

NetBackup™ Add-in for Microsoft SCVMM Console ガイド

リリース 11.0

NetBackup™ Add-in for Microsoft SCVMM Console ガイド

最終更新日: 2025-04-24

法的通知と登録商標

Copyright © 2025 Cohesity, Inc. All rights reserved.

Cohesity, Veritas, Cohesity ロゴ、Veritas ロゴ、Veritas Alta, Cohesity Alta, NetBackup は、Cohesity, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Cohesity 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア(「サードパーティ製プログラム」)が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このCohesity製品に付属するサードパーティの法的通知文書は次の場所です。

<https://www.veritas.com/about/legal/license-agreements>

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Cohesity, Inc. からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Cohesityがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

<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。サポート内容および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>

次の URL で **Cohesity Account** の情報を管理できます。

<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

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、**Cohesity** の **Web** サイトで入手できます。

<https://sort.veritas.com/documents>

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次の **Cohesity** コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

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

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity SORT (Service and Operations Readiness Tools) は、特定の時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する **Web** サイトです。製品によって異なりますが、**SORT** はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。**SORT** がお客様の製品に提供できるサービスとツールについては、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

第 1 章	概要およびメモ	6
	システムセンターの仮想マシンマネージャのための NetBackup のアドイン について (SCVMM)	6
	SCVMM 用 NetBackup アドインに関する注意事項	7
第 2 章	NetBackup Add-in for SCVMM のインストール	8
	SCVMM 用 NetBackup アドインの必要条件	8
	NetBackup Add-in for SCVMM のインストール	8
	14
	17
	外部証明書を使用するためのアドインの構成	18
	NetBackup CA が署名した証明書を使用するためのアドインの再構成	20
	SCVMM 用 NetBackup アドインのアンインストール	21
	NetBackup リカバリウィザードの設定	21
	SCVMM 用 NetBackup アドインのための認証トークンの作成	22
	24
	認証トークンのホスト名または IP アドレスの追加または追加したホスト 名または IP アドレスの削除	28
	認証トークンの取り消し	31
	認証トークンの更新	32
	すべての現在の認証トークンのリスト	33
第 3 章	仮想マシンのリカバリ	35
	リカバリウィザードを使った Hyper-V 仮想マシンのリストアに関する注意事 項	35
	リカバリウィザードへのアクセス	36
	リカバリジョブの状態を調べる	37
第 4 章	トラブルシューティング	40
	SCVMM 対応 NetBackup アドインのログについて	40
	SCVMM 対応 NetBackup アドインのログメッセージの表示	41
	SCVMM 対応 NetBackup アドインのログレベルの変更	43

SCVMM の NetBackup アドインのリカバリウィザードによるリカバリ前検査 で VM に関する古い情報が返される	44
NetBackup アドインリカバリウィザードの[次へ (Next)]ボタンが、必要な入 力が入力されなくても有効になる	45
NetBackup アドインリカバリウィザードで、VM を上書きするよう求められず、 リカバリが失敗する	46
NetBackup Add-in for SCVMM におけるプライマリサーバーの通信エラー のトラブルシューティング	46

概要およびメモ

この章では以下の項目について説明しています。

- システムセンターの仮想マシンマネージャのための **NetBackup** のアドインについて (SCVMM)
- SCVMM 用 **NetBackup** アドインに関する注意事項

システムセンターの仮想マシンマネージャのための **NetBackup** のアドインについて (SCVMM)

Microsoft System Center Virtual Machine Manager (SCVMM) 用 **NetBackup** アドインを利用して、**NetBackup** バックアップイメージから仮想マシンをリカバリできます。

SCVMM コンソールでアドインを使うと次のことができます。

- 元の場所か代替の場所に完全な仮想マシンをリカバリします。
- アドインで開始されたリカバリジョブの進捗状況を監視します。

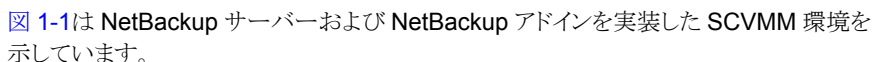
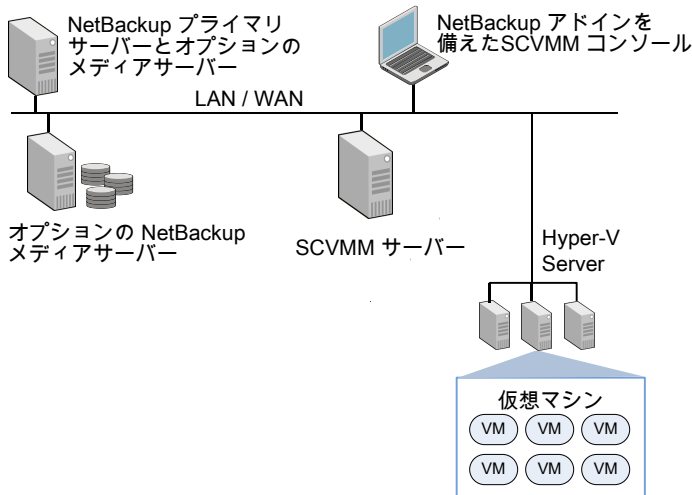
 図 1-1 は **NetBackup** サーバーおよび **NetBackup** アドインを実装した SCVMM 環境を示しています。

図 1-1 NetBackup アドインを実装した NetBackup および SCVMM 環境



SCVMM 用 NetBackup アドインに関する注意事項

NetBackup アドインについては次の点に注意してください。

- SCVMM 用 NetBackup アドインのリリースでは、仮想マシンのバックアップの監視、仮想マシンバックアップからの個々のファイルのリストア、ステージング場所への仮想マシンのリストアはサポートしません。
p.35 の「[リカバリウィザードを使った Hyper-V 仮想マシンのリストアに関する注意事項](#)」を参照してください。
- NetBackup アドインを使うには、管理者ロールで SCVMM コンソールにログオンする必要があります。異なる役割でログオンすると、アドイン機能は無効になります。
- NetBackup アドインを使うすべてのユーザーは NetBackup アドインをインストールする必要があります。
p.36 の「[リカバリウィザードへのアクセス](#)」を参照してください。
- SCVMM 用の NetBackup アドインの今後のバージョンでは、サードパーティアドインに対する Microsoft 社の制限により、NetBackup アドインはその既存バージョンへのアップグレードをサポートしません。アドインの新しいリリースが利用できるようになったときに、現在のバージョンをアンインストールする必要があります。

メモ: アドインを再インストールせずに SCVMM をアップグレードできます。

NetBackup Add-in for SCVMM のインストール

この章では以下の項目について説明しています。

- [SCVMM 用 NetBackup アドインの必要条件](#)
- [NetBackup Add-in for SCVMM のインストール](#)
-
-
- [外部証明書を使用するためのアドインの構成](#)
- [NetBackup CA が署名した証明書を使用するためのアドインの再構成](#)
- [SCVMM 用 NetBackup アドインのアンインストール](#)
- [NetBackup リカバリウィザードの設定](#)

SCVMM 用 NetBackup アドインの必要条件

サポート対象の NetBackup バージョンと SCVMM バージョンのリストについては、次の場所ですぐ入手可能な NetBackup ソフトウェア互換性リスト (SCL) を参照してください。

[NetBackup のすべてのバージョンの互換性リスト](#)

NetBackup Add-in for SCVMM のインストール

このトピックでは、インストールファイルの取得方法と NetBackup Add-in for SCVMM のインストール方法について説明します。

表 2-1 NetBackup Add-in for SCVMM: インストールの必要条件

要件	注意事項
NetBackup アドインのインストールファイル	次の場所からインストールファイル NetBackup_11.0_Plugins.zip をダウンロードできます。 https://my.veritas.com/
SCVMM コンソールホスト	SCVMM コンソールホストまたは別の Windows ホストにインストール用 .zip ファイルをダウンロードします。 メモ: Windows ホストは SCVMM サーバーにネットワーク接続できる必要があります。
SCVMM サーバーとそのクレデンシャル	アドインをインストールしている場合は、SCVMM コンソールで実行されます。 アドインのインストールを完了するには、次の情報が必要です。 <ul style="list-style-type: none">■ 各 SCVMM サーバーのホスト名または IP アドレス■ 各 SCVMM サーバーのユーザー名とパスワード■ 各 SCVMM サーバーのポート番号 (デフォルトは 443 番)
追加のユーザーアクセス	次の状況ではユーザーアクセスの追加が必要になることがあります。 <ul style="list-style-type: none">■ SCVMM コンソールホストでユーザーアカウント制御が有効になっている■ アドインをインストールするユーザーが System Center をインストールしたユーザーではない p.14 の「」を参照してください。

NetBackup Add-in for SCVMM をインストールするには

- 1 MyVeritas の Web サイトで、MyVeritas アカウントを使ってログオンします。

<https://my.veritas.com/>

ログオンのサポートが必要な場合には、アカウント管理者または Cohesity に問い合わせてください。

[ベリタスのサポート](#)

電子メール: CustomerCare@veritas.com

- 2 [MyVeritas] メニューバーで、[ライセンス (Licensing)] をクリックします。
Veritas Entitlement Management System (VEMS) が表示されます。
- 3 [資格 (Entitlements)] をクリックして、[その他のオプション (More Options)] をクリックします。
- 4 [製品名 (Product Name)] フィールドに NetBackup と入力して、[フィルタの適用 (Apply Filters)] をクリックします。
リストに NetBackup 製品の資格が表示されます。

- 5 リスト内の **NetBackup** 製品のいずれかで、[処理 (Actions)] の下の [製品のダウンロード (Download Product)] アイコンをクリックします。

