

ActiveImage Protector 2022 Cloud

セットアップガイド

第3版 2024年2月



目次

1.	はじめに	3
	システム要件.....	3
2.	インストール	5
3.	バックアップの設定と実行.....	6
3-1.	ボリューム バックアップ：ワンタイム.....	6
3-2.	ボリューム バックアップ：スケジュール	12
4.	リストア	21
4-1.	ファイル/フォルダー単位のリストア.....	21
4-2.	システムリカバリー（In-Cloud Recovery）	26
4-3.	システムリカバリー（RescueBoot）	34
5.	仮想スタンバイマシンの作成（In-Cloud Standby）	45
5-1.	バックアップからスナップショットの作成.....	45
5-2.	スナップショットからボリューム作成とアタッチ	53
6.	リモート管理コンソール.....	62
7.	参考情報	67

1. はじめに

ActiveImage Protector は、物理・仮想・クラウドといった多様なシステム環境に対応したシステム・データ保護ソリューションです。このセットアップガイドでは、パブリッククラウド（Amazon Web Services（以下 AWS）、Microsoft Azure（以下 Azure）、Google Cloud Platform（以下 Google Cloud）、Oracle Cloud Infrastructure（以下 Oracle Cloud））向け「ActiveImage Protector 2022 Cloud」の導入から基本的な設定方法などを説明しています。詳細な設定方法や制限事項などについては、以下のオンラインヘルプを参照してください。

- ・ Windows 環境用オンラインヘルプ

https://webhelp.actiphy.com/AIP/2022/ja_JP/

- ・ Linux 環境用オンラインヘルプ

https://webhelp.actiphy.com/AIP/linux/2022/ja_JP/

システム要件

ActiveImage Protector 2022（Windows 用 バージョン 7.0.3.8919、Linux 用 バージョン 7.0.3.8919）のシステム要件は下記のとおりです。インストール先のコンピューターが、以下のシステム要件を満たしていることをご確認ください。なお、最新のシステム要件は、Web サイトのシステム要件ページ（<https://www.actiphy.com/ja-jp/support/system-requirements/>）よりご確認ください。

Windows 仮想マシン	
CPU	Pentium 4 または同等以上の CPU
メモリ (RAM)	4GB 以上 (8GB 以上を推奨)
ハードディスク	1.5GB 以上の空き容量が必要
インターネット接続	製品のアクティベーション、ライセンスファイル発行および製品アップデートに必要
サポート対象 OS	・ Windows Server 2022 ・ Windows Server 2019 ・ Windows Server 2016 ・ Windows Server 2012 R2 ・ Windows Server IoT 2019 / 2022 for Storage ・ Windows Storage Server 2016 ・ Windows Storage Server 2012 R2

Linux 仮想マシン	
CPU	Pentium 4、または同等以上の CPU ※ x86_64 アーキテクチャのみサポートします。 ※ セキュアブートには対応していません。
メモリ (RAM)	2GB 以上
ハードディスク	2GB の空き容量が必要
インターネット接続	製品のアクティベーションに必要
サポート対象 OS	• Red Hat Enterprise Linux : 9.0 – 9.3 / 8.0 – 8.9 / 7.0 – 7.9 • CentOS : 8.1 – 8.4 / 7.0 – 7.9 • Oracle Linux : 9.0 – 9.3 / 8.1 – 8.9 / 7.0 – 7.9 • AlmaLinux 9.0 – 9.3 / 8.3 – 8.9 • MIRACLE LINUX 9.0, 9.2 / 8.4, 8.6, 8.8 • Rocky Linux 9.0 – 9.3 / 8.3 – 8.9 • Amazon Linux 2 • SUSE Linux Enterprise Server 15 / Desktop 15 • OpenSUSE Leap 15 • Ubuntu 18.04LTS / 20.04LTS / 22.04LTS • Debian 9 – 12

2. インストール

ActiveImage Protector Cloud は、パブリッククラウド (AWS、Azure、Google Cloud、Oracle Cloud) の Windows、および Linux 仮想マシンのバックアップ運用を行うことができます。クラウドの仮想マシンへの ActiveImage Protector の導入や基本的な設定方法については、以下のセットアップガイドを参照してください。

※クラウドの仮想マシンへの ActiveImage Protector のインストールの際には、「クラウド用のプロダクトキー」を使用してください。

- ・ Windows 環境：ActiveImage Protector 2022 Server セットアップガイド

https://www.actiphys.com/ja-jp/setup_guide/actiphys_activeimage_protector_2022_server

- ・ Linux 環境：ActiveImage Protector 2022 Linux セットアップガイド

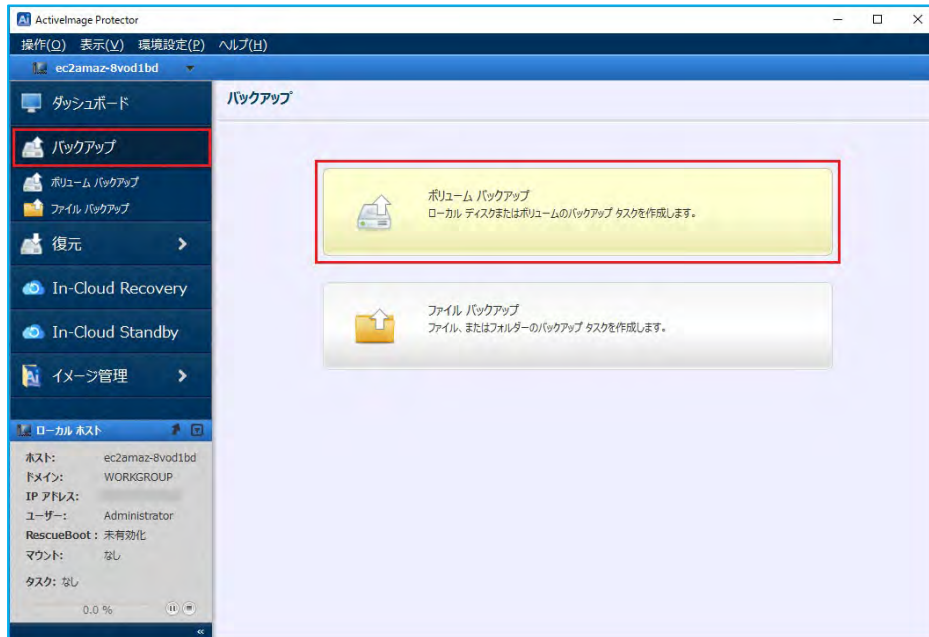
https://www.actiphys.com/ja-jp/setup_guide/actiphys_activeimage_protector_2022_linux

3. バックアップの設定と実行

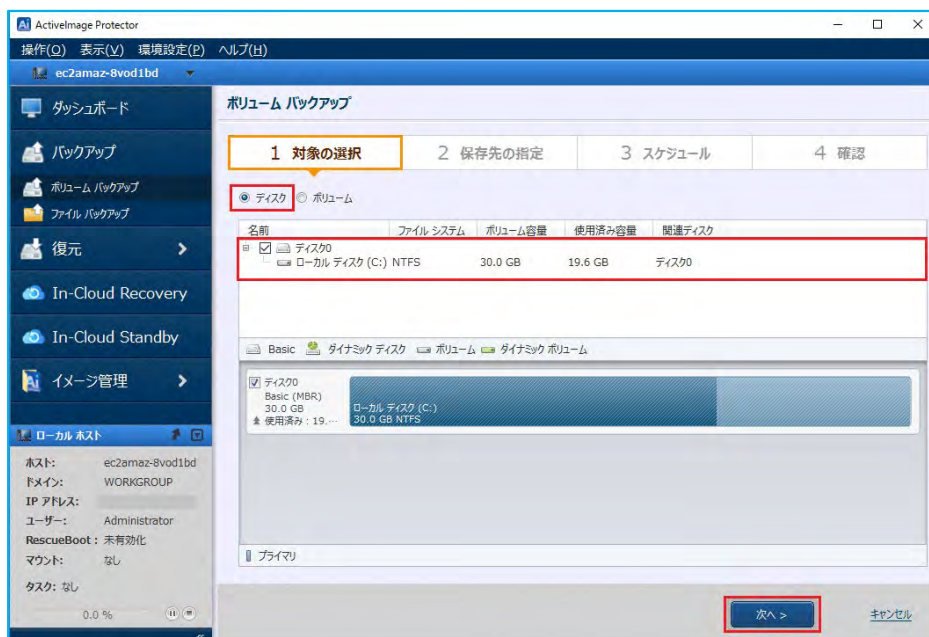
3-1. ボリューム バックアップ：ワンタイム

今すぐバックアップを実行する、ワンタイム バックアップの手順について説明します。

1. Windows スタートメニューから [Actiphy] → [ActiveImage Protector] をクリックして ActiveImage Protector のコンソールを起動します。ActiveImage Protector のコンソールのメニュータブから [バックアップ] → [ボリューム バックアップ] をクリックします。

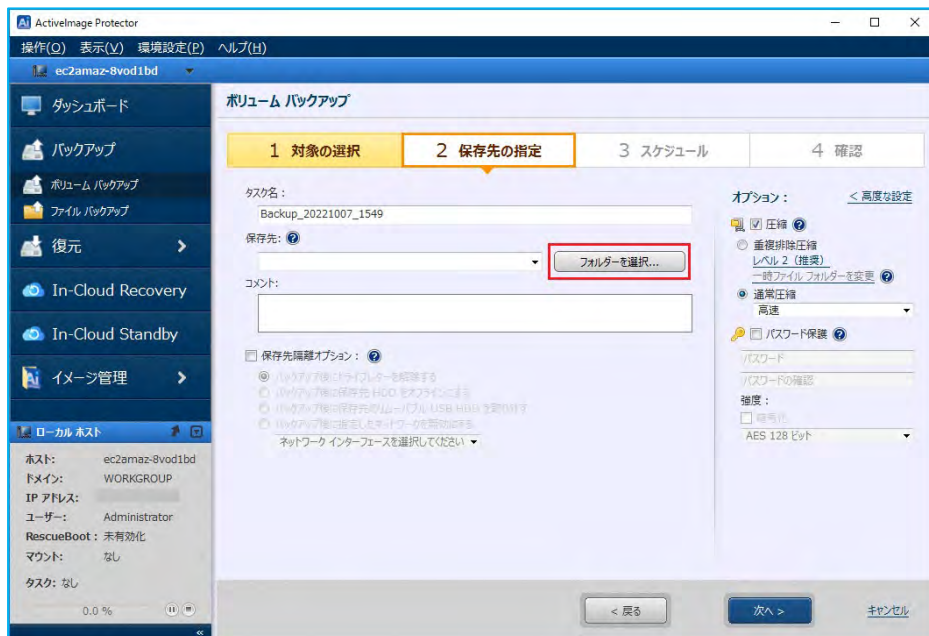


2. バックアップ対象を選択します。ここでの設定例として、バックアップ対象は [ディスク] を選択し、[ディスク 0] にチェックを入れます。バックアップ対象の選択が完了したら、[次へ] をクリックします。

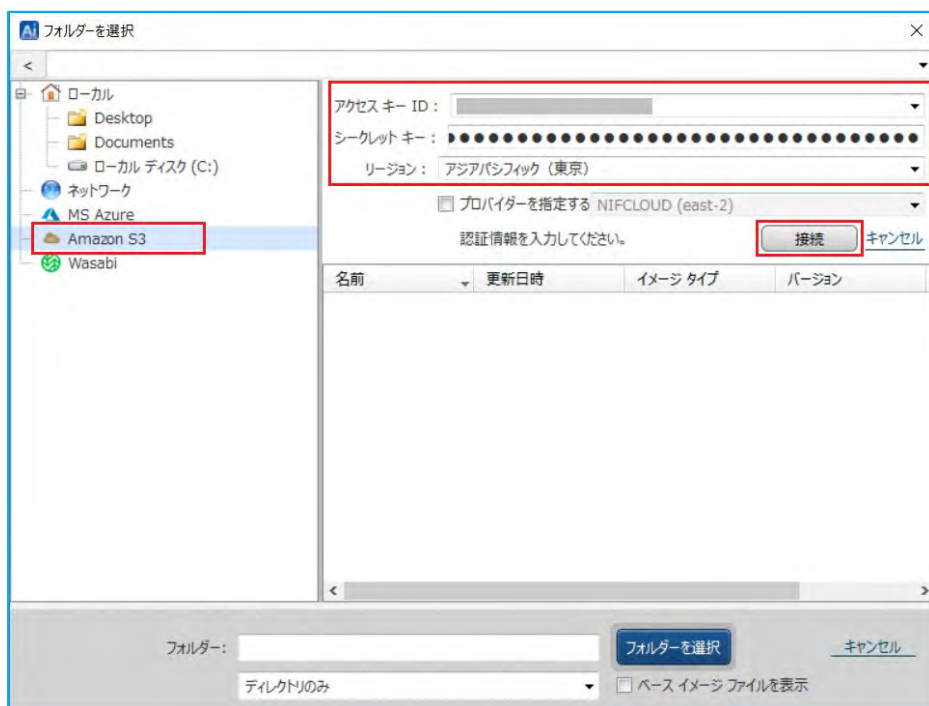


バックアップの設定と実行

3. バックアップの保存先を指定します。バックアップの保存先として、ローカルディスク、クラウド内のネットワーク共有フォルダー、クラウドストレージ（Azure Storage、Amazon S3、Wasabi）など、システム構成や目的に合わせて保存場所を設定することができます。ここでの設定例として、バックアップ保存先として、クラウドストレージ「Amazon S3」を保存先として説明します。最初に、[フォルダーを選択] をクリックします。

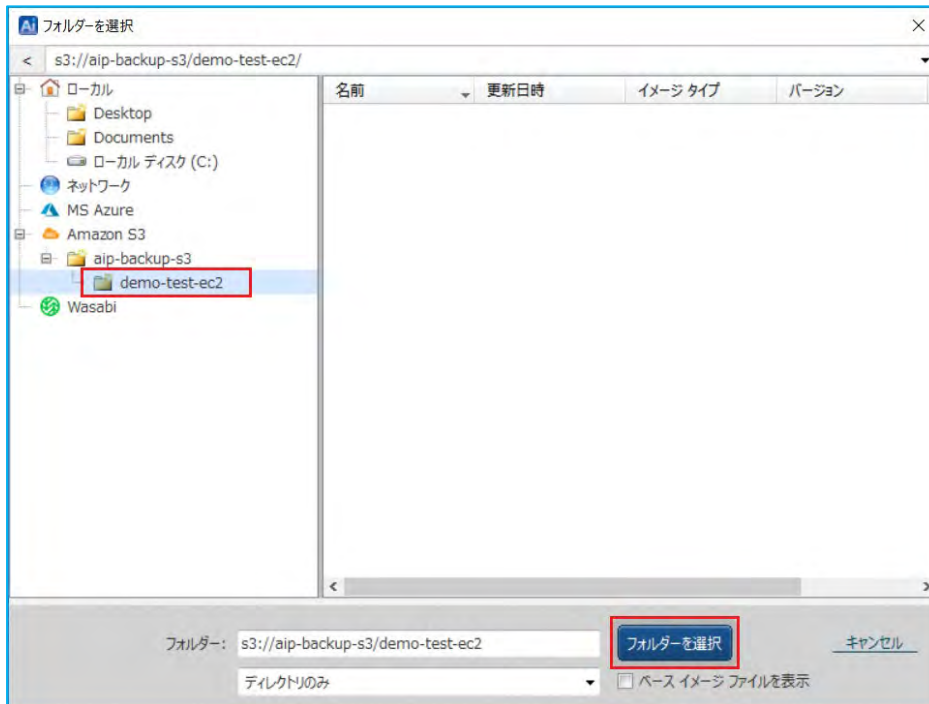


4. [フォルダー選択] から [Amazon S3] をクリックします。次に、保存先の Amazon S3 に対する認証情報を入力します。AWS の [アクセス ID:]、[シークレットキー:] を入力し、[リージョン:] を選択して [接続] をクリックします。

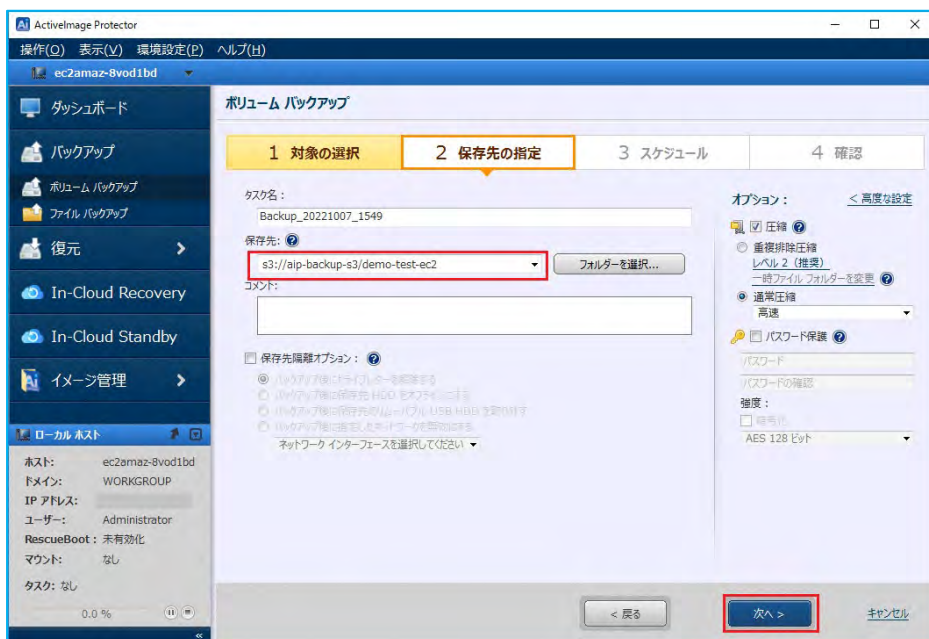


バックアップの設定と実行

5. Amazon S3 への接続が成功するとバケットが表示されます。ここでの設定例として、Amazon S3 にあらかじめ作成したバケット「aip-backup-s3」内のフォルダー「demo-test-ec2」を選択し、[フォルダーを選択]をクリックします。



6. [保存先:] に、選択した Amazon S3 のフォルダーが登録されていることを確認後に、[次へ] をクリックします。[保存先隔離オプション:]、[オプション] は必要に応じて設定します。[オプション] の設定については、「3-2.ボリューム バックアップ: スケジュール (P.12)」の項で説明していますので、そちらを参照してください。



バックアップの設定と実行

7. [スケジュールの設定] では、[タスク タイプ:] に [ワンタイム バックアップ] を選択し、[OK] をクリックします。

スケジュールの設定

Backup_20221007_1549 有効化日時: 2022/10/07 16:02 ~ 2023/10/07 16:02 ☒ 期限なし

タスク タイプ: ☒ ワンタイム バックアップ ☐ スケジュール バックアップ

ベース ☒ 月単位 ☒ 週単位

増分 ☒ 週単位

日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日

開始時刻: 02:00 終了時刻: 21:00 実行間隔: 60 分ごと

実行時間: 16:02

新規トリガーを追加 (ベース) 新規トリガーを追加 (増分)

イベント バックアップ: ☐ システムのシャットダウン/再起動 ベースと増分

オプション: ☐ スキップされたスケジュール タスクを自動的に実行する ☐ ベース バックアップがスキップされていた場合、優先して実行する

OK キャンセル

8. ここでは、このまま [次へ] をクリックします。

ActiveImage Protector

操作(O) 表示(V) 環境設定(E) ヘルプ(H)

ec2amaz-8vod1bd

ダッシュボード バックアップ ボリューム バックアップ ファイル バックアップ 復元 In-Cloud Recovery In-Cloud Standby イメージ管理 ローカル ホスト

ホスト: ec2amaz-8vod1bd
ドメイン: WORKGROUP
IP アドレス:
ユーザー: Administrator
RescueBoot: 未有効化
マウント: なし
タスク: なし

ボリューム バックアップ

1 対象の選択 2 保存先の指定 3 スケジュール 4 確認

タスク タイプ: ワンタイム バックアップ
有効化日時: 2022/10/07 16:02
ベース:
増分:

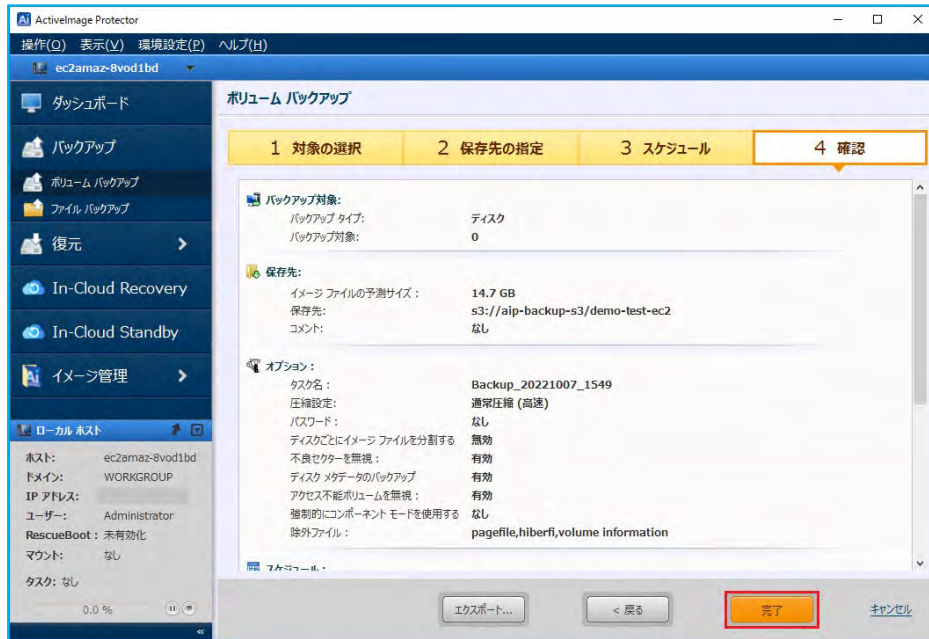
スケジュールを編集

オプション: ☐ 保持対象外となった世代のイメージ ファイルを全て削除 ☐ 保持するバックアップ イメージの世代数: 3 ☐ 新世代作成時には旧世代を削除する ☐ Eメール通知を行う タスク失敗時

タスクの優先順位 ☐ フル(ベース): 最低 低 中 高
増分: 最低 低 中 高

< 戻る 次へ > キャンセル

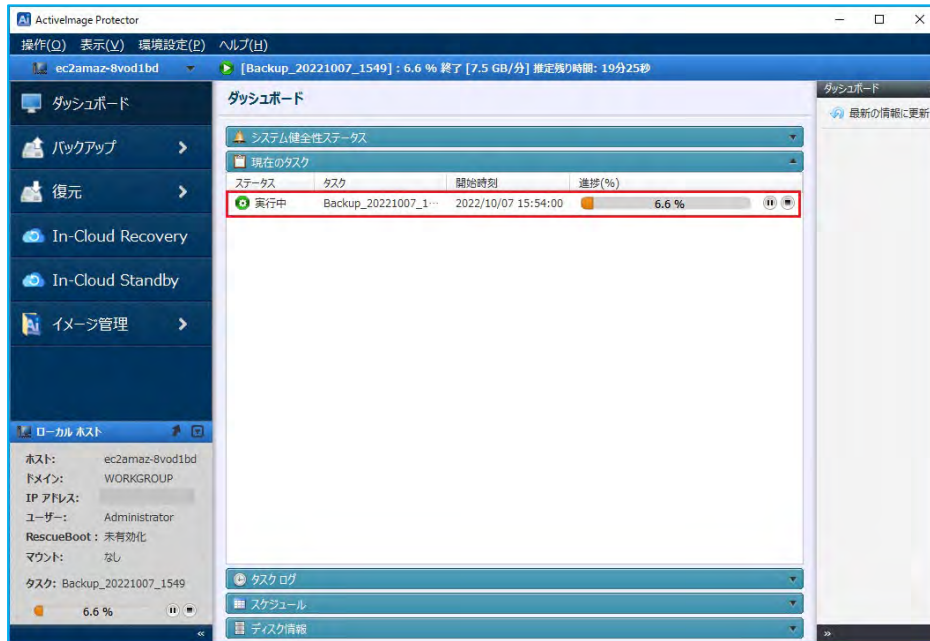
9. バックアップの内容を確認してから、[完了] をクリックします。



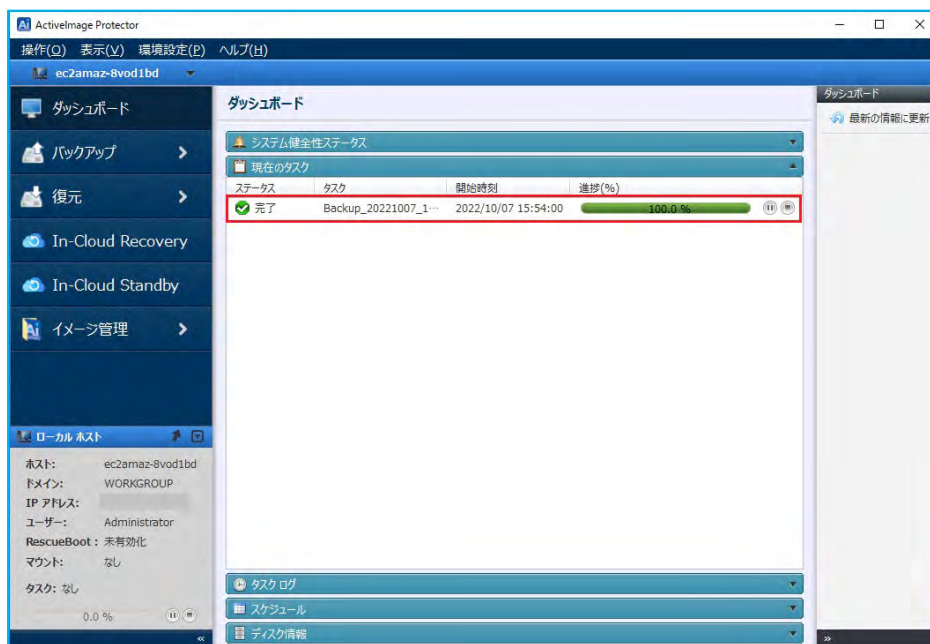
10. [直ちに実行] を選択し、[OK] をクリックするとバックアップが開始されます。
[タスク終了後の追加処理] は、バックアップ完了後にシステムのシャットダウンや再起動が必要な場合に設定します。



