# Veritas Access 7.2.1 トラブルシューティングガイド

Linux

7.2.1

VERITAS

# Veritas Access トラブルシューティングガイド

最終更新: 2017-05-10

マニュアルバージョン: 7.2.1 Rev 0

## 法的通知と登録商標



Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

## テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容とテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

Veritas Account 情報は、次の URL で管理できます。

https://my.veritas.com

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

| | |
|---|---|
| 世界共通 (日本を除く) | CustomerCare@veritas.com |
| 日本 | CustomerCare_Japan@veritas.com |

## マニュアル

マニュアルが最新版であることを確認してください。各マニュアルの 2 ページ目には最新更新日が記載されています。マニュアルのバージョンは各ガイドの 2 ページ目に記載されています。最新のマニュアルはベリタスの Web サイトで入手できます。

https://sort.veritas.com/documents

## マニュアルに関するご意見やご感想

ご意見、ご感想をお待ちしています。マニュアルに対する改善点の提案や誤植や抜けについての報告をお願いします。送信の際は、マニュアルの題名とバージョン、章、セクションの題名を明記してください。次の宛先にお送りください。

doc.feedback@veritas.com

また、ベリタスコミュニティのサイトで、マニュアル情報を確認したり質問したりできます。

http://www.veritas.com/community/

## Veritas SORT (Services and Operations Readiness Tools)

Veritas SORT (Services and Operations Readiness Tools) は、時間のかかる特定の管理タスクを自動化および単純化するための情報とツールを提供する Web サイトです。製品に応じて、SORT はインストールとアップグレードの準備、データセンターのリスクの識別、効率性の改善に役立ちます。使用している製品に対して SORT が提供しているサービスおよびツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

# 目次

1

# 概要

この章では以下の項目について説明しています。

- トラブルシューティングについて
- トラブルシューティングプロセスに関する一般的なヒント
- トラブルシューティングプロセスの一般的な手法
- サポートユーザーのアカウントについて
- サポートユーザーのアカウントの設定
- support ログインの使用

## トラブルシューティングについて

Veritas Access のトラブルシューティングには、次のような手順があります。

- 警告とログメッセージの確認
- 定期的なメンテナンスタスク
- 通常使用する回復手順
- 機能固有の問題と解決方法

各手順については、このマニュアルの以降の章で説明します。

このマニュアルのトラブルシューティングの手順では、`support` ユーザーとしてのログインが必要な場合もあります。

p.8 の「サポートユーザーのアカウントについて」を参照してください。

## トラブルシューティングプロセスに関する一般的なヒント

問題をトラブルシューティングする際、次の点を確認してください。

- 以前発生したかどうかを確認する
  既存のトラブルシューティング情報を確認すると、以前にも発生した問題かどうかがわかります。既存のトラブルシューティング情報は、『Veritas Access リリースノート』で参照できます。リリースノートには、Veritas Access の既知の問題と考えられる回避策のリストが示されています。
- 最近変更した点を確認する
  何らかのメンテナンス、ソフトウェアのアップグレード、その他の変更後すぐにシステムで問題が発生した場合、問題はその変更に関係がある可能性があります。
- 適切に運用されているかを判断する
  システムが予想どおりの処理を行わなかったり、予想どおりの結果が得られない場合は、適切に運用されているかを確認します。問題がないことがわかったら、他の原因を探します。適切に運用されている機能で必要なコンポーネントやサブシステムは、正常に動作している可能性が高いと言えます。
- 経験に基づいて考える
  システムの動作方法に関する知識に基づいて、問題の発生原因になる可能性があるさまざまなエラーを考えます。考えられるエラーについて調べます。エラーの状況、履歴、既存の機能の弱点に関する知識に基づいて、最も可能性の高いエラーから調べます。

# トラブルシューティングプロセスの一般的な手法

一般的なトラブルシューティングのヒントをいくつか実行して問題の範囲を絞り込んだら、以下の手法でさらに問題を切り分けます。

- 同一部品の交換
  同一または類似の部品やサブシステムを備えるシステムにおいて、これらのサブシステム間でコンポーネントを交換して、交換先のコンポーネントに問題が移ったかどうかを確認することをお勧めします。たとえば、クラスタのノードで Veritas Access のネットワーク接続の問題が発生した場合、イーサネットインターフェースカードを交換して問題が交換先のノードに移ったかどうかを確認します。
- 類似コンポーネントの削除
  システムが複数の類似コンポーネントや重複コンポーネントから成り、システム全体の機能を損なわずにこれらのコンポーネントを削除できる場合は、まずこれらのコンポーネントを 1 つずつ削除して、機能するかどうかを確認します。たとえば、クラスタでノードを 1 台ずつシャットダウンして、問題が解決するかどうかを確認します。
- システムをセクションに分割する
  複数のセクションやステージがあるシステムで、各ステージで出入力されている変数を慎重に調べて正しく機能していない変数があるステージを確認します。たとえば、レプリケーションジョブで問題が発生した場合は、以前にこのジョブが正常に実行されたかどうかを確認して、ジョブに失敗し始めた時間を判断します。

- 時間の経過 (または場所) に応じたシステムの動作を監視する

  `Support> services show all` コマンドを使用して、サービスとその現在の状態のリストを表示します。

  `Support> traceroute` コマンドや一連の `Support> iostat` コマンドなどでプロセスを設定して、一定期間システム活動を監視するか、またはネットワーク全体でシステム活動を監視します。この監視は、断続的な問題、プロセッサの活動の問題、ノード接続の問題などを追跡する場合に特に役立ちます。

# サポートユーザーのアカウントについて

通常、Veritas Access にアクセスするには、Veritas Access ユーザーアカウントで管理コンソールにログインします。ログインすると、コマンドラインインターフェースシェル (CLISH) になります。コマンドラインオプションは、ユーザーアカウントに割り当てられている役割によって異なります。

このマニュアルのトラブルシューティング手法では、基になる Linux コマンドラインやその他のサポートユーティリティへのアクセスが必要な場合があります。サポートユーザーのアカウントで、これらのユーティリティにアクセスできます。サポートユーザーのアカウントを有効にする必要があります (デフォルト)。

サポートユーザーとしてログインすると、CLISH 外に存在するログやその他のファイルにアクセスできます。

---

**警告:** サポートユーザーとしてコマンドを実行する場合は注意が必要です。サポートコマンドは、Veritas Access の機能に詳しい上級ユーザーを対象にしています。これらのコマンドの使用について質問がある場合やサポートが必要な場合は、ベリタステクニカルサポート担当者にお問い合わせください。

