **security login motd modify -vserver * { [-message "*text*"] | [-uri *ftp_or_http_addr*] }** **注:** CLIの対話型モードでは、クラスタとそれぞれのSVMについて、MOTDを個別に入力するように求められます。この場合は、それぞれのプロンプトに同じMOTDを貼り付けます。
クラスタレベルのMOTDをすべてのSVMで必要に応じて表示できるようにし、クラスタログインに対しては表示されないようにする	クラスタレベルのMOTDを設定し、クラスタに対する表示を無効にします。 **security login motd modify -vserver *cluster_name* { [-message "*text*"] | [-uri *ftp_or_http_addr*] } -is-cluster-message-enabled false**
一部のSVMのみクラスタレベルとSVMレベルの両方のMOTDが設定されている場合に、クラスタレベルとSVMレベルのすべてのMOTDを削除する	MOTDに空の文字列を使用するようにクラスタとすべてのSVMを設定します。 **security login motd modify -vserver * -message ""**
他のSVMで空の文字列が使用されている場合やクラスタレベルで別のMOTDが使用されている場合に、文字列が空でないSVMのMOTDだけを変更する	拡張クエリを使用して選択したMOTDを変更します。 **security login motd modify { -vserver !"*cluster_name*" -message !"" } { [-message "*text*"] | [-uri *ftp_or_http_addr*] }**
該当するテキストが複数行にまたがる場合も含め、メッセージ内に特定のテキスト（例:「January」「2015」）を含むすべてのMOTDを表示する	クエリを使用してMOTDを表示します。 **security login motd show -message *"January"*"2015"***
複数の連続する改行（EOL）を含むMOTDを対話型モードで作成する	対話型モードで、スペース キーのあとに続けてEnterキーを押します。MOTDの入力を終了せずに空白行を入力できます。

- SVMレベルのMOTDの管理タスクを次に示します。

  SVMのコンテキストでは、`-vserver svm_name`を指定する必要はありません。

目的	操作
すでにSVMレベルのMOTDが設定されたSVMで、別のSVMレベルのMOTDを使用する	SVMレベルのMOTDを変更します。 **`security login motd modify -vserver svm_name { [-message "text"] | [-uri ftp_or_http_addr] }`**
すでにSVMレベルのMOTDが設定されたSVMで、クラスタレベルのMOTDだけを使用する	SVMレベルのMOTDを空の文字列に設定し、そのSVMに対してクラスタレベルのMOTDを有効にするようにクラスタ管理者に依頼します。 1. **`security login motd modify -vserver svm_name -message ""`** 2. （クラスタ管理者）**`security login motd modify -vserver svm_name -is-cluster-message-enabled true`**
現在クラスタレベルとSVMレベルの両方のMOTDが表示されているSVMで、いずれのMOTDも表示されないようにする	SVMレベルのMOTDを空の文字列に設定し、そのSVMに対してクラスタレベルのMOTDを無効にするようにクラスタ管理者に依頼します。 1. **`security login motd modify -vserver svm_name -message ""`** 2. （クラスタ管理者）**`security login motd modify -vserver svm_name -is-cluster-message-enabled false`**

関連タスク

MOTDの作成（172ページ）

関連情報

clustered Data ONTAP 8.3.1マニュアル ページ:security login motd modify - Modify the message of the day

clustered Data ONTAP 8.3.1マニュアル ページ:security login motd show - Display the message of the day

ライセンスの管理（クラスタ管理者のみ）

ライセンスには、ソフトウェアの使用権が1つ以上記録されています。ライセンス キー（*ライセンス コード*とも呼ばれます）をインストールすることで、クラスタ上の特定の機能やサービスを使用できるようになります。Data ONTAPで、機能ライセンスを管理したり、機能の使用状況やライセンス使用権のリスクを監視したりすることができます。

クラスタごとにクラスタ ベースのライセンス キーが必要になります。このライセンスキーは、クラスタのセットアップ中またはセットアップ後にインストールできます。一部の機能には追加のライセンスが必要です。Data ONTAPの機能ライセンスはパッケージとして発行されます。各パッケージには複数または単一の機能が含まれます。パッケージにはライセンス キーが必要であり、キーをインストールすることで、パッケージのすべての機能にアクセスできるようになります。Data ONTAPでは、先にクラスタ ベースのライセンス キーをインストールしないと、機能ライセンスをインストールできません。

Data ONTAP 8.2以降、すべてのライセンス キーは28文字です。Data ONTAP 8.2より前にインストールされたライセンスは、Data ONTAP 8.2以降のリリースでも有効です。ただし、ライセンスを再インストールする場合（たとえば、以前のリリースでインストールしたライセンスを削除してData ONTAP 8.2以降で再インストールする場合、またはData ONTAP 8.2以降を実行するクラスタのノードのコントローラを交換する場合）は、ライセンス キーを28文字で入力する必要があります。

初回購入のソフトウェアまたはアドオン ソフトウェアのライセンス キーは、ネットアップ サポート サイトの**[My Support]** > **[Software Licenses]**で入手できます（ログインする必要があります）。[Software Licenses]ページでライセンス キーを見つけられない場合は、営業またはサポート担当者にお問い合わせください。

Data ONTAPでは、次の方法で機能ライセンスを管理できます。

- 1つ以上のライセンス キーを追加する（`system license add`）
- インストール済みのライセンスに関する情報を表示する（`system license show`）
- ライセンスが必要なパッケージと、クラスタ上でのそのパッケージ現在のライセンス ステータスを表示する（`system license status show`）
- シリアル番号を指定してクラスタまたはノードからライセンスを削除する（`system license delete`）
  クラスタが機能するためには、クラスタ ベースのライセンスが必要です。ユーザはクラスタ ライセンスを削除できません。
- 期限切れのライセンスまたは未使用のライセンスを表示または削除する（`system license clean-up`）

Data ONTAPでは、次の方法で機能の使用状況やライセンス使用権のリスクを監視できます。

- クラスタでの機能の使用状況の概要をノード単位で表示する（`system feature-usage show-summary`）
  この概要には、機能の使用週数、機能の最後の使用日時などのカウンタ情報が含まれます。
- クラスタでの機能の使用ステータスをノード単位および週単位で表示する（`system feature-usage show-history`）
  機能の使用ステータスは、**`not-used`**、**`configured`**、**`in-use`**のいずれかで示されます。使用状況の情報がない場合は、ステータスに**`not-available`**と表示されます。
- 各ライセンス パッケージについて、ライセンス使用権のリスクをステータスで表示する（`system license entitlement-risk show`）

リスク ステータスは、**low**、**medium**、**high**、**unlicensed**、**unknown**のいずれかで示されます。リスク ステータスはAutoSupportメッセージにも記載されます。ライセンス使用権のリスクは基本ライセンス パッケージには該当しません。
ライセンス使用権のリスクは、以下に挙げるような複数の要因に基づいて評価されます。

- 各パッケージのライセンスの状態
- 各ライセンスの種類と有効期限ステータス、およびクラスタ全体でのライセンスの統一性
- ライセンス パッケージに関連付けられた機能の使用状況

評価プロセスでクラスタにライセンス使用権のリスクがあると判断された場合、推奨される対処方法も出力されます。

関連情報

NetApp KB Article 3013749: Data ONTAP 8.2 and 8.3 Licensing Overview and References
NetApp KB Article 1014509: How to verify Data ONTAP Software Entitlements and related License Keys using the Support Site
ネットアップ：Data ONTAP Entitlement Risk Status

ライセンス タイプとライセンス方式

ライセンス タイプとライセンス方式について理解しておくと、クラスタのライセンスを管理する際に役に立ちます。

ライセンス タイプ

パッケージには、クラスタにインストールされる次のライセンス タイプが1つ以上含まれます。
`system license show`コマンドを実行すると、パッケージのインストール済みライセンス タイプが表示されます。

- 標準ライセンス（**license**）
  標準ライセンスはノード ロック ライセンスです。特定のシステム シリアル番号（*コントローラのシリアル番号*とも呼ばれる）を持つノードに対して発行されます。標準ライセンスは、シリアル番号が一致するノードに対してのみ有効です。
  標準ノード ロック ライセンスをインストールすると、ノードで、ライセンスされた機能を使用できるようになります。クラスタでライセンス機能を使用するには、少なくとも1つのノードに、その機能のライセンスをインストールする必要があります。機能の使用権がないノードでライセンス機能を使用すると、ライセンス違反となる場合があります。
  Data ONTAP 8.2以降のリリースでは、Data ONTAP 8.2より前にインストールされたライセンスは標準ライセンスとして扱います。したがって、Data ONTAP 8.2以降のリリースでは、クラスタ内のノードはすべて自動的に、以前ライセンスされた機能が含まれているパッケージの標準ライセンスを保有していることになります。`system license show`コマンドに`-legacy yes`パラメータを指定して実行すると、このようなライセンスが表示されます。

- サイト ライセンス（**site**）
  サイト ライセンスは、特定のシステム シリアル番号に関連付けられません。サイト ライセンスをインストールすると、クラスタ内のすべてのノードで、ライセンスされた機能を使用できるようになります。`system license show`コマンドを実行すれば、該当するクラスタ シリアル番号のサイト ライセンスが表示されます。
  サイト ライセンスがあるクラスタからノードを削除した場合、そのノードはサイト ライセンスを保持できず、ライセンスされた機能を使用できなくなります。また、サイト ライセンスのあるクラスタにノードを追加した場合、そのノードには自動的にサイト ライセンスが付与され、ライセンスされた機能を使用できるようになります。

- 評価用ライセンス（**demo**）

評価用ライセンスは、一定期間（`system license show`コマンドで表示可能）が経過すると失効する一時的なライセンスです。評価用ライセンスを使用すれば、ライセンスを購入せずに特定のソフトウェア機能を試すことができます。評価用ライセンスはクラスタ全体のライセンスです。また、ノードの特定のシリアル番号には関連付けられません。
パッケージの評価用ライセンスがあるクラスタからノードを削除した場合、そのノードは評価用ライセンスを保持できません。

ライセンス方式

パッケージにはクラスタ全体のライセンス（**site**タイプまたは**demo**タイプ）とノード ロック ライセンス（**license**タイプ）の両方をインストールできます。したがって、インストールされたパッケージには、クラスタ内に複数のライセンス タイプが存在する場合があります。ただし、パッケージの*ライセンス方式*はクラスタに対して1つしか存在しません。`system license status show`コマンドの**licensed method**フィールドには、パッケージに使用されるライセンスが表示されます。このコマンドにより、次のようにライセンス方式が決定します。

- クラスタにインストールされるライセンス タイプがパッケージに1つしか含まれていない場合、そのインストールされるライセンス タイプがライセンス方式となります。
- ライセンスがクラスタにインストールされず、パッケージに含まれていない場合、ライセンス方式は**none**となります。
- クラスタにインストールされるライセンス タイプがパッケージに複数含まれている場合、ライセンス方式は、次のライセンス タイプの優先順位（**site**、**license**、**demo**）に従って決定されます。次に例を示します。
  - パッケージのサイト ライセンス、標準ライセンス、評価用ライセンスがある場合、クラスタのパッケージのライセンス方式は**site**です。
  - パッケージの標準ライセンス、評価用ライセンスがある場合、クラスタのパッケージのライセンス方式は**license**です。
  - パッケージの評価用ライセンスしかない場合、クラスタのパッケージのライセンス方式は**demo**です。

ライセンスの管理用コマンド

クラスタの機能のライセンスを管理するには、`system license`コマンドを使用します。機能の使用状況を監視するには、`system feature-usage`コマンドを使用します。

状況	使用するコマンド
ライセンスを1つ以上追加する	*`system license add`*

状況	使用するコマンド
インストール済みのライセンスに関する次のような情報を表示する。たとえば、 • ライセンスのパッケージ名と説明 • ライセンス タイプ（**site**、**license**、または**demo**） • 有効期限（存在する場合） • パッケージのライセンス対象であるクラスタまたはノード • ライセンスがData ONTAP 8.2よりも前にインストールされたかどうか（**legacy**） • 顧客ID	*system license show* **注:** `-instance`パラメータを指定しないと表示されない情報があります。
ライセンスが必要なパッケージすべてと、次のようなパッケージの現在のライセンス ステータスを表示する • パッケージ名 • ライセンス方式 • 有効期限（存在する場合）	*system license status show*
クラスタまたは指定したシリアル番号のノードからパッケージのライセンスを削除する	*system license delete*
期限切れのライセンスまたは未使用のライセンスを表示または削除する	*system license clean-up*
クラスタでの機能の使用状況の概要をノード単位で表示する	*system feature-usage show-summary*
クラスタでの機能の使用ステータスをノード単位および週単位で表示する	*system feature-usage show-history*
各ライセンス パッケージのライセンス使用権リスク ステータスを表示する	*system license entitlement-risk show* **注:** `-detail`パラメータおよび`-instance`パラメータを指定しないと表示されない情報があります。

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

ジョブおよびスケジュールの管理

*ジョブ*はジョブ マネージャによって管理される非同期タスクです。通常、ジョブはコピー、移動、ミラーリングなど、長時間実行されるボリューム操作です。ジョブは監視、一時停止、停止、および再開できます。また、指定されたスケジュールで実行されるように設定することもできます。

ジョブのカテゴリ

管理可能なジョブには、3つのカテゴリ（サーバ関連、クラスタ関連、プライベート）があります。

ジョブは、次のいずれかのカテゴリに分類されます。

サーバ関連ジョブ

このジョブは、実行する特定のノードに対して、管理フレームワークによってキューに登録されます。

クラスタ関連ジョブ

このジョブは、実行するクラスタ内の任意のノードに対して、管理フレームワークによってキューに登録されます。

プライベート ジョブ

このジョブはノードに固有で、レプリケートされたデータベース（RDB）またはその他のクラスタ メカニズムを使用しません。プライベート ジョブの管理用コマンドには、advanced 権限レベル以上が必要です。

ジョブの管理用コマンド

ジョブはジョブ キューに配置され、リソースが利用可能になるとバックグラウンドで実行されます。ジョブで使用するクラスタ リソースが多すぎる場合は、そのジョブを停止するか、またはクラスタに対する要求が少なくなるまで一時停止できます。また、ジョブを監視して再開することもできます。

あるジョブを呼び出すコマンドを入力すると、通常、ジョブがキューに登録されたというメッセージが表示され、CLIのコマンド プロンプトに戻ります。ただし、一部のコマンドではジョブの進捗状況が表示され、ジョブが完了するまでCLIのコマンド プロンプトに戻りません。このような場合は、Ctrl+Cキーを押してジョブをバックグラウンドに移動できます。

状況	使用するコマンド
すべてのジョブに関する情報を表示する	`job show`
ジョブに関する情報をノード単位で表示する	`job show bynode`
クラスタ関連ジョブに関する情報を表示する	`job show-cluster`
完了したジョブに関する情報を表示する	`job show-completed`
ジョブ履歴に関する情報を表示する	`job history show` クラスタ内の各ノードには、最高25,000個のジョブ レコードが格納されます。このため、ジョブ履歴全体を表示しようとすると長い時間がかかることがあります。待ち時間が長くならないようにするには、ジョブをノード、Storage Virtual Machine（SVM）、またはレコードIDごとに表示します。

状況	使用するコマンド
プライベート ジョブのリストを表示する	*job private show* （advanced権限レベル）
完了したプライベート ジョブに関する情報を表示する	*job private show-completed* （advanced権限レベル）
ジョブ マネージャの初期化状態に関する情報を表示する	*job initstate show* （advanced権限レベル）
ジョブの進捗状況を監視する	*job watch-progress*
プライベート ジョブの進捗状況を監視する	*job private watch-progress* （advanced権限レベル）
ジョブを一時停止する	*job pause*
プライベート ジョブを一時停止する	*job private pause* （advanced権限レベル）
一時停止したジョブを再開する	*job resume*
一時停止したプライベート ジョブを再開する	*job private resume* （advanced権限レベル）
ジョブを停止する	*job stop*
プライベート ジョブを停止する	*job private stop* （advanced権限レベル）
ジョブを削除する	*job delete*
プライベート ジョブを削除する	*job private delete* （advanced権限レベル）
クラスタ関連ジョブと、そのジョブが所有する利用できないノードとの関連付けを解除し、別のノードがジョブの所有権を取得できるようにする	*job unclaim* （advanced権限レベル）

注: 完了したジョブの結果は、`event log show`コマンドを使用して確認できます。

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

ジョブ スケジュールの管理用コマンド

多くのタスク（Volume Snapshotコピーなど）は、指定したスケジュールで実行するように設定できます。特定の時間に実行されるスケジュールは、*cron*スケジュールと呼ばれます（UNIXの`cron`スケジュールに類似しています）。周期的に実行されるスケジュールは、*インターバル* スケジュールと呼ばれます。ジョブ スケジュールを管理するには、`job schedule`コマンドを使用します。

手動でのクラスタの日付や時刻の変更は、ジョブ スケジュールには反映されません。ジョブは、ジョブが作成された時点または最後に実行された時点のクラスタの時刻に基づいて実行されます。そのため、クラスタの日付や時刻を手動で変更した場合は、`job show`コマンドおよび`job history show`コマンドを使用して、スケジュール済みのすべてのジョブが必要に応じて適切にキューに格納されているか完了していることを確認する必要があります。

クラスタがMetroCluster構成に属している場合、両方のクラスタのジョブ スケジュールが同一である必要があります。そのため、ジョブ スケジュールを作成、変更、削除する場合、リモート クラスタでも同じ処理を実行する必要があります。

状況	使用するコマンド
すべてのスケジュールに関する情報を表示する	*job schedule show*
ジョブのリストをスケジュール別に表示する	*job schedule show-jobs*
cronスケジュールに関する情報を表示する	*job schedule cron show*
インターバル スケジュールに関する情報を表示する	*job schedule interval show*
cronスケジュールを作成する	*job schedule cron create*
インターバル スケジュールを作成する	*job schedule interval create* -days、-hours、-minutes、または-seconds パラメータから、少なくとも1つを指定する必要があります。
cronスケジュールを変更する	*job schedule cron modify*
インターバル スケジュールを変更する	*job schedule interval modify*
スケジュールを削除する	*job schedule delete*
cronスケジュールを削除する	*job schedule cron delete*
インターバル スケジュールを削除する	*job schedule interval delete*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

クラスタ構成のバックアップおよびリストア（クラスタ管理者のみ）

クラスタ構成をバックアップすると、障害または緊急事態が発生した場合に、ノードまたはクラスタの設定をリストアできます。

構成バックアップ ファイルとは

構成バックアップ ファイルは、クラスタとクラスタ内のノードが正しく動作するために必要な、設定可能なすべてのオプションに関する情報が含まれているアーカイブ ファイル（.7z）です。

このファイルには、各ノードのローカル設定に加えて、クラスタ全体にレプリケートされる設定が格納されます。構成バックアップ ファイルは、クラスタ設定のバックアップとリストアに使用します。

構成バックアップ ファイルには、次の2つの種類があります。

ノード構成バックアップ ファイル

クラスタ内の正常なノードにはそれぞれノード構成バックアップ ファイルが含まれています。このファイルには、クラスタ内でノードの動作の正常性を確保するために必要な、すべての設定情報とメタデータが含まれています。

クラスタ構成バックアップ ファイル

クラスタ構成バックアップ ファイルには、クラスタ内のすべてのノード構成バックアップ ファイルのアーカイブと、レプリケートされたクラスタ構成情報（RDB[レプリケートされたデータベース]ファイル）が含まれています。クラスタ構成バックアップ ファイルを使用すると、クラスタ全体またはクラスタ内のノードの設定をリストアできます。クラスタ構成バックアップ スケジュールを使用すると、これらのファイルが自動的に作成され、クラスタ内の複数のノードに格納されます。

注: 構成バックアップ ファイルに含まれているのは設定情報だけです。ユーザ データは含まれていません。ユーザ データのリストアについては、*『clustered Data ONTAP データ保護ガイド』*を参照してください。

構成バックアップの管理

構成バックアップ スケジュールは、クラスタ内の各ノードおよび、そのクラスタ自体の構成バックアップ ファイルを自動的に作成します。これらのスケジュールの一部の構成を変更したり、構成バックアップ ファイルを手動で作成したりできます。

ノードおよびクラスタ構成を自動的にバックアップする方法

3通りのスケジュールで、クラスタおよびノードの構成バックアップ ファイルが自動的に作成され、クラスタのノード間で複製します。

構成バックアップ ファイルは、次のスケジュールに従って自動的に作成されます。

- 8時間ごと
- 毎日
- 毎週

それぞれのスケジュールで、ノード構成バックアップ ファイルが、クラスタの正常な各ノードに作成されます。これらの構成バックアップ ファイルはすべて、複製されたクラスタ構成とともに単一のクラスタ構成バックアップ ファイルに収集され、クラスタ内の1つ以上のノードに保存されます。

シングル ノード クラスタの場合（Data ONTAP Edgeシステムを含む）、ソフトウェアのセットアップ中に構成のバックアップ先を指定できます。セットアップ後、これらの設定はData ONTAPコマンドを使用して変更できます。

構成バックアップ スケジュールの管理用コマンド

構成バックアップ スケジュールを管理するには、`system configuration backup settings`コマンドを使用します。

これらのコマンドはadvanced権限レベルで使用できます。

状況	使用するコマンド
構成バックアップ スケジュールの次のような設定を変更する • クラスタ内のデフォルトの場所に加えて構成バックアップ ファイルがアップロードされるリモートURL（HTTPまたはFTP）を指定する • リモートURLへのログインに使用するユーザ名を指定する • それぞれの構成バックアップ スケジュールについて維持するバックアップ数を設定する	*system configuration backup settings modify*
リモートURLへのログインに使用するパスワードを設定する	*system configuration backup settings set-password*
構成バックアップ スケジュールの設定を表示する	*system configuration backup settings show* **注:** ユーザ名、および各スケジュールについて維持するバックアップ数を表示するには、`-instance`パラメータを設定します。

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

構成バックアップ ファイルの管理用コマンド

クラスタとノードの構成バックアップ ファイルを管理するには、`system configuration backup`コマンドを使用します。

これらのコマンドはadvanced権限レベルで使用できます。

状況	使用するコマンド
新しいノードまたはクラスタの構成バックアップ ファイルを作成する	*system configuration backup create*
クラスタ内のノードから別のノードに構成バックアップ ファイルをコピーする	*system configuration backup copy*

状況	使用するコマンド
クラスタ内のノードからリモートURL（HTTPまたはFTP）に構成バックアップ ファイルをアップロードする	`system configuration backup upload` **注:** 構成バックアップ ファイルのアップロード先のWebサーバでは、PUT処理が有効になっている必要があります。詳細については、Webサーバのマニュアルを参照してください。
リモートのURLからクラスタ内のノードに構成バックアップ ファイルをダウンロードする	`system configuration backup download`
クラスタ内のノードで構成バックアップ ファイルの名前を変更する	`system configuration backup rename`
クラスタ内の1つ以上のノードについてノードおよびクラスタ構成バックアップ ファイルを表示する	`system configuration backup show`
ノード上の構成バックアップ ファイルを削除する	`system configuration backup delete` **注:** このコマンドを実行すると、指定したノードにある構成バックアップ ファイルだけが削除されます。その構成バックアップ ファイルがクラスタ内の他のノードにあっても、それらはノードに残ります。

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

ノード構成のリカバリ

ノード、そのルート ボリューム、またはその構成情報のいずれかが損失または破損した場合に、構成バックアップ ファイルを使用してノードの設定をリカバリします。

手順

1. ノードのリカバリに使用する構成バックアップ ファイルの検索（185ページ）
2. 構成バックアップ ファイルを使用したノード構成のリストア（186ページ）

ノードのリカバリに使用する構成バックアップ ファイルの検索

ノード構成をリカバリするには、リモートURLまたはクラスタのノードにある構成バックアップ ファイルを使用します。

タスク概要

ノード構成をリストアするには、クラスタまたはノード構成バックアップ ファイルのいずれかを使用します。

手順

1. 構成のリストアに必要なノードに構成バックアップ ファイルを利用できるようにします。

構成バックアップ ファイルの場所	操作
リモートURL	リカバリするノードにシステム構成バックアップをダウンロードするには、advanced権限レベルでsystem configuration backup downloadコマンドを使用します。
クラスタのノード上	**a.** リカバリするノードの構成を含むクラスタで利用可能な構成バックアップ ファイルのリストを表示するには、system configuration backup showコマンドをadvanced権限レベルで使用します。 **b.** 特定した構成バックアップ ファイルがリカバリするノードにない場合は、system configuration backup copyコマンドを使用して、リカバリ ノードにコピーします。

以前にクラスタを作成し直したことがある場合は、クラスタの再作成後に作成した構成バックアップ ファイルを選択します。クラスタの再作成の前に作成した構成バックアップ ファイルを使用する必要がある場合は、ノードをリカバリしたあとで、クラスタを再度、作成し直す必要があります。

構成バックアップ ファイルを使用したノード構成のリストア

ノード構成をリストアするには、特定し、リカバリ ノードに利用可能にした構成バックアップ ファイルを使用します。

タスク概要

このタスクは、ノードのローカル構成ファイルが失われた障害からリカバリする場合にのみ実行します。

手順

1. ノードが正常な場合は、別のノードのadvanced権限レベルでcluster modifyコマンドに-nodeパラメータおよび-eligibilityパラメータを指定して実行し、ノードの参加資格を無効にしてクラスタから分離します。

   ノードが正常でない場合は、この手順を省略する必要があります。

   例

   この例では、node2を変更してクラスタへの参加資格を無効にし、構成をリストアできるようにします。

   ```
   cluster1::*> cluster modify -node node2 -eligibility false
   ```

2. system configuration recovery node restoreコマンドをadvanced権限レベルで使用し、ノード構成を構成バックアップ ファイルからリストアします。

   名前を含むIDがノードから失われている場合は、-nodename-in-backupパラメータを使用して構成バックアップ ファイルのノード名を指定する必要があります。

   例

   この例では、ノードに保存されている構成バックアップ ファイルの1つを使用してノードの構成をリストアします。

   ```
   cluster1::*> system configuration recovery node restore -backup
   cluster1.8hour.2011-02-22.18_15_00.7z

   Warning: This command overwrites local configuration files with
            files contained in the specified backup file. Use this
   ```

```
          command only to recover from a disaster that resulted
          in the loss of the local configuration files.
          The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

構成がリストアされ、ノードがリブートします。

3. ノードをクラスタの対象外にした場合は、`system configuration recovery cluster sync`コマンドを使用してノードを対象とし、クラスタと同期します。

4. SAN環境を使用している場合は、`system node reboot`コマンドを使用して、ノードをリブートし、SANクォーラムを再確立します。

終了後の操作

以前にクラスタを作成し直したことがある場合、またクラスタの再作成の前に作成された構成バックアップ ファイルを使用してノードの構成をリストアする場合は、再度クラスタを作成し直す必要があります。

関連タスク

ノードのクラスタとの同期（190ページ）

クラスタ構成のリカバリ

クラスタ全体のクォーラムが存在しない場合は、クラスタのリカバリに使用する設定を見つけ、クラスタを再作成し、各ノードをそのクラスタに結合することで、クラスタ構成をリカバリします。

手順

1. クラスタのリカバリに使用する構成の検索（187ページ）
2. 既存の構成からのクラスタ構成のリストア（188ページ）

クラスタのリカバリに使用する構成の検索

クラスタ内のノード、またはクラスタ構成バックアップ ファイルのいずれかの構成を使用してクラスタをリカバリできます。

手順

1. クラスタのリカバリに使用する構成の種類を選択します。

   - クラスタ内のノード
     クラスタが複数のノードで構成されている場合で、クラスタが適切な構成であった時点で作成されたクラスタ構成がいずれかのノードに存在していれば、そのノードに格納された構成を使用してクラスタをリカバリできます。
     ほとんどの場合は、クラスタ構成のリストアに使用するノードは最新のトランザクションのIDを持つレプリケーション リングが含まれているノードが最適です。advanced権限レベルで`cluster ring show`コマンドを使用すると、クラスタ内の各ノードで利用可能な一連のレプリケーション リングを表示できます。

   - クラスタ構成バックアップ ファイル
     適切なクラスタ構成を持つノードが特定できない場合、またはクラスタがシングル ノードで構成されている場合は、クラスタ構成バックアップ ファイルを使用してクラスタをリカバリできます。
     構成バックアップ ファイルからクラスタをリカバリするには、診断ツールを使用して、リカバリするノード上のバックアップとクラスタ構成との間の矛盾を解決しなければならないことがあ

ります。そのため、構成バックアップ ファイルを使用する場合は、テクニカル サポートに問い合わせる準備をしておいてください。

2. クラスタ構成バックアップ ファイルを使用する場合は、クラスタのリカバリに使用するノードでそのファイルを利用できるようにします。

構成バックアップ ファイルの場所	操作
リモートURL	リカバリするノードにシステム構成バックアップをダウンロードするには、advanced権限レベルで`system configuration backup download`コマンドを使用します。
クラスタのノード上	**a.** advanced権限レベルで`system configuration backup show`コマンドを使用し、クラスタが適切な構成であった時点で作成されたクラスタ構成バックアップ ファイルを検索します。 **b.** クラスタのリカバリに使用するノード上にクラスタ構成バックアップ ファイルがない場合は、`system configuration backup copy`コマンドを使用してリカバリするノードにコピーします。

既存の構成からのクラスタ構成のリストア

クラスタ障害後に既存の構成からクラスタ構成をリストアするには、クラスタ構成を選択してリカバリするノードで利用できるようにし、次にその構成を使用してクラスタを再作成し、残りのノードを新しいクラスタに再追加します。

タスク概要

クラスタ構成の損失となる障害からリカバリするには、このタスクのみを実行する必要があります。

注意: 構成バックアップ ファイルからクラスタを再作成する場合は、テクニカル サポートに問い合わせて、構成バックアップ ファイルと現在のクラスタ構成との矛盾をすべて解決しておく必要があります。

手順

1. 各HAペアのストレージ フェイルオーバーを無効にします。

   storage failover modify -node *node_name* -enabled false

   ストレージ フェイルオーバーを無効にするのは、各HAペアに対して1度だけです。一方のノードでストレージ フェイルオーバーを無効にすると、そのノードのパートナーでもストレージ フェイルオーバーが無効になります。

2. リカバリするノード以外の各ノードを停止します。

   system node halt -node *node_name* -reason *"text"*

   例

   ```
   cluster1::*> system node halt -node node0 -reason "recovering cluster"

   Warning: Are you sure you want to halt the node? {y|n}: y
   ```

3. 権限レベルをadvancedに設定します。

   set -privilege advanced

4. リカバリ ノード上で、`system configuration recovery cluster recreate`コマンドを使用してクラスタを再作成します。

例

この例では、リカバリ ノードに保存された構成情報を使用してクラスタを再作成します。

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

新しいクラスタはリカバリ ノードに作成されます。

5. 構成バックアップ ファイルからクラスタを再作成する場合は、クラスタのリカバリがまだ進行中であることを確認します。

   system configuration recovery cluster show

   正常なノードからクラスタを再作成する場合、クラスタのリカバリの状態を確認する必要はありません。

   例

   ```
   cluster1::*> system configuration recovery cluster show
    Recovery Status: in-progress
    Is Recovery Status Persisted: false
   ```

6. 再作成したクラスタに再追加が必要な各ノードをブートします。

   ノードは一度に1つずつリブートする必要があります。

7. 再作成したクラスタに再追加が必要な各ノードで、以下を実行します。

   a. 再作成したクラスタ上の正常なノードから、ターゲット ノードを再追加します。

      system configuration recovery cluster rejoin -node *node_name*

      例

      この例では、ターゲット ノード（「node2」）を新しく作成したクラスタに再追加します。

      ```
      cluster1::*> system configuration recovery cluster rejoin -node
      node2

      Warning: This command will rejoin node "node2" into the local
               cluster, potentially overwriting critical cluster
               configuration files. This command should only be used
               to recover from a disaster. Do not perform any other
               recovery operations while this operation is in progress.
               This command will cause node "node2" to reboot.
      Do you want to continue? {y|n}: y
      ```

      ターゲット ノードがリブートし、クラスタに追加されます。

   b. ターゲット ノードが正常であり、クラスタ内の残りのノードとクォーラムを形成していることを確認します。

      cluster show -eligibility true

      別のノードを再追加する前に、ターゲット ノードを再作成したクラスタに再追加する必要があります。

例

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. 構成バックアップ ファイルからクラスタを再作成した場合は、リカバリ ステータスを「complete」に設定します。

   `system configuration recovery cluster modify -recovery-status complete`

9. admin権限レベルに戻ります。

   `set -privilege admin`

10. クラスタが2つのノードだけで構成されている場合、`cluster ha modify`コマンドを使用してクラスタHAを再度有効にします。

11. `storage failover modify`コマンドを使用して、各HAペアのストレージ フェイルオーバーを再度有効にします。

終了後の操作

クラスタにSnapMirrorピア関係がある場合は、それらの関係も再作成する必要があります。詳細については、*『clustered Data ONTAP データ保護ガイド』*を参照してください。

ノードのクラスタとの同期

クラスタ全体のクォーラムが存在するものの、1つまたは複数のノードがクラスタと同期していない場合は、ノードを同期し、そのノード上でレプリケートされたデータベース（RDB）をリストアしてクォーラムに加える必要があります。

手順

1. 正常なノードから、advanced権限レベルで`system configuration recovery cluster sync`コマンドを入力し、同期していないノードをクラスタ構成と同期します。

   例

   次の例では、残りのクラスタとノード（*node2*）を同期します。

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify
that the cluster applications go online.
```

タスクの結果

RDBがノードにレプリケートされ、そのノードがクラスタに参加できるようになります。

コア ダンプの管理（クラスタ管理者のみ）

ノードに何らかの障害が発生した場合、コア ダンプが発生し、システムによってコア ダンプ ファイルが作成されます。このファイルをテクニカル サポートが使用して問題を解決できる可能性があります。コア ダンプの属性は、設定または表示できます。また、コア ダンプ ファイルは保存、表示、分割、アップロード、または削除できます。

コア ダンプ ファイルは、次の方法で管理できます。

- コア ダンプの設定および構成設定の表示
- コア ダンプの基本情報、ステータス、および属性の表示
  コア ダンプ ファイルおよびレポートは、ノードの`/mroot/etc/crash/`ディレクトリに保存されます。`system node coredump`コマンドまたはWebブラウザを使用して、ディレクトリのコンテンツを表示できます。
- コア ダンプの内容の保存と、指定された場所またはテクニカル サポートへの保存済みファイルのアップロード
  Data ONTAPでは、テイクオーバー、アグリゲートの再配置、またはギブバック中にコア ダンプ ファイルの保存を開始することはできません。
- 必要がなくなったコア ダンプ ファイルの削除

コア ダンプ ファイルは非常に大きくなり、アップロードに時間がかかる場合があります。コア ダンプ ファイルは、それ以上圧縮しないでください。ただし、次の方法でファイルを分割できます。

- コア ダンプ ファイルの自動分割の設定
- コア ダンプ ファイルの手動での分割およびコア セグメントの管理

関連タスク

Webブラウザを使用したノードのログファイル、コア ダンプ ファイル、およびMIBファイルへのアクセス（42ページ）

コア ダンプ ファイルの分割方法

コア ダンプ ファイルは肥大化することがあり、テクニカル サポートへのアップロードが必要になったとき、時間がかかる結果になります。コア ダンプ ファイルを分割すると、ファイル全体ではなく、必要な部分のみをアップロードできます。

保存したコア ダンプ ファイルは、最大で3つのコア セグメントに分割できます。

対象のコア セグメント	システム情報が含まれているメモリ
プライマリ コア セグメント	Data ONTAPおよびシステムシェル
キャッシング モジュール コア セグメント	Flash Cacheのモジュール ファミリー
NVRAMコア セグメント	NVRAM

コア ダンプ ファイルを分割すると、必要なファイルの部分をアップロードできます。たとえば、コア ダンプ分析のためにコア ダンプ ファイル全体をテクニカル サポートにアップロードする代わりに、ファイルのプライマリ コア セグメントのみをアップロードし、必要な場合はあとでキャッシング モジュール コア セグメントまたはNVRAMコア セグメントをアップロードします。

`system node coredump segment config`コマンドを使用すると、コア ダンプ ファイルの自動分割を次のように設定できます。

- コア ダンプ ファイルを保存後に自動的に分割するかどうかを指定する
  自動分割のデフォルト設定はシステムによって異なります。
- 分割後に元のコア ダンプ ファイルを自動的に削除するかどうかを指定する
  デフォルトでは、元のコア ダンプ ファイルの自動削除は無効になっています。
- コア ダンプ ファイルの自動分割の現在の設定を表示する

`system node coredump segment`コマンドを使用すると、コア ダンプ ファイルの分割を次のように手動で管理できます。

- コア分割ジョブを手動でスケジュールしてノード上の指定されたコア ダンプ ファイルをコア セグメントに分割し、コア分割の完了後に元のコア ダンプ ファイルを削除するかどうかを指定する
- コア セグメントについての情報を表示する
- 指定したコア セグメントまたはすべてのセグメントをノードから削除する
- コア分割ジョブのステータスを表示する
- ジョブIDで指定したコア分割ジョブをキャンセルする

コア ダンプの管理用コマンド

コア ダンプの設定を管理するには`system node coredump config`コマンド、コア ダンプ ファイルを管理するには`system node coredump`コマンド、アプリケーション コア レポートを管理するには`system node coredump reports`コマンドをそれぞれ使用します。

状況	使用するコマンド
コア ダンプを設定する	*system node coredump config modify*
コア ダンプの構成設定を表示する	*system node coredump config show*
コア ダンプに関する基本情報を表示する	*system node coredump show*
ノードをリブートする際にコア ダンプを手動でトリガーする	*system node reboot*に`-dump`と`-skip-lif-migration`パラメータを両方指定
ノードをシャットダウンする際にコア ダンプを手動でトリガーする	*system node halt*に`-dump`と`-skip-lif-migration`パラメータの両方を指定
指定したコア ダンプを保存する	*system node coredump save*
指定したノード上で保存されていないすべてのコア ダンプを保存する	*system node coredump save-all*
AutoSupportメッセージを生成し、指定したコア ダンプ ファイルと一緒に送信する	*system node autosupport invoke-core-upload* **注:** オプションのパラメータ`-uri`に、AutoSupportメッセージのAutoSupportの代替の送信先を指定できます。
コア ダンプに関するステータス情報を表示する	*system node coredump status*
指定したコア ダンプを削除する	*system node coredump delete*
ノード上で保存されていないすべてのコア ダンプ、または保存されているすべてのコア ファイルを削除する	*system node coredump delete-all*

状況	使用するコマンド
アプリケーション コア ダンプ レポートを表示する	*system node coredump reports show*
アプリケーション コア ダンプ レポートを削除する	*system node coredump reports delete*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

コア分割の管理用コマンド

コア ダンプ ファイルの自動分割（セグメント化）を管理するには、`system node coredump segment config`コマンドを使用します。コア セグメントを管理するには、`system node coredump segment`コマンドを使用します。

状況	使用するコマンド
ノードのコア ダンプ ファイルの自動分割を設定する • コア ダンプ ファイルの保存後に自動的に分割するかどうか • 分割後に元のコア ダンプ ファイルを自動的に削除するかどうか	*system node coredump segment config modify*
自動コア分割の現在の設定を表示する	*system node coredump segment config show*
ノード上の指定したコア ダンプ ファイルをコア セグメントに分割する処理を手動で開始し、コア分割の完了後に元のコア ダンプ ファイルを削除するかどうかを指定する	*system node coredump segment start*
ノード上のコア セグメントに関する情報を表示する • コア セグメントの名前 • コア内のコア セグメントの総数 • パニックが発生しコア ダンプ ファイルが生成された時間	*system node coredump segment show*
ノード上の指定したコア セグメントを削除する	*system node coredump segment delete*
ノードからすべてのコア セグメントを削除する	*system node coredump segment delete-all*

状況	使用するコマンド
コア分割ジョブのステータスを表示する • ジョブID • 分割されているコア ダンプ ファイルの名前 • ジョブ ステータス • 完了した割合	`system node coredump segment status`
ジョブIDで指定したコア分割ジョブをキャンセルする	`system node coredump segment stop`

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

ストレージ システムの監視

ストレージ システムを監視するには、イベント メッセージ、AutoSupport機能、ダッシュボード、統計、環境コンポーネント センサーを使用します。

クラスタ管理者は、すべてのシステム監視タスクを実行できます。Storage Virtual Machine（SVM）管理者は、次の監視タスクのみを実行できます。

- SVM健全性ダッシュボードの表示（`dashboard health vserver show`コマンドを使用）
  `dashboard health vserver show`コマンドは古いコマンドで推奨されていませんが、システムを監視するために引き続き使用できます。
- パフォーマンス データの管理および取得（`statistics`コマンドを使用）

イベント メッセージの管理

Event Management System（EMS;イベント管理システム）は、クラスタに発生したイベントについて情報を収集して表示します。イベントの送信先、イベント ルート、メール履歴レコード、SNMPトラップの履歴レコードを管理できます。また、イベント通知およびイベント ロギングを設定することもできます。

重大度の高いイベントに関するイベント メッセージは、システム コンソールに表示され、クラスタのイベント ログに書き込まれます。イベント メッセージは次の要素で構成されます。

- メッセージ名
- 重大度レベル
  緊急度の高い順に次のような値があります。
  - EMERGENCY（クラスタが使用できない）
  - ALERT（システム障害を防ぐための処置をすぐにとる必要がある）
  - CRITICAL
  - ERROR
  - WARNING
  - NOTICE（正常であるが注意を要する状況が発生した）
  - INFORMATIONAL
  - DEBUG
- 説明
- 修正措置（該当する場合）

イベントについて次のような機能を管理できます。

- イベントの送信先
  イベントを送信する送信先を指定します。送信先としては、Eメール アドレス、SNMPトラップ ホスト、syslogサーバがあります。
- イベント ルート
  通知が生成されるイベントを指定します。イベント ルートは、イベントとその送信先とのマッピングです。イベント ルートには、重大度、送信先、通知しきい値に関する情報が含まれています。

- イベント通知およびイベント ロギング
  Eメールの「送信元」アドレス、「宛先」アドレス、およびイベントをコンソールに表示するかどうかを指定します。
- メール履歴レコード
  Eメールで送信されたイベント通知のリストです。
- SNMPトラップ履歴レコード
  SNMPトラップ ホストに送信されたイベント通知のリストです。SNMPトラップについては、*『clustered Data ONTAP ネットワーク管理ガイド』*を参照してください。

イベント管理システムのセットアップ

EMSを設定して、受信するイベント メッセージの数を減らしたり、特定のイベント重大度のイベント送信先とイベント ルートを設定したりすることができます。

手順

1. メール サーバ設定を表示します。

   `event config show`

   例

   ```
   cluster1::> event config show

     Mail From: admin@localhost
   Mail Server: localhost
   ```

2. オプション: 必要に応じて、要件に合わせてメール サーバ設定を変更します。

   `event config modify -mailserver` *`name`* `-mailfrom` *`email address`*

   例

   次の例に、メール サーバを変更し、結果を表示する方法を示します。

   ```
   cluster1::> event config modify -mailserver mailhost.example.com
   -mailfrom admin@node1-example.com

   cluster1::> event config show

     Mail From: admin@node1-example.com
   Mail Server: mailhost.example.com
   ```

3. `event destination create`コマンドを使用して、イベントの送信先を作成します。

   イベントはEメール アドレス、SNMPトラップ ホスト、およびsyslogサーバに送信できます。

   例

   次のコマンドでは、Eメールの送信先を作成し、指定したEメール アドレスに重要なすべてのイベントを送信し、結果を表示します。

   ```
   cluster1::> event destination create -name test_dest -mail me@example.com

   cluster1::> event destination show
                                                          Hide
   Name      Mail Dest.      SNMP Dest.  Syslog Dest.  Params
   --------  --------------- ----------- ------------- ------
   allevents -               -           -             false
   asup      -               -           -             false
   ```

```
criticals -                -           -             false
pager     -                -           -             false
test_dest me@example.com   -           -             false
traphost  -                -           -             false
```

4. event route add-destinationsコマンドを使用して、受信するメッセージの重大度レベルを定義します。

   クリティカル以上のイベントには、イベント ルートを設定する必要があります。

   例

   次の例では、すべてのクリティカル、アラート、および緊急のイベントをtest_destイベント送信先に送信します。

```
cluster1::> event route add-destinations -messagename * -severity <=CRITICAL -
destinations test_dest
```

5. クリティカル以上のすべてのイベントを表示するには、次のコマンドを入力します。

   event route show -severity -CRITICAL

   例

   次の例に、クリティカル以上の重大度レベルを持つイベントを示します。

```
cluster1::> event route show -severity <=CRITICAL
                                                    Freq        Time
Message                 Severity    Destinations    Threshd     Threshd
-----------------------------------------------------------------------
adminapi.time.zoneDiff  ALERT       test_dest       0           3600
api.engine.killed       CRITICAL    test_dest       0           0
app.log.alert           ALERT       test_dest       0           0
app.log.crit            CRITICAL    test_dest       0           0
app.log.emerg           EMERGENCY   test_dest       0           0
```