11. バックアップが開始されると、タスクの進捗状況が表示されます。



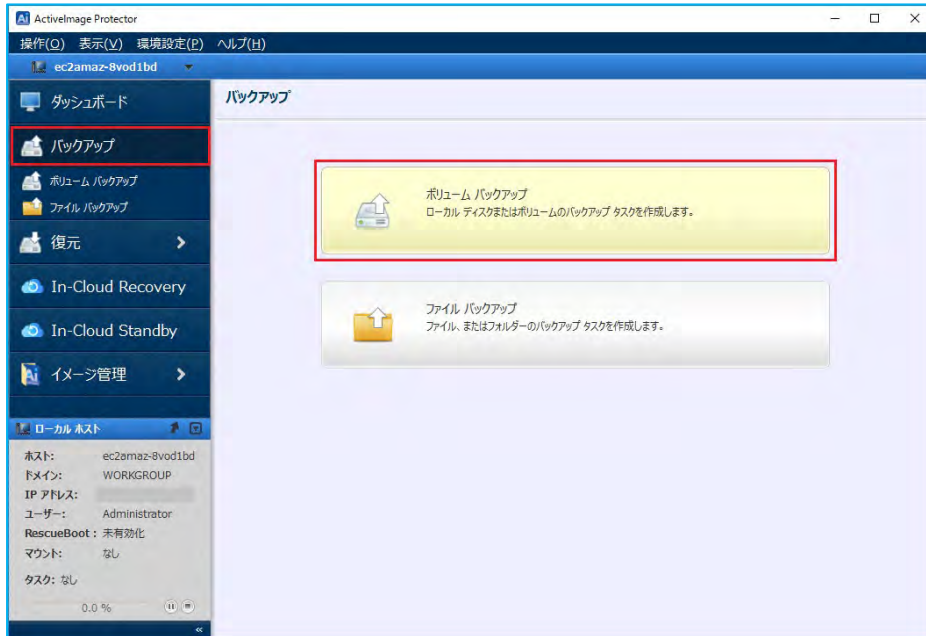
12. 進捗が100%になるとバックアップは完了です。



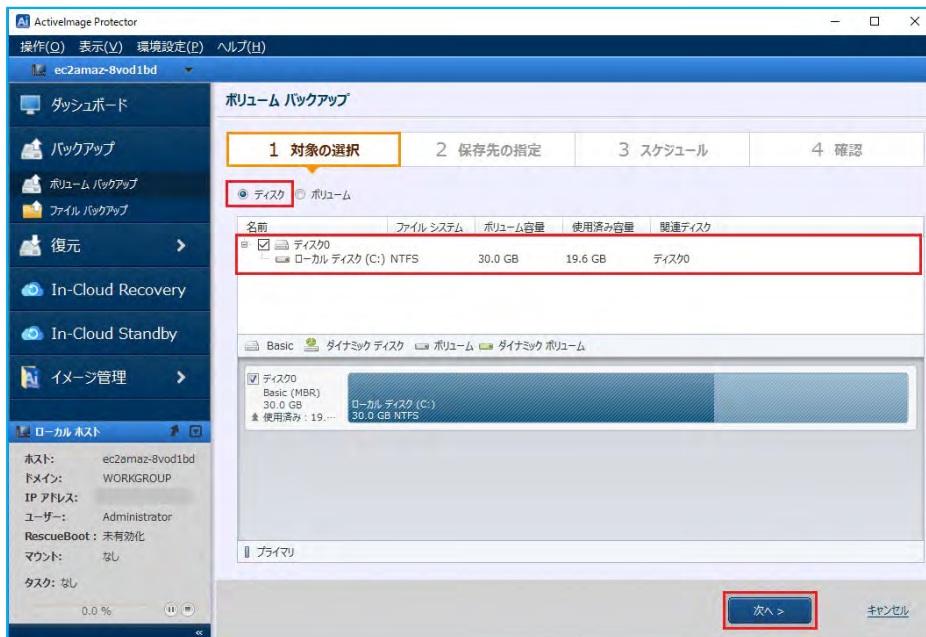
3-2. ボリューム バックアップ：スケジュール

定期的にバックアップを実行する、スケジュール バックアップの設定手順について説明します。

1. Windows スタートメニューから [Actiphy] → [ActiveImage Protector] をクリックして ActiveImage Protector のコンソールを起動します。ActiveImage Protector のコンソールのメニュータブから [バックアップ] → [ボリューム バックアップ] をクリックします。

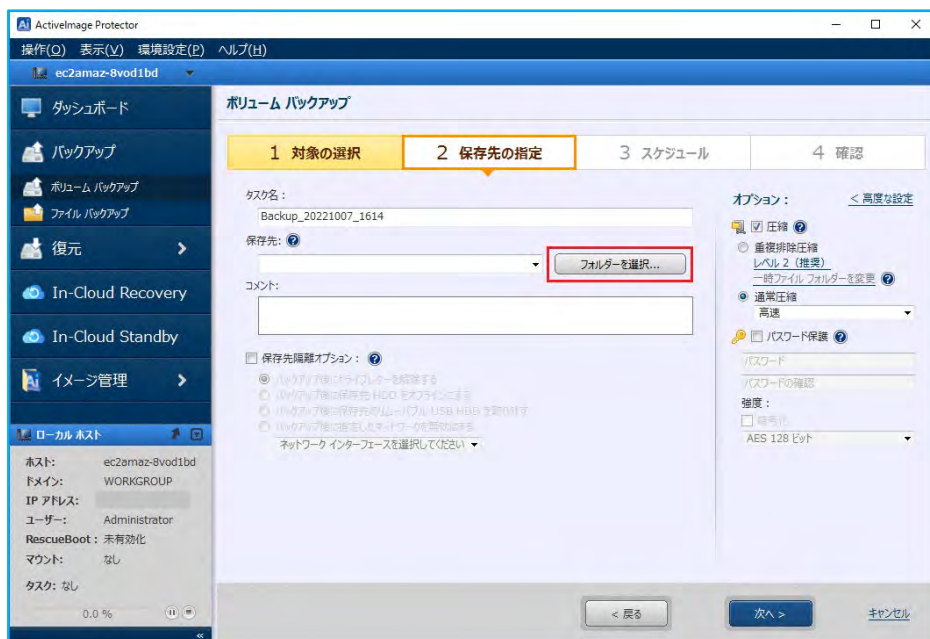


2. バックアップ対象を選択します。ここでの設定例として、バックアップ対象は [ディスク] を選択し、[ディスク 0] にチェックを入れます。バックアップ対象の選択が完了したら、[次へ] をクリックします。

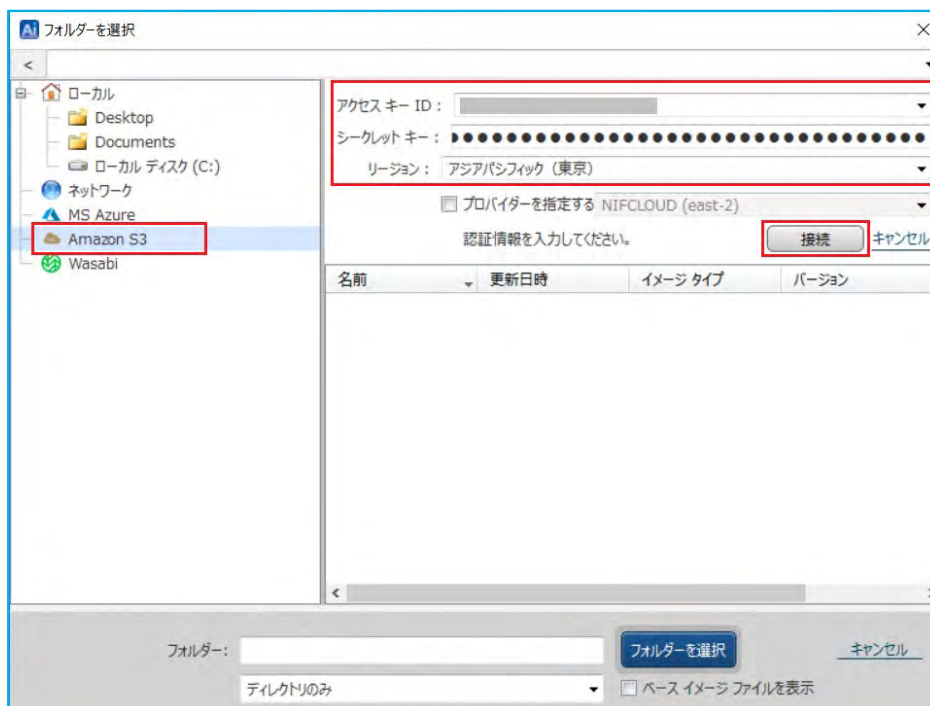


バックアップの設定と実行

3. バックアップの保存先を指定します。ここでの設定例として、クラウドストレージ「Amazon S3」を保存先として説明します。テキストボックスの右にある [▼] をクリックすると、これまでのバックアップ プロセスやバックアップで使用した保存先が表示されますので、ここから選択もできます。新規にバックアップ保存先を登録する場合は、[フォルダーを選択...] をクリックします。

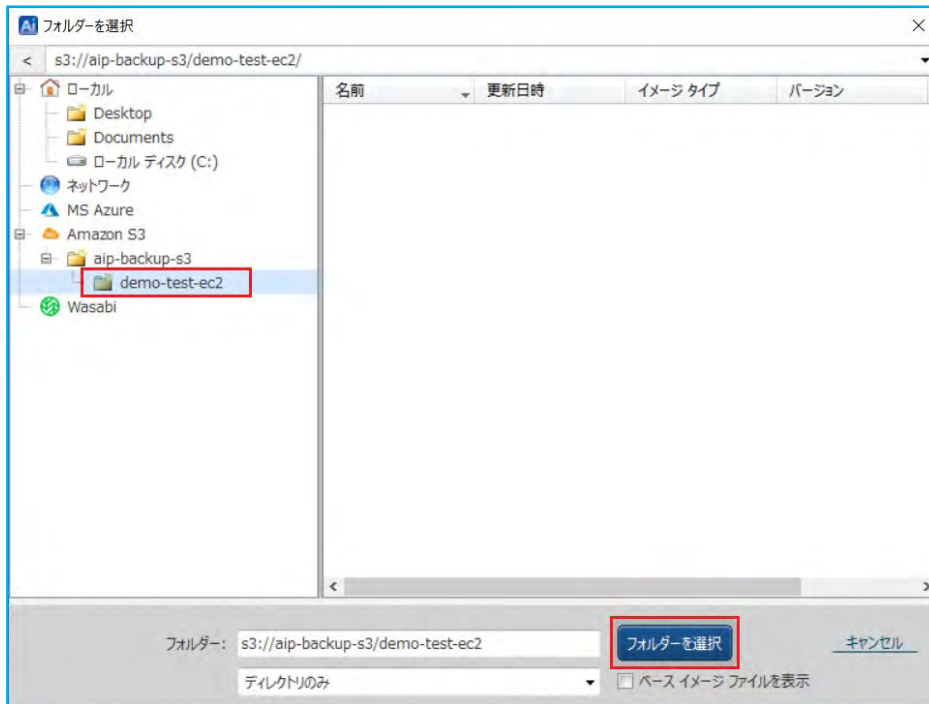


4. [フォルダーを選択] では、[Amazon S3] をクリックします。次に、保存先の Amazon S3 に対する認証情報を入力します。AWS の [アクセス ID:]、[シークレットキー:] を入力し、[リージョン:] を選択して [接続] をクリックします。

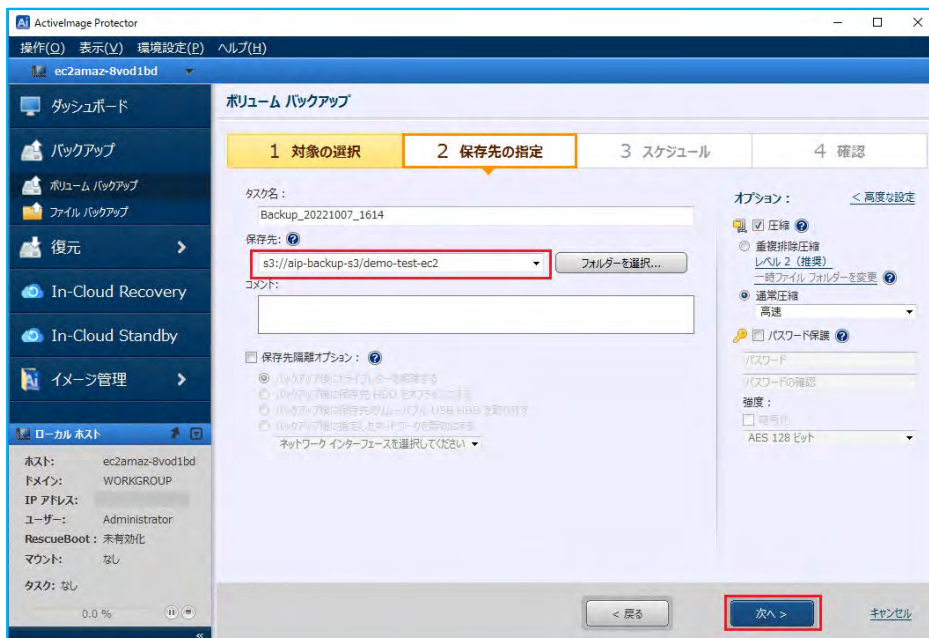


バックアップの設定と実行

- Amazon S3 への接続が成功するとバケットが表示されます。ここでの設定例として、Amazon S3 にあらかじめ作成したバケット「aip-backup-s3」内のフォルダー「demo-test-ec2」を選択し、[フォルダーを選択]をクリックします。



- [保存先:] に、選択した Amazon S3 のフォルダーが登録されていることを確認後に、[次へ] をクリックします。「オプション」の設定は次項で説明します。



バックアップの設定と実行

7. バックアップのスケジュール設定を行います。

ActiveImage Protector は、「月単位」、「週単位」、「指定曜日」、「指定日時」など柔軟なバックアップのスケジュール設定を行うことができます。ここでの設定例として、[タスクタイプ:] に「スケジュール バックアップ」を選択します。次に、ベースバックアップ（フルバックアップ）は「週単位」を選択して日曜日の午前 1 時に実行、増分バックアップは、月曜日から土曜日の午前 1 時に実行するスケジュール設定を行います。スケジュールの設定が完了したら、[OK] をクリックします。

スケジュールの設定

Backup_20221007_1614 有効化日時: 2022/10/07 16:27 ~ 2023/10/07 16:27 期限なし

タスクタイプ: ☐ フォンタイム バックアップ ☒ スケジュール バックアップ

ベース

☒ 週単位

日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日

実行時間: 01:00

増分

☒ 週単位

日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日

☒ 一定間隔で複数回実行

開始時刻: 01:00 終了時刻: 01:00 実行間隔: 60 分ごと

☒ 一回のみ実行: 01:00

新規トリガーを追加 (ベース) 新規トリガーを追加 (増分)

イベント バックアップ:
☐ システムのシャットダウン/再起動 ベースと増分

オプション:
☐ スキップされたスケジュール タスクを自動的に実行する
☐ タスクのバックアップがスキップされている場合は、実行して実行する

OK キャンセル

8. マルチスケジュール設定例: [新規トリガーを追加] をクリックすると、スケジュール設定を追加することができます。週単位のスケジュール設定に加え、例えば、月末にフルバックアップを行うといった設定も可能です。

スケジュールの設定

Backup_20221007_1614 有効化日時: 2022/10/07 17:26 ~ 2023/10/11 17:26 期限なし

タスクタイプ: ☐ フォンタイム バックアップ ☒ スケジュール バックアップ

ベース

☒ 月単位

1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31 月末

実行時間: 00:00

増分

☒ 週単位

日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日

☒ 一定間隔で複数回実行

開始時刻: 01:00 終了時刻: 01:00 実行間隔: 60 分ごと

☒ 一回のみ実行: 01:00

新規トリガーを追加 (ベース) 新規トリガーを追加 (増分)

イベント バックアップ:
☐ システムのシャットダウン/再起動 ベースと増分

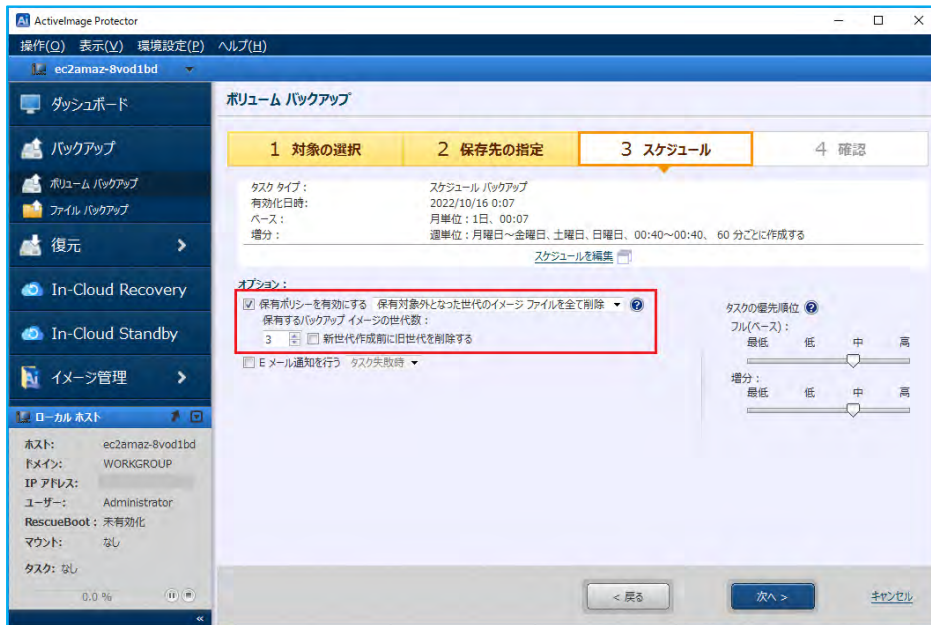
オプション:
☐ スキップされたスケジュール タスクを自動的に実行する
☐ ベース/増分バックアップがスキップされている場合は、実行して実行する

OK キャンセル

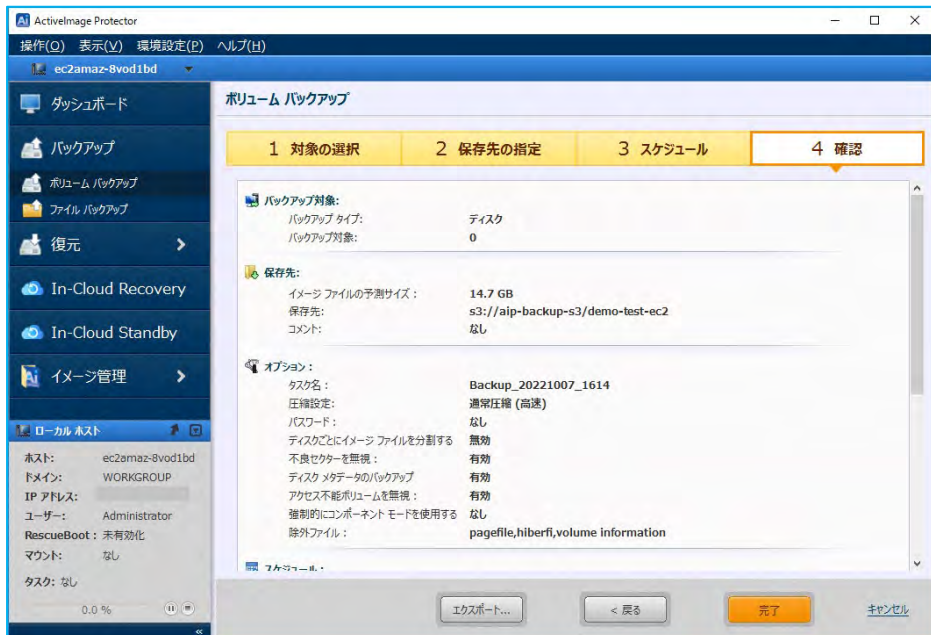
バックアップの設定と実行

9. [スケジュール] タブの [オプション] では、「バックアップ保存先に残すバックアップの世代数」とタスクスケジュール処理の成功や失敗を通知する「E メール通知」の設定ができます。ここでの設定例として、[保有ポリシーを有効にする] にチェックを入れ、[保有するバックアップの世代数:] をデフォルト設定の「3」にします。この設定で、バックアップの保存先に 3 世代分のバックアップが残ります。

※ActiveImage Protector は、ベースバックアップとそれに紐づく増分バックアップを 1 世代として管理しています。

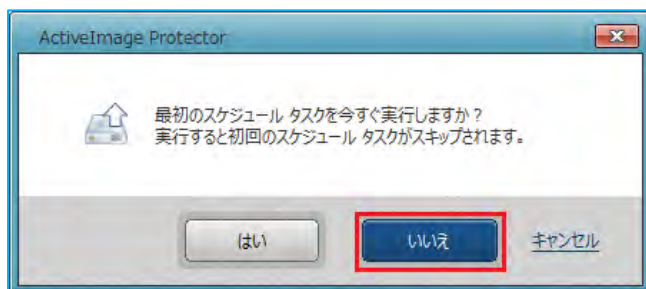


10. バックアップの設定内容が表示されます。内容を確認してから [完了] をクリックします。

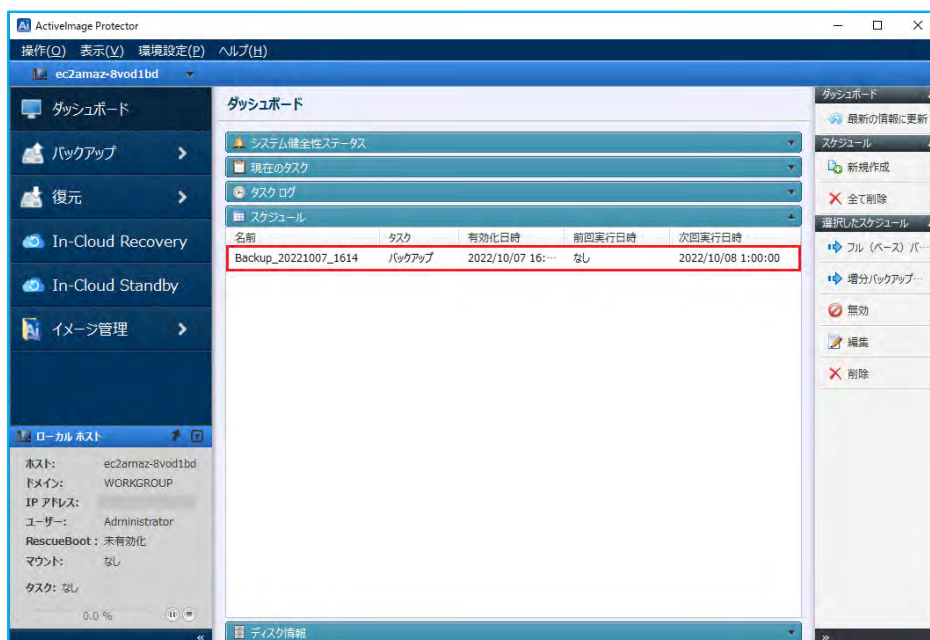


バックアップの設定と実行

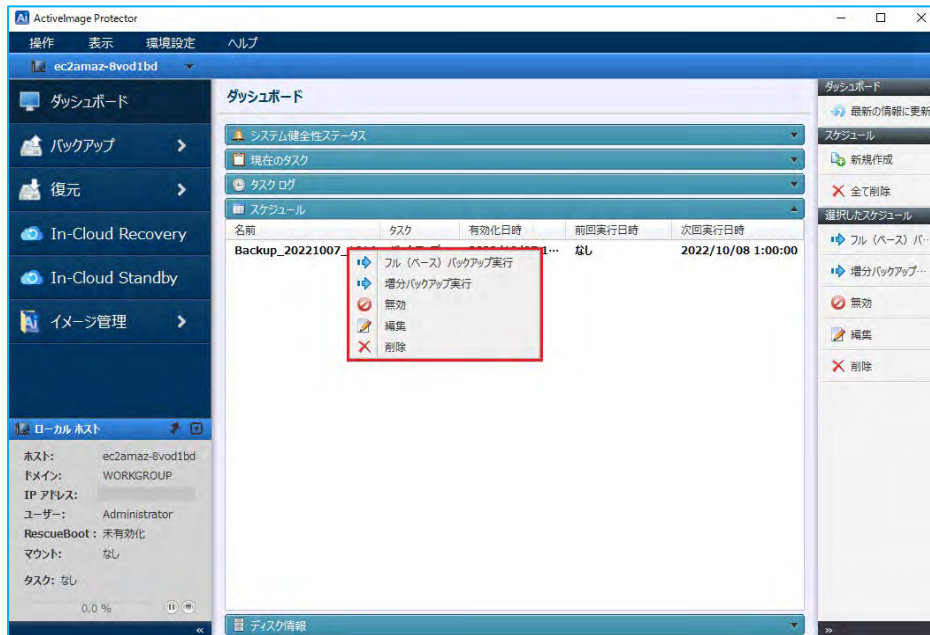
11. ここでは、[いいえ] をクリックして、ダッシュボードに戻ります。[はい] をクリックすると最初のスケジュール タスクが実行されます。



12. 作成済みのスケジュールは、[ダッシュボード] → [スケジュール] から確認できます。指定した時刻になると、スケジュールバックアップが実行されます。



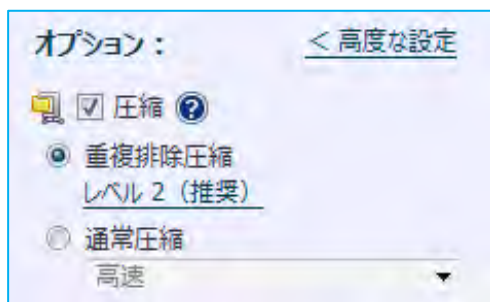
13. [スケジュール名] を右クリックすると、直ちにフルバックアップや増分バックアップの実行、スケジュールの編集などを行うことができます。



14. [オプション] や [高度な設定] は、必要に応じて設定します。ここでは、設定例について説明します。

(1) オプション：圧縮レベルの設定

標準設定の通常圧縮と重複排除圧縮の2種類の圧縮方式をサポートします。圧縮率は、データの種類により異なりますが、通常圧縮で70%、重複排除圧縮では50%程度を目安としてください。重複排除圧縮を選択すると、その下の「レベル2（推奨）」と重複排除処理の一時作業領域の「一時ファイルフォルダーを変更」の設定が可能になります。



(2) オプション：暗号化の設定

バックアップファイルのパスワード保護と暗号化をサポートしています。まず、[パスワード保護] のチェックボックスにチェックを入れ、パスワードを入力します。次に、暗号化レベルの「RCS」、「AES128 ビット」、「AES256 ビット」から選択して設定します。バックアップファイルの外部サイト保管やサイバー攻撃からバックアップファイルを安全に保護します。

The screenshot shows a settings window with a key icon and a checked box for 'パスワード保護' (Password Protection). Below it are two password input fields, each with 12 dots representing characters. The strength is indicated as '強度: 強' (Strength: Strong). There is a checked box for '暗号化' (Encryption) and a dropdown menu set to 'AES 256 ビット' (AES 256 bits).