---

# サポートユーザーのアカウントの設定

`Master` 役割が割り当てられた Veritas Access ユーザーは、パスワードを有効化、無効化、変更したり、サポートユーザーの状態を調べたりできます。

デフォルトでは、サポートユーザーのアカウントは有効になっています。

### サポートユーザーのアカウントを設定するには

1 サポートユーザーを有効にするには、次のように入力します。

```
Admin> supportuser enable
Enabling support user.
support user enabled.
```

2 サポートユーザーが有効になっていることを確認するには、次のように入力します。

```
Admin> supportuser status
support user status : Enabled
```

3 サポートユーザーのパスワードを変更するには、次のように入力します。

```
Admin> supportuser password
Changing password for support.
Old password:
New password:
Re-enter new password:
Password changed
```

### サポートユーザーのアカウントを無効にするには

1 サポートユーザーを無効にするには、次のように入力します。

```
Admin> supportuser disable
Disabling support user.
support user disabled.
```

2 サポートユーザーが無効になっていることを確認するには:

```
Admin> supportuser status
support user status : Disabled
```

# support ログインの使用

サポートユーザーとしてログインすると、CLISH 外に存在するログやその他のファイルにアクセスできます。このガイドのトラブルシューティングでは、サポートユーザーとしてログインする必要がある場合があります。

support ユーザーアカウントは、master の役割を持つ管理者が有効にする必要があります。

p.8 の「サポートユーザーのアカウントの設定」を参照してください。

**メモ:** support アカウントは、テクニカルサポートおよび詳しい知識のあるユーザーが使用します。

### support ログインを使用するには

**1** support アカウントを使用してクラスタの物理 IP アドレスにログインするには、以下のように入力します。

```
support
```

次にパスワードを入力します。デフォルトのパスワードは次のとおりです。

```
veritas
```

例:

```
login as: support
support@<ip_address>'s password:
Last login: Tue Apr 26 14:53:32 2016 from 172.31.172.139
************************************************************
*                     Veritas Access                       *
*                                                          *
*                   Enterprise Edition                     *
*       Warning: Only Veritas Access distributed           *
*     patches & RPMs can be installed on this system!      *
*    Do not delete contents of lost+found directory of     *
*    filesystems as it may contain critical temporary      *
*          Veritas Access configuration data!              *
************************************************************

WARNING: System configured with default password. It's recommended
 to
change password now. Please proceed with changing the password :

Changing password for support.
New password:
Re-enter new password:
Password changed
Default password is changed successfully on all the nodes.
ACCESSRC2_01:~ #
```

**2** CLISH にアクセスする必要がある場合、以下のコマンドを使用できます。

```
su - master
```

2

# 一般的なトラブルシューティング手順

この章では以下の項目について説明しています。



## 一般的なトラブルシューティングの手順について

この章では、問題の検出や解決のために使用できる一般的なトラブルシューティング手順の概要を示します。

## Veritas Access ログファイルの表示

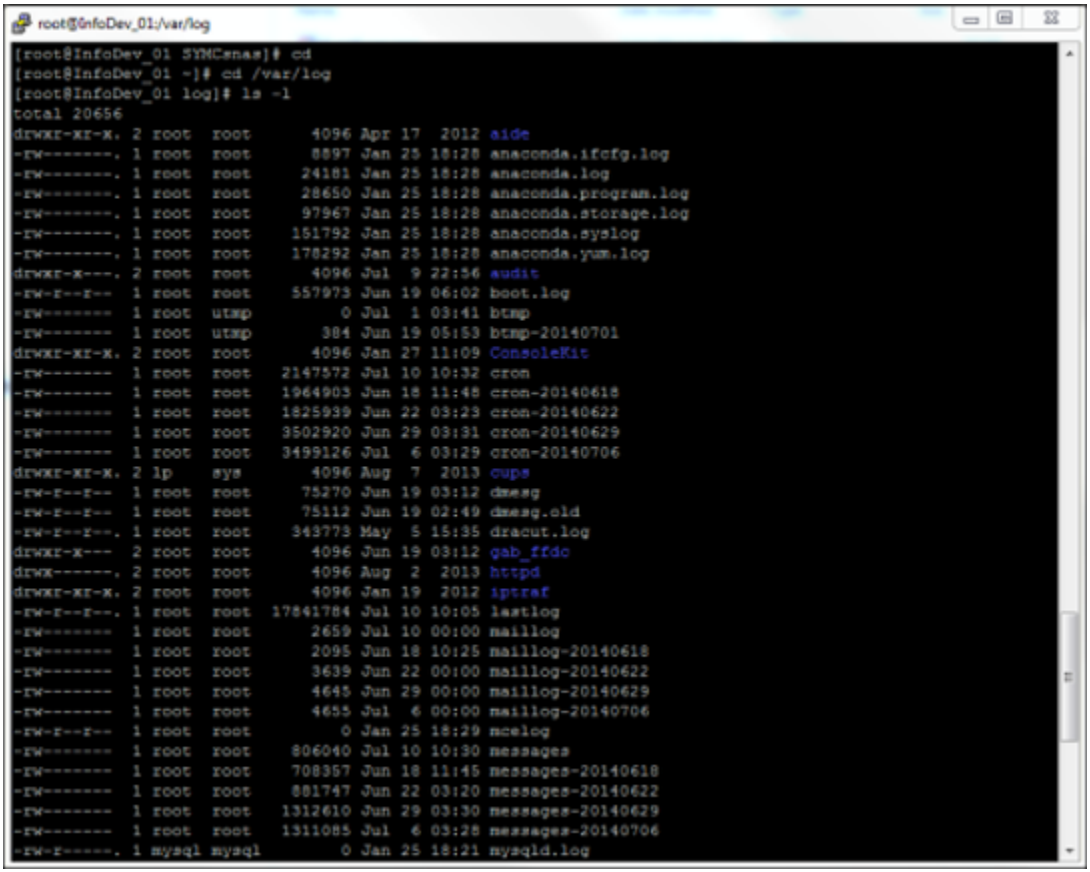
Veritas Access Operations Manager コンソールのダッシュボードにある[警告]パネルや Veritas Access `/var/log` ディレクトリで、発生する可能性がある問題について詳しく調べられます。