6. 受信するイベント メッセージの数が多すぎる場合は、-timethresholdパラメータを使用して、送信先に送信するイベントの頻度を指定します。

   例

   たとえば、次のイベントは1時間に1回しか送信先に送信されません。

```
cluster1::> event route modify -messagename adminapi.time.zoneDiff
-timethreshold 3600
```

タスクの結果

上記の手順を完了すると、event routeに指定した送信先にクリティカル以上のすべてのイベントが自動的に送信されます。

イベントの管理用コマンド

クラスタ上のイベントを管理するには、eventファミリーのData ONTAPコマンドを使用します。

次の表に、イベントの管理用コマンドを示します。

状況	使用するコマンド
イベントの送信先を作成する	*event destination create*
イベントの送信先に関する情報を表示する	*event destination show*
イベントの送信先を変更する	*event destination modify*

状況	使用するコマンド
イベントの送信先を削除する	`event destination delete`
イベント ルートまたはイベント通知の間隔を変更する	`event route modify`
1つ以上の既存の送信先をイベント ルートに追加する	`event route add-destinations`
イベント ルートの重大度レベルを指定する	`event route add-destinations` で、`-messagename`パラメータを指定
イベント ルートから1つ以上の送信先を削除する	`event route remove-destinations`
イベント ルートに関する情報を表示する	`event route show`
イベント ログを表示する	`event log show`
イベントの修正措置を表示する	`event log show`で、`-instance`パラメータを指定
イベント通知およびイベント ロギングの設定を表示する	`event config show`
イベント通知およびイベント ロギングの設定を変更する	`event config modify`
イベントの発生に関する情報を表示する	`event status show`
メール履歴レコードを表示する	`event mailhistory show`
メール履歴レコードを削除する	`event mailhistory delete`
SNMPトラップに送信されたイベント通知のリストを表示する	`event snmphistory show`
SNMPトラップ履歴レコードを削除する	`event snmphistory delete`

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

AutoSupportの管理

AutoSupportは、システム ヘルスをプロアクティブに監視し、NetApp テクニカル サポート、社内のサポート部門、およびサポート パートナーにメッセージを自動的に送信します。テクニカル サポートへのAutoSupportメッセージの送信はデフォルトで有効になりますが、メッセージを社内のサポート部門に送信する場合は、適切なオプションを設定し、有効なメール ホストを指定する必要があります。

クラスタ管理者のみがAutoSupport管理を実行できます。Storage Virtual Machine（SVM）管理者にはAutoSupportへのアクセス権はありません。

AutoSupportは、ストレージ システムの初回設定時に、デフォルトで有効になります。AutoSupportは、AutoSupportが有効化されてから24時間後にテクニカル サポートへのメッセージ送信を開始します。この間隔を24時間よりも短くするには、システムをアップグレードまたはリバートするか、AutoSupport設定を変更するか、システムの時間を24時間以外の時間に変更します。

注: AutoSupportはいつでも無効にできますが、常に有効にしておく必要があります。AutoSupportを有効な状態にすると、ストレージ システムに問題が発生したときに、迅速に原因

を判断し解決できます。デフォルトでは、AutoSupportを無効にした場合でも、AutoSupportの情報が収集されてローカルに格納されます。

AutoSupportの詳細については、ネットアップ サポート サイトを参照してください。

関連情報

ネットアップ サポート サイト：mysupport.netapp.com

AutoSupportメッセージが送信されるタイミングおよび場所

AutoSupportは、メッセージのタイプに応じた宛先にメッセージを送信します。AutoSupportがメッセージを送信するタイミングと場所を知ると、Eメールで受信するメッセージまたはMy AutoSupport Webサイトに表示されるメッセージを把握するのに役立ちます。

特に指定がないかぎり、次の表に示す設定は、`system node autosupport modify`コマンドのパラメータです。

イベントトリガー型メッセージ

修正措置を必要とするシステムでイベントが発生した場合には、AutoSupportからイベントトリガー型メッセージが自動的に送信されます。

メッセージが送信されるタイミング	メッセージの送信先
AutoSupportがEMSのトリガー イベントに応答するとき	`-to`と`-noteto`で指定されているアドレス（送信されるのはサービスに影響がある重要なイベントのみ） `-partner-address`で指定されているアドレス テクニカル サポート（`-support`を**`enable`**に設定した場合）

スケジュールされたメッセージ

AutoSupportは、定期的にいくつかのメッセージを自動的に送信します。

メッセージが送信されるタイミング	メッセージの送信先
毎日（デフォルトでは、午前0時から 午前1時までの間に ログ メッセージとして送信される）	`-partner-address`で指定されているアドレス テクニカル サポート（`-support`を**`enable`**に設定した場合）
毎日（デフォルトでは、午前0時から 午前1時までの間に パフォーマンス メッセージとして送信される）（`-perf`パラメータを**`true`**に設定した場合）	`-partner-address`で指定されているアドレス テクニカル サポート（`-support`を**`enable`**に設定した場合）
毎週（デフォルトでは、日曜日の午前0時から午前1時までの間に送信される）	`-partner-address`で指定されているアドレス テクニカル サポート（`-support`を**`enable`**に設定した場合）

手動でトリガーされるメッセージ

AutoSupportメッセージは、手動で送信または再送信できます。

メッセージが送信されるタイミング	メッセージの送信先
system node autosupport invokeコマンドを使用して、手動でメッセージを送信したとき	system node autosupport invokeコマンドで-uriパラメータを使用してURIを指定すると、そのURIにメッセージが送信されます。-uriを省略すると、-toおよび-partner-addressで指定したアドレスにメッセージが送信されます。-supportを**enable**に設定した場合は、テクニカル サポートにもメッセージが送信されます。
system node autosupport invoke-core-uploadコマンドを使用して、手動でメッセージを送信したとき	system node autosupport invoke-core-uploadコマンドで-uriパラメータを使用してURIを指定すると、そのURIにメッセージが送信され、コア ダンプ ファイルがアップロードされます。 system node autosupport invoke-core-uploadコマンドで-uriを省略すると、テクニカル サポートにメッセージが送信され、テクニカル サポート サイトにコア ダンプ ファイルがアップロードされます。 どちらのシナリオでも、-supportを**enable**に設定し、-transportを**https**または**http**に設定する必要があります。 コア ダンプ ファイルは大容量のため、メッセージは-toパラメータと-partner-addressesパラメータで指定したアドレスには送信されません。
system node autosupport invoke-performance-archiveコマンドを使用して、手動でメッセージを送信したとき	system node autosupport invoke-performance-archiveコマンドで-uriパラメータを使用してURIを指定すると、そのURIにメッセージが送信され、パフォーマンス アーカイブ ファイルがアップロードされます。 system node autosupport invoke-performance-archiveコマンドで-uriを省略すると、テクニカル サポートにメッセージが送信され、テクニカル サポート サイトにパフォーマンス アーカイブ ファイルがアップロードされます。 どちらのシナリオでも、-supportを**enable**に設定し、-transportを**https**または**http**に設定する必要があります。 パフォーマンス アーカイブ ファイルは大容量のため、メッセージは-toパラメータと-partner-addressesパラメータで指定したアドレスには送信されません。
system node autosupport history retransmitコマンドを使用して、手動で過去のメッセージを再送信したとき	system node autosupport history retransmitコマンドの-uriパラメータで指定したURIだけに送信されます。

テクニカル サポートによってトリガーされるメッセージ

テクニカル サポートは、AutoSupport OnDemand機能を使用してAutoSupportからのメッセージを要求できます。

メッセージが送信されるタイミング	メッセージの送信先
新しいAutoSupportメッセージを生成するという送信指示をAutoSupportが受け取ったとき	`-partner-address`で指定されているアドレス テクニカル サポート（`-support`を**`enable`**に設定し、`-transport`を**`https`**に設定した場合）
過去のAutoSupportメッセージを再送信するという送信指示をAutoSupportが受け取ったとき	テクニカル サポート（`-support`を**`enable`**に設定し、`-transport`を**`https`**に設定した場合）
コア ダンプ ファイルまたはパフォーマンス アーカイブ ファイルをアップロードする新しいAutoSupportメッセージを生成するという送信指示をAutoSupportが受け取ったとき	テクニカル サポート（`-support`を**`enable`**に設定し、`-transport`を**`https`**に設定した場合）。テクニカル サポート サイトにコア ダンプ ファイルまたはパフォーマンス アーカイブ ファイルがアップロードされます。

関連コンセプト

AutoSupport OnDemandがテクニカル サポートから送信指示を取得する仕組み（206ページ）

AutoSupportによるイベントトリガー型メッセージの作成および送信

イベントトリガー型AutoSupportメッセージは、EMSがトリガー イベントを処理したときに作成されます。イベントトリガー型AutoSupportメッセージは、対応処置が必要な問題を受信者に通知します。メッセージには、問題に関連する情報のみが記載されています。このメッセージの内容と受信者はカスタマイズできます。

AutoSupportは、次のプロセスを使用してイベントトリガー型AutoSupportメッセージを作成し、送信します。

1. EMSがトリガー イベントを処理するときにAutoSupportに要求を送信します。
   トリガー イベントは、AutoSupportの送信先と`callhome`という プレフィックスで始まる名前が指定されたEMSイベントです。

2. AutoSupportによってイベントトリガー型AutoSupportメッセージが作成されます。
   AutoSupportは、トリガーに関連付けられたサブシステムから基本的な情報とトラブルシューティング情報を収集し、トリガー イベントに関連する情報のみが含まれたメッセージを作成します。
   一連のデフォルトのサブシステムが各トリガーに関連付けられています。ただし、`system node autosupport trigger modify`コマンドを使用して、トリガーに関連付ける追加サブシステムを選択できます。

3. AutoSupportは、`system node autosupport modify`コマンドと`-to`、`-noteto`、`-partner-address`、`-support`パラメータによって定義された受信者にイベントトリガー型AutoSupportメッセージを送信します。
   `system node autosupport trigger modify`コマンドと`-to`および`-noteto`パラメータを使用して、特定のトリガーについてのAutoSupportメッセージの配信を有効または無効にできます。

特定イベントについて送信されるデータの例

`storage shelf PSU failed` EMSイベントは、必須、ログ ファイル、ストレージ、RAID、HA、プラットフォーム、およびネットワークの各サブシステムからの基本データと、必須、ログ ファイル、およびストレージの各サブシステムからのトラブルシューティング データを含んだメッセージをトリガーします。

今後のstorage shelf PSU failedイベントへの応答で送信するAutoSupportメッセージにNFSについてのデータを含めることを決定します。次のコマンドを入力し、callhome.shlf.ps.faultイベントのNFSについてのトラブルシューティング レベルのデータを有効にします。

```
cluster1::> system node autosupport trigger modify -node node1 -
autosupport-message shlf.ps.fault -troubleshooting-additional nfs
```

callhome. プレフィックスは、system node autosupport triggerコマンドを使用した場合、または、CLIでAutoSupportおよびEMSイベントから参照された場合、callhome.shlf.ps.faultイベントから省略されます。

AutoSupportメッセージとそのコンテンツのタイプ

AutoSupportメッセージには、サポートされているサブシステムに関するステータス情報が含まれています。AutoSupportメッセージの内容を把握しておくと、Eメールで受信したメッセージまたはMy AutoSupport Webサイトに表示されたメッセージを解釈したり、応答したりするときに役立ちます。

メッセージの種類	メッセージに含まれているデータの種類
イベントトリガー型	イベントが発生した特定のサブシステムに関するコンテキスト依存データが含まれるファイル
日次	ログ ファイル
パフォーマンス	過去24時間以内にサンプリングされたパフォーマンス データ
週次	設定データおよびステータス データ
system node autosupport invokeコマンドによってトリガーされる	-typeパラメータに指定した値によって異なります。 • **test**:いくつかの基本データが記載された、ユーザ トリガー型メッセージが送信されます。 -toオプションを使用すると、テクニカル サポートからの自動応答メールが指定したEメール アドレス宛てに送信されるため、AutoSupportメッセージが受信されていることを確認できます。 • **performance**:パフォーマンス データが送信されます。 • **all**:各サブシステムのトラブルシューティング データを含む、週次メッセージと同様の一連のデータを記載したユーザ トリガー型メッセージが送信されます。 一般に、テクニカル サポートからはこのメッセージが要求されます。
system node autosupport invoke-core-uploadコマンドによってトリガーされる	ノードのコア ダンプ ファイル
system node autosupport invoke-performance-archiveコマンドによってトリガーされる	指定された期間のパフォーマンス アーカイブ ファイル

メッセージの種類	メッセージに含まれているデータの種類
AutoSupport OnDemandによってトリガーされる	AutoSupport OnDemandでは、新しいメッセージまたは過去のメッセージを要求できます。 • 新しいメッセージは、AutoSupportによるデータ収集の種類によって、`test`、`all`、または`performance`のいずれかになります。 • 過去のメッセージは、再送信されるメッセージの種類によって異なります。 Autosupport OnDemandでは、NetApp サポート サイトに次のファイルをアップロードする新しいメッセージを要求できます。 • コア ダンプ • パフォーマンス アーカイブ

AutoSupportサブシステムとは

各サブシステムは、AutoSupportがメッセージに使用する基本情報およびトラブルシューティング情報を提供します。各サブシステムはトリガー イベントとも関連付けられており、AutoSupportはトリガー イベントに関連する情報のみをサブシステムから収集できます。

AutoSupportは状況に応じたコンテンツを収集します。サブシステムおよびトリガー イベントについての情報を表示するには、`system node autosupport trigger show`コマンドを使用します。

AutoSupportのサイズ割当量と時間割当量

AutoSupportは、サブシステムごとにまとめられた情報を収集し、各サブシステムのコンテンツにサイズ割当量と時間割当量を適用します。AutoSupportの割当量により、ストレージ システムの拡張に合わせてAutoSupportのペイロードが制御され、拡張性の高いAutoSupportデータの配信が可能になります。

サブシステムのコンテンツがサイズ割当量または時間割当量を超えた場合、AutoSupportは情報の収集を停止し、AutoSupportのコンテンツを切り捨てます。コンテンツを切り捨てるのが容易ではない場合（バイナリ ファイルなど）、AutoSupportはそのコンテンツを除外します。

デフォルトのサイズ割当量と時間割当量の変更は、テクニカル サポートから指示があった場合にのみ行うようにしてください。AutoSupportのサイズ割当量と時間割当量のCLIはdiagnostic権限のコマンド セットです。

サブシステム	サイズ割当量（バイト）	時間割当量（秒）
asup_ems	2097152	60
av	2097152	60
cifs	2097152	60
cluster_peer	2097152	60
cps	2097152	60
crs	2097152	60
dedupe	10485760	120
fpolicy	2097152	60
ha	2097152	60
hm	2097152	60

サブシステム	サイズ割当量（バイト）	時間割当量（秒）
kcs	2097152	60
kernel	2097152	60
log_files	5242880	120
mandatory	無制限	無制限
memevt	2097152	60
metrocluster	8388608	300
mhost	3670016	120
mot	2097152	60
ndmp	2097152	60
ndu	2097152	60
networking	4194304	60
nfs	2097152	60
nht	2097152	60
nwd	2097152	60
performance	20971520	300
performance_asup	52428800	300
platform	2097152	60
raid	2097152	60
repository	2097152	60
san	2097152	120
san_fcp	2097152	60
san_ffdc	367001600	120
secd	2097152	60
snapmirror	2097152	60
splog_before_spreboot	512000	30
splog_downcontroller	512000	30
splog_latest	512000	30
splog_rnode	2097152	60
splog_rnode_down	2097152	60
splog_rnode_latest	2097152	60
storage	10485760	180
vscan	2097152	60
vserver_dr	2097152	60
wafl	23068672	300

イベントトリガー型AutoSupportメッセージで送信されるファイル

イベントトリガー型AutoSupportメッセージには、AutoSupportがメッセージを作成する原因となったイベントに関連付けられたサブシステムからの基本情報とトラブルシューティング情報のみが含まれています。特定のデータは、NetApp サポートおよびサポート パートナーによる問題のトラブルシューティングに役立ちます。

AutoSupportでは、イベントトリガー型AutoSupportメッセージの内容の制御に次の基準を使用します。

- 含まれているサブシステム
  データは、ログ ファイルなどの共通サブシステムや、RAIDなどの特定のサブシステムといったサブシステムにグループ化されます。各イベントは、特定のサブシステムからのデータのみを含むメッセージをトリガーします。
- 含まれている各サブシステムの詳細レベル
  含まれている各サブシステムのデータは、基本レベルかトラブルシューティング レベルで提供されます。

考えられるすべてのイベントを表示し、各イベントについてのメッセージにどのサブシステムが含まれているかを特定するには、`-instance`パラメータを指定して`system node autosupport trigger show`コマンドを実行します。

各イベントにデフォルトで含まれるサブシステムのほかに、基本レベルまたはトラブルシューティング レベルのサブシステムを追加するには、`system node autosupport trigger modify`コマンドを使用します。

AutoSupportメッセージで送信されるログ ファイル

AutoSupportメッセージには、ネットアップのテクニカル サポート担当者が最近のシステム アクティビティを確認できる、複数の主要ログ ファイルを含めることができます。

ログ ファイル サブシステムが有効になっている場合は、すべてのタイプのAutoSupportメッセージに次のログ ファイルが含まれる可能性があります。

ログ ファイル	ファイルから含められたデータの量
• `/mroot/etc/log/mlog/`ディレクトリからのログ ファイル • MESSAGESログ ファイル	最後のAutoSupportメッセージ以降にログに追加された、指定最大数までの新しい行のみ これにより、AutoSupportメッセージに、一意の、関連するデータが重複データを除いて含められます。 （パートナーからのログファイルは例外です。パートナーについては、最大許容データが含められます。）
• `/mroot/etc/log/shelflog/`ディレクトリからのログ ファイル • `/mroot/etc/log/acp/`ディレクトリからのログ ファイル • Event Management System（EMS）ログ データ	指定された最大数までの最新データの行

AutoSupportメッセージの内容は、Data ONTAPのリリースによって変わる場合があります。

週単位のAutoSupportメッセージで送信されるファイル

週単位のAutoSupportメッセージには、追加の設定およびステータスが含まれ、時間の経過に伴うシステム内の変更の追跡に役立ちます。

週単位のAutoSupportメッセージでは、次の情報が送信されます。

- 各サブシステムについての基本情報
- 選択された`/mroot/etc`ディレクトリ ファイルの内容
- ログ ファイル
- システム情報を表示するコマンドの出力
- レプリケートされたデータベース（RDB）情報、サービス統計情報などの追加情報

AutoSupport OnDemandがテクニカル サポートから送信指示を取得する仕組み

AutoSupport OnDemandは、定期的にテクニカル サポートとの通信を行って、AutoSupportメッセージの処理（送信、再送信、または拒否）および大容量ファイルのNetApp サポート サイトへのアップロードに関する送信指示を受け取ります。AutoSupport OnDemandを使用すると、週次のAutoSupportジョブの実行を待たずにAutoSupportメッセージをオンデマンドで送信できます。

AutoSupport OnDemandは次のコンポーネントで構成されています。

- 各ノードで稼働するAutoSupport OnDemandクライアント
- テクニカル サポートで稼働するAutoSupport OnDemandサービス

AutoSupport OnDemandクライアントは、AutoSupport OnDemandサービスを定期的にポーリングし、テクニカル サポートから送信指示を取得します。たとえば、テクニカル サポートは、AutoSupport OnDemandサービスを使用して、新しいAutoSupportメッセージを生成するよう要求できます。AutoSupport OnDemandクライアントはAutoSupport OnDemandサービスをポーリングして、送信指示を取得し、要求に応じて新しいAutoSupportメッセージをオンデマンドで送信します。

AutoSupport OnDemandは、デフォルトで有効になっています。ただし、AutoSupport OnDemandがテクニカル サポートとの通信を継続するかどうかは、いくつかのAutoSupport設定によって決まります。次の要件を満たしている場合、AutoSupport OnDemandはテクニカル サポートと自動的に通信を行います。

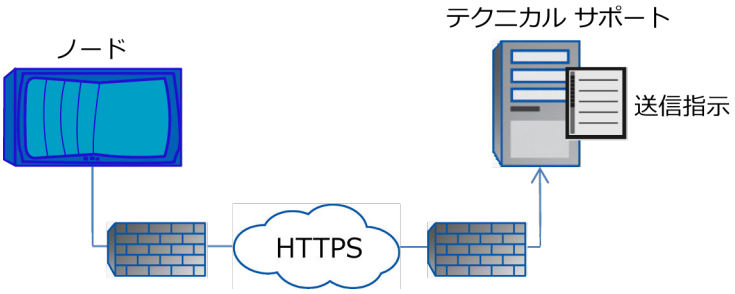
- AutoSupportが有効になっている。
- テクニカル サポートにメッセージを送信するようにAutoSupportが設定されている。
- HTTPS転送プロトコルを使用するようにAutoSupportが設定されている。

AutoSupport OnDemandクライアントは、AutoSupportメッセージの送信先と同じ場所のテクニカル サポートにHTTPS要求を送信します。AutoSupport OnDemandクライアントは、着信接続は受け入れません。

> **注:** AutoSupport OnDemandは、「autosupport」ユーザ アカウントを使用してテクニカル サポートと通信します。このアカウントを削除することはできません。

AutoSupport OnDemandを無効にして、AutoSupportは有効な状態のまま、HTTPS転送プロトコルを使用してテクニカル サポートにメッセージを送信するように設定する場合は、テクニカル サポートにお問い合わせください。

AutoSupport OnDemandがテクニカル サポートにHTTPS要求を送って送信指示を取得する処理を図式化すると次のようになります。



送信指示には、AutoSupportが行う処理として、次のような内容を含むことができます。

- 新規のAutoSupportメッセージの生成
  テクニカル サポートからは、問題の優先度を選別できるように、新たなAutoSupportメッセージが要求されることがあります。
- コア ダンプ ファイルまたはパフォーマンス アーカイブ ファイルをNetApp サポート サイトにアップロードする新規のAutoSupportメッセージの生成
  問題の優先度を選別できるように、テクニカル サポートからコア ダンプ ファイルまたはパフォーマンス アーカイブ ファイルを要求されることがあります。
- 以前に生成したAutoSupportメッセージの再送信
  この要求は、あるメッセージが配信失敗などの理由で受信されなかった場合に、自動的に出されます。
- 特定のトリガー イベントに対するAutoSupportメッセージ送信の無効化
  テクニカル サポートは、使用されていないデータの送信を無効にすることがあります。

Eメールで送信したAutoSupportメッセージの構造

AutoSupportメッセージをEメールで送信すると、メッセージには標準的な件名、簡単な本文、およびデータが含まれた7zファイル形式の大きな添付ファイルが含められます。

注: プライベート データを非表示にするようにAutoSupportが設定されている場合は、ヘッダー、件名、本文、添付ファイル内のホスト名などの特定の情報が省略されるか、マスクされます。

件名

AutoSupportメカニズムによって送信されたメッセージの件名行には、その通知の理由を特定するテキスト文字列が含まれています。件名行の形式は次のとおりです。

HA GroupNotification from *System_Name*（*Message*） *Severity*

- *System_Name*はAutoSupportの設定に応じてホスト名かシステムIDです。

本文

AutoSupportメッセージの本文には次の情報が含まれます。

- メッセージの日付と時間
- メッセージを生成したノード上の Data ONTAPのバージョン
- メッセージを生成したノードの システムID、シリアル番号、およびホスト名
- AutoSupportシーケンス番号
- SNMPの担当者の名前と住所（指定されている場合）
- HAパートナー ノードのシステムIDおよびホスト名

添付ファイル

AutoSupportメッセージの重要な情報は、body.7zという7zファイルにまとめて圧縮されたファイルに含められ、メッセージに添付されます。

添付ファイルに含まれているファイルは、AutoSupportメッセージ タイプに固有です。

AutoSupportの重大度のタイプ

AutoSupportメッセージには、各メッセージの目的を示す重大度のタイプが設定されます。これにより、たとえば、すぐに対処する必要がある重大な問題を示すメッセージなのか、情報提供のみを目的としたメッセージなのかがわかります。

メッセージには次のいずれかの重大度が設定されます。

- Critical：クリティカルな状態
- Error：エラー状態
- Warning：警告状態
- Notice：通常の状態だが重要な状態
- Info：情報メッセージ
- Debug：デバッグレベルのメッセージ

社内のサポート部門がAutoSupportメッセージをEメールで受信する場合、重大度はEメール メッセージの件名に表示されます。

AutoSupportの使用要件

セキュリティを確保し、AutoSupportの最新機能をすべてサポートするには、HTTPSを使用してAutoSupportメッセージを配信する必要があります。AutoSupportではAutoSupportメッセージの配信用にHTTPとSMTPがサポートされていますが、HTTPSが推奨されます。

サポートされるプロトコル

これらのプロトコルはいずれも、名前が解決されるアドレス ファミリーに応じてIPv4またはIPv6で実行されます。

プロトコルとポート	説明
HTTPS（ポート443）	デフォルトのプロトコルです。できるだけこのプロトコルを使用することを推奨します。 このプロトコルでは、AutoSupport OnDemandと大容量ファイルのアップロードがサポートされます。 検証を無効にしていないかぎり、リモート サーバからの証明書がルート証明書に照らして検証されます。 配信にはHTTP PUT要求が使用されます。PUTでは、要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。要求の受信側のサーバでPUTがサポートされていない場合は、HTTP POST要求が使用されます。

プロトコルとポート	説明
HTTP（ポート80）	このプロトコルはSMTPよりも推奨されます。 このプロトコルでは、大容量ファイルのアップロードはサポートされますが、AutoSupport OnDemandはサポートされません。 配信にはHTTP PUT要求が使用されます。PUTでは、要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。要求の受信側のサーバでPUTがサポートされていない場合は、HTTP POST要求が使用されます。
SMTP（ポート25または別のポート）	このプロトコルを使用するのは、ネットワーク接続でHTTPSまたはHTTPを使用できない場合だけにしてください。 ポートのデフォルト値は25ですが、別のポートを使用するようにAutoSupportを設定できます。 SMTPを使用する場合は、次の制限事項に注意してください。 • AutoSupport OnDemandと大容量ファイルのアップロードはサポートされません。 • データは暗号化されません。 SMTPではデータがクリア テキストで送信されるため、AutoSupportメッセージ内のテキストの傍受や読み取りが容易になります。 • メッセージの長さや行の長さが制限されることがあります。

AutoSupportの設定で社内のサポート部門またはサポート パートナーのEメール アドレスを指定した場合、それらのメッセージは常にSMTPで送信されます。

たとえば、推奨されるプロトコルを使用してテクニカル サポートにメッセージを送信し、同時に社内のサポート部門にもメッセージを送信する場合は、それぞれHTTPSとSMTPを使用して転送されます。

AutoSupportでは、各プロトコルの最大ファイル サイズが制限されています。HTTPおよびHTTPS転送のデフォルト設定は10MBです。SMTP転送のデフォルト設定は5MBです。AutoSupportメッセージのサイズが設定した制限を超えた場合、メッセージの一部が最大サイズの範囲で配信されます。最大サイズは、AutoSupportの設定を変更することで編集できます。詳細については、`system node autosupport modify`のマニュアル ページを参照してください。

注: AutoSupportでは、コア ダンプ ファイルまたはパフォーマンス アーカイブ ファイルをアップロードするAutoSupportメッセージを生成してNetApp サポート サイトや指定のURIに送信する場合に、HTTPSプロトコルとHTTPプロトコルの最大ファイル サイズの上限が自動的にオーバーライドされます。自動的にオーバーライドされるのは、`system node autosupport invoke-core-upload`コマンドまたは`system node autosupport invoke-performance-archive`コマンドを使用してファイルをアップロードする場合のみです。

設定に関する要件

ネットワークの設定によっては、HTTPプロトコルまたはHTTPSプロトコルを使用するためにはプロキシURLの設定も必要になることがあります。HTTPまたはHTTPSを使用したテクニカル サポートへのAutoSupportメッセージの送信でプロキシを使用する場合は、そのプロキシのURLを指定する必要があります。プロキシでデフォルトのポート（3128）以外のポートが使用されている場合、プロキシのポートを指定できます。また、プロキシ認証のユーザ名とパスワードも指定できます。

SMTPを使用して社内のサポート部門やテクニカル サポートにAutoSupportメッセージを送信する場合は、外部のメール サーバを設定する必要があります。ストレージ システムはメール サーバとしては機能しないため、メール送信用に外部のメール サーバが別途必要になります。このメール サーバをSMTPポート（25）または別のポートを監視するホストにして、8ビットのMultipurpose Internet Mail Extensions（MIME）エンコーディングを送受信するように設定する必要があります。メ

ール サーバには、たとえば、SMTPサーバを実行するUNIXホスト（sendmailプログラムなど）や、Microsoft Exchangeサーバを実行するWindowsサーバなどを使用できます。メール ホストは1つでも複数でもかまいません。

AutoSupportの設定

テクニカル サポートまたは社内のサポート部門にAutoSupport情報を送信するかどうかおよびその方法を管理し、その設定が正しいことをテストできます。

タスク概要

AutoSupportを設定するクラスタ内の各ノードで、次の手順を実行する必要があります。

デフォルトでは、各ノードでAutoSupportが有効になっており、HTTPS転送プロトコルを使用してテクニカル サポートにメッセージを送信できます。

手順

1. `system node autosupport modify`コマンドの`-state`パラメータを**`enable`**に設定し、AutoSupportを有効にします。
2. テクニカル サポートにAutoSupportメッセージを送信する場合は、`system node autosupport modify`コマンドの`-support`パラメータを**`enable`**に設定します。

   AutoSupportでAutoSupport OnDemandを使用可能にする場合や、大容量ファイル（コア ダンプ ファイルやパフォーマンス アーカイブ ファイルなど）をテクニカル サポートまたは指定のURIにアップロードする場合は、このオプションを有効にする必要があります。
3. テクニカル サポートがAutoSupportメッセージを受信できるようになっている場合は、次のいずれかのオプションを選択して、メッセージに使用する転送プロトコルを指定します。

状況	**`system node autosupport modify`** コマンドで設定するパラメータ
デフォルトのHTTPSプロトコルを使用する	**a.** `-transport`を**`https`**に設定します。 **b.** プロキシを使用する場合は、`-proxy-url`をプロキシのURLに設定します。 この設定では、AutoSupport OnDemandとの通信および大容量ファイルのアップロードがサポートされます。
SMTPよりも推奨されるHTTPを使用する	**a.** `-transport`を**`http`**に設定します。 **b.** プロキシを使用する場合は、`-proxy-url`をプロキシのURLに設定します。 この設定では、大容量ファイルのアップロードがサポートされますが、AutoSupport OnDemandはサポートされません。
SMTPを使用する	`-transport`を**`smtp`**に設定します。 この設定では、AutoSupport OnDemandや大容量ファイルのアップロードはサポートされません。

4. 社内のサポート部門またはサポート パートナーにAutoSupportメッセージを送信するには、次の操作を実行します。
   a. 社内部門の受信者を特定するには、`system node autosupport modify`コマンドの次のパラメータを設定します。

設定するパラメータ	パラメータの値
-to	重要なAutoSupportメッセージを受け取る社内サポート部門の、カンマで区切った5つまでの個別Eメール アドレスまたは配信リスト
-noteto	重要なAutoSupportメッセージの携帯電話またはその他のモバイル デバイス用の短縮版を受け取る社内サポート部門の、カンマで区切った5つまでの個別Eメール アドレスまたは配信リスト
-partner-address	すべてのAutoSupportメッセージを受け取るサポートパートナー部門の、カンマで区切った5つまでの個別Eメール アドレスまたは配信リスト

b. アドレスが正しく設定されていることを確認するには、`system node autosupport destinations show`コマンドを使用します。

5. メッセージを社内のサポート部門に送信するか、テクニカル サポートへのメッセージにSMTP転送を選択する場合は、`system node autosupport modify`コマンドの次のパラメータを設定してSMTPを設定します。

- `-mail-hosts`を、1つまたはカンマで区切って複数のメール ホストに設定します。
  5つまでのメール ホストを設定できます。
  メール ホスト名のあとにコロンとポート番号を指定することによって、各メール ホストのポート値を設定できます。たとえば、`mymailhost.example.com:5678`のように設定します。5678はメール ホストのポートです。
- `-from`を、AutoSupportメッセージを送信するEメール アドレスに設定します。

6. DNSを設定します。

7. オプション: 次の設定を変更します。

実行する処理	**system node autosupport modify**コマンドで設定するパラメータ
メッセージ内の機密データの削除、マスキング、またはエンコーディングによってプライベート データを非表示にする	`-remove-private-data`を**true**に設定します。 **false**を**true**に変更すると、AutoSupportの履歴と関連するファイルがすべて削除されます。
定期的なAutoSupportメッセージでのパフォーマンス データの送信を停止する	`-perf`を**false**に設定します。

8. 設定全体を確認するには、`-node`パラメータを指定して`system node autosupport show`コマンドを使用します。

9. AutoSupportメッセージが送受信されていることをテストします。

a. `-type`パラメータが**test**の`system node autosupport invoke`コマンドを使用します。

例

```
cluster1::> system node autosupport invoke -type test -node node1
```

b. NetAppがAutoSupportメッセージを受信していることを確認します。

system node autosupport history -node local

最新のAutoSupportの送信メッセージのステータスは、適切なすべてのプロトコルの宛先で最終的には`sent-successful`に変わります。

c. オプション: AutoSupportメッセージが社内のサポート部門、またはサポート パートナーに送信されていることを確認するには、`system node autosupport modify`コマンドの`-to`、`-noteto`、または`-partner-address`パラメータに設定したEメール アドレスを確認します。

関連タスク

メッセージを受信しない場合のAutoSupportのトラブルシューティング（216ページ）

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference
clustered Data ONTAP 8.3 ネットワーク管理ガイド

コア ダンプ ファイルのアップロード

ノードのコア ダンプ ファイルを含むAutoSupportメッセージを生成して送信できます。デフォルトでは、AutoSupportメッセージはNetAppテクニカル サポートに送信され、コア ダンプ ファイルはNetAppサポート サイトにアップロードされます。メッセージの送信先とアップロード先には別の場所を指定できます。

開始する前に

- 次の設定を使用してAutoSupportをセットアップしておく必要があります。
  - AutoSupportがノードで有効になっている。
  - テクニカル サポートにメッセージを送信するようにAutoSupportが設定されている。
  - HTTPまたはHTTPS転送プロトコルを使用するようにAutoSupportが設定されている。
    大容量ファイル（コア ダンプ ファイルなど）を含むメッセージを送信する場合、SMTP転送プロトコルはサポートされません。

手順

1. `system node coredump show`コマンドを使用して、ノードのコア ダンプ ファイルを表示します。

   例

   次の例では、ローカル ノードのコア ダンプ ファイルが表示されます。

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
--------- ------------------------------------------- -----
-----------------
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. `system node autosupport invoke-core-upload`コマンドを使用して、AutoSupportメッセージを生成し、コア ダンプ ファイルをアップロードします。

   例

   次の例では、AutoSupportメッセージが生成され、デフォルトの場所（テクニカル サポート）に送信されます。コア ダンプ ファイルはデフォルトの場所（NetApp サポート サイト）にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

次の例では、AutoSupportメッセージが生成され、URIに指定した場所に送信されます。コア ダンプ ファイルはそのURIにアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -uri https//
files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

関連タスク

AutoSupportの設定（210ページ）

パフォーマンス アーカイブ ファイルのアップロード

パフォーマンス アーカイブを含むAutoSupportメッセージを生成して送信できます。デフォルトでは、AutoSupportメッセージはNetAppテクニカル サポートに送信され、パフォーマンス アーカイブはNetAppサポート サイトにアップロードされます。メッセージの送信先とアップロード先には別の場所を指定できます。

開始する前に

- 次の設定を使用してAutoSupportをセットアップしておく必要があります。
  - AutoSupportがノードで有効になっている。
  - テクニカル サポートにメッセージを送信するようにAutoSupportが設定されている。
  - HTTPまたはHTTPS転送プロトコルを使用するようにAutoSupportが設定されている。
    大容量ファイル（パフォーマンス アーカイブ ファイルなど）を含むメッセージを送信する場合、SMTP転送プロトコルはサポートされません。

タスク概要

アップロードするパフォーマンス アーカイブ データの開始日を指定する必要があります。ほとんどのストレージ システムでは、パフォーマンス アーカイブが2週間保存されるので、2週間前までの開始日を指定できます。たとえば、今日が1月15日の場合は、1月2日を開始日として指定できます。アップロードするパフォーマンス アーカイブの開始日をいつにすればよいか判断できない場合は、テクニカル サポートにお問い合わせください。

手順

1. `system node autosupport invoke-performance-archive`コマンドを使用して、AutoSupportメッセージを生成し、パフォーマンス アーカイブ ファイルをアップロードします。

   例

   次の例では、2015年1月12日から4時間分のパフォーマンス アーカイブ ファイルがAutoSupportメッセージに添付され、デフォルトの場所（NetApp サポート サイト）にアップロードされます。

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   次の例では、2015年1月12日から4時間分のパフォーマンス アーカイブ ファイルがAutoSupportメッセージに添付され、URIで指定した場所にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -uri https://
files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

関連タスク

AutoSupportの設定（210ページ）

AutoSupportメッセージの説明の取得

受信したAutoSupportメッセージの説明を取得するには、オンラインの「AutoSupport Message Matrices」ページを使用します。

手順

1. [AutoSupport Message Matrices]ページに移動します。*support.netapp.com/NOW/knowledge/docs/olio/autosupport/matrices/*
2. [AutoSupport Message Matrices]ページの[Select a Release]で、使用しているData ONTAPのバージョンを選択して、**[View Matrix]**をクリックします。

   [Syslog Translator]ページが表示され、すべてのAutoSupportメッセージの説明が、件名のアルファベット順に示されます。

AutoSupportの管理用コマンド

AutoSupportの設定を変更または表示し、過去のAutoSupportメッセージに関する情報を表示し、AutoSupportメッセージを送信、再送信、またはキャンセルするには、`system node autosupport`コマンドを使用します。

AutoSupportを設定する

状況	使用するコマンド
AutoSupportメッセージを送信するかどうかを制御する	`-state`パラメータを指定した`system node autosupport modify`
AutoSupportメッセージがテクニカル サポートに送信されるかどうかを制御する	`-support`パラメータを指定した`system node autosupport modify`
AutoSupportをセットアップするか、AutoSupportの設定を変更する	`system node autosupport modify`
個々のトリガー イベントについて、AutoSupportメッセージを社内のサポート部門に送信するかどうかを指定する。また、各トリガー イベントで送信されるメッセージに含める追加のサブシステム レポートを指定する	`system node autosupport trigger modify`

AutoSupportの設定に関する情報を表示する

状況	使用するコマンド
AutoSupportの設定を表示する	`-node`パラメータを指定した`system node autosupport show`
AutoSupportメッセージを受信するすべてのアドレスとURLの概要を表示する	`system node autosupport destinations show`

状況	使用するコマンド
個々のトリガー イベントについて社内のサポート部門に送信されるAutoSupportメッセージを表示する	`system node autosupport trigger show`

過去のAutoSupportメッセージに関する情報を表示する

状況	使用するコマンド
過去50件のうち、1つ以上のAutoSupportメッセージに関する情報を表示する	`system node autosupport history show`
テクニカル サポート サイトまたは指定のURIにコア ダンプ ファイルまたはパフォーマンス アーカイブ ファイルをアップロードするために生成された最新のAutoSupportメッセージに関する情報を表示する	`system node autosupport history show-upload-details`
AutoSupportメッセージ内の情報を表示する。メッセージ用に収集された各ファイルの名前とサイズのほか、エラーがある場合はその情報も含まれる	`system node autosupport manifest show`

AutoSupportメッセージを送信、再送信、またはキャンセルする

状況	使用するコマンド
ローカルに保存されていて、そのAutoSupportシーケンス番号で特定されるAutoSupportメッセージを再転送する **注:** AutoSupportメッセージを再転送し、サポート部門がすでにそのメッセージを受信している場合、サポート システムは重複するケースを作成しません。一方、サポート部門がそのメッセージを受信しなかった場合には、AutoSupportシステムはメッセージを分析し、必要に応じてケースを作成します。	`system node autosupport history retransmit`
テスト目的などでAutoSupportメッセージを生成し送信する	`system node autosupport invoke` **注:** AutoSupportが無効になっている場合でも、`-force`パラメータを使用してメッセージを送信します。設定されている宛先ではなく、指定した宛先にメッセージを送信する場合は、`-uri`パラメータを使用します。
AutoSupportメッセージをキャンセルする	`system node autosupport history cancel`

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

AutoSupportマニフェストに含まれる情報

AutoSupportマニフェストには、イベントトリガー型の各AutoSupportメッセージについて収集されるファイルの詳細が表示されます。AutoSupportが必要とするファイルを収集できない場合には、AutoSupportマニフェストに収集エラーに関する情報も表示されます。

AutoSupportマニフェストには次の情報が含まれています。

- AutoSupportメッセージのシーケンス番号
- AutoSupportメッセージに含まれるファイル
- 各ファイルのサイズ（バイト数）
- AutoSupportマニフェストによる収集のステータス
- AutoSupportが1つ以上のファイルの収集に失敗した場合のエラーの説明

AutoSupportマニフェストを表示するには、`system node autosupport manifest show`コマンドを使用します。

AutoSupportマニフェストは、すべてのAutoSupportメッセージにXML形式で含まれています。したがって、表示するためには一般的なXMLビューアを使用するか、AutoSupportポータルを使用する必要があります。

My AutoSupportとは

My AutoSupportはAutoSupportと連携して機能するWebベースのアプリケーションであり、ストレージ インフラのモデル化や最適化に使用するデータを簡単に分析するための情報を提供します。

My AutoSupportは、ネットアップ サポート サイト（*mysupport.netapp.com*）でホストされているWebベースのアプリケーションであり、ブラウザを使用してアクセスできます。システムからにデータを返送するためには、そのシステムでAutoSupportを有効にし、設定しておく必要があります。My AutoSupportには、*http://support.netapp.com/NOW/asuphome/*からアクセスできます。

My AutoSupportでは、以下の操作を実行できるダッシュボードが提供されます。

- レポートの生成と、レポートのPDFまたはCSVファイルでのエクスポート
- 設定、パフォーマンス、システム ヘルス、インストールされているソフトウェア、ストレージ効率などに関する情報の表示
- システムおよびAutoSupportのツールへのアクセス

AutoSupportのトラブルシューティング

AutoSupportのメッセージを受信できない場合は、さまざまな設定を確認して問題を解決できます。

メッセージを受信しない場合のAutoSupportのトラブルシューティング

システムがAutoSupportメッセージを送信しない場合には、それがAutoSupportがメッセージを生成できないためであるか、配信できないためであるかを判別できます。

手順

1. `system node autosupport history show`コマンドを使用してメッセージの配信ステータスを確認します。
2. ステータスを読みます。

ステータス	意味
initializing	収集プロセスが開始しています。この状態が一時的なものであれば問題はありません。ただしこの状態が持続する場合は、問題が発生しています。
collection-failed	AutoSupportが、スプール ディレクトリ内にAutoSupportコンテンツを作成できません。AutoSupportが収集しようとしているものを表示するには、`system node autosupport history show -detail`コマンドを入力します。
collection-in-progress	AutoSupportがAutoSupportコンテンツを収集しています。AutoSupportが収集しているものを表示するには、`system node autosupport manifest show`コマンドを入力します。
queued	AutoSupportメッセージが配信のためにキューに登録されていますが、まだ配信されていません。
transmitting	AutoSupportが現在メッセージを配信しています。
sent-successful	AutoSupportがメッセージを正常に配信しました。AutoSupportによるメッセージの配信先を特定するには、`system node autosupport history show -delivery`コマンドを入力します。
ignore	AutoSupportでメッセージの宛先が指定されていません。配信の詳細を表示するには、`system node autosupport history show -delivery`コマンドを入力します。
re-queued	AutoSupportがメッセージの配信を試行しましたが、失敗しました。その結果AutoSupportでは、再度配信を試行するために、メッセージが配信キューに戻されました。このエラーを表示するには、`system node autosupport history show`コマンドを入力します。
transmission-failed	AutoSupportで、指定された回数のメッセージ配信が失敗したため、メッセージ配信の試行が停止されました。このエラーを表示するには、`system node autosupport history show`コマンドを入力します。
ondemand-ignore	AutoSupportメッセージは正常に処理されましたが、AutoSupport OnDemandサービスによって無視されました。

3. 次のいずれかを実行します。

ステータス	処理
initializingまたはcollection-failed	AutoSupportがメッセージを生成できないため、テクニカル サポートに問い合わせます。
ignore、re-queued、または transmission failed	AutoSupportがメッセージを配信できないため、SMTP、HTTP、またはHTTPSのデスティネーションが正しく設定されていることを確認します。

関連タスク

SMTP経由のAutoSupportメッセージ配信のトラブルシューティング（219ページ）
HTTPまたはHTTPS経由でのAutoSupportメッセージ配信のトラブルシューティング（217ページ）

HTTPまたはHTTPS経由でのAutoSupportメッセージ配信のトラブルシューティング

HTTPまたはHTTPSを使用していて、AutoSupportメッセージが送信されない場合は、いくつかの設定を確認することで問題を解決できます。

開始する前に

基本的なネットワーク接続とDNSルックアップについて、以下の点を確認しておく必要があります。

- ネットワーク管理LIFの動作ステータスおよび管理ステータスがupになっている。

- 同じサブネット上の機能しているホストに、（ノード上のLIFではなく）クラスタ管理LIFからpingを実行できる。
- サブネットの外部の機能しているホストに、クラスタ管理LIFからpingを実行できる。
- サブネットの外部の機能しているホストに、（IPアドレスではなく）ホストの名前を使用してクラスタ管理LIFからpingを実行できる。

タスク概要

以下の手順は、AutoSupportでメッセージを生成できているが、HTTPまたはHTTPS経由でメッセージを配信できていないと判断した場合に実行します。

エラーが発生したり、いずれかの手順を完了できない場合は、問題を特定し、対処してから次の手順に進んでください。

手順

1. ノード管理LIFのステータスを確認します。

   `network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role`

   `status-oper`フィールドと`status-admin`フィールドが**`up`**になっている必要があります。

2. あとで使用できるように、SVM名、LIF名、およびLIFのIPアドレスを書き留めておきます。
3. DNSが有効になっていて正しく設定されていることを確認します。

   `vserver services name-service dns show`

4. AutoSupportメッセージからエラーが返された場合、対処します。

   `system node autosupport history show -node * -fields node,seq-num,destination,last-update,status,error`

   デジタル証明書に問題があることを示すエラーの場合は、テクニカル サポートにお問い合わせください。

5. クラスタが必要なサーバとインターネットの両方にアクセスできることを確認します。

   a. **`network traceroute -node local -destination`** ***`network_management_LIF`***

   b. **`network traceroute -node local -destination support.netapp.com`**

   c. **`system node autosupport show -fields proxy-url`**

   d. **`network traceroute -node local -destination`** ***`proxy_url`***

   いずれかのルートが機能していない場合は、「traceroute」ユーティリティまたは「tracert」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これらのユーティリティは、ほとんどのサードパーティ製ネットワーク クライアントで使用できます。これにより、ネットワーク設定とクラスタ構成のどちらに問題があるかを判断できます。

6. AutoSupportの転送プロトコルとしてHTTPSを使用する場合は、HTTPSトラフィックがネットワークから送信可能であることを確認します。

   a. クラスタ管理LIFと同じサブネットにWebクライアントを設定します。

      プロキシ サーバ、ユーザ名、パスワード、およびポートを含む、すべての設定パラメータの値がAutoSupportの設定と同じであることを確認します。

   b. Webクライアントを使用して`https://support.netapp.com`にアクセスします。

アクセスが成功します。成功しない場合は、HTTPSトラフィックとDNSトラフィックを許可するようにすべてのファイアウォールが設定されていること、およびプロキシ サーバが正しく設定されていることを確認します。

関連タスク

メッセージを受信しない場合のAutoSupportのトラブルシューティング(216ページ)

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

SMTP経由のAutoSupportメッセージ配信のトラブルシューティング

システムがSMTP経由でAutoSupportメッセージを配信できない場合、さまざまな設定を確認して問題を解決できます。

開始する前に

基本的なネットワーク接続とDNSルックアップについて、以下の点を確認しておく必要があります。

- ネットワーク管理LIFの動作ステータスおよび管理ステータスがupになっている。
- 同じサブネット上の機能しているホストに、(ノード上のLIFではなく)クラスタ管理LIFからpingを実行できる。
- サブネットの外部の機能しているホストに、クラスタ管理LIFからpingを実行できる。
- サブネットの外部の機能しているホストに、(IPアドレスではなく)ホストの名前を使用してクラスタ管理LIFからpingを実行できる。

タスク概要

以下の手順は、AutoSupportでメッセージを生成できているが、SMTP経由でメッセージを配信できていないと判断した場合に実行します。

エラーが発生したり、いずれかの手順を完了できない場合は、問題を特定し、対処してから次の手順に進んでください。

特に指定がないかぎり、すべてのコマンドをData ONTAPのCLIに入力します。

手順

1. ノード管理LIFのステータスを確認します。

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   `status-oper`フィールドと`status-admin`フィールドが**up**になっている必要があります。

2. あとで使用できるように、SVM名、LIF名、およびLIFのIPアドレスを書き留めておきます。
3. DNSが有効になっていて正しく設定されていることを確認します。

   ```
   vserver services name-service dns show
   ```

4. AutoSupportで使用するように設定されているすべてのサーバを表示します。

   ```
   systerm node autosupport show -fields mail-hosts
   ```

   表示されたすべてのサーバ名を書き留めておきます。

5. 前の手順で表示された各サーバと`support.netapp.com`にノードからアクセスできることを確認します。

network traceroute -node local -destination *server_name*

いずれかのルートが機能していない場合は、「traceroute」ユーティリティまたは「tracert」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これらのユーティリティは、ほとんどのサードパーティ製ネットワーク クライアントで使用できます。これにより、ネットワーク設定とクラスタ構成のどちらに問題があるかを判断できます。

6. メール ホストとして指定したホストにログオンし、このホストがSMTP要求を処理できることを確認します。

   netstat -aAn|grep 25

   25は、リスナーSMTPのポート番号です。

   次のようなメッセージが表示されます。

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. 他のホストで、メール ホストのSMTPポートを使用したTelnetセッションを開始します。

   telnet *mailhost* 25

   次のようなメッセージが表示されます。

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. Telnetのプロンプトで、メール ホストからメッセージをリレーできることを確認します。

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   *domain_name*はネットワークのドメイン名です。

   リレーが拒否されたというエラーが返された場合は、メール ホストでリレーが有効になっていません。システム管理者にお問い合わせください。

9. Telnetのプロンプトで、テスト メッセージを送信します。

   DATA

   SUBJECT: TESTING

   THIS IS A TEST

   .