(3) オプション：高度な設定

オプション中の[高度な設定]では、バックアップファイルの分割、ネットワーク共有フォルダーに保存する際の帯域制御やキャッシュ使用、バックアップファイルの仮想化処理、In-Cloud Standby 向けの仮想化処理、バックアップ処理と連動したユーザー作成のスクリプトの実行などの設定が可能です。ここでは、[バックアップファイルの仮想化処理]、[In-Cloud Standby 向けの仮想化処理]、[スクリプト]について解説します。

The screenshot shows the '一般設定' (General Settings) tab of an advanced settings window. It contains various checkboxes for disk partitioning, network throttling, cache usage, bad sector handling, MD5 file creation, access error handling, and backup timeouts. At the bottom, under the 'イメージ準備' (Image Preparation) section, two options are highlighted with red boxes: 'バックアップ時にあらかじめ仮想化処理を行う' (Perform virtualization processing in advance during backup) and 'バックアップ時にあらかじめ In-Cloud Standby 向けの仮想化処理を行う' (Perform virtualization processing in advance during backup for In-Cloud Standby). Both are currently unchecked.

・ バックアップファイルの仮想化処理：

エージェントの「仮想化」機能を使わずに、仮想マシンに直接復元する場合は「バックアップ時にあらかじめ仮想化処理を行う」のオプションを有効にしてください。あらかじめ、エージェントの「仮想化」機能と同じ処理（VMware vSphere / Microsoft Hyper-V のドライバー追加、レジストリ変更など）を行った状態でバックアップを作成します。例えば、バックアップ元より小さなサイズの仮想ディスクで構成された仮想マシンに、ボリューム単位での縮小復元やディスクのボリュームレイアウトの変更など、柔軟な復元を行うことができます。

・ In-Cloud Standby 向けの仮想化処理：

あらかじめ In-Cloud Standby でシステムを起動した際に必要な処理（ドライバー追加、設定変更）をした状態でバックアップを作成します。In-Cloud Standby を使用する場合は、このオプションを有効にします。

バックアップの設定と実行

- ・ スクリプトの設定：

指定したスクリプトをスナップショット実行前、実行後、およびバックアップ作成後に実行することができます。使用例として、Microsoft ボリューム・シャドウコピー・サービス (Volume Shadow Copy Service) に対応していないデータベース・アプリケーションの場合は、バックアップデータの整合性を保つために、バックアップ開始前にサービスを停止する必要がありますが、スナップショット実行前後に、サービス停止/起動のスクリプトを設定することができます。サービスの停止時間は、スナップショットを取得する約1分～2分となります。

スクリプト

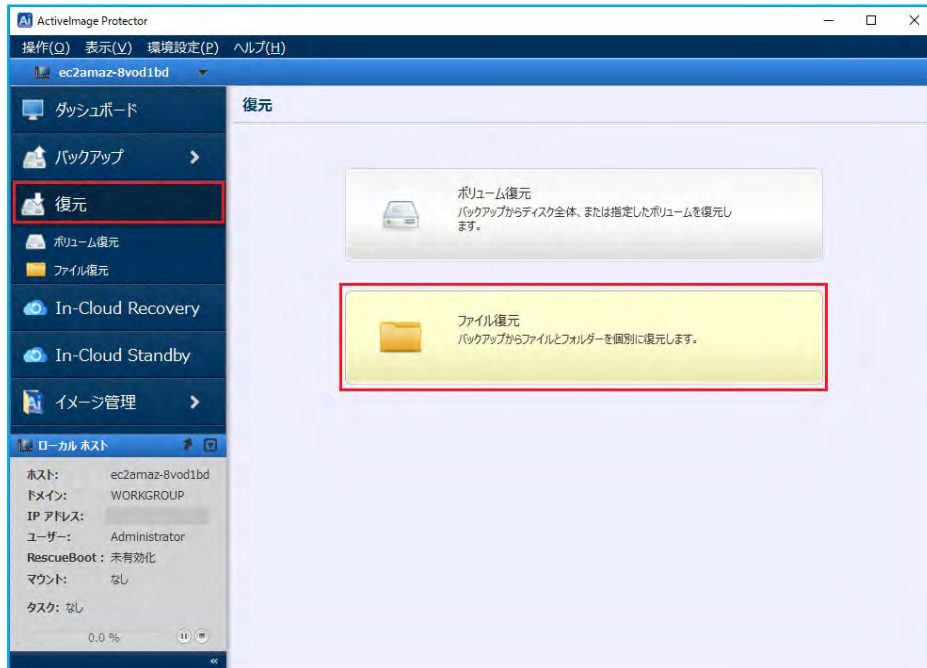
スナップショット実行前に実行するスクリプト：	タイムアウト	実行設定：
C:\tem\DB_shutdown.ps1	30 分	ベースと増分 ▼
スナップショット実行後に実行するスクリプト：		
C:\tem\DB_startup.ps1	30 分	ベースと増分 ▼

4. リストア

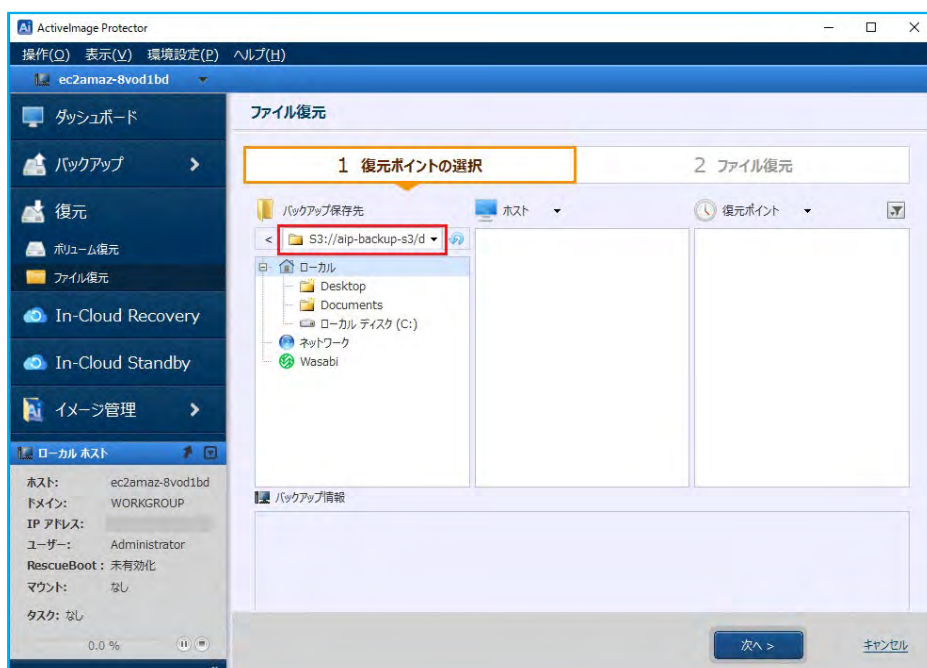
4-1. ファイル/フォルダー単位のリストア

ここでは、バックアップからファイル/フォルダー単位の復元手順について説明します。

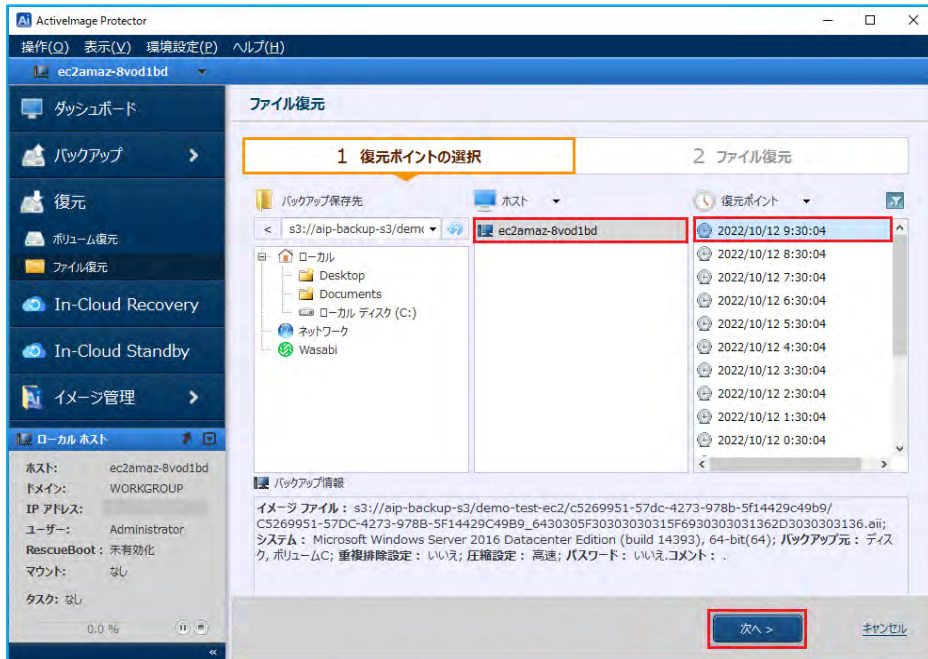
1. ActiImage Protector のコンソールのメニュータブから [復元] → [ファイル復元] をクリックします。



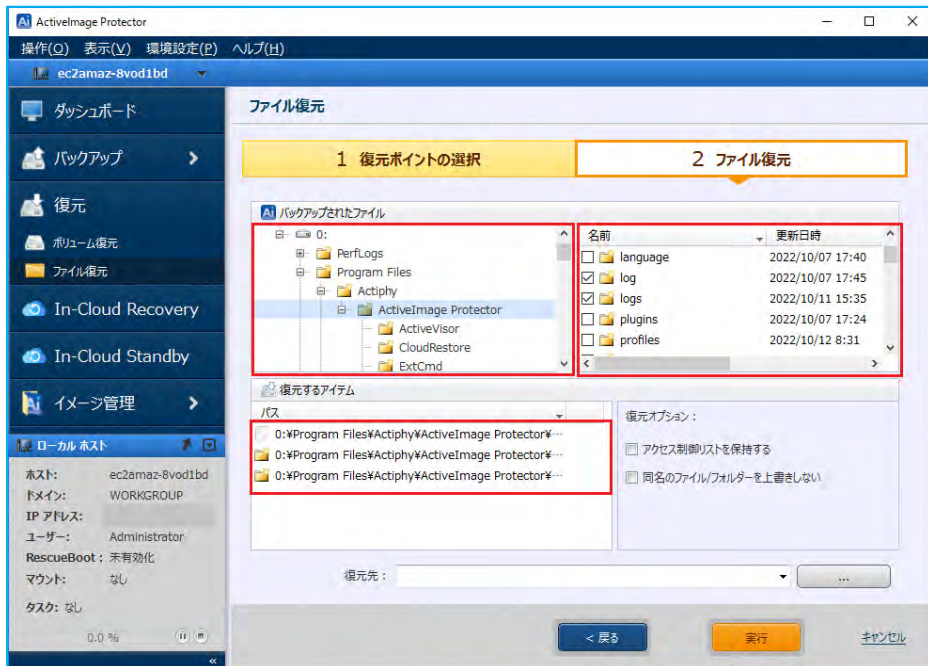
2. [バックアップ保存先] を選択します。ここでの設定例として、下記の場所にバックアップ保存先の Amazon S3 の直接パス「S3://aip-backup-s3/demo-test-ec2」を入力して、Enter キーを押します。AWS の認証情報の入力を求められた場合は、AWS の [アクセス ID:]、[シークレットキー:] を入力し、[リージョン:] を選択して [接続] をクリックします。



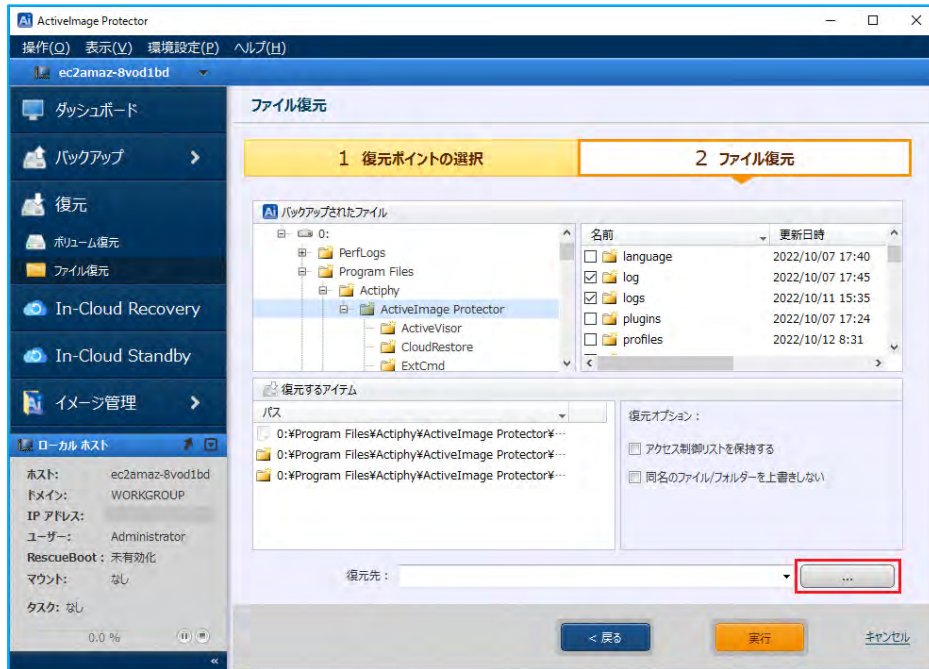
3. [ホスト] から復元対象マシンを選択し、復元ポイントを指定したら [次へ] をクリックします。選択した復元ポイントの情報は [バックアップ情報] に表示されます。



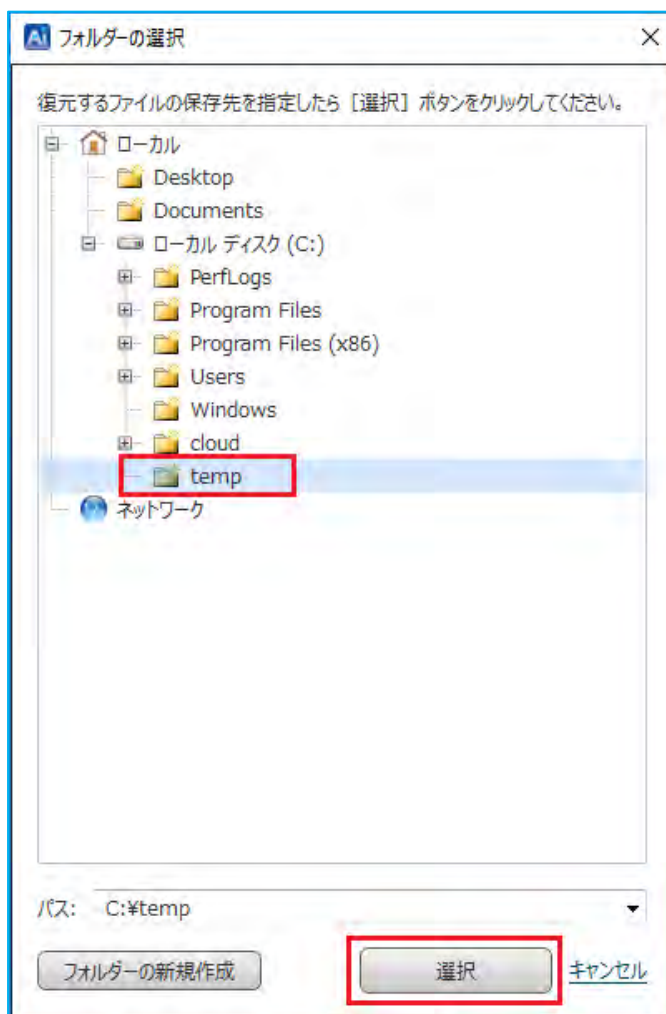
4. [バックアップされたファイル] から、復元するアイテムにチェックを入れます。チェックされたアイテムは [復元するアイテム] にリストされます。復元時のオプションとして、[アクセス制御リストを保持する:] にチェックを入れると、復元対象のファイルに設定されているアクセス制御リスト (ACL) を保持して復元します。[同名のファイル/フォルダーを上書きしない:] にチェックを入れると、保存先に同名のファイル/フォルダーがある場合、上書きせずに別名で復元します。



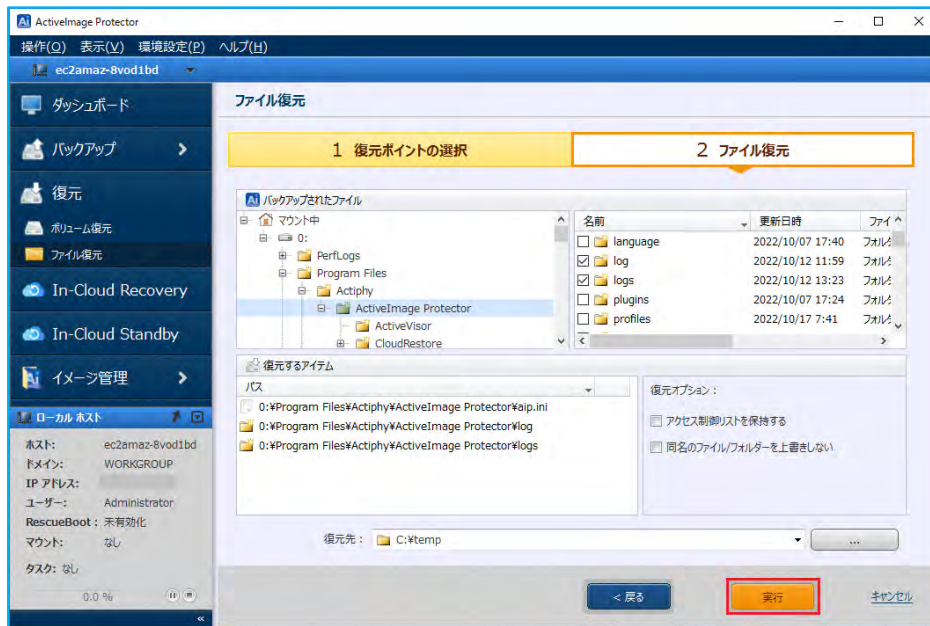
5. 次に、復元するアイテムの保存先を指定します。 [...] をクリックします。



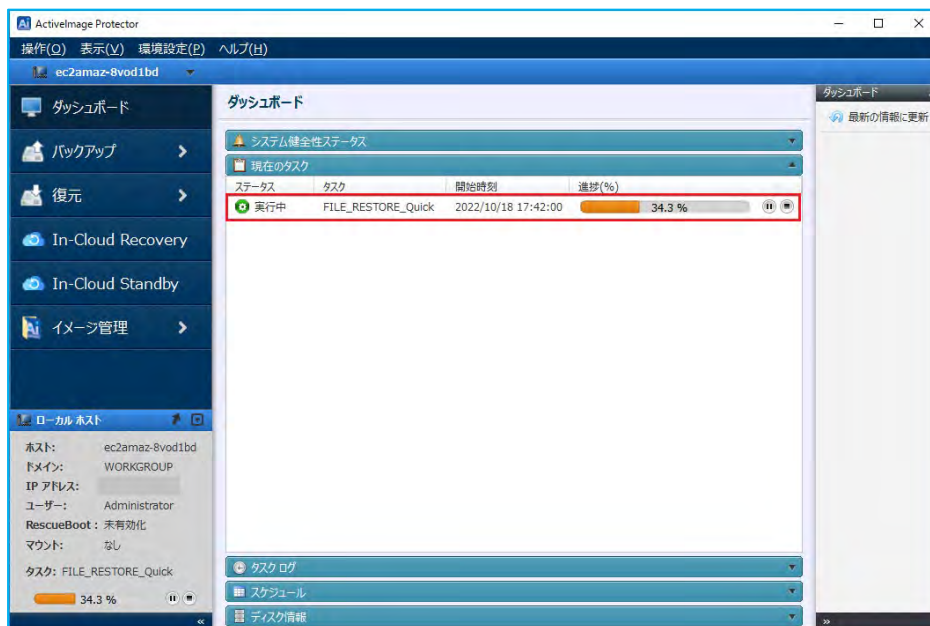
6. 保存先フォルダーを選択し、[選択] をクリックします。



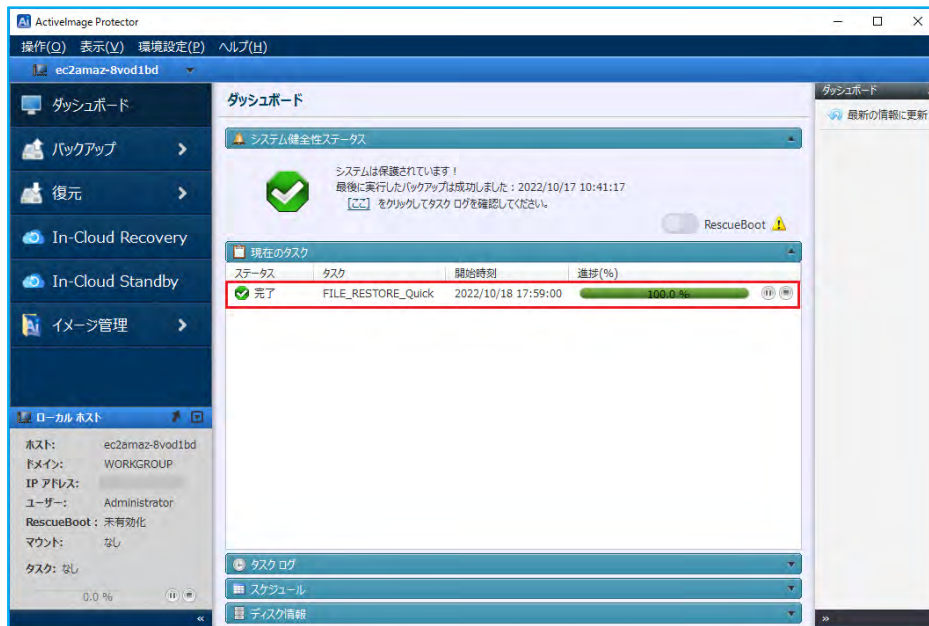
7. 「実行」をクリックすると、復元が開始されます。



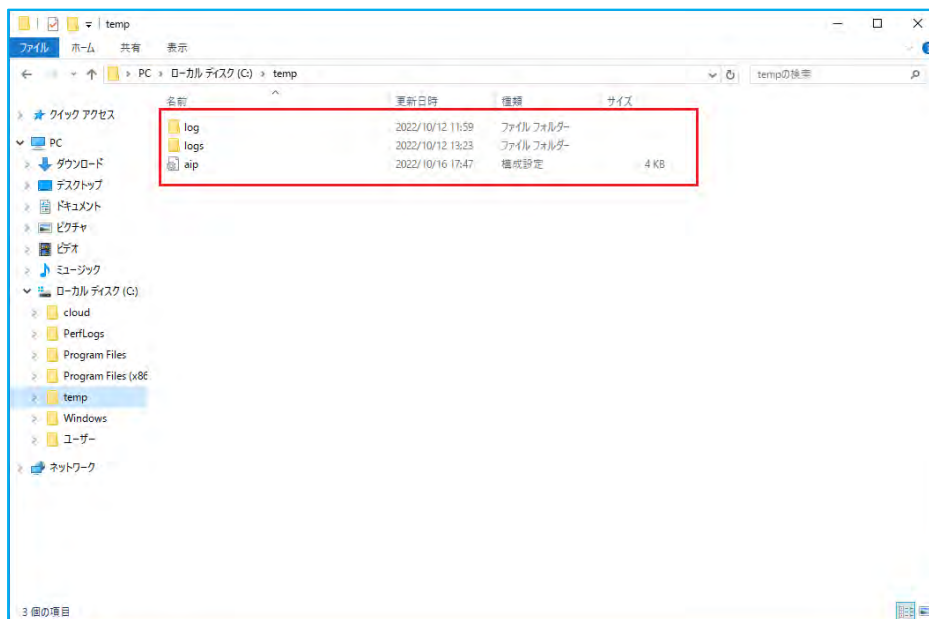
8. 復元処理が開始されると、タスクの進捗状況が表示されます。



9. 進捗状況が100%になれば、復元は完了です。



10. 指定した復元先に、復元アイテムとして選択したファイル、およびフォルダーが保存されます。



4-2. システムリカバリー (In-Cloud Recovery)