**Veritas Access ログファイルを表示するには**

1 サポートアカウントを使用してログインします。

2 `/var/log` ディレクトリに移動します。

**図 2-1** Veritas Access ログファイル




# イベントログについて

システムログに加えて、各 Veritas Access 機能には、関連イベントログがあります。問題が発生した場合に、発生した問題の詳細を最も簡単に調べる方法の一つとして、これらのログファイルを確認します。Veritas Access 機能のイベントログは、 `/opt/VRTSnas/log` ディレクトリに格納されます。

**メモ:** トラブルシューティングの際にログファイルを削除したり変更したりしないでください。ベリタステクニカルサポートの調査の妨げになることがあります。

**イベントログを表示するには、次の操作を実行します。**

1. サポートアカウントを使用してログインします。
2. `/Opt/VRTSnas/log` ディレクトリに移動します。

   Veritas Access 機能のイベントログは、このディレクトリに格納されます。

   たとえば、`cifs.log` には CIFS イベントログが格納されます。

# シェルアクティビティのログについて

シェルアクティビティのログを使用すると、エンドユーザーまたは顧客によって実行された任意のコマンドライン操作を取得できます。シェルアクティビティのログから、エンドユーザーが意図的または偶発的に実行した不要な操作を把握できます。

シェルアクティビティのログは次の場所にあります。

- サポートアカウント - `/var/log/shell_activity_log`
- CLI コマンド - `/opt/VRTSnas/log/command.log`

# CIFS ログレベルの設定

Veritas Access クラスタの CIFS ログレベルを設定して、トラブルシューティングのために外部サーバーにデバッグ情報をアップロードできます。

`support_debug.1` の man ページを参照してください。

p.15 の「デバッグ情報の取得と送信」を参照してください。

**CIFS ログレベルを設定するには**

- Veritas Access クラスタの CIFS 関連のログレベルを設定します。

  ```
  Support> debuginfo setlog cifs loglevel
  ```

  有効な `loglevel` は `0` から `10` までの範囲です。`10` は最も詳細なログレベルです。CIFS ログレベルを高くして CIFS の問題を再現し、CIFS の問題のデバッグ情報をアップロードすることをお勧めします。

  デフォルトのログレベルは `2` です。

  たとえば、Veritas Access クラスタの CIFS ログレベルを `10` に設定する場合は、次のように入力します。

  ```
  Support> debuginfo setlog cifs 10
  ```

# NetBackup クライアントのログレベルの設定とデバッグオプション

NetBackup クライアントのログレベルとさまざまなデバッグオプションを設定してから、外部の FTP または SCP サーバーに情報をアップロードできます。このデバッグ情報を使用して、ベリタステクニカルサポートに送信できます。

p.15 の「デバッグ情報の取得と送信」を参照してください。

`Backup> show` コマンドを使用して、NetBackup ログ情報を検索できます。
`backup_show(1)` のマニュアルページを参照してください。

`Backup> show` コマンドを実行することで、どの NetBackup ログレベルとデバッグオプションが有効になっているかを確認できます。

NetBackup のログ記録について詳しくは、『Veritas NetBackup 管理者ガイド Vol. 1』を参照してください。

有効なログレベルの値は、`1` から `5` の範囲で、`5` が最も詳細です。
`support_debuginfo(1)` のマニュアルページを参照してください。

### NetBackup クライアントのログレベルを設定するには

1. NetBackup データベースのログレベルを設定します。

   ```
   Support> debuginfo setlog nbu database loglevel
   ```

2. NetBackup グローバルデバッグのログレベルを設定します。

   ```
   Support> debuginfo setlog nbu global loglevel
   ```

   グローバルログは、NetBackup 管理コンソールの［Logging］ダイアログボックスで設定されるプロセスのログレベルを制御します。

**NetBackup のデバッグオプションを設定するには**

1 クラスタで NetBackup クライアントが信頼性の高いログ記録を実行できるようにします。

```
Support> debuginfo setlog nbu enable robust
```

信頼性の高いログ記録は、ログディレクトリが消費するディスク容量を制限します。

2 クラスタで NetBackup クライアントが重要なプロセスのログ記録を実行できるようにします。

```
Support> debuginfo setlog nbu enable critical
```

重要なプロセスの有効化オプションを使用すると、重要な NetBackup プロセスを自動的にログ記録できます。NetBackup 管理コンソールの［Logging］ホストプロパティでこのオプションを有効にすると、重要なプロセスのログディレクトリが作成され、ログ記録が開始されます。

# デバッグ情報の取得と送信

Veritas Access ノードから Veritas Access デバッグ情報を取得して、取得した情報を外部 FTP または SCP サーバーを使用してサーバーに送信できます。

データの提供方法について詳しくは、ベリタステクニカルサポートで次の記事を参照してください。

https://www.veritas.com/support/ja_JP/article.000097935

**指定したノードから外部サーバーにデバッグ情報をアップロードするには**

◆ 指定したノードから外部サーバーにデバッグ情報をアップロードします。

```
Support> debuginfo upload nodenamedebug-URL module
```

たとえば、すべてのデバッグ情報を FTP サーバーにアップロードする場合は次のように入力します。

```
Support> debuginfo upload node1_1
ftp://admin@ftp.docserver.company.com/patches/ all
```

たとえば、SCP サーバーに CIFS 関連のデバッグ情報をアップロードする場合は次のように入力します。

```
Support> debuginfo upload node1_1
scp://root@server.company.com:/tmp/node1_1-cifs-debuginfo.tar.gz
```

*nodename* デバッグ情報の収集元のノード名 を指定します。

*debug-URL*

デバッグ情報をアップロードするリモートファイルまたはディレクトリを指定します。

デバッグ情報のアップロード元サーバーの種類に応じて、次の例の URL 形式のいずれかを使用します。

```
ftp://admin@ftp.docserver.company.com/
patches/
```

```
scp://root@server.company.com:/tmp/
```

*debug-URL* にリモートファイルを指定すると、debuginfo ファイルはそのリモートファイル名で保存されます。*debug-URL* にリモートディレクトリを指定すると、debuginfo ファイル名は次のように表示されます。

```
nas_debuginfo_nodename_modulename_timestamp.tar.gz
```

*module*

モジュールの値を指定します。

サポート対象のモジュール値は次のとおりです。

- all - すべてのデバッグ情報を収集する
- generic - ベリタス製品に関連する情報を除くすべてのデバッグ情報を収集する
- cifs - CIFS 関連のデバッグ情報を収集する
- nas - Veritas Access 関連のデバッグ情報を収集する
- netbackup - NetBackup クライアント関連のデバッグ情報を収集する