NetBackup 製品のバージョンのリストが表示されます。

- 6 **NetBackup** 製品のいずれかで、[製品のダウンロード (Download Product)] アイコンを再度クリックします。

- 7 NetBackup_11.0_Plugins.zip ファイルを選択して、SCVMM コンソールホストにファイルをダウンロードします。

Veritas Entitlement Management System のサポートについて詳しくは、次の記事を参照してください。

Veritas Entitlement Management ユーザーズガイド

- 8 ダウンロードした NetBackup_11.0_Plugins.zip ファイルを解凍し、VRTSNBUAddIn.zip ファイルを見つけます。

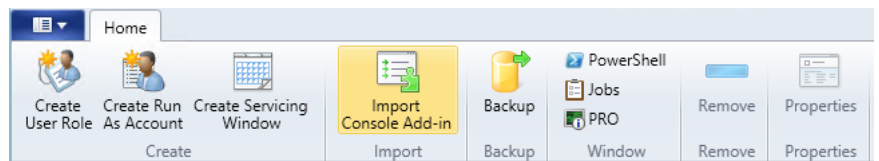
VRTSNBUAddIn.zip ファイルへのパスは次のとおりです。

¥NB_11.0_Plugins¥NBscvmmAddIn¥NetBackup_scvmmAddIn_Win¥VRTSNBUAddIn.zip

メモ: VRTSNBUAddIn.zip ファイルを解凍しないでください。その zip ファイルは、アドインのインストールで必要になります。

ダウンロードした NetBackup_11.0_Plugins.zip ファイルには、その他の **NetBackup** プラグインの zip ファイルも含まれています。それらのファイルは **NetBackup Add-in for SCVMM** には不要です。

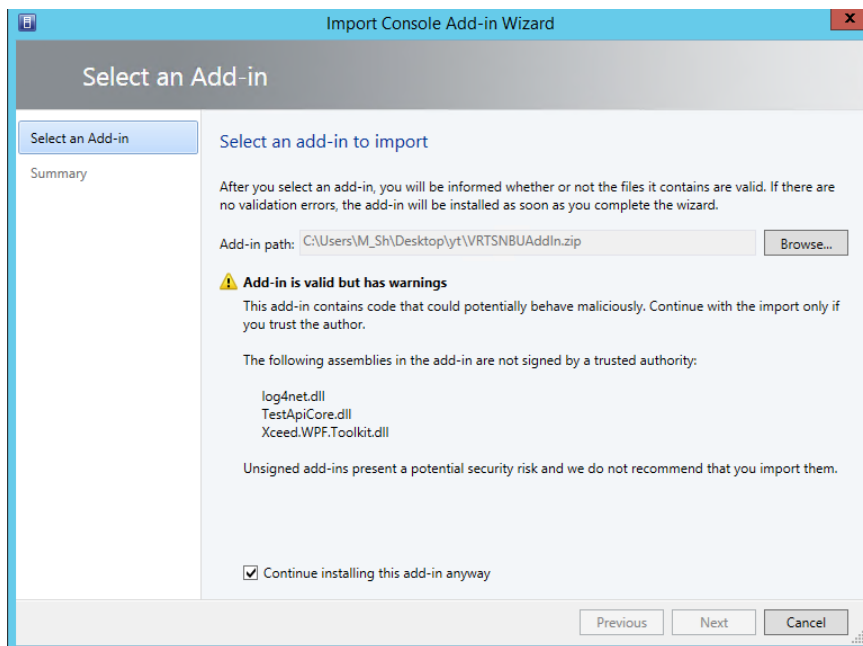
- 9 SCVMM コンソールを起動し、SCVMM サーバーに接続します。
- サーバーのホスト名または IP アドレスとそのログオンクレデンシャルが必要です。
- 10 SCVMM コンソールで、[設定 (Settings)] ワークスペースを開いて SCVMM リボンの [コンソールアドインのインポート (Import Console Add-in)] オプションをクリックします。



[コンソールアドインのインポートウィザード (Import Console Add-in Wizard)] が表示されます。

- 11 [アドインの選択 (Select an Add-in)]画面で、[参照 (Browse)]をクリックし、VRTSNBUAddIn.zip ファイルを見つけます。

複数の警告が表示されます。これらの警告は無視しても問題ありません。



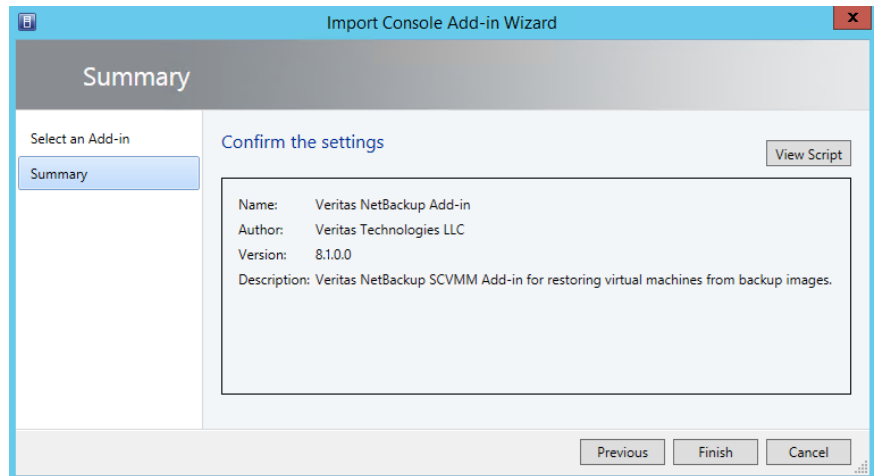
- 12 [このアドインのインストールを続行する (Continue installing this add-in anyway)]をクリックします。

[コンソールアドインのインポートウィザード (Import Console Add-in Wizard)]に「アドインをインストールできません」と表示された場合は、ユーザーアクセスの追加が必要なこともあります。

p.14 の「」を参照してください。

必要なユーザーアクセス権を所有している場合は、NetBackup アドインのファイルを再び参照して (ステップ 11)、このインストール手順を続行します。

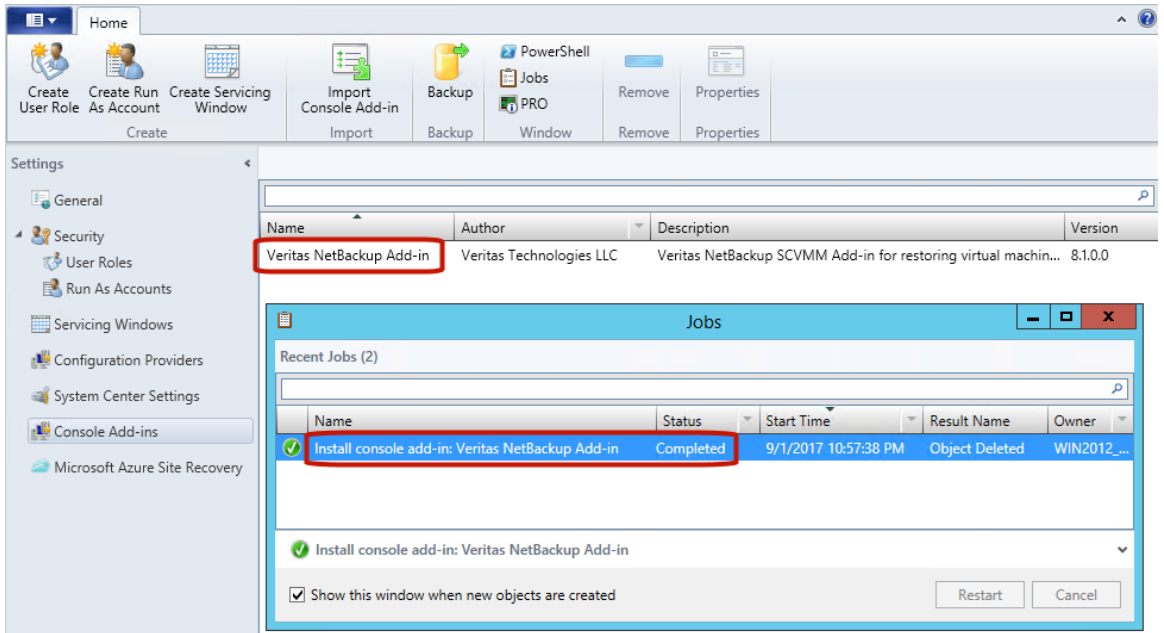
- 13 [概略 (Summary)]画面で[完了 (Finish)]をクリックします。



英語以外のシステムロケールの Windows ホストに NetBackup アドインをインストールすると、インストールが完了したときに SCVMM にメッセージが表示されることがあります。

p.17 の「」を参照してください。

インポートしたアドインが SCVMM コンソールの[ジョブ (Jobs)]ウィンドウと、[設定 (Setting)]ワークスペースの[コンソールアドイン (Console Add-ins)]に表示されます。



- 14 自分自身のクレデンシャルを使って SCVMM コンソールにログインした場合は、メッセージが表示されたら SCVMM コンソールを再起動します。

メモ: [現在の Microsoft Windows セッションの ID を使用する (Use current Microsoft Windows session identity)] オプションを選択した場合は、再起動は不要です。

メモ: NetBackup アドインを使うには、管理者ロールで SCVMM コンソールにログインする必要があります。異なるロールで SCVMM にログインすると、アドイン機能は無効になります。

メモ: NetBackup アドインを初めて使うときに、エンドユーザー使用許諾契約 (EULA) が表示されます。アドインを使うには、EULA に同意する必要があります。

- 15 NetBackup プライマリサーバーが外部証明書を使用している場合は、次のトピックを参照してください。

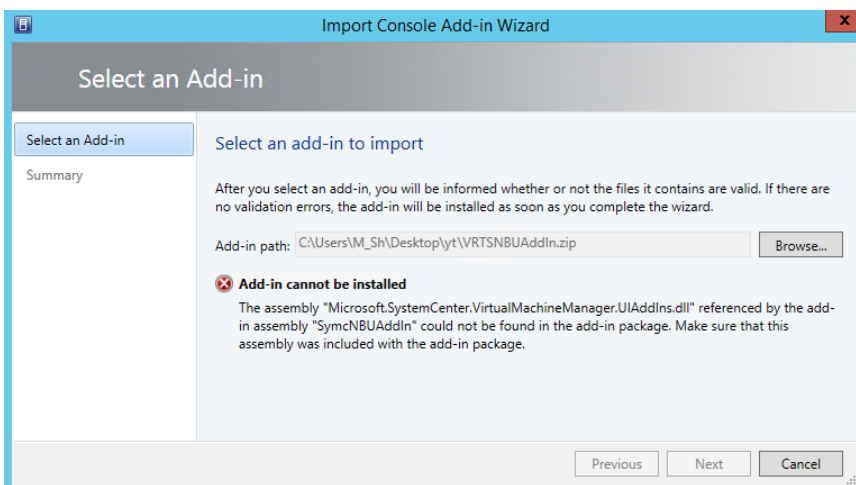
p.18 の「[外部証明書を使用するためのアドインの構成](#)」を参照してください。

ユーザー権限が足りないと、SCVMM 対応 NetBackup アドインのインストール中、「アドインをインストールできません (Add-in cannot be installed)」エラーが発生することがあります。