ActivImage Protector の「In-Cloud Recovery」は、バックアップから AWS、および Azure のクラウド上の仮想マシンに復元して、システム全体を復旧することができます。クラウドの管理コンソールやコマンドラインなどを駆使した複雑な操作を必要としません。ここでは、「In-Cloud Recovery」によるバックアップから AWS EC2 インスタンスのシステム復旧手順について説明します。

※ In-Cloud Recovery は、Google Cloud、Oracle Cloud 環境では使用できません。仮想マシンの復元作業は、RescueBoot から起動した起動環境を使用してこなってください。（次項「4-3. システムリカバリー (RescueBoot)」を参照）

1. In-Cloud Recovery を起動します。

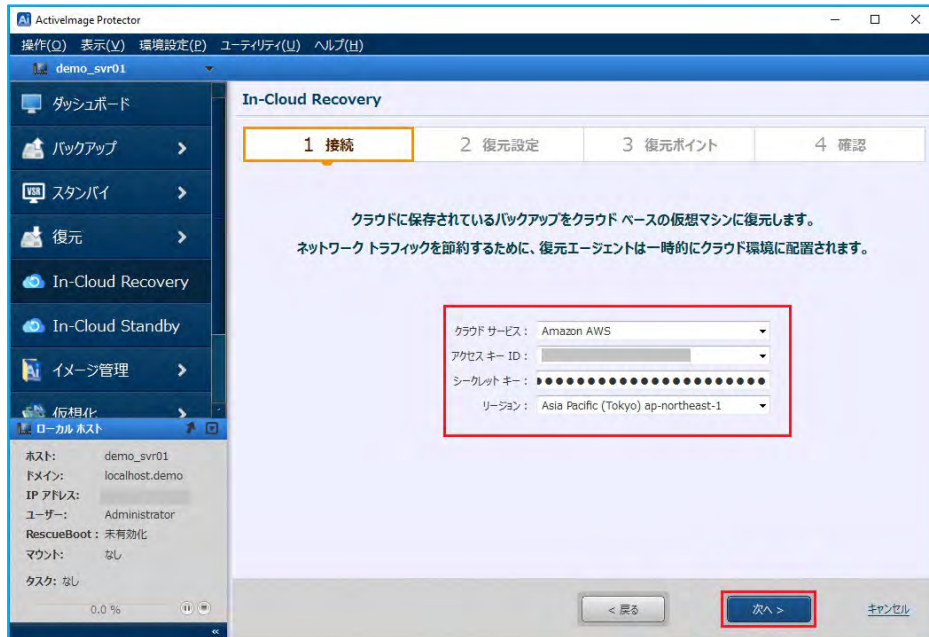
※In-Cloud Recovery は、復元先の仮想マシンから実行することはできません。クラウドにアクセス可能な別のコンピューターから行う必要があります。

ActivImage Protector のコンソールのメニュータブから [In-Cloud Recovery] をクリックします。この処理の実行には、クラウドの各リージョンに配置されている「Actiphy Cloud エージェント」という仮想マシンイメージの一時的な起動、および復元の際に作成されるボリュームのストレージやデータ転送など、クラウドプロバイダーの所定の利用料金がかかります。これに同意して、[追加費用に関して確認しました] にチェックを入れ、[次へ] をクリックしてください。

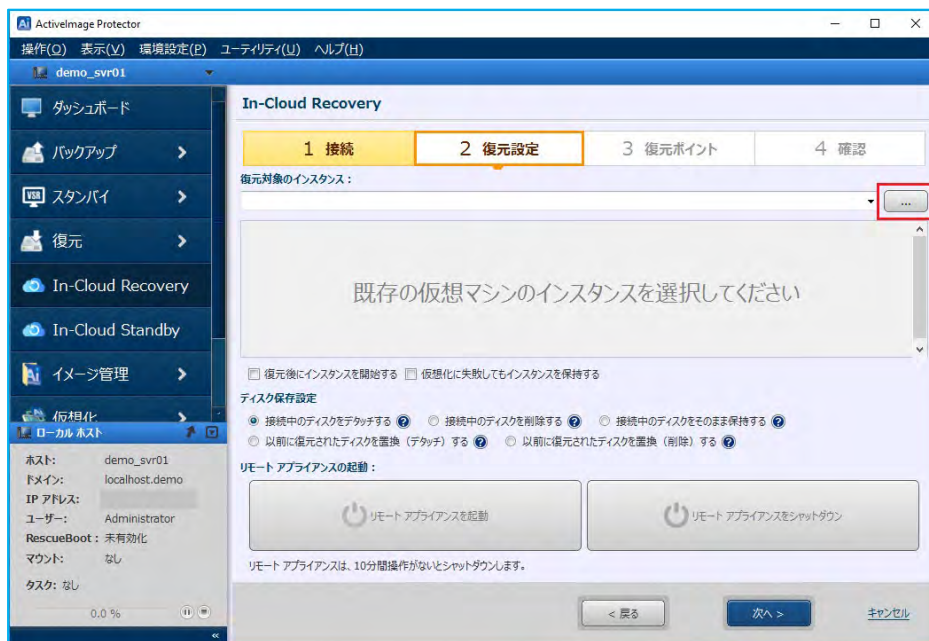


- 接続するクラウドサービスを選択し、必要な認証情報を入力します。

ここでの設定例として、クラウドサービスに [Amazon AWS] を選択して、AWS の [アクセスキー] と [シークレットキー] を入力し、[リージョン] を選択して [次へ] をクリックします。

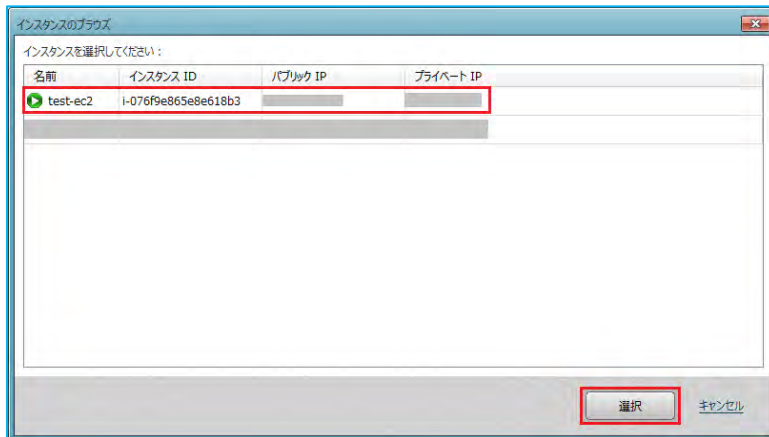


- 復元先となるインスタンスを選択します。 [...] をクリックします。

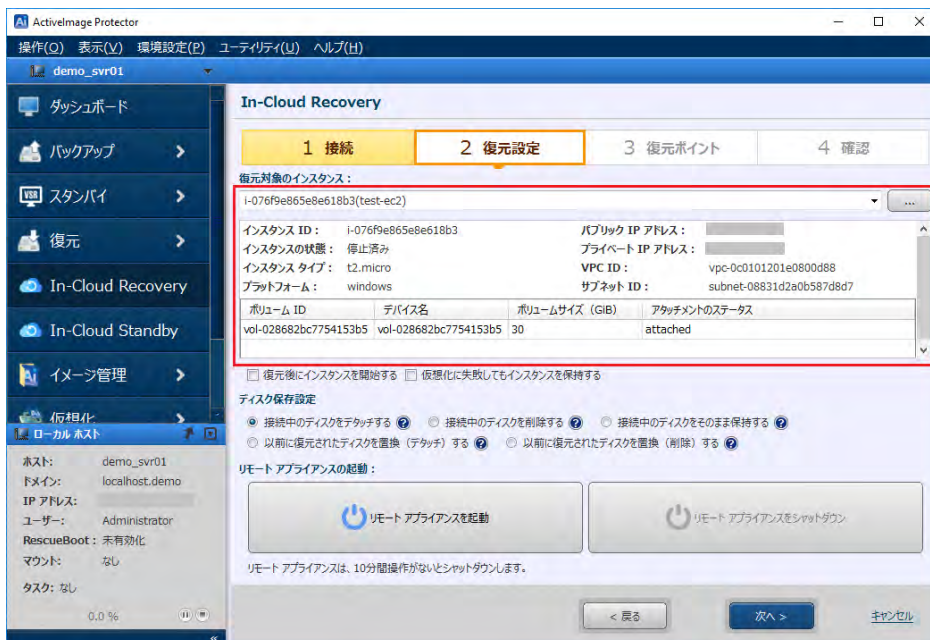


リストア

4. 復元先となるインスタンスを選択してから、「選択」をクリックします。
ここでの設定例として、バックアップ元のインスタンス「test-ec2」を選択します。

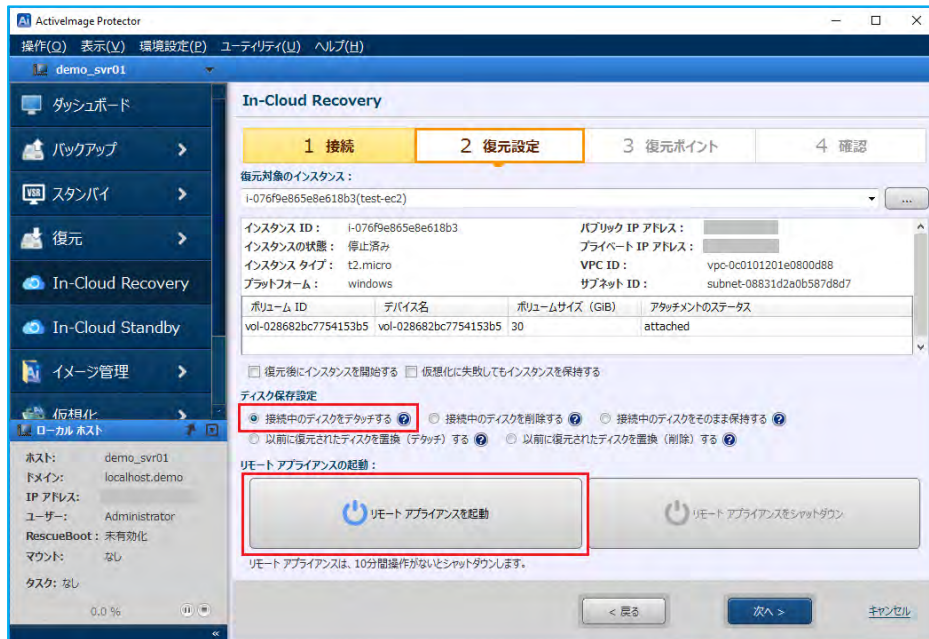


5. 復元先となるインスタンスの情報が表示されます。



6. 復元したボリュームの処理方法を選択します。

ここでの設定例として、[ディスク保存設定] は、標準設定の [接続中のディスクをデタッチする] にします。次に、[リモートアプライアンスを起動] をクリックして、「Actiphys Cloud エージェント（起動環境）」を起動します。起動するまでしばらく待ちます。



ディスク保存設定：

(1) 接続中のディスクをデタッチする：

インスタンスに接続中のボリュームをデタッチ（切り離し）し、復元したボリュームをインスタンスにアタッチ（接続）します。デタッチされたボリュームは削除されずに残ります。

(2) 接続中のディスクを削除する：

インスタンスに接続中のボリュームをデタッチ後に削除し、復元したボリュームをインスタンスにアタッチします。

(3) 接続中のディスクをそのまま保持する：

インスタンスに接続中のボリュームはデタッチせず、復元したボリュームを追加でアタッチします。

(4) 以前に復元されたディスクを置換（デタッチ）する：

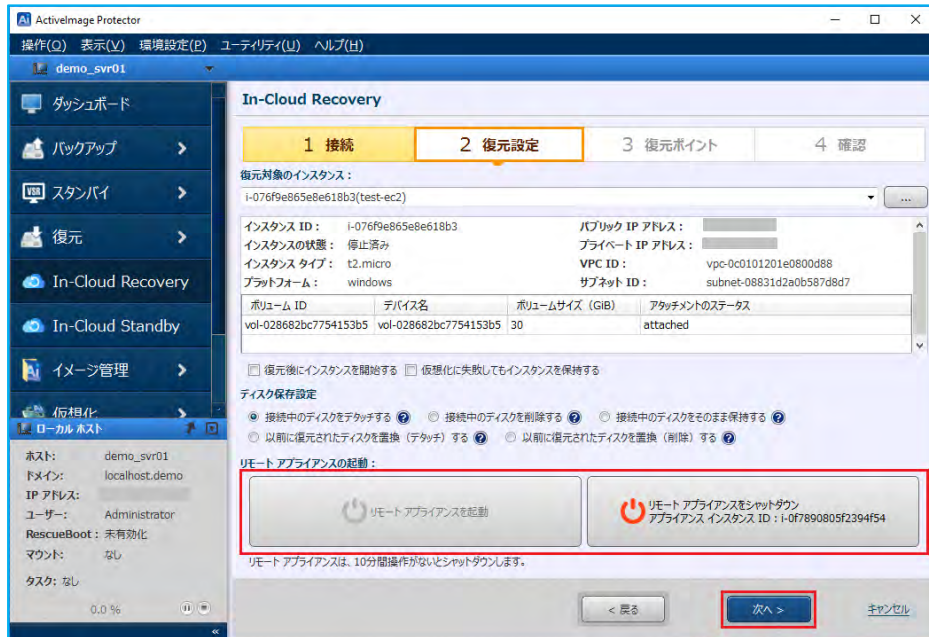
インスタンスに接続中の ActiImage Protector から復元したボリュームをデタッチし、復元したボリュームをインスタンスにアタッチします。デタッチされたボリュームは削除されずに残ります。ActiImage Protector から復元されていないボリュームはインスタンスからデタッチされません。

(5) 以前に復元されたディスクを置換（削除）する：

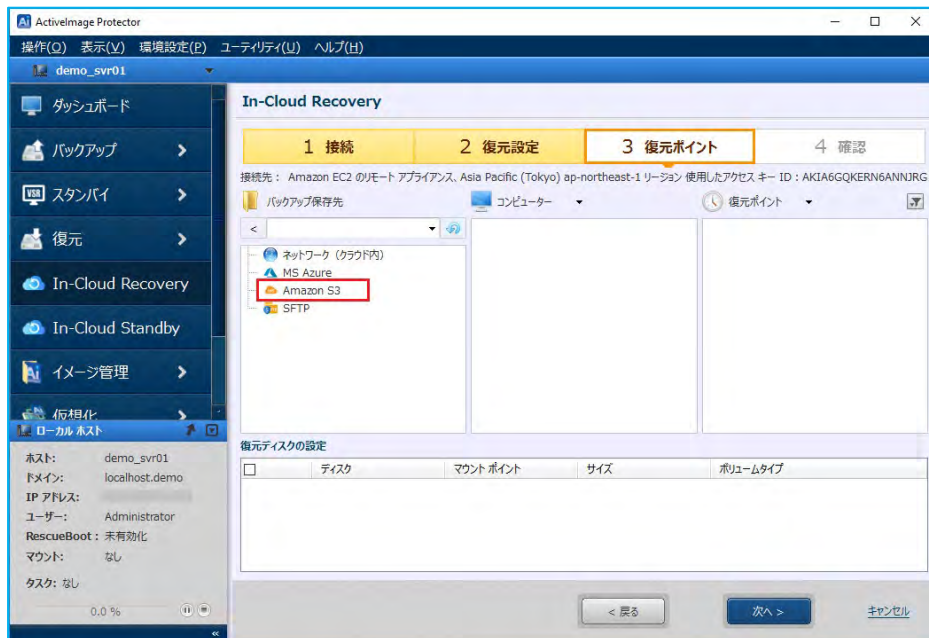
インスタンスに接続中の ActiImage Protector から復元したボリュームをデタッチ後に削除し、復元したボリュームをインスタンスにアタッチします。ActiImage Protector から復元されていないボリュームはインスタンスからデタッチされません。

リストア

7. 以下の様に、[リモートアプライアンスを起動] ボタンがグレーアウトされ、[リモートアプライアンスをシャットダウン] ボタンが選択可能になったら、「Actiphy Cloud エージェント（起動環境）」の起動は完了です。[次へ] をクリックします。



8. 復元したいマシンのバックアップ保存先を選択します。
 ここでの設定例として、[バックアップ保存先] は [Amazon S3] をクリックします。



9. Amazon S3 に対する AWS の [アクセスキー] と [シークレットキー] を入力し、[リージョン] を選択して [接続] をクリックします。

ActivImage Protector

アクセス キー ID :

シークレット キー :

リージョン : アジアパシフィック (東京)

☐ プロバイダーを指定する NIFCLOUD (east-2)

認証情報を入力してください。

接続 キャンセル

10. バックアップ保存先の「フォルダー」→「コンピューター」→「復元ポイント」を選択して、[次へ] をクリックします。[復元ディスクの設定] において、復元するディスクのサイズやタイプを設定することもできます。

ActivImage Protector

操作(Q) 表示(V) 環境設定(E) ユーティリティ(U) ヘルプ(H)

demo_svr01

ダッシュボード

バックアップ

スタンバイ

復元

In-Cloud Recovery

In-Cloud Standby

イメージ管理

仮想化

ローカルホスト

ホスト: demo_svr01

ドメイン: localhost.demo

IP アドレス:

ユーザー: Administrator

RescueBoot: 未有効化

マウント: なし

タスク: なし

0.0 %

In-Cloud Recovery

1 接続 2 復元設定 3 復元ポイント 4 確認

接続先: Amazon EC2 のリモート アプライアンス, Asia Pacific (Tokyo) ap-northeast-1 リージョン 使用したアクセス キー ID : AKIA6GQKERN6ANNJRG

バックアップ保存先

バックアップ先: iip-backup-s3/demo-test-ec2

コンピューター

復元ポイント

ec2amaz-8vod1bd

2022/10/12 9:30:04

2022/10/12 8:30:04

2022/10/12 7:30:04

2022/10/12 6:30:04

2022/10/12 5:30:04

2022/10/12 4:30:04

2022/10/12 3:30:04

2022/10/12 2:30:04

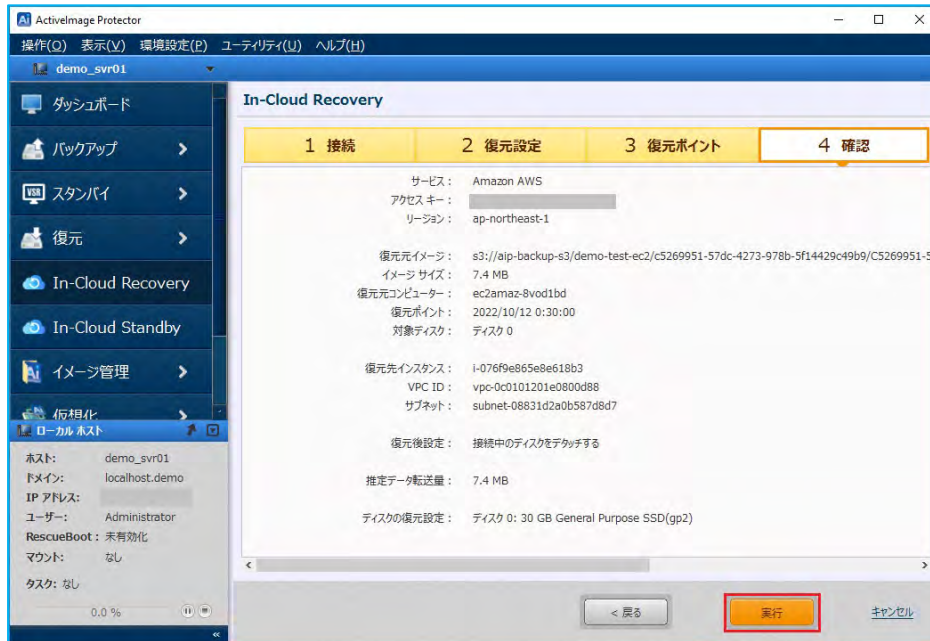
2022/10/12 1:30:04

復元ディスクの設定

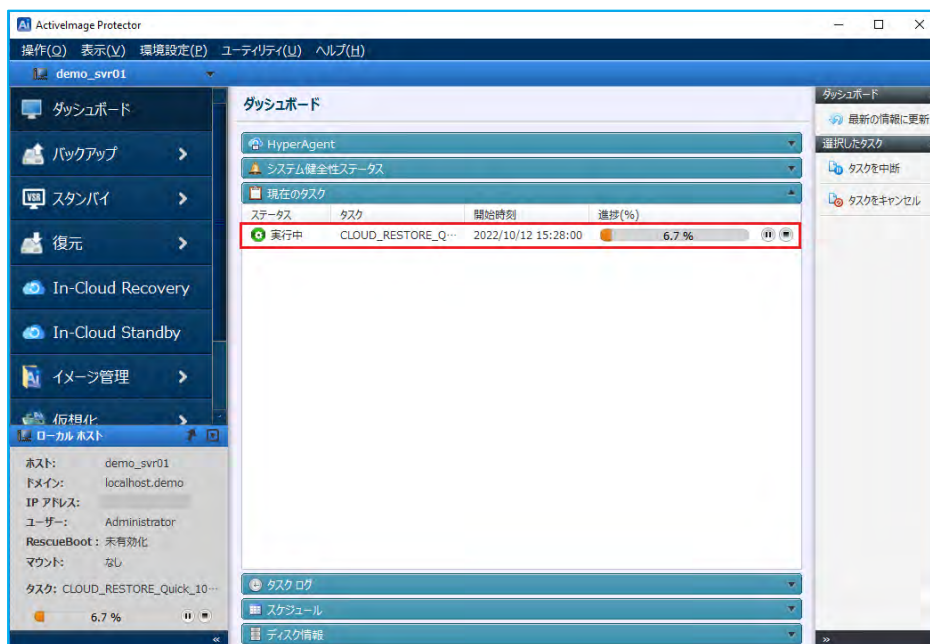
ディスク	マウント ポイント	サイズ	ボリュームタイプ
ディスク 0	/dev/xvddg	30	General Purpose SSD(gp2)