   > **注:** 必ず最後の行にピリオド(.)を単独で入力してください。このピリオドで、メッセージの完了をメール ホストに示します。

   エラーが返された場合は、メール ホストが正しく設定されていません。システム管理者にお問い合わせください。

10. Data ONTAPのCLIから、アクセス可能な信頼できるEメール アドレスにAutoSupportのテスト メッセージを送信します。

    system node autosupport invoke -node local -type test

11. 送信したテスト メッセージのシーケンス番号を確認します。

    system node autosupport history show -node local -destination smtp

    シーケンス番号はタイムスタンプを基に探します。おそらく、最後に送信されたメッセージです。

12. テスト メッセージに関するエラーを表示します。

```
system node autosupport history show -node local -seq-num seq_num -
fields error
```

表示されるエラーがLogin deniedである場合、クラスタ管理LIFからの送信要求をSMTPサーバが受け入れていません。転送プロトコルをHTTPSに変更しない場合は、この問題に対処するSMTPゲートウェイの設定をサイトのネットワーク管理者に依頼してください。

このテストが成功しても、mailto:autosupport@netapp.comへの同じメッセージの送信が成功しない場合は、すべてのSMTPメール ホストでSMTPリレーが有効になっていることを確認するか、転送プロトコルとしてHTTPSを使用してください。

ローカルで管理されているEメール アカウントへのメッセージの送信も失敗する場合は、次の両方の条件に該当する添付ファイルを転送するようにSMTPサーバが設定されていることを確認してください。

- サフィックスが「7z」
- MIMEタイプが「application/x-7x-compressed」

関連タスク

メッセージを受信しない場合のAutoSupportのトラブルシューティング（216ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

システム ヘルスの監視

ヘルスモニタは、クラスタ内の特定のクリティカルな状態をプロアクティブに監視します。アクティブなアラートがある場合、クラスタのヘルス ステータスはデグレードとレポートされます。アラートには、デグレードのシステム ヘルスへの対処に必要な情報が含まれています。

ステータスがデグレードになっている場合は、考えられる原因や推奨されるリカバリ アクションなど、問題の詳細を表示できます。問題を解決すると、システム ヘルス ステータスは自動的にOKに戻ります。

システム ヘルス ステータスには、複数の異なるヘルスモニタの結果が反映されます。1つのヘルスモニタのステータスがデグレードになると、システム ヘルス全体のステータスがデグレードになります。

クラスタ内のシステム ヘルスの監視では、次のクラスタ スイッチがサポートされます。

- NetApp CN1601
- NetApp CN1610
- Cisco Nexus 5010
- Cisco Nexus 5020
- Cisco Nexus 5596
- Cisco Catalyst 2960-24TT-L

ヘルスモニタの動作

個々のヘルスモニタには、条件または状態に特定の変化が発生したときにアラートをトリガーする、一連のヘルス ポリシーがあります。問題に対応し今後のアラートを制御するために、ヘルスモニタの仕組みを理解しておくと役に立ちます。

ヘルスモニタは、次のコンポーネントから構成されています。

- それ自体のヘルス ステータスを持つ、特定のサブシステムに個別のヘルスモニタ
  たとえば、ストレージ サブシステムにはノード接続性のヘルスモニタがあります。
- 個々のヘルスモニタのヘルス ステータスを統合したシステム全体のヘルスモニタ
  単一サブシステムでのデグレード ステータスは、システム全体のデグレード ステータスを招きます。サブシステムにアラートがなければ、システム全体のステータスはOKです。

各ヘルスモニタは、次の主要な要素から構成されています。

- ヘルスモニタが発生させる可能性があるアラート
  各アラートには定義があり、これにはアラートの重大度や考えられる原因などの詳細が含まれます。
- 各アラートをいつトリガーするかを特定するヘルス ポリシー
  各ヘルス ポリシーには、アラートをトリガーする正確な条件または変更であるルールがあります。

ヘルスモニタは、サブシステム内のリソースの条件または状態の変化を 継続的に監視し、評価します。条件または状態の変化がヘルス ポリシーのルール式に一致すると、ヘルスモニタはアラートを発生させます。アラートによって、サブシステムのヘルス ステータスおよびシステム全体のヘルス ステータスがデグレードします。

システム ヘルス アラートへの対応方法

システム ヘルス アラートが発生したら、承認（応答）し、その詳細を調べ、原因となっている状況を修正して、再発しないようにします。

ヘルスモニタからアラートが発せられた場合、次のいずれかの方法で対応できます。

- 影響を受けるリソース、アラートの重大度、考えられる原因、考えられる影響、対処方法など、アラートに関する情報を入手する
- アラートが発せられた時間、すでに誰かが承認しているかどうかなど、アラートに関する詳細情報を入手する
- 特定のシェルフやディスクなど、影響を受けるリソースまたはサブシステムの状態に関するヘルス関連の情報を入手する
- アラートを承認してその問題に対応中であることを示し、自分自身を「承認者」として特定する
- ケーブル配線を修正して接続の問題を解決するなど、アラートで指定された対処方法を実施することによって、問題を解決する
- アラートが自動的に解除されない場合は、そのアラートを削除する
- サブシステムのヘルスの状態に影響しないようにアラートを抑制する
  問題を把握した場合は、抑制が役に立ちます。アラートを抑制すると、そのアラートは引き続き発生する可能性がありますが、その場合もサブシステムのヘルスは「ok-with-suppressed」と 表示されます。

システム ヘルス アラートのカスタマイズ

ヘルスモニタが生成するアラートは、アラートをいつトリガーするかを定義するシステム ヘルス ポリシーを有効または無効にすることによって制御できます。これによって、特定の環境に合わせてヘルス監視システムをカスタマイズできるようになります。

ポリシーの名前は、生成されたアラートの詳細情報を表示するか、特定のヘルスモニタ、ノード、またはアラートIDのポリシー定義を表示することによって把握できます。

ヘルス ポリシーの無効化と、アラートの抑制は違います。アラートを抑制した場合はサブシステムのヘルス ステータスに影響しませんが、アラートは発生します。

ポリシーを無効にした場合は、そのポリシー ルール式に定義された条件または状態によるアラートがトリガーされなくなります。

無効にするアラートの例

たとえば、役に立たないアラートが発生するとします。そのアラートのポリシーIDを取得するには、`system health alert show -instance`コマンドを使用します。ポリシーについての情報を表示するには、`system health policy definition show`コマンドでポリシーIDを使用します。ポリシーのルール式およびその他の情報を確認したあとで、ポリシーを無効にするかどうかを決定します。ポリシーを無効にするには、`system health policy definition modify`コマンドを使用します。

ヘルス アラートによるAutoSupportメッセージおよびイベントのトリガー方法

システム ヘルス アラートはAutoSupportメッセージとEvent Management System（EMS;イベント管理システム）のイベントをトリガーし、AutoSupportメッセージとEMSを使用するか、ヘルス監視システムを直接使用してシステムの正常性を監視できるようにします。

システムは、アラートから5分以内にAutoSupportメッセージを送信します。AutoSupportメッセージには、最後のAutoSupportメッセージ以降に生成されたすべてのメッセージが含まれます。ただし、同じリソースで前週に原因があると考えられる重複するアラートは除きます。

アラートによっては、AutoSupportメッセージをトリガーしないものがあります。ヘルス ポリシーでAutoSupportメッセージの送信が無効になっている場合は、アラートが発生しても、AutoSupportメッセージがトリガーされません。たとえば、問題の発生時にAutoSupportからすでにメッセージが生成されているという理由で、ヘルス ポリシーによりデフォルトでAutoSupportメッセージを無効にすることもできます。`system health policy definition modify`コマンドを使用して、AutoSupportメッセージをトリガーしないようにポリシーを設定できます。

`system health autosupport trigger history show`コマンドを使用して、前週に送信されたAutoSupportメッセージをトリガーしたすべてのアラートのリストを表示できます。

また、アラートはEMSに対するイベントの生成もトリガーします。イベントは、アラートが作成されるたび、およびアラートがクリアされるたびに生成されます。

使用可能なクラスタ ヘルスモニタ

ヘルスモニタは複数あり、それぞれがクラスタの異なる部分を監視します。ヘルスモニタは、イベント検出、アラート送信、およびクリアされたイベントの削除を行い、Data ONTAPサブシステム内で発生したエラーからのリカバリに役立ちます。

ヘルスモニタ名（識別子）	サブシステム名（識別子）	検証目的
クラスタ スイッチ（cluster-switch）	スイッチ（Switch-Health）	温度、利用率、インターフェイスの設定、冗長性（クラスタ ネットワーク スイッチのみ）、ファンおよび電源の動作に関して、クラスタ ネットワーク スイッチと管理ネットワーク スイッチを監視します。クラスタ スイッチ ヘルスモニタはSNMPでスイッチと通信します。デフォルトの設定はSNMPv2cです。
MetroCluster ファブリック	スイッチ	MetroCluster構成のバックエンド ファブリック トポロジを監視して、間違ったケーブル接続およびゾーニングなどの設定ミスや、ISLの障害を検出します。
MetroCluster ヘルス	インターコネクト、RAID、およびストレージ	FC-VIアダプタ、FCイニシエータ アダプタ、取り残されたアグリゲートやディスク、およびクラスタ間ポートを監視します。

ヘルスモニタ名（識別子）	サブシステム名（識別子）	検証目的
ノード接続（node-connect）	CIFSの無停止運用（CIFS-NDO）	SMB接続を監視して、Hyper-Vアプリケーションへの無停止運用を維持します。
	ストレージ（SAS-connect）	ノード レベルでシェルフ、ディスク、およびアダプタを監視して、適切なパスと接続を維持します。
システム	利用不可	他のヘルスモニタからの情報を集約します。
システム接続（system-connect）	ストレージ（SAS-connect）	クラスタ レベルでシェルフを監視して、2つのHAクラスタ ノードへの適切なパスを維持します。

システム ヘルス アラートの自動受信

`system health alert show`コマンドを使用して、システム ヘルス アラートを手動で表示できます。ただし、ヘルスモニタがアラートを生成した時点で通知を自動受信するには、特定のEvent Management System（EMS;イベント管理システム）メッセージに登録する必要があります。

タスク概要

次の手順では、すべてのhm.alert.raisedメッセージ、およびすべてのhm.alert.clearedメッセージに対する通知のセットアップ方法を示します。

すべてのhm.alert.raisedメッセージおよびhm.alert.clearedメッセージにはSNMPトラップが含まれています。SNMPトラップの名前は、`HealthMonitorAlertRaised`および`HealthMonitorAlertCleared`です。SNMPトラップについては、*『clustered Data ONTAP ネットワーク管理ガイド』*を参照してください。

手順

1. `event destination create`コマンドを使用して、EMSメッセージの送信先を定義します。

   例

   ```
   cluster1::> event destination create -name health_alerts -mail
   admin@example.com
   ```

2. `event route add-destinations`コマンドを使用して、`hm.alert.raised`メッセージと`hm.alert.cleared`メッセージを宛先に送信します。

   例

   ```
   cluster1::> event route add-destinations -messagename hm.alert* -
   destinations health_alerts
   ```

関連コンセプト

イベント メッセージの管理（195ページ）

関連情報

clustered Data ONTAP 8.3 ネットワーク管理ガイド

デグレードしたシステム ヘルスへの対応

システムのヘルス ステータスがデグレードした場合は、アラートを表示して考えられる原因および対処方法について一読し、デグレードしたサブシステムについての情報を表示して、問題を解決できます。抑制されたアラートも表示されるため、変更して承認済みかどうかを確認できます。

タスク概要

AutoSupportメッセージやEMSイベントを表示することによって、または`system health`コマンドを使用することによって、アラートが生成されたことを確認できます。

手順

1. `system health alert show`コマンドを使用して、システム ヘルスを侵害しているアラートを表示します。
2. アラートに示された考えられる原因、考えられる影響、および対処方法を一読し、問題を解決できるか、または詳細情報が必要かを判断します。
3. 詳細情報が必要な場合は、次のいずれかの対処方法を実行します。
   - `system health alert show -instance`コマンドを使用してアラートについての入手可能なその他の情報を表示する
   - 影響を受けたサブシステムについて`system health`コマンドで特定のコマンドを使用して、問題を検証する

   例

   たとえば、ディスクに問題がある場合は`system health node-connectivity disk`コマンドを使用してディスクについての詳細情報を取得します。
4. `system health alert modify`コマンドに`-acknowledge`パラメータを指定し、そのアラートに対して対処中であることを示します。
5. アラートの`[Corrective Actions]`フィールドに説明されている対処方法を実行し、問題を解決します。

   対処方法にはシステムのリブートが含まれている場合があります。

   問題が解決すると、アラートは自動的にクリアされます。サブシステムに他のアラートがない場合は、サブシステムのヘルスは`[OK]`に変わります。すべてのサブシステムのヘルスが[OK]の場合は、システム全体のヘルス ステータスが`[OK]`に変わります。
6. システム ヘルス ステータスが`[OK]`であることを確認するには、`system health status show`コマンドを使用します。

   システム ヘルス ステータスが`[OK]`でない場合は、この手順を繰り返します。

デグレードしたシステム ヘルスへの対応の例

ノードへの2つのパスが不足しているシェルフが原因でデグレードしたシステム ヘルスの特定の例を使用して、アラートに対応するときにCLIに表示される内容を確認します。

Data ONTAPを起動したあと、システム ヘルスを確認すると、ステータスがデグレードしていることがわかります。

```
cluster1::>system health status show
        Status
        ---------------
        degraded
```

アラートを表示して、問題箇所を見つけ、シェルフ2にノード1へのパスが2つないことを確認します。

```
cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two paths following the
rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

アラートの詳細を表示して、アラートIDなどの詳細情報を取得します。

```
cluster1::>system health alert show -monitor node-connect -alert-id DualPathToDiskShelf_Alert
-
instance
                   Node: node1
                Monitor: node-connect
               Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
              Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller node1.
    Corrective Actions: 1. Halt controller node1 and all controllers attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via two paths following
the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
               Suppress: false
                 Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

アラートの受信を確認して対応を続行します。

```
cluster1::>system health alert modify -node node1 -alert-id DualPathToDiskShelf_Alert -
acknowledge true
```

シェルフ2とノード1との間のケーブルを修正してから、システムをリブートします。次に、システム ヘルスを再度確認し、ステータスが「OK」であることを確認します。

```
cluster1::>system health status show
        Status
        ---------------
        OK
```

クラスタと管理ネットワーク スイッチの検出の設定

クラスタ スイッチ ヘルスモニタは、Cisco Discovery Protocol（CDP）を使用して、クラスタと管理ネットワーク スイッチの検出を自動的に試みます。ヘルスモニタがスイッチを自動的に検出できない場合、またはCDPを自動検出に使用することを望まない場合は、ヘルスモニタを設定する必要があります。

タスク概要

`system cluster-switch show`コマンドは、ヘルスモニタが検出したスイッチをリスト表示します。想定していたスイッチがこのリストに表示されない場合、ヘルスモニタは自動的にスイッチを検出できない状態にあります。

手順

1. CDPを自動検出に使用する場合は、以下の操作を行います。それ以外の場合は、手順2に進みます。

   a. スイッチでCDPが有効になっていることを確認します。

      手順については、スイッチのマニュアルを参照してください。

   b. クラスタ内の各ノードで次のコマンドを実行し、CDPが有効か無効かを確認します。

      `run -node node_name -command options cdpd.enable`

      CDPが有効になっている場合は、手順dに進みます。CDPが無効になっている場合は、手順cに進みます。

   c. 次のコマンドを実行して、CDPを有効にします。

      `run -node node_name -command options cdpd.enable on`

      5分ほど待ってから次の手順に進みます。

   d. `system cluster-switch show`コマンドを使用して、Data ONTAPがスイッチを自動的に検出できるようになったことを確認します。

2. ヘルスモニタがスイッチを自動的に検出できない場合は、`system cluster-switch create`コマンドを使用してスイッチの検出を設定します。

   例

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -
   type cluster-network
   ```

   5分ほど待ってから次の手順に進みます。

3. `system cluster-switch show`コマンドを使用して、情報を追加したスイッチをData ONTAPが検出できることを確認します。

終了後の操作

ヘルスモニタがスイッチを監視できることを確認します。

クラスタおよび管理ネットワーク スイッチの監視の確認

クラスタ スイッチ ヘルスモニタは検出されたスイッチの監視を自動的に試みますが、スイッチが正しく設定されていないと監視が自動的に行われないことがあります。ヘルスモニタがスイッチを監視するよう適切に設定されていることを確認する必要があります。

手順

1. `system health cluster-switch show`コマンドを使用し、クラスタ スイッチ ヘルスモニタによって検出されたスイッチを特定します。

   `Model`列に値`OTHER`が表示されている場合、Data ONTAPはそのスイッチを監視できません。自動検出されたスイッチがヘルスモニタのサポート対象でない場合、Data ONTAPは値を`OTHER`に設定します。

   注: コマンド出力にスイッチが表示されない場合は、そのスイッチの検出を設定する必要があります。

2. *Cisco Ethernet Switchのページ*で、サポートされている最新のスイッチ ソフトウェアとReference Configuration File（RCF）にアップグレードします。

スイッチのRCF内のコミュニティ ストリングは、ヘルスモニタで使用するように構成されているコミュニティストリングと同じである必要があります。デフォルトでは、ヘルスモニタはコミュニティ ストリング**cshm1!**を使用します。

クラスタが監視するスイッチの情報を変更する必要がある場合は、`system health cluster-switch modify`コマンドを使用し、ヘルスモニタが使用するコミュニティ ストリングを変更できます。

3. スイッチの管理ポートが管理ネットワークに接続されているかを確認します。

   SNMPクエリの実行にはこの接続が必要となります。

関連タスク

クラスタと管理ネットワーク スイッチの検出の設定(226ページ)

システムの健全性の監視用コマンド

`system health`コマンドを使用すると、システム リソースの健全性に関する情報の表示、アラートへの応答、および以後のアラートの設定を行うことができます。CLIコマンドを使用すると、ヘルスモニタの設定に関する詳しい情報を表示できます。詳細については、これらのコマンドのマニュアル ページを参照してください。

システムのヘルス ステータスの表示

状況	使用するコマンド
個々のヘルスモニタのステータス全体が反映された、システムのヘルス ステータスを表示する	`system health status show`
ヘルス監視が可能なサブシステムのヘルス ステータスを表示する	`system health subsystem show`

クラスタ接続ステータスの表示

状況	使用するコマンド
クラスタ レベル ビューからシェルフ ステータスを表示する	`system health system-connectivity shelf show`
シェルフのUUIDとID、接続しているノード、シェルフへのパス数など、各シェルフの詳細な情報を表示する	`system health system-connectivity shelf show-instance`

ノード接続ステータスの表示

状況	使用するコマンド
ノード レベル ビューでのシェルフ ステータスと、所有者ノード、シェルフ名、シェルフのディスク数やパス数などのその他の情報を表示する	`system health node-connectivity shelf show` 各シェルフの詳細な情報を表示するには、`-instance`パラメータを使用します。
ディスク ステータスと、所有者ノード、ディスク名とベイ番号、ディスクへのパス数などのその他の情報を表示する	`system health node-connectivity disk show` 各ディスクの詳細な情報を表示するには、`-instance`パラメータを使用します。

状況	使用するコマンド
アダプタ ステータスと、所有者ノード、使用および有効化されているかどうか、接続されているシェルフ数などのその他の情報を表示する	`system health node-connectivity adapter show` 各アダプタの詳細な情報を表示するには、`-instance`パラメータを使用します。

クラスタと管理ネットワーク スイッチの検出管理

状況	使用するコマンド
クラスタが監視するスイッチを表示する	`system health cluster-switch show`
削除したスイッチ（コマンド出力のReason列に表示）を含め、クラスタが現在監視するスイッチ、およびクラスタと管理ネットワーク スイッチへのネットワーク アクセスに必要な設定情報を表示する このオプションは、advanced権限レベルで使用できます。	`system health cluster-switch show-all`
未検出スイッチの検出を設定する	`system health cluster-switch create`
クラスタが監視するスイッチについての情報（デバイス名、IPアドレス、SNMPバージョン、コミュニティ ストリングなど）を変更する	`system health cluster-switch modify`
スイッチの監視を無効にする	`system health cluster-switch modify -disable-monitoring`
情報収集のためにヘルスモニタがスイッチをポーリングする間隔を表示する	`system health cluster-switch polling-interval show`
情報収集のためにヘルスモニタがスイッチをポーリングする間隔を変更する このオプションは、advanced権限レベルで使用できます。	`system health cluster-switch polling-interval modify`
スイッチの検出と監視を無効にし、スイッチの設定情報を削除する	`system health cluster-switch delete`
データベースに格納されているスイッチの設定情報を完全に削除する（スイッチの自動検出が再度有効になります）	`system health cluster-switch delete -force`

生成されたアラートへの対応

状況	使用するコマンド
アラートがトリガーされたリソースやノード、アラートの重大度や考えられる原因など、生成されたアラートに関する情報を表示する	`system health alert show`
生成された各アラートに関する情報を表示する	`system health alert show -instance`
特定のアラートに対して作業が行われていることを示す	`system health alert modify`
アラートを承認する	`system health alert modify -acknowledge`

状況	使用するコマンド
サブシステムのヘルス ステータスに影響しないように、以降のアラートを抑制する	`system health alert modify -suppress`
自動的に消去されなかったアラートを削除する	`system health alert delete`
あるアラートでAutoSupportメッセージがトリガーされたかどうかを確認するためなど、過去1週間にアラートによりトリガーされたAutoSupportメッセージに関する情報を表示する	`system health autosupport trigger history show`

以後のアラートの設定

状況	使用するコマンド
リソースの状態に応じて特定のアラートを発行するかどうかを制御するポリシーを有効または無効にする	`system health policy definition modify`

ヘルスモニタの設定に関する情報を表示する

状況	使用するコマンド
ヘルスモニタについて、ノード、名前、サブシステム、ステータスなどの情報を表示する	`system health config show` **注:** 各ヘルスモニタの詳細な情報を表示するには、`-instance`パラメータを使用します。
ヘルスモニタで生成される可能性があるアラートの情報を表示する	`system health alert definition show` **注:** 各アラートの定義に関する詳細な情報を表示するには、`-instance`パラメータを使用します。
アラートが発行されるタイミングを決定する、ヘルスモニタのポリシーに関する情報を表示する	`system health policy definition show` **注:** 各ポリシーの詳細な情報を表示するには、`-instance`パラメータを使用します。ポリシーのステータス（有効または無効）、ヘルスモニタ、アラートなどによってアラートのリストをフィルタリングするには、その他の適切なパラメータを使用します。

マイナー リリース間のソフトウェア バージョンのダウングレード

Data ONTAP 8.2.1からData ONTAP 8.2にダウングレードすると、削除済みスイッチの履歴が消去されます。また、自動検出されたスイッチがヘルスモニタのサポート対象でない場合、`Model`列が`OTHER`に設定されます。

状況	使用するコマンド
ソフトウェアのバージョンをダウングレードする	`system health cluster-switch prepare-to-downgrade`

ダッシュボードを使用した重要なシステム情報の表示

ダッシュボードでは、Storage Virtual Machine（SVM、旧Vserver）の健常性、システムとクラスタのパフォーマンス、ストレージ スペースの利用率など、クラスタの重要な要素を視覚的に確認できます。また、アラームしきい値を設定し、アラームに関する情報を表示することもできます。

次の項目についてアラームしきい値を設定できます。

- アグリゲート利用率（aggregate-used）
- NFS処理とCIFS処理のクライアント平均遅延（op-latency）
- CPU利用率（cpu-busy）
- パケット エラー率（port-problems）
- ポート利用率（port-util）

たとえば、アグリゲートで使用されるスペースについて、警告およびクリティカルのアラームしきい値を変更することができます。警告のしきい値を50%に設定し、クリティカルのしきい値を60%に設定できます。設定されたしきい値を超えると、クラスタで「しきい値超過」アラームが生成されます。さらに、アラームが生成またはクリアされた場合にEvent Management System（EMS;イベント管理システム）でメッセージが生成されるように設定することもできます。

ダッシュボード アラームの通知

ダッシュボード アラームは、`dashboard alarm show`コマンドを使用して表示できます。特定のEvent Management System（EMS;イベント管理システム）メッセージに登録して、ダッシュボード アラームの通知を受け取ることができます。

開始する前に

アラームの生成時に、`dashboard alarm thresholds modify`コマンドを使用してEMSがメッセージを送信するように指定する必要があります。

タスク概要

しきい値がクリティカルなしきい値以上になった時点（上昇時）、または警告値を下回った時点（下降時）で、EMSはダッシュボード アラームのメッセージを生成します。アラームの通知が必要なオブジェクトの種類に対するEMSメッセージの経路を次のように設定する必要があります。

aggregate-used

このオブジェクトの種類には、次のEMSメッセージが関連します。

- mgmtgwd.aggregate.used.rising
- mgmtgwd.aggregate.used.falling

cpu-busy

このオブジェクトの種類には、次のEMSメッセージが関連します。

- mgmtgwd.cpu.busy.rising
- mgmtgwd.cpu.busy.falling

op-latency

このオブジェクトの種類には、次のEMSメッセージが関連します。

- mgmtgwd.op.latency.rising

- mgmtgwd.op.latency.falling

port-problems

このオブジェクトの種類には、次のEMSメッセージが関連します。

- mgmtgwd.port.problems.rising
- mgmtgwd.port.problems.falling

port-util

このオブジェクトの種類には、次のEMSメッセージが関連します。

- mgmtgwd.port.util.rising
- mgmtgwd.port.util.falling

手順

1. `event destination create`コマンドを使用して、EMSメッセージの送信先を定義します。

   例

   ```
   cluster1::> event destination create -name dashboard_alarms -mail
   admin@example.com
   ```

2. `event route add-destinations`コマンドを使用して、EMSメッセージの宛先への経路を指定します。

   例

   次の例では、アグリゲートの利用率に関するメッセージをdashboard_alarmsという宛先に送信するように指定します。

   ```
   cluster1::> event route add-destinations -messagename
   mgmtgwd.aggregate.used* -destinations dashboard_alarms
   ```

   例

   次の例では、ダッシュボード アラームのメッセージをすべてdashboard_alarmsという宛先に送信するように指定します。

   ```
   cluster1::> event route add-destinations -messagename
   mgmtgwd.aggregate.used*,mgmtgwd.port.problems*,mgmtgwd.op.latency*,
   mgmtgwd.port.util*,mgmtgwd.cpu.busy* -destinations dashboard_alarms
   ```

ダッシュボードの管理用コマンド

`dashboard`コマンドは古いコマンドで推奨されていませんが、ダッシュボードの設定、ダッシュボード情報の表示、SVMのヘルス ステータスの表示に引き続き使用できます。

注: `dashboard health vserver`コマンドは、NFSプロトコルとCIFSプロトコルをサポートします。FCプロトコルとiSCSIプロトコルはサポートされません。

状況	使用するコマンド
次のようなクラスタ全体のアラームを設定する • イベントに関する警告または重大なアラームを生成するしきい値 • アラームが生成された場合にEMSメッセージを送信するかどうか • アラーム ダッシュボードによってオブジェクトが監視される間隔	`dashboard alarm thresholds modify`
アラームしきい値に関する設定を表示する	`dashboard alarm thresholds show`
その値が設定されているしきい値を超えたアラームに関する情報を表示する	`dashboard alarm show`
システムとクラスタのパフォーマンスに関する情報を表示する	`dashboard performance show`
ストレージ スペースの利用率と傾向に関する情報を表示する	`dashboard storage show`
現在の動作ステータス、問題、重大なアラート、警告、情報メッセージなど、SVMの一般的な健常性に関する情報を表示する	`dashboard health vserver show`
SVM内のアグリゲート、LIF、ポート、プロトコル、およびボリュームのヘルス ステータスを表示する	`dashboard health vserver show-combined`
SVM内のアグリゲートのヘルス ステータスを表示する	`dashboard health vserver show-aggregate`
SVM内のボリュームのヘルス ステータスを表示する	`dashboard health vserver show-volume`
SVM内のLIFのヘルス ステータスを表示する	`dashboard health vserver show-lif`
SVMネットワーク ポートのヘルス ステータスを表示する	`dashboard health vserver show-port`
SVM内のプロトコルのヘルス ステータスを表示する	`dashboard health vserver show-protocol`

詳細については、マニュアル ページを参照してください。

クラスタのパフォーマンスの監視

クラスタに関するデータを表示して、クラスタのパフォーマンスを監視できます。たとえば、スループットやレイテンシを表す統計を表示することによって、ボリュームのパフォーマンスを監視できます。統計を表示するには、パフォーマンス プリセットに関連付けられている設定済みのコマンドを使用するか、詳細な設定を必要とする高度なコマンドを使用します。

`system node autosupport invoke-performance-archive`コマンドを使用して、NetApp サポート サイトまたは指定のURIにパフォーマンス アーカイブをアップロードできます。NetApp サポート サイトにパフォーマンス アーカイブをアップロードしたら、SmartSolveツールを使用してデータを表示できます。このツールは、NetApp サポート サイトで入手できます。

関連タスク

パフォーマンス アーカイブ ファイルのアップロード(213ページ)

オブジェクト、インスタンス、カウンタとは

クラスタ内の特定のオブジェクトのパフォーマンス データを表示できます。オブジェクトは、インスタンスとカウンタから構成されます。カウンタは、オブジェクトのインスタンスに関するデータを提供します。

オブジェクトは次のいずれかです。

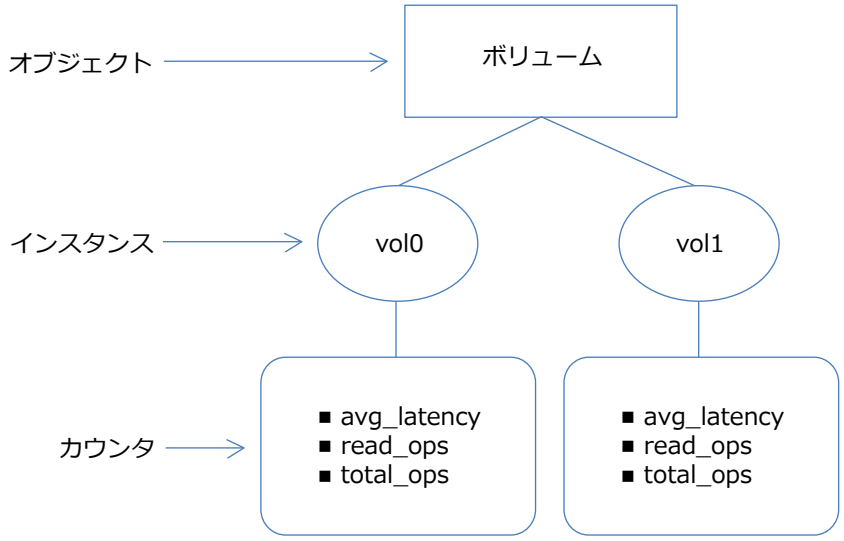
- ディスク、プロセッサ、ポートなどの物理エンティティ
- LUN、ボリューム、ワークロードなどの論理エンティティ
- CIFS、NFS、iSCSI、FCなどのプロトコル

各オブジェクトには、インスタンスが存在しないことも、インスタンスが複数存在することもあります。たとえば、LUNオブジェクトにはクラスタ内のLUNごとにインスタンスがあります。

カウンタは、事前定義されたパフォーマンス指標であり、オブジェクトに関するデータを提供します。カウンタが提供するデータには次のようなものがあります。

- ディスク容量
- ボリュームの平均レイテンシ
- 確立されているSMBセッションとSMB2セッションの数

次の図は、オブジェクトとそのインスタンスおよびカウンタとの関係を示しています。この図では、ボリューム オブジェクトに2つのインスタンス、vol0とvol1が存在します。このオブジェクトのカウンタは、これらのインスタンスのそれぞれに関するデータを提供します。この図には、オブジェクトのカウンタのうちの3つ、avg_latency、read_ops、およびtotal_opsが示されています。



パフォーマンス プリセットによる収集データの定義

パフォーマンス プリセットは、どのカウンタを使用してオブジェクトのデータを収集するか、およびパフォーマンス アーカイブにデータを追加するかどうかを定義します。`statistics`コマンドにパフォ

ーマンス プリセットが関連付けられることで、オブジェクトのパフォーマンス データを簡単に収集して表示することができます。

システムは多数のパフォーマンス プリセットを使用します。statisticsコマンドに関連付けられるパフォーマンス プリセットと、内部のプロセス（パフォーマンス アーカイブ用のデータの収集など）に使用されるパフォーマンス プリセットがあります。

パフォーマンス プリセットには次の情報が含まれています。

- パフォーマンス プリセットの名前
- パフォーマンス プリセットがデータを収集するオブジェクトの名前
- サンプリング期間における収集データをパフォーマンス アーカイブに追加するかどうか
- 各オブジェクトのデータを収集するカウンタの名前

statisticsコマンドにパフォーマンス プリセットが関連付けられることで、簡単なコマンドを使用してオブジェクトのパフォーマンス データを収集および表示できます。たとえば、-presetパラメータを指定して、statistics startコマンドとstatistics show-periodicコマンドでパフォーマンス プリセットを使用できます。

関連コンセプト

高度な方法を使用したクラスタのパフォーマンスの監視（238ページ）

関連タスク

オブジェクトのパフォーマンス データの収集と表示（235ページ）

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

オブジェクトのパフォーマンス データの収集と表示

簡易版のstatisticsコマンドを使用して、オブジェクトのパフォーマンス データを収集および表示できます。コマンドに関連付けられたパフォーマンス プリセットがオブジェクトのデータを収集するカウンタを定義し、statisticsコマンドでデータを収集する回数を定義します。

タスク概要

この手順では、statistics volume showコマンドを使用して、クラスタ内のボリュームの各インスタンスのパフォーマンス データを収集および表示する例を示します。パフォーマンス プリセットがstatistics volume showコマンドに関連付けられており、クラスタ内のボリュームの各インスタンスのデータを収集するカウンタが定義されています。

statisticsコマンド ファミリーの多くのコマンドにはパフォーマンス プリセットが関連付けられており、さまざまなオブジェクトのパフォーマンス データを簡単に収集して表示することができます。

手順

1. statistics volume showコマンドを使用して、ボリュームの各インスタンスのパフォーマンス データを収集および表示します。

   デフォルトでは、ボリュームの上位25個のインスタンスのデータが返されます（最大数は100個）。

   例

   次の例では、ボリュームの各インスタンスのパフォーマンス データが5秒間収集（回数は1回）されて、表示されます。デフォルトでは、1回につき5秒間データが収集されます。

```
cluster1::> statistics volume show -iterations 1
```

次の例では、Ctrl+Cキーを押してデータ収集を手動で停止するまで、ボリュームの各インスタンスのパフォーマンス データが収集および表示されます。

```
cluster1::> statistics volume show -iterations 0
```

関連コンセプト

パフォーマンス プリセットによる収集データの定義(234ページ)

関連参照情報

クラスタのパフォーマンスの監視用コマンド(241ページ)

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

統計のフィルタリング

フィルタを使用して、特定のオブジェクトのリソース利用率を追跡したり、収集する統計の量を絞り込んだりできます。たとえば、システム内の30,000個のLUNから統計を収集するには長い時間がかかる可能性がありますが、ボリューム名で統計をフィルタリングすれば、収集する統計の量を絞り込み、処理にかかる時間を短縮できます。

タスク概要

次の手順では、パフォーマンス データをボリュームでフィルタリングする方法を例として示しています。

手順

1. `statistics volume show`コマンドを使用して、ボリュームのパフォーマンス データを表示します。

   出力には主要なカウンタが表示され、結果は指定したオブジェクトの最もアクティブなインスタンス順にソートされます。

   例

   この出力例には、IOP値の高いボリュームが表示されています。

```
cluster1::> statistics volume show
cluster1 : 12/31/2013
16:00:04



                          *Total Read Write Other  Read Write
Latency
Volume Vserver Aggregate    Ops  Ops   Ops   Ops (Bps) (Bps)
(us)
------ ------- --------- ------ ---- ----- ----- ----- -----
-------
vol0       -   aggr0         58   13    15    29 9585   3014
39
vol1       -   aggr0_n0      56    0    11    45 8192  28826      47
```

2. 出力をボリューム名でフィルタリングします。

   例

   この出力例には、vol1の統計が表示されます。

```
cluster1::> statistics volume show –volume
vol1
cluster1 : 12/31/2013
16:00:04



                         *Total Read Write Other   Read Write
Latency
Volume Vserver Aggregate    Ops  Ops   Ops   Ops  (Bps) (Bps)
(us)
------ ------- --------- ------ ---- ----- ----- ------ -----
-------

vol1       -   aggr0_n0      56    0    11    45   8192 28826      47
```

統計のソート

任意のカウンタで統計をソートして、パフォーマンスの問題を診断したり、ホット スポットを特定したりできます。たとえば、ボリュームの統計を収集して合計処理数でソートし、最もアクティブなボリュームのリストを取得できます。

手順

1. `set -privilege advanced`コマンドを使用して、advanced権限レベルに切り替えます。
2. `statistics show`コマンドを使用して、サンプル データを表示します。

例

この出力例には、ボリューム名、読み取り処理数、および書き込み処理数が表示され、`read_ops`カウンタで出力がソートされます。

```
 ::>statistics show -object volume -counter read_ops|write_ops -
filter "vserver_name=vs1,read_ops>15" -sort-key read_ops -sort-order
ascending

Object: volume
Instance: vol1
Start-time: 05/23/2014 4:00 PM
End-time: 05/23/2014 4:10 PM
Cluster: cluster1
Number of Constituents: 1 (complete_aggregation)
  Counter                                Value
  ---------------------------- -----------
  read_ops                                  20
  write_ops                                 90

Object: volume
Instance: vol2
Start-time: 05/23/2014 4:00 PM
End-time: 05/23/2014 4:10 PM
Cluster: cluster1
Number of Constituents: 1 (complete_aggregation)
  Counter                                Value
  ---------------------------- -----------
  read_ops                                  40
  write_ops                                 30
```

パフォーマンス プリセット設定のインポート（クラスタ管理者のみ）

XMLファイル形式のパフォーマンス プリセット設定をインポートして、独自のパフォーマンス プリセットを作成したり、編集可能なパフォーマンス プリセットを変更したりできます。また、この方法で、収集してパフォーマンス アーカイブに格納するデータを変更することもできます。

開始する前に

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- XMLファイル形式のパフォーマンス プリセット設定が必要です。
  パフォーマンス プリセット定義のMLファイルの作成については、テクニカル サポートにお問い合わせください。

タスク概要

Data ONTAPのパフォーマンス アーカイブは、事前に決められた時間にパフォーマンス統計を自動的に収集して格納します。パフォーマンス プリセットをインポートすると、パフォーマンス アーカイブ用に収集するデータを変更できます。インポート方法については、テクニカル サポートにお問い合わせください。

読み取り専用のパフォーマンス プリセットを変更することはできません。変更できるのは、`read-only`パラメータがfalseに設定されているパフォーマンス プリセットのみです。

手順

1. `set -privilege advanced`コマンドを使用して、advanced権限レベルに切り替えます。
2. `statistics preset import`コマンドを使用して、パフォーマンス プリセット設定をインポートします。

   例

   次の例では、NetApp サポート サイトからパフォーマンス プリセット設定がインポートされます。