たとえば、このエラーは次のような状況で発生します。

- ユーザーアカウント制御が SCVMM コンソールホストで有効になっている。
- SCVMM コンソールでアドインをインストールしているユーザーが System Center をインストールしたユーザーではない。

アドインのインストール中、次のメッセージが表示されます。

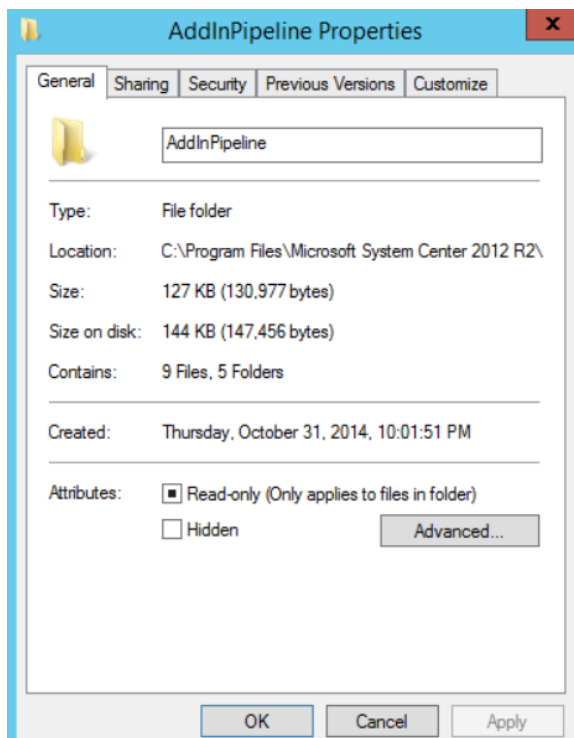


SCVMM コンソールホスト上ですべての認証済みユーザーにインストール権限を付与する方法

- 1 SCVMM コンソールホスト上で、次の場所まで移動します。

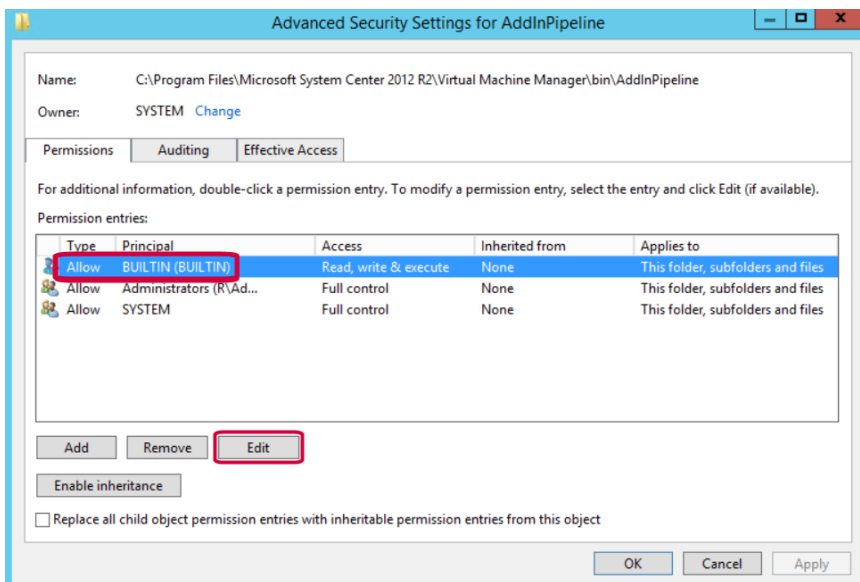
C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\bin

- 2 AddInPipeline フォルダを右クリックし、[プロパティ (Properties)] をクリックします。

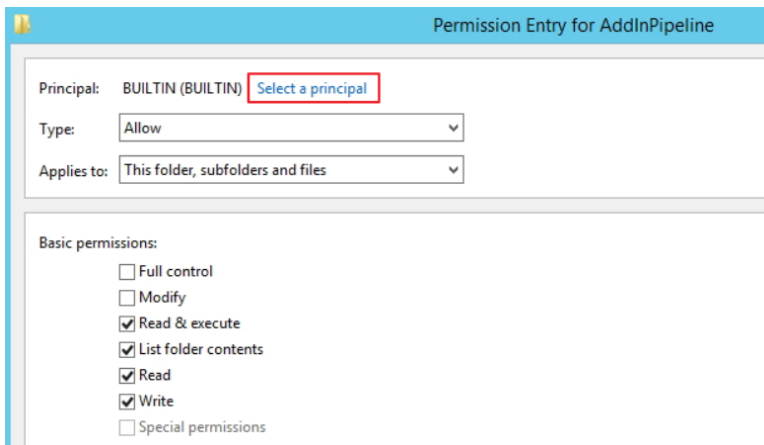


- 3 [セキュリティ (Security)] タブの [詳細 (Advanced)] をクリックし、[続行 (Continue)] をクリックします。

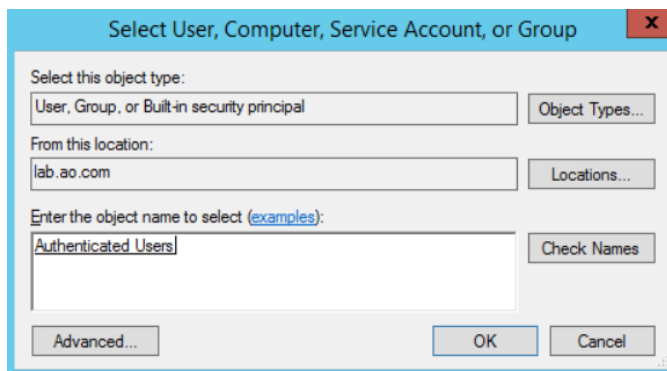
- 4 BUILTIN グループを選択し、[編集 (Edit)]をクリックします。



- 5 [プリンシパルの選択 (Select a principal)]をクリックします。



- 6 「認証済みユーザー (Authenticated Users)」と入力し、[OK]をクリックします。



- 7 各プロパティダイアログボックスを閉じるには、[OK]をクリックします。
次の Microsoft 社の記事に、この問題の詳細情報が記載されています。

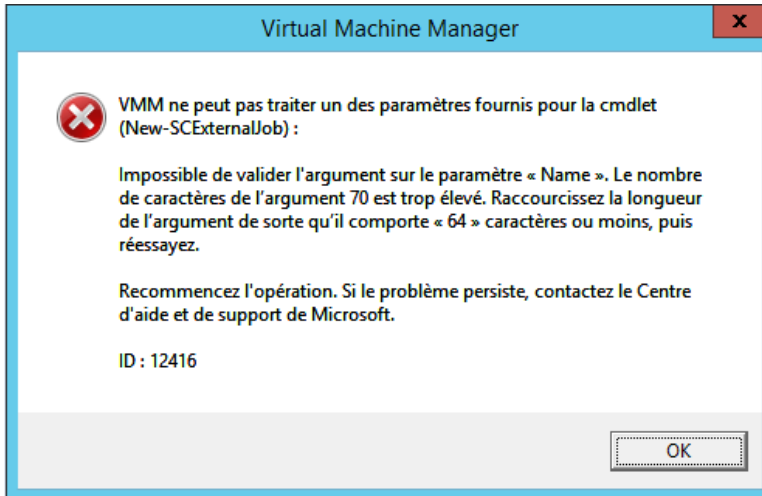
<http://support.microsoft.com/kb/2904712>

- 8 SCVMM 対応 NetBackup アドインをインストールするには:

p.8 の「NetBackup Add-in for SCVMM のインストール」を参照してください。

英語以外のシステムロケールの Windows ホストに NetBackup アドインをインストールすると、インストールが完了したときに SCVMM にメッセージが表示されることがあります。これは、引数が 65 文字以上であるため、これを検証できないことを伝えるメッセージです。このエラーは、選択されたロケールに依存するアドイン名の長さに関する Microsoft 社の制限事項に起因します。

例: 次は、Windows がフランスのシステムロケールに設定されている場合に表示されます。



メモ: このメッセージは無視できます。アドインは正しくインストールされています。

外部証明書を使用するためのアドインの構成

アドインは、証明書ベースの認証を使用して NetBackup プライマリサーバーと安全に通信します。デフォルトでは、プライマリサーバーは、NetBackup CA が署名した証明書を使用します。または、外部で発行された証明書を使用するようにプライマリサーバーを構成できます。その場合は、次の手順により、外部証明書を使用するようにアドインを構成します。

外部証明書を使用するためのアドインの構成

- 1 プライマリサーバーで次のコマンドを入力します。

Windows の場合

```
install_path¥NetBackup¥wmc¥bin¥install¥configureCertsForPlugins.bat  
-registerExternalCert -certPath  
"path_to_external_certificate_file"  
-privateKeyPath "path_to_certificate_key_file"  
-trustStorePath "path_to_ca_certificate_file"
```

UNIX および Linux の場合

```
/usr/opensv/wmc/bin/install/configureCertsForPlugins  
-registerExternalCert -certPath  
"path_to_external_certificate_file"
```

```
-privateKeyPath "path_to_certificate_key_file"  
-trustStorePath "path_to_ca_certificate_file"
```

次に例を示します。

```
configureCertsForPlugins.bat -registerExternalCert -certPath  
"c:\%server.pem" -privateKeyPath "c:\%key.pem" -trustStorePath  
"c:\%intermediateOrRootCA.pem"
```

このコマンドで、証明書をプライマリサーバー上のキーストアにインポートして、外部証明書を使用するようにアドインを構成します。コマンドのオプションは次のとおりです。

- `-certPath`: **Web** サーバー証明書へのパスを指定します。このファイルには、**PEM** 形式の 1 つの証明書が必要です。
- `-privateKeyPath`: **Web** サーバー証明書の秘密鍵へのパスを指定します。
- `-trustStorePath`: **Web** サーバー証明書を発行した中間認証局またはルート認証局の証明書へのパスを指定します。このファイルには、**PEM** 形式の 1 つの証明書が必要です。この証明書のサブジェクトは、**Web** サーバー証明書の発行者と一致する必要があります。
外部証明書について詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』を参照してください。

- 2 プライマリサーバーで NetBackup Web Management Console サービスを再起動します。

アクティビティモニターで、[デーモン (Daemons)] タブを選択します。サービスを見つけて、[処理]>[停止]を選択します。サービスが停止したら、[処理]>[開始]を選択します。