< 戻る **次へ >** キャンセル

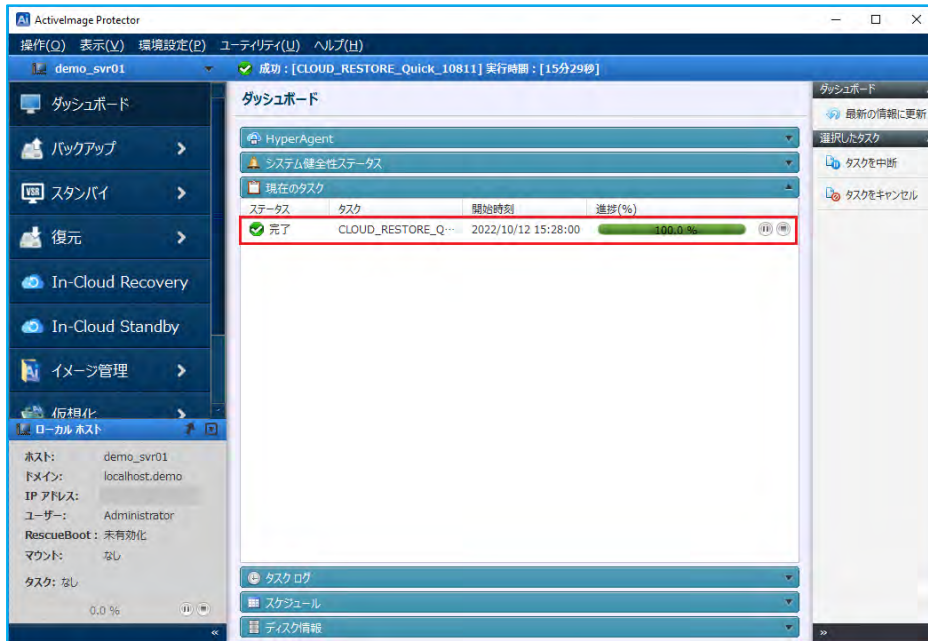
11. 内容を確認して、[実行] をクリックすると復元が開始されます。



12. 復元が開始されると、タスクの進捗状況が表示されます。

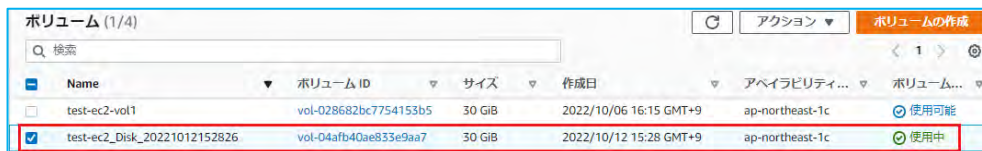


13. 進捗が100%になると復元は完了です。



14. 復元完了後、AWS マネジメントコンソールから、インスタンスに接続されていたボリュームがデタッチされ、復元したボリュームが復元先のインスタンスに接続されていることが確認できます。

(1) バックアップから新規ボリュームが作成されています。ボリューム名は、[<インスタンス名>_disk_YYYYMMDDhhmmss] で作成されます。復元管理後に、正常動作を確認したら、デタッチされた元のボリュームは明示的に削除します。



(2) 作成されたボリュームがインスタンスのルートデバイスとして接続されています。



4-3. システムリカバリー (RescueBoot)

ActivelImage Protector の「RescueBoot」は、Actiphy Boot Environment (起動環境) の外部メディアを必要とすることなく、AWS、Azure、Google Cloud、Oracle Cloud の仮想マシンから起動環境を直接起動させることができます。また、RescueBoot から起動した起動環境にリモートから接続し、クラウド仮想マシンのシステムの復元をおこなうことができます。ここでは、「RescueBoot」による AWS EC2 インスタンス (仮想マシン) のシステム復元手順について説明します。

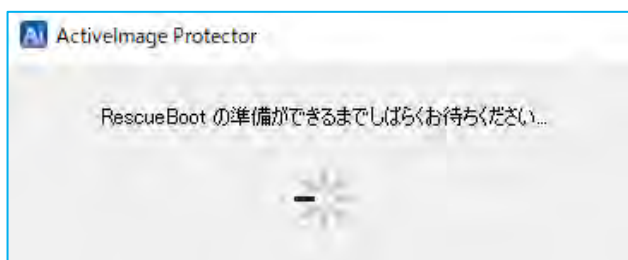
1. RescueBoot の起動

ActivelImage Protector がインストールされている、復元先の仮想マシンから操作をおこないます。

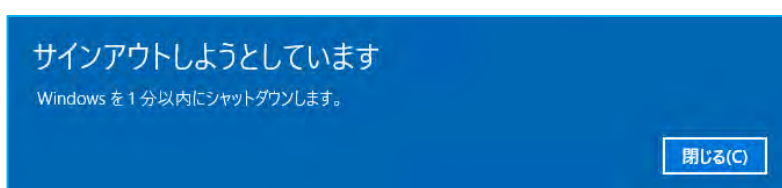
- (1) Windows の通知領域 (デスクトップ画面の右下) にある ActivelImage Protector のアイコンメニューから、[RescueBoot の実行] をクリックします。



- (2) RescueBoot が実行されると、内蔵ディスク内に起動環境が作成されます。起動環境の作成が完了するまでしばらく待ちます。(2 分から 3 分)



- (3) 起動環境の作成が完了すると、システムのシャットダウンを通知するメッセージが表示され起動環境が起動します。この時点で、リモート接続は切断されます。



2. 起動環境への接続

復元先の仮想マシンから起動環境が起動したら、ActivelImage Protector のリモート管理コンソールから接続して復元操作をおこないます。

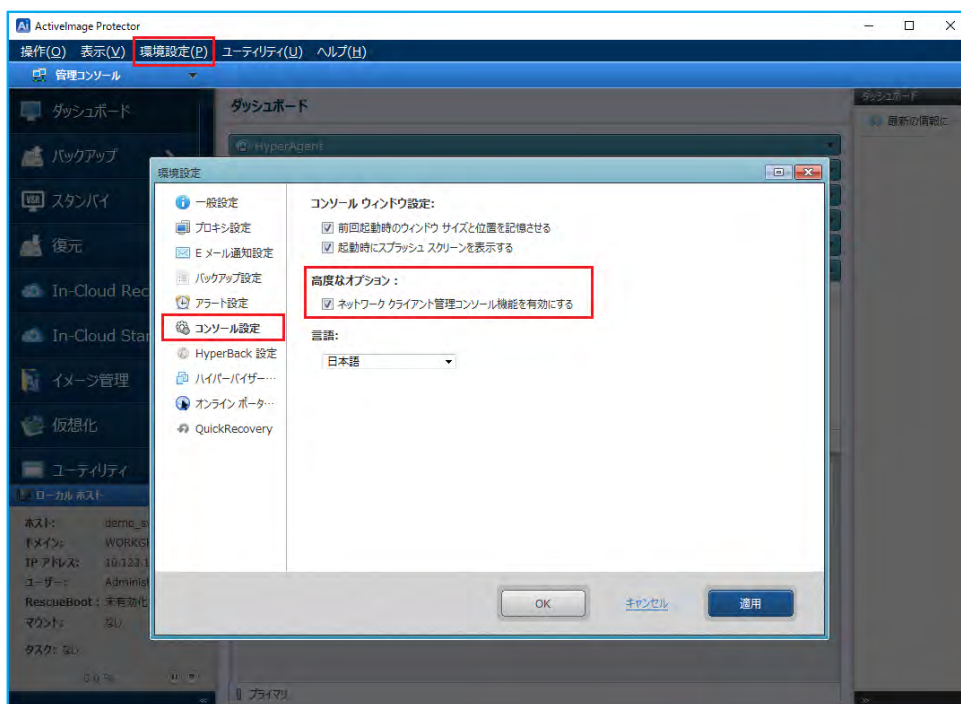
※ここでは、AWS のインスタンスのセキュリティ設定で以下のポートを開放しています。

- ・TCP ポート 48236
- ・UDP ポート 48238
- ・UDP ポート 48239

(1) ActivelImage Protector のコンソールを起動します。

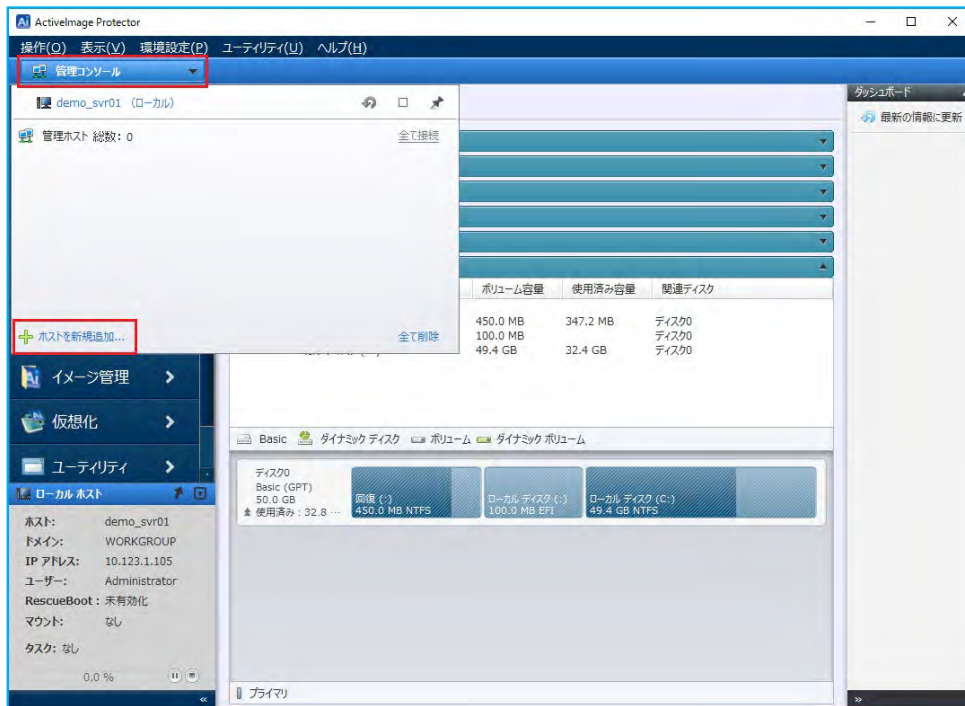
Windows スタートメニューから [Actiphy] → [ActivelImage Protector] をクリックして ActivelImage Protector のコンソールを起動します。

(2) 最初に、リモート管理コンソールを使用するためには、ActivelImage Protector の管理コンソールのメニューから、[環境設定] → [コンソール設定] → [ネットワーク クライアント管理コンソール機能を有効にする] にチェックを入れ、[適用] をクリックします。[OK] をクリックしてダッシュボードに戻ります。

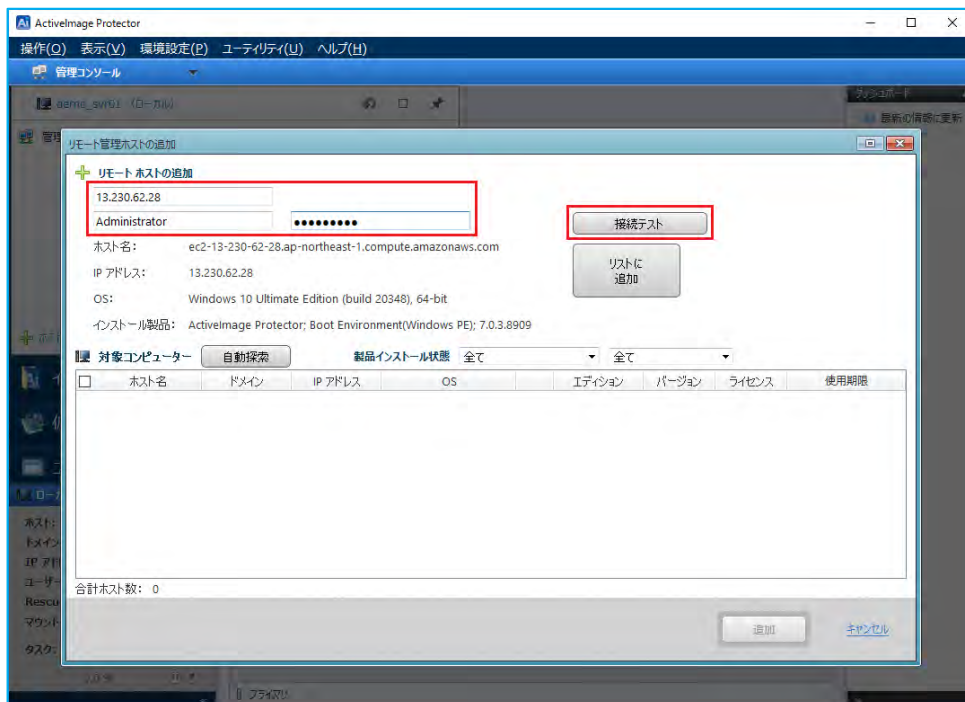


リストア

- (3) コンソール左上にある「管理コンソール」から操作を行います。リモート管理を行うためには、最初にホストリストを作成します。「ホストを新規追加...」をクリックします。

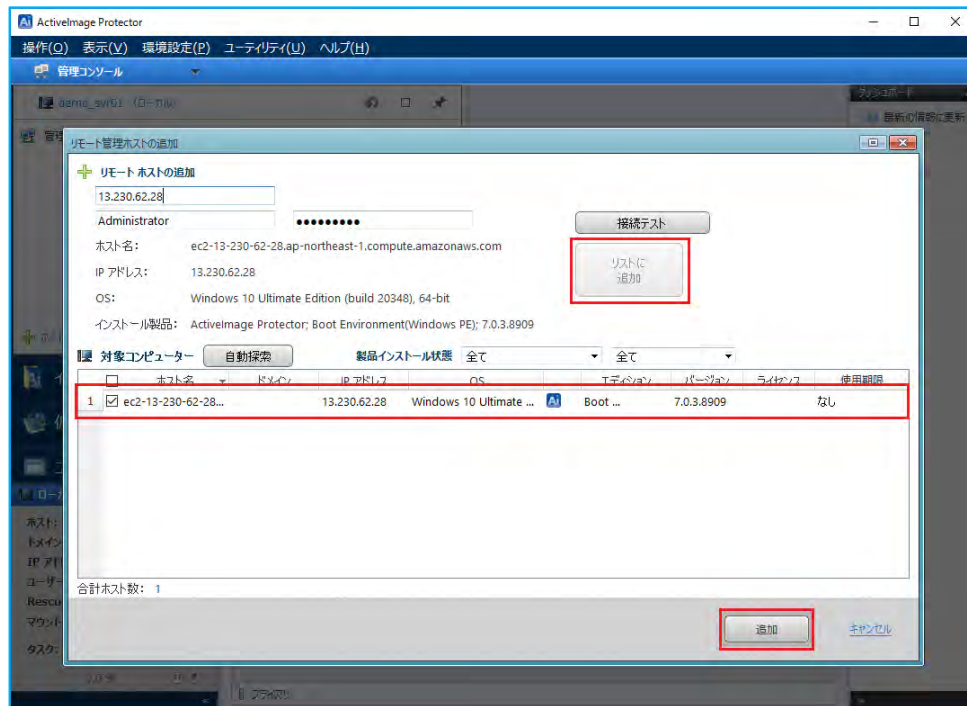


- (4) リストに追加する復元先の起動環境が起動している仮想マシンを指定します。ここでの設定例として、[リモートホストの追加] から「インスタンスのパブリック IP アドレス」、「管理者ユーザー名」、「パスワード」を入力し、[接続テスト] をクリックします。接続テストに成功すると [ホスト名]、[IP アドレス]、[インストール製品](Actiphy Boot Environment)が表示されます。

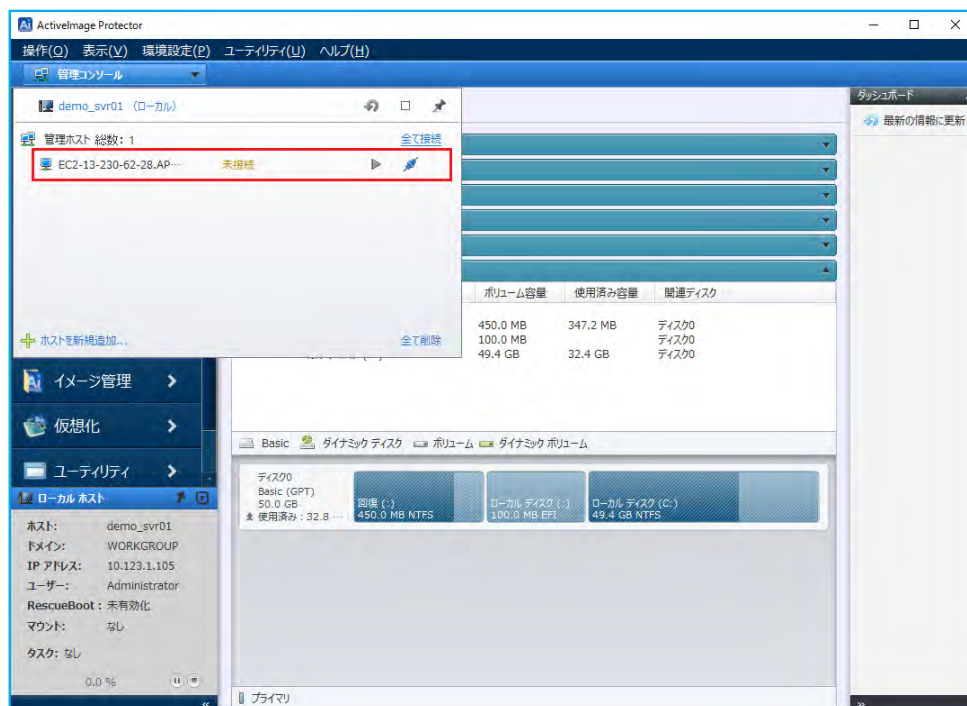


リストア

- (5) 次に、[リストに追加] をクリックすると、[対象コンピューター] のリストに追加されますので、[追加] をクリックして管理対象コンピューターに登録します。

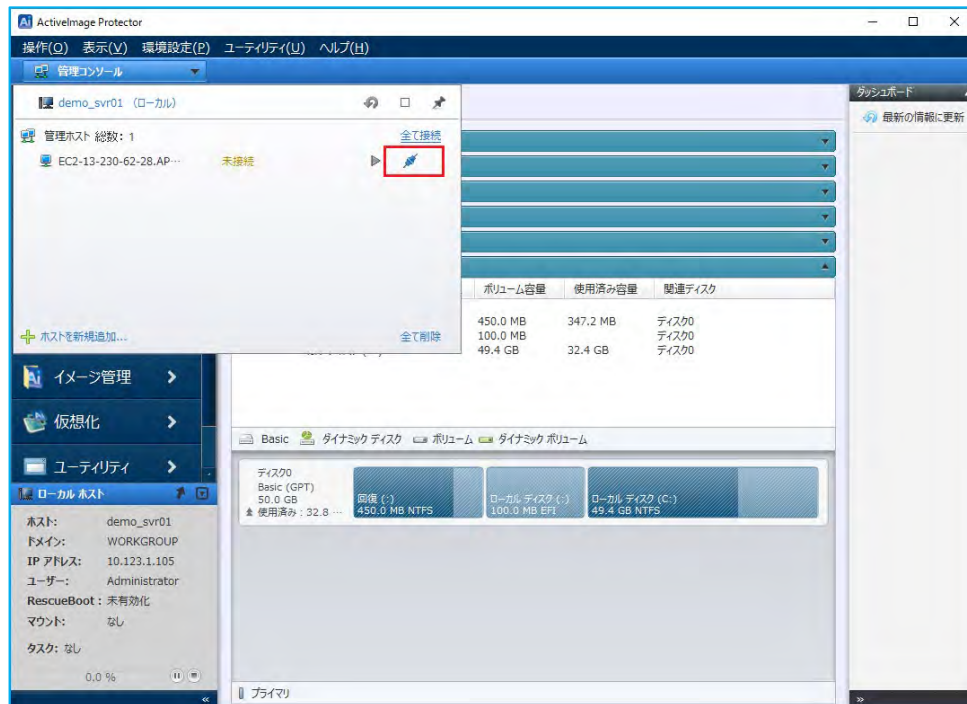


- (6) 管理対象ホストとして、リモートホストが追加されます。

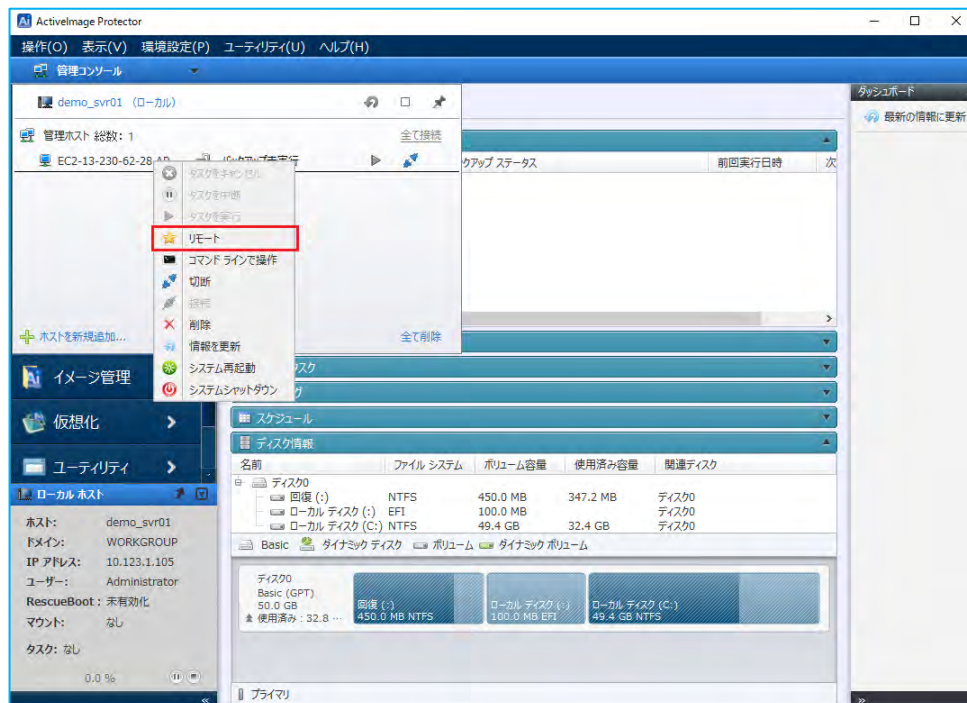


リストア

- (7) ホストリストからホストを選択し、右クリックすると、以下のようなコンテキストメニューが表示されます。ここから、右端の「コネクタマーク」をクリックします。

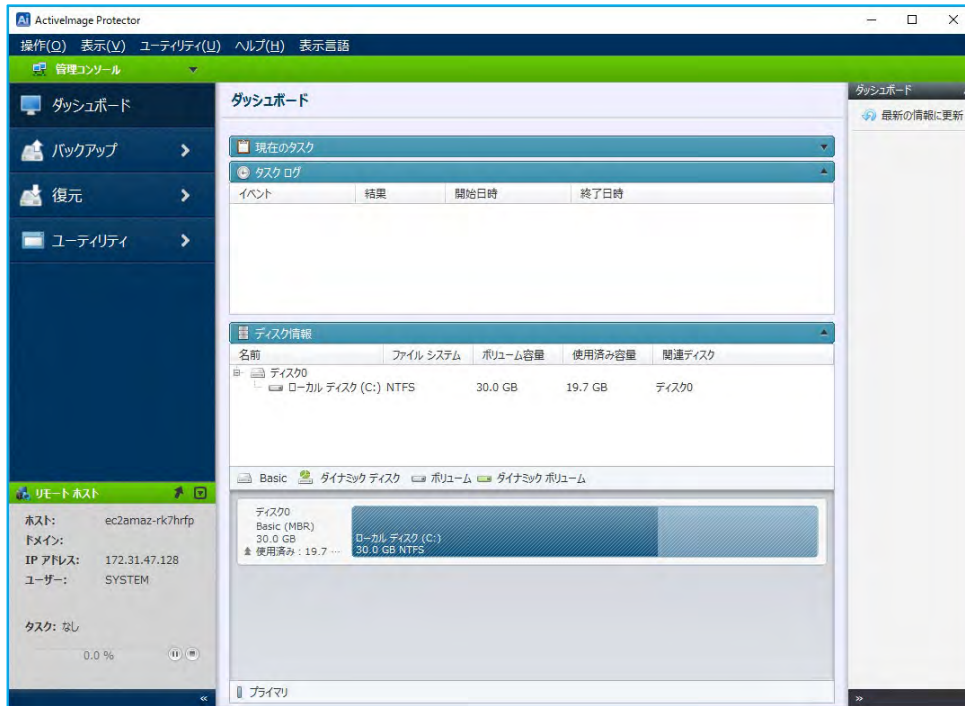


- (8) ホストリストからホストを選択し、右クリックメニューから「リモート」をクリックすると起動環境にリモート管理コンソールから接続できます。



(9) 接続に成功すると、ステータスバーの色が緑になります。

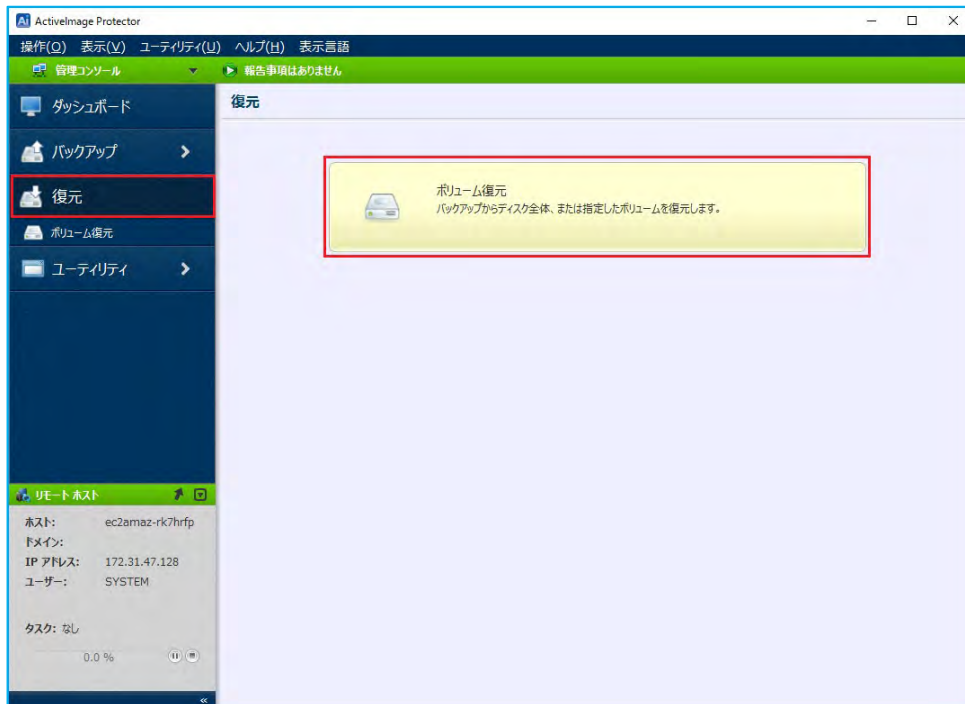
※リモートホストへの接続を解除する場合は、ローカルホスト名をダブルクリックします。