```
cluster1::*> statistics preset import -source-uri http://
www.netapp.com/support/
nfs_monitor.xml -comment "New NFS Monitor preset."
```

高度な方法を使用したクラスタのパフォーマンスの監視

`statistics start`、`statistics stop`、および`statistics show`の各コマンドを使用して、パフォーマンス データを収集および表示できます。これらのコマンドを使用すると、パフォーマンス データを収集して表示する方法を指定できます。これらのコマンドを実行するには、advanced権限とオブジェクトおよびカウンタに関する知識が必要です。

設定済みのコマンドを使用して、特定のオブジェクトに関するデータを収集および表示する場合は、簡易版の`statistics`コマンド（`statistics volume show`コマンドなど）を使用します。

関連コンセプト

パフォーマンス プリセットによる収集データの定義（234ページ）

パフォーマンス データを表示する前の決定事項

パフォーマンス データはいくつかの方法で表示できます。データを表示する前に決定すべきことがあります。

パフォーマンス データを表示する前に、次のことを決定する必要があります。

決定内容	考慮事項
データの取得および表示をどのように行うか	次の2つの方法があります。 • 特定の期間内のデーター式を収集して表示できます。 この場合、複数のオブジェクトとインスタンスのデータを一度に表示できます。 • 継続的に更新されるデータを表示できます。 この場合、`statistics show-periodic`コマンドで一度に表示できるのは1つのオブジェクトと1つのインスタンスのデータに限られます。
どのオブジェクトのデータを表示するか	データを表示するオブジェクトを1つ以上指定する必要があります。
すべてのカウンタのデータを表示するか、それとも特定のカウンタのデータを表示するか	デフォルトの設定ではオブジェクト内のすべてのカウンタのデータが表示されますが、特定のカウンタを指定して必要なデータのみを正確に取得できます。
オブジェクトの全インスタンスのデータが必要か、特定のインスタンスのデータが必要か	• 一定期間内のデータを収集する場合、デフォルトの設定ではすべてのインスタンスのデータが表示されますが、1つまたは複数のインスタンスを指定できます。 • 継続的に更新されるデータを表示する場合、および**`cluster`**以外のオブジェクトを指定する場合は、`statistics show-periodic`コマンドの使用時にインスタンスを指定する必要があります。
クラスタ全体のデータを表示するか、データの範囲を限定するか	デフォルトの設定ではクラスタ全体のデータが表示されますが、データの範囲を特定のSVMまたは特定のノードに限定できます。

一定期間のパフォーマンス データの表示

一定期間内のデータ（サンプル）を収集して表示することにより、クラスタ のパフォーマンスを監視できます。データの表示は、複数のオブジェクトとインスタンスについて一度に行うことができます。

タスク概要

複数のデータ サンプルを一度に収集することができます。また、同じオブジェクトから複数のサンプルを一度に収集することもできます。

注: インスタンスが5,000個を超えるオブジェクトについては、データを収集して表示することはできません。1つのオブジェクトに5,000個を超えるインスタンスが存在する場合は、データを収集するインスタンスを特定する必要があります。これはすべての `statistics`コマンド（`statistics`ビューを含む）に当てはまります。

`statistics`コマンドの詳細については、マニュアル ページを参照してください。

手順

1. `set -privilege advanced`コマンドを使用して、advanced権限レベルに切り替えます。

2. `statistics start`コマンドを使用してデータの収集を開始します。

   このコマンドで`-sample-id`パラメータを指定しないと、サンプル識別子が生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。同じCLIセッションで`-sample-id`パラメータを指定せずにこのコマンドを再び実行した場合、前回のデフォルト サンプルが上書きされます。そのため、前回のデフォルト サンプルを上書きするかどうかを確認するメッセージが表示されます。

3. オプション: サンプルのデータ収集を停止するには、`statistics stop`コマンドを使用します。

   データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しなければ、以前のクエリとの比較に使用できる更新されたデータを入手できます。この比較は、パフォーマンスの傾向を確認するのに役立ちます。

4. `statistics show`コマンドを使用してサンプル データを表示します。

例:NFSv3のパフォーマンスの監視

以下に、NFSv3プロトコルのパフォーマンス データを表示する例を示します。

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、正常に行われた読み込み要求および書き込み要求の数と読み込み要求と書き込み要求の総数の比較を示すカウンタを指定することにより、サンプルのデータを表示します。

```
cluster1::*> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                                 Value
    --------------------------- ---------------------------
    read_success                                            40042
    read_total                                              40042
    write_success                                         1492052
    write_total                                           1492052
```

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

継続的に更新されるパフォーマンス データの表示

クラスタのパフォーマンスは、最新のステータスで継続的に更新されるデータを表示して監視できます。一度に表示できるのは1つのオブジェクトと1つのインスタンスのデータに限られます。

タスク概要

`statistics show-periodic`コマンドの詳細については、マニュアル ページを参照してください。

注: `statistics show-periodic`コマンドは古いコマンドで推奨されていませんが、パフォーマンス データを表示するために引き続き使用できます。

また、statistics showコマンドに-tabパラメータを指定して、継続的に更新されるデータを表示することもできます。

手順

1. set -privilege advancedコマンドを使用して、advanced権限レベルに切り替えます。
2. statistics show-periodicコマンドを使用して、継続的に更新されるパフォーマンス データを表示します。

   -objectパラメータを指定しない場合、このコマンドではクラスタの要約データが返されます。

例:ボリューム パフォーマンスの監視

この例は、ボリューム パフォーマンスの監視方法を示しています。たとえば、ボリューム上で重要なアプリケーションを実行している場合などにボリューム パフォーマンスを監視できます。パフォーマンス データを表示することで次のような情報を把握できます。

- ボリュームの平均応答時間
- 1秒間に実行される処理数

次のコマンドでは、1秒あたりの処理数とレイテンシを表示するカウンタを指定することでボリュームのパフォーマンス データを表示しています。

```
cluster1::*> statistics show-periodic -object volume -instance
vol0  -counter write_ops|read_ops|total_ops|read_latency|
write_latency|avg_latency
cluster1: volume.vol0: 1/7/2013 20:15:51
      avg     read              total    write    write
  latency  latency read_ops       ops  latency      ops
 -------- -------- -------- -------- -------- --------
    202us    218us        0       22    303us        7
     97us     43us       31       71    149us       34
     39us      0us        0        3      0us        0
    152us      0us        0       16    152us       16
    162us      0us        0      342    144us      289
    734us      0us        0       15      0us        0
     49us      0us        0        1      0us        0
cluster: volume.vol0: 1/7/2013 20:16:07
      avg     read              total    write    write
  latency  latency read_ops       ops  latency      ops
 -------- -------- -------- -------- -------- --------
Minimums:
     39us      0us        0        1      0us        0
Averages for 7 samples:
    205us     37us        4       67    106us       49
Maximums:
    734us    218us       31      342    303us      289
```

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

クラスタのパフォーマンスの監視用コマンド

statisticsコマンドを使用して、パフォーマンス データの表示と、データ表示用の設定を行うことができます。これらのコマンドの詳細については、マニュアル ページを参照してください。

パフォーマンス プリセットを使用したオブジェクトのデータ収集

次のコマンドを使用して、オブジェクトのデータ サンプルを収集および表示できます。次の各コマンドはパフォーマンス プリセットに関連付けられています。パフォーマンス プリセットは、オブジェクト

のデータを収集するカウンタを定義するものです。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
アグリゲートのデータ サンプルを収集して表示する	`statistics aggregate show`
キャッシュのデータ サンプルを収集して表示する	`statistics cache flash-pool show`
ディスクのデータ サンプルを収集して表示する	`statistics disk show` このコマンドは、advanced権限レベルで使用できます。
LIFのデータ サンプルを収集して表示する	`statistics lif show`
LUNのデータ サンプルを収集して表示する	`statistics lun show`
クラスタ内の各ノードのデータ サンプルを収集して表示する	`statistics node show`
FCポートのデータ サンプルを収集して表示する	`statistics port fcp show`
クラスタのデータ サンプルを収集して表示する	`statistics system show`
ボリュームのデータ サンプルを収集して表示する	`statistics volume show`
Storage Virtual Machine（SVM）のデータ サンプルを収集して表示する	`statistics vserver show`
QoSワークロードのデータ サンプルを収集して表示する	`statistics workload show` このコマンドは、advanced権限レベルで使用できます。

パフォーマンス プリセットの表示

次のコマンドを使用して、パフォーマンス プリセットを表示できます。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
すべてのパフォーマンス プリセットを表示する	`statistics preset show`
各パフォーマンス プリセットの詳細を表示する	`statistics preset detail show`

パフォーマンス プリセットの作成、変更、および削除

次のコマンドを使用して、パフォーマンス プリセットを作成、変更、および削除できます。これらのコマンドには、advanced権限が必要です。

注: 読み取り専用のパフォーマンス プリセットを変更または削除することはできません。変更および削除できるのは、`read-only`パラメータがfalseに設定されているパフォーマンス プリセットのみです。

状況	使用するコマンド
パフォーマンス プリセットのプロパティ（名前やコメントなど）を変更する	`statistics preset modify`

状況	使用するコマンド
定義が記載されたXMLファイルをインポートしてパフォーマンス プリセットを作成または変更する	`statistics preset import` 定義が記載されたXMLファイルの作成については、テクニカル サポートにお問い合わせください。
パフォーマンス プリセットを削除する	`statistics preset delete`

高度な方法を使用したサンプル期間のデータ収集

次のコマンドを使用して、データ サンプルの収集と収集したサンプルの管理を行うことができます。`statistics show`コマンドを使用する前に、データ サンプルを収集しておく必要があります。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
サンプルのデータ収集を開始する	`statistics start` `-preset`パラメータを指定することで、パフォーマンス プリセットを使用してデータを収集できます。
サンプルのデータ収集を停止する	`statistics stop`
すべてのサンプルを表示する	`statistics samples show`
サンプルを削除する	`statistics samples delete`

高度な方法を使用したパフォーマンス データの表示

次のコマンドを使用して、パフォーマンス データを表示できます。`statistics show`コマンドを使用する前に、データ サンプルを収集しておく必要があります。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
サンプル期間のパフォーマンス データを表示する	`statistics show` システム パフォーマンスに大きく影響しないように、このコマンドの対象範囲は、一度に少数のオブジェクトに限定してください。
継続的に更新されるパフォーマンス データを表示する	`statistics show-periodic` このコマンドは古いコマンドで推奨されていませんが、パフォーマンス データを表示するために引き続き使用できます。

すべてのオブジェクト、インスタンス、カウンタの表示

`statistics catalog`コマンドを使用して、オブジェクト、インスタンス、およびカウンタについての情報を表示できます。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
オブジェクトの説明を表示する	`statistics catalog object show`
オブジェクトのすべてのインスタンスを表示する	`statistics catalog instance show`
オブジェクトにおけるカウンタの説明を表示する	`statistics catalog counter show`

統計コマンドの設定の管理

`statistics settings`コマンドを使用して、`statistics`コマンドの設定を変更できます。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
`statistics`コマンドの設定を表示する	`statistics settings show`
コマンドを実行したときに1秒あたりの比率で統計が表示されるかどうかを変更する	`statistics settings modify`

詳細なパフォーマンス データの表示

次のコマンドは古いコマンドで推奨されていませんが、クラスタに関する詳細なパフォーマンス データを表示するために引き続き使用できます。これらのコマンドには、advanced権限が必要です。

状況	使用するコマンド
クラスタ内のノードのSecD RPC使用率に関する統計情報を表示する	`statistics secd show` このコマンドは、パフォーマンスの分析と問題の診断を目的として、必ずサポート担当者の指示に従って使用してください。
クラスタ内のノードで実行されるONC RPC呼び出しに関する情報を表示する	`statistics oncrpc show-rpc-calls`

関連タスク

パフォーマンス アーカイブ ファイルのアップロード（213ページ）

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

環境情報の表示

センサーによって、システムの環境コンポーネントを効果的に監視できます。環境センサーについて表示できる情報には、タイプ、名前、状態、値、しきい値警告などがあります。

手順

1. 環境センサーに関する情報を表示するには、`system node environment sensors show`コマンドを使用します。

システム パフォーマンスの管理（クラスタ管理者のみ）

さまざまな機能を使用してシステムのパフォーマンスを向上させることができます。システムのパフォーマンスを管理できるのは、クラスタ管理者だけです。SVM管理者はこれらのタスクを実行できません。

ストレージQoSを使用したワークロード パフォーマンスの管理

ストレージQuality of Service（QoS;サービス品質）は、パフォーマンス目標の達成に伴うリスクへの対応に役立ちます。ストレージQoSを使用してワークロードに対するスループットを制限し、ワークロードのパフォーマンスを監視します。パフォーマンスに関する問題に対処するために事後対応としてワークロードを制限することも、パフォーマンスに関する問題を防ぐために事前対応としてワークロードを制限することもできます。

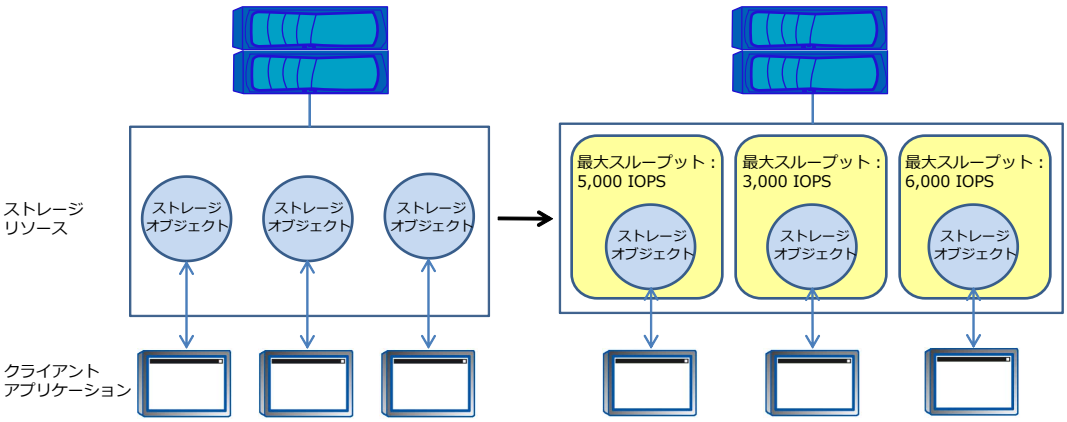
ストレージQoSは、最大8ノードまでのクラスタでサポートされます。

ワークロードとは、次のいずれかの種類のストレージ オブジェクトに対する入出力（I/O）操作のことです。

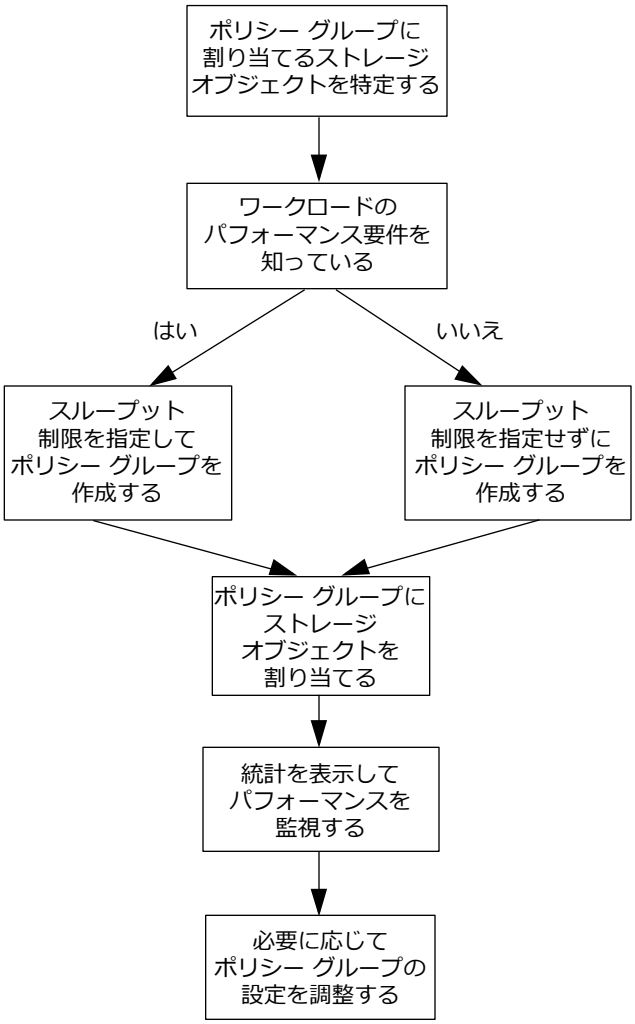
- FlexVolを備えたSVM
- FlexVol
- LUN
- ファイル（主に仮想マシン）

ストレージ オブジェクトをポリシー グループに割り当てて、ワークロードの制御と監視を行います。ワークロードを制御せずに監視することもできます。

次の図は、ストレージQoSの使用前と使用後の環境の例を示しています。左の図では、複数のワークロードがI/Oを送信するためにクラスタ リソースを奪い合っています。これらのワークロードのパフォーマンスは「ベスト エフォート」によって決まるため、パフォーマンスを予測することは困難です（たとえば、あるワークロードのパフォーマンスが高くなると、他のワークロードが悪影響を受ける場合があります）。右の図は、同じワークロードをポリシー グループに割り当てた状態を表しています。ポリシー グループによって最大スループット制限が適用されています。



次のワークフローは、ストレージQoSを使用してワークロードを制御および監視する方法を示しています。



関連タスク

ワークロード パフォーマンスの制御と監視(250ページ)

ストレージQoSの仕組み

ストレージQoSは、クライアント処理(SANおよびNASデータ要求)とシステム処理のスロットリングと優先順位付けを行うことで、ポリシー グループに割り当てられるワークロードを制御します。

ポリシー グループとは

ポリシー グループは、1つ以上のワークロードと、ポリシー グループ内のすべてのワークロードに一律に適用されるパフォーマンス制限で構成されます。次の2種類のポリシー グループがあります。

ユーザ定義のポリシー グループ

入出力(I/O)要求のスロットリングにより、ポリシー グループに属するストレージ オブジェクトに最大スループットを適用します。

システム定義のポリシー グループ

クラスタが実行する内部処理を管理します。

両方の種類のポリシー グループのパフォーマンス データを表示できます。システム定義のポリシー グループの名前はアンダースコアで開始されます。

ワークロードとは

ワークロードとは、クラスタが実行する処理です。次の2種類のワークロードがあります。

ユーザ定義のワークロード

ポリシー グループに属するストレージ オブジェクトへのクライアントからの入出力（I/O）処理です。ストレージ オブジェクトとしては次のものがあります。

- FlexVolを備えたSVM
- FlexVol
- LUN
- ファイル（主に仮想マシン）

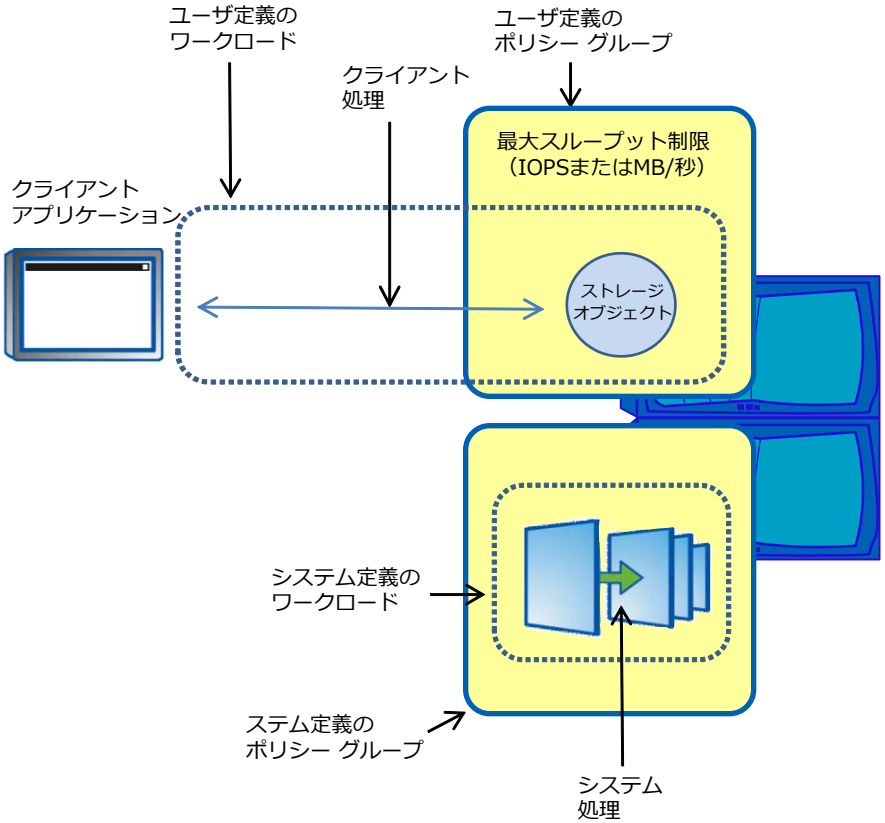
ポリシー グループに割り当てられていないストレージ オブジェクトに対するI/Oは、「ユーザのデフォルト」のワークロードに属します。

システム定義のワークロード

クラスタが実行する内部処理です。ストレージQoSは、特定のシステム処理を制御して、クライアント処理への影響を防ぎます。対象となるのは、ストレージ効率化処理やデータレプリケーション処理などです。

両方の種類のワークロードのパフォーマンス データを表示できます。システム定義のワークロードの名前はアンダースコアで開始されます。

次の図は、ユーザ定義のポリシー グループとシステム定義のポリシー グループを示しています。ユーザ定義のポリシー グループはユーザ定義のワークロード、つまりアプリケーションからストレージ オブジェクトへのクライアント処理を制御します。システム定義のポリシー グループは、システム定義のワークロード、つまりクラスタが実行する内部システム処理を制御します。



最大スループット制限の仕組み

ストレージQoSポリシー グループには、1つのサービス レベル目標、つまり最大スループット制限を指定できます。最大スループット制限はIOPSまたはMbps単位で定義します。ポリシー グループ内のすべてのワークロードのスループットの合計がこの値を超えることはできません。

あるポリシー グループに最大スループットを指定すると、ストレージQoSは、そのポリシー グループ内のすべてのワークロードの合計スループットがこの最大スループットを超えることがないように、クライアント処理を制御します。

たとえば、「untested_apps」というポリシー グループを作成し、最大スループットとして300Mbpsを指定したとします。このポリシー グループに3つのボリュームを割り当てます。3つのボリュームを合わせたスループットが300Mbpsを超えることはできません。

注: あるポリシー グループ内の各ワークロードの合計スループットは、最大スループットを10%までは超えることができます。このような例外的な状況は、あるワークロードのスループットが急激に変化（「*ワークロードの集中*」）した場合に発生することがあります。

最大スループットの指定については、次の点に注意してください。

- スループット制限は、ストレージ オブジェクトにアクセスするすべてのクライアントに適用される。
- クラスタの利用率が十分に上がらないことがあるため、低すぎる設定は避ける。
- 制限を適用しないワークロードに対して確保しておくべき最低限のスループット量を考慮する。
  たとえば、クリティカルでないワークロードを制限することにより、クリティカルなワークロードに必要なスループットを確保できます。
- スループットの増加に対応できる余地を残す。
  たとえば、平均的な利用率が500IOPSの場合は、制限を1,000IOPSに指定することが考えられます。

ワークロードのスロットルが、同じクライアントでスロットルを適用していないワークロード要求に与える影響

状況によっては、ワークロードにスロットル（ストレージ オブジェクトへのI/O）を適用すると、同じクライアントからI/O要求が送られた場合に、スロットルを適用していないワークロードのパフォーマンスに影響が及ぶことがあります。

あるクライアントから複数のストレージ オブジェクトにI/O要求が送信され、そのストレージ オブジェクトの一部がストレージQoSポリシー グループに属している場合、ストレージQoSポリシー グループに属していないストレージ オブジェクトのパフォーマンスがデグレードすることがあります。このようなパフォーマンス低下は、バッファや未処理要求など、クライアント側のリソースが共有されていることが原因で生じます。

たとえば、同じホスト上で複数のアプリケーションが使用されている場合や、仮想マシンが実行されている場合などの構成で影響が生じることがあります。

こうした状況は、設定された最大スループット制限が低い場合やクライアントからのI/O要求数が多すぎる場合などに生じる可能性があります。

このような状況が生じる場合は、最大スループット制限を高くするか、アプリケーションを分離して、クライアント リソースの争奪が起きないようにします。

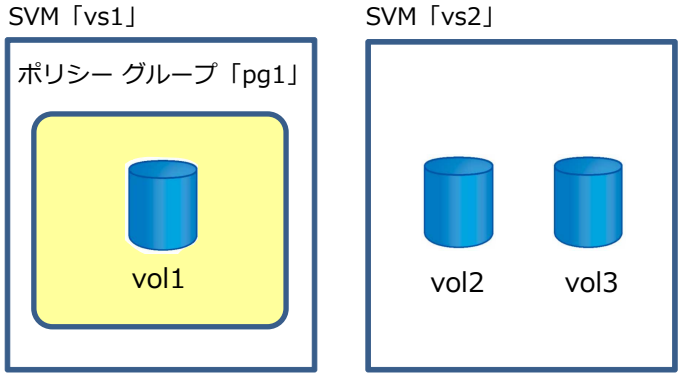
ポリシー グループへのストレージ オブジェクトの割り当てに関するルール

ストレージQoSポリシー グループにストレージ オブジェクトを割り当てる際のルールを把握しておく必要があります。

ストレージ オブジェクトとポリシー グループは同じSVMに属していなければならない

ストレージ オブジェクトは、ポリシー グループが属しているStorage Virtual Machine（SVM）に含まれている必要があります。ポリシー グループが属するSVMは、ポリシー グループを作成するときに指定します。同じSVMに複数のポリシー グループを作成することができます。

次の図では、ポリシー グループpg1がSVM vs1に属しています。ボリュームvol2とボリュームvol3は別のSVMに含まれているため、これらのボリュームをポリシー グループpg1に割り当てることはできません。

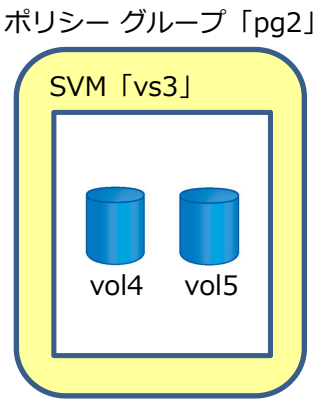


ネストされたストレージ オブジェクトはポリシー グループに追加できない

下位のオブジェクトまたは子オブジェクトがポリシー グループに属している場合、そのストレージ オブジェクトをポリシー グループに割り当てることはできません。次の表に、詳しく記載します。

割り当て内容	以下のオブジェクトはポリシー グループに割り当てできない
SVM	SVMに含まれているストレージ オブジェクト
ボリューム	そのボリュームを含むSVM / 子LUN / ファイル
LUN	そのLUNを含むボリュームまたはSVM
ファイル	そのファイルを含むボリュームまたはSVM

次の図では、SVM vs3がポリシー グループpg2に割り当てられています。ストレージ階層のオブジェクト（SVM vs3）がポリシー グループに割り当てられているため、ボリュームvol4またはボリュームvol5をポリシー グループに割り当てることはできません。



一部のボリューム タイプはストレージQoSでサポートされない

FlexVolはポリシー グループに割り当てることができます。Infinite VolumeはストレージQoSではサポートされていません。

ストレージQoSでサポートされないFlexVolの種類は次のとおりです。

- データ保護ミラー
- 負荷共有ミラー
- ノードのルート ボリューム

ストレージQoSの使用時にワークロード パフォーマンスを監視する方法

適切なスループット制限を決定するには、クラスタ側からパフォーマンスを監視する必要があります。ホスト上にあるツールを使用して、パフォーマンスを監視することは避けてください。ホストからの報告とクラスタからの報告で結果が異なることがあります。

ストレージQoSにより、クラスタに対するI/Oが制限されます。クラスタで生じるI/O速度とアプリケーションで生じるI/O速度が異なる場合があります。たとえば、アプリケーションからの読み取りがファイルシステムのバッファ キャッシュまでを対象とし、クラスタまで到達しないことがあります。

こうした動作の違いがあるため、パフォーマンスの監視は、ホスト側のツールではなく、クラスタ側から実施する必要があります。

サポートされるストレージQoSポリシー グループ数とワークロード数

クラスタごとに最大3,500個のポリシー グループを作成できます。これらのポリシー グループには、最大10,000個のストレージ オブジェクトを割り当てることができます。ポリシー グループにストレージ オブジェクトを割り当てると、ワークロードが作成されます。その他の制限はありません。

ワークロード パフォーマンスの制御と監視

ワークロードのパフォーマンスの制御と監視は、パフォーマンスの問題を解決し、パフォーマンスの目標が定義されているワークロードを事前に制限するために行います。

開始する前に

- *最大スループット制限の仕組み*(248ページ)を理解している必要があります。
- *QoSポリシー グループへのストレージ オブジェクトの割り当てに関するルール*(249ページ)を理解している必要があります。

タスク概要

ストレージQoSは、最大8ノードまでのクラスタでサポートされます。

手順

1. ストレージQoSポリシー グループに割り当てるストレージ オブジェクトを識別します。

   すべてのポリシー グループに同じタイプのストレージ オブジェクトを割り当てることを推奨します。

2. `qos policy-group create`コマンドを使用して新しいポリシー グループを作成するか、`qos policy-group modify`コマンドを使用して既存のポリシー グループを変更します。

   最大スループット制限の指定は、ポリシー グループの作成時に行うか、ワークロードを監視してから行うことができます。ワークロードの監視を先に行うと、設定する必要がある制限の特定に役立ちます。最大スループットを指定しない場合、ワークロードのパフォーマンスはベストエフォートになります。

   例

   次のコマンドでは、最大スループットが5,000 IOPSのポリシー グループpg-vs1が作成されます。

   ```
   cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
   throughput 5000iops
   ```

   例

   次のコマンドでは、最大スループットが未指定のポリシー グループpg-app2が作成されます。

   ```
   cluster1::> qos policy-group create pg-app2 -vserver vs2
   ```

3. ストレージ オブジェクトをポリシー グループに割り当てるには、SVM、ボリューム、LUN、またはファイルのcreateまたはmodifyコマンドを使用します。

   例

   次のコマンドでは、SVM vs1をポリシー グループpg-vs1に割り当てます。

   ```
   cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
   ```

   例

   次のコマンドでは、ボリュームapp2を作成し、これをポリシー グループpg-app2に割り当てます。

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr2 -
   qos-policy-group pg-app2
   ```

4. パフォーマンスの目標を満たしているかどうかを識別するには、`qos statistics`コマンドを使用して、ポリシー グループとワークロードのパフォーマンスを監視します。

   パフォーマンスはクラスタ側から監視する必要があります。ホスト上にあるツールを使用して、パフォーマンスを監視することは避けてください。

   例

   次のコマンドでは、ポリシー グループのパフォーマンスが表示されます。

   ```
   cluster1::> qos statistics performance show
   Policy Group           IOPS      Throughput   Latency
   -------------------- -------- --------------- ----------
   -total-                 12316       47.76MB/s  1264.00us
   ```

```
pg_app2                    7216        28.19MB/s   420.00us
pg_vs1                     5008        19.56MB/s     2.45ms
_System-Best-Effort          62        13.36KB/s     4.13ms
_System-Background           30            0KB/s        0ms
```

例

次のコマンドでは、ワークロードのパフォーマンスが表示されます。

```
cluster1::> qos statistics workload performance show
Workload           ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-               -    12320        47.84MB/s  1215.00us
app2-wid7967       7967     7219        28.20MB/s   319.00us
vs1-wid12279      12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS      14       55        10.92KB/s   236.00us
_Scan_Backgro..    5688       20            0KB/s        0ms
```

5. 必要に応じて、`qos policy-group modify`コマンドを使用して、ポリシー グループの最大スループット制限を調整します。

例

次のコマンドでは、ポリシー グループpg-app2の最大スループットが20MB/秒に変更されます。

```
cluster1::> qos policy-group modify pg-app2 -max-throughput 20mb/s
```

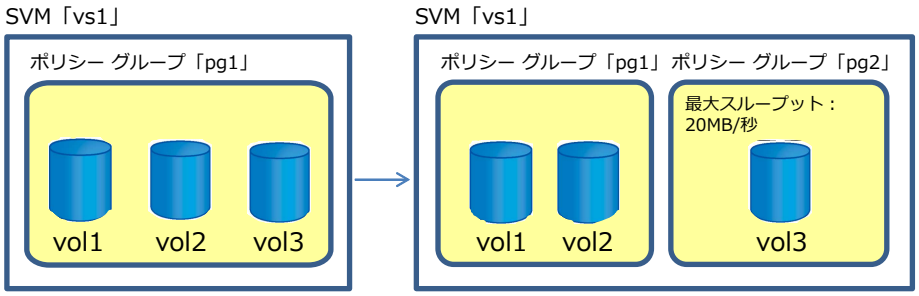
関連参照情報

ワークロードの制御および監視用コマンド(255ページ)

例:ワークロードの分離

あるワークロードのパフォーマンスが必要以上に高いためにほかのワークロードのパフォーマンスに影響が出ることがあります。この問題に対応するには、ストレージQoSを使用してそのワークロードにスロットルを適用します。これにより、クラスタ リソースがほかのワークロードに解放されます。この例では、ワークロードはボリューム レベルにあります。

次の図は、3つのボリュームを示したものです。各ボリュームをポリシー グループpg1に配置し、最大スループットは設定しません。これはまずワークロードを監視したいためです。するとワークロードの監視中に、vol3のパフォーマンスがほかのワークロードよりも高いことが判明しました。このワークロードのリソース消費を制限するには、vol3をポリシー グループpg2に移動します。これにより、ほかのワークロードの速度が上ります。



CLIを使用したワークロードの分離

次のコマンドでは、最大スループットが未指定のポリシー グループが作成されます。

```
cluster1::> qos policy-group create pg1 -vserver vs1
```

次のコマンドでは、3つの既存のボリュームがポリシー グループに割り当てられます。

```
cluster1::> volume modify vol1,vol2,vol3 -vserver vs1 -qos-policy-
group pg1
```

次のコマンドでは、ワークロードのパフォーマンス データが表示されます。

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-               -    16645        64.77MB/s   411.00us
vol3-wid12459    12459    10063        39.31MB/s   410.00us
vol2-wid1445      1445     3505        13.69MB/s   437.00us
vol1-wid11344    11344     3007        11.75MB/s   277.00us
_USERSPACE_APPS     14       40        26.40KB/s     8.68ms
_Scan_Backgro..   5688       30            0KB/s        0ms
```

vol3ワークロードのパフォーマンスが高いため、ほかのワークロードはパフォーマンス目標に達することができません。そこで、このワークロードを最大スループットを指定した新しいポリシー グループに移すことにします。

次のコマンドでは、最大スループットを指定したポリシー グループが作成されます。

```
cluster1::> qos policy-group create pg2 -vserver vs1 -max-
throughput 20mb/s
```

次のコマンドでは、作成した新しいポリシー グループにvol3が割り当てられます。

```
cluster1::> volume modify vol3 -vserver vs1 -qos-policy-group pg2
```

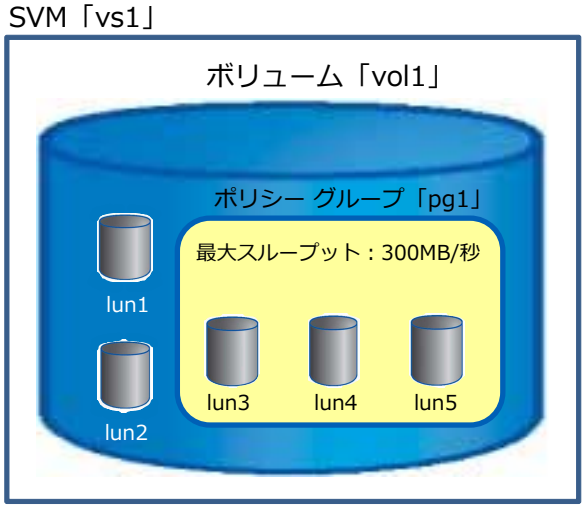
ワークロードのパフォーマンス データを表示すると、vol3を制限したことにより、ほかのワークロードのパフォーマンスが向上したことがわかります。

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-               -    15691        61.17MB/s  1001.00us
vol1-wid11344    11344     6016        23.50MB/s   355.00us
vol3-wid12459    12459     5133        20.05MB/s     2.42ms
vol2-wid1445      1445     4462        17.43MB/s   253.00us
_USERSPACE_APPS     14       50       204.20KB/s   355.00us
_Scan_Backgro..   5688       30            0KB/s        0ms
```

例：非クリティカルなワークロードに制限をプロアクティブに設定する

クリティカルなワークロードで最適のパフォーマンスが達成できるようにするには、ストレージQoSを使用して非クリティカルなワークロードに対するスループットを制限します。この例では、ワークロードはLUNレベルにあります。

次の図は、ボリューム「vol1」にある5つのLUNを示したものです。lun1とlun2は、クリティカルなアプリケーションに使用されます。lun3、lun4、およびlun5は、非クリティカルなアプリケーションに使用されます。lun1とlun2ではベスト エフォートのパフォーマンスを確保したいため、lun3、lun4、およびlun5を最大スループット制限のあるポリシー グループにそれぞれ割り当てることにより制限します。



CLIを使用した非クリティカルなワークロードへの制限の設定

次のコマンドでは、最大スループットが300MB/秒のポリシー グループが作成されます。

```
cluster1::> qos policy-group create pg1 -vserver vs1 -max-
throughput 300mb/s
```

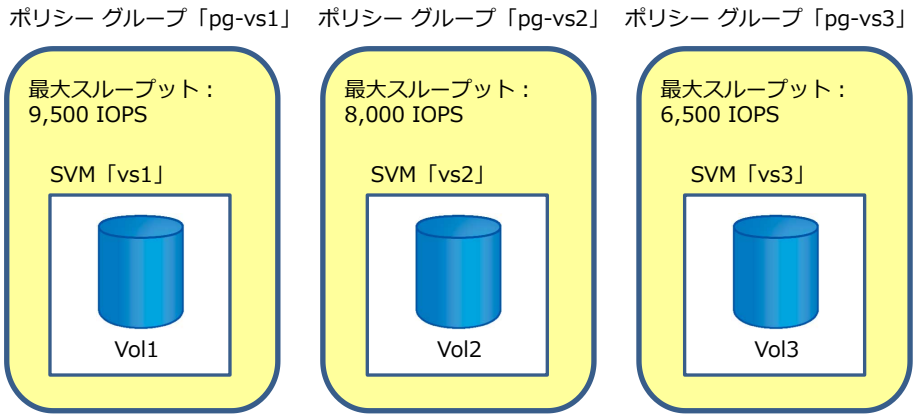
次のコマンドでは、新たに3つのLUNがポリシー グループに割り当てられます。

```
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun3 -size
50GB -ostype windows_2008 -qos-policy-group pg1
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun4 -size
50GB -ostype windows_2008 -qos-policy-group pg1
cluster1::> lun create -vserver vs1 -volume vol1 -lun lun5 -size
50GB -ostype windows_2008 -qos-policy-group pg1
```

例：共有ストレージ インフラのワークロードに制限をプロアクティブに設定する

共有ストレージ インフラを使用している場合、個々のワークロードで必要以上に高いパフォーマンスが出ていないかの確認が必要な場合があります。この例では、ストレージQoSポリシー グループを使用して各ワークロード（いずれもStorage Virtual Machine（SVM）レベル）に制限を設定します。

次の図は、3台のSVMがそれぞれ個別のポリシー グループに割り当てられた状態を示したものです。各SVMを1つのポリシー グループに割り当てます。これは、各ワークロードのパフォーマンス オブジェクトがわかっており、特定のテナントが他のテナントからシステム リソースを奪うことがないようにするためです。



CLIを使用して共有ストレージ インフラ内のワークロードに制限を設定

次のコマンドでは、最大スループット制限のある3つのポリシー グループが作成されます。

```
cluster1::> qos policy-group create pg-vs1 -vserver vs1 -max-
throughput 9500iops
cluster1::> qos policy-group create pg-vs2 -vserver vs2 -max-
throughput 8000iops
cluster1::> qos policy-group create pg-vs3 -vserver vs3 -max-
throughput 6500iops
```

次のコマンドでは、3台の既存のSVMがポリシー グループに割り当てられます。

```
cluster1::> vserver modify -vserver vs1 -qos-policy-group pg-vs1
cluster1::> vserver modify -vserver vs2 -qos-policy-group pg-vs2
cluster1::> vserver modify -vserver vs3 -qos-policy-group pg-vs3
```

ワークロードの制御および監視用コマンド

コマンドを使用して、ストレージQoSポリシー グループの管理、ポリシー グループへのストレージ オブジェクトの割り当て、ポリシー グループに属するストレージ オブジェクトの識別、ワークロードとポリシー グループのパフォーマンスの監視を行うことができます。

- *ポリシー グループの管理用コマンド*（255ページ）
- *ポリシー グループへのストレージ オブジェクトの割り当て用コマンド*（256ページ）
- *ポリシー グループに属するストレージ オブジェクトの確認用コマンド*（256ページ）
- *ポリシー グループのパフォーマンスの監視用コマンド*（256ページ）
- *ワークロードのパフォーマンスの監視用コマンド*（257ページ）

これらのコマンドの詳細については、マニュアル ページを参照してください。

ポリシー グループの管理用コマンド

`qos policy-group`コマンドを使用して、ポリシー グループを管理します。ポリシー グループを使用して、ワークロードのパフォーマンスを制御および監視します。

状況	使用するコマンド
ポリシー グループの作成	`qos policy-group create`

状況	使用するコマンド
ポリシー グループの変更	`qos policy-group modify`
ポリシー グループの名前変更	`qos policy-group rename`
ユーザ定義のポリシー グループをすべて表示	`qos policy-group show`
ポリシー グループの削除	`qos policy-group delete`

ポリシー グループへのストレージ オブジェクトの割り当て用コマンド

ストレージ オブジェクトの`create`コマンドまたは`modify`コマンドを使用して、ストレージ オブジェクトをポリシー グループに割り当てます。またストレージ オブジェクトをポリシー グループに割り当てることで、ワークロードのパフォーマンスの制御と監視を行います。

注: ストレージ オブジェクトをポリシー グループから削除するには、`-qos-policy-group`パラメータを**none**に設定します。

割り当てる項目	`-qos-policy-group`パラメータを指定して使用するコマンド
FlexVolを備えたSVM	`vserver modify`
新しいFlexVol	`volume create`
既存のFlexVol	`volume modify`
新しいFlexCloneボリューム	`volume clone create`
新しいLUN	`lun create`
既存のLUN	`lun modify`
ファイル	`volume file modify`
ファイルまたはLUNの新しいクローン	`volume file clone create`

ポリシー グループに属するストレージ オブジェクトの確認用コマンド

ストレージ オブジェクトの`show`コマンドを使用して、ポリシー グループに属するストレージ オブジェクトを確認します。

確認する項目	`-qos-policy-group`パラメータを指定して使用するコマンド
ポリシー グループに属するFlexVolを備えたSVM	`vserver show`
ポリシー グループに属するFlexVol	`volume show`
ポリシー グループに属するLUN	`lun show`

ポリシー グループとワークロードのパフォーマンスの監視用コマンド

次のコマンドを使用して、ポリシー グループとワークロードのパフォーマンスをIOPS、スループット、およびレイテンシの観点から監視します。

表示する項目	使用するコマンド
1つのポリシー グループ内の全ワークロードの全体的なパフォーマンス	`qos statistics performance show`

表示する項目	使用するコマンド
個々のワークロードのパフォーマンス	`qos statistics workload performance show`

ポリシー グループのパフォーマンスの高度な監視用コマンド

次のコマンドを使用して、ポリシー グループの詳細なパフォーマンス データを表示します。これらのコマンドでは、1つのポリシー グループ内の全ワークロードの全体的なパフォーマンスが表示されます。

表示するデータ	使用するコマンド
クラスタ内のクライアントのロード（要求サイズ、読み取りの割合、同時実行について）	`qos statistics characteristics show`
Data ONTAPサブシステム全体のレイテンシ（応答時間が遅い原因の特定に役立つ）	`qos statistics latency show`
CPU利用率	`qos statistics resource cpu show`
ディスク利用率（読み取りおよび書き込み処理中にディスク上で費やされた時間の割合について）	`qos statistics resource disk show`

ワークロードのパフォーマンスの高度な監視用コマンド

次のコマンドを使用して、個々のワークロードの詳細なパフォーマンス データを表示します。

表示するデータ	使用するコマンド
クラスタ内のクライアントのロード（要求サイズ、読み取りの割合、同時実行について）	`qos statistics workload characteristics show`
Data ONTAPサブシステム全体のレイテンシ（応答時間が遅い原因の特定に役立つ）	`qos statistics workload latency show`
CPU利用率	`qos statistics workload resource cpu show`
ディスク利用率（読み取りおよび書き込み処理中にディスク上で費やされた時間の割合について）	`qos statistics workload resource disk show`