- 3 プライマリサーバーで認証トークンを更新します。
p.32 の「[認証トークンの更新](#)」を参照してください。

メモ: この手順を、プライマリサーバーと通信する必要がある各アドインで実行します。

- 4 アドインで、既存のプライマリサーバーを削除し、トークンを更新したプライマリサーバーを追加します。
p.24 の「」を参照してください。

NetBackup CA が署名した証明書を使用するためのアドインの再構成

NetBackup CA が署名した証明書を使用するようにプライマリサーバーを再構成した場合、この証明書を使用するようにアドインを構成するには、次の手順を実行します。

NetBackup CA が署名した証明書を使用するためのアドインの再構成

- 1 プライマリサーバーで次のコマンドを入力します。

Windows の場合:

```
install_path¥NetBackup¥wmc¥bin¥install¥configureCertsForPlugins.bat  
-registerNBCAcert
```

UNIX または Linux の場合:

```
/usr/opensv/wmc/bin/install/configureCertsForPlugins  
-registerNBCAcert
```

このコマンドにより、NetBackup CA が署名した証明書を使用するようにアドインが再構成されます。

- 2 プライマリサーバーで NetBackup Web Management Console サービスを再起動します。

アクティビティモニターで、[デーモン (Daemons)] タブを選択します。サービスを見つけて、[処理]>[停止]を選択します。サービスが停止したら、[処理]>[開始]を選択します。

- 3 プライマリサーバーで認証トークンを更新します。

p.32 の「[認証トークンの更新](#)」を参照してください。

メモ: この手順を、プライマリサーバーと通信する必要がある各アドインで実行します。

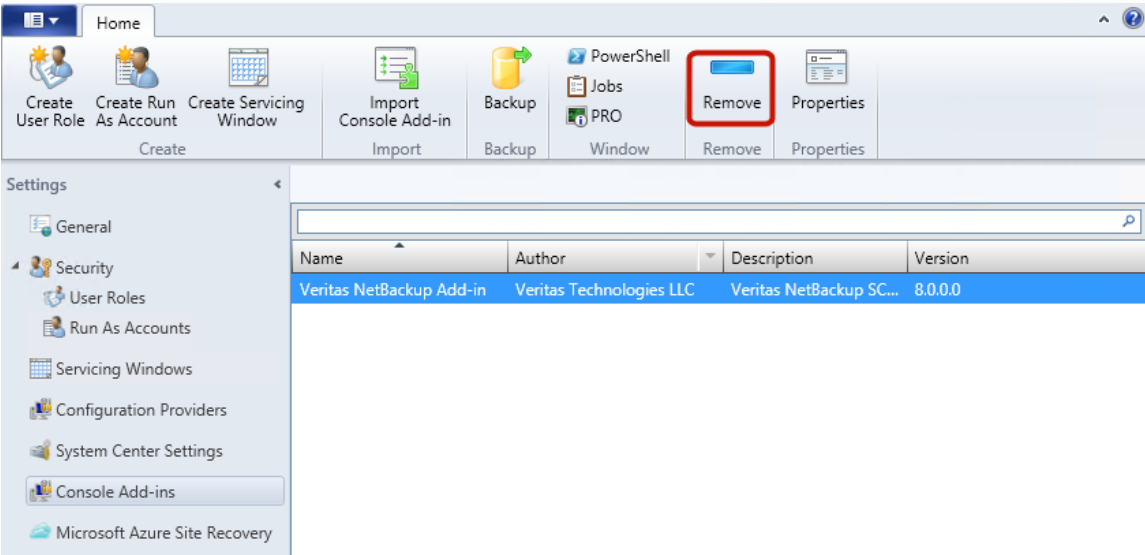
- 4 アドインで、既存のプライマリサーバーを削除し、トークンを更新したプライマリサーバーを追加します。

p.24 の「[」](#)を参照してください。

SCVMM 用 NetBackup アドインのアンインストール

SCVMM 用 NetBackup アドインをアンインストールするには

- 1
- SCVMM コンソールで、[設定 (Settings)]ワークスペースを開きます。
- 2
- [コンソールアドイン (Console Add-ins)]ノードで、Veritas NetBackup アドインをクリックしてから[削除 (Remove)]をクリックします。



- 3
- 削除を確認するように求められたら、[はい (Yes)]をクリックします。
- アンインストールされたことが SCVMM コンソールの[ジョブ (Jobs)]ウィンドウに示されます。

NetBackup リカバリウィザードの設定

仮想マシンをリストアするために NetBackup リカバリウィザードを使用するには、次のように設定します。

表 2-2 NetBackup リカバリウィザードの設定

手順	説明	参照トピック
1	認証トークンファイルを作成します。*	p.22 の「SCVMM 用 NetBackup アドインのための認証トークンの作成」を参照してください。

手順	説明	参照トピック
2	NetBackup アドインを承認して仮想マシンをリストアします。	p.24 の「 J 」を参照してください。

*特定の状況では、認証トークンを追加の SCVMM コンソールホスト名または IP アドレスに関連付ける必要があります。

p.28 の「[認証トークンのホスト名または IP アドレスの追加または追加したホスト名または IP アドレスの削除](#)」を参照してください。

SCVMM 用 NetBackup アドインのための認証トークンの作成

アドインに仮想マシンのリストアを許可するには、NetBackup プライマリサーバーで認証トークン (またはプライマリサーバーとしての NetBackup Appliance で証明書) を生成する必要があります。認証トークンがプライマリサーバー上で作成され、NetBackup アドインに配備されると、アドインがそのプライマリサーバーから Hyper-V バックアップをリストアできるようになります。

NetBackup プライマリサーバーで認証トークンを作成するには

- 1 プライマリサーバーで次を入力します。

Windows の場合

```
install_path¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat  
-create clientName
```

UNIX および Linux の場合

```
/usr/opensv/wmc/bin/install/manageClientCerts -create clientName
```

clientName は、アドインがインストールされている SCVMM コンソールホストの DNS 名です。manageClientCerts コマンドは認証トークンを含んでいる圧縮ファイルの場所を返します。

メモ: SCVMM コンソールホストが SCVMM サーバーとは別のホストの場合は、(SCVMM サーバーのホスト名ではなく) SCVMM コンソールホストのトークンを生成します。

- 2 SCVMM サーバー管理者に圧縮認証トークンファイルを提供します。

注意: 圧縮ファイルの共有や送信には、必ず安全な方法を使用してください。

プライマリサーバートークンを使用すると、仮想マシンをリストアするためにアドインを認証できます。

p.24 の「」を参照してください。

プライマリサーバーとして、**NetBackup Appliance** で認証トークン (証明書) を作成するには

- 1 証明書を生成するには、次の場所で入手可能な『NetBackup Appliance 管理者ガイド』内の「管理 > 証明書」トピックを参照してください。

<http://www.veritas.com/docs/000002217>

- 2 SCVMM 管理者に証明書の圧縮ファイルを提供してください。

注意: 圧縮ファイルの共有や送信には、必ず安全な方法を使用してください。

プライマリサーバー証明書を使用すると、仮想マシンをリストアするためにアドインを認証できます。

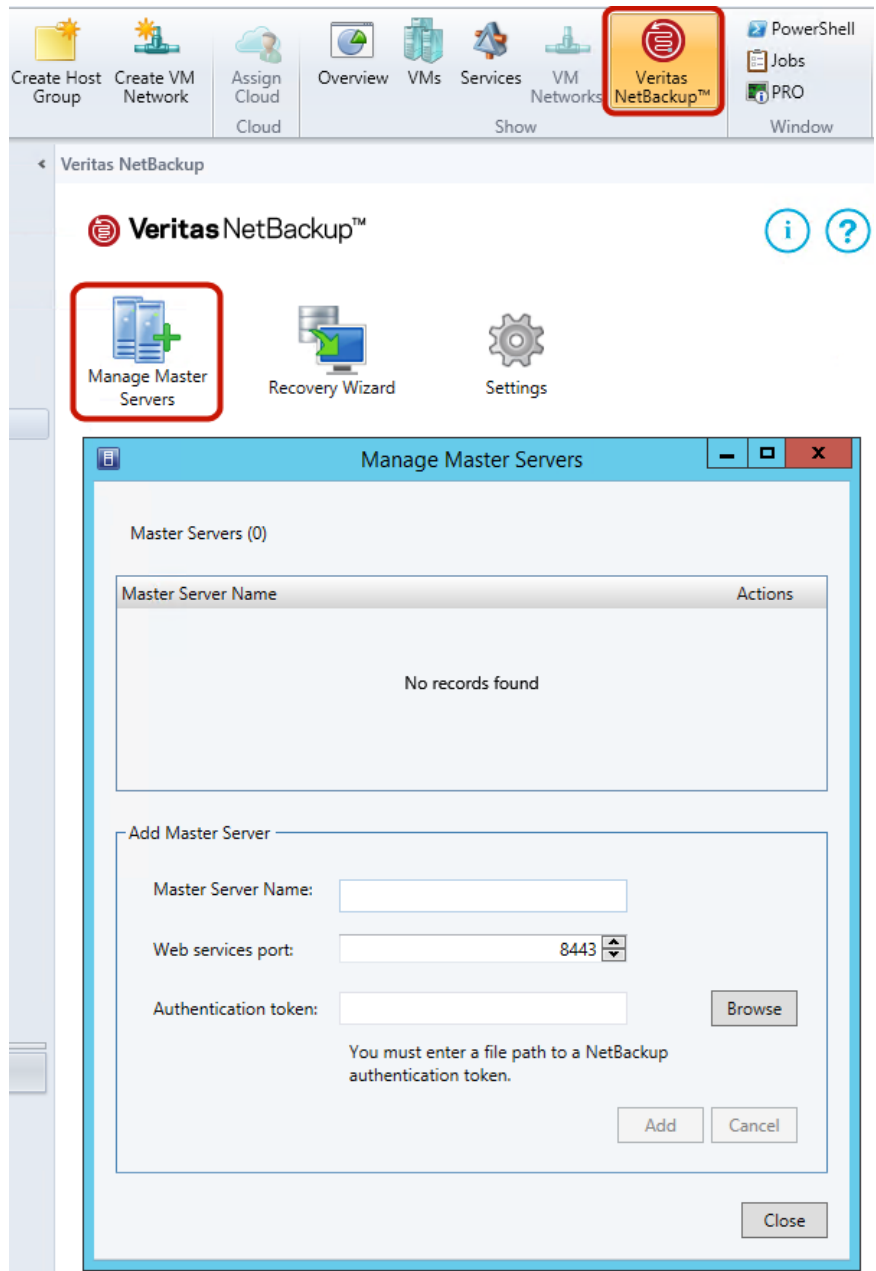
p.24 の「」を参照してください。

NetBackup プライマリサーバーは、仮想マシンのバックアップを開始および制御します。仮想マシンのリストアにアドインを使用するには、プライマリサーバー認証トークンを NetBackup 管理者から入手する必要があります。トークンを入手したら、アドインを承認することでプライマリサーバーによってバックアップされた仮想マシンをリストアできます。