3. システムの復元操作

起動環境に接続した、リモート管理コンソールから復元操作をおこないます。

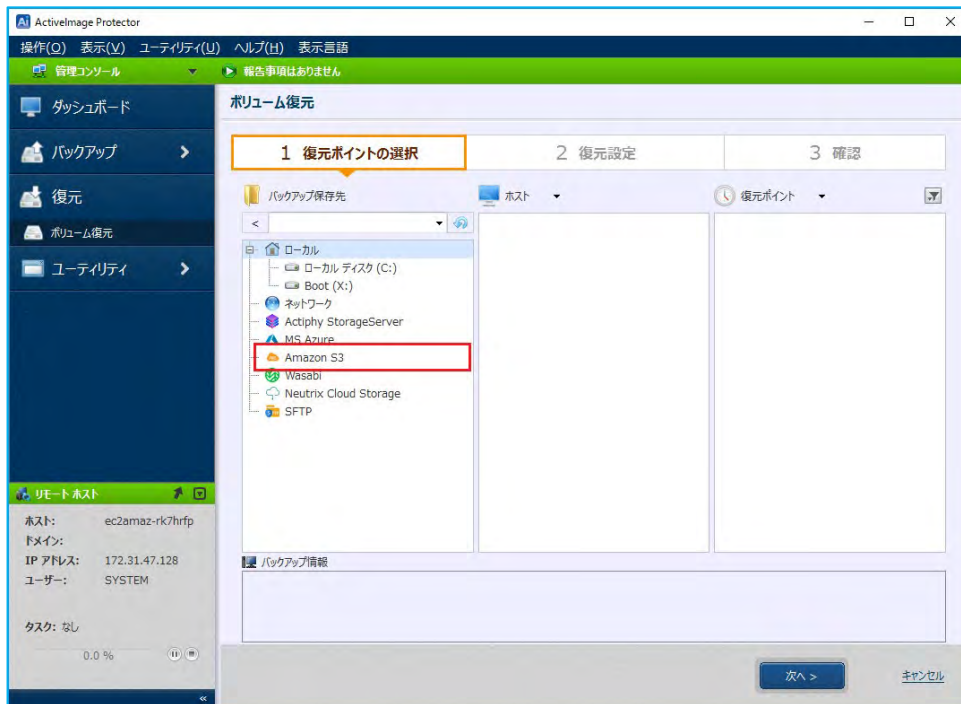
(1) 「復元」 → 「ボリューム復元」 をクリックします。



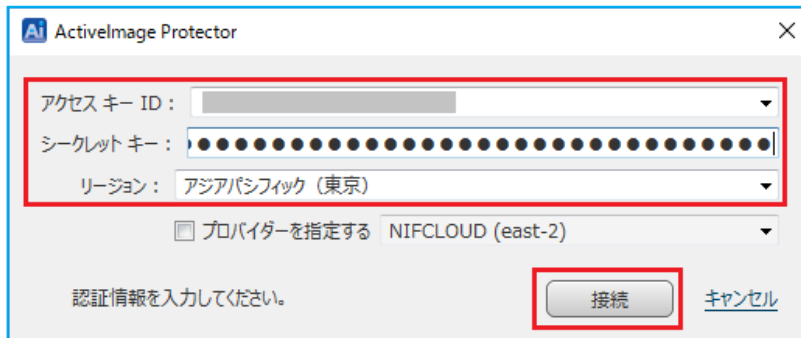
リストア

(2) 復元したい仮想マシンのバックアップ保存先を選択します。

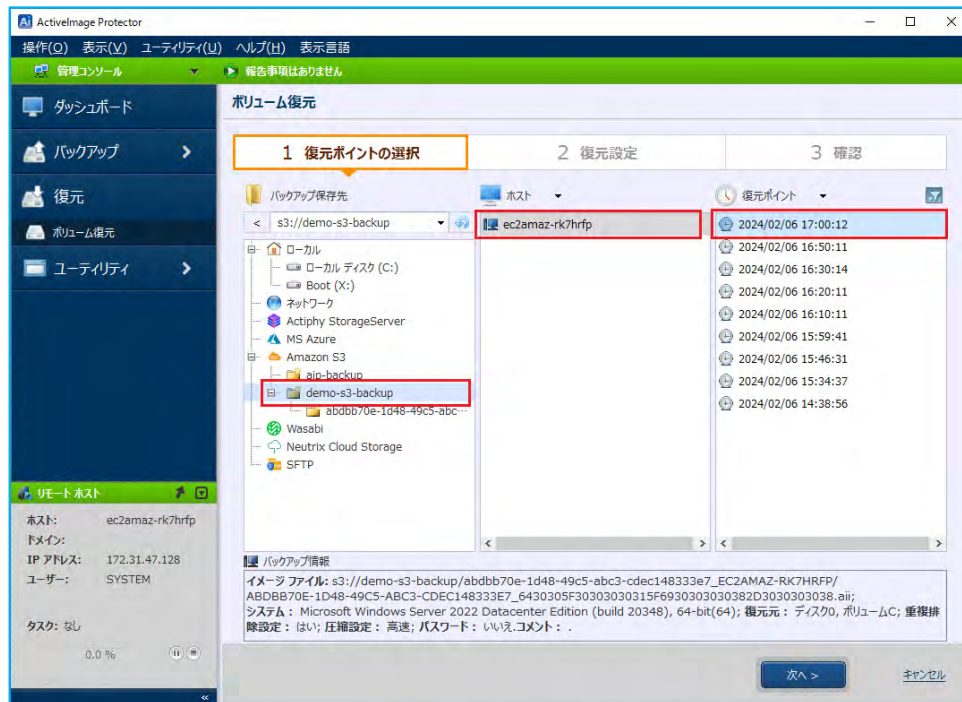
ここでの設定例として、[バックアップ保存先] は [Amazon S3] をクリックします。



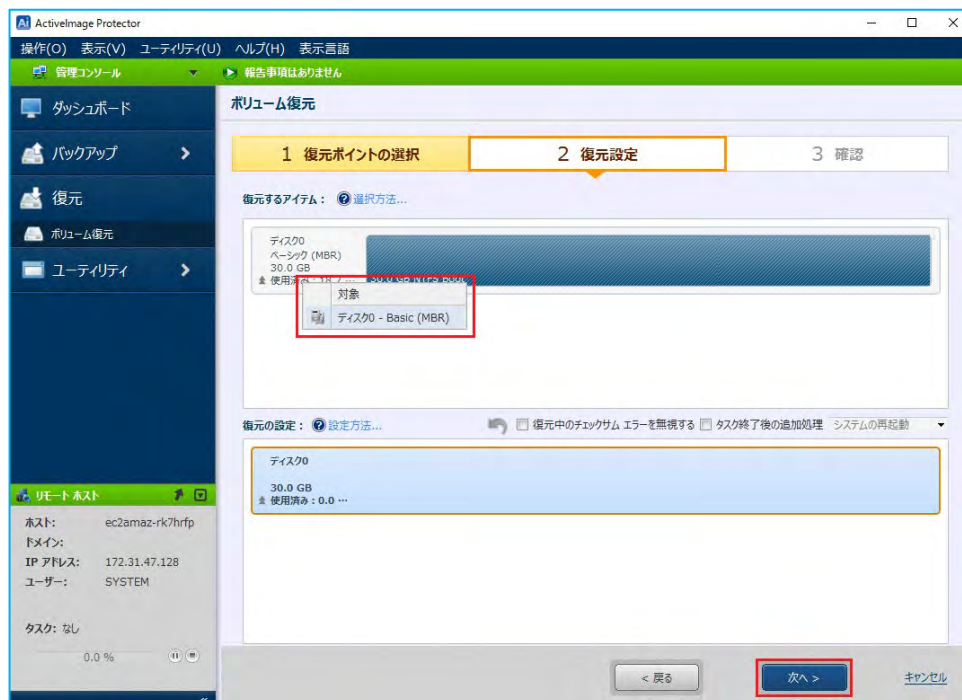
(3) Amazon S3 に対する AWS の [アクセスキーID] と [シークレットキー] を入力し、[リージョン] を選択して [接続] をクリックします。または、[アクセスキーID] のテキストボックスの右にある [▼] をクリックすると、これまでのバックアッププロセスやバックアップで使用した保存先が表示されますので、ここから選択もできます。



- (4) バックアップ保存先の「フォルダー」→「コンピューター」→「復元ポイント」を選択して、[次へ]をクリックします。

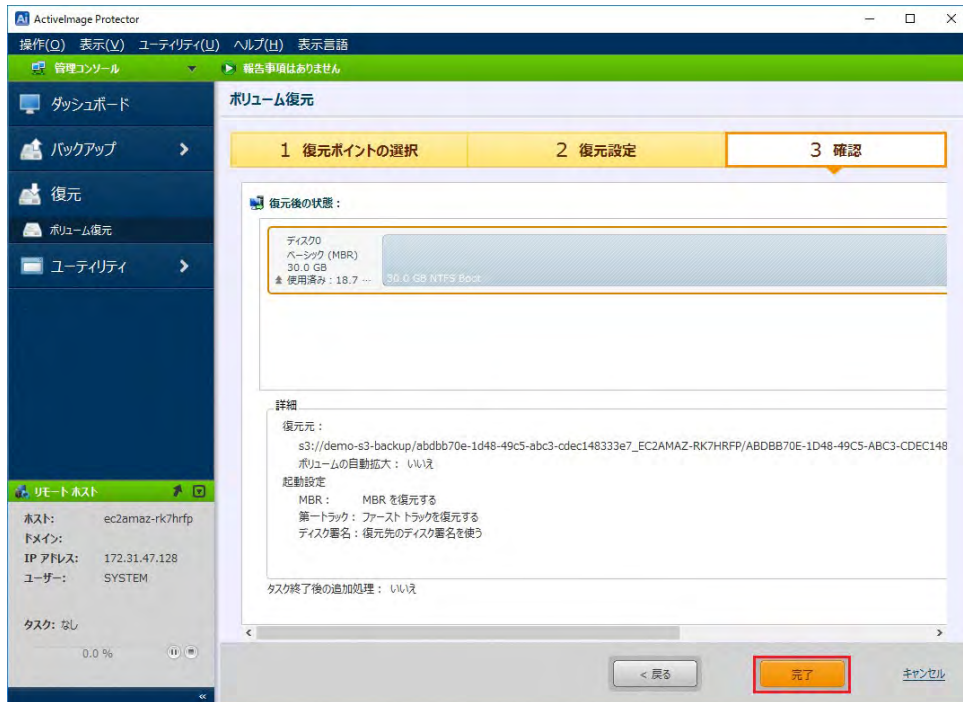


- (5) [復元するアイテム] からディスクマップの左部分（ベーシック（MBR）あたり）を右クリックして、[対象] で「ディスク0 - Basic (MBR)」を選択します。[復元の設定] に復元する内容が表示されるので、確認し [次へ] をクリックします。

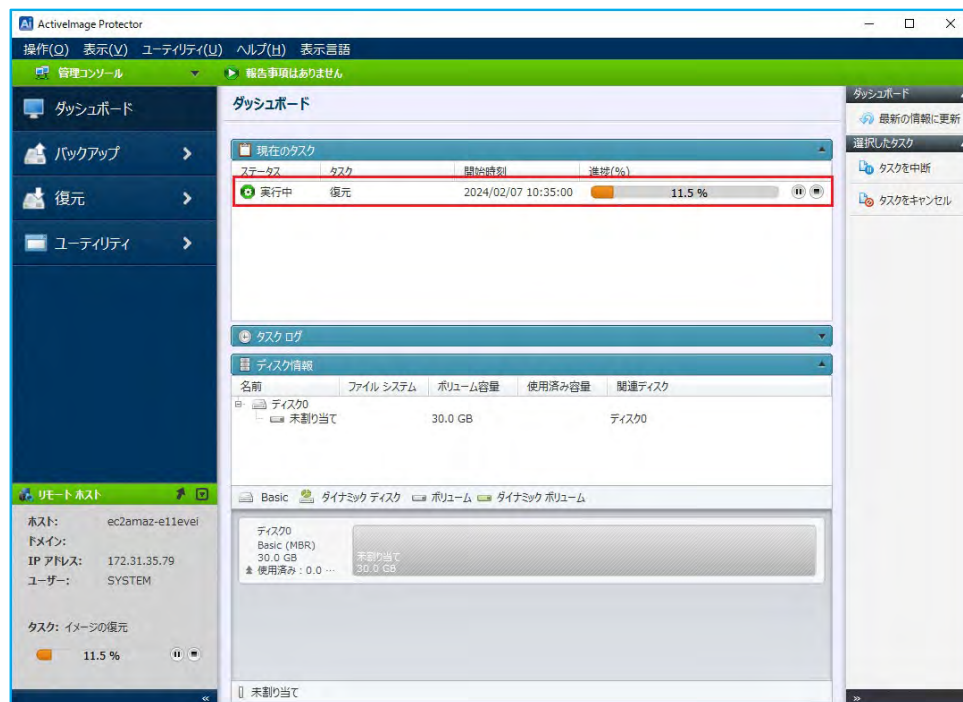


リストア

(6) 確認画面になりますので、その内容を確認し、[完了] をクリックします。

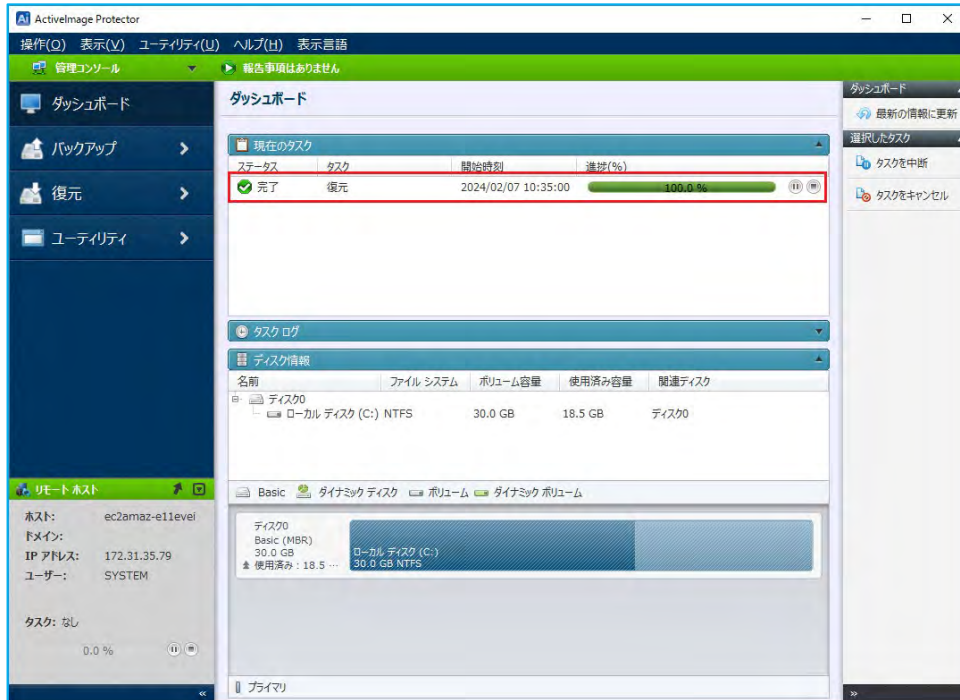


(7) リカバリーが開始されると、タスクの進捗状況が表示されます。

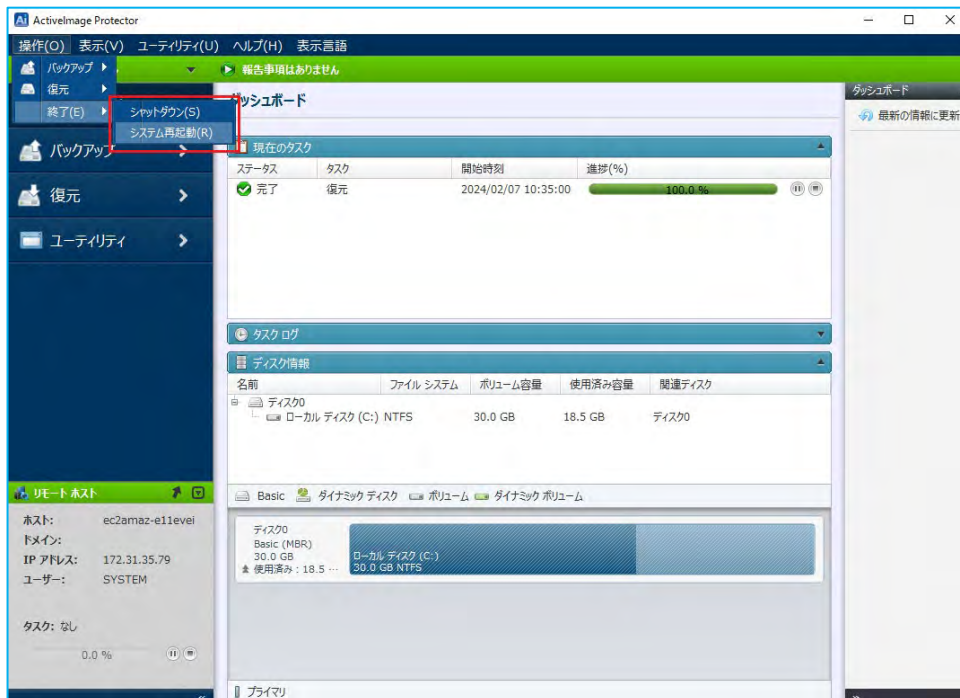


リストア

(8) タスクが100%になれば、クラウド仮想マシンのリカバリーの完了です。

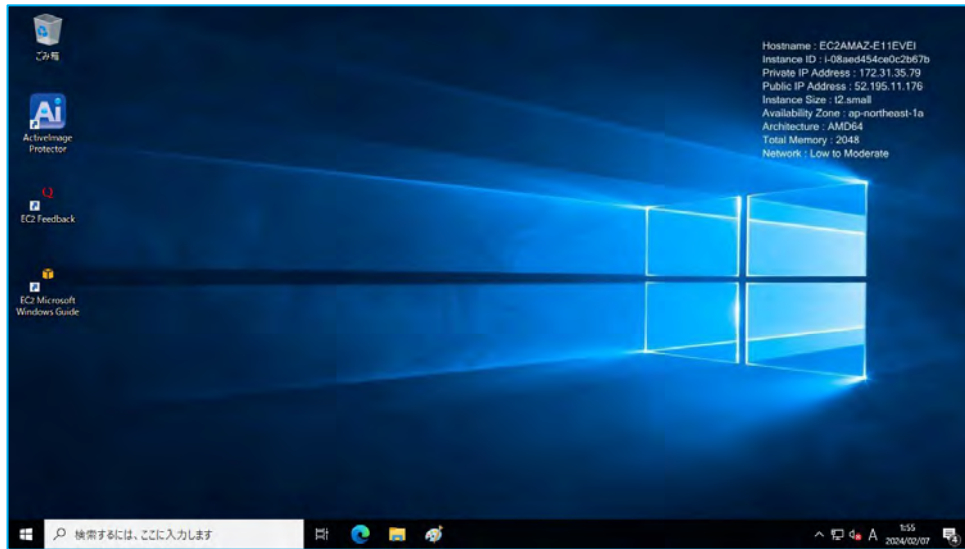


(9) [操作] → [終了] を選択し、シャットダウン、もしくは再起動します。



リストア

(10) 復元した仮想マシンに接続し、リカバリーが正しくできているかを確認します。



5. 仮想スタンバイマシンの作成 (In-Cloud Standby)

ActiveImage Protector の「In-Cloud Standby」は、AWS、または Azure のクラウド上の仮想マシンのバックアップから、システムを復旧するためのスナップショットをスケジュールで作成することができます。緊急時には、復旧させたい時点のスナップショットから、AWS、または Azure のクラウド上の元の仮想マシン、または新規に仮想マシンを作成し、迅速にシステムを復旧することができます。

ここでは、「In-Cloud Standby」による AWS EC2 インスタンスのバックアップからスナップショットの作成手順、および AWS マネジメントコンソールを使用したスナップショットからボリュームの作成、新規作成のインスタンスへのボリュームのアタッチ（接続）など、一連のシステム復旧手順について説明します。

5-1. バックアップからスナップショットの作成

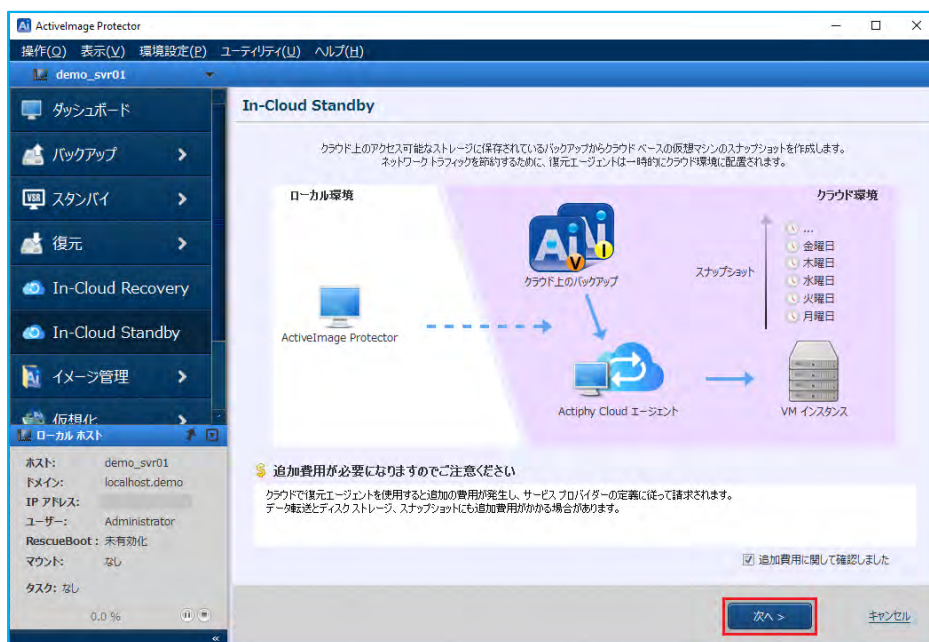
※「In-Cloud Standby」が使用するバックアップは、バックアップ設定の「高度な設定」から「バックアップ時にあらかじめ In-Cloud Standby 向けの仮想化処理を行う」を有効にしてバックアップを作成する必要があります。設定については、「3-2.ボリューム バックアップ：スケジュール (P.12)」の項で説明していますので、そちらを参照してください。

1. ActiveImage Protector のコンソールを起動します。

ActiveImage Protector のコンソールのメニュータブから [In-Cloud Standby] をクリックします。

この処理の実行には、クラウドの各リージョンに配置されている「Actiphy Cloud エージェント」という仮想マシンイメージの一時的な起動、およびスナップショットやスナップショットから作成されるボリュームのストレージ、データ転送など、クラウドプロバイダーの所定の利用料金がかかります。