`Support> debuginfo` コマンドは、RHEL (Red Hat Enterprise Linux の `sosreport` コマンドに関する情報も収集します。`sosreport` は、`selinux` モジュール以外のすべてのロード済みモジュールを収集します。

3

# Veritas Access の監視

この章では以下の項目について説明しています。



## Veritas Access 操作の監視について

この章では、Veritas Access 操作の監視に役立つサポートタスクをいくつか説明します。監視タスクを定期的に実行して、Veritas Access が円滑に実行されていることを確認します。

Veritas Access と連携すると、監視コマンドで作成される現在進行中の出力レコードが保持されます。これにより、通常の操作を判断する基準がわかり、重大な問題になる前に潜在的な問題を見つけられます。

## プロセッサアクティビティの監視

`Support> top` コマンドにより、実行中のタスクの動的なリアルタイムビューが表示されます。指定されたノードで指定の時間にユーザーとプロセスが消費するリソースが表示されます。

### top コマンドを使用するには

◆ Support> top コマンドを使用するには、以下のように入力します。

```
Support> top [nodename] [iterations] [delay]
```

*nodename* 指定されたノードに対する指定時間のリソースとプロセスが表示されます。

*iterations* 繰り返し実行する回数を指定します。デフォルトでは 3 回です。

*delay* 画面更新の間の遅延を指定します。デフォルトは 5 秒です。

たとえば、ノード access_01 で実行中のタスクの動的なリアルタイムビューを表示するには、以下のように入力します。

```
Support> top access_01 1 1
top - 16:28:27 up 1 day, 3:32, 4 users, load average: 1.00, 1.00,
 1.00
Tasks: 336 total, 1 running, 335 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.1% us, 0.1% sy, 0.0% ni, 99.7% id, 0.0% wa, 0.0% hi,
0.0% si
Mem: 16405964k total, 1110288k used, 15295676k free, 183908k
buffers
Swap: 1052248k total, 0k used, 1052248k free, 344468k cached

PID   USER  PR  NI  VIRT   RES  SHR  S  %CPU  %MEM   TIME+
COMMAND
6314  root  15  0   5340  1296  792  R   3.9   0.0  0:00.02  top
1     root  16  0    640   260  216  S   0.0   0.0  0:04.86  init
```

# CPU とデバイスの使用率レポートの生成

**iostat コマンドを使用するには**

- Support> iostat cpu コマンドを使用するには、以下のように入力します。

  Support> iostat cpu [*nodename*] [*interval*] [*count*]

  | | |
  |---|---|
  | *nodename* | レポートが生成されるノードの名前。デフォルトは管理コンソールの console です。 |
  | *interval* | 各レポート間の秒単位の間隔。デフォルトは 2 秒です。 |
  | *count* | 秒単位で入力した interval コマンドで生成されるレポートの数。デフォルトは 1 つのレポートです。 |

  *nodename* オプションでは、レポートが生成されるノードの名前が要求されます。デフォルトは Veritas Access Operations Manager コンソールの console です。

  たとえば、コンソールノードの CPU 使用率レポートを生成するには、以下のように入力します。

```
Support> iostat cpu access_01
Linux 2.6.16.60-0.21-smp (access_01)       02/09/16

avg-cpu:  %user   %nice  %system  %iowait  %steal   %idle
           1.86    0.07     4.53     0.13    0.00   93.40
```

**iostat device コマンドを使用するには**

- `Support> iostat device` コマンドを使用するには、以下のように入力します。

  ```
  Support> iostat device [nodename] [dataunit]
  [interval] [count]
  ```

  | | |
  |---|---|
  | *nodename* | *nodename* オプションでは、レポートが生成されるノードの名前が要求されます。デフォルトは管理コンソールの `console` です。 |
  | *dataunit* | *dataunit* オプションを使用すると、レポートをブロック単位または KB 単位で生成できます。デフォルトはブロック単位です。 |
  | *interval* | 各レポート間の秒単位の間隔。デフォルトは 2 秒です。 |
  | *count* | 秒単位で入力した `interval` コマンドで生成されるレポートの数。デフォルトは 1 つのレポートです。 |

  たとえば、ノードのデバイス使用率レポートを生成するには、以下のように入力します。

  ```
  Support> iostat device access_01 Blk
  Linux 2.6.16.60-0.21-smp (access_01)       02/09/16

  Device:      tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
  hda         4.82        97.81        86.11    1410626    1241992
  sda         1.95        16.83         4.05     242712      58342
  hdc         0.00         0.01         0.00        136          0
  ```

# ネットワークトラフィックの監視

Tethereal は、Linux オペレーティングシステムでサポートされているネットワークプロトコルアナライザである Ethereal のコマンドラインバージョンです。これを使用して、パケットデータをライブネットワークからキャプチャしたり、前に保存したキャプチャファイルからパケットを読み取ったりできます。

Veritas Access ではネットワークトラフィックの監視用に `Support> tethereal` コマンドを使用でき、これによりネットワークトラフィックデータの表示とエクスポートが可能になります。

- `Support> tethereal show` コマンドにより、ライブネットワークからキャプチャされたパケットデータが表示されます。
- `Support> tethereal export` コマンドにより、ネットワークトラフィックの詳細を分析用にエクスポートできます。

# ネットワークトラフィック詳細のエクスポートと表示

### tethereal コマンドを使用するには

- `Support> tethereal export` コマンドを使用するには、以下のように入力します。

  ```
  Support> tethereal export url [nodename] [interface] [count]
  [source]
  ```

  | | |
  |---|---|
  | *url* | ネットワークトラフィック詳細をエクスポートする場所を指定します。ファイル名が url で指定されていない場合、デフォルトのファイル名 `tethereal.log` が使用されます。 |
  | *nodename* | トラフィック詳細の生成元となるノードの名前。 |
  | *interface* | パケットキャプチャ用ネットワークインターフェースを指定します。 |
  | *count* | 読み取るパケットの最大数を指定します。<br>ネットワークトラフィック詳細のキャプチャに可能なファイルの最大サイズは、128 MB です。「count」の値が非常に大きい場合、ファイルサイズが 128 MB を超えると、コマンドはネットワークトラフィック詳細のキャプチャを停止します。 |
  | *source* | パケットをフィルタするノードを指定します。 |

  たとえば、ネットワークトラフィック詳細をエクスポートするには、以下のように入力します。

  ```
  Support> tethereal export scp://user1@172.31.168.140:~/
  Password: *******
  Capturing on pubeth0 ...
  Uploading network traffic details to scp://user1@172.31.168.140:~/

  is completed.
  ```