アドインで仮想マシンをリストアすることを承認 (または、承認を編集、削除) するには

- 1 NetBackup 管理者に認証トークンファイルを提供するように依頼します。
p.22 の「[SCVMM 用 NetBackup アドインのための認証トークンの作成](#)」を参照してください。
- 2 SCVMM コンソールを起動するコンピュータまたはノートパソコンに認証トークンファイルをコピーします。
場所を書き留め ておきます。
- 3 SCVMM コンソールのリボンで、[NetBackup] オプションをクリックします。

- 4 [マスターサーバーの管理 (Manage Master Servers)]をクリックします。



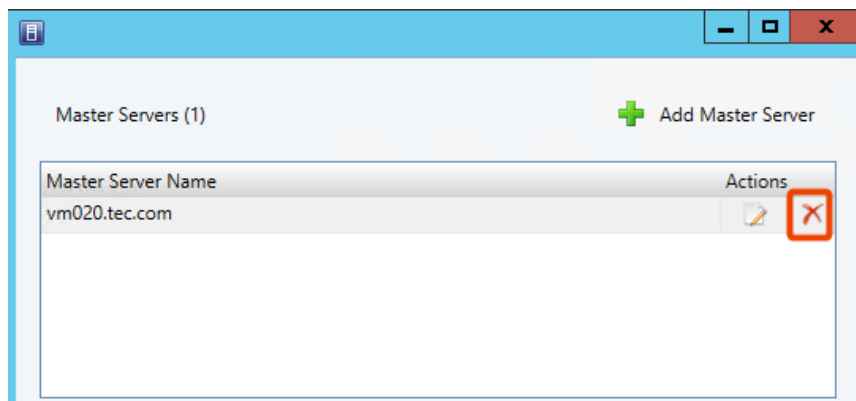
- 5 [マスターサーバーの追加 (Add Master Server)]で次の項目を入力して NetBackup プライマリサーバーと認証トークンを指定します。

- マスターサーバーの追加 (Add Master Server)
- マスターサーバー名 (Master Server Name)
プライマリサーバーの完全修飾ドメイン名を入力します。
 - Web サービスポート (Web services port)
NetBackupの管理者がポートを変更していない場合は、デフォルト (8443) を受け入れてください。ポートが変更されている場合は、正しいポート番号を管理者に問い合せてください。
 - 認証トークン (Authentication token)
[参照 (Browse)]をクリックし、NetBackup 管理者が提供した認証トークンファイルを選択します。
[追加 (Add)]をクリックします。アドインが通信できるプライマリサーバーのリストにサーバーが追加されます。

- 6 SCVMM コンソールがプライマリサーバーと通信できることを検証するには、[状態の確認 (Check Status)]をクリックします。

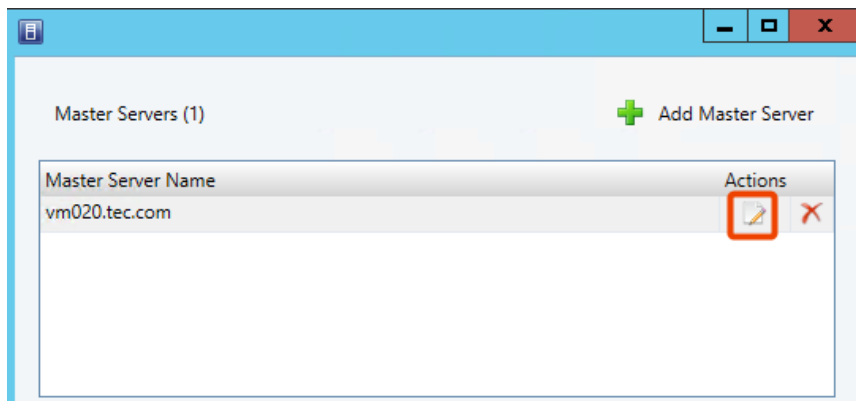
正常に通信している場合は、[接続の状態 (Connection Status)]フィールドに[接続済み (Connected)]と表示されます。

- 7 他のプライマリサーバーとその認証トークンを追加するには、右上にある[マスターサーバーの追加 (Add Master Server)]をクリックして手順 5 と 6 を繰り返します。
- 8 承認を削除するには、プライマリサーバー名の隣にある削除アイコンをクリックします。

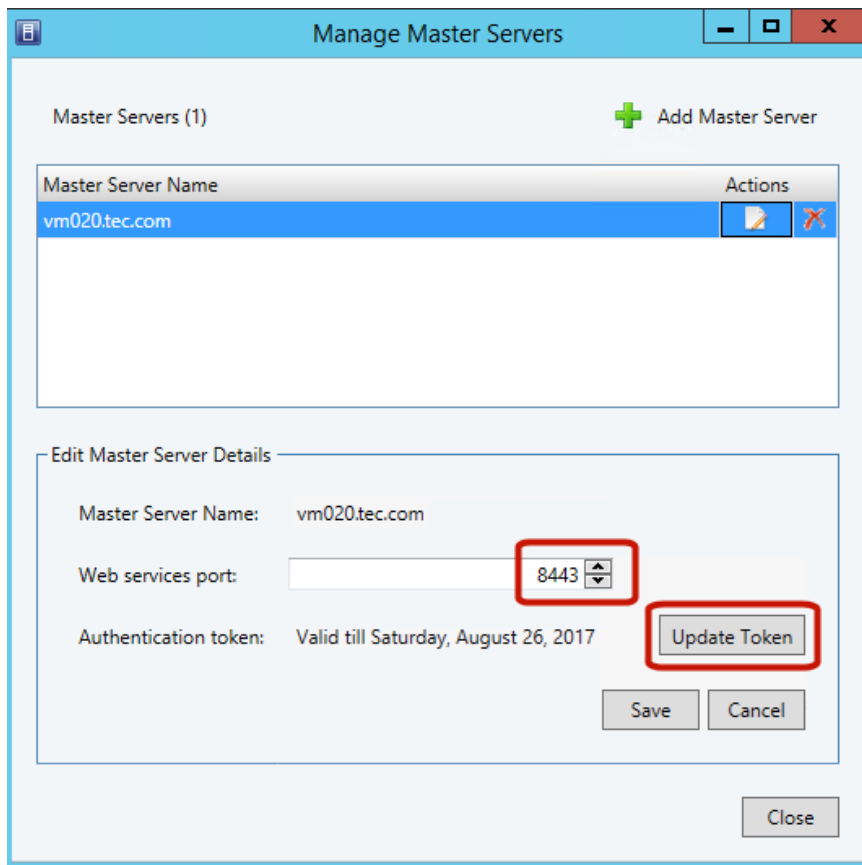


承認を削除すると、アドインはプライマリサーバーが実行したバックアップからリストアできなくなります。

- 9 承認を編集するには、プライマリサーバー名の反対側にある編集アイコンをクリックします。



異なる Web サービスポートを入力することも、[トークンの更新 (Update Token)]をクリックして異なる認証トークンを選択することもできます。



- 10 [保存 (Save)]をクリックします。
- 11 [閉じる (Close)]をクリックします。

認証トークンのホスト名または IP アドレスの追加または追加したホスト名または IP アドレスの削除

manageClientCerts コマンドは、特定の SCVMM コンソールホストの認証トークンを生成します。このトークンにより、トークンが生成された NetBackup プライマリサーバーに SCVMM コンソールホストがアクセスできるようになります。トークンは、SCVMM コンソールホスト名が manageClientCerts コマンドで入力した名前と同一である場合に有効になります。

環境によっては、トークンを複数のホスト名または IP アドレスでできるようにする必要があります。例として、クラスタ化された SCVMM サーバーでは、NetBackup プライマリ

サーバーへのアクセス要求が、トークンの生成時に指定されたものとは異なるホスト名または IP アドレスから来ることがあります。

このような環境から NetBackup にアクセスできるようにするには、manageClientCerts コマンドを使って次のことを行います。

- 既存のトークンに SCVMM コンソールホストの他のホスト名 (または IP アドレス) を追加します。追加されたホスト名または IP アドレスは、エイリアスとよばれます。注意: エイリアスは、1 つのトークンに複数追加することができます。
IPv4 および IPv6 のアドレスがサポート対象です。
- トークンからホスト名または IP アドレスを削除します。
- 任意の SCVMM コンソールホストでトークンの使用を許可します。
- トークンの既存のエイリアスを一覧表示します。

manageClientCerts コマンドは、次の場所に格納されています。

Windows の場合:

```
install_path¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat
```

UNIX および Linux の場合:

```
/usr/opensv/wmc/bin/install/manageClientCerts
```

表 2-3 既存の認証トークンへのホスト名または IP アドレスの追加

タスク	NetBackup プライマリサーバーで次を入力:
ホスト名の追加	<pre>manageClientCerts -addAlias host_name_used_to_generate_token -HOST additional_host_name_for_token</pre> <p><i>host_name_used_to_generate_token</i> はトークンを生成するときに指定したホスト名、<i>additional_host_name_for_token</i> は追加する SCVMM コンソールホストのホスト名です。</p> <p>例:</p> <pre>manageClientCerts -addAlias SCVMM1 -HOST SCVMM1.example.com</pre> <p>コマンドの出力:</p> <pre>Successful -addAlias, for client: SCVMM1, type: HOST, alias: SCVMM1.example.com</pre> <p>この例では、追加したホスト名は SCVMM1.example.com です。</p> <p>メモ: 1 つのトークンに複数ホスト名を追加できます。manageClientCerts の各インスタンスに 1 つずつホスト名を追加します。</p>