RAVEを使用したヒストグラムベースの予測

Data ONTAP 8.2.1以降、WAFLのSpeculative Read-Ahead Engine（RAVE;推測的な先読みエンジン）では、ファイルへの過去のユーザの読み取り要求に関するデータも一時的に収集し、この情報に基づいて、将来の読み取り要求をインテリジェントに推測できるようになりました。以前のリリースでは、この推測は現在のユーザI/O情報にのみ基づいていました。

clustered Data ONTAPを実行しているシステムでは、QoS先読み設定の一部としてヒストグラムベースの予測を有効にし、QoSワークロードに割り当てることができます。`qos settings read-ahead create` | `modify` *`read_ahead_setting_name`* `-use-histogram` **`true`** | **`false`**コマンドを使用して、この機能を有効または無効にできます。`qos workload modify -read-ahead` *`read_ahead_setting_name`* `-workload` *`workload_name`*コマンドを使用して、先読み設定を任意のワークロードに割り当てることができます。

WAFLキャッシュ メモリの増加

WAFL外部キャッシュは追加のWAFLキャッシュ メモリを提供し、ディスクの読み取り回数を減らすことでストレージ システムのパフォーマンスを向上させます。ユーザ データ ブロックをキャッシュする方法は、キャッシング モジュールの動作モードを変更することで制御できます。デフォルトのモード（通常のユーザ データ ブロック）のほかに、メタデータ モードとロープライオリティ ブロック モードを選択できます。

キャッシング モジュールの取り付け後に、WAFL外部キャッシュ機能が有効になっていることを確認する必要があります。

注: Data ONTAP 8.1以降を実行しているシステムの場合、WAFL外部キャッシュを使用するために別途ライセンスが必要になることはありません。

注: すべてのシステムにキャッシング モジュールが搭載されているわけではありません。そのため、すべてのシステムでWAFL外部キャッシュ機能を使用できるわけではありません。

WAFL外部キャッシュでは、SSDで構成されるRAIDグループに格納されているデータはキャッシュされません。

ハイアベイラビリティ（HA）構成のストレージ システムでWAFL外部キャッシュを使用する場合は、両方のノードで同じWAFL外部キャッシュ オプションを指定する必要があります。そうしないと、テイクオーバー時に、テイクオーバー先のノードにWAFL外部キャッシュがないことが原因でパフォーマンスが低下する可能性があります。

WAFL外部キャッシュの管理に使用できるData ONTAPオプションに加えて、キャッシング モジュールを完全消去するための診断コマンドも使用できます。詳細については、*『診断ガイド』*を参照してください。

Flash PoolアグリゲートとFlash Cacheの比較

Flash PoolテクノロジとFlash Cacheファミリー（Flash CacheとFlash Cache 2）は、どちらも高性能なキャッシュを提供してストレージのパフォーマンスを向上させるモジュールです。ただし、これらの2つのモジュールはそれぞれ特徴が異なるため、その違いを理解したうえで選択することが重要です。

同じシステムで両方のモジュールを使用することも可能です。ただし、Flash Poolアグリゲートに関連付けられたボリュームに格納されたデータはFlash Cacheではキャッシュされません。

基準	Flash Poolアグリゲート	Flash Cache
適用範囲	特定のアグリゲート	ノードに割り当てられたすべてのアグリゲート
サポートされているキャッシュ タイプ	読み取りおよび書き込み	読み取り
テイクオーバーの実行中および実行後のキャッシュ データの利用	利用可能。計画的テイクオーバーまたは計画外テイクオーバーによる影響はありません。	テイクオーバーの実行中はキャッシュ データを利用できません。計画的テイクオーバーのギブバック後、以前のキャッシュ データのうち引き続き有効なデータは自動的に再度キャッシュされます。
ストレージ コントローラにPCIeスロットが必要か	いいえ	はい
圧縮されたブロックがキャッシュされるか	はい	いいえ

基準	Flash Poolアグリゲート	Flash Cache
アレイLUNでサポートされるか	いいえ	はい

Flash Poolアグリゲートの詳細については、*『clustered Data ONTAP物理ストレージ管理ガイド』*を参照してください。

WAFL外部キャッシュの有効化と無効化

キャッシング モジュール（Performance Acceleration Module、Flash Cacheモジュール、Flash Cache 2モジュール）が搭載されているストレージ システムでは、WAFL外部キャッシュ機能を有効または無効にすることができます。キャッシング モジュールの取り付け後に、WAFL外部キャッシュ機能が有効になっていることを確認する必要があります。

タスク概要

`flexscale.enable`オプションにより、WAFL外部キャッシュ機能を有効化または無効化します。ストレージ システムにキャッシング モジュールがインストールされていない場合は、`flexscale.enable`オプションによってPredictive Cache Statistics（PCS;予測キャッシュ統計情報）を有効または無効にします。PCSは、キャッシング モジュールをサポートするプラットフォームでサポートされます。

Data ONTAP 8.1以降を実行しているシステムの場合、WAFL外部キャッシュを使用するために別途ライセンスが必要になることはありません。PCSの場合、ライセンスは必要ありません。

次のコマンドはノードシェルから実行できます。ノードシェルにアクセスするには、`system node run`コマンドを使用します。詳細については、マニュアル ページを参照してください。

手順

1. WAFL外部キャッシュが有効か無効かを確認するには、次のコマンドを入力します。

   `options flexscale.enable`

2. WAFL外部キャッシュを有効または無効にするには、次のコマンドを入力します。

   `options flexscale.enable {on|off}`

PCSでエミュレートされるキャッシュ サイズの変更

ストレージ システムでPredictive Cache Statistics（PCS）が有効になっている場合は、PCSでエミュレートするキャッシュのサイズを変更して、キャッシング モジュールによってワークロードの処理がどう変わるかをより正確に予測することができます。設定可能なキャッシュ サイズは、コントローラのメモリ容量によって異なります。

開始する前に

PCSが有効になっている必要があります。

タスク概要

`flexscale.pcs_size`オプションを使用して、PCSでエミュレートされるキャッシュ サイズを変更します。このオプションは、PCSが有効になっており（`flexscale.enable`を**on**に設定）、ストレージ システムにキャッシング モジュールが搭載されていない場合にのみ使用します。

ノードシェルにアクセスするには、`system node run`コマンドを使用します。次のコマンドはノードシェルから実行できます。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドを入力して、PCSでエミュレートされる現在のキャッシュ サイズを表示します。

   options flexscale.pcs_size

   デフォルト値は、コントローラのメモリ容量に基づいて自動的に選択されます。

2. 次のコマンドを入力して、PCSでエミュレートされるキャッシュのサイズを変更します。

   options flexscale.pcs_size *integer*

   16～16383の整数を指定できます。

関連タスク

WAFL外部キャッシュの有効化と無効化（259ページ）

PCSでエミュレートされるキャッシュの高解像度サンプリングの有効化と無効化

ストレージ システムでPredictive Cache Statistics（PCS）が有効になっている場合は、PCSでエミュレートされるキャッシュの高解像度サンプリングを有効または無効にできます。高解像度サンプリングを使用すると、小規模なホット スポットを含むワークロードをより正確に測定できるようになります。

開始する前に

PCSが有効になっている必要があります。

タスク概要

`flexscale.pcs_high_res`オプションを使用して、PCSでエミュレートされるキャッシュの高解像度サンプリングを有効または無効にします。このオプションは、PCSが有効になっており（`flexscale.enable`を**on**に設定）、ストレージ システムにキャッシング モジュールが搭載されていない場合にのみ使用します。

ノードシェルにアクセスするには、`system node run`コマンドを使用します。次のコマンドはノードシェルから実行できます。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドを入力して、PCSのキャッシュの高解像度サンプリングを有効または無効にします。

   options flexscale.pcs_high_res {on|off}

   デフォルト値は**off**で、ほとんどのワークロードには十分です。この値を**on**に設定すると、小規模なホット スポットを含むワークロードをより正確に測定できるようになります。

関連タスク

WAFL外部キャッシュの有効化と無効化（259ページ）

標準ユーザ データ ブロックのキャッシング

標準ユーザ データ ブロックをキャッシングする場合、WAFL外部キャッシュはこの設定のバッファ キャッシュ ポリシーを**keep**とみなして、外部キャッシュに標準ユーザ データ ブロックを保存します。

タスク概要

次のコマンドはノードシェルから実行できます。ノードシェルにアクセスするには、`system node run`コマンドを使用します。詳細については、マニュアル ページを参照してください。

手順

1. 標準ユーザ データ ブロックのキャッシングを有効または無効にするには、次のコマンドを入力します。

   `options flexscale.normal_data_blocks {on|off}`

   デフォルト値は**on**です。

   `flexscale.normal_data_blocks`オプションが**on**に設定されている場合、WAFL外部キャッシュはこの設定のバッファ キャッシュ ポリシーを**keep**とみなして、拡張キャッシュに標準ユーザ データ ブロックを保存します。

   このオプションが**`off`**に設定されている場合は、メタデータ ブロックのみがキャッシングされます。

優先度が低いユーザ データ ブロックのキャッシング

WAFL外部キャッシュでは、通常は格納されない、優先度が低いユーザ データ ブロックをキャッシングすることができます。優先度が低いブロックとしては、通常再利用されない多量のシーケンシャル スキャンで読み取られるブロックや、iSCSI、NFS、またはCIFSプロトコルを通じてストレージ システムに書き込まれたブロックなどがあります。

タスク概要

WAFL外部キャッシュ メモリに適合する負荷、および書き込み後の読み取りや大規模な順次読み取りによる負荷が存在する場合は、優先度の低いユーザ データ ブロックをキャッシングすると便利です。

優先度が低いユーザ データ ブロックをキャッシングできるのは（`flexscale.lopri_blocks`を**on**に設定）、標準ユーザ データ ブロックもキャッシングする場合のみです（`flexscale.normal_data_blocks`を**on**に設定）。

次のコマンドはノードシェルから実行できます。ノードシェルにアクセスするには、`system node run`コマンドを使用します。詳細については、マニュアル ページを参照してください。

手順

1. 優先度が低いユーザ データ ブロックをキャッシングするかどうかを制御するには、次のコマンドを入力します。

   `options flexscale.lopri_blocks {on|off}`

   デフォルト値は**`off`**です。

   オプションを**on**に設定すると、優先度の低いユーザ データ ブロックがキャッシングされます。

システム メタデータのみのキャッシング

ストレージ システムの作業セットのサイズが非常に大きい場合は（大規模なメール サーバなど）、標準ユーザ データ ブロックのキャッシングと優先度の低いユーザ データ ブロックのキャッシングを両方ともオフにして、WAFL外部キャッシュ メモリにシステム メタデータのみをキャッシングすることができます。

タスク概要

`flexscale.normal_data_blocks`と`flexscale.lopri_blocks`の両方を**`off`**に設定して、システム メタデータのみをキャッシングする場合、WAFL外部キャッシュはこの設定のバッファ キャッシュ ポリシーを**reuse**とみなして、標準データ ブロックまたは優先度の低いブロックを外部キャッシュに保存しません。

次のコマンドはノードシェルから実行できます。ノードシェルにアクセスするには、`system node run`コマンドを使用します。詳細については、マニュアル ページを参照してください。

手順

1. 標準ユーザ データ ブロックのキャッシングをオフにするには、次のコマンドを入力します。

   options flexscale.normal_data_blocks off

2. 優先度の低いユーザ データ ブロックのキャッシングをオフにするには、次のコマンドを入力します。

   options flexscale.lopri_blocks off

ランダム ライト ワークロード ブロックのキャッシュの有効化と無効化

書き込みブロックは、ブロックがディスクに書き込まれるまでメモリにキャッシュされます。書き込みブロックがディスクに書き込まれたあと、Data ONTAPでランダムとみなされる書き込みブロックをメモリからWAFL拡張キャッシュに移動すると、特定のワークロードの読み取りキャッシュ速度が向上します。

タスク概要

ランダム ライト ワークロード ブロックのキャッシュを有効にすると、Data ONTAPがランダム ブロックがディスクに書き込まれた直後にデータ ブロックを読み取るワークロードの処理速度が向上する可能性があります。

ノードシェルにアクセスするには、`system node run`コマンドを使用します。次のコマンドはノードシェルから実行できます。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドを入力して、ランダム ライト ワークロード ブロックのキャッシュを有効または無効にします。

   options flexscale.random_write_through_blocks {on|off}

先読みデータのキャッシュの有効化と無効化

シーケンシャル リード ブロック（先読みデータ）は、通常、ランダム リード ブロック用のスペースを確保するためにバッファ キャッシュからすぐに削除されます。シーケンシャル リード データをWAFL外部キャッシュに追加すると、クライアントが繰り返しアクセスするシーケンシャル データの読み取り応答時間を短縮できます。

タスク概要

ノードシェルにアクセスするには、`system node run`コマンドを使用します。次のコマンドはノードシェルから実行できます。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドを入力して、先読みデータのキャッシュを有効または無効にします。

   options flexscale.readahead_blocks {on|off}

WAFL外部キャッシュ設定の表示

Data ONTAPでは、WAFL外部キャッシュの設定情報を表示することができます。

タスク概要

次のコマンドはノードシェルから実行できます。ノードシェルにアクセスするには、`system node run`コマンドを使用します。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドを入力します。

   stats show -p flexscale

WAFL外部キャッシュの利用率およびアクセスに関する情報の表示

WAFL外部キャッシュの利用率およびアクセスに関する情報を表示したり、出力を定期的に生成したりすることができます。また、指定回数分だけ反復したあとで出力をターミネイトすることも可能です。

タスク概要

ノードシェルにアクセスするには、`system node run`コマンドを使用します。次のコマンドはノードシェルから実行できます。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドを入力します。

   stats show -p flexscale-access [-i *interval*] [-n *num*]

   - オプションを使用しない場合は、統計の1秒間のSnapshotが1つ使用されます。
   - `-i` *`interval`*を指定すると、*`interval`*秒間隔で出力が定期的に生成されます。
   - `-i`オプションと同時に`-n` *`num`*を指定すると、*`num`*回の反復後に出力はターミネイトされます。*`num`*値を指定しない場合は、ユーザがブレークを送信しないかぎり、出力は永続的に実行されます。
   - 出力を中断するには、Ctrl+Cキーを押します。

   例

   次に、`stats show -p flexscale-access`コマンドの出力例を示します。

```
Cache                                        Reads       Writes    Disk Read
Usage Hit Meta Miss Hit Evict Inval Insrt Chain Blcks Chain Blcks Replcd
   %   /s  /s   /s   %   /s    /s      /s    /s    /s    /s     /s    /s
   0  581   0   83  87    0   604   13961   579   581   218  13960   552
   0  777   0  133  85    0   121   21500   773   777   335  21494   744
   0  842   0   81  91    0  1105   23844   837   842   372  23845   812
   0  989   0  122  89    0     0   23175   981   989   362  23175   960
```

   例

   次のコマンドでは、WAFL外部キャッシュのアクセスおよび利用率に関する情報が10秒間隔で5回表示されます。

   stats show -p flexscale-access -i 10 -n 5

モジュールのFlash Cacheファミリーでのキャッシュの保持

ノードがシャットダウンされると、Flash CacheモジュールまたはFlash Cache 2モジュールからデータが提供されなくなります。ただし、WAFL外部キャッシュは、正常なシャットダウン時にキャッシュを保持し、ギブバック後に「ウォームアップ状態」のデータを提供することができます。

WAFL外部キャッシュは、正常なシャットダウン時にキャッシュをFlash Cacheモジュールに保持できます。このモジュールは、「キャッシュ再ウォームアップ」と呼ばれるプロセスを通じてキャッシュを保持します。これは、正常なシャットダウン後のシステムのパフォーマンスの維持に役立ちます。たとえば、ハードウェアの追加やソフトウェアのアップグレードのためにシステムをシャットダウンする場合があります。

キャッシュの再ウォームアップは、Flash CacheモジュールまたはFlash Cache 2モジュールが搭載されていればデフォルトで有効になります。キャッシュの再ウォームアップは、HAペアの両方のノードがData ONTAP 8.1以降を実行している場合に利用できます。

関連コンセプト

WAFLキャッシュ メモリの増加（258ページ）

キャッシュの再ウォームアップの動作

WAFL外部キャッシュは、リブート時とテイクオーバーおよびギブバック時にキャッシュの再ウォームアップ プロセスを開始します。このプロセスは、Flash CacheモジュールおよびFlash Cache 2モジュールのキャッシュを「ウォームアップ状態」に保ちます。

ストレージ システムの電源がオフになると、WAFL外部キャッシュにFlash CacheモジュールとFlash Cache 2モジュール内のデータのスナップショットが作成されます。システムの電源がオンになると、そのスナップショットを使用してキャッシュがリビルドされます。このプロセスが完了すると、キャッシュからデータを読み取れるようになります。

HA構成では、テイクオーバーおよびギブバック中にデータに最小限度の変更が加えられた場合のキャッシュの再ウォームアップの方が正常に実行できます。テイクオーバーとギブバックを開始する際、テイクオーバーのパートナーは下位のパートナーのストレージに書き込まれるデータのログを維持します。キャッシュに保存された大量のデータに変更がある場合は、ノードがオンラインに戻るとキャッシュの再ウォームアップ プロセスで再ウォームアップするデータが多くなります。その結果、キャッシュの再ウォームアップに時間がかかる場合があります。

注: WAFL外部キャッシュ機能が無効になっている場合、キャッシュの再ウォームアップは動作しません。

キャッシュの再ウォームアップを開始するイベント

ノードをシャットダウンするか、テイクオーバーとギブバックを開始する場合には、キャッシュの再ウォームアップを開始できます。

キャッシュの再ウォームアップを開始するには、次のコマンドを実行します。

- `system node halt`
- `storage failover takeover ([-ofnode] | [-bynode]) node -option takeover_option`
- `cf takeover [-node]`
- `cf takeover [-f]`

キャッシュの再ウォームアップを開始しないイベント

WAFL外部キャッシュでは、ストレージ システムがクラッシュした場合、突然の停電があった場合、または特定のコマンドを実行した場合に、キャッシュの再ウォームアップは開始されません。

次のコマンドを実行しても、キャッシュの再ウォームアップは開始されません。

- `system node halt -dump`
- `system node reboot -dump`
- `cf forcetakeover [-f]`

キャッシュの再ウォームアップ中止イベントとエラー メッセージ

キャッシュの再ウォームアップ プロセスが開始されたあと、イベントによっては、プロセス全体が中止されたり、特定のアグリゲートのプロセスが中止されたりする場合があります。キャッシュの再ウォームアップ エラーおよび重要なイベントは、すべてEMSメッセージで報告されます。

キャッシュの再ウォームアップ プロセスを中止するイベント

- WAFL外部キャッシュがSnapshotコピーを作成してからキャッシュをリビルドするまでの間に、Flash CacheまたはFlash Cache 2モジュールを追加、削除、または移動した。
- テイクオーバー ノードがクラッシュした。
- WAFL外部キャッシュがキャッシュをリビルドする間にローカル ノードがクラッシュした。
- ノードがリブートしてからWAFL外部キャッシュがキャッシュをリビルドするまでに、ノードがシャットダウンした。
- WAFL外部キャッシュがキャッシュをリビルドする前に、ノードのルート アグリゲートでSnapRestore処理を開始した。
- `wafliron`プロセスによってルート アグリゲートがマウントされた。

影響を受けるアグリゲートでキャッシュの再ウォームアップを中止するイベント

- WAFL外部キャッシュがキャッシュをリビルドする前にアグリゲートでSnapRestore処理を開始した。
- WAFL外部キャッシュがキャッシュのリビルドを開始してから20分経ってもアグリゲートがオンラインにならない。
- `wafliron`プロセスによってアグリゲートがマウントされた。

キャッシュの再ウォームアップ エラーを示すEMSメッセージ

キャッシュの再ウォームアップ プロセス中に発生したイベントの詳細は、該当するEMSメッセージに示されます。次に挙げるのは、表示される可能性があるEMSメッセージの一例です。

- extCache.rw.snap.canceled
- extCache.rw.snap.canceled
- extCache.rw.replay.canceled
- extCache.rw.replay.timeout
- extCache.rw.terminated
- extCache.rw.configChange
- extCache.rw.timeout

これらのEMSメッセージは、再ウォームアップ プロセスが完了しなかった理由を説明したり、テクニカル サポートがイベントを解釈して説明する手助けをする、情報レベルのメッセージです。通常、これらのメッセージに対処する必要はありませんが、修正措置がある場合はEMSログに記載されています。

キャッシュの再ウォームアップの有効化と無効化

キャッシュの「再ウォームアップ」は、Flash CacheモジュールまたはFlash Cache 2モジュールが搭載されていればデフォルトで有効になります。キャッシュの再ウォームアップは、必要に応じて、無効

にしてから再度有効にすることができます。この操作を行う場合は、必ずテクニカル サポートの指示に従ってください。

開始する前に

キャッシュの再ウォームアップは、次の場合に有効にすることができます。

- Flash CacheモジュールまたはFlash Cache 2モジュールがインストールされている。
- WAFL外部キャッシュ機能が有効になっている。

タスク概要

キャッシュの再ウォームアップはノード レベルで機能します。キャッシュの再ウォームアップがテイクオーバーとギブバックの過程で機能するように、すべてのノードで再ウォームアップを有効にします。

ノードシェルにアクセスするには、`system node run`コマンドを使用します。次のコマンドはノードシェルから実行できます。詳細については、マニュアル ページを参照してください。

手順

1. 次のコマンドのいずれかを入力します。

状況	使用するコマンド
キャッシュの再ウォームアップを無効にする	**`options flexscale.rewarm off`**
キャッシュの再ウォームアップを有効にする	**`options flexscale.rewarm on`**

関連タスク

WAFL外部キャッシュの有効化と無効化（259ページ）

読み取りパフォーマンスの向上

ストレージ システムの読み取りパフォーマンスは、ボリュームでの読み取り再配置を有効にすることで改善できます。読み取り再配置は、デフォルトでは無効です。

読み取り再配置とは

ランダム書き込みと大規模な複数の順次読み取りを組み合わせて実行する際の負荷については、読み取り再配置によってファイルのレイアウトを改善することで、順次読み取りパフォーマンスが向上します。読み取り再配置は、FlexVolとInfinite Volumeで有効にすることができます。

読み取り再配置では、順次読み取りが行われるファイルの部分が分析されます。関連するブロックが大きく連続していない場合、Data ONTAPはそれらのブロックをディスク上の他の場所に書き換えることによってファイル レイアウトを更新します。書き換えによってファイル レイアウトが改善されると、その後、ファイルのそのセクションを読み取るときの順次読み取りのパフォーマンスが向上します。ただし、読み取り再配置によってストレージ システムに対する負荷が高まる場合があります。

読み取り再配置は、圧縮ボリュームではサポートされていません。

読み取り再配置の管理用コマンド

volume modifyおよびvolume showコマンドを使用して、読み取り再配置を管理します。

目的	使用するコマンド
ボリューム上で読み取り再配置を有効にする	volume modifyで-read-reallocパラメータを**on**または**space-optimized**に設定する **注: space-optimized**を指定すると、Snapshotコピーがある場合にはスペースが節約されますが、それによってSnapshotコピーの読み取りのパフォーマンスが低下する可能性があります。また**space-optimized**の場合は**on**とは異なり、重複排除ボリューム内の共有ブロックが再配置されます。
ボリューム上で読み取り再配置を無効にする	volume modifyで-read-reallocパラメータを**off**に設定する
ボリューム上で読み取り再配置が有効であるか無効であるかを特定する	volume show -fields read-realloc

詳細については、マニュアル ページを参照してください。

書き込みパフォーマンスの向上

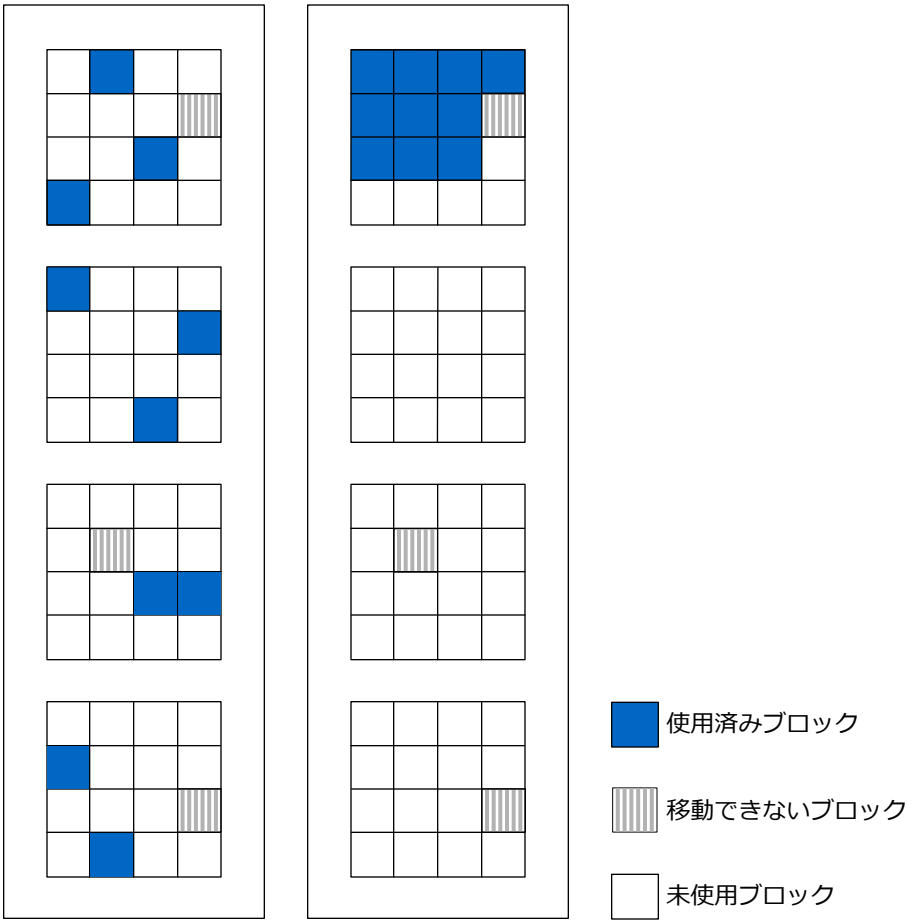
アグリゲート上での空きスペースの再配置を有効にして、書き込みパフォーマンスを向上させることができます。空きスペースの再配置を行うと、アグリゲート内の空きスペースが最適化されて書き込みパフォーマンスが向上します。デフォルトでは、空きスペースの再配置は無効になっています。

空きスペースの再配置による空きスペースの最適化方法

空きスペースの再配置は、Data ONTAPがアグリゲート内のブロックにデータを書き込む直前に、そのアグリゲート内の空きスペースを最適化します。

Data ONTAPがアグリゲート内のブロックのセグメントにデータを書き込む前に、空きスペースの再配置がそれらのブロックのレイアウトを評価します。レイアウトが最適でないと、空きスペースの再配置機能によってブロックが再編成されます。ブロックを再編成すると、アグリゲート内に利用可能な隣接する空きスペースの量が増え、それによってそれらのブロックへのData ONTAPの書き込みパフォーマンスが向上します。

次の図に、空きスペースの再配置でブロックのセグメント内の空きスペースがどのように最適化されるかを示します。



空きスペース再配置実行前のブロックのセグメント

空きスペース再配置実行後のブロックのセグメント

空きスペースの再配置を有効化する状況

空きスペースの再配置は、少量のランダムな上書きと連続またはランダムな読み取りが混在するワークロードで最も効果があります。空きスペースの再配置を有効にすると、CPU利用率が上がる可能性があります。高いCPU利用率が維持されるストレージ システムでは、空きスペースの再配置を有効にしないでください。

注: `statistics show-periodic`コマンドを使用すると、CPU利用率を監視できます。

最大限の効果を得るには、新しいアグリゲートを作成したときに空きスペースの再配置を有効にします。既存のアグリゲートで空きスペースの再配置を有効にすると、Data ONTAPで空きスペースを最適化するための動作が実行される場合があります。それがシステムのパフォーマンスに一時的に影響する可能性があります。

他の再配置機能と合わせて空きスペースの再配置を使用する状況

空きスペース再配置を有効にする場合は、読み取り再配置も有効にすることを検討してください。空きスペース再配置と読み取り再配置は、データ レイアウトを最適化する相互補完的なテクノロジです。読み取り再配置はシーケンシャル読み取りのシステムを最適化し、空きスペース再配置は書き込みを最適化します。

関連コンセプト

読み取り再配置とは（266ページ）

空きスペースの再配置によって最適化が可能または不可能なアグリゲートのタイプ

空きスペースの再配置によって、特定のタイプのアグリゲート内で空きスペースが最適化されます。

空きスペースの再配置によって、次の場所で空きスペースが最適化されます。

- FlexVolまたはInfinite Volumeにストレージを提供するアグリゲート
- アグリゲート内のHDD RAIDグループ

空きスペースの再配置では、次の場所の空きスペースは最適化されません。

- アグリゲート内のSSD RAIDグループ
- ロード シェアリングやデータ保護ミラーなどの読み取り専用ボリューム

空きスペース再配置の管理用コマンド

空きスペースの再配置を管理するには、`storage aggregate modify`および`storage aggregate show`コマンドを使用します。

目的	使用するコマンド
アグリゲートで空きスペースの再配置を有効にする	`storage aggregate modify`で`-free-space-realloc`パラメータを**on**に設定する
アグリゲートで空きスペースの再配置を無効にする	`storage aggregate modify`で`-free-space-realloc`パラメータを**off**に設定する
アグリゲートで空きスペースの再配置が有効であるか無効であるかを特定する	`storage aggregate show -fields free-space-realloc`

詳細については、マニュアル ページを参照してください。

データ バックアップおよびリカバリのためのピア関係の管理（クラスタ管理者のみ）

2つのクラスタ間または2つのStorage Virtual Machine（SVM）間にピア関係を確立することで、クラスタまたはSVMのデータをバックアップおよびリカバリできるようになります。

クラスタ ピア関係の管理

クラスタ ピアの関係がある場合は、1つのクラスタから別のクラスタにデータ保護のミラーリング関係を作成したり、リモート クラスタ上のジョブを別のクラスタから管理したりできます。

関連コンセプト

SVMピア関係の管理（292ページ）

クラスタ ピアとは

クラスタ ピア機能により、2つのクラスタが連携し、それらの間でリソースを共有できるようになります。

クラスタ ピア関係の管理用コマンド

Data ONTAPには、クラスタ ピア関係を管理するための固有のコマンドが用意されています。

状況	使用するコマンド
認証されたクラスタ ピア関係を作成する	*cluster peer create* デフォルトでは、認証されたクラスタ ピア関係が作成されます。認証されていないクラスタ ピア関係を作成するには、このコマンドに`-no-authentication`パラメータを指定します。その場合、クラスタ ピア ポリシーでも、認証されていないクラスタ ピア関係を許可する必要があります。
認証されたクラスタ ピア関係を認証時間を拡張して作成する	*cluster peer create*に`-offer-expiration`パラメータを指定 このコマンドは、ピア関係の2番目のクラスタが、デフォルトの1時間以内に認証できない場合に役立ちます。
認証されていないクラスタ ピア関係を作成する	*cluster peer create*に`-no-authentication`パラメータを指定 クラスタ ピア ポリシーでも、認証されていないクラスタ ピア関係を許可する必要があります。
認証されたクラスタ ピア関係を特定のIPspaceを使用して作成する	*cluster peer create*に`ipspace`パラメータを指定
クラスタ ピア関係を削除する	*cluster peer delete*
クラスタ ピア関係のIPspaceをデフォルトのIPspaceに戻す	*cluster peer modify*の`ipspace`パラメータを**`Default`**に設定
クラスタ ピア関係を変更する	*cluster peer modify*

状況	使用するコマンド
クラスタ ピア関係のクラスタのIPspaceを変更する	*cluster peer modify*にipspaceパラメータを指定 これは、クラスタ ピア関係がすでに存在し、指定したIPspaceのクラスタ間LIFを使用する場合に便利です。
クラスタ間接続テストを開始する	*cluster peer ping*
クラスタ ピア関係に関する情報を表示する	*cluster peer show*
クラスタ ピアのTCP接続情報を表示する	*cluster peer connection show*
ローカル クラスタから見た、クラスタ ピア関係にあるノードの健常性情報を表示する	*cluster peer health show*
ピア クラスタへの未承認の認証要求に関する情報を表示する	*cluster peer offer show*
既存のクラスタ ピア関係を無効にする	*cluster peer modify*の-auth-status-adminパラメータを**revoked**に設定
異なるパスフレーズの認証を使用するようにクラスタ ピア関係を更新する	*cluster peer modify*の-auth-status-adminパラメータを**use-authentication**に設定 このコマンドを使用すると、次のいずれかのタスクを実行できます。 • 既存の認証されていないクラスタ ピア関係に認証を追加する • 取り消されたクラスタ ピア関係に認証を追加する • 認証されたクラスタ ピア関係のパスフレーズを変更する
無効になっているクラスタ ピア関係を認証なしで再確立する	*cluster peer modify*の-auth-status-adminパラメータを**no-authentication**に設定
ピア クラスタへの未承認の認証要求を変更する	*cluster peer offer modify*に-offer-expirationパラメータを指定 認証要求が期限切れになるまでに、クラスタ ピア関係を認証できないと判断した場合は、要求の有効期限を変更できます。
ピア クラスタへの未承認の認証要求をキャンセルする	*cluster peer offer cancel*
認証されていないクラスタ ピア関係が許可されているかどうか、およびパスフレーズの最小文字数を表示する	*cluster peer policy show*
認証されていないクラスタ ピア関係を許可するかどうか、およびパスフレーズの最小文字数を変更する	*cluster peer policy modify*

関連情報

Clustered Data ONTAP 8.3 Commands: Manual Page Reference

認証パスフレーズを使用したクラスタ ピアのセキュリティ

クラスタ ピア関係を作成する際、各クラスタの管理者は、パスフレーズを使用してピア関係を認証します。これは、データの送信先クラスタが、確かにデータを送信しようとしているクラスタであることを確認するための手法です。

クラスタ ピアを作成する際には、パスフレーズを使用してクラスタ ピアを相互に認証する必要があります。パスフレーズは、最初のクラスタから2番目のクラスタへのピア関係を作成するときにまず使用され、2番目のクラスタから最初のクラスタへのピア関係を作成するときにもう一度使用されます。Data ONTAPがネットワーク上でパスフレーズを交換することはありませんが、Data ONTAPがクラスタ ピア関係を作成する際、クラスタ ピア関係にある各クラスタがパスフレーズを認識します。

最初のクラスタから2番目のクラスタへのクラスタ ピア関係を作成すると、最初のクラスタは、2番目のクラスタの管理者によってクラスタ ピア関係が作成されるまで待機します。2番目のクラスタの管理者は、待機期限（デフォルトは1時間で短縮可能）内にクラスタ ピア関係を作成する必要があります。待機期限内に2番目のクラスタから最初のクラスタへのクラスタ ピア関係が作成されないと、クラスタ ピア関係は作成されず、管理者は最初からやり直す必要があります。

関連タスク

クラスタ ピア関係の作成（290ページ）

関連参照情報

クラスタ ピア関係の管理用コマンド（270ページ）

クラスタのピア関係での相互接続

情報を共有し、ピア クラスタ上の処理へのアクセスを提供するために、クラスタをクラスタ ピア関係で相互接続します。

タスク概要

クラスタを相互接続するには、ネットワーク ポートと、クラスタ間ロールで構成されたネットワーク インターフェイスが必要であり、クラスタ ピア関係を作成する必要があります。

手順

1. クラスタ ピア クラスタ間接続とは（273ページ）
2. サポートされるクラスタ ピア ネットワーク トポロジ（273ページ）
3. 指定のクラスタ間接続と未指定のクラスタ間接続の違い（276ページ）
4. クラスタ ピアリングの前提条件（277ページ）
5. データ ポートを共有する場合の考慮事項（278ページ）
6. 専用のポートを使用する場合の考慮事項（278ページ）
7. データ ポートを共有するためのクラスタ間LIFの設定（279ページ）
8. 専用のクラスタ間ポートを使用するためのクラスタ間LIFの設定（281ページ）
9. 独自のネットワークのクラスタ間ポートを使用するためのクラスタ間LIFの設定（284ページ）
10. クラスタ ピア関係の作成（290ページ）

クラスタ ピア クラスタ間接続とは

クラスタ ピア クラスタ間接続を構成するインターフェイスおよびポートと、それらがどのように使用されるかを理解しておくと、クラスタ ピア クラスタ間接続の作成にかかる時間を短縮できます。

クラスタ ピア クラスタ間接続は、ネットワーク ポートに割り当てられたインタークラスタLIF（論理インターフェイス）で構成されます。クラスタ間接続は2つの異なるクラスタ間のレプリケーションに使用されるネットワークで、インタークラスタLIFの作成時に定義されます。2つのクラスタ間のレプリケーションは、クラスタ間接続でのみ発生します。これは、同じクラスタ内のデータ ネットワークと同じサブネットにクラスタ間接続があるかどうかに依存しません。

インタークラスタLIFには、データLIFと同じサブネット内や、別のサブネット内のIPアドレスを割り当てることができます。インタークラスタLIFの作成時には、そのインタークラスタLIFを含むシステムSVMに属するルートが使用されます。

関連コンセプト

データ ポートを共有する場合の考慮事項（278ページ）
専用のポートを使用する場合の考慮事項（278ページ）

サポートされるクラスタ ピア ネットワーク トポロジ

データ保護を提供するには、一方のクラスタのすべてのクラスタ間LIFが、*ペアワイズのフルメッシュ*接続を使用して他方のクラスタのすべてのクラスタ間LIFと通信できる必要があります。この接続が、異なるクラスタ トポロジに対してどのように動作するかを理解する必要があります。

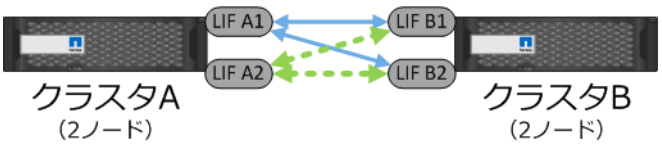
*ペアワイズのフルメッシュ*接続は、ピア関係にある2つのクラスタにのみ適用されます。一方のクラスタのIPspaceのすべてのクラスタ間LIFが、他方のクラスタのIPspaceのすべてのクラスタ間LIFと通信できる必要があります。

*ペアワイズのフルメッシュ*接続の概念を理解することは、より複雑なクラスタ ピア トポロジを構築するうえで役立ちます。この接続が、2つのクラスタ、クラスタ カスケード、クラスタ ファンアウトまたはファンインの各トポロジに対してどのように動作するかを理解しておくことで、不要なクラスタ間ネットワークを追加することなく、実現可能なクラスタ間ネットワークを構築することができます。

2つのクラスタ間のクラスタ間ネットワーク

2つのクラスタ間でのクラスタ間ネットワークの作成は、基本的なクラスタ ピア設定です。たとえば、クラスタAとクラスタBの2つのクラスタ間で、クラスタ間ネットワークを作成するとします。クラスタAにはデフォルトのIPspaceにA1とA2の2つのクラスタ間LIFがあり、クラスタBにはデフォルトのIPspaceにB1とB2の2つのクラスタ間LIFがあります。このとき、LIFは次のように接続されます。

- A1はB1と通信する
- A1はB2と通信する
- A2はB1と通信する
- A2はB2と通信する



クラスタ カスケード内のクラスタ間ネットワーク

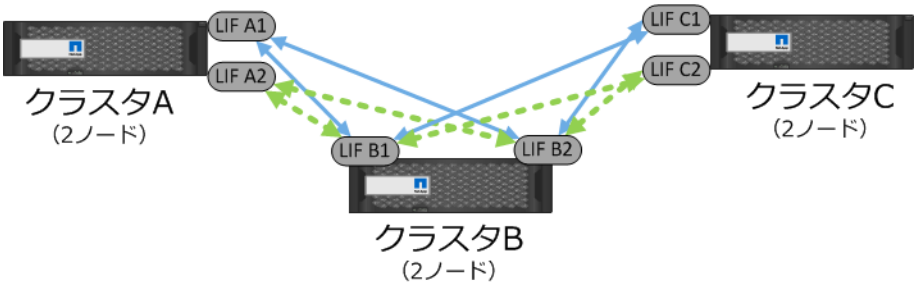
カスケード内の3つのクラスタを接続する場合、プライマリ クラスタのすべてのクラスタ間LIFが、セカンダリ クラスタのすべてのクラスタ間LIFと通信できる必要があります。同様に、セカンダリ クラスタのすべてのクラスタ間LIFが、ターシャリ(3番目の)クラスタのすべてのクラスタ間LIFと通信できる必要があります。プライマリ クラスタとターシャリ クラスタをクラスタ ピア関係で接続しない場合、この2つのクラスタの間にクラスタ間ネットワークを作成する必要はありません。

たとえば、クラスタAとクラスタBの間にクラスタ間ネットワークを作成し、クラスタBとクラスタCの間にクラスタ間ネットワークを作成するとします。クラスタAにはデフォルトのIPspaceにA1とA2の2つのクラスタ間LIFがあり、クラスタBにはデフォルトのIPspaceにB1とB2の2つのクラスタ間LIFがあり、クラスタCにはデフォルトのIPspaceにC1とC2の2つのクラスタ間LIFがあります。このときに、クラスタAとクラスタBの間のクラスタ間LIFは次のように接続されます。

- A1はB1と通信する
- A1はB2と通信する
- A2はB1と通信する
- A2はB2と通信する

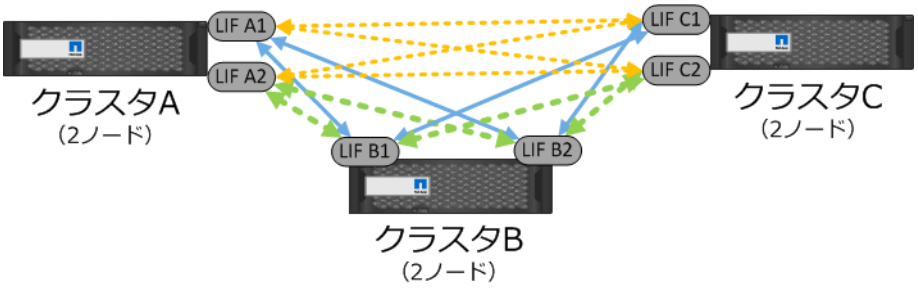
クラスタBとクラスタCの間のクラスタ間LIFは次のように接続されます。

- B1はC1と通信する
- B1はC2と通信する
- B2はC1と通信する
- B2はC2と通信する



セカンダリ クラスタで問題が発生したときにはターシャリ クラスタをプライマリ クラスタと接続する、クラスタ カスケードを設定する場合があります。たとえば、プライマリ クラスタとセカンダリ クラスタとの間にディザスタ リカバリ関係があり、セカンダリ クラスタとターシャリ クラスタとの間にバックアップ関係がある場合、セカンダリ クラスタに何か起きたときはターシャリ クラスタがプライマリ クラスタと通信するようにします。このような設定を希望する場合、ターシャリ クラスタのすべてのクラスタ間LIFが、プライマリ クラスタのすべてのクラスタ間LIFと通信できる必要があります。そのため、前述の接続に加えて、クラスタCとクラスタAの間に次のクラスタ間LIF接続が必要です。

- A1はC1と通信する
- A1はC2と通信する
- A2はC1と通信する
- A2はC2と通信する



クラスタ ファンアウトまたはファンイン内のクラスタ間ネットワーク

ファンアウトまたはファンイン構成でクラスタを接続する場合、プライマリ クラスタに接続する各クラスタのクラスタ間LIFが、プライマリ クラスタのすべてのクラスタ間LIFと通信できる必要があります。リモート クラスタが相互に接続する必要がない場合、リモート クラスタ間でクラスタ間LIFを接続する必要はありません。

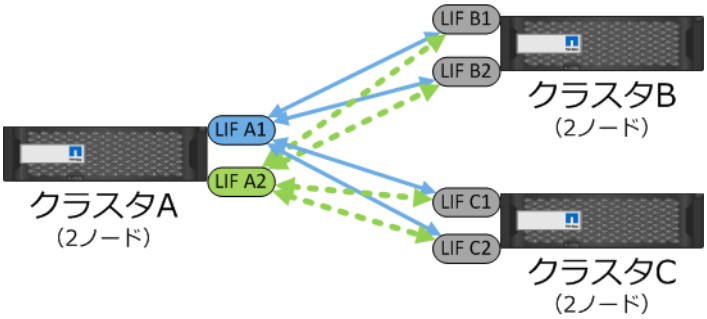
たとえば、クラスタAとクラスタBの間にクラスタ間ネットワークを作成し、クラスタAとクラスタCの間にクラスタ間ネットワークを作成するとします。クラスタAにはデフォルトのIPspaceにA1とA2の2つのクラスタ間LIFがあり、クラスタBにはデフォルトのIPspaceにB1とB2の2つのクラスタ間LIFがあり、クラスタCにはデフォルトのIPspaceにC1とC2の2つのクラスタ間LIFがあります。このときに、クラスタAとクラスタBの間のクラスタ間LIFは次のように接続されます。