  ネットワークトラフィック詳細をエクスポートする場合、Ctrl + C キーを押してキャプチャプロセスを停止し、トラフィック詳細を URL サイトにアップロードします。

### tethereal show コマンドを使用するには

◆ Support> tethereal show コマンドを使用するには、以下のように入力します。

```
Support> tethereal show [nodename] [interface] [count]
[source]
```

| | |
|---|---|
| *nodename* | トラフィック詳細の表示元となるノードの名前。 |
| *interface* | パケットキャプチャ用ネットワークインターフェースを指定します。 |
| *count* | 読み取るパケットの最大数を指定します。<br>count 値を指定しない場合、ネットワークトラフィックは中断されるまで引き続き表示されます。 |
| *source* | パケットをフィルタするノードを指定します。 |

たとえば、5 つのパケットのトラフィック詳細は次のようになります。

```
Support> tethereal show access_01 pubeth0 5 172.31.168.140
0.000000 172.31.168.140 -> 10.209.105.147 ICMP Echo (ping) request
0.000276 10.209.105.147 -> 172.31.168.140 ICMP Echo (ping) reply
0.000473 10.209.105.147 -> 172.31.168.140 SSH Encrypted response

packet len=112
0.000492 10.209.105.147 -> 172.31.168.140 SSH Encrypted response

packet len=112
```

4

# 一般的なリカバリ手順

この章では以下の項目について説明しています。



## 一般的な回復手順について

この章では、Veritas Access で発生した問題のトラブルシューティングに使用できる最も一般的な回復手順をいくつか示します。

## サーバーの再起動

一部の設定は変更しても、関連付けられているサーバーを再起動するまで有効になりません。そのため、関連付けられたサーバーを停止して再起動すると、設定の問題を解決

できる場合があります。たとえば、AD ドメインの設定を変更した場合は CIFS サーバーの再起動が必要です。

表 4-1 に、Veritas Access サーバーの起動と停止に使用できるコマンドを示します。

**表 4-1 サーバーを起動および停止するコマンド**

| コマンド | 定義 |
|---|---|
| `Backup> start` | 設定したバックアップサービスをすべて開始します。 |
| `Backup> stop` | 設定したバックアップサービスをすべて停止します。 |
| `CIFS> server start` | CIFS サーバーを起動します。 |
| `CIFS> server stop` | CIFS サーバーを停止します。 |
| `FTP> server start` | FTP サーバーを起動します。 |
| `FTP> server stop` | FTP サーバーを停止します。 |
| `NFS> server start` | NFS サーバーを起動します。 |
| `NFS> server stop` | NFS サーバーを停止します。 |
| `Storage> iscsi start` | ISCSI イニシエータサービスを開始します。 |
| `Storage> iscsi stop` | ISCSI イニシエータサービスを停止します。 |

**メモ:** `server` 引数が含まれるコマンドと含まれないコマンドがあります。`server` ではなく `service` 引数を使用する `Support>` コマンドもあります。

# サービスをオンラインにする

`Support> services` コマンドを使用して、OFFLINE または FAULTED の状態にあるサービスを ONLINE の状態に戻せます。

**メモ:** `Support> services` コマンドを使用した後に、サービスがまだオフラインかまたは障害がある場合は、テクニカルサポートに連絡する必要があります。

サービスには以下が含まれます。

- バックアップ
- コンソールサービス
- CIFS サーバー
- FTP
- FS マネージャ
- GUI
- IP アドレス
- NIC 情報
- NFS サーバー

## services コマンドの使用

### サービスの状態を表示するには

◆ ノードで実行中の重要なサービスを表示するには、次のように入力します。

```
Support> services show
                          access
Service             01         02
-------          -------- --------
nfs                ONLINE   ONLINE
cifs               ONLINE   ONLINE
ftp                ONLINE   ONLINE
iSCSIInitiator     OFFLINE  OFFLINE
gui                ONLINE   ONLINE
console            ONLINE   ONLINE
nic_pubeth0        ONLINE   ONLINE
nic_pubeth1        ONLINE   ONLINE
fs_manager         ONLINE   ONLINE
```

### すべてのサービスの状態を表示するには

◆ ノードで実行中のすべてのサービスを表示するには、次のように入力します。

```
Support> services showall
                        access
Service             01        02
-------          -------- --------
nfs                ONLINE   ONLINE
cifs               ONLINE   ONLINE
ftp                ONLINE   ONLINE
iSCSIInitiator     OFFLINE  OFFLINE
console            ONLINE   ONLINE
gui                ONLINE   ONLINE
nic_pubeth0        ONLINE   ONLINE
nic_pubeth1        ONLINE   ONLINE
fs_manager         ONLINE   ONLINE
10.182.107.201     ONLINE   ONLINE
10.182.107.202     ONLINE   ONLINE
10.182.107.203     ONLINE   ONLINE
10.182.107.204     ONLINE   ONLINE
/vx/fs1            ONLINE   ONLINE
```

### すべてのサービス障害を修正するには

◆ すべてのサービス障害を修正するには、次のように入力します。

```
Support> services autofix
Attempting to fix service faults...........done
```

### サービスをオンラインにするには

◆ サービスをノードでオンラインにするには、次のように入力します。

```
Support> services online servicename
```

*servicename* は、オンラインにするサービスの名前です。

例:

```
Support> services online 10.182.107.203
```

# 異常なシャットダウンからのリカバリ

場合によっては、ノードで異常なシャットダウンが発生したとき (たとえば、予期しないシステム障害、電源障害など)、ノードのファイルを修復するために Linux の `fsck` (ファイル

システムチェック)コマンドを使用するように要求するエラーメッセージがローカルノードで表示されることがあります。

fsck コマンドを使用したノードの修復は推奨されません (不可能な場合もあります)。代わりに、クラスタの正常なノードを使用して、障害が発生したノードに Veritas Access ソフトウェアを再インストールします。

**ノードを回復するには**

1. master アカウントを使用して、Veritas Access にログインします。
2. 障害が発生したノードをクラスタから削除します。ノードを削除するには、次のように入力します。

   ```
   Cluster> del nodename
   ```

   *nodename* は、障害が発生したノードの名前です。

   例:

   ```
   Cluster > del access_01
   ```

   **メモ:** 障害が発生したノードの情報はクラスタから削除されます。障害が発生したノードは再起動時に削除されたことを検出し、クリーンアップします。

3. ノードがクラスタから削除された後、削除されたノードを再起動すると、(ノードがクラスタに追加される前の) 元の物理 IP アドレスを使用してアクセスできるようになります。
4. 次のように入力して、ノードを追加し直します。