タスク	NetBackup プライマリサーバーで次を入力:
1 つの IP アドレスまたは IP アドレスの範囲の追加	<pre>manageClientCerts -addAlias host_name_used_to_generate_token -IP IP_address_for_token IP_address_with_netmask_for_token</pre> <p>ここで、host_name_used_to_generate_token はトークンが生成されたときに指定されたホスト名です。IP アドレスは、1 つのアドレス (IP_address_for_token) またはアドレスの範囲 (IP_address_with_netmask_for_token) として追加できます。</p> <p>例:</p> <p>1 つの IP アドレスの追加:</p> <pre>manageClientCerts -addAlias SCVMM1 -IP 10.80.154.1</pre> <p>ネットマスクの使用による IP アドレスの範囲の追加:</p> <pre>manageClientCerts -addAlias SCVMM1 -IP 10.80.154.0/29</pre> <p>この例では、10.80.154.0/29 により、IP アドレスが 10.80.154.1 から 10.80.154.7 までの 6 つのホストが同じトークンを使用できるようになります。</p> <p>メモ: IP アドレスの範囲については、manageClientCerts は IP ネットマスク、別名 Classless Inter-Domain Routing (CIDR) 表記に対応します。</p> <p>メモ: 1 つのトークンに複数の IP アドレスを追加できます。範囲として追加するのではない場合、manageClientCerts の各インスタンスに1つずつ IP アドレスを追加します。</p> <p>メモ: IPv4 および IPv6 のアドレスがサポート対象です。</p>
任意のホストによるトークンの使用の許可	<pre>manageClientCerts -addAlias host_name_used_to_generate_token -ANY</pre> <p>ここで、host_name_used_to_generate_token はトークンが生成されたときに指定されたホスト名です。-ANY では、任意のホストまたは任意の IP アドレスが、このトークンを使用して NetBackup サーバーと通信できるようになります。</p> <p>注意:-ANY オプションの使用には注意が必要です。任意のホストがトークンを使用できるようにすると、セキュリティリスクを招くおそれがあります。</p>

表 2-4 既存の認証トークンからのホスト名または IP アドレスの削除

タスク	NetBackup プライマリサーバーで次を入力:
ホスト名の削除	<pre>manageClientCerts -deleteAlias host_name_used_to_generate_token -HOST host_name_to_delete</pre> <p>ここで、host_name_used_to_generate_token はトークンが生成されたときに指定されたホスト名、host_name_to_delete は削除される名前です。</p>
IP アドレスの削除	<pre>manageClientCerts -deleteAlias host_name_used_to_generate_token -IP IP_address_to_delete</pre> <p>ここで、host_name_used_to_generate_token はトークンが生成されたときに指定されたホスト名、IP_address_to_delete は削除される IP アドレスです。</p>

タスク	NetBackup プライマリサーバーで次を入力:
-ANY オプションの削除	<pre>manageClientCerts -deleteAlias host_name_used_to_generate_token -ANY</pre> <p>ここで、<i>host_name_used_to_generate_token</i> はトークンが生成されたときに指定されたホスト名です。 -ANY オプションがトークンから削除されます。トークンに特定のエイリアス (ホスト名または IP アドレス) が追加されていた場合、それらのエイリアスは有効なまま残ります。</p>

表 2-5 トークンに対して定義されたホスト名または IP アドレス (エイリアス) の一覧表示

タスク	NetBackup プライマリサーバーで次を入力:
ホスト名または IP アドレス (エイリアス) の一覧表示	<pre>manageClientCerts -listAliases host_name_used_to_generate_token</pre> <p>ここで、<i>host_name_used_to_generate_token</i> はトークンが生成されたときに指定されたホスト名です。</p> <p>例:</p> <pre>manageClientCerts -listAliases SCVMM1</pre> <p>コマンドの出力:</p> <pre>Aliases for SCVMM1: HOST = SCVMM1.example.com</pre> <p>この例では、エイリアスは SCVMM1.example.com です。トークンに -ANY オプションが設定されている (任意のホストまたは任意の IP アドレスからの接続を受け入れる) 場合、-listAliases の出力は次のようになります。</p> <pre>Aliases for SCVMM1: HOST = *</pre>

補足情報が利用可能です。

p.46 の「[NetBackup Add-in for SCVMM におけるプライマリサーバーの通信エラーのトラブルシューティング](#)」を参照してください。

認証トークンの取り消し

次のように、認証トークンを削除または取り消すことができます。

認証トークンを取り消すには

- ◆ プライマリサーバーで次を入力します。

Windows の場合

```
install_path¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat  
-delete clientName
```

UNIX および Linux の場合

```
/usr/opensv/wmc/bin/install/manageClientCerts -delete clientName
```

clientName は、アドインがインストールされている SCVMM コンソールホストの DNS 名です。

-delete オプションにより、プライマリサーバーから認証トークンとその圧縮ファイルを削除します。このプライマリサーバーが作成したバックアップから仮想マシンをリストアする権限がアドインからなくなります。

認証トークンの更新

有効期限が切れた認証トークンは、次のように更新することができます。

メモ: 認証トークンは、1 年後に期限が切れます。

認証トークンを更新するには

- 1 プライマリサーバーで次を入力します。

Windows の場合

```
install_path¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat  
-renew clientName
```

UNIX および Linux の場合

```
/usr/opensv/wmc/bin/install/manageClientCerts -renew clientName
```

clientName は、アドインがインストールされている SCVMM コンソールホストの DNS 名です。

-renew オプションを使うと、トークンが削除され、新しいトークンが作成されます。トークンに存在するエイリアスはすべて保持されます。

p.33 の「すべての現在の認証トークンのリスト」を参照してください。

p.28 の「認証トークンのホスト名または IP アドレスの追加または追加したホスト名または IP アドレスの削除」を参照してください。

- 2 アドインの[マスターサーバー登録 (Register Master Servers)]オプションを使用し、更新された認証トークンを使用してプライマリサーバーを再登録します。

p.24 の「」を参照してください。

すべての現在の認証トークンのリスト

現在のプライマリサーバーで生成されたすべての現在の認証トークンを一覧表示できます。

すべての現在の認証トークンをリストするには

- ◆ プライマリサーバーで次を入力します。

Windows の場合

```
install_path¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat -list
```

UNIX および Linux の場合

```
/usr/opensv/wmc/bin/install/manageClientCerts -list
```

次に出力例を示します。

Client	Expiry Date
SCVMM_console_host_1	Thu Feb 06 16:16:51 GMT+05:30 2016
SCVMM_console_host_2	Fri Feb 07 11:22:53 GMT+05:30 2016

このコマンドはトークンを作成した **SCVMM** コンソールホストとその有効期限を表示します。この情報は、証明書が期限切れになったときに **SCVMM** コンソールホストとプライマリサーバー間で起きる通信の問題の診断に役立ちます。

- 書式付きで出力する場合は、コマンドプロンプトまたはシェルの画面サイズを 100 単位以上に設定します。
- 40 文字を超えるサーバー名は切り捨てられ、先頭から 40 文字を超える文字が "..." に置換されます。

仮想マシンのリカバリ

この章では以下の項目について説明しています。

- リカバリウィザードを使った **Hyper-V** 仮想マシンのリストアに関する注意事項
- リカバリウィザードへのアクセス
- リカバリジョブの状態を調べる

リカバリウィザードを使った **Hyper-V** 仮想マシンのリストアに関する注意事項

NetBackup イメージから仮想マシンをリストアするには、**SCVMM** コンソールの **NetBackup** リカバリウィザードを使います。

NetBackup アドインリカバリウィザードについては、次の点に注意してください。

- **NetBackup** リカバリウィザードは仮想マシン全体をリストアするもので、個別ファイルのリストアには使えません。仮想マシンのバックアップから個々のファイルをリストアするには、**NetBackup** のバックアップ、アーカイブ、リストアインターフェースを使います。
『**NetBackup for Hyper-V** 管理者ガイド』で個々のファイルのリストアに関するトピックを参照してください。
- **NetBackup** リカバリウィザードはステージング場所に対するリストアをサポートしません。ステージング場所に仮想マシンをリストアするには、**NetBackup** のバックアップ、アーカイブ、リストアインターフェースを使います。
- **Hyper-V** マネージャを使って個々の **Hyper-V** ホストまたはクラスタに対して行った変更は、**SCVMM** コンソールに反映されるまで最大で **24 時間** かかる場合があります。それまでは、**NetBackup** アドインリカバリウィザードには最新の仮想マシン構成状態が反映されていません。その場合、リカバリウィザードの **VM** の場所に関連するリカバリ前チェックは、**SCVMM** の最新データに基づいていない場合があります。リカバリウィザードで異なる選択を実行しなければならない場合があります。

p.44 の「[SCVMM の NetBackup アドインのリカバリウィザードによるリカバリ前検査で VM に関する古い情報が返される](#)」を参照してください。

- NetBackup Web UI には、仮想マシンをリストアするための次の拡張機能が含まれています。
 - 代替の場所に仮想マシンをリストアする際に、新しい VM GUID がデフォルトで生成されます。
 - 仮想マシンをリストアする際に、新しい仮想マシンの表示名を指定できます。

メモ: NetBackup リカバリウィザードは、これらのリストアのための拡張機能をサポートしません。NetBackup Web UI または `nbrestorevm` コマンドを使用して、仮想マシンをリストアするときに新しい GUID を生成するか、または新しい表示名を設定します。

- リカバリウィザードを使用する前提条件:
p.21 の「[NetBackup リカバリウィザードの設定](#)」を参照してください。

リカバリウィザードへのアクセス

このトピックで説明しているように、SCVMM コンソールで NetBackup アドインからリカバリウィザードを起動できます。

メモ: アドインにアクセスするには、自分でアドインをインストールする必要があります。アドインをインストールしていない場合は、[NetBackup] オプションが SCVMM リボンに表示されません。