- A1はB1と通信する
- A1はB2と通信する
- A2はB1と通信する
- A2はB2と通信する

この場合、クラスタAとクラスタCの間のクラスタ間LIFは次のように接続されます。

- A1はC1と通信する
- A1はC2と通信する
- A2はC1と通信する
- A2はC2と通信する

クラスタBはクラスタCに接続されません。



ファンインまたはファンアウト構成に加えて、2つのリモート クラスタ間にもクラスタ ピア関係が必要な場合、*ペアワイズのフルメッシュ*接続の概念を使用してクラスタ間ネットワークを作成します。

指定のクラスタ間接続と未指定のクラスタ間接続の違い

未指定のクラスタ間接続ではそれぞれのクラスタがデフォルトのIPspace内で接続されるのに対し、指定のクラスタ間接続では、デフォルト以外のIPspaceを使用してクラスタ ピアとのやり取りが行われます。この接続の違いについて理解すると、指定のクラスタ間接続を使用するかどうかを判断するのに役立ちます。

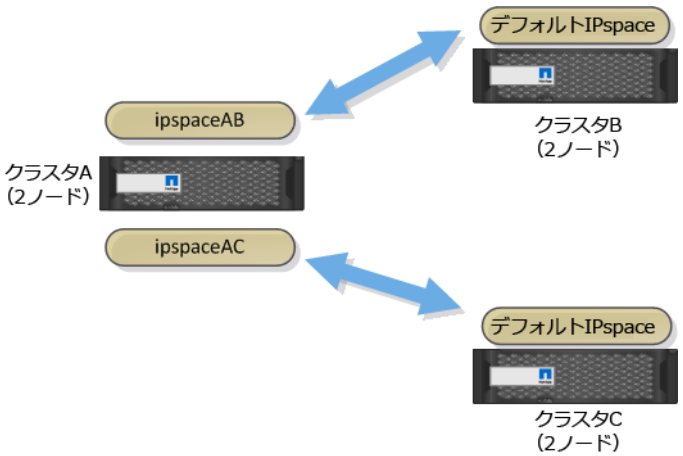
未指定のクラスタ間接続では、それぞれのクラスタがデフォルトのIPspace内で接続されます。IPspace内ではペアワイズのフルメッシュ接続にする必要があるため、クラスタ ピア関係にある2つのクラスタのすべてのクラスタ間LIFが相互に接続できる必要があります。そのため、ストレージ サービス プロバイダが必要に応じて接続を分離することはできません。これらのクラスタ間接続を分離するには、ネットワークにルータなどのハードウェアを導入する必要があります。

指定のクラスタ間接続では、ピア関係にある1つ以上のクラスタとの間で、指定したデフォルト以外のIPspaceを使用してやり取りが行われます。この場合もペアワイズのフルメッシュ接続にする必要がありますが、接続はピア関係用に各クラスタで定義したIPspace内で行われ、他のIPspaceにまたがることはありません。そのため、クラスタ間接続が他のピアとの間の別のIPspaceから分離され、フルメッシュ接続にしなければならない範囲も小さくなります。この方法では、ストレージ サービス プロバイダが必要に応じてクラスタ間接続の分離を制御できます。

たとえば、クラスタAでクラスタBおよびクラスタCの2つとそれぞれピア関係を確立するとします。クラスタAとクラスタBの間の接続とクラスタAとクラスタCの間の接続は分離させる必要があります。これを行うには、クラスタAにIPspaceを2つ作成します。1つ目のIPspace（ipspaceAB）に、クラスタBとの通信に使用するクラスタAのクラスタ間LIFを含めます。同様に、もう1つのIPspace（ipspaceAC）に、クラスタCとの通信に使用するクラスタAのクラスタ間LIFを含めます。

クラスタBとクラスタCのクラスタ間LIFは、それぞれのクラスタのデフォルトのIPspaceに含まれます。これらのクラスタ間LIFは、必ずしもデフォルトのIPspaceに含まれている必要はありません。デフォルトのIPspaceのほか、それぞれ独自に指定したIPspaceに含めることもできます。

クラスタAでは、クラスタBおよびクラスタCとのピア関係において、クラスタBとの通信にはIPspace ipspaceABのLIFのみを使用し、クラスタCとの通信にはIPspace ipspaceACのLIFのみを使用します。クラスタBのクラスタ間LIFでクラスタAのIPspace ipspaceAB以外のクラスタ間LIFと通信したり、クラスタCのクラスタ間LIFでクラスタAのIPspace ipspaceAC以外のクラスタ間LIFと通信したりする必要はありません。



クラスタ ピアリングの前提条件

クラスタ ピアリングを設定する前に、IPspace、接続、ポート、IPアドレス、サブネット、ファイアウォール、およびクラスタの命名要件が下記の条件を満たしているか確認してください。

接続要件

クラスタ間通信で各クラスタが使用するサブネットは、次の要件を満たしている必要があります。

- サブネットがクラスタ間通信で使用するポートを含むブロードキャスト ドメインに属している。
- インタークラスタLIFで使用されるIPアドレスがすべて同じサブネットに含まれている必要はないが、構成としてはよりシンプルである。
- サブネットをクラスタ間通信専用にするか、データ通信との共有にするかを検討済みである。
- サブネットには、1つのノードにつき1つのインタークラスタLIFが割り当てられるよう、十分な数のIPアドレスを準備する必要があります。
  たとえば、6ノード クラスタの場合、クラスタ間通信で使用するサブネットには使用可能なIPアドレスが6つ必要です。

クラスタ間ネットワークは、クラスタ ピアどうしが該当するIPspace内で*ペアワイズのフルメッシュ接続*状態になるように構成する必要があります。具体的には、クラスタ ピア関係にある各クラスタ ペアの、すべてのインタークラスタLIFの間に接続が確立されている必要があります。

1つのクラスタで使用するインタークラスタLIFでは、同じバージョンのIPアドレスを使用する必要があります（IPv4アドレスまたはIPv6アドレス）。同様に、ピア関係にあるクラスタのすべてのインタークラスタLIFでも、同じバージョンのIPアドレスを使用する必要があります。

ポート要件

クラスタ間通信で使用されるポートは、次の要件を満たす必要があります。

- クラスタ間通信で使用されるブロードキャスト ドメインに、1ノードあたり最低2つのポートがあり、クラスタ間通信で別のポートへのフェイルオーバーが可能になっている。
  ブロードキャスト ドメインに追加されるポートは、物理ネットワーク ポート、VLAN、インターフェイス グループ（ifgrps）です。
- すべてのポートが接続されている。
- すべてのポートが正常な状態である。
- ポートのMTU設定が一貫している。
- クラスタ間通信に使用するポートをデータ通信と共有するかどうかを検討済みである。

ファイアウォールの要件

ファイアウォールとクラスタ間ファイアウォール ポリシーでは、以下を許可する必要があります。

- ICMPサービス
- 次のポート経由でのすべてのインタークラスタLIFのIPアドレスへのTCP接続：10000、11104、および11105
- HTTPS
  HTTPSはクラスタ ピアリングのセットアップ時には必要ありませんが、OnCommand System Managerを使用してデータ保護を設定する場合にはあとで必要になります。ただし、コマンドライン インターフェイスを使用してデータ保護を設定する場合、クラスタ ピアリングやデータ保護の設定にHTTPSは必要ありません。

デフォルトの**クラスタ間**ファイアウォール ポリシーは、HTTPSプロトコル経由のアクセス、およびすべてのIPアドレス（0.0.0.0/0）からのアクセスを許可しますが、このポリシーは変更したり置き換えることができます。

クラスタの要件

クラスタは、次の要件を満たす必要があります。

- 各クラスタの名前が固有である。
  同じ名前のクラスタ、または同じ名前のクラスタとピア関係になっているクラスタとのクラスタ ピア関係を作成することはできません。
- クラスタ ピア関係にあるクラスタどうしは、300秒（5分）以内の時間差で同期する。
  クラスタ ピアは、異なるタイム ゾーンにあっても構いません。

データ ポートを共有する場合の考慮事項

クラスタ間レプリケーションのためにデータ ポートを共有することが、クラスタ間ネットワーク ソリューションとして適切であるかどうかを判断するには、LANのタイプ、利用可能なWAN帯域幅、レプリケーション間隔、変更率、ポート数などの設定や要件を考慮する必要があります。

データ ポートを共有することがクラスタ間接続ソリューションとして適切であるかどうかを判断するには、ネットワークについて次の事項を考慮してください。

- 10ギガビット イーサネット（10GbE）ネットワークのように高速なネットワークの場合は、データ アクセスに使用されるのと同じ10GbEポート上に、レプリケーションを実行するためのローカル LAN帯域幅が十分にあると考えられます。
  多くの場合、使用できるWAN帯域幅は、10GbEのLAN帯域幅よりもはるかに少なくなります。
- クラスタ内のすべてのノードが、データをレプリケートし、使用できるWAN帯域幅を共有しなければならない場合、データ ポートを共有する方法は、比較的許容できる選択肢となります。
- データ用とレプリケーション用のポートを共有すると、ポートをレプリケーション専用にする場合のようにポート数を増やす必要がありません。
- レプリケーション ネットワークの最大転送単位（MTU）サイズは、データ ネットワークに使用されるサイズと同じになります。
- データの変更率とレプリケーション間隔について検討し、データ ポートを共有した場合に、間隔ごとにレプリケートする必要があるデータの量が、データ プロトコルとの競合を引き起こすほどの帯域幅を消費するかどうかを検討します。
- データ ポートをクラスタ間レプリケーション用に共有すると、同じノード上にある他の任意のクラスタ間対応ポートにクラスタ間LIFを移行して、レプリケーションに使用する特定のデータ ポートをコントロールできます。

専用のポートを使用する場合の考慮事項

専用のポートを使用することが適切なクラスタ間ネットワーク ソリューションであるかどうかを判断するには、LANのタイプ、利用可能なWAN帯域幅、レプリケーション間隔、変更率、ポート数などの設定や要件を考慮する必要があります。

専用のポートを使用することがクラスタ間ネットワーク ソリューションとして適切であるかどうかを判断するには、ネットワークについて次の事項を考慮してください。

- 使用できるWAN帯域幅がLANポートの帯域幅とほぼ同じで、レプリケーション間隔の設定により、通常のクライアント アクティビティが実行されている間にレプリケーションが実行される場合は、クラスタ間レプリケーションにイーサネット ポートを専用に割り当てて、レプリケーションとデータ プロトコルとの競合を回避します。

- データ プロトコル（CIFS、NFS、iSCSI）によるネットワーク利用率が50%を超える場合は、レプリケーションにポートを専用に割り当てて、ノード フェイルオーバーの場合も、パフォーマンスが低下しないようにします。
- 物理10GbEポートがデータとレプリケーションの両方に使用されている場合は、レプリケーション用にVLANポートを作成し、論理ポートをクラスタ間レプリケーション専用にすることができます。
  すべてのVLANおよびベース ポートでポートの帯域幅が共有されます。
- データの変更率とレプリケーション間隔について検討し、データ ポートを共有した場合に、間隔ごとにレプリケートする必要があるデータの量が、データ プロトコルとの競合を引き起こすほどの帯域幅を消費するかどうかを検討します。

データ ポートを共有するためのクラスタ間LIFの設定

クラスタ間LIFでデータ ポートを共有する設定にすると、既存のデータ ポートを使用して、クラスタピア関係用のクラスタ間ネットワークを作成できます。データ ポートを共有することで、クラスタ間ネットワークに必要なポート数を減らすことができます。

タスク概要

データ ポートを共有するクラスタ間LIFの作成には、既存のデータ ポートへのLIFの割り当てが含まれます。この手順では、2ノード クラスタを使用します。各ノードにはデータ ポートが2つ（e0cおよびe0d）あり、これらのデータ ポートはデフォルトIPspaceに属しています。これら2つのデータ ポートが、クラスタ間のレプリケーションで共有されます。クラスタ ピア関係を作成する前に、ピア クラスタでクラスタ間LIFを設定する必要があります。実際の環境では、ポート、ネットワーク、IPアドレス、サブネット マスク、およびサブネットを、環境固有のものに置き換えます。

手順

1. `network port show`コマンドを使用して、クラスタ内のポートを表示します。

   例

   ```
   cluster01::> network port show
                                                            Speed (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- ------- ------------
   cluster01-01
          e0a       Cluster      Cluster          up       1500  auto/1000
          e0b       Cluster      Cluster          up       1500  auto/1000
          e0c       Default      Default          up       1500  auto/1000
          e0d       Default      Default          up       1500  auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up       1500  auto/1000
          e0b       Cluster      Cluster          up       1500  auto/1000
          e0c       Default      Default          up       1500  auto/1000
          e0d       Default      Default          up       1500  auto/1000
   ```

2. `network interface create`コマンドを使用して、管理SVM cluster01にクラスタ間LIFを作成します。

   例

   この例では、
   *adminSVMname*_icl#
   というLIF命名規則を使用して、クラスタ間LIFに名前を付けています。

   ```
   cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01 -role
   intercluster
   -home-node cluster01-01 -home-port e0c -address 192.168.1.201 -netmask 255.255.255.0
   ```

```
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl02 -role
intercluster
-home-node cluster01-02 -home-port e0c -address 192.168.1.202 -netmask 255.255.255.0
```

3. `network interface show`コマンドで`-role` **`intercluster`**パラメータを指定して、クラスタ間LIFが正しく作成されたことを確認します。

   例

```
cluster01::> network interface show –role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c     true
```

4. `network interface show`コマンドで`-role` **`intercluster`**パラメータと`-failover`パラメータを指定して、クラスタ間LIFの冗長性が確保されていることを確認します。

   例

   この例のLIFは、各ノード上のe0cポートに割り当てられています。e0cポートに障害が発生した場合、LIFはe0dポートにフェイルオーバー可能です。

```
cluster01::> network interface show -role intercluster –failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only      192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only      192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

5. `network route show`コマンドを使用してクラスタ内のルートを表示し、クラスタ間ルートがすでに確保されているか、または新たに作成する必要があるかを確認します。

   ルートを作成する必要があるのは、両方のクラスタ内のクラスタ間アドレスが同じサブネット上になく、クラスタ間で通信するために特定のルートが必要な場合のみです。

   例

   この例では、クラスタ間ルートはありません。

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster
          0.0.0.0/0       192.168.0.1     20
cluster01
          0.0.0.0/0       192.168.0.1     10
```

6. 異なるクラスタのクラスタ間LIF間の通信でルーティングが必要な場合は、`network route create`コマンドを使用してクラスタ間ルートを作成します。

   新しいルートのゲートウェイは、クラスタ間LIFと同じサブネットになければなりません。

   例

   この例では、192.168.1.1が192.168.1.0/24ネットワークのゲートウェイ アドレスです。デスティネーションを0.0.0.0/0と指定すると、これがクラスタ間ネットワークのデフォルト ルートになります。

```
cluster01::> network route create -vserver cluster01
-destination 0.0.0.0/0 -gateway 192.168.1.1 -metric 40
```

7. `network route show`コマンドを使用して、ルートが正しく作成されたことを確認します。

   例

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster
          0.0.0.0/0       192.168.0.1     20
cluster01
          0.0.0.0/0       192.168.0.1     10
          0.0.0.0/0       192.168.1.1     40
```

8. 接続先のクラスタで上記の手順を繰り返します。

専用のクラスタ間ポートを使用するためのクラスタ間LIFの設定

クラスタ間LIFで専用のデータ ポートを使用する設定では、クラスタ間ネットワーク上のデータ ポートをクラスタ ピア関係で共有する場合よりも広い帯域幅を確保できます。

タスク概要

専用ポートを使用するクラスタ間LIFの作成には、専用ポートのフェイルオーバー グループの作成とそれらのポートへのLIFの割り当てが含まれます。この手順では、2ノード クラスタを使用します。各ノードには、追加したデータ ポートが2つ（e0eおよびe0f）あり、現在はデフォルトIPspaceに属しています。これらのポートをクラスタ間のレプリケーション専用として割り当てます。これらのポートを、設定するクラスタ間LIFのターゲットとしてグループ化します。クラスタ ピア関係を作成する前に、ピア クラスタでクラスタ間LIFを設定する必要があります。実際の環境では、ポート、ネットワーク、IPアドレス、サブネット マスク、およびサブネットを、環境固有のものに置き換えます。

手順

1. `network port show`コマンドを使用して、クラスタ内のポートを表示します。

   例

```
cluster01::> network port show
                                                         Speed (Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- ------------
cluster01-01
       e0a       Cluster      Cluster          up       1500  auto/1000
       e0b       Cluster      Cluster          up       1500  auto/1000
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
cluster01-02
       e0a       Cluster      Cluster          up       1500  auto/1000
       e0b       Cluster      Cluster          up       1500  auto/1000
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
```

2. `network interface show`コマンドを使用して、レプリケーション専用のポートを使用しているLIFがあるかどうかを確認します。

   例

   次の出力には、ポートe0eおよびe0fは表示されません。そのため、これらのポートにはLIFが配置されていません。

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. クラスタ間接続の専用ポートにするポートを使用しているLIFがある場合は、そのLIFを別のポートに移行します。

   a. `network interface migrate`コマンドを使用して、LIFを別のポートに移行します。

      例

      次の例では、ポートe0eがcluster01_data01という名前のデータLIFで使用されており、そのポートをクラスタ間LIFだけで使用するとします。

      ```
      cluster01::> network interface migrate -vserver cluster01
      -lif cluster01_data01 -dest-node cluster01-01 -dest-port e0d
      ```

   b. 必要に応じて、`network interface modify`コマンドを使用して、移行したLIFのホームポートを移行先の新しいポートに変更します。

      例

      ```
      cluster01::> network interface modify -vserver cluster01
      -lif cluster01_data01 -home-node cluster01-01 -home-port e0d
      ```

4. `network interface failover-groups create`コマンドを使用して、クラスタ間LIFに使用するポートをグループ化します。

   例

   ```
   cluster01::> network interface failover-groups create -vserver cluster01
   -failover-group intercluster01 -targets cluster01-01:e0e,cluster01-01:e0f,
   cluster01-02:e0e,cluster01-02:e0f
   ```

5. `network interface failover-groups show`コマンドを使用して、作成したフェイルオーバー グループを表示します。

   例

   ```
   cluster01::> network interface failover-groups show
                                     Failover
   Vserver          Group            Targets
   ---------------- ---------------- --------------------------------------------
   Cluster
                    Cluster
                                     cluster01-01:e0a, cluster01-01:e0b,
                                     cluster01-02:e0a, cluster01-02:e0b
   cluster01
                    Default
                                     cluster01-01:e0c, cluster01-01:e0d,
                                     cluster01-02:e0c, cluster01-02:e0d,
                                     cluster01-01:e0e, cluster01-01:e0f
                                     cluster01-02:e0e, cluster01-02:e0f
                    intercluster01
                                     cluster01-01:e0e, cluster01-01:e0f
                                     cluster01-02:e0e, cluster01-02:e0f
   ```

6. `network interface create`コマンドを使用して、管理SVM cluster01にクラスタ間LIFを作成します。

   例

   この例では、***adminSVMname*_icl#**というLIF命名規則を使用して、クラスタ間LIFに名前を付けています。

```
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01 -role
intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201 -netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif cluster01_icl02 -role
intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202 -netmask 255.255.255.0 -failover-group intercluster01
```

7. `network interface show`コマンドを使用して、クラスタ間LIFが正しく作成されたことを確認します。

   例

```
cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Cluster
            cluster01-01_clus_1
                         up/up    192.168.0.xxx/24   cluster01-01  e0a     true
            cluster01-01_clus_2
                         up/up    192.168.0.xxx/24   cluster01-01  e0b     true
            cluster01-02_clus_1
                         up/up    192.168.0.xxx/24   cluster01-01  e0a     true
            cluster01-02_clus_2
                         up/up    192.168.0.xxx/24   cluster01-01  e0b     true
cluster01
            cluster_mgmt up/up    192.168.0.xxx/24   cluster01-01  e0c     true
            cluster01_icl01
                         up/up    192.168.1.201/24   cluster01-01  e0e     true
            cluster01_icl02
                         up/up    192.168.1.202/24   cluster01-02  e0e     true
            cluster01-01_mgmt1
                         up/up    192.168.0.xxx/24   cluster01-01  e0c     true
            cluster01-02_mgmt1
                         up/up    192.168.0.xxx/24   cluster01-02  e0c     true
```

8. `network interface show`コマンドで`-role` **intercluster**パラメータと`-failover`パラメータを指定して、クラスタ間LIFの冗長性が確保されていることを確認します。

   例

   この例のLIFは、各ノード上のe0eホーム ポートに割り当てられています。e0eポートに障害が発生した場合、LIFはe0fポートにフェイルオーバー可能です。

```
cluster01::> network interface show -role intercluster –failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01-01
         cluster01-01_icl01 cluster01-01:e0e   local-only      intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01-01_icl02 cluster01-02:e0e   local-only      intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

9. `network route show`コマンドを使用してクラスタ内のルートを表示し、クラスタ間ルートがすでに確保されているか、または新たに作成する必要があるかを確認します。

   ルートを作成する必要があるのは、両方のクラスタ内のクラスタ間アドレスが同じサブネット上になく、クラスタ間で通信するために特定のルートが必要な場合のみです。

例

この例では、クラスタ間ルートはありません。

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster
          0.0.0.0/0       192.168.0.1     20
cluster01
          0.0.0.0/0       192.168.0.1     10
```

10. 異なるクラスタのクラスタ間LIF間の通信でルーティングが必要な場合は、`network route create`コマンドを使用してクラスタ間ルートを作成します。

    新しいルートのゲートウェイは、クラスタ間LIFと同じサブネットになければなりません。

    例

    この例では、192.168.1.1が192.168.1.0/24ネットワークのゲートウェイ アドレスです。デスティネーションを0.0.0.0/0と指定すると、これがクラスタ間ネットワークのデフォルト ルートになります。

```
cluster01::> network route create -vserver cluster01
-destination 0.0.0.0/0 -gateway 192.168.1.1 -metric 40
```

11. `network route show`コマンドを使用して、ルートが正しく作成されたことを確認します。

    例

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster
          0.0.0.0/0       192.168.0.1     20
cluster01
          0.0.0.0/0       192.168.0.1     10
          0.0.0.0/0       192.168.1.1     40
```

12. 上記の手順を繰り返し、ピア クラスタでクラスタ間ネットワークを設定します。

13. ポートが適切なサブネットやVLANなどにアクセスできることを確認します。

    あるクラスタ内でレプリケーションに専用ポートを割り当てた場合でも、すべてのクラスタ内で専用ポートを割り当てる必要はありません。あるクラスタでは専用ポートを使用し、別のクラスタではデータ ポートをクラスタ間レプリケーション用に共有できます。

独自のネットワークのクラスタ間ポートを使用するためのクラスタ間LIFの設定

クラスタ間トラフィックを特定のネットワーク経由で転送しなければならないことがあります。たとえば、デフォルトのIPspaceで到達できない別のクラスタに接続する必要がある場合などです。これを行うには、ポートを独自のIPspaceに移動し、クラスタ間LIFを設定します。

タスク概要

この手順では、2ノード クラスタを使用します。各ノードには、クラスタ ピア関係に使用するポートが2つ（e0eおよびe0f）あり、それらのポートをデフォルトのIPspaceから独自のIPspaceに移動します。この例では、これらのポートでクラスタ間LIFのみを設定していますが、データLIFを共有するように設定することもできます。実際の環境では、ポート、ネットワーク、IPアドレス、サブネット マスク、およびサブネットを、環境固有のものに置き換えます。

手順

1. `network port show`コマンドを使用して、クラスタ内のポートを表示します。

例

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- ------------
cluster01-01
       e0a       Cluster      Cluster          up       1500  auto/1000
       e0b       Cluster      Cluster          up       1500  auto/1000
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
cluster01-02
       e0a       Cluster      Cluster          up       1500  auto/1000
       e0b       Cluster      Cluster          up       1500  auto/1000
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
```

2. `network ipspace create`コマンドを使用して、クラスタ間ネットワークを分離するクラスタにデフォルト以外のIPspaceを作成します。

   例

   ```
   cluster01::> network ipspace create -ipspace ipspace-IC1
   ```

3. `network interface show`コマンドを使用して、レプリケーション専用のポートを使用しているLIFがあるかどうかを確認します。

   例

   次の出力には、ポートe0eおよびe0fは表示されません。そのため、これらのポートにはLIFが配置されていません。

   ```
   cluster01::> network interface show -fields home-port,curr-port
   vserver lif                  home-port curr-port
   ------- -------------------- --------- ---------
   Cluster cluster01-01_clus1   e0a       e0a
   Cluster cluster01-01_clus2   e0b       e0b
   Cluster cluster01-02_clus1   e0a       e0a
   Cluster cluster01-02_clus2   e0b       e0b
   cluster01
           cluster_mgmt         e0c       e0c
   cluster01
           cluster01-01_mgmt1   e0c       e0c
   cluster01
           cluster01-02_mgmt1   e0c       e0c
   ```

4. クラスタ間接続の専用ポートにするポートを使用しているLIFがある場合は、そのLIFを別のポートに移行します。

   a. `network interface migrate`コマンドを使用して、LIFを別のポートに移行します。

      例

      次の例では、ポートe0eがcluster01_data01という名前のデータLIFで使用されており、そのポートをクラスタ間LIFだけで使用するとします。

      ```
      cluster01::> network interface migrate -vserver cluster01
      -lif cluster01_data01 -dest-node cluster01-01 -dest-port e0d
      ```

   b. 必要に応じて、`network interface modify`コマンドを使用して、移行したLIFのホームポートを移行先の新しいポートに変更します。

例

```
cluster01::> network interface modify -vserver cluster01
-lif cluster01_data01 -home-node cluster01-01 -home-port e0d
```

5. `network port broadcast-domain remove-ports`コマンドを使用して、デフォルトのブロードキャストドメインからポートe0eとe0fを削除します。

   ポートは同時に複数のブロードキャストドメインに割り当てることはできないため、別のブロードキャストドメインに追加する前に、現在のブロードキャストドメインから削除する必要があります。

   例

```
cluster01::> network port broadcast-domain remove-ports -broadcast-
domain Default
-ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

6. network port showコマンドを使用して、ポートの割り当てが解除されたことを確認します。

   ブロードキャストドメインに割り当てられていないポートは、Broadcast Domain列に「-」と表示されます。

   例

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/
Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up       9000  auto/
1000
       e0b       Cluster      Cluster          up       9000  auto/
1000
       e0c       Default      Default          up       1500  auto/
1000
       e0d       Default      Default          up       1500  auto/
1000
       e0e       Default      -                up       1500  auto/
1000
       e0f       Default      -                up       1500  auto/
1000
       e0g       Default      Default          up       1500  auto/
1000
cluster01-02
       e0a       Cluster      Cluster          up       9000  auto/
1000
       e0b       Cluster      Cluster          up       9000  auto/
1000
       e0c       Default      Default          up       1500  auto/
1000
       e0d       Default      Default          up       1500  auto/
1000
       e0e       Default      -                up       1500  auto/
1000
       e0f       Default      -                up       1500  auto/
1000
       e0g       Default      Default          up       1500  auto/
1000
```

7. `network port broadcast-domain create`コマンドを使用して、クラスタ間処理専用にするポート用のブロードキャストドメインを「ipspace-IC1」IPspaceに作成します。

ポートのブロードキャストドメインを作成するプロセスの一環として、割り当てを解除したポートをブロードキャストドメインに割り当てます。

例

この例では、「ipspace-IC1-bd」というブロードキャストドメインを「ipspace-IC1」IPspaceに作成します。

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

8. オプション: `network interface failover-groups create`コマンドを使用して、クラスタ間LIFに使用するポートをグループ化します。

   クラスタ間LIFによるブロードキャストドメインの任意のポートの使用がクラスタ間接続の要件で許容されている場合は、フェイルオーバー グループを別途作成する必要はありません。

   例

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group intercluster01 -targets cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

9. `network port broadcast-domain show`コマンドを使用して、ブロードキャストドメインが作成され、ポートが割り当てられたことを確認します。

   例

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                         Update
Name    Domain Name    MTU  Port List                     Status
Details
------- ----------- ------  ------------------------------
--------------
Cluster Cluster       9000
                            cluster01-01:e0a              complete
                            cluster01-01:e0b              complete
                            cluster01-02:e0a              complete
                            cluster01-02:e0b              complete
Default Default       1500
                            cluster01-01:e0c              complete
                            cluster01-01:e0d              complete
                            cluster01-01:e0f              complete
                            cluster01-01:e0g              complete
                            cluster01-02:e0c              complete
                            cluster01-02:e0d              complete
                            cluster01-02:e0f              complete
                            cluster01-02:e0g              complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e              complete
                            cluster01-01:e0f              complete
                            cluster01-02:e0e              complete
                            cluster01-02:e0f              complete
```

10. `network interface failover-groups show`コマンドを使用して、作成したフェイルオーバー グループを表示します。

例

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ---------------- --------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
ipspace-IC1      ipspace-IC-bd
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

11. `network interface create`コマンドを使用して、システムSVM ipspace-IC1にクラスタ間LIFを作成します。

例

この例では、*adminSVMname*_icl#というLIF命名規則を使用して、クラスタ間LIFに名前を付けています。

```
cluster01::> network interface create -vserver ipspace-IC1 -lif cluster01_icl01 -role
intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201 -netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver ipspace-IC1 -lif cluster01_icl02 -role
intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202 -netmask 255.255.255.0 -failover-group intercluster01
```

12. `network interface show`コマンドを使用して、クラスタ間LIFが正しく作成されたことを確認します。

例

```
cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Cluster
            cluster01-01_clus_1
                         up/up    192.168.0.xxx/24   cluster01-01  e0a     true
            cluster01-01_clus_2
                         up/up    192.168.0.xxx/24   cluster01-01  e0b     true
            cluster01-02_clus_1
                         up/up    192.168.0.xxx/24   cluster01-01  e0a     true
            cluster01-02_clus_2
                         up/up    192.168.0.xxx/24   cluster01-01  e0b     true
cluster01
            cluster_mgmt up/up    192.168.0.xxx/24   cluster01-01  e0c     true
            cluster01_icl01
                         up/up    192.168.1.201/24   cluster01-01  e0e     true
            cluster01_icl02
                         up/up    192.168.1.202/24   cluster01-02  e0e     true
            cluster01-01_mgmt1
                         up/up    192.168.0.xxx/24   cluster01-01  e0c     true
            cluster01-02_mgmt1
                         up/up    192.168.0.xxx/24   cluster01-02  e0c     true
```

13. `network interface show`コマンドで`-role` **`intercluster`**パラメータと`-failover`パラメータを指定して、クラスタ間LIFの冗長性が確保されていることを確認します。

例

この例のLIFは、各ノード上のe0eホーム ポートに割り当てられています。e0eポートに障害が発生した場合、LIFはe0fポートにフェイルオーバー可能です。

```
cluster01::> network interface show -role intercluster –failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01-01
         cluster01-01_icl01 cluster01-01:e0e   local-only      intercluster01
                              Failover Targets:  cluster01-01:e0e,
                                                 cluster01-01:e0f
         cluster01-01_icl02 cluster01-02:e0e   local-only      intercluster01
                              Failover Targets:  cluster01-02:e0e,
                                                 cluster01-02:e0f
```

14. `network route show`コマンドを使用してクラスタ内のルートを表示し、クラスタ間ルートがすでに確保されているか、または新たに作成する必要があるかを確認します。

    ルートを作成する必要があるのは、両方のクラスタ内のクラスタ間アドレスが同じサブネット上になく、クラスタ間で通信するために特定のルートが必要な場合のみです。

    例

    この例では、クラスタ間ルートはありません。

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster
          0.0.0.0/0       192.168.0.1     20
cluster01
          0.0.0.0/0       192.168.0.1     10
```

15. 異なるクラスタのクラスタ間LIF間の通信でルーティングが必要な場合は、`network route create`コマンドを使用してクラスタ間ルートを作成します。

    新しいルートのゲートウェイは、クラスタ間LIFと同じサブネットになければなりません。

    例

    この例では、192.168.1.1が192.168.1.0/24ネットワークのゲートウェイ アドレスです。デスティネーションを0.0.0.0/0と指定すると、これがクラスタ間ネットワークのデフォルト ルートになります。

```
cluster01::> network route create -vserver cluster01
-destination 0.0.0.0/0 -gateway 192.168.1.1 -metric 40
```

16. `network route show`コマンドを使用して、ルートが正しく作成されたことを確認します。

    例

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster
          0.0.0.0/0       192.168.0.1     20
cluster01
          0.0.0.0/0       192.168.0.1     10
          0.0.0.0/0       192.168.1.1     40
```

17. 上記の手順を繰り返し、ピア クラスタでクラスタ間ネットワークを設定します。

    2つのクラスタのクラスタ間LIF間で接続が確立されていれば、ピア クラスタのクラスタ間LIFは、デフォルトのIPspaceに含めても、それ以外のIPspaceに含めてもかまいません。

18. ポートが適切なサブネットやVLANなどにアクセスできることを確認します。

    あるクラスタ内でレプリケーションに専用ポートを割り当てた場合でも、すべてのクラスタ内で専用ポートを割り当てる必要はありません。あるクラスタでは専用ポートを使用し、別のクラスタではデータ ポートをクラスタ間レプリケーション用に共有できます。

クラスタ ピア関係の作成

一連のクラスタ間LIFを使用してクラスタ ピア関係を作成し、クラスタ ピアリング アプリケーションで、一方のクラスタに関する情報をもう一方のクラスタが使用できるようにします。

開始する前に

- ピア関係を作成する両方のクラスタのIPspaceにクラスタ間LIFを作成しておく必要があります。
- クラスタのクラスタ間LIFが、相互にルーティングできることを確認しておきます。
- クラスタ間で管理者が異なる場合、クラスタ ピア関係の認証に使用するパスフレーズを決めておく必要があります。

タスク概要

クラスタ間LIFをデフォルト以外のIPspaceに作成した場合は、クラスタ ピアの作成時にIPspaceを指定する必要があります。

手順

1. `cluster peer create`コマンドを使用して、各クラスタにクラスタ ピア関係を作成します。

   使用するパスフレーズは、入力時に表示されません。

   クラスタ間接続用にデフォルト以外のIPspaceを作成した場合は、`ipspace`パラメータを使用してそのIPspaceを選択します。

   例

   次の例では、cluster01を、cluster02という名前のリモート クラスタとピア関係に設定します。cluster01は、各ノードにクラスタ間LIFが1つある2ノード クラスタです。cluster01に作成したクラスタ間LIFのIPアドレスは、192.168.2.201と192.168.2.202です。同様にcluster02も、各ノードにクラスタ間LIFが1つある2ノード クラスタです。cluster02に作成したクラスタ間LIFのIPアドレスは、192.168.2.203と192.168.2.204です。これらのIPアドレスを使用して、クラスタ ピア関係を作成します。

   ```
   cluster01::> cluster peer create -peer-addrs
   192.168.2.203,192.168.2.204
   Please type the passphrase:
   Please type the passphrase again:
   ```

   ```
   cluster02::> cluster peer create -peer-addrs
   192.168.2.201,192.168.2.202
   Please type the passphrase:
   Please type the passphrase again:
   ```

   クラスタ間IPアドレスのホスト名の解決にDNSが設定されている場合は、`-peer-addrs`オプションにホスト名を指定します。クラスタ間IPアドレスが頻繁に変更されることは稀ですが、ホスト名を使用すれば、クラスタ間IPアドレスを変更してもクラスタ ピア関係を変更する必要はありません。

   例

   次の例では、クラスタ間接続用にIP01AというIPspaceをcluster01に作成してあります。前の例のIPアドレスを使用して、クラスタ ピア関係を作成します。

```
cluster01::> cluster peer create -peer-addrs
192.168.2.203,192.168.2.204
-ipspace IP01A
Please type the passphrase:
Please type the passphrase again:
```

```
cluster02::> cluster peer create -peer-addrs
192.168.2.201,192.168.2.202
Please type the passphrase:
Please type the passphrase again:
```

2. `cluster peer show`コマンドに`-instance`パラメータを指定して、クラスタ ピア関係を表示します。

   クラスタ ピア関係を表示することで、関係が正常に確立されたことを確認できます。

   例

```
cluster01::> cluster peer show –instance
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.168.2.203,192.168.2.204
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.203,192.168.2.204
Cluster Serial Number: 1-80-000013
```

3. `cluster peer health show`コマンドを使用して、ピア クラスタ内のノードの健常性を確認します。

   健常性を確認することで、ピア クラスタ上のノードの接続状態とステータスを確認できます。

   例

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  --------------- --------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

関連タスク

データ ポートを共有するためのクラスタ間LIFの設定（279ページ）
専用のクラスタ間ポートを使用するためのクラスタ間LIFの設定（281ページ）

クラスタ ピア関係の変更

接続しているクラスタの名前、使用している論理インターフェイス、またはクラスタ ピア関係を作成するときに使用したIPアドレスが変更された場合は、クラスタ ピア関係を変更できます。たとえば、変更された関係を作成するときに使用したクラスタのIPアドレスなどです。

手順

1. クラスタ ピア関係の設定を変更するには、`cluster peer modify`コマンドを使用します。

次の例では、cluster_bという名前のクラスタのクラスタピア設定のIPアドレスを172.19.7.3に変更します。

```
node::> cluster peer modify -cluster cluster_b -stable-addrs
172.19.7.3
```

クラスタ ピアリング関係の削除

不要になったクラスタ ピア関係は削除できます。クラスタ ピア関係は、関係を構成するそれぞれのクラスタから削除する必要があります。

開始する前に

2つのクラスタ ピア間のすべてのStorage Virtual Machine（SVM）ピア関係を削除しておく必要があります。

タスク概要

次の手順では、クラスタ ピア関係の一方のクラスタのみの管理者を想定しています。

手順

1. `cluster peer delete`コマンドを使用し、自分が管理者しているクラスタからクラスタ ピア関係を削除します。

   例

   次の例では、cluster1クラスタからcluster2クラスタとのクラスタ ピア関係を削除します。

   ```
   cluster1::> cluster peer delete -cluster cluster2
   ```

2. パートナー クラスタの管理者に、`cluster peer delete`コマンドを使用してそのクラスタからクラスタ ピア関係を削除するよう依頼します。

   例

   次の例では、cluster2クラスタからcluster1クラスタとのクラスタ ピア関係を削除します。

   ```
   cluster2::> cluster peer delete -cluster cluster1
   ```

関連タスク

SVMピア関係の削除（300ページ）

SVMピア関係の管理

クラスタ管理者は、SVMピア関係を、クラスタ内またはピア クラスタ（クラスタ間）にある2つのStorage Virtual Machine（SVM、旧Vserver）間に作成および管理して、SnapMirrorなどのピアリングアプリケーション用のインフラを確立できます。

ピア クラスタとピアSVMの管理は、同じクラスタ管理者が行っても別のクラスタ管理者が行っても構いません。

クラスタ管理者は、次のSVMピア管理タスクを実行できます。

- SVMピア関係の作成

- SVMピア関係の受け入れ
- SVMピア関係の拒否
- SVMピア関係の中断
- SVMピア関係の再開
- SVMピアリング アプリケーションに対するSVMピア関係の変更
- SVMピア関係の削除
- SVMピア関係の表示
- ピアSVMのボリューム間へのSnapMirror関係の設定

  注: クラスタ間SVMピアのボリューム間に負荷共有SnapMirror関係を設定することはできません。

SVM管理者は、次のSVMピア管理タスクのみを実行できます。

- SVMピア関係を表示してピアSVMを特定
- ピアSVMのボリューム間でのデータ保護関係（DP）、SnapVault関係（XDP）、移行関係（TDP）などのSnapMirror関係の設定

注: Data ONTAPのコマンドライン インターフェイス（CLI）では、コマンドやパラメータ名が`vserver`のまま変更されておらず、出力にもこれまでどおり*Vserver*と表示されます。

関連コンセプト

クラスタ ピア関係の管理（270ページ）

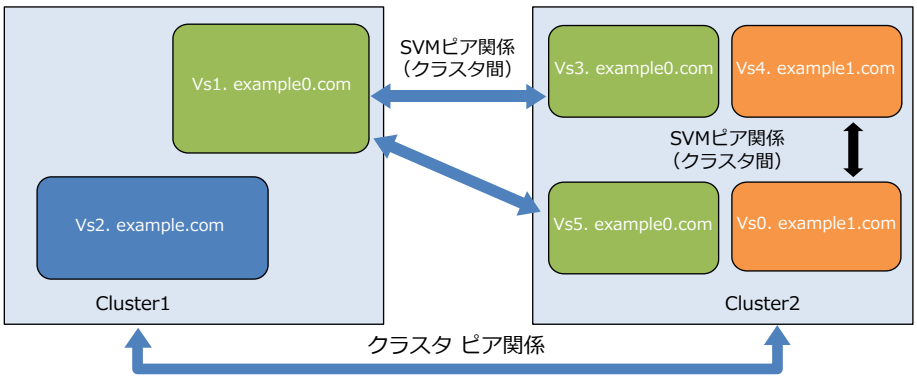
関連情報

clustered Data ONTAP 8.3 データ保護ガイド

SVMピア関係とは

SVMピア関係は、クラスタ管理者が、1つのクラスタ内またはピア クラスタ内（クラスタ間）にあるSVM間にSnapMiror関係などのピアリング アプリケーションを設定できる認証インフラです。SVMピア関係を設定できるのはクラスタ管理者だけです。

次の図は、クラスタ間およびクラスタ内のSVMのピア関係を示しています。



SVMピア インフラを利用することで、SVM間にバックアップとリカバリのメカニズムを設定できます。ピアSVM間には、ボリューム レベルでミラー関係を設定できます。SVMのボリュームが使用で

きなくなった場合には、クラスタ管理者またはSVM管理者は、代わりにデータを提供するようにピアSVMの対応するミラー ボリュームを設定できます。

1つのSVMには、1つのクラスタ内、または複数のクラスタにまたがる複数のSVMとのピア関係を設定できます。

SVMピア インフラを使用して設定できるのは、SnapMirrorデータ保護（DP）関係およびSnapVault（XDP）関係のみです。

SVMピア関係の状態

SVMピア関係は、SVMピア関係で実行された操作に応じてさまざまな状態に変化します。SnapMirrorでのピアSVM間データ転送などの別の操作を実行するには、SVMピア関係の状態を把握しておく必要があります。

次の表に、SVMピア関係の各状態を示します。この表から、SVMピア関係がどういう状況のときにどの状態になるかを理解できます。

SVMピア関係の状態	状況
ローカル クラスタで**initializing**状態	• SVMピア関係を初期化するためにローカル クラスタがピア クラスタと通信している
ローカル クラスタで**initiated**状態 ピア クラスタで**pending**状態	• ローカル クラスタからクラスタ間SVMピア関係が要求された
ローカル クラスタとピア クラスタで**peered**状態	• ピア クラスタからクラスタ間SVMピア関係が承認された • クラスタ内SVMピア関係が確立された • クラスタ間またはクラスタ内SVMピア関係が再開された
ローカル クラスタで**rejected**状態	• ピア クラスタからクラスタ間SVMピア関係が拒否された
ローカル クラスタとピア クラスタで**suspended**状態	• ローカル クラスタまたはピア クラスタから、クラスタ間またはクラスタ内SVMピア関係が中断された

SVMピア関係の作成

クラスタ管理者は、`vserver peer create`コマンドを使用して、Storage Virtual Machine（SVM）ピア関係を作成し、2つのSVM間でSVMピアリング アプリケーションを実行するための認証インフラを整備できます。SVMピア関係は、単一のクラスタ内（クラスタ内）またはピア関係にあるクラスタ間（クラスタ間）の2つのSVM間に作成できます。

開始する前に

- クラスタ間SVMピア関係を作成する場合は、両方のクラスタどうしがピア関係にある必要があります。
- ピア クラスタ内のSVMの名前は、ピア関係にある2つのクラスタ間で一意である必要があります。さらに、どちらかかのクラスタがピア関係にあるその他のクラスタとの間でも一意である必要があります。

SVMの名前が一意でない場合は、`vserver rename`コマンドを使用して一方のSVMの名前を変更する必要があります。
たとえば、クラスタAとクラスタBの2つのクラスタがあり、それぞれがクラスタCとピア関係にあるとします。クラスタAとクラスタBの間にピア関係がなくても、同じ名前のSVMは使用はできません。同一の名前のSVMがある場合、どちらかのSVMの名前を変更する必要があります。

- 管理状態が`initializing`または`deleting`のSVMには、ピア関係を設定することはできません。
- 同じSVM間に以前に作成して`rejected`状態になっているSVMピア関係がある場合、そのSVMピア関係を削除しておく必要があります。

タスク概要

- ピア関係にある各クラスタは、1人のクラスタ管理者が管理することも、別々のクラスタ管理者が管理することもできます。
- SVMピア関係の作成時に、そのピア関係を使用するアプリケーションを指定できます。
  ピア関係を使用する**`snapmirror`**などのアプリケーションを指定しなかった場合、SVM管理者は、ピアSVM間でそのアプリケーションに関連付けられた処理を実行できません。
- FlexVolを備えたSVMには、クラスタ間およびクラスタ内SVMピア関係を作成できます。
- Infinite Volumeを備えたSVMには、クラスタ間SVMピア関係のみを作成できます。
- FlexVolを備えたSVMとInfinite Volumeを備えたSVM間にSVMピア関係を作成することはできません。
- 複数のSSHセッションを使用するか、スクリプトを使用すると、複数のSVMピア関係を同時に作成できます。