   ```
   Cluster> add nodeip
   ```

   *nodeip* は削除されたノードのアクセス可能な IP アドレスです。

   例:

   ```
   Cluster > add 172.16.113.118
   ```

# ネットワーク接続性のテスト

特定のホストまたはゲートウェイに IP ネットワークでアクセスできるかどうかをテストできます。

**ping コマンドを使用するには**

- ping コマンドを使用するには、以下のように入力します。

```
Network> ping destination [nodename]
[devicename] [packets]
```

たとえば、node1 を使用する host1 に ping 送信できます。

```
Network> ping host1 node1
```

*destination* 情報の送信先となるホストまたはゲートウェイを指定します。

destination フィールドには、DNS 名または IP アドレスを含められます。

*nodename* ping 送信元となる *nodename* を指定します。任意のノードから ping 送信するには、*nodename* フィールドで `any` を使用します。*nodename* フィールドはオプションのフィールドです。*nodename* が省略されると、ノードは ping 送信元に選択されます。

*devicename* ping 送信で使用するデバイスを指定します。クラスタの任意のデバイスから ping 送信するには、`devicename` フィールドで `any` 変数を使用します。

*packets* 送信先に送信する必要があるパケット数を指定します。

packets フィールドを省略すると、デフォルトで 5 つのパケットが送信先に送信されます。

packets フィールドには、符号なし整数が含まれている必要があります。

# traceroute によるトラブルシューティング

Traceroute は、広く使用されているユーティリティで、Linux オペレーティングシステムでサポートされています。traceroute は ping のように、ネットワークの接続を確認するための有用なツールです。Veritas Access `Support> ping` コマンドを使用して、2 つのシステム間の接続を検出できます。`Support> traceroute` コマンドではシステムの接続も確認されますが、2 つのシステム間の中間ホストも示されます。ユーザーはパケットのシステム間での可能性があるルートを確認できます。`Support > traceroute` コマンドを使用して、リモートホストへのルートを検出します。たとえば、`Support> traceroute` コマンドを使用して、クラスタの各ノードの接続を確認する場合があります。

# traceroute コマンドの使用

Support> traceroute コマンドにより、2 つのノード間の 1 つのルートのすべての中間ノードが表示されます。

**traceroute コマンドを使用するには**

◆ Support> traceroute コマンドを使用するには、以下のように入力します。

```
Support> traceroute destination [source]
[maxttl]
```

| | |
|---|---|
| *destination* | ターゲットノード。1 つのネットワーク上の 2 つのノードにあるすべての中間ノードを表示するには、*destination* ノードを入力します。<br>IPv4 の場合は IPv4 のアドレス、IPv6 の場合は IPv6 のアドレスの指定が必要です。<br>IPv6 のプレフィックスの許容範囲は 0 から 128 までの整数です。 |
| *source* | 追跡を開始する *source* のノード名を指定します。 |
| *maxttl* | ホップの最大数を指定します。デフォルトは 7 つのホップです。 |

たとえば、ネットワークホストへのルートを追跡するには、以下のように入力します。

```
Support> traceroute www.veritas.com fssClus_01 10
traceroute to www.veritas.com (23.5.150.79), 10 hops max, 60 byte packets
 1  puna-sli-core-b01-vlan329.net.symantec.com (10.209.192.2) 0.356 ms  0.354 ms 0.376
 ms
 2  punb-vfpi-eng-1-aggregate2-104.net.veritas.com (10.209.186.14) 0.298 ms 0.322 ms
0.379 ms
 3  puna-spi-core-b02-vlan105.net.symantec.com (143.127.185.130) 1.851 ms  1.964 ms
1.940 ms
 4  bnrcatcore01-teng6-2.net.symantec.com (143.127.185.205)  1.902 ms 1.903 ms 1.932 ms

 5  puna-vfpi-main-1-vip.net.veritas.com (10.212.252.50) 1.886 ms 1.945 ms 1.922 ms
```

# ファイルシステムの metasave イメージの収集

ファイルシステムの問題をトラブルシューティングするために、標準またはスケールアウトファイルシステムの metasave イメージを収集できます。メタデータには、ファイルシステム内のデータの属性が含まれますが、実際のデータ自体は含まれないデータ構造です。ファイルシステムのファイルサイズ、経過時間、情報の種類など、ファイルシステムの傾向を追跡するために、メタデータイメージを使用できます。

**メモ:** Support> metasave コマンドを使用する場合、一貫性のある metasave イメージを作成するために、すべてのクラスタノードでファイルシステムをオフラインにする必要があります。metasave イメージを収集する前に、Storage> fs offline コマンドを使用してファイルシステムをオフラインにします。metasave イメージの収集には時間がかかります。必要な合計時間は、ファイルシステムに存在するメタデータの情報量によって異なります。スケールアウトファイルシステムを使用する場合、metasave イメージの収集にはかなりの時間がかかります。metasave 処理の実行中は、別の端末から Veritas Access のその他の処理を実行できます。

**ファイルシステムの metasave イメージを収集するには**

- Support> metasave コマンドを使用するには、次のコマンドを入力します。

  Support> metasave [fsname] [output_location]

  fsname — metasave イメージを収集するファイルシステムの名前を指定します。

  output_location — metasave イメージのディレクトリの場所を指定します。

  通常のファイルシステムの場合、output_location で指定されたディレクトリの場所に metasave イメージが 1 つ格納されています。

  スケールアウトファイルシステムの場合、スケールアウトファイルシステム内のコンテナファイルシステムの数に応じて、複数の metasave イメージが生成されます。スケールアウトファイルシステムでは、名前空間のマッピングも metasave イメージに含まれます。

  たとえば、ファイルシステムの metasave イメージ testfs を収集するには、/tmp/meta_out_dir 内に保存し、次のコマンドを入力します。

```
Support> metasave testfs /tmp/meta_out_dir
Collecting metasave image of file system testfs. This may take some time...
SUCCESS: Metasave image of testfs collected successfully. Image is stored at
/tmp/meta_out_dir.
```

# イーサネットインターフェースカードの交換

場合によっては、ノードのイーサネットインターフェースカードを交換する必要があります。このセクションでは、カードを交換する手順について説明します。

**メモ:** 以下の手順で、既存のイーサネットインターフェースカードを交換します。この手順では、クラスタにイーサネットインターフェースカードを追加することはできません。追加するイーサネットインターフェースカードに新しいデバイスドライバが必要な場合は、ノードにイーサネットインターフェースカードを搭載する前に新しいデバイスドライバを設置します。