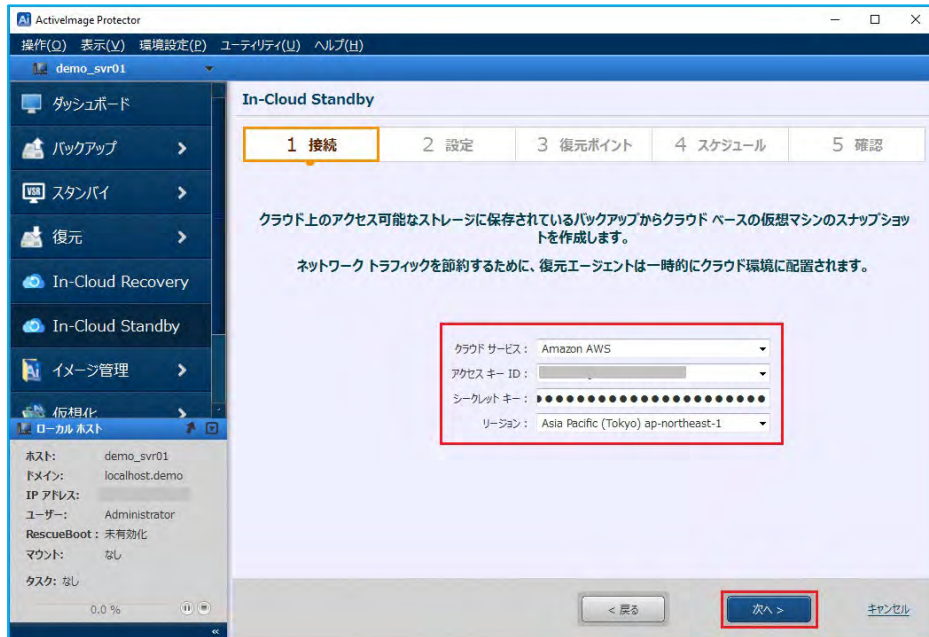
これに同意して、「追加費用に関して確認しました」にチェックを入れ、「次へ」をクリックします。



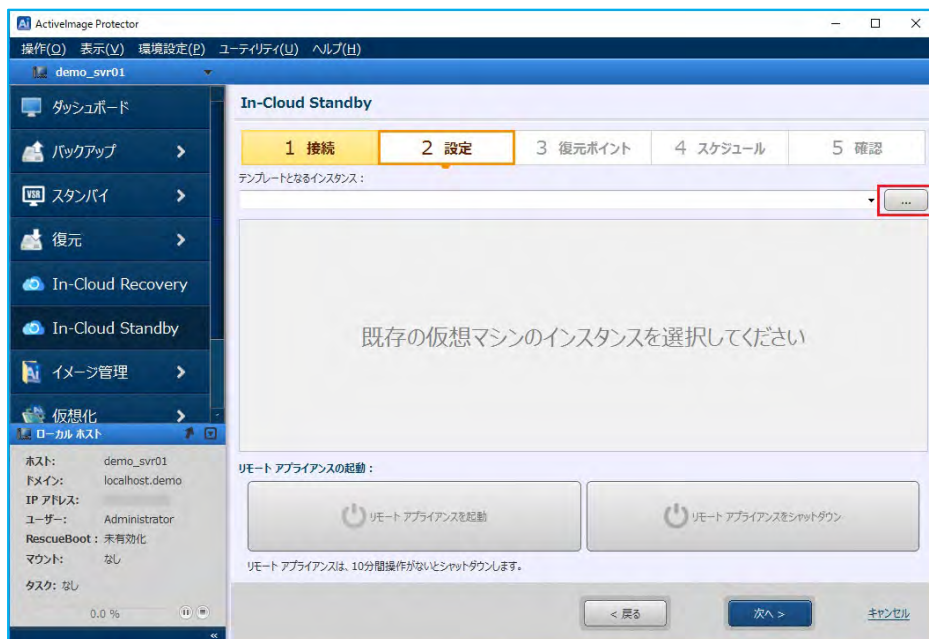
仮想スタンバイマシンの作成 (In-Cloud Standby)

2. 接続するクラウドサービスを選択し、必要な認証情報を入力します。

ここでの設定例として、クラウドサービスに [Amazon AWS] を選択して、AWS の [アクセスキー] と [シークレットキー] を入力し、[リージョン] を選択して [次へ] をクリックします。



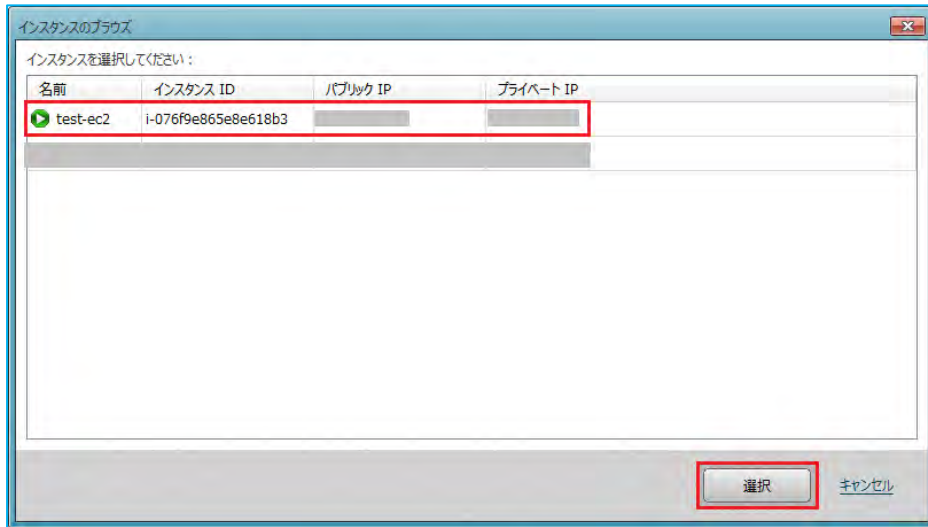
3. テンプレートとなるインスタンスを指定します。 [...] をクリックします。



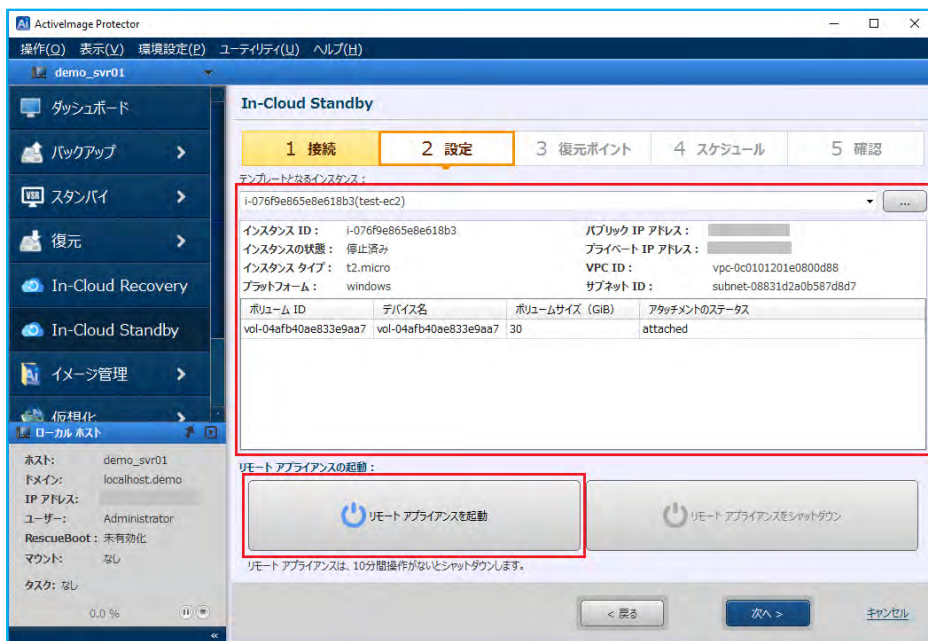
仮想スタンバイマシンの作成 (In-Cloud Standby)

4. テンプレートとなるインスタンスを選択します。

ここでの設定例として、バックアップ元のインスタンス「test-ec2」を選択し、[選択] をクリックします。

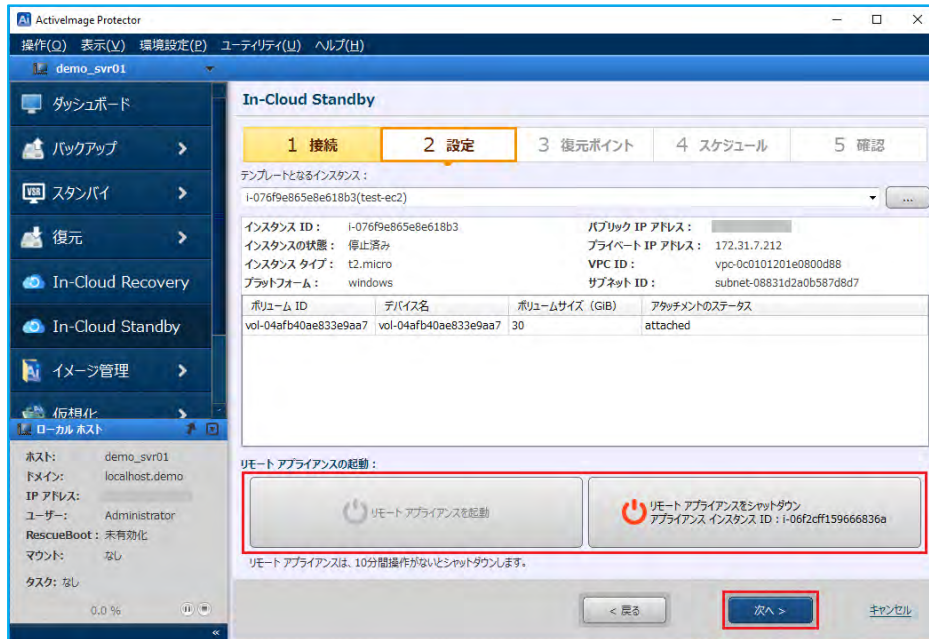


5. テンプレートとなるインスタンスの情報が表示されます。次に、[リモートアプライアンスを起動] をクリックし、「Actiphy Cloud エージェント (起動環境)」を起動します。起動するまでしばらく待ちます。

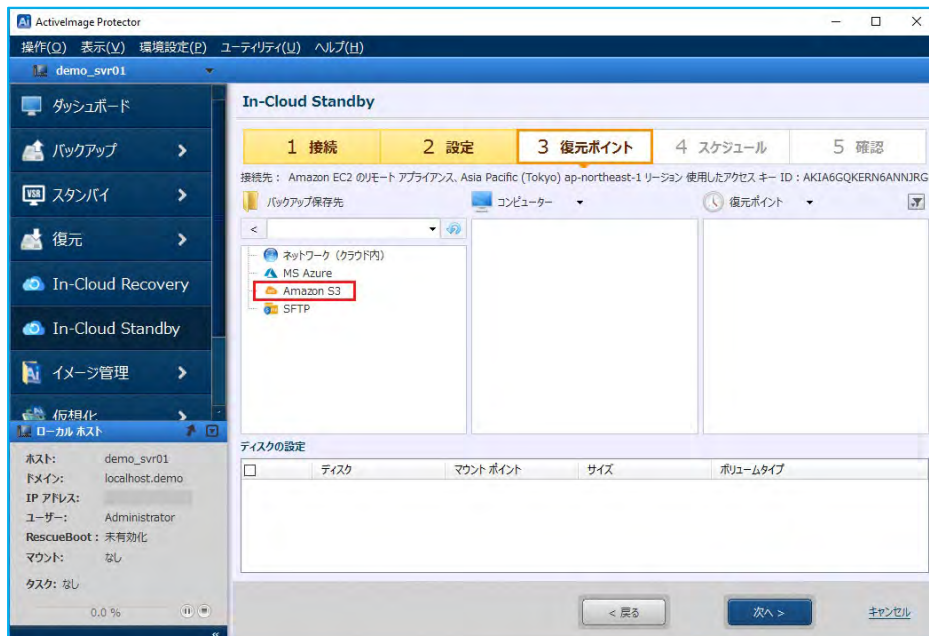


仮想スタンバイマシンの作成 (In-Cloud Standby)

6. 以下の様に、[リモートアプライアンスを起動] ボタンがグレーアウトされ、[リモートアプライアンスをシャットダウン] ボタンが選択可能になったら、「Actiphy Cloud エージェント (起動環境)」の起動は完了です。[次へ] をクリックします。

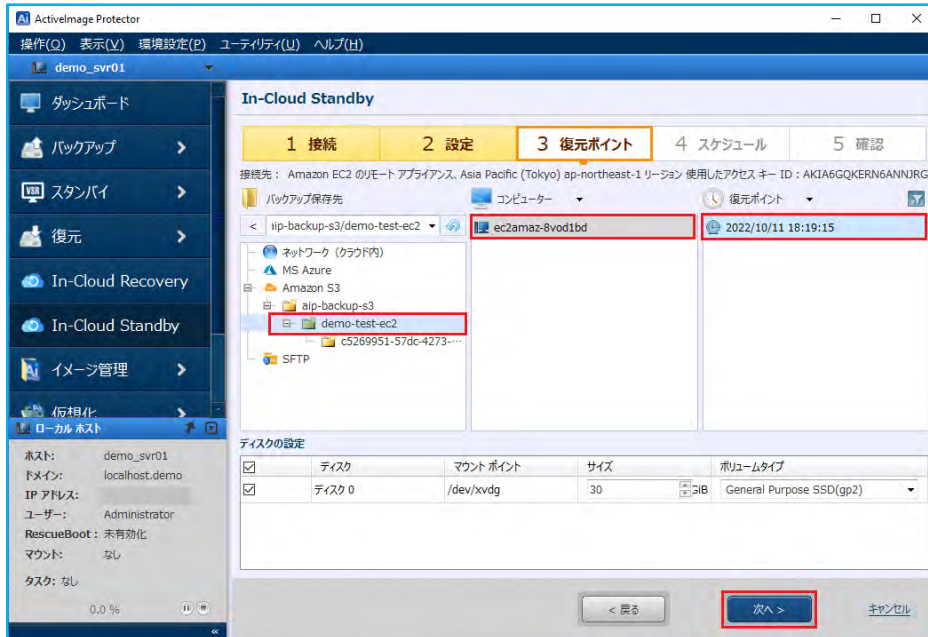


7. バックアップ元のインスタンスのバックアップ保存先を選択します。
 ここでの設定例として、[バックアップ保存先] は [Amazon S3] をクリックします。Amazon S3 の認証情報の入力を求められた場合は、AWS の [アクセスキー] と [シークレットキー] を入力し、[リージョン] を選択して [接続] をクリックします。

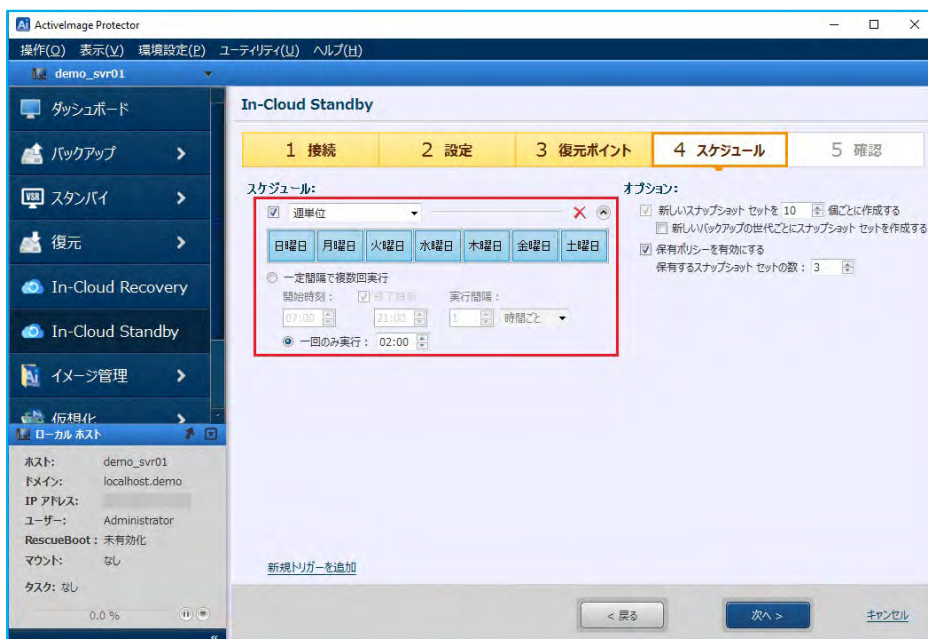


仮想スタンバイマシンの作成 (In-Cloud Standby)

8. バックアップ保存先の「フォルダー」→「コンピューター」→「復元ポイント」(ベースバックアップ)を選択して、[次へ]をクリックします。



9. ActivImage Protector は、週単位、月単位、指定曜日など柔軟なスケジュール設定を行うことができます。ここでの設定例として、「週単位」を選択して日曜日から土曜日の午前2時にバックアップからスナップショットを作成するスケジュール設定を行います。スケジュール タスク実行時に、バックアップごとにスナップショットが作成されます。例えば、スケジュール実行時にスナップショットが作成されていないバックアップが2つ存在したら、2つのスナップショットが作成されます。また、スナップショットが作成されていない、あたらしいバックアップが存在しない場合は、スケジュール タスクはスキップされます。



仮想スタンバイマシンの作成 (In-Cloud Standby)

10. 次に、[オプション:] でスナップショットの世代管理の設定を行います。以下の設定が完了したら、[次へ] をクリックします。

(1) 新しいスナップショット セットを xx 個ごとに作成する

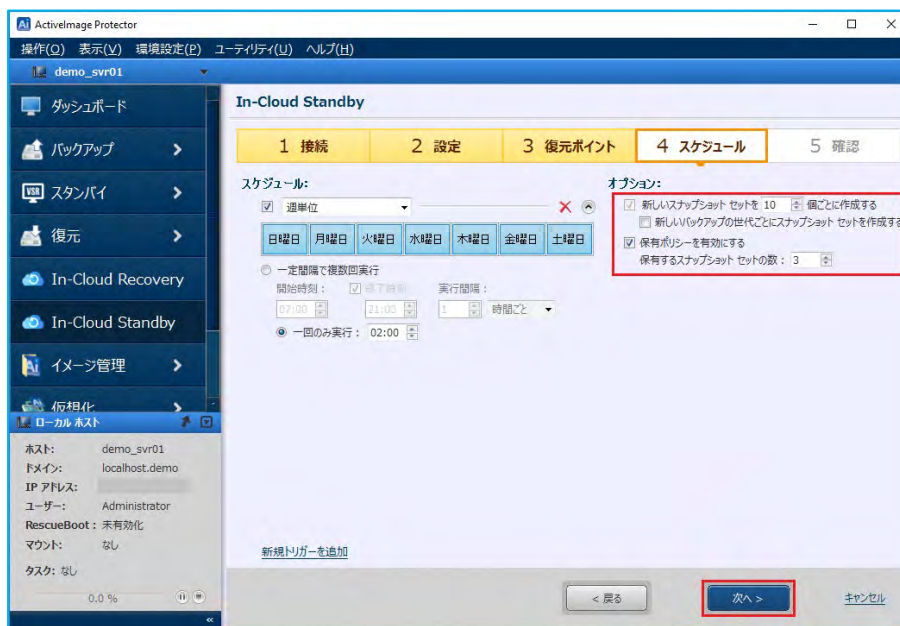
スナップショット セットとして管理するスナップショットの数を設定します。ここでの設定例として、10 と設定し、10 個のスナップショットを 1 世代として管理します。

(2) 新しいバックアップの世代ごとにスナップショット セットを作成する

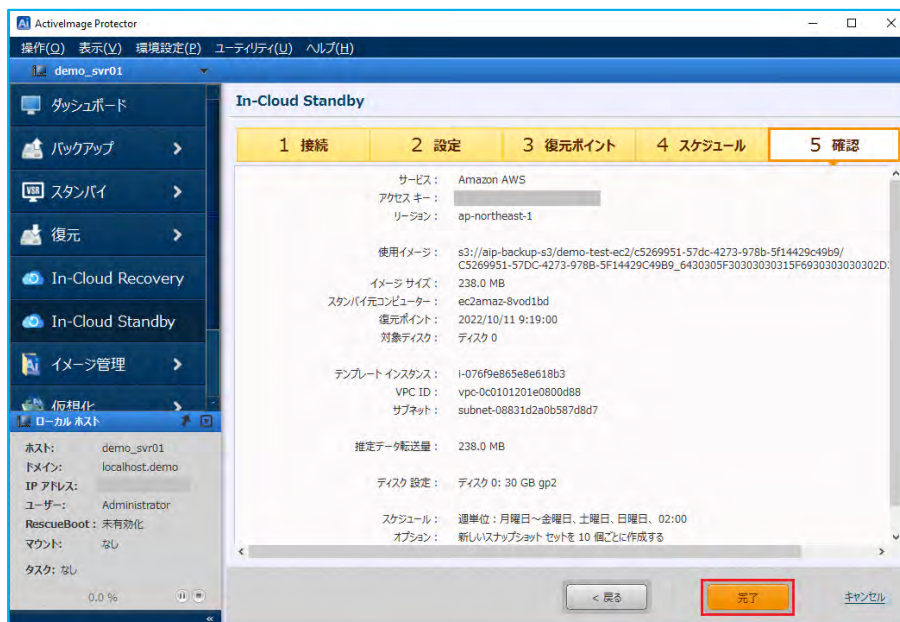
バックアップの世代ごとにスナップショット セットが作成されます。

(3) 保有ポリシーを有効

保有するスナップショット セットの数を設定します。ここでの設定例として、デフォルトの 3 と設定し、クラウド上に 3 世代分のスナップショット セットを残します。

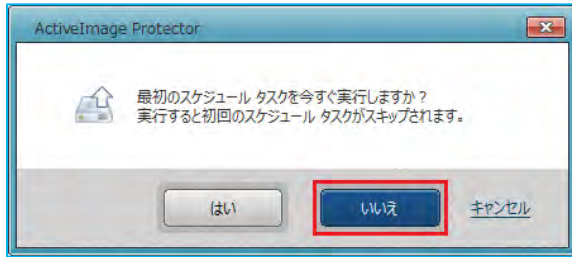


11. 設定内容を確認してから [完了] をクリックします。

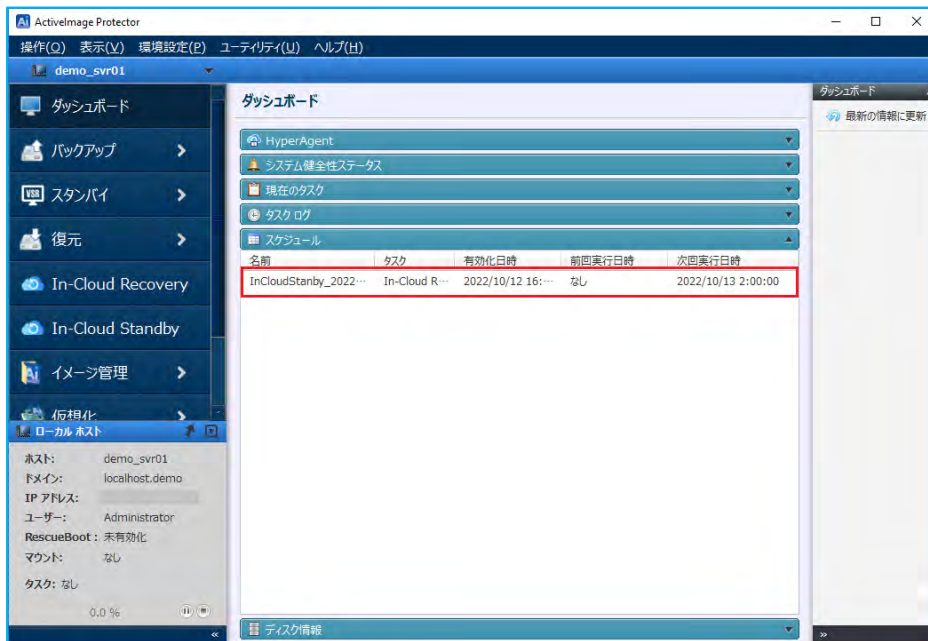


仮想スタンバイマシンの作成 (In-Cloud Standby)

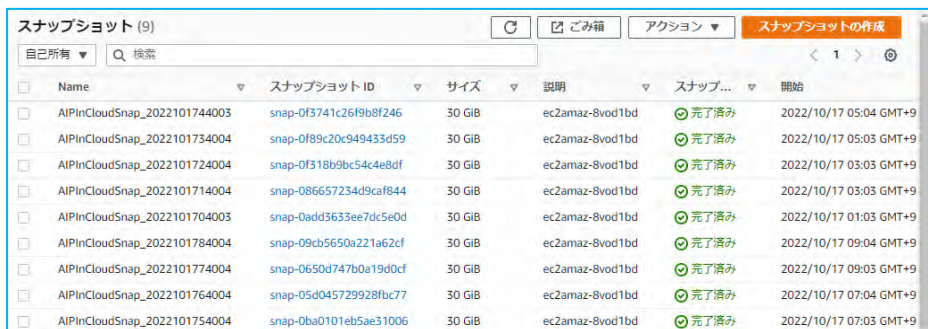
12. スケジュール タスク実行の確認メッセージが表示されますので、[いいえ] をクリックして、ダッシュボードに戻ります。[はい] をクリックすると最初のスケジュール タスクが実行されます。