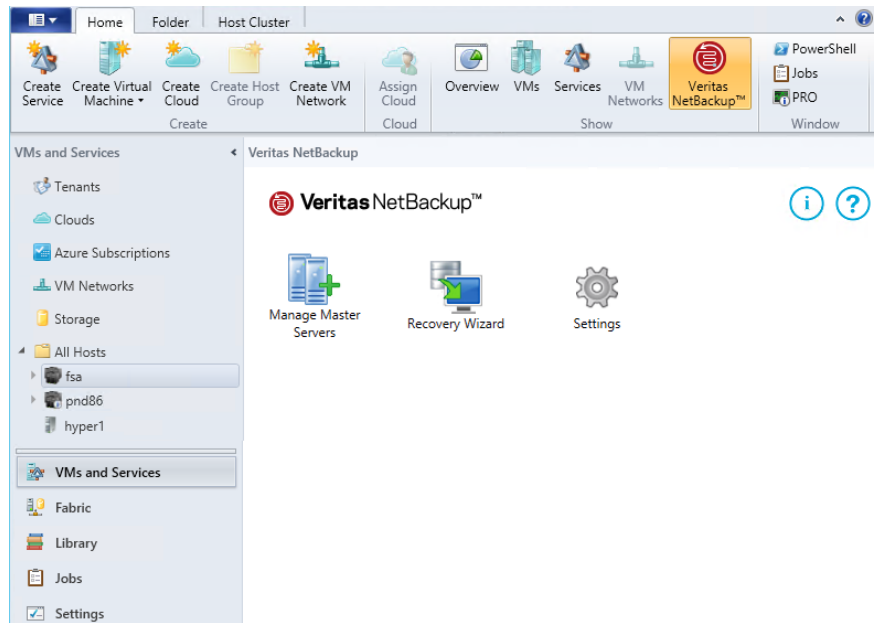
リカバリウィザードにアクセスするには

- 1 SCVMM コンソールで、[VM とサービス (VMs and Services)] ワークスペースを開きます。
- 2 [すべてのホスト (All Hosts)] をクリックします。

- 3 SCVMM リボンで、[NetBackup] オプションをクリックします。

NetBackup アドインを初めて使うときに、エンドユーザー使用許諾契約 (EULA) が表示されます。アドインを使うには、EULA に同意する必要があります。

NetBackup アドインのコンポーネントが表示されます。



- 4 [リカバリウィザード (Recovery Wizard)] をクリックします。

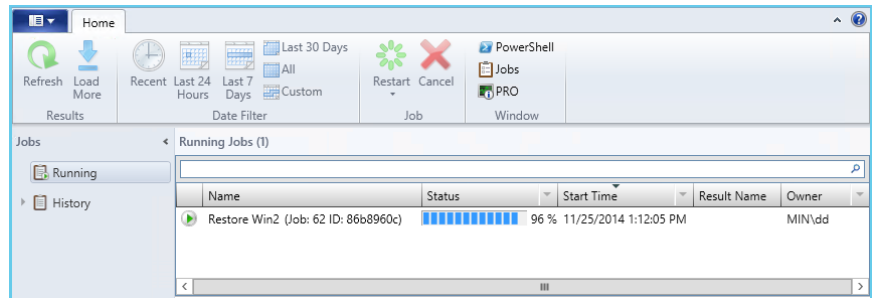
[仮想マシンの選択 (Virtual Machine Selection)] 画面が表示されます。

リカバリジョブの状態を調べる

進行中のリカバリジョブの状態を調べることも、すべてのリカバリジョブの履歴を表示することもできます。

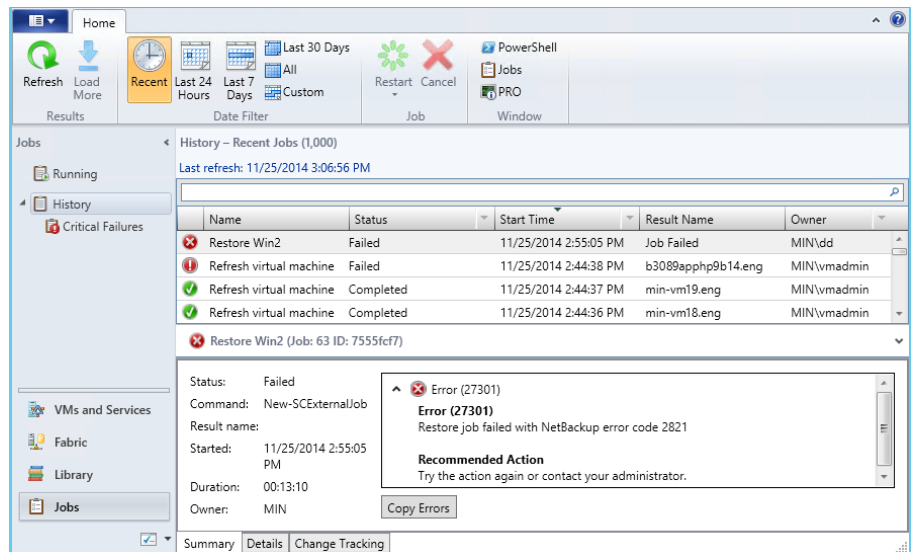
リカバリジョブの状態を調べるには

- 1 SCVMM コンソールで、[ジョブ (Jobs)]ワークスペースを開きます。
- 2 進行中のジョブの場合は、[実行中 (Running)]をクリックします。



[状態 (Status)]列にジョブの完了率が表示されます。

- 3 最近のジョブと過去のジョブを表示する場合は、[履歴 (History)]をクリックします。



進行中のジョブすべての[状態 (Status)]列に、[完了 (Completed)]または[失敗 (Failed)]の状態が示されます。

NetBackup プライマリサーバーが切断された場合やリカバリ中に停止した場合は、[状態 (Status)]列が次のように更新されます。

Failed - Lost connection with NetBackup Master Server.

注意: 列ヘッダーをクリックするとリストの順序を変更できます。

注意: [再起動 (Restart)]ボタンと[キャンセル (Cancel)]ボタンは利用できないのでグレー表示されます。

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。

- [SCVMM 対応 NetBackup アドインのログについて](#)
- [SCVMM 対応 NetBackup アドインのログメッセージの表示](#)
- [SCVMM 対応 NetBackup アドインのログレベルの変更](#)
- [SCVMM の NetBackup アドインのリカバリウィザードによるリカバリ前検査で VM に関する古い情報が返される](#)
- [NetBackup アドインリカバリウィザードの\[次へ \(Next\)\]ボタンが、必要な入力が入力されなくても有効になる](#)
- [NetBackup アドインリカバリウィザードで、VM を上書きするよう求められず、リカバリが失敗する](#)
- [NetBackup Add-in for SCVMM におけるプライマリサーバーの通信エラーのトラブルシューティング](#)

SCVMM 対応 NetBackup アドインのログについて

SCVMM 対応 NetBackup アドインは、次の活動をログメッセージとして記録します。

- NetBackup アドインによる VM のリストア。
- NetBackup アドインからの NetBackup プライマリサーバーの追加または削除。

表 4-1 SCVMM 対応 NetBackup アドインのログ

ログの詳細	説明
ログメッセージ形式	<p>yyyy-mm-dd hh:mm:ss,ms [pid] message</p> <p>次に例を示します。</p> <p>2014-09-24 14:57:32,408 [1] INFO - Loading SCVMMAddin</p>
ログレベル	<p>複数のログ記録レベル (詳細度) があります。</p> <p>p.43 の「SCVMM 対応 NetBackup アドインのログレベルの変更」を参照してください。</p>
ログの場所	<p>ログの場所は SCVMM のインストール場所とログオンユーザーによって異なります。</p> <p>次に、ユーザー JDoe のログ先の例を示します。</p> <p>C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\JDoe\SymcNBAddIn\Logs</p> <p>p.41 の「SCVMM 対応 NetBackup アドインのログメッセージの表示」を参照してください。</p>
ログの保持期間	<p>すべてのログメッセージは 24 時間同じログファイルに書き込まれます。各ログファイルは 7 日間保有され、その後、自動的に削除されます。</p>

SCVMM 対応 NetBackup アドインのログメッセージの表示

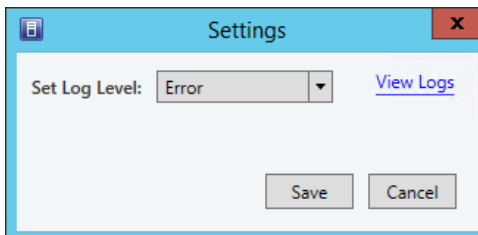
メモ: ログファイルは 7 日間保有され、その後自動的に削除されます。

メモ: NetBackup アドインに対して 24 時間ログ活動が発生しなければ、ログファイルは作成されません。

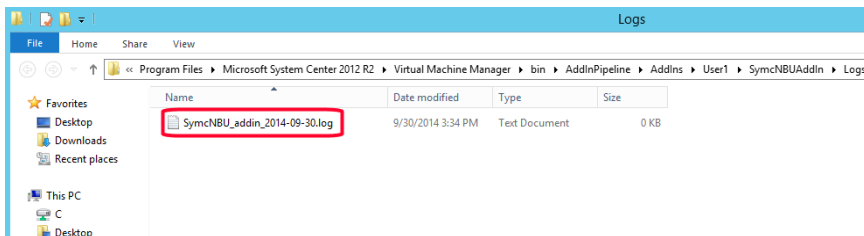
SCVMM 対応 NetBackup アドインのログメッセージを表示する方法

- 1 SCVMM コンソールで、[VM とサービス (VMs and Services)]ワークスペースを開きます。
- 2 [すべてのホスト (All Hosts)]をクリックします。
- 3 SCVMM リボンで、[NetBackup]オプションをクリックします。

- 4 [設定]をクリックします。
- 5 [ログの表示 (View Logs)]をクリックします。

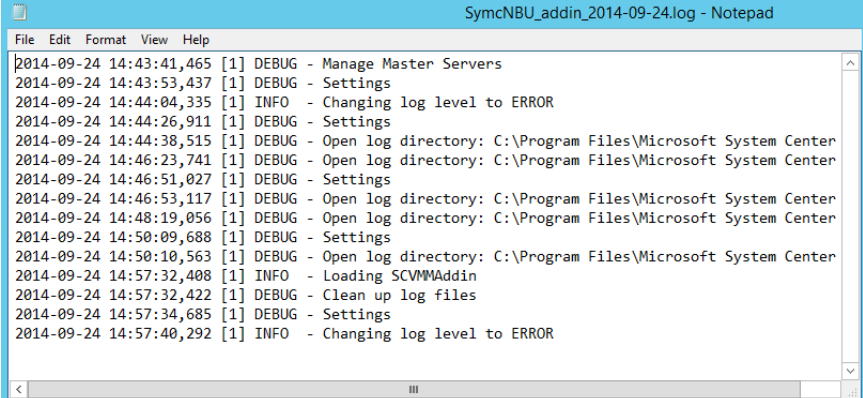


次のようなログファイルが表示されます。



メモ: ログは NetBackup アドインをインストールしたディレクトリに書き込まれます。

- 6 ログファイルをダブルクリックします。
次のようなログファイルが開きます。



```

SymcNBU_addin_2014-09-24.log - Notepad
File Edit Format View Help
2014-09-24 14:43:41,465 [1] DEBUG - Manage Master Servers
2014-09-24 14:43:53,437 [1] DEBUG - Settings
2014-09-24 14:44:04,335 [1] INFO - Changing log level to ERROR
2014-09-24 14:44:26,911 [1] DEBUG - Settings
2014-09-24 14:44:38,515 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:46:23,741 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:46:51,027 [1] DEBUG - Settings
2014-09-24 14:46:53,117 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:48:19,056 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:50:09,688 [1] DEBUG - Settings
2014-09-24 14:50:10,563 [1] DEBUG - Open log directory: C:\Program Files\Microsoft System Center
2014-09-24 14:57:32,408 [1] INFO - Loading SCVMMAddin
2014-09-24 14:57:32,422 [1] DEBUG - Clean up log files
2014-09-24 14:57:34,685 [1] DEBUG - Settings
2014-09-24 14:57:40,292 [1] INFO - Changing log level to ERROR