### イーサネットインターフェースカードを交換するには

1. `Cluster> shutdown` コマンドを使用してノードをシャットダウンします。

   例:

   ```
   Cluster> shutdown access_03
   Stopping Cluster processes on access_03.......done
   Sent shutdown command to access_03
   ```

2. `Cluster> del` コマンドを使用してクラスタからノードを削除します。

   例:

   ```
   Cluster> del access_03
   ```

3. ノードに交換用のイーサネットインターフェースカードを設置します。
4. ノードの電源を入れます。
5. イーサネットインターフェースカードがアクティブでオンラインであることを確認します。
6. `Cluster> add` コマンドを使用してクラスタにノードを戻します。

   例:

   ```
   Cluster> add 172.16.113.118
   ```

このセクションの説明にある `Cluster> add` と `Upgrade>` コマンドについて詳しくは、関連 man ページを参照してください。

# レプリケーションの高速化

場合によっては、レプリケーションジョブに予想より時間がかかることがあります。この場合、レプリケーションジョブの再同期が必要なことがあります。

# レプリケーションジョブの同期について

レプリケーションジョブの初回実行時に、Veritas Access はレプリケーション元からレプリケーション先にデータを完全にコピーします。以降のジョブ (手動またはスケジュールに従って実行) では、増分の変更のみをコピーします。

まれに、レプリケーション先にすでにデータが存在する場合、レプリケーションジョブでは増分の変更は行えません。このような状況になる例を以下に示します。

- 数日間または数週間レプリケーションを実行していない場合、VxFS ファイル変更ログで追跡している変更が上書きされたり、壊れたりしている可能性があります。レプリケーションにはこのログが必要です。
- レプリケーションジョブを一時的に無効にして再開すると、次回のジョブでデータが完全にコピーされます。
- レプリケーションの定義にいくつか変更を加えた場合。たとえば、以前は `fs1/folder1` のレプリケーションジョブだったが、`fs1/folder2` のデータもレプリケーションする場合などです。`fs1/folder2` を完全にコピーする必要があるため、`fs1/folder1` は増分変更のみが必要な場合でも再びコピーされます。
- レプリケーションの方向を、レプリケーション先からレプリケーション元に逆にする必要がある場合。ほとんどのデータがレプリケーション先とレプリケーション元の両方に存在する場合でも、レプリケーション先で新しいジョブを作成すると、常に初回レプリケーション時に自動的に完全にコピーされます。
- 管理者がレプリケーション用の内部データベースを誤って削除してしまったときに利用可能なバックアップが存在しない場合、既存の設定で新しいジョブを作成しても完全にコピーされます。

このような場合、完全なコピーが開始されるまで待機せずに `Replication> job sync` コマンドを使用し、レプリケーション先の既存のデータを活用して完全なコピーを避けられます。`Replication> job sync` コマンドは、レプリケーションジョブを適切に定義された状態に戻すため、増分のレプリケーションを行えます。

ジョブを同期すると再び有効になるため、標準的なジョブを実行することも、レプリケーションの頻度を設定して増分のレプリケーションの実行もできます。

---

**メモ:** 同期は、有効になっているジョブでのみサポートされます。失敗したジョブから再開できない場合に `Replication> job sync` コマンドを使用して失敗した状態から回復するには、まずジョブを無効にしてから再び有効にします。次に、`Replication> job sync` コマンドを使用してジョブを同期します。

---

**メモ:** 一時停止しているレプリケーションジョブでは同期は実行できません。中断または停止している一時停止中のジョブで同期を実行する場合、一時停止しているジョブの前回の回復ポイントの目標 (RPO) は利用できません。

---

## レプリケーションジョブの同期

**有効になっているレプリケーションジョブを同期するには**

- 有効になっているレプリケーションジョブを同期するには、次のように入力します。

  ```
  Replication> job sync job_name
  ```

  *job_name*　　同期するレプリケーションジョブの名前を指定します。

  例:

  ```
  Replication> job sync job14
  ```

# パッチリリースまたはソフトウェアのアップグレードのアンインストール

多くの場合、問題は製品の既知の不具合が原因で発生します。不具合が修正されたら、パッチリリースやソフトウェアのアップグレードをインストールして問題を解決できます。

パッチのリリースやソフトウェアのアップグレードをインストールする場合は、次の操作を実行します。

- インストールを開始する前に `System> config export` コマンドを使用して設定のコピーを保存します。アップグレード後に `System> config import` コマンドを使用して設定を復元できます。
- 最小限の停止時間でアップグレードするには、アップグレード時に使用する一時的な VIP と IP アドレスのセットを取得する必要があります。一時的な VIP アドレスと IP アドレスを使用せずにアップグレードすることもできますが、停止時間が長くなります。

Veritas Access のアップグレードについて詳しくは、『Veritas Access インストールガイド』を参照してください。

5

# Veritas Access のインストールと設定に関する問題のトラブルシューティング

この章では以下の項目について説明しています。



## インストールログの表示

インストール中に問題が発生した場合は、インストールログの内容を表示すると問題を特定できます。

**Veritas Access インストールログを表示するには**

1. Veritas Access のインストールや設定時に `/var/tmp` にある一時フォルダのインストーラログを参照できます。
2. Veritas Access をインストールして設定したら、次の場所でインストールログのレプリケーションを表示できます。

| | |
|---|---|
| Veritas Access インストール後のログ | `/opt/VRTS/install/logs/installaccess-`*`timestamp`*<br>このディレクトリは、インストーラをトリガするノード (ドライバノード) にあります。このディレクトリには、Veritas Access の特定のインストールログが含まれています。<br>例:<br>`/opt/VRTS/install/logs/installaccess-201602021544AsJ` |
| Veritas Access サービスグループの設定ログ | `/opt/VRTSnas/log/Install.log`<br>このディレクトリには、Veritas Access の特定の設定ログが含まれています。<br>例:<br>`/opt/VRTSsnas/log/Install.log.201407030655` |
| Veritas Access ネットワークのインストールと設定のログ | `/opt/VRTSnas/log/install_network.log`<br>このディレクトリには、Veritas Access のネットワーク設定ログが含まれています。<br>例:<br>`/opt/VRTSnas/log/install_network.log.201407030655` |