13. 作成済みのスケジュールは、[ダッシュボード] → [スケジュール] で確認できます。指定した時刻になると、バックアップからスナップショットが作成されます。

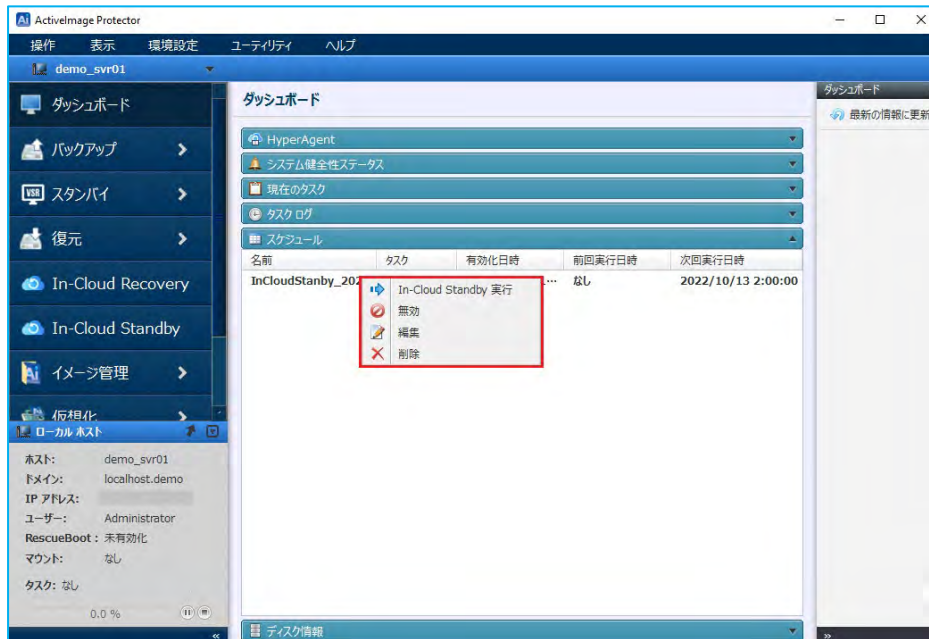


14. 作成されたスナップショットは、[AIPIInCloudSnap_YYYYMMDDhhmmss] の形式で名前がつきます。



仮想スタンバイマシンの作成 (In-Cloud Standby)

15. [スケジュール名] を右クリックすると、直ちに In-Cloud Standby の実行やスケジュールの編集などを行うことができます。



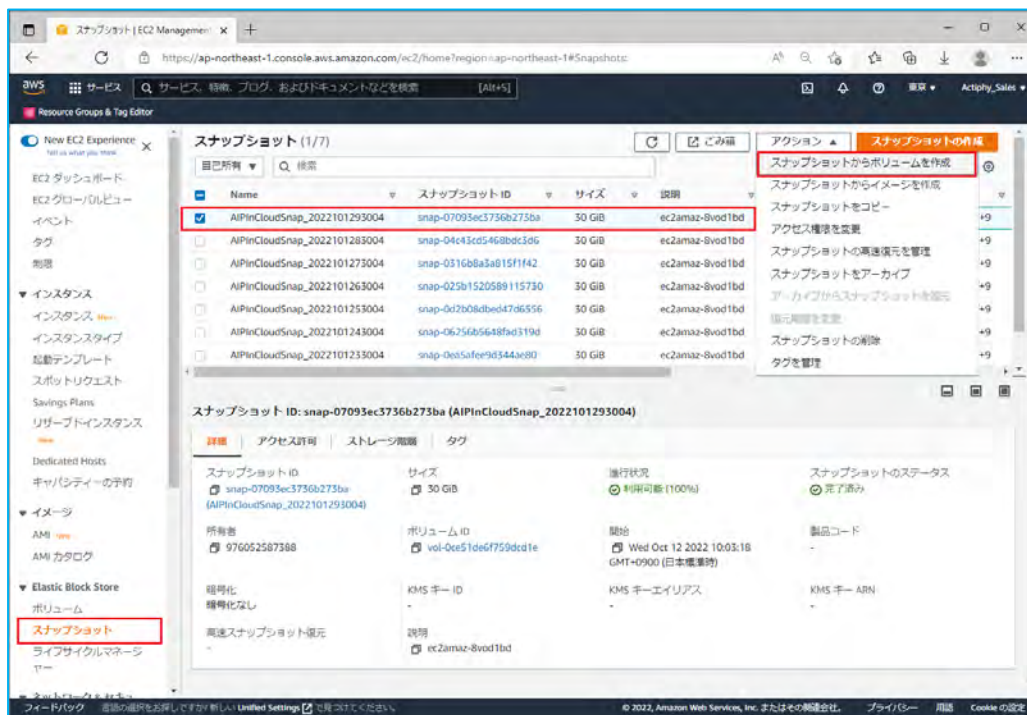
5-2. スナップショットからボリューム作成とアタッチ

AWS マネジメントコンソールから、「In-Cloud Standby」が作成したスナップショットよりボリュームを作成し、新規作成のインスタンスへのボリュームのアタッチ手順など、一連のシステム復旧手順について説明します。
※AWS マネジメントコンソールの画面は変わる可能性があります。基本的な操作手順として参考にしてください。

1. スナップショットからボリュームを作成します。

AWS マネジメントコンソールのメニューから、「EC2」→「スナップショット」を選択し、復旧したい時点のスナップショットにチェックを入れ、「アクション」のプルダウンメニューから「スナップショットからボリュームを作成」をクリックします。

ここでの設定例として、「In-cloud Standby」が作成したホスト名「ec2amaz-8vod1bd」の最新のスナップショットを選択します。



2. 以下のボリューム設定をおこないます。

(1) ボリューム設定

ボリュームの作成先は、そのボリュームをアタッチするインスタンスのアベイラビリティゾーンと合わせる必要があります。ここでの設定例として、アベイラビリティゾーンは「ap-northeast-1c」を選択します。その他は、特に指定がない場合はそのまま問題ありません。

ボリューム設定

スナップショット ID
snap-07093ec3736b273ba (APIInCloudSnap_2022101293004)

ボリュームタイプ 情報
汎用 SSD (gp2)

サイズ (GiB) 情報
30
最小: 1 GiB、最大: 16384 GiB。値は整数である必要があります。

IOPS
100 / 3000
1 GiB あたり 3 IOPS のベースライン、最小 100 IOPS、3000 IOPS にバースト可能。

スループット (MiB/秒) 情報
該当しません

アベイラビリティゾーン 情報
ap-northeast-1c

高速スナップショット復元 情報
☒ 選択されたスナップショットでは有効になっていません

暗号化 情報
EC2 インスタンスに関連付けられた EBS リソースの暗号化ソリューションとして、Amazon EBS 暗号化を使用します。
☐ このボリュームを暗号化する

(2) タグ - オプションの設定

ここでの設定例として、ボリューム名を「test-ec2-standby」に設定します。

[キー] に「Name」、[値 - オプション] に「test-ec2-standby」を入力します。ボリューム作成のすべての設定が完了したら、[ボリューム作成] をクリックします。

タグ - オプション 情報
タグは、AWS リソースに割り当てられるラベルです。各タグはキーとオプションの値で構成されています。タグは、リソースの検索とフィルタリング、および AWS のコストの追跡に使用できます。

キー
Name

値 - オプション
test-ec2-standby

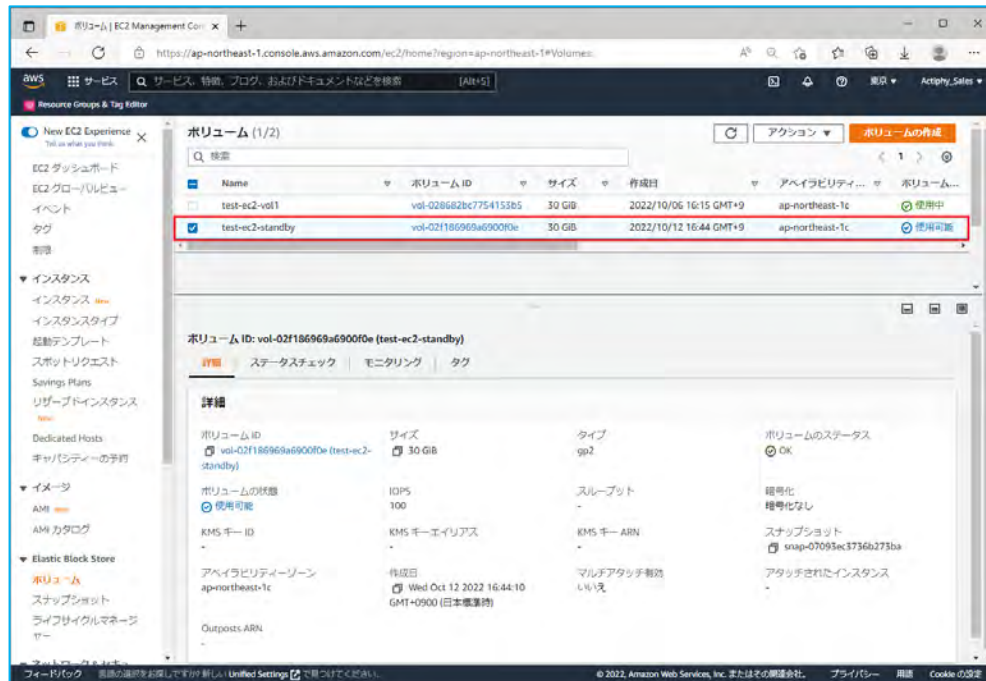
削除

タグを追加
さらに 49 個のタグを追加できます。

キャンセル ボリュームの作成

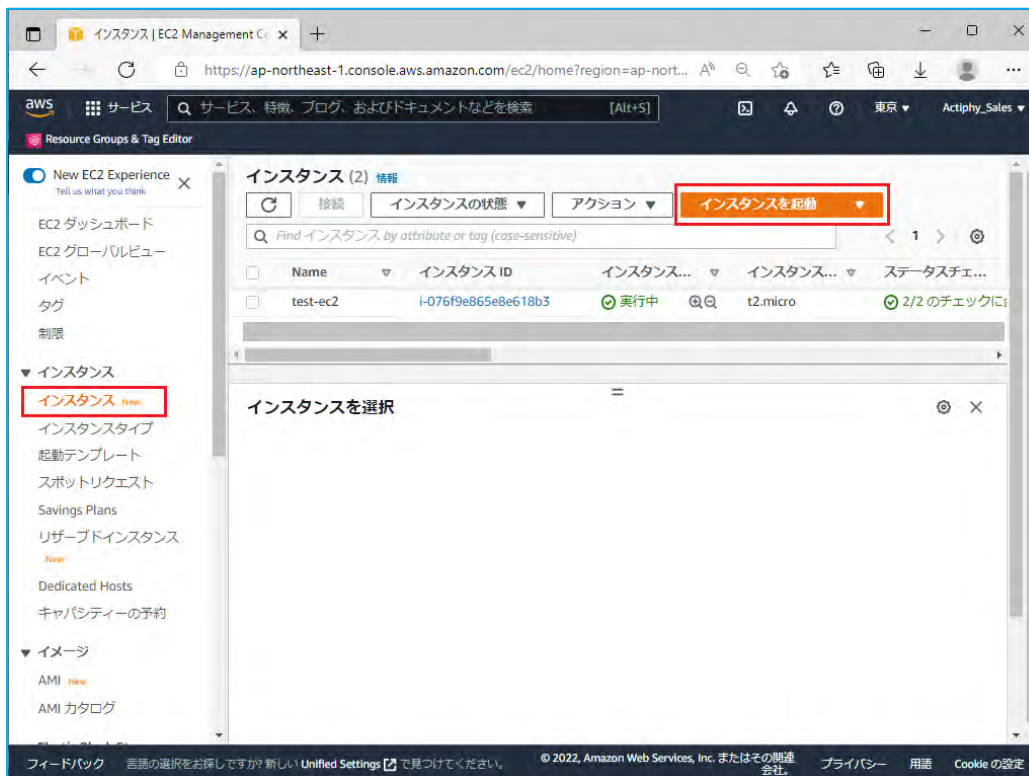
仮想スタンバイマシンの作成 (In-Cloud Standby)

(3) 以下の様に「test-ec2-standby」という名前のボリュームが作成されます。



3. インスタンスを新規に作成します。

AWS マネジメントコンソールのメニューから、「EC2」→「インスタンス」を選択し、「インスタンスを起動」をクリックするとインスタンス作成画面が表示されます。



仮想スタンバイマシンの作成 (In-Cloud Standby)

- (1) 「名前とタグ」は、インスタンスに任意の名前を設定します。ここでの設定例として、インスタンス名を「test-ec2-standby」とします。

名前とタグ 情報

名前

test-ec2-standby

さらにタグを追加

- (2) 「アプリケーションおよび OS イメージ (Amazon マシンイメージ)」は、仮想マシンのイメージを選択します。ここでの設定例として、バックアップ元のインスタンスと同じ「Windows Server 2016 Japanese Full Base」を選択します。

▼ アプリケーションおよび OS イメージ (Amazon マシンイメージ) 情報

AMI は、インスタンスの起動に必要なソフトウェア設定 (オペレーティングシステム、アプリケーションサーバー、アプリケーション) を含むテンプレートです。お探しのものが以下に表示されない場合は、AMI を検索または参照してください。

Q 何千ものアプリケーションイメージと OS イメージを含むカタログ全体を検索します。

カタログからの AMI | 最新 | クイックスタート

Amazon マシンイメージ (AMI)

Windows_Server-2016-Japanese-Full-Base-2022.09.14
ami-0e5e6cd3680e5aa0e

検証済みプロバイダー

その他の AMI を開
覧する

AWS、Marketplace、
コミュニティからの
AMI 有効

カタログ	発行済み	アーキテクチャ	仮想化	ルートデバイス タイプ	検証済み プロバイダー
コミュニティ AMI	2022-09- 14T19:00:09.0 00Z	x86_64	hvm	ebs	はい

- (3) 「インスタンスタイプ」は、インスタンスタイプを選択します。ここでの設定例として、バックアップ元のインスタンスと同じ「t2.micro」を選択します。

▼ インスタンスタイプ 情報

インスタンスタイプ

t2.micro

無料利用枠の対象

インスタンスタイプを比較

ファミリー: t2 1 vCPU 1 GiB メモリ
オンデマンド Linux 料金: 0.0152 USD 1 時間あたり
オンデマンド Windows 料金: 0.0198 USD 1 時間あたり

仮想スタンバイマシンの作成 (In-Cloud Standby)

- (4) [キーペア (ログイン)] は、キーペアを選択します。ここでの設定例として、バックアップ元のインスタンスと同じ既存のキーペア「test-ec2-key」を選択します。

▼ キーペア (ログイン) 情報

キーペアを使用してインスタンスに安全に接続できます。インスタンスを起動する前に、選択したキーペアにアクセスできることを確認してください。

キーペア名 - 必須

test-ec2-key ▼

新しいキーペアの作成

Windows インスタンスの場合は、キーペアを使用して管理者パスワードを復号します。その後、復号されたパスワードを使用してインスタンスに接続します。

- (5) [ネットワーク設定] は、セキュリティグループを設定します。ここでの設定例として、バックアップ元のインスタンスと同じ既存のセキュリティグループを選択します。

▼ ネットワーク設定 情報

ネットワーク 情報

vpc-0c0101201e0800d88 | test-ec2-vpc

サブネット 情報

優先順位なし (アベイラビリティゾーンのデフォルトサブネット)

パブリック IP の自動割り当て 情報

有効化

ファイアウォール (セキュリティグループ) 情報

セキュリティグループとは、インスタンスのトラフィックを制御する一連のファイアウォールルールです。特定のトラフィックがインスタンスに到達できるようにルールを追加します。

☐ セキュリティグループを作成する

☒ 既存のセキュリティグループを選択する

共通のセキュリティグループ 情報

セキュリティグループを編集 ▼

launch-wizard-1 sg-0ab413092c7e90814 ✕

VPC: vpc-0c0101201e0800d88

セキュリティグループのルールを比較

ここで追加または削除したセキュリティグループは、すべてのネットワークインターフェイスに追加または削除されます。

- (6) [ストレージ設定] は、特に変更がない場合そのまま問題ありません。新規インスタンス作成の設定がすべて完了したら、[インスタンスを起動] をクリックするとインスタンスが作成されます。

▼ ストレージを設定 情報

アドバンスド

1x 30 GiB gp2 ルートボリューム (Not encrypted)

① 無料利用枠の対象のお客様は、最大 30 GB の EBS 汎用 (SSD) ストレージまたはマグネティックストレージを取得できます。

Add new volume

選択した AMI には、インスタンスで許可されているよりも多くのインスタンスストアボリュームが含まれています。インスタンスからアクセスできるのは、AMI の最初の 0 のインスタンスストアボリュームだけです。

0x ファイルシステム

ファイアウォール (セキュリティグループ)

launch-wizard-1

ストレージ (ボリューム)

1 ボリューム - 30 GiB

① 無料利用枠: 最初の 1 年には、1 か月あたりの無料利用枠による AMI での t2.micro (または t3.micro) が利用できないリージョンでは t3.micro インスタンスの 750 時間の使用、30 GiB の EBS ストレージ、200 万の I/Os、1 GiB のスナップショット、インターネットへの 100 GB の帯域幅が含まれます。

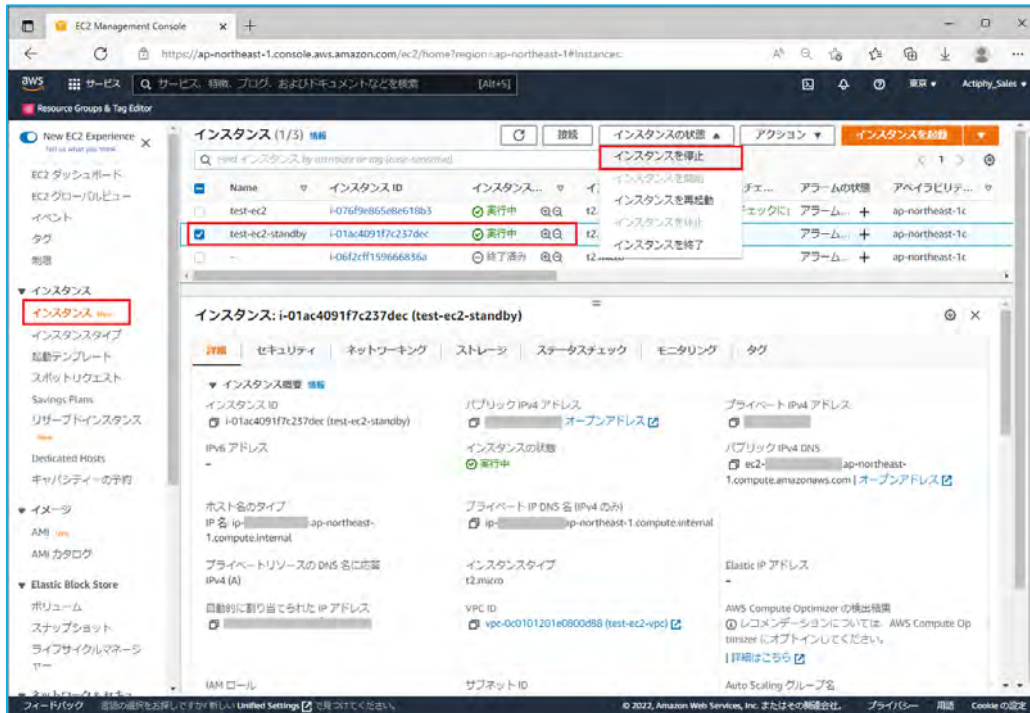
キャンセル

インスタンスを起動

仮想スタバイマシンの作成 (In-Cloud Standby)

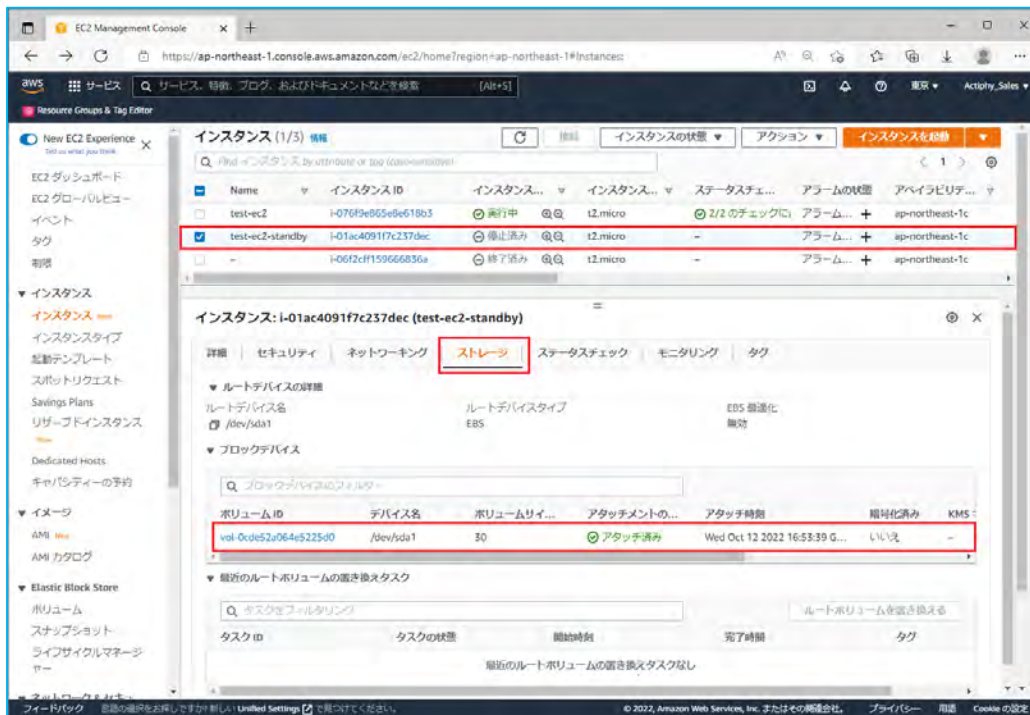
4. ボリュームを入れ替えるために、新規作成のインスタンスを停止します。

ここでの設定例として、AWS マネジメントコンソールのメニューより、[インスタンス] を選択して、新規作成のインスタンス「test-ec2-standby」にチェックを入れ、[インスタンスの状態] のプルダウンメニューから [インスタンスを停止] をクリックします。



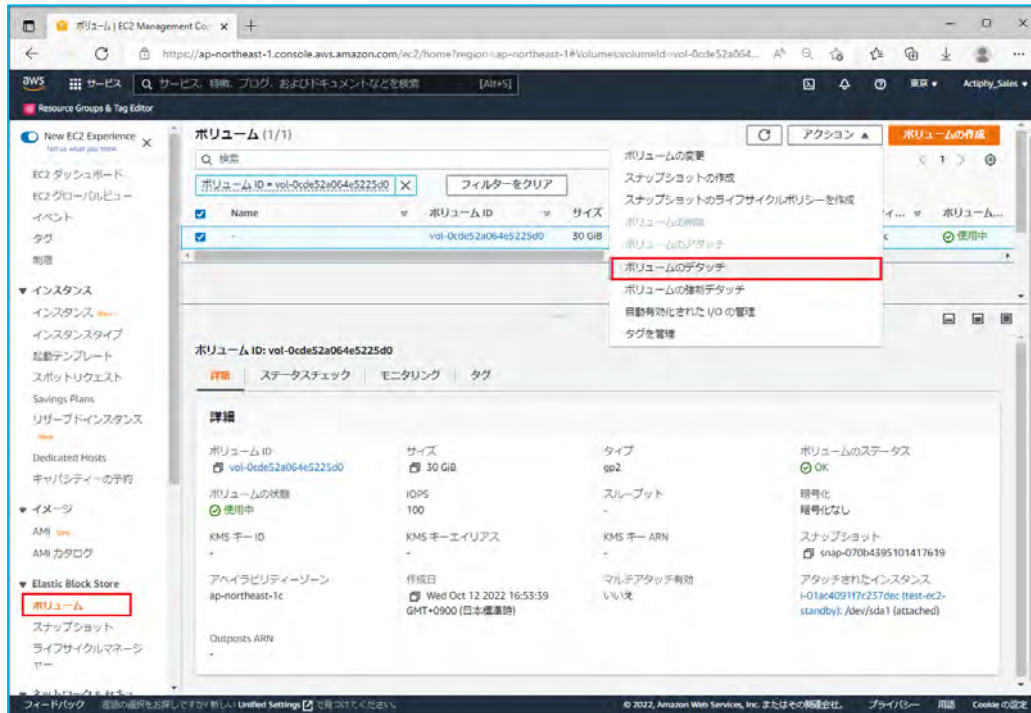
5. 新規作成のインスタンスのルートボリュームをデタッチ（切り離す）します。

デタッチ前に、該当のインスタンスの[ストレージ]タブ内で、ルートデバイス名を確認（ここでは、/dev/sda1）してから、「ボリューム ID」をクリックします。