  注: パフォーマンスの低下を避けるため、同時に作成するSVMピア関係は5個以下にすることを推奨します。

選択肢

- クラスタ間SVMピア関係の作成（295ページ）
- クラスタ内SVMピア関係の作成（296ページ）

クラスタ間SVMピア関係の作成

2つのクラスタ間にクラスタ間SVMピア関係を作成して、クラスタ間Volume SnapMirror構成などの環境用のインフラを構築できます。2つのクラスタ間にクラスタ間SVMピア関係を作成して、クラスタ間Volume SnapMirror構成やSVMディザスタ リカバリなどの環境用のインフラを構築できます。

開始する前に

2つのクラスタ間にピア関係が設定されている必要があります。

手順

1. `vserver peer create`コマンドを使用して、SVMピア関係を作成します。

   例

   次のコマンドは、vs1.example0.com（cluster1）とvs3.example0.com（cluster2）の間にクラスタ間SVMピア関係を作成します。

```
cluster1::> vserver peer create -vserver vs1.example0.com -peer-vserver vs3.example0.com -
applications snapmirror -peer-cluster cluster2

 Info: [Job 43] 'vserver peer create' job queued
```

クラスタ間SVMピア関係がinitiated状態になります。

2. vserver peer show-allコマンドを使用して、SVMピア関係の状態とその他の詳細情報を表示します。

例

```
cluster1::> vserver peer show-all
                    Peer              Peer                          Peering
Vserver             Vserver           State       Peer Cluster      Applications
-----------         -----------       ----------- -------------- ----------------
vs1.example0.com    vs3.example0.com  initiated   Cluster2           snapmirror
```

このコマンドの詳細については、マニュアル ページを参照してください。

終了後の操作

認証が完了するように、パートナー クラスタの管理者にSVMピアのピア要求について通知する必要があります。

SVMピア関係は、パートナー クラスタのクラスタ管理者がSVMピア要求を承認するまでは確立されません。

関連タスク

SVMピア関係の承認（297ページ）

クラスタ内SVMピア関係の作成

クラスタ内でのSVMデータのバックアップなどの処理を実行するために、クラスタ内のSVM間にSVMピア関係を作成できます。

タスク概要

クラスタ内SVMピア関係は、Infinite Volumeを備えたSVMに作成することはできません。

手順

1. vserver peer createコマンドを使用して、SVMピア関係を作成します。

例

次のコマンドは、クラスタ内SVMピア関係を、cluster2のSVM vs4.example1.comとvs0.example1.comの間に作成します。

```
cluster2::> vserver peer create -vserver vs4.example1.com -peer-vserver vs0.example1.com -
applications snapmirror

Info: 'vserver peer create' command is successful.
```

クラスタ内SVMピア関係が作成され、peered状態になります。クラスタは単独のクラスタ管理者が管理しているため、認証は必要ありません。

2. vserver peer show-allコマンドを使用して、SVMピア関係の状態とその他の詳細情報を表示します。

例

```
cluster2::> vserver peer show-all
                    Peer                Peer                    Peering
Vserver             Vserver             State   Peer Cluster    Applications
-----------        ---------------    --------- ------------- ---------------
vs4.example1.com  vs0.example1.com   peered    cluster2       snapmirror
vs0.example1.com  vs4.example1.com   peered    cluster2       snapmirror
```

SVMピア関係の承認

クラスタ管理者がクラスタ間SVMピア関係を作成した場合、リモート クラスタのクラスタ管理者は、`vserver peer accept`コマンドを使用してSVMピア要求を承認し、SVM間にピア関係を確立できます。

タスク概要

ピア関係を設定した双方のクラスタの管理は、1人のクラスタ管理者が行っても、別々のクラスタ管理者が行っても構いません。1人のクラスタ管理者がピア クラスタを管理する場合は、そのクラスタ管理者がピア クラスタのSVMピア要求を承認する必要があります。別々のクラスタ管理者が管理する場合は、SVMピア要求を出したクラスタ管理者が、Eメールなどのチャネルを使用して相手側のクラスタの管理者に、SVMピア要求を送信した旨を通知する必要があります。

手順

1. `vserver peer show`コマンドを使用して、SVMピア要求を表示します。

   例

   次の例は、cluster2に対するSVMピア要求を表示する方法を示しています。

   ```
   cluster2::> vserver peer show

                       Peer                Peer
   Vserver             Vserver             State
   -----------         -----------         ------------
   vs3.example0.com    vs1.example0.com    pending
   ```

2. `vserver peer accept`コマンドを使用してSVMピア要求を承認し、SVMピア関係を確立します。

   例

   次の例は、受信SVMピア要求を承認し、cluster1とcluster2のそれぞれでvs1.example0.comとvs3.example0.comの間にSVMピア関係を確立する方法を示しています。

   ```
   cluster2::> vserver peer accept -vserver vs3.example0.com -peer-
   vserver vs1.example0.com

   Info: [Job 46] 'vserver peer accept' job queued
   ```

   SVMピア関係が確立され、状態が`peered`になります。

3. どちらかのピア クラスタで`vserver peer show`コマンドを使用して、SVMピア関係の状態を表示します。

   例

   次の例は、SVMピア関係の状態を表示する方法を示しています。

```
cluster2::> vserver peer show
                 Peer               Peer
Vserver          Vserver            State
-----------     ---------------     ------------
vs3.example0.com vs1.example0.com    peered
```

これらのコマンドの詳細については、マニュアル ページを参照してください。

タスクの結果

クラスタ管理者およびSVM管理者は、SVMピア間でSnapMirrorなどのピアリング アプリケーションを利用できます。

SVMピア関係の拒否

クラスタ管理者がクラスタ間SVMピア関係を作成した場合、ピア クラスタのクラスタ管理者は、`vserver peer reject`コマンドを使用してSVMピア要求を拒否し、SVM間のピア関係を防ぐことができます。

タスク概要

許可されていないSVMによってSVMピア要求が開始された場合、ピア クラスタのクラスタ管理者はその関係を拒否できます。拒否されたピアリング関係に対して別のピアリング操作を実行することはできません。

手順

1. `vserver peer show`コマンドを使用して、ピア クラスタに対するSVMピア要求を表示します。

   例

   次の例は、cluster2に対するSVMピア要求を表示する方法を示しています。

   ```
   cluster2::> vserver peer show
                    Peer               Peer
   Vserver          Vserver            State
   -----------      -----------        ------------
   vs5.example0.com vs1.example0.com    pending
   ```

2. `vserver peer reject`コマンドを使用して、SVMピア要求を拒否します。

   例

   次の例は、cluster1とcluster2のそれぞれでvs1.example0.comとvs5.example0.comの間の受信SVMピア要求を拒否する方法を示しています。

   ```
   cluster2::> vserver peer reject -vserver vs5.example0.com -peer-
   vserver vs1.example0.com

   Info: [Job 48] 'vserver peer reject' job queued
   ```

   SVMピア関係は拒否された状態になります。

3. SVMピア要求が作成されたクラスタで`vserver peer show`コマンドを使用して、SVMピア関係の状態を表示します。

   例

   次の例は、SVMピア関係の状態を表示する方法を示しています。

```
cluster1::> vserver peer show
                  Peer                Peer
Vserver           Vserver             State
-----------       -----------         ------------
vs1.example0.com  vs5.example0.com    rejected
```

4. 同じSVMの間に再度SVM関係を作成すると失敗するため、`vserver peer delete`コマンドを使用して、拒否されたSVMピア要求を削除します。

   例

   次の例は、拒否されたSVMピア要求を削除する方法を示しています。

```
cluster1::> vserver peer delete -vserver vs1.example0.com -peer-
vserver vs5.example0.com

Info: 'vserver peer delete' command is successful.
```

   これらのコマンドの詳細については、マニュアル ページを参照してください。

SVMピア関係に対するピアリング アプリケーションの変更

クラスタ管理者は、`vserver peer modify`コマンドを使用して、SVMピア関係で実行されるSVMピアリング アプリケーションを変更できます。SVMピア関係にはSnapMirrorとFileCopyのどちらかを設定するか、またはアプリケーションを設定しないこともできます。

タスク概要

SVMピア関係では、ピアSVM間のすべてのSnapMirror処理には**`snapmirror`**、ピアSVM間のすべてのFileCopy関連処理には**`file-copy`**のピアリング アプリケーションをそれぞれ設定する必要があります。

手順

1. `vserver peer modify`コマンドを使用して、SVMピア関係のアプリケーションを変更します。

   例

   次のコマンドを実行すると、SVMピア関係のアプリケーションが変更されます。

```
cluster2::>vserver peer modify -vserver vs4.example.com -peer-vserver vs0.example.com -
applications snapmirror

Warning: The following applications were enabled between Vserver "vs4.example.com" and
peer Vserver "vs0.example.com": file-copy, snapmirror. The following applications will be
removed: file-copy. Any operations related to the removed application in the context of
this Vserver peer relationship will be disabled.
Do you want to continue? {y|n}: y

Info: 'vserver peer modify' command is successful.
```

2. `vserver peer show-all`を使用して、SVMピア関係で実行されているアプリケーションを表示します。

   例

   次のコマンドを実行すると、SVMピア関係で実行されているアプリケーションが表示されます。

```
cluster2::> vserver peer show-all

Vserver            Vserver           State      Peer Cluster   Applications
-----------        -----------       -------    ------------  ------------
vs4.example1.com   vs0.example1.com  peered     cluster2        snapmirror
```

SVMピア関係の削除

2つのStorage Virtual Machine（SVM）間の関係が不要になった場合、クラスタ管理者は、`vserver peer delete`コマンドを使用してそのSVMピア関係を削除できます。

開始する前に

SVMピア関係に基づいて定義されているSnapMirror関係を削除しておく必要があります。

タスク概要

ピア関係にあるクラスタのどちらかがclustered Data ONTAP 8.2または8.2.1を実行している場合、両方のピア クラスタからSVMピア関係を削除する必要があります。

複数のSSHセッションを使用するか、スクリプトを使用すると、複数のSVMピア関係を同時に削除できます。

注: パフォーマンスの低下を避けるため、同時に削除するSVMピア関係は5個以下にすることを推奨します。

手順

1. どちらかのピア クラスタで`vserver peer delete`コマンドを実行し、SVMピア関係を削除します。

   例

   次のコマンドを実行すると、両方のクラスタからSVMピア関係が削除されます。

   ```
   cluster1::> vserver peer delete -vserver vs1.example0.com -peer-
   vserver vs3.example0.com

   Info: [Job 47] 'vserver peer delete' job queued
   ```

2. ピア クラスタのどちらか1つを使用できないために`vserver peer delete`コマンドが失敗した場合、次のいずれかを実行します。

   - 2つのクラスタ間にネットワーク接続を確立し、`vserver peer delete`コマンドを使用してSVMピア関係を削除します（推奨）。
   - クラスタ ピア関係が再確立されない場合は、ローカル クラスタとピア クラスタの両方で、`vserver peer delete`コマンドに`-force`オプションを指定して使用し、SVMピア関係を削除します。

3. 両方のクラスタで`vserver peer show`コマンドを使用して、削除したSVMピア関係が表示されないことを確認します。

   例

   ```
   cluster1::> vserver peer show

                     Peer                Peer
     Vserver         Vserver             State
   -----------       -----------         ------------
   vs1.example0.com  vs3.example0.com     peered
   ```

4. `deleted`状態のSVMピア関係がある場合、`vserver peer delete`コマンドを使用してそのSVMピア関係を削除します。

関連タスク

クラスタのピア関係での相互接続（272ページ）

SVMピア関係の中断

クラスタ管理者は、必要に応じてvserver peer suspendコマンドを使用し、確立しているSVMピア関係を中断できます。たとえば、メンテナンス時にはSVMピア関係を中断することを推奨します。

タスク概要

SVMピア関係を一時中断しても、SVMピア関係の中断前に開始されたSnapMirrorのデータ転送は影響を受けず、処理を完了させることができます。中断期間にスケジュールされていたデータ転送は開始されません。

手順

1. どちらかのピア クラスタでvserver peer suspendコマンドを使用して、アクティブなSVMピア関係を中断します。

   例

   次の例は、SVMSVMピア関係を中断する方法を示しています。

   ```
   cluster2::> vserver peer suspend -vserver vs4.example1.com -peer-
   vserver vs0.example1.com

   Info: [Job 50] 'vserver peer suspend' job queued
   ```

   SVMピア関係は中断の状態になります。

2. vserver peer showコマンドを使用して、SVMピア関係のステータスを確認します。

   例

   次の例は、SVMピア関係のステータスを確認する方法を示しています。

   ```
   cluster2::> vserver peer show
                       Peer                Peer
   Vserver             Vserver             State
   -----------        -----------         ------------
   vs4.example1.com   vs0.example1.com    suspended
   ```

   これらのコマンドの詳細については、マニュアル ページを参照してください。

SVMピア関係の再開

クラスタ管理者は、vserver peer resumeコマンドを使用して、中断していたSVMピア関係を再開できます。たとえば、保守の完了後に、中断していたSVMピアリング関係を再開できます。

タスク概要

中断期間にスケジュールされていたSnapMirrorのデータ転送は、SVMピア関係を再開しても開始されません。したがって、手動でデータ転送を開始する必要があります。

手順

1. どちらかのピア クラスタでvserver peer resumeコマンドを使用して、中断していたSVMピア関係を再開します。

例

次の例は、中断していたSVMピア関係を再開する方法を示しています。

```
cluster1::> vserver peer resume -vserver vs4.example1.com -peer-
vserver vs0.example1.com

Info: [Job 76] 'vserver peer resume' job queued
```

SVMピア関係はpeeredの状態になります。

2. `vserver peer show`コマンドを使用して、SVMピア関係のステータスを確認します。

例

次の例は、SVMピア関係のステータスを確認する方法を示しています。

```
cluster1::> vserver peer show

                  Peer              Peer
Vserver           Vserver           State
-----------       -----------       ---------
vs4.example1.com  vs0.example1.com   peered
```

これらのコマンドの詳細については、マニュアル ページを参照してください。

SVMピア関係に関する情報の表示

ピアStorage Virtual Machine（SVM）は、完全に機能するSVMで、ローカルまたはリモートのどちらかです。クラスタ管理者とSVM管理者は、`vserver peer show`コマンドを使用してSVMのピアを表示し、ピアSVMのボリューム間のピアリング アプリケーション（SnapMirrorなど）をセットアップすることができます。

タスク概要

また、SVMピア関係のステータスと、そのピア関係上で稼働しているアプリケーションを表示することもできます。

手順

1. 該当するコマンドを使用し、SVMピア関係の詳細を表示します。

表示する情報	入力するコマンド

ピアSVMとピア状態	`vserver peer show`
	次の例は、ピアStorage Virtual Machine（SVM、旧Vserver）に関する情報を表示する方法を示しています。
	`cluster1::> vserver peer show`
	`Vserver  Peer Vserver  Peer State`
	`vs1.example0.com  vs3.example0.com  peered`
	`vs1.example0.com  vs5.example0.com  rejected`
	`2 entries were displayed.`

表示する情報	入力するコマンド

SVMピア関係で稼働しているアプリケーション	`vserver peer show-all`
	次の例は、ピアSVMに関する情報を表示する方法を示しています。
	`cluster1::> vserver peer show-all`
	`Peer Vserver Peer State Peer Cluster Peering Applications`
	`--- --- --- --- ---`
	`vs1.example0.com vs5.example0.com peered cluster2 snapmirror`

このコマンドの詳細については、マニュアル ページを参照してください。

用語集

A

ACL

Access Control List（アクセス制御リスト）の略。

active/active configuration（アクティブ / アクティブ構成）

- Data ONTAP 7.2および7.3リリース ファミリーで、2つのシステムのどちらかが機能を停止した場合に、相互にデータを処理するように設定されたストレージ システムまたはVシリーズ システム（別名*ノード*）のペアのことです。*アクティブ / アクティブ ペア*と呼ぶこともあります。
- Data ONTAP 8.xリリース ファミリーでは、*high-availability（HA;ハイアベイラビリティ）構成*または*HAペア*と呼ばれます。
- Data ONTAP 7.1リリース ファミリーとそれ以前のリリースでは、*クラスタ*と呼ばれます。

address resolution（アドレス解決）

LANまたはWANの宛先に対応するアドレスを判定する手順。

管理SVM

以前の名称はVserverです。clustered Data ONTAPで、他のSVMが所有するオブジェクトも含め、クラスタ内のすべてのオブジェクトへの全般的な管理アクセス権を持つが、クライアントまたはホストへのデータ アクセスは提供しないStorage Virtual Machine（SVM）。

administration host（管理ホスト）

Telnetまたはリモート シェル接続経由でストレージ システムを管理するために使用されるクライアント コンピュータ。

Application Program Interface（API;アプリケーション プログラム インターフェイス）

アプリケーション プログラムが、オペレーティング システムまたはその他のシステム、制御プログラム、通信プロトコルとの通信に使用する言語およびメッセージ形式。

authentication（認証）

セキュリティで保護されたシステムまたはネットワークにログインするユーザのIDを検証するプロセス。

AutoSupport

Unified Managerサービスで障害が発生した場合に、お客様のサイトからテクニカル サポートまたはその他の指定した宛先にEメール メッセージを送信する統合テクノロジ。これらのメッセージには、機能の利用率指標、構成およびユーザ設定、システム ヘルスなどの情報が含まれています。

B

big-endian（ビッグエンディアン）

最上位バイトから処理される、ストレージおよび伝送用のバイナリ データ形式。

C

caching module（キャッシング モジュール）

PCIeベースのFlash Cache 2、Flash Cache、またはPerformance Acceleration Module（PAM）メモリ モジュール。インテリジェントな外部読み取りキャッシュとして機能し、ランダム リード中心のワークロードのパフォーマンスを最適化します。このハードウェアは、

Data ONTAPのWAFL外部キャッシュ ソフトウェア コンポーネントと連携して機能します。

CIFS share（CIFS共有）

- Data ONTAPにおいて、ネットワーク ユーザが使用できるように設定されたディレクトリまたはディレクトリ構造。CIFSクライアントのドライブ レターにマッピングできます。単に*共有*と呼ぶこともあります。
- OnCommand Insight（旧SANscreenスイート）において、NASデバイスから公開されるサービス。CIFSプロトコルでファイルベースのストレージを提供します。CIFSは主にMicrosoft Windowsクライアントを対象としていますが、その他のさまざまなオペレーティング システムもCIFS共有にアクセスできます。

CLI

command-line interface（コマンドライン インターフェイス）の略。ストレージ システム プロンプトは、コマンドライン インターフェイスの一例です。

client（クライアント）

クライアント / サーバ アーキテクチャのワークステーションまたはPC。サービスを要求し、別のコンピュータ システムまたはプロセスの応答を受け入れるコンピュータ システムまたはプロセスです。

cluster（クラスタ）

- clustered Data ONTAP 8.xでは、ネームスペースを共有し、1つまたは複数の仮想サーバとして管理できる接続されたノード（ストレージ システム）のグループを指します。これにより、パフォーマンス、信頼性、拡張性が向上します。
- Data ONTAP 7.1リリース ファミリーおよび以前のリリースでは、2つのシステムのどちらかが機能を停止した場合に、相互にデータを処理するように設定されたストレージ システム（別名*ノード*）のペアのことです。
- Data ONTAP 7.3および7.2リリース ファミリーでは、*アクティブ / アクティブ構成*といいます。
- ストレージ アレイ ベンダーによっては、ホスト アダプタとポートが存在するハードウェア コンポーネントを*クラスタ*と呼んでいます。同様のコンポーネントを*コントローラ*と呼ぶストレージ アレイ ベンダーもあります。

cluster SVM（クラスタSVM）

データSVMの旧称。「data SVM（データSVM）」を参照してください。

Common Internet File System（CIFS）

Microsoftのファイル共有ネットワーク プロトコル。Server Message Block（SMB;サーバ メッセージ ブロック）から発展したものです。

community（コミュニティ）

SNMPエージェントおよび1つ以上のSNMPマネージャ間の論理的な関係。コミュニティは名前によって識別され、コミュニティの全メンバーは、同じアクセス権を持ちます。

console（コンソール）

ストレージ システムの監視と制御に使用される物理端末または仮想端末。

Copy-On-Write（COW）

過度のディスク スペースを消費せずにSnapshotコピーを作成する手法。

D

data SVM（データSVM）

以前の名称はデータVserverです。clustered Data ONTAPでは、クラスタからデータ アクセスを提供するStorage Virtual Machine（SVM）を指します。クラスタのハードウェアとストレージ リソースは、クラスタ内のデータSVMによって動的に共有されます。

degraded mode（デグレード モード）

RAIDグループで1本のディスクに障害が発生した場合、またはNVRAMカードのバッテリ残量が少ない場合に使用される、ストレージ システムの動作モード。

disk ID number（ディスクID番号）

ストレージ システムが、起動時にディスクを確認する際に各ディスクに割り当てる番号。

disk sanitization（ディスク完全消去）

指定したディスク上の既存データを、周知のデータ リカバリ手段ではリカバリできないように物理的に完全に消去する、複数の書き込みプロセス。

disk shelf（ディスク シェルフ）

ディスク ドライブを搭載し、ストレージ システムに接続されるシェルフ。

E

emulated storage system（エミュレート ストレージ システム）

テイクオーバー ストレージ システムによってホストされる、障害ストレージ システムのソフトウェア コピー。ユーザおよび管理者からは、障害ストレージ システムが正しく動作しているように見えます。たとえば、エミュレート ストレージ システムには障害ストレージ システムと同じ名前が付けられます。

Ethernet adapter（イーサネット アダプタ）

イーサネット インターフェイス カード。

expansion card（拡張カード）

ストレージ システムの拡張スロットに挿入するSCSIカード、NVRAMカード、ネットワーク カード、ホットスワップ カード、またはコンソール カード。*アダプタ*と呼ぶこともあります。

expansion slot（拡張スロット）

拡張カードを挿入するストレージ システム ボード上のスロット。

F

failed storage system（障害ストレージ システム）

動作を停止した物理ストレージ システム。ハイアベイラビリティ構成では、ギブバックが正常に行われるまで、このストレージ システムは障害システムのままとなります。

Flash Cache module（Flash Cacheモジュール）

PCIeベースのソリッド ステート メモリ モジュール。インテリジェントな外部読み取りキャッシュとして機能し、ランダム リード中心のワークロードのパフォーマンスを最適化します。Flash Cache 2モジュールはFlash Cacheモジュールの後継です（Flash CacheモジュールはPerformance Acceleration Module（PAM）の後継です）。このハードウェアは、Data ONTAPのWAFL外部キャッシュ ソフトウェア コンポーネントと連携して機能します。

G

giveback（ギブバック）

コントローラ フェイルオーバーの原因となった問題が解決されたあと、2つのストレージ システムが相手データの制御を返すことができるようにするテクノロジ。

global namespace（グローバル ネームスペース）

*「namespace（ネームスペース）」*を参照してください。

group（グループ）

Data ONTAP 7-Modeにおいて、ストレージ システムの`/etc/group`ファイルに定義されているユーザの集まり。

Group ID（GID;グループID）

UNIXシステムがグループの識別に使用する番号。

H

HA（high availability;ハイアベイラビリティ）

- Data ONTAP 8.xでは、2つのノードのどちらかが機能を停止した場合に相互にデータを処理するように設定されたノード（ストレージ システム）のペアが提供するリカバリ機能を指します。このノード ペアは*HAペア*と呼ばれます。
- Data ONTAP 7.3および7.2リリース ファミリーでは、*アクティブ / アクティブ構成*といいます。

HA pair（HAペア）

- Data ONTAP 8.xでは、2つのノードのどちらかが機能を停止した場合に相互にデータを処理するようにコントローラが設定されたノードのペアを指します。
  システム モデルに応じて、両方のコントローラを1つのシャーシに配置することも、別々のシャーシに配置することもできます。
- Data ONTAP 7.3および7.2リリース ファミリーでは、*アクティブ / アクティブ構成*といいます。

heartbeat（ハートビート）

アクティブ / アクティブ構成において、一方のストレージ システムから他方のストレージ システムに対して繰り返し送信される信号。ストレージ システムが動作中であることを示します。ハートビート情報はディスク上にも格納されます。

hot swap（ホット スワップ）

ストレージ システムの実行中にディスクの追加、取り外し、交換を行うプロセス。

hot swap adapter（ホット スワップ アダプタ）

ファイルシステム アクティビティへの影響を最小限に抑えて、ハード ディスクを追加または取り外しできるようにする拡張カード。

I

inode

ストレージ システム上およびUNIXファイルシステム内のファイルに関する情報を含むデータ構造。

interrupt switch（割り込みスイッチ）

一部のストレージ システムの前面パネルに装備されているスイッチ。デバッグに使用します。

M

Maintenance mode（保守モード）

システム ブート ディスクからストレージ システムをブートするときに利用できるオプション モードの1つ。保守モードでは、ハードウェアと設定のトラブルシューティング用の特別なコマンドを使用できます。

N

namespace（ネームスペース）

Network-Attached Storage（NAS;ネットワーク接続型ストレージ）環境において、ファイルとファイルへのパス名の集合。

NDMP

Network Data Management Protocol（ネットワークデータ管理プロトコル）の略。ストレージ システムがバックアップ アプリケーションと通信できるようにし、複数のテープ バックアップ デバイスの自動制御機能を提供するプロトコル。

network adapter（ネットワーク アダプタ）

イーサネット、FDDI、またはATMカード。

node SVM（ノードSVM）

以前の名称はノードVserverです。clustered Data ONTAPにおいて、ある時点においてクラスタ内の1つのノードでのみ動作可能で、そのノードが所有するオブジェクトへの管理アクセスを提供するStorage Virtual Machine（SVM）。ノードSVMは、クライアントやホストへのデータ アクセスは提供しません。

normal mode（通常モード）

HA構成でテイクオーバーが実行されていないときのストレージ システムの状態。

NVMEM

揮発性メモリの略。

NVRAM cache（NVRAMキャッシュ）

ストレージ システム上の不揮発性ランダム アクセス メモリ。受信する書き込みデータおよびNFS要求のロギングに使用されます。NVRAMキャッシュはシステム パフォーマンスを向上させ、ストレージ システムの障害または電源障害が発生した場合のデータ損失を防ぎます。

NVRAM card（NVRAMカード）

ストレージ システムのNVRAMキャッシュを搭載するアダプタ カード。

NVRAM mirror（VRAMミラー）

アクティブ / アクティブ構成において、ストレージ システムのNVRAM（不揮発性RAM）の内容が同期的に更新されたコピー。パートナー ストレージ システムによって維持されます。

P

PAM（Performance Acceleration Module）

PCIeベースのDRAMメモリ モジュール。インテリジェントな外部読み取りキャッシュとして機能し、ランダム リード中心のワークロードのパフォーマンスを最適化します。このハードウェアはFlash Cacheモジュールの前身で、Data ONTAPのWAFL外部キャッシュ ソフトウェア コンポーネントと連携して機能します。

panic（パニック）

Data ONTAPを実行しているシステムの動作停止を引き起こしている重大なエラー状況。Windowsシステム環境のソフトウェア クラッシュに似ています。

parity disk（パリティ ディスク）

RAID 4ディスクドライブ アレイのパリティ情報が格納されているディスク。RAID-DP保護機能を持つRAIDグループでは、2本のパリティ ディスクにパリティ情報およびダブルパリティ情報が格納されます。障害が発生したディスク ブロック内またはディスク上のデータの再構築に使用されます。

partner mode（パートナー モード）

テイクオーバー時にコマンドライン インターフェイスから仮想ストレージ システムを制御するために使用される方法。

partner node（パートナー ノード）

ローカル ノード（ストレージ システム）から見て、HA構成のもう一方のノード。

Performance Acceleration Module（PAM）

*「PAM（Performance Acceleration Module）」*を参照してください。

POST

Power-on self-tests（電源投入時自己診断テスト）の略。電源投入時にストレージ システムによって実行されるテスト。

Q

qtree

仮想サブ ボリュームとして動作するボリュームのルートにある特別なサブディレクトリ。特殊な属性を備えています。

R

RAID

Redundant Array of Independent Disksの略。ストレージ アレイ内の全ディスクの内容に基づいてパリティ情報を算定することにより、ディスク障害から保護する手法。ストレージ システムでは、RAID4（すべてのパリティ情報を単一ディスクに格納）またはRAID-DP（すべてのパリティ情報を2本のディスクに格納）を使用します。

RAID disk scrubbing（RAIDディスク スクラビング）

システムがRAIDグループ内の各ディスクを読み取り、データを別のディスク領域に再書き込みすることでメディア エラーを修正しようとするプロセス。

S

serial adapter（シリアル アダプタ）

一部のストレージ システム モデルにおいて、端末をコンソールとして接続するための拡張カード。

serial console（シリアル コンソール）

ストレージ システムのシリアル ポートに接続されるASCII端末またはANSI端末。ストレージ システムの動作を監視および管理するために使用されます。

SFO

*「storage failover（SFO;ストレージ フェイルオーバー」*を参照してください。

SID

Windowsオペレーティング システムによって使用されるセキュリティ識別子。

Snapshot copy（Snapshotコピー）

ファイルシステム全体のオンラインの読み取り専用コピー。これによって、ファイルの内容を複製しないで、ユーザのミスによる削除や変更からファイルを保護できます。ユーザがファイルをリストアしたり、使用中のストレージ システムをテープにバックアップしたりできるようになります。

storage failover（SFO;ストレージ フェイルオーバー）

clustered Data ONTAPでは、障害が発生したノードのデータ サービスをHAペアの別のノードに移行してデータの可用性を確保する方法です。一般的に、データ サービスの移行はユーザやアプリケーションに対して透過的に行われます。Data ONTAP 7.2以降およびData ONTAP 7-Modeでは、このフェイルオーバー方法は*コントローラ フェイルオーバー*と呼ばれます。

Storage Virtual Machine（SVM）

clustered Data ONTAP 8.2.1より前の名称は*Vserver*。CLI画面およびvserverコマンド構文では引き続き「Vserver」を使用。一意のネットワーク アドレスでネットワーク アクセスを提供し、個別のネームスペースからデータを提供することができる仮想マシン。クラスタの残りのエンティティとは別に管理可能です。SVMには*管理*、*データ*、および*ノード*の3つの種類があります。特に明示する必要がないかぎり、「SVM」は通常データSVMを指します。

SVM

Storage Virtual Machineの略。clustered Data ONTAP 8.2.1より前の名称は*Vserver*。CLI画面およびvserverコマンド構文では引き続き「Vserver」を使用。一意のネットワーク アドレスでネットワーク アクセスを提供し、個別のネームスペースからデータを提供することができる仮想マシン。クラスタの残りのエンティティとは別に管理可能です。SVMには*管理*、*データ*、および*ノード*の3つの種類があります。特に明示する必要がないかぎり、「SVM」は通常データSVMを指します。

T

takeover（テイクオーバー）

HAペアにおいて、障害ノードのアイデンティティをテイクオーバー ノードがエミュレートすること。*ギブバック*の逆です。

takeover mode（テイクオーバー モード）

パートナーの処理を引き継いでいるノード（ストレージ システム）と対話する方法。ノードが現在テイクオーバー モードかどうかは、コンソール プロンプトに示されます。

takeover node（テイクオーバー ノード）

一方のノード（ストレージ システム）が動作を停止した場合に運用を続行するノード。障害ノードのディスク シェルフおよびネットワーク接続へのアクセスを管理する仮想ノードをホストします。テイクオーバー ノードは自身のIDを保持し、仮想ノードが障害ノードのIDを引き継ぎます。

trap（トラップ）

ストレージ システムでイベントが発生したことを示すために、SNMPエージェントからSNMPマネージャにリクエストなしで送信される非同期メッセージ。

U

UID

ユーザ識別番号の略。

Unicode

16ビットの文字セット標準。非営利協会であるUnicode Inc.によって制定および運営されています。

V

volume

ファイルシステム。

Vserver

clustered Data ONTAP 8.2.1移行の名称は「Storage Virtual Machine（SVM）」。一意のネットワーク アドレスでネットワーク アクセスを提供し、個別のネームスペースからデータを提供することができる仮想マシン。クラスタの残りのエンティティとは別に管理可能です。Vserverには*管理*、*ノード*、および*クラスタ*（「クラスタVserver」はData ONTAP 8.2以降では「データVserver」と呼ばれます）の3つの種類があります。特に明示する必要がないかぎり、「Vserver」は通常クラスタ / データVserverを指します。

W

WAFL

Write Anywhere File Layoutの略。書き込みパフォーマンスを最適化するように設計された、ストレージ システム用のファイルシステム。

WAFL External Cache（WAFL外部キャッシュ）

Performance Acceleration Module（PAM）、Flash Cache、またはFlash Cache 2モジュールが搭載されているストレージ システムでは、このキャッシュによってディスクの読み取り回数を減らしてストレージ システムのパフォーマンスを改善できます。*WAFL拡張キャッシュ*とも呼ばれます。

WINS

Windows Internet Name Serviceの略。

workgroup（ワークグループ）

参照および共有のためにグループ化された、Windows NTまたはWindows for Workgroupsを実行しているコンピュータの集合。

著作権に関する情報

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によ って保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988年10月）およびFAR 52-227-19（1987年6月）のRights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の(c) (1) (ii)項、に規定された制限が適用されます。

商標に関する情報

NetApp、NetAppのロゴ、Go Further, Faster、AltaVault、ASUP、AutoSupport、Campaign Express、Cloud ONTAP、clustered Data ONTAP、Customer Fitness、Data ONTAP、DataMotion、Fitness、Flash Accel、Flash Cache、Flash Pool、FlashRay、FlexArray、FlexCache、FlexClone、FlexPod、FlexScale、FlexShare、FlexVol、FPolicy、GetSuccessful、LockVault、Manage ONTAP、Mars、MetroCluster、MultiStore、NetApp Insight、OnCommand、ONTAP、ONTAPI、RAID DP、RAID-TEC、SANtricity、SecureShare、Simplicity、Simulate ONTAP、Snap Creator、SnapCenter、SnapCopy、SnapDrive、SnapIntegrator、SnapLock、SnapManager、SnapMirror、SnapMover、SnapProtect、SnapRestore、Snapshot、SnapValidator、SnapVault、StorageGRID、Tech OnTap、Unbound Cloud、WAFL、その他の名称は、米国またはその他の国あるいはその両方におけるNetApp,Inc.の登録商標です。その他のブランドまたは製品は、それぞれを保有する各社の商標または登録商標であり、相応の取り扱いが必要です。ネットアップの商標の最新のリストは、*http://www.netapp.com/jp/legal/netapptmlist.aspx*でご覧いただけます。

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitterアカウントもあります。

ご意見やご要望は、*ng-gpso-jp-documents@netapp.com*までお寄せください。その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。

索引

数字

2ノード クラスタ
　説明 *31*

A

Active Directory
　次を参照 : AD
AD
　ユーザとグループに対するクラスタおよびSVMへのアクセスの許可 *121*
admin
　管理権限レベルの使用 *21*
ADユーザまたはグループ
　SVM管理者用のアクセスの許可 *94*
auditlogファイル
　管理アクティビティの監査設定の管理の概要 *162*
AutoSupport
　Eメールで送信したメッセージの構造 *207*
　Eメールで送信したメッセージの内容 *207*
　HTTPまたはHTTPSを使用したメッセージ配信のトラブルシューティング *217*
　Message Matrices *214*
　SMTPを使用したメッセージ配信のトラブルシューティング *219*
　イベント *205*
　イベントトリガー型 *205*
　イベントトリガー型メッセージの内容 *202*
　管理用コマンド *214*
　コア ダンプ ファイルのアップロード *212*
　コア ダンプ ファイルを含むメッセージの送信 *212*
　コンテンツ *205*, *206*
　サブシステム *205*
　サブシステムの概要 *203*
　サポートされる転送プロトコル *208*
　週次メッセージ *206*
　週次メッセージの内容 *202*
　収集サイズと時間割当量 *203*
　重大度のタイプ *208*
　使用するための要件 *198*, *208*
　情報の表示 *214*
　設定 *214*
　セットアップ *210*
　定義 *198*
　トリガーの変更 *214*
　日次メッセージの内容 *202*
　パフォーマンス アーカイブ ファイルのアップロード *213*
　パフォーマンス アーカイブ ファイルを含むメッセージの送信 *213*
　パフォーマンス メッセージの内容 *202*
　ファイル *206*
　マニフェスト *214*
　マニフェスト, 内容 *216*
　メール ホスト サポート
　　転送プロトコル *208*
　メッセージ, 収集されるファイル *216*
　メッセージが送信されるタイミングおよび場所 *199*
　メッセージに含まれるログ ファイル *205*
　メッセージの再送信 *214*
　メッセージの説明の取得 *214*
　メッセージの送信 *214*
　メッセージの内容 *205*
　メッセージを受信しない場合のトラブルシューティング *216*
　有効化と無効化 *214*
　要件
　　サポート, AutoSupportのメール ホスト *208*
　履歴 *214*
AutoSupport OnDemand
　テクニカル サポートへの連絡方法 *206*
AutoSupportのメール ホスト サポート *208*
Autosupportメッセージおよびイベント
　アラートによるトリガー方法 *223*
AutoSupportメッセージおよびイベント
　システム ヘルス アラートによるトリガー *223*

C

callhomeイベント *205*
CA証明書
　サーバのための, クラスタまたはSVMをSSLサーバとして認証するためのインストール *147*
CLI
　Data ONTAPの使用方法の概要 *16*
　値を指定する際のルール *19*
　位置指定パラメータの概要 *25*
　クラスタへのアクセスの概要（クラスタ管理者のみ） *11*
　権限レベルの設定 *22*
　コマンド ディレクトリの移動方法 *18*
　セッション, 自動タイムアウト *28*
　セッション, レコード *27*
　表示環境設定 *22*
CLIコマンド
　実行するシェルの概要 *17*
　ストレージQoS *255*
　編集用キーボード ショートカット *20*
CLIセッション
　管理の概要（クラスタ管理者のみ） *27*
　記録 *27*
　自動タイムアウト時間の管理用コマンド *28*
　レコードの管理用コマンド *27*
command-history.logファイル
　管理アクティビティの監査設定の管理の概要 *162*
　管理アクティビティの監査設定の管理用コマンド *165*
　コマンド履歴ログの転送 *163*

D

Data ONTAL CLI
　位置指定パラメータの概要 *25*
Data ONTAP
　CLIの使用方法の概要 *16*

管理インターフェイスの概要 *11*
ブート環境のプロンプトからのブート *47*
マニュアル ページへのアクセス *26*
Data ONTAP-vプラットフォーム
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール *150*
Data ONTAPコマンド
SPの管理用 *71*

E

EMS
AutoSupportメッセージのデータ *205*
callhomeイベント
EMS *201*
イベント メッセージの管理 *195*
イベントトリガー型AutoSupportメッセージとの関係 *201*
イベントの管理用コマンド *197*
システム ヘルス アラートの通知 *224*
ダッシュボード アラームの通知 *231*
EMSメッセージ
キャッシュの再ウォームアップ *265*
Eメール メッセージ
AutoSupportの構造 *207*

F

FIPS 140-2
Webプロトコル エンジンの管理の概要 *155*
Flash Cache
Flash Poolアグリゲートとの比較 *258*
Flash Cacheモジュール
WAFLキャッシュ メモリの増量について *258*
Flash Poolアグリゲート
Flash Cacheとの比較 *258*
flexscale.rewarmオプション *265*
FlexVol
I/Oのパフォーマンスの制御 *250*
SVM, 説明 *76*
ストレージQoSポリシー グループへの割り当てに関するルール *249*
SVMのルートへの昇格 *106*
FlexVolを備えたSVM
I/Oのパフォーマンスの制御 *110*, *250*
最大数 *79*
作成 *86*
ストレージQoSポリシー グループへの割り当てに関するルール *249*
説明 *76*

G

get要求
管理アクティビティの監査設定の管理の概要 *162*

H

HTTP
AutoSupportメッセージ配信のトラブルシューティング *217*
HTTPS
AutoSupportメッセージ配信のトラブルシューティング *217*
SSL管理, 概要 *158*

I

Infinite Volume
SVM, 説明 *76*
ルート ボリュームとしての新しいボリュームの作成 *106*
Infinite Volumeを備えたSVM
新しいルート ボリュームの作成 *109*
最大数 *79*
作成 *90*
説明 *76*
IPspace
SVM作成時の考慮事項 *83*
クラスタ ピア接続に使用 *284*
クラスタ ピアリングの要件 *277*
IPアドレス
SPへのアクセスの管理 *62*
クラスタ ピアリングの要件 *277*

K

Key Management Interoperability Protocol
次を参照 : KMIP
KMIP証明書
インストールしてクラスタと外部キー管理ツールの相互認証に使用 *150*

L

LDAP
ユーザがクラスタにアクセスできるようにする *123*
LDAPユーザ アカウント
SVM管理者用のアクセスの許可 *93*
LIF
専用のクラスタ間ポートを使用するための設定 *281*
独自のクラスタ間ネットワークの専用ポートを使用するための設定 *284*
LIF, クラスタ間
データ ポートを共有するための設定 *279*
LUN
I/Oのパフォーマンスの制御 *250*
ストレージQoSポリシー グループへの割り当てに関するルール *249*

M

Message Of The Day
次を参照 : MOTD
MetroCluster構成
SVMの起動 *103*
SVMの作成 *89*
命名に関するガイドライン
SVM
作成に関するガイドライン *83*
mgwd.logファイル
管理アクティビティの監査設定の管理の概要 *162*

管理アクティビティの監査設定の管理用コマンド *165*
MIBファイル
ノード, Webブラウザを使用してアクセス *42*
SVMのMOTD
作成 *172*
MOTD
MOTDとバナーの管理, 概要 *168*
クラスタ レベルおよびSVMレベルでの管理 *173*
作成 *172*
My AutoSupport
説明 *216*
ダッシュボード タスク *216*

N

NIS
ユーザがクラスタにアクセスできるようにする *123*
NISユーザ アカウント
SVM管理者用のアクセスの許可 *93*
nsswitch
NISまたはLDAPユーザに対するクラスタへのアクセスの許可 *123*
NTP
クラスタ時間の管理 *166*
クラスタ時間の管理用コマンド *167*

O

OnCommand System Manager
アクセス管理方法 *29*
ブラウザベースのGUIを使用したクラスタへのアクセス *28*

P

PAM
WAFLキャッシュ メモリの増量について *258*
PCS
キャッシュ サイズの変更 *259*
サンプリング解像度の変更 *260*
ワークロード測定の向上 *260*
Performance Acceleration Moduleファミリー
WAFLキャッシュ メモリの増量について *258*
Predictive Cache Statistics
次を参照 : PCS

Q

QoS
次を参照 : ストレージQoS
QoSポリシー グループ
SVMの変更 *100*

R

RAVE
ヒストグラムベースの予測のサポート *257*
RAVEを使用したヒストグラムベースの予測サポート *257*
RBAC
アクセス制御ロールのカスタマイズに関する考慮事項 *129*
RDB
クラスタ レプリケーション リング, 説明 *34*
rowsコマンド
CLIでの表示環境設定 *22*
RSH
クラスタへのアクセスに使用 *15*
クラスタへのアクセスの有効化 *13*

S

Secure Socket Layer
次を参照 : SSL
security certificateコマンド
デジタル証明書の管理用 *153*
setコマンド
CLIでの表示環境設定 *22*
set要求
管理アクティビティの監査設定の管理の概要 *162*
showコマンドの出力
フィールドを使用したカスタマイズ方法 *24*
SMTP
AutoSupportメッセージ配信のトラブルシューティング *219*
Snapshotポリシー
SVMの変更 *100*
SP
APIサービス設定の変更 *56*
CLIでのオンライン ヘルプの使用 *63*
Data ONTAPからの管理用コマンド *71*
SP CLIセッション, SPコンソール セッション, システム コンソール セッションの関係 *61*
SPネットワーク設定に関する考慮事項 *52*
アクセス, 概要 *59*
アクセスできるIPアドレスの管理 *62*
アクセスできるアカウント *59*
概要 *50*
管理ホストからのアクセス *59*
システム コンソールからのアクセス *60*
システム センサー コマンド出力内のディスクリートセンサーのステータス値の概要 *69*
自動ネットワーク設定の有効化 *53*
センサーの読み取り値とsystem sensorsコマンドのしきい値ベースのステータス値の概要 *67*
ネットワーク インターフェイスを使用したファームウェア更新 *58*
ネットワークの手動設定 *54*
ネットワークの設定, 概要 *52*
ノードのシステム コンソールへのアクセス *43*
ノードのリモート管理用コマンド *63*
ファームウェアの更新の管理方法 *57*
リモートからのノードの管理に使用, 概要 *50*
SSH
クラスタへのアクセスに使用 *11*
使用したSPへのアクセス, 概要 *59*
セキュリティ設定, 管理の概要 *137*
セキュリティ設定の管理用コマンド *139*
ssh要求
SPにアクセスできるIPアドレスの管理 *62*
SSL
Webプロトコル エンジンの管理の概要 *155*