```

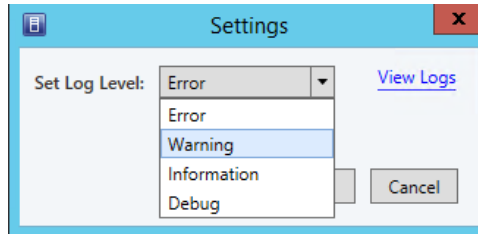
- 7 終了したら、[ログ (Logs)] ウィンドウを閉じ、[キャンセル (Cancel)] をクリックします。

SCVMM 対応 NetBackup アドインのログレベルの変更

ログレベルを変更する方法

- 1 SCVMM コンソールで、[VM とサービス (VMs and Services)] ワークスペースを開きます。
- 2 [すべてのホスト (All Hosts)] をクリックします。
- 3 SCVMM コンソールリボンの [NetBackup] オプションをクリックします。
- 4 [設定] をクリックします。

- 5 [ログレベルの設定 (Set Log Level)]を使って、別のレベルを選択します。



デフォルトでは、ログは最小詳細レベル (エラーレベル) に設定されます。利用可能なレベルは次のとおりです。

エラー	デフォルトレベル。
警告 (Warning)	エラーメッセージを含みます。
情報	警告およびエラーメッセージを含みます。
= デバッグ	情報、警告、およびエラーメッセージを含みます。最高詳細レベルです。

- 6 [保存 (Save)]をクリックします。

SCVMM の NetBackup アドインのリカバリウィザードによるリカバリ前検査で VM に関する古い情報が返される

リカバリウィザードの[設定の確認 (Review Settings)]画面の[リカバリ (Recover)]をクリックすると、選択内容とリカバリ対象を検証するためのリカバリ前検査がウィザードで実行されます。ただし、SCVMM ではなく、Hyper-V マネージャを介して最近 VM に変更が加えられた場合は、リカバリ前検査で、その VM に関する古い情報が提供される場合があります。個別の Hyper-V ホストまたはクラスターで Hyper-V マネージャを通して適用された変更が SCVMM に反映されるまで、最大で 24 時間かかる場合があります。この遅延は、Microsoft SCVMM の更新サイクルが原因で、NetBackup アドインはこれを制御しません。

たとえば、VM が Hyper-V マネージャを通して最近削除された場合は、この削除が SCVMM にまだ反映されていない可能性があります。この場合は、アドインのリカバリ前検査で、VM がまだ残っている状態がレポートされます。次のメッセージが表示されます。

NetBackup アドインリカバリウィザードの[次へ (Next)]ボタンが、必要な入力が入力されなくても有効になる

```
A virtual machine with the same identity exists on <host> and the
overwrite option was not selected. Please review restore options and
select overwrite to continue.
```

VM をリカバリするには、ウィザードの[リストアオプション (Restore Options)]画面に戻り、[既存の仮想マシンの上書き (Overwrite existing virtual machine)]を選択してリカバリを再実行します。

メモ: Microsoft 社は、SCVMM 環境では、VM 設定の変更を (個別のホストまたはクラスターの Hyper-V マネージャからではなく) SCVMM を通して行うことを推奨しています。SCVMM コンソールから行われた変更は、SCVMM ですぐに反映されます。この方法では、アドインのリカバリ前検査に VM の現在の状態が反映されます。

NetBackup アドインリカバリウィザードの[次へ (Next)]ボタンが、必要な入力が入力されなくても有効になる

SCVMM 用 NetBackup アドインのリカバリウィザードでは、[次へ (Next)]ボタンは必要な入力が入力されなくても有効になります。次のような場合、SCVMM 用 NetBackup アドインのリカバリウィザードは、完了前に[次へ (Next)]ボタンを有効にします。

- アドインの[マスターサーバーの管理 (Manage Master Servers)]画面で、無効なプライマリサーバー用に認証トークンが追加されました。例: トークンは既存のプライマリサーバー用に生成されましたが、[マスターサーバーの管理 (Manage Master Servers)]画面でサーバー名が不正確に入力されました。
- 第 2 プライマリサーバーとその認証トークンが追加され、プライマリサーバー名が正しく入力されました。

ウィザードの[仮想マシンの選択 (Virtual Machine Selection)]画面で第 2 プライマリサーバーを選択するときに、VM 識別子を選択しないで[次へ (Next)]をクリックできます。このウィザードでは各画面の入力を完了しないで画面から画面に進むことができます。必要な入力をしないで続行した場合には、ウィザードの最後の画面の[リカバリ (Recovery)]ボタンは灰色になります。

メモ: ウィザードの[次へ (Next)]ボタンは各画面の入力が完了するまで灰色のままになります。リストアを実行するには、ウィザードを戻って必要な入力を行います。無効なプライマリサーバーも削除してください。

NetBackup アドインリカバリウィザードで、VM を上書きするよう求められず、リカバリが失敗する

Microsoft SCVMM コンソール用 NetBackup アドインが、次の状況で VM のリカバリを完了しません。

- アドインリカバリウィザードの[仮想マシンの選択 (Virtual Machine Selection)]画面で、VM がその表示名ではなく、GUID またはホスト名で識別される。
- ウィザードの[リストアオプション (Restore Options)]画面で、[既存の仮想マシンの上書き (Overwrite existing virtual machine)]オプションが選択されていない。
- リカバリ先に同じ VM が存在する。

[リカバリ (Recover)]をクリックしたときに、ウィザードは、リカバリ先の VM を検出し、次に上書きオプションを選択するようにメッセージを表示するはずですが、プロンプトが表示されず、リカバリジョブを開始しても状態 2821 で失敗します。

VM をリカバリするために、[リストアオプション (Restore Options)]画面で[既存の仮想マシンの上書き (Overwrite existing virtual machine)]を選択してリカバリを再実行します。

NetBackup Add-in for SCVMM におけるプライマリサーバーの通信エラーのトラブルシューティング

VM をリカバリするには、アドインに、有効で正しい認証トークンを持つ登録済みの NetBackup プライマリサーバーが設定されている必要があります。NetBackup 管理者は、特定の SCVMM コンソールホストの特定の NetBackup プライマリサーバーで認証トークンを生成します。このトークンにより、トークンが生成された NetBackup プライマリサーバーに SCVMM コンソールホストがアクセスできるようになります(注意: アドインのリカバリポータル[マスターサーバーの管理 (Manage Master Servers)]オプションを使用して、現在登録されているプライマリサーバーの認証トークンを検証できます)。

SCVMM コンソールホストの TCP/IP アドレスまたはホスト名が認証トークンの情報と厳密に一致しない場合、マスターサーバーの管理操作および VM のリカバリ操作は失敗します。次のようなエラーメッセージが表示されます。

```
Unable to connect the Netbackup Master Server. Do you want to add
this master server?
```

```
Authentication failed. Please verify that the master server token is
valid and correct using the 'Manage Master Servers' dialog box
```

問題と訂正処理を正しく判断するには、VxUL ログファイルを確認する必要があります。プライマリサーバーで、次のコマンドを入力します。

```
vxlogview -i nbweb service -p nb -L -E
```

エラーの例 1

ログファイルには、次のようなメッセージが含まれています。

```
02/17/2017 10:03:37.831 [Error] Remote host name does not match the  
  
name in the certificate, remote name:scvmm02.domain.com, name from  
certificate:scvmm02
```

上に示すログの一部で、トークン内の名前は scvmm02、必要な名前は scvmm02.domain.com です。

Cohesity ベリタスでは、既存のトークンを取り消し、必要な名前と新しいトークンを生成して、SCVMM コンソールホストでその新しいトークンを使用することをお勧めします。これを実行できない場合、次のように、既存のトークンのエイリアスとして SCVMM コンソールホストの完全修飾ドメイン名を追加します。

```
manageClientCerts -addAlias scvmm02 -HOST scvmm02.domain.com
```

代わりに、-ANY オプションを使用できます。

```
manageClientCerts -addAlias scvmm02 -ANY
```

-ANY では、任意のホストまたは任意の IP アドレスが、このトークンを使用して NetBackup サーバーと通信できるようになります。

注意: -ANY オプションは、安全なリストア方法ではありません。manageClientCerts コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

エラーの例 2

ログファイルには、次のようなメッセージが含まれています。

```
02/17/2017 16:18:13.951 [Error] Remote host name does not match the  
  
name in the certificate, remote name:10.10.10.11, name from  
certificate:scvmm02
```

上に示すログの一部で、トークン内の名前は scvmm02、必要な名前は 10.10.10.11 です。

Cohesity ベリタスでは、既存のトークンを取り消し、必要な名前と新しいトークンを生成して、SCVMM コンソールホストでその新しいトークンを使用することをお勧めします。これを実行できない場合、次のように、既存のトークンのエイリアスとして SCVMM コンソールホストの TCP/IP アドレスを追加します。

```
manageClientCerts -addAlias scvmm02 -IP 10.10.10.11
```

代わりに、-ANY オプションを使用できます。

```
manageClientCerts -addAlias scvmm02 -ANY
```

-ANY では、任意のホストまたは任意の IP アドレスが、このトークンを使用して NetBackup サーバーと通信できるようになります。

注意: -ANY オプションは、安全なリストア方法ではありません。

詳細情報が利用可能です。

p.28 の「[認証トークンのホスト名または IP アドレスの追加または追加したホスト名または IP アドレスの削除](#)」を参照してください。

『NetBackup コマンドリファレンスガイド』で manageClientCerts コマンドを参照してください。