# インストールの失敗または未完了

インストールエラーの一般的な原因を以下にいくつか挙げます。

- メモリ制限。ノードに Veritas Access ソフトウェアをインストールするには、少なくとも 32 GB のメモリが必要です。
- コアが 1 つ (単一の CPU)
  Veritas Access をインストールするには、クラスタ (デュアル CPU システム) に少なくとも 2 台のノードが必要です。
- 必要なオペレーティングシステムパッケージがない

必要なオペレーティングシステムパッケージがない場合はYUMを使用するか、手動でインストールできます。
詳しくは『Veritas Access インストールガイド 』を参照してください。

- ゲートウェイへのアクセス
  Veritas Access ノードは、パブリックネットワークを使用してデフォルトのゲートウェイに接続できる必要があります。ゲートウェイに接続できることをネットワーク管理者に確認します。

# PCI ID をクラスタから除外する

1 番目のノードへの最初の Veritas Access ソフトウェアインストール時に、クラスタの特定の PCI ID を除外して、今後使用するために予約できます。別のノードをクラスタに追加するときに追加分の PCD ID を除外する場合があります。PCI ID を除外リストに追加できます。PCI ID が PCI 除外リストに追加されているインターフェースカードは、後続のクラスタノードのインストール用のプライベートインターフェースまたはパブリックインターフェースとして使用されません。新しいノードのインストール時に、残りの PCI バスインターフェースが検索され、パブリックインターフェースまたはプライベートインターフェースとして追加されます。

`Network> pciexclusion` コマンドは、さまざまなオプションと使用できます。

- `Network> pciexclusion show` コマンドは、除外に選択されている PCI ID を表示します。ノード名に対応する y (yes) または n (no) の記号を表示して、除外されているかどうかに関する情報も提供します。ノードが INSTALLED の状態でない場合、ノードの UUID が表示されます。
- `Network> pciexclusion add` *`pcilist`* コマンドを使用して管理者は除外対象の特定の PCI ID を追加できます。これらの値は、インストール前の指定が必要です。コマンドにより、2 番目のノードインストールから PCI が除外されます。
  *pcilist* は、PCI ID のカンマ区切りリストです。
- `Network> pciexclusion delete` *`pci`* コマンドを使用して管理者は指定の PCI ID を除外から削除できます。このコマンドは有効にするためにインストール前に使用する必要があります。コマンドは、次回のノードのインストールで有効になります
  *PCI* ID ビット形式は 16 進数 (XXXX:XX:XX.X) です。

`Network> pciexclusion` コマンドを使用するには、次のように入力します。

```
Network> pciexclusion show
PCI ID       EXCLUDED    NODENAME/UUID
------       --------    -------------

Network> pciexclusion add FFFF:FF:00.0
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has
```

```
 been
added for exclusion

Network> pciexclusion add FFFF:FF:00.1
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has
 been
added for exclusion

Network> pciexclusion show
PCI ID        EXCLUDED    NODENAME/UUID
------        --------    -------------
0000:0e:00.0 y            ACCESS_1
0000:0e:00.0 y            a79a7f43-9fe2-4eeb-aa1f-27a70e7a0820
0000:04:00:1 n

Network> pciexclusion delete ffff:ff:00.1
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has
 been
added for exclusion ACCESS pciexclusion SUCCESS V-288-1364 Given PCI
 ID
ffff:ff:00.1 has been deleted from exclusion list

Network> pciexclusion show
PCI ID              EXCLUDED      NODENAME/UUID
------              --------      -------------
ffff:ff:00.0         n
Network>
```

# ファイルシステムチェックの実行が必要な場合に Red Hat Enterprise Linux オペレーティングシステムを修復できない

Red Hat Enterprise Linux オペレーティングシステムのパーティションが破損している場合、`fsck` (ファイルシステムチェック) を実行できないため、ノードの再起動が必要です。ノードを再起動しようとすると、オペレーティングシステムにより、ファイルシステムチェックを実行するための `root` ユーザーのパスワードの入力が求められます。

この問題を解決するには、Red Hat Enterprise Linux のマニュアルを参照してください。

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/System_Administration_Guide/s1-rescuemode-boot.html

# 管理コンソール IP の検索方法

**どのノードがコンソール IP (管理コンソール IP) かを識別するには**

1 どのノードが管理コンソール IP かを識別します。

```
# hares - state | grep -I console
```

2 セキュアシェル (ssh) を使用して、管理コンソール (管理コンソールを持つのは 1 つのノードだけです)。

3 管理コンソールで、次のコマンドを使用して CLISH にログオンします。

```
su - master
```

# storage disk list コマンドが空のディスク名を表示する

次の理由により、`storage disk list` コマンドが空のディスク名を表示する場合があります。

- 仮想環境では、Virtual Machine Disk (VMDK) のディスクは、クラスタのノード間で共有されます。
  解決方法:
  理想的には、VMDK ディスクをローカルディスクとして関連付ける必要があります。
- ローカルディスクは、一意ではない一意のデバイス識別子 (UDID) を持ちます。
  たとえば、node1 と node2 を持つクラスタで、node1 に接続されているローカルディスクが node2 に接続されているローカルディスクと同じ UDID を持つ場合があります。
  解決方法:
  次のコマンドを実行します。

  ```
  # storage disk configure local <node_name> <vendor_id> <product_id>
  [serial_num]
  ```

  ここで、*<vendor_id>* はベンダーの ID
  *product_id>* は製品の ID
  *node_name>* はコマンドが実行されるノードの名前です。
  *serial_num* は、ディスクのシリアル番号形式から慎重に計算された "opcode/pagecode/offset/length" の形式で指定する必要があります。
  すべてのノードでコマンドを実行する場合は、*<node_name>* 値を *all* として指定します。
  `storage disk configure local` コマンドについて詳しくは、storage_disk のマニュアルページを参照してください。

6

# Veritas Access CIFS の問題のトラブルシューティング

この章では以下の項目について説明しています。



## ユーザーアクセスが CTDB ディレクトリ共有で拒否される

場合によっては、正しい ACL が共有に設定されている場合でも、ユーザーまたはグループが CTDB ディレクトリ共有へのアクセスを拒否されることがあります。この問題は、親ディレクトリにユーザーまたはグループのアクセスを妨げる ACL が含まれているために発生する可能性があります。

この動作は想定内です。アクセスを有効にするには

- ルートレベルのディレクトリ (親ディレクトリ) が CIFS 共有として追加されていることを確認します。
- アクセスできるようにするには、元の CTDB ディレクトリ共有に適用したものと同じ ACL 設定を親ディレクトリに適用します。

# 索引

## た



## な



## は



## ま



## や



## ら