管理, 概要 158
管理用コマンド 159
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール 150
サーバまたはクライアント認証用のデジタル証明書の管理 140
SSLv3
Webプロトコル エンジンの管理の概要 155
SSLクライアント
クラスタまたはSVM, 認証するためのクライアントCA証明書またはルートCA証明書のインストール 144
クラスタまたはSVMを認証するためのクライアント証明書のインストール 148
SSLサーバ
クラスタまたはSVMを認証するためのサーバCA証明書のインストール 147
クラスタまたはSVMを認証するためのサーバ証明書のインストール 141
statisticsコマンド
クラスタとSVMのパフォーマンスの監視用 241
SVM
ADユーザまたはグループ アカウントの作成 94
FlexVolを備えたSVM, 説明 76
Infinite Volumeを備えたSVM, 説明 76
MetroCluster構成用に作成 89
NISまたはLDAPユーザ アカウントの作成 93
SVMコンテキストからの管理 105
SVMの属性の変更 100
アクセス方式と認証方式 113
アクセスをSVM管理者に提供するためのユーザ アカウントの作成 92
管理 76
管理機能 112
管理に関する詳細情報 117
管理の委譲 95
管理の定義 32
起動 103
クラスタ間ピア関係の作成 295
クラスタ内ピア関係の作成 296
言語オプション 84
言語設定 86
高度な方法を使用したパフォーマンスの監視の概要 238
削除 102
作成計画 80
作成に関するガイドライン 83
使用する利点 78
情報の表示 100, 115
設定 92
セットアップ 80
タイプ 78
停止 104
デスティネーション, ディザスタリカバリ用に作成 88
名前変更 102
ネットワーク設定の表示 116
パスワードの変更 115
パフォーマンスの監視の概要 233
ピア関係の管理 292
ピア関係の拒否 298
ピア関係の再開 301
ピア関係の削除 298, 300
ピア関係の作成 294
ピア関係の状態 294
ピア関係の承認 297
ピア関係の説明 293
ピア関係の中断 301
ピア関係の表示 302
ピア関係の変更 299
変更 97
ルート ボリューム, LSミラーの昇格 107
ルート ボリューム, データ保護ミラーの昇格 108
ルート ボリュームとしての新しいFlexVolの昇格 108
ルート ボリュームの概要 78
ローカル ユーザ アカウントの作成 93
ログイン 114
SVM管理者
クラスタ管理者との違い 10
事前定義されたロール 127
SVM属性の変更 100
SVMの作成
データ アクセス用 87
SVMの停止の失敗
トラブルシューティング 104
SVMの起動の失敗
トラブルシューティング 103
SVMレベルのMOTD
管理 173
SVMレベルのバナー
管理 171
syslogサーバ
コマンド履歴ログの転送 163
sysmgr Webサービス
OnCommand System Managerへのアクセス管理方法 29
System Manager
OnCommand, アクセス管理方法 29
OnCommand, ブラウザベースのグラフィカル インターフェイスを使用したクラスタへのアクセス 28
概要 29
実行できる作業 29

T

Telnet
クラスタへのアクセスの有効化 13
クラスタへのアクセスに使用 14
TLSv1
Webプロトコル エンジンの管理の概要 155
Twitter
マニュアルの変更に関する自動通知の受信方法 314

U

UUID
クラスタ ノードに関する情報の表示 34

V

Vserver
次を参照 : SVM

W

WAFLcacheメモリ
　増量の概要 *258*
WAFL外部キャッシュ
　Flash Poolアグリゲートとの比較 *258*
　再ウォームアップ *263*
　シーケンシャル リード データのキャッシュ *262*
　システム メタデータのキャッシング *261*
　設定の表示 *262*
　標準ユーザ データ ブロック *260*
　無効化 *259*
　有効化 *259*
　優先度が低いユーザ データ ブロック *261*
　ランダム ライト ワークロード ブロックのキャッシュ *262*
　利用率およびアクセスに関する情報の表示 *263*
watchdog
　システム, システム センサー コマンド出力内のディスクリートSPセンサーのステータス値の概要 *69*
Webアクセス
　SSL管理, 概要 *158*
Webサービス
　OnCommand System Managerのブラウザベースのグラフィカル インターフェイスを使用したクラスタへのアクセス *28*
　アクセス権を設定する *159*
　アクセスに関する問題のトラブルシューティング *160*
　アクセスの管理 *154*
　管理方法 *156*
　管理用コマンド *157*
　ユーザ アクセスの要件 *156*
Webブラウザ
　ノードのログ ファイル、コア ダンプ ファイル、MIBファイルにアクセス *42*
Webプロトコル エンジン
　管理の概要 *155*
　管理用コマンド *156*
Write Anywhere File Layout
　*次を参照：*WAFL

あ

アーカイブ ファイル
　パフォーマンス, テクニカル サポートへのアップロード *213*
アカウント
　SPへのアクセス用 *59*
　パスワード ルールの設定に関する考慮事項 *134*
　ユーザのアクセス方法 *120*
　ユーザの管理用コマンド *125*
　ユーザを管理する方法 *119*
空きスペースの再配置
　概要 *267*
　サポートされるアグリゲート *269*
　仕組み *267*
　ステータスの表示 *269*
　他の再配置機能と合わせて使用する *268*
　無効化 *269*
　有効化 *269*
　有効化する状況 *268*
アクセス
　ADユーザとグループに対するクラスタおよびSVMへのアクセスの許可 *121*
　Data ONTAPマニュアル ページ *26*
　NISまたはLDAPユーザに対するクラスタへのアクセスの許可 *123*
　OnCommand System Manager, 管理方法 *29*
　OnCommand System Managerのブラウザベースのグラフィカル インターフェイスを使用したクラスタ *28*
　RSHを使用したクラスタ *15*
　SP, 概要 *59*
　SPにアクセスできるIPアドレスの管理 *62*
　SPにアクセスできるアカウント *59*
　SSHを使用したクラスタ *11*
　SVM管理者用のADユーザまたはグループへのアクセスの許可 *94*
　SVM管理者用のNISまたはLDAPユーザ アカウントへのアクセスの許可 *93*
　Telnetを使用したクラスタ *14*
　Webサービスについての設定 *159*
　Webサービス用の管理 *154*
　Webブラウザを使用してノードのログ ファイル、コア ダンプ ファイル、およびMIBファイルに *42*
　アクセス制御ロールをカスタマイズして、指定されたコマンドにユーザ アクセスを制限する *132*
　管理ホストからのSP *59*
　クラスタ, CLIを使用する場合の概要（クラスタ管理者のみ） *11*
　クラスタ管理の概要（クラスタ管理者のみ） *119*
　クラスタシェル内のノードシェル コマンドおよびオプション *17*
　シリアル ポートがあるクラスタ *11*
　ノードのシステム コンソール *43*
　リモート, SPの概要 *50*
アクセス制御ロール
　カスタマイズして指定されたコマンドにユーザ アクセスを制限する *132*
　カスタマイズに関する考慮事項 *129*
　管理の概要 *126*
　管理用コマンド *135*
　クラスタ管理者の事前定義されたロール *127*
　のユーザ名およびパスワードのルール設定の管理 *133*
アクセスに関する問題
　Webサービスのトラブルシューティング *160*
アクセス方式
　SVM *113*
アクセス方法
　ユーザ アカウント *120*
アグリゲート
　書き込みパフォーマンスの向上 *267*
　ノードのルートに関するルール *44*
　SVMへのアグリゲート リストの変更 *98*
値
　CLIで指定する際のルール *19*
アップロード
　コア ダンプ ファイル *212*
　パフォーマンス アーカイブ ファイル *213*
アプリケーション タイプ
　SPにアクセスできるアカウント *59*
アラート

AutoSupportメッセージおよびイベントのトリガー方法 *223*
システム ヘルスのカスタマイズ *222*
システム ヘルスの監視の概要 *221*
対応 *222*
ヘルスモニタで使用されるトリガー *221*
アラートによるAutoSupportメッセージおよびイベントのトリガー方法
ヘルスの監視 *223*
アラートへの対応方法
ヘルスの監視 *222*
アルゴリズム
キー交換とデータ暗号化, SSHセキュリティ設定の管理の概要 *137*
暗号
キー交換とデータ暗号化, SSHセキュリティ設定の管理の概要 *137*
暗号化アルゴリズム
データ, SSHセキュリティ設定の管理の概要 *137*

い

委譲
SVMの管理 *95*
位置指定パラメータ
概要 *25*
イプシロン
クラスタ ノードに設定されているかどうかに関する情報の表示 *34*
クラスタの概要 *33*
イベント
AutoSupportメッセージ *205*
管理用コマンド *197*
イベント管理システム
イベントの管理用コマンド *197*
セットアップ *196*
次も参照 : EMS
イベントトリガー型AutoSupportメッセージ
AutoSupportよる作成および送信 *201*
送信されるタイミングおよび場所 *199*
イベント メッセージ
数の削減 *196*
管理 *195*
インスタンス
説明 *234*
インターフェイス
Data ONTAP管理の概要 *11*
Data ONTAPコマンドラインの使用方法の概要 *16*
グラフィカル, OnCommand System Managerのブラウザベースインターフェイスを使用したクラスタへのアクセス *28*

え

エラー メッセージ
キャッシュの再ウォームアップ *265*
演算子
クエリの使用方法 *23*

お

オブジェクト
説明 *234*
データ収集をパフォーマンス プリセットで定義する方法 *234*
パフォーマンス データの収集と表示 *235*
パフォーマンス プリセットのインポート *238*
オンライン ヘルプ
SP CLIを使用する場合 *63*

か

ガイドライン
SVMの作成 *83*
外部キー管理ツール
クラスタとの相互認証に使用するKMIP証明書のインストール *150*
外部キャッシュ
WAFLメモリの増量の概要 *258*
概要 *266*
カウンタ
説明 *234*
パフォーマンス プリセットのインポート *238*
書き込みワークロード
ランダム ブロックのキャッシュ *262*
拡張クエリ
使用方法 *24*
カスケード構成
クラスタ ピアリングのネットワーク要件 *277*
環境設定
CLIでの表示の設定 *22*
環境センサー
情報の表示 *244*
関係
SVMのピアリング, 説明 *293*
SVMピア関係の削除 *300*
クラスタ間SVMピアの作成 *295*
クラスタ内SVMピアの作成 *296*
クラスタ ピアの管理用コマンド *270*
クラスタ ピアの削除 *292*
クラスタ ピアの作成 *290*
クラスタ ピアの認証 *272*
SVMピアの作成 *294*
監査設定
管理アクティビティについての管理の概要 *162*
管理用コマンド, 管理アクティビティ *165*
監査ログ
コマンド履歴の転送 *163*
監視
システム接続, 概要 *221*
システム ヘルス アラートを使用 *222*
スイッチ, 概要 *221*
dashboard（ダッシュボード） *231*
ダッシュボードの管理用コマンド *232*
ノード接続, 概要 *221*
リモート, SPの概要 *50*
管理
SVMの委譲 *95*
クラスタ上のイベント, コマンド *197*
管理SVM
説明 *78*

定義 32
管理アクティビティ
監査設定の管理の概要 162
監査設定の管理用コマンド 165
管理インターフェイス
Data ONTAPの概要 11
管理権限
レベルの使用 21
管理者
クラスタとSVMの違い 10
クラスタの事前定義されたロール 127
管理デバイス
リモート, SPの概要 50
管理の基礎
クラスタ, 概要 31
管理ホスト
SPにアクセスできるIPアドレスの管理 62
SPへのアクセス 59
SPへのアクセス, 概要 59

き

キー
公開の管理方法 139
ライセンスの管理 176
キー管理ツール
クラスタと外部ツールの相互認証に使用するKMIP証明書のインストール 150
キー交換アルゴリズム
SSHセキュリティ設定の管理の概要 137
キーボード ショートカット
CLIコマンドの編集 20
起動
SVM
起動 103
キャッシュ
Flash PoolとFlash Cacheの比較 258
PCSでエミュレートされるキャッシュ サイズの変更 259
PCSのサンプリング解像度の変更 260
WAFL外部メモリの増量について 258
シーケンシャル リード データのキャッシュ 262
ランダム ライト ワークロード ブロックのキャッシュ 262
キャッシュの再ウォームアップ
概要 263
仕組み 264
中止イベントとエラー メッセージ 265
トリガー イベント 264
無効化 265
有効化 265
許可
SVMのプロトコル 99
禁止
SVMのプロトコル 99

く

クエリ
拡張の使用方法 24
クエリ演算子
使用方法 23
クォータ ポリシー
SVMの変更 100
クォーラム
クラスタの概要 33
クライアント
サーバの認証用のデジタル証明書の管理 140
クライアントCA証明書
クラスタまたはSVMのSSLクライアントを認証するためのインストール 144
クライアント証明書
SSLクライアントとしてクラスタまたはSVMを認証するためのインストール 148
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール 150
クラスタ
CLIセッションの管理の概要（クラスタ管理者のみ） 27
CLIを使用したアクセスの概要（クラスタ管理者のみ） 11
NISまたはLDAPユーザに対するアクセスの許可 123
RSHによるアクセス 15
SSHによるアクセス 11
Telnetを使用したアクセス 14
アクセスにシリアル ポートを使用 11
アクセスの管理の概要（クラスタ管理者のみ） 119
外部キー管理ツールとの相互認証に使用するKMIP証明書のインストール 150
管理の基礎の概要 31
クォーラムとイプシロンについて 33
クラスタ ピアリングの命名要件 277
構成のバックアップおよびリストア 183
構成バックアップ スケジュールの管理用コマンド 184
構成バックアップ ファイル 183
構成バックアップ ファイルの管理用コマンド 184
自動構成バックアップ 183
シングルノード, 考慮事項 32
説明 31
属性の変更 35
とノードの同期 190
名前変更 35
ノードに関する情報の表示 34
ノードの管理の概要 37
ノードの削除 40
ノードの追加 38
の構成のリカバリ 187
の構成バックアップの管理 183
場所の変更 35
レプリケーション リング, 説明 34
連絡先情報の変更 35
cluster（クラスタ）
属性, 表示 35
レプリケーション リング, ステータスの表示 36
クラスタ アクセス
CLIを使用した概要（クラスタ管理者のみ） 11
TelnetまたはRSHの有効化 13
クラスタ間LIF
専用のクラスタ間ポートを使用するための設定 281
データ ポートを共有するための設定 279
データ ポートを共有する場合の考慮事項 278

独自のネットワークの専用ポートを使用するための設定 *284*
クラスタ間関係
削除 *292*
クラスタ間接続
指定と未指定の違い *276*
クラスタ間ネットワーク
LIFの設定 *284*
クラスタ間LIFの設定 *279*, *281*
クラスタ ピアの定義 *273*
サポートされるトポロジ *273*
データ ポートとクラスタ間ポートを共有する場合の考慮事項 *278*
クラスタ間ポート
専用のクラスタ間を使用する場合の考慮事項 *278*
専用を使用するためのクラスタ間LIFの設定 *281*
クラスタ管理サーバ
定義 *32*
クラスタ管理者
SVM管理者との違い *10*
クラスタへのアクセスの管理の概要 *119*
事前定義されたロール *127*
クラスタ構成
構成バックアップ ファイルを使用したリストア *188*
自動バックアップ *183*
バックアップおよびリストア *183*
バックアップ スケジュールの管理用コマンド *184*
バックアップの管理 *183*
バックアップ ファイル *183*
バックアップ ファイルの管理用コマンド *184*
リカバリ *187*
リカバリする構成の選択 *187*
クラスタシェル
概要 *17*
ノードシェル コマンドおよびオプションへのアクセス *17*
クラスタ時間
管理 *166*
管理用コマンド *167*
クラスタ スイッチ ヘルスモニタ
概要 *223*
コマンド *228*
スイッチ監視の確認 *227*
トラブルシューティング *226*
クラスタのMOTD
作成 *172*
クラスタのバナー
作成 *169*
クラスタ ピア
関係の削除 *292*
関係の作成 *290*
クラスタ間ネットワークの定義 *273*
サポートされるネットワーク トポロジ *273*
クラスタ ピア関係
管理用コマンド *270*
認証 *272*
要件 *277*
クラスタ ユーザ アカウント
SPへのアクセス用 *59*
クラスタ レベルのMOTD
管理 *173*
クラスタ レベルのバナー
管理 *171*
グループ
Active Directory, SVM管理者用のアクセスの許可 *94*
クラスタおよびSVMのADアクセス, ユーザの許可 *121*

け

計画
SVMの作成 *80*
権限レベル
CLIでの設定 *22*
管理の使用 *21*
言語設定
SVMの変更 *100*
言語に関する考慮事項
SVMの作成 *83*

こ

コア セグメント
管理用コマンド *193*
コア ダンプ
管理用コマンド *192*
コア ダンプ ファイル
AutoSupportメッセージの送信 *212*
管理 *191*
テクニカル サポートへのアップロード *212*
ノード, Webブラウザを使用してアクセス *42*
分割方法 *191*
公開鍵
管理方法 *139*
管理用コマンド *140*
パスワードの両方が認証方式に含まれる場合の認証動作 *121*
公開鍵証明書
サーバまたはクライアント認証用のデジタル証明書の管理 *140*
更新
SPファームウェアの管理方法 *57*
構成
カスケード, クラスタ ピアリング *277*
ファンアウト, クラスタ ピアリング *277*
構成バックアップ スケジュール
概要 *183*
管理用コマンド *184*
構成バックアップ ファイル
管理用コマンド *184*
クラスタ構成のリストアに使用 *188*
定義 *183*
ノード構成のリカバリの検索 *185*
ノード構成のリストアに使用 *186*
リカバリするクラスタ構成の検索 *187*
構成ファイル
ノードのルート ボリュームとルート アグリゲートに関するルール *44*
コマンド
CLI, 編集用キーボード ショートカット *20*
CLIセッションの自動タイムアウト時間の管理 *28*
CLIセッションのレコードの管理用 *27*
CLIで値を指定する際のルール *19*

CLIを実行するシェルの概要 *17*
Data ONTAPからのSPの管理用 *71*
SSHセキュリティ設定の管理用 *139*
SSLの管理用 *159*
SVM属性の変更 *100*
Webプロトコル エンジンの管理用 *156*
アクセス制御ロールの管理 *135*
アクセス制御ロールをカスタマイズして、指定されたものにユーザ アクセスを制限する *132*
イベントの管理用 *197*
環境センサー情報の表示用 *244*
管理アクティビティの監査設定の管理用 *165*
クラスタ時間の管理用 *167*
クラスタとSVMのパフォーマンス データの監視用 *241*
クラスタ ピア関係の管理用 *270*
コア ダンプの管理用 *192*
公開鍵の管理用 *140*
システム ヘルス *228*
ジョブ スケジュールの管理用 *181*
ジョブの管理用 *180*
ダッシュボードの管理用 *232*
デジタル証明書の管理用 *153*
ノードシェルで利用可能なコマンドを表示する *18*
ノード上のマウント ポイントの管理用 *158*
フィールドを使用したshow出力のカスタマイズ方法 *24*
ユーザ アカウントの管理用 *125*
ライセンスの管理用 *178*
リモートからのノードの管理用 *63*
履歴表示方法と再発行方法 *20*
コマンド ディレクトリ
CLIの移動方法 *18*
コマンド入力
位置指定パラメータの概要 *25*
コマンドの再発行
方法 *20*
コマンドライン インターフェイス
次を参照 : CLI
コマンド履歴
表示方法 *20*
コマンド履歴ログ
転送 *163*
コメント
マニュアルに関するフィードバックの送信方法 *314*
コンソール
SPへのアクセス, 概要 *59*
システム, ノードへのアクセス *43*
システムからSPへのアクセス *60*
コンソール セッション
SP CLI, SPコンソール, システムの関係 *61*

さ

サーバ
クライアントの認証用のデジタル証明書の管理 *140*
クラスタ管理の定義 *32*
サーバCA証明書
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール *150*
クラスタまたはSVMをSSLサーバとして認証するためのインストール *147*
サーバ証明書
クラスタまたはSVMをSSLサーバとして認証するためのインストール *141*
サービス
Webの管理用コマンド *157*
Webへのアクセスの設定 *159*
Webへのユーザ アクセスの要件 *156*
Webを管理する方法 *156*
サービス プロセッサ
次を参照 : SP
サイズ割当量
AutoSupport *203*
再追加
クラスタへのノード *188*
サイト ライセンス
ライセンス タイプとライセンス方式 *177*
再配置
空きスペース *267*
空きスペース再配置を使用する状況 *268*
読み取り *266*
先読みデータ
キャッシュの有効化 *262*
削除
SVMのプロトコル *99*
SVMピア関係 *300*
SVMへのアグリゲート *98*
作成
FlexVolを備えたSVM *86*
Infinite Volumeを備えたSVM *90*
MetroCluster構成用のSVM *89*
SVM管理者用のローカル ユーザ アカウント *93*
クラスタ間SVMピア関係 *295*
クラスタ内SVMピア関係 *296*
ディザスタ リカバリのデスティネーションSVM *88*
SVMピア関係 *294*
サブシステム
AutoSupport *205*
AutoSupport, 収集サイズと時間割当量 *203*
AutoSupportの概要 *203*
サブネット
SP自動ネットワーク設定の有効化 *53*
クラスタ ピアリングの要件 *277*
サンプリング解像度
PCSでエミュレートされるキャッシュについての変更 *260*

し

シェル
CLIコマンドの概要 *17*
資格
クラスタ ノードに関する情報の表示 *34*
クラスタの参加, ノード属性の変更 *37*
時間
クラスタの管理用コマンド *167*
時間割当量
AutoSupport *203*
しきい値
環境センサーに関する情報の表示 *244*
しきい値ベースのSPセンサー
読み取り値とステータス値の概要, system sensorsコマンド出力 *67*

時刻
クラスタの管理 *166*
資産タグ
ノード属性の変更 *37*
システム
監視の概要 *195*
システムSVM
説明 *78*
システム構成
バックアップおよびリストア *183*
システム コンソール
SPへのアクセス *60*
ノードへのアクセス *43*
システム コンソール セッション
SP CLIセッションとSPコンソール セッションの関係 *61*
システムシェル
概要 *17*
システム接続ヘルスモニタ
概要 *223*
コマンド *228*
システム センサー コマンド出力
しきい値ベースのSPセンサーの読み取り値とステータス値の概要 *67*
ディスクリートSPセンサーのステータス値の概要 *69*
システム パニック
コア ダンプ ファイルの管理 *191*
システム パフォーマンス
管理の概要 *245*
システム プロンプト
ノードのリブート *46*
システム ヘルス
AutoSupportによる監視 *198*
アラートのカスタマイズ *222*
監視の概要 *221*
デグレードへの対応 *225*
デグレードへの対応の例 *225*
システム ヘルス アラート
AutoSupportメッセージおよびイベントのトリガー方法 *223*
対応 *222*
システム ヘルスの監視
コマンド *228*
事前定義されたロール
クラスタ管理者用 *127*
自動設定
SPネットワークの有効化 *53*
自動タイムアウト
CLIセッションの時間の管理用コマンド *28*
シャットダウン
ノード *48*
週次AutoSupportメッセージ
送信されるタイミングおよび場所 *199*
含まれるデータのタイプ *202*
重大度
AutoSupport *208*
出力
フィールドを使用したshowコマンドのカスタマイズ方法 *24*
手動でトリガーされるAutoSupportメッセージ
送信されるタイミングおよび場所 *199*
含まれるデータのタイプ *202*
使用可能なヘルスモニタ
クラスタ用 *223*
使用権のリスク
ライセンスの管理 *176*
詳細
管理権限レベルの使用 *21*
情報
マニュアルの品質向上に関するフィードバックの送信方法 *314*
証明書
KMIP, インストールしてクラスタと外部キー管理ツールの相互認証に使用 *150*
SP API設定の変更 *56*
期限切れのデジタルの交換 *152*
クライアント, SSLクライアントとしてクラスタまたはSVMを認証するためのインストール *148*
サーバ, クラスタまたはSVMをSSLサーバとして認証するためのインストール *141*
サーバCA, クラスタまたはSVMをSSLサーバとして認証するためのインストール *147*
デジタル, サーバまたはクライアント認証用の管理 *140*
デジタル管理のためのコマンド *153*
ショートカット
キーボード, CLIコマンドの編集 *20*
ジョブ
カテゴリ *180*
管理用コマンド *180*
情報の表示 *180*
スケジュールの管理 *180*
ジョブ スケジュール
管理用コマンド *181*
ジョブのカテゴリ
概要 *180*
所有者
ノード属性の変更 *37*
シリアル コンソール
SPへのアクセス *60*
SPへのアクセス, 概要 *59*
ノードへのアクセス *43*
シリアル ポート
クラスタへのアクセスに使用 *11*
新機能
RAVEを使用したヒストグラムベースの予測のサポート *257*
シングルノード クラスタ
説明 *31*
注意事項 *32*
診断
管理権限レベルの使用 *21*

す

スイッチ
クラスタ スイッチ ヘルスモニタを使用する監視の確認 *227*
検出のトラブルシューティング *226*
ヘルスモニタの概要 *221*
スケジュール
ジョブおよびスケジュールの管理 *180*
ジョブの管理用コマンド *181*
スタンドアロン ノード

クラスタに関する考慮事項 *32*
ストレージQoS
概要 *245*
コマンド *255*
最大スループットの仕組み *248*
最大ポリシー グループ数 *250*
最大ワークロード数 *250*
仕組み *245*, *246*
スロットルを適用していないワークロードへの影響 *248*
ポリシー グループの作成 *250*
ポリシー グループの種類 *246*
ポリシー グループのパフォーマンスの監視 *250*
ポリシー グループへのストレージ オブジェクトの割り当て *250*
ポリシー グループへのストレージ オブジェクトの割り当てに関するルール *249*
例
全ワークロードに制限を設定 *254*
非クリティカルなワークロードにプロアクティブな制限を設定 *253*
ワークロードの分離 *252*
ワークフロー *245*
ワークロードの種類 *246*
ワークロードのパフォーマンスの監視 *250*
ワークロード パフォーマンスを監視する方法 *250*
ストレージ暗号化機能
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール *150*
ストレージ システム
監視の概要 *195*
スペース
ノードのルート ボリュームの解放 *45*

せ

セキュアなキー
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール *150*
セキュアなデータ アクセス
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール *150*
セキュリティ
アクセス制御ルールでのユーザ名およびパスワードの管理 *133*
セキュリティ設定
SSHの管理の概要 *137*
SSHの管理用コマンド *139*
セッション
CLIの管理の概要（クラスタ管理者のみ） *27*
CLIの記録 *27*
接続
サポートされるクラスタ ピア ネットワーク トポロジ *273*
指定のクラスタ間接続と未指定のクラスタ間接続の違い *276*
設定
AutoSupport, コマンド *214*
SP APIサービスの変更 *56*
SP自動ネットワークの有効化 *53*
SPネットワークに関する考慮事項 *52*
SVM *92*
管理アクティビティの監査についての管理の概要 *162*
ルールの管理, ユーザ名およびパスワード *133*
セットアップ
AutoSupport *210*
SVM *80*
センサー
環境に関する情報の表示 *244*
しきい値ベースのSPの読み取り値とステータス値の概要, system sensorsコマンド出力 *67*
ディスクリートSPのステータス値の概要, システム センサー コマンド出力 *69*
専用ポート
クラスタ間レプリケーションに使用する場合の考慮事項 *278*

そ

相互認証
クラスタと外部キー管理ツール用のKMIP証明書のインストール *150*
サーバまたはクライアント認証用のデジタル証明書の管理 *140*
双方向認証
クラスタと外部キー管理ツールの相互認証に使用するKMIP証明書のインストール *150*
サーバまたはクライアント認証用のデジタル証明書の管理 *140*
属性
クラスタの変更 *35*
ノードの表示 *37*
ノードの変更 *37*
ソフトウェアの使用権
ライセンスの管理 *176*

た

対応
アラート *222*
システム ヘルス アラート *222*
ダッシュボード
My AutoSupportタスクの実行 *216*
アラームの通知 *231*
概要 *231*
管理用コマンド *232*
ダンプ ファイル
テクニカル サポートへのアップロード *212*

つ

追加
SVMのプロトコル *99*
SVMへのアグリゲート *98*

て

提案
マニュアルに関するフィードバックの送信方法 *314*
ディザスタ リカバリ
デスティネーションSVMの作成 *88*
停止

SVM
停止 *104*
ディスクリートSPセンサー
ステータス値の概要, システム センサー コマンド出力 *69*
ディレクトリ
CLIコマンドの移動方法 *18*
データ
SVMのパフォーマンス, 高度な方法を使用した監視の概要 *238*
シーケンシャル リード ブロックのキャッシュ *262*
パフォーマンス, オブジェクトについての収集と表示 *235*
パフォーマンス, クラスタとSVMの監視用コマンド *241*
パフォーマンス, 継続的に更新されるクラスタとSVMの表示 *240*
データSVM
説明 *78*
データ, パフォーマンス
一定期間のクラスタとSVMの表示 *239*
データ アクセス
FlexVolを備えたSVMの作成 *87*
データ アクセス用に作成 *87*
データ暗号化アルゴリズム
SSHセキュリティ設定の管理の概要 *137*
データのソート
問題の診断または特定 *237*
データ ポート
クラスタ間LIFで共有するための設定 *279*
クラスタ間と共有する場合の考慮事項 *278*
テクニカル サポート
AutoSupport OnDemandが通信する仕組み *206*
デグレードしたシステム ヘルス
対応の例 *225*
デジタル証明書
SSL管理, 概要 *158*
管理用コマンド *153*
期限切れの交換 *152*
クラスタまたはSVMのSSLクライアントを認証するためのクライアントCAまたはルートCA証明書のインストール *144*
クラスタまたはSVMをSSLクライアントとして認証するためのクライアント証明書のインストール *148*
クラスタまたはSVMをSSLサーバとして認証するためのサーバCA証明書のインストール *147*
クラスタまたはSVMをSSLサーバとして認証するためのサーバ証明書のインストール *141*
サーバまたはクライアント認証用の管理 *140*
転送プロトコル
AutoSupportでのサポート *208*
添付ファイル
AutoSupportメッセージ *205*

と

同期
クラスタとノード *190*
統計
ソート *237*
フィルタリング *236*
次も参照 : パフォーマンス
ドキュメント
SVMの管理に関する詳細情報 *117*
トポロジ
サポートされるクラスタ ピア ネットワーク *273*
トラブルシューティング
AutoSupportメッセージの配信ステータス *216*
FlexVolを備えたSVMの作成エラー *87*
HTTPまたはHTTPSを使用したAutoSupportメッセージ配信 *217*
Infinite Volumeを備えたSVMの作成エラー *90*
MetroCluster構成用SVMの作成エラー *89*
SMTPを使用したAutoSupportメッセージ配信 *219*
SVMの起動に失敗したとき *103*
SVMの停止に失敗したとき *104*
Webサービスへのアクセスに関する問題 *160*
デスティネーションSVMの作成エラー *88*
のコア ダンプ ファイルの管理 *191*
ヘルス監視のためのスイッチ検出 *226*
リモート, SPの概要 *50*
トリガー
AutoSupportの変更用コマンド *214*
トリガー イベント
AutoSupportが応答する仕組み *201*
トンネル
ADユーザとグループに対するクラスタおよびSVMへのアクセスの許可 *121*

な

名前
クラスタの変更 *35*
名前変更
クラスタ *35*

に

日次AutoSupportメッセージ
送信されるタイミングおよび場所 *199*
含まれるデータのタイプ *202*
authentication（認証）
認証方式に公開鍵とパスワードの両方が含まれる場合の動作 *121*
認証
クラスタ ピア関係 *272*
サーバまたはクライアント用のデジタル証明書の管理 *140*
認証方式
NISまたはLDAPユーザに対するクラスタへのアクセスの許可 *123*
SVMへのアクセス *113*
ユーザ アカウント *120*

ね

ネーム サービス
NISまたはLDAPユーザに対するクラスタへのアクセスの許可 *123*
ネットワーク
SP自動設定の有効化 *53*
SPの手動設定 *54*
SPの設定, 概要 *52*

クラスタ ピアリングの要件 *277*
フルメッシュ接続の説明 *277*
ネットワーク インターフェイス
ファームウェア更新に使用 *58*
ネットワーク設定
SPに関する考慮事項 *52*
ネットワーク タイム プロトコル
次を参照 : NTP

の

ノード
SPを使用したリモートからの管理, 概要 *50*
Webブラウザを使用してログ ファイル、コア ダンプ ファイル、MIBファイルにアクセス *42*
管理の概要 *37*
起動または停止の概要 *46*
クラスタからの削除 *40*
クラスタとの同期 *190*
クラスタに関する情報の表示 *34*
クラスタへの追加 *38*
構成バックアップ スケジュールの管理用コマンド *184*
構成バックアップ ファイル *183*
構成バックアップ ファイルの管理用コマンド *184*
再作成したクラスタへの再追加 *188*
システム プロンプトでのリブート *46*
自動構成バックアップ *183*
シャットダウン *48*
シングルノード クラスタ
次を参照 : シングルノード クラスタ
シングルのクラスタに関する考慮事項 *32*
属性の表示 *37*
名前変更 *38*
の構成のリカバリ *185*
の構成バックアップの管理 *183*
パニック後のコア ダンプ ファイルの管理 *191*
ブート メニューによる管理 *49*
マウント ポイントの管理用コマンド *158*
リモートからの管理用コマンド *63*
ルート ボリュームのスペースの解放 *45*
ノードSVM
説明 *78*
ノード構成
構成バックアップ ファイルを使用したリストア *186*
自動バックアップ *183*
バックアップ スケジュールの管理用コマンド *184*
バックアップの管理 *183*
バックアップ ファイル *183*
バックアップ ファイルの管理用コマンド *184*
リカバリ *185*
リカバリ用の構成バックアップファイルの検索 *185*
ノードシェル
概要 *17*
クラスタシェル内でのコマンドおよびオプションへのアクセス *17*
利用可能なコマンドを表示する *18*
ノード接続ヘルスモニタ
概要 *223*
コマンド *228*
ノード属性
変更 *37*
ノードの結合
クラスタへ *38*
ノードの統合解除
クラスタから *40*
ノードのルート アグリゲート
適用されるルール *44*
ノードのルート ボリューム
適用されるルール *44*
ノード名
変更 *38*

は

場所
クラスタの変更 *35*
ノード属性の変更 *37*
パスフレーズ
クラスタ ピア認証 *272*
パスワード
アクセス制御ロールでのルール設定の管理 *133*
と公開鍵の両方が認証方式に含まれる場合の認証動作 *121*
パスワード ルール
設定に関する考慮事項 *134*
バックアップ ファイル
クラスタとノードの構成の管理用コマンド *184*
SVMのバナー *169*
バナー
クラスタ レベルおよびSVMレベルでの管理 *171*
作成 *169*
バナーとMOTDの管理, 概要 *168*
パニック
コア ダンプ ファイルの管理 *191*
パフォーマンス
書き込みパフォーマンスの向上 *267*
クラスタの監視の概要 *233*
データ
オブジェクト、インスタンス、カウンタとは *234*
パフォーマンス プリセットの定義 *234*
表示前の決定事項 *238*
読み取り *266*
読み取り再配置 *266*
ワークロードのパフォーマンスの制御 *250*
パフォーマンスAutoSupportメッセージ
送信されるタイミングおよび場所 *199*
テクニカル サポートへのパフォーマンス アーカイブのアップロード *213*
含まれるデータのタイプ *202*
パフォーマンス アーカイブ ファイル
AutoSupportメッセージの送信 *213*
収集するデータの変更 *238*
テクニカル サポートへのアップロード *213*
パフォーマンス プリセットによる収集データの定義 *234*
パフォーマンス データ
SVM, 高度な方法を使用した監視の概要 *238*
一定期間のクラスタとSVMの表示 *239*
オブジェクトについての収集と表示 *235*
クラスタとSVMの監視用コマンド *241*
継続的に更新されるクラスタとSVMの表示 *240*
テクニカル サポートへのアップロード *213*
パフォーマンス プリセット

オブジェクトのパフォーマンス データの収集 *235*
収集定義のインポート *238*
定義 *234*
パラメータ
CLIで値を指定する際のルール *19*
位置指定, 概要 *25*

ひ

ピア関係
SVM, 説明 *293*
SVM間の作成 *294*
SVMの削除 *300*
SVMの状態 *294*
SVMの管理 *292*
クラスタ間, SVMでの作成 *295*
クラスタ内SVMの作成 *296*
クラスタの管理用コマンド *270*
クラスタの削除 *292*
クラスタの作成 *290*
クラスタの認証 *272*
クラスタの要件 *277*
SVMの変更 *299*
評価用ライセンス
ライセンス タイプとライセンス方式 *177*
表示
SVMの詳細 *100*, *115*
表示環境設定
CLIでの設定 *22*
標準ライセンス
ライセンス タイプとライセンス方式 *177*

ふ

ファームウェア
システム, システム センサー コマンド出力内のディスクリートSPセンサーのステータス値の概要 *69*
ファームウェアの更新
SPの管理方法 *57*
ネットワーク インターフェイスを使用 *58*
ファイアウォール
クラスタ ピアリングの要件 *277*
ファイアウォール ポリシー
クラスタへのTelnetアクセスまたはRSHアクセスの有効化 *13*
ファイル
I/Oのパフォーマンスの制御 *250*
クラスタとノードの構成バックアップの管理用コマンド *184*
コア ダンプの分割方法 *191*
ストレージQoSポリシー グループへの割り当てに関するルール *249*
ファブリック ヘルスモニタ
概要 *223*
ファンアウト構成
クラスタ ピアリングのネットワーク要件 *277*
フィードバック
マニュアルに関するコメントの送信方法 *314*
フィールド
showコマンド出力のカスタマイズ方法 *24*
フィルタ
使用した統計の表示 *236*
ブート
ブート環境のプロンプトからのData ONTAP *47*
ブート環境
ノードのシステム コンソールへのアクセス *43*
ブート環境のプロンプトのブート
Data ONTAPのブート *47*
ブート メニュー
ノードの管理 *49*
ノードのシステム コンソールへのアクセス *43*
ブラウザベース
グラフィカル インターフェイス, OnCommand System Managerを使用したクラスタへのアクセス *28*
プリセット
パフォーマンス, データ収集定義のインポート *238*
フルメッシュ接続
説明 *277*
blocks
ランダム ライト ワークロードのキャッシュ *262*
プロトコル
SVMへの追加または削除 *99*
プロトコル エンジン
Web管理の概要 *155*
Web管理用のコマンド *156*
プロンプト
Data ONTAPコマンドの概要 *16*
システムでのノードのリブート *46*
ブート環境からのData ONTAPのブート *47*

へ

ペアワイズのフルメッシュ接続
サポートされるクラスタ ピア ネットワーク トポロジ *273*
ヘルス
クラスタ ノードに関する情報の表示 *34*
ヘルスの監視
アラートによるAutoSupportメッセージおよびイベントのトリガー方法 *223*
アラートの通知 *224*
アラートの発生タイミングを制御する方法 *222*
アラートへの対応方法 *222*
コマンド *228*
システムの概要 *221*
ダッシュボードの管理用コマンド *232*
デグレードしたヘルスへの対応 *225*
デグレードしたヘルスへの対応の例 *225*
ヘルス ポリシー
アラートと一致条件の概要 *221*
ヘルスモニタ
アラートの概要 *221*
使用可能なクラスタ *223*
ヘルスモニタの動作とヘルス ポリシーの概要 *221*
変更
SVMのプロトコル *99*
SVM属性 *97*
SVMピア関係 *299*
SVMへのアグリゲート リスト *98*

ほ

方法
ユーザ アカウント アクセス *120*

ポート
SP APIサービス設定の変更 56
クラスタ ピアリングの要件 277
専用のクラスタ間を使用するためのクラスタ間LIFの設定 281
専用のクラスタ間を使用する場合の考慮事項 278
データ ロールとクラスタ間ロールを共有する場合の考慮事項 278
ポート, 専用
独自のネットワークのポートを使用するためのクラスタ間LIFの設定 284
ポート, データ
クラスタ間LIFで共有するための設定 279
ホスト
管理からのSPへのアクセス 59
ポリシー グループ
監視 250
最大数 250
最大スループットの仕組み 248
作成 250
種類 246
ストレージ オブジェクトの割り当てに関するルール 249
説明 246
ボリューム
FlexVolを備えたSVM, 説明 76
Infinite Volumeを備えたSVM, 説明 76
Infinite Volumeを備えたSVM用の新しいルート ボリュームの作成 109
SVM内のボリューム数の変更 100
ノードのルートに関するルール 44
ノードのルートのスペースの解放 45
ルート ボリュームとしての新しいFlexVolの昇格 108

ま

マウント ポイント
ノードの管理用コマンド 158
マニフェスト
含まれるAutoSupportメッセージ 216
マニュアル
フィードバックの送信方法 314
変更に関する自動通知の受信方法 314
マニュアル ページ
Data ONTAPへのアクセス 26

め

メール ホスト
AutoSupportでのサポート 208
メッセージ
AutoSupportについて収集されるファイル 216
EMSの設定 196
イベントの管理 195

ゆ

ユーザ
Active Directory, SVM管理者用のアクセスの許可 94
NISまたはLDAPに対するクラスタへのアクセスの許可 123
クラスタおよびSVMのADアクセス, グループの許可 121
ユーザ アカウント
NISまたはLDAP, SVM管理者に対するアクセスの許可 93
SPへのアクセス用 59
SVM管理者用の作成 92
SVMの認証方式とアクセス方式 113
アクセス方法 120
管理方法 119
管理用コマンド 125
認証方式 120
パスワード ルールの設定に関する考慮事項 134
ローカル, SVM管理者用の作成 93
ユーザ名
アクセス制御ロールでのルール設定の管理 133

よ

要件
AutoSupportの使用
大容量ファイルのアップロード 208
クラスタ ピアリングのIPspace 277
クラスタ ピアリングのIPアドレス 277
クラスタ ピアリングのサブネット 277
クラスタ ピアリングのネットワーク 277
クラスタ ピアリングのファイアウォール 277
クラスタ ピアリングのポート 277
ピアリング時のクラスタ命名 277
予測
ヒストグラムベースの予測のサポート, RAVE 257
読み取り再配置
ステータスの表示 267
無効化 267
有効化 267

ら

ライセンス
管理 176
管理用コマンド 178
タイプとライセンス方式 177
ランダム ライト ワークロード
ブロックのキャッシュ 262

り

リカバリ
クラスタ構成 187
ノード構成 185
リストア
SVMのルート ボリューム 106
クラスタ構成 188
ノード構成 186
利点
SVMの使用 78
リブート
システム プロンプトでのノード 46
リモート アクセス

NISまたはLDAPユーザに対するクラスタへのアクセスの許可 *123*
ノードのシステム コンソール *43*
リモート管理
ノードに対するSPの使用の概要 *50*
リモート管理デバイス
SPの概要 *50*
リリース ノート
RAVEを使用したヒストグラムベースの予測のサポート *257*
履歴ログ
コマンドのログの転送, 宛て先 *163*

る

ルートCA証明書
クラスタまたはSVMのSSLクライアントを認証するためのインストール *144*
ルート アグリゲート
ノードに関するルール *44*
ルート ボリューム
SVM, 概要 *78*
Infinite Volumeの新しいルート ボリュームの作成 *106*
Infinite Volumeを備えたSVM用の作成 *109*
SVMのFlexVolの昇格 *106*
SVMの新しいFlexVolの昇格 *108*
ノードに関するルール *44*
ノードのスペースの解放 *45*
ルール
パスワードの設定に関する考慮事項 *134*
ルールの設定
ユーザ名およびパスワードの管理 *133*

れ

レコード
CLIセッションの管理用コマンド *27*
レプリケーション リング
クラスタ, 説明 *34*
レプリケートされたデータベース
次を参照 : RDB
レベル
管理権限の使用 *21*
連絡先情報
クラスタの変更 *35*

ろ

ローカル ユーザ
SVM管理者用のアカウントの作成 *93*
ロール
RBAC
アクセス制御ロールの管理, 概要 *126*
SVM管理者用に事前定義 *127*
アクセス制御のカスタマイズに関する考慮事項 *129*
アクセス制御の管理の概要 *126*
アクセス制御の管理用コマンド *135*
アクセス制御のため、カスタマイズして指定されたコマンドにユーザ アクセスを制限する *132*
アクセス制御のユーザ名およびパスワードのルール設定の管理 *133*
クラスタ管理者用に事前定義 *127*
パスワード ルールの設定に関する考慮事項 *134*
ロールベース アクセス制御
アクセス制御ロールの管理, 概要 *126*
ログ
OnCommand System Managerへのアクセス管理方法 *29*
管理アクティビティの監査設定の管理用コマンド *165*
コマンド履歴の転送 *163*
ログイン
NISまたはLDAPユーザに対するクラスタへのアクセスの許可 *123*
ログ ファイル
AutoSupportメッセージ, 含まれる *205*
ノード, Webブラウザを使用してアクセス *42*

わ

ワークロード
最大数 *250*
種類 *246*
スロットルを適用していないワークロードへのスロットルの影響 *248*
説明 *246*
パフォーマンスの制御 *250*
パフォーマンスを監視する方法 *250*
ランダム ライト ブロックのキャッシュ *262*
割当量
AutoSupportのサイズと時間 *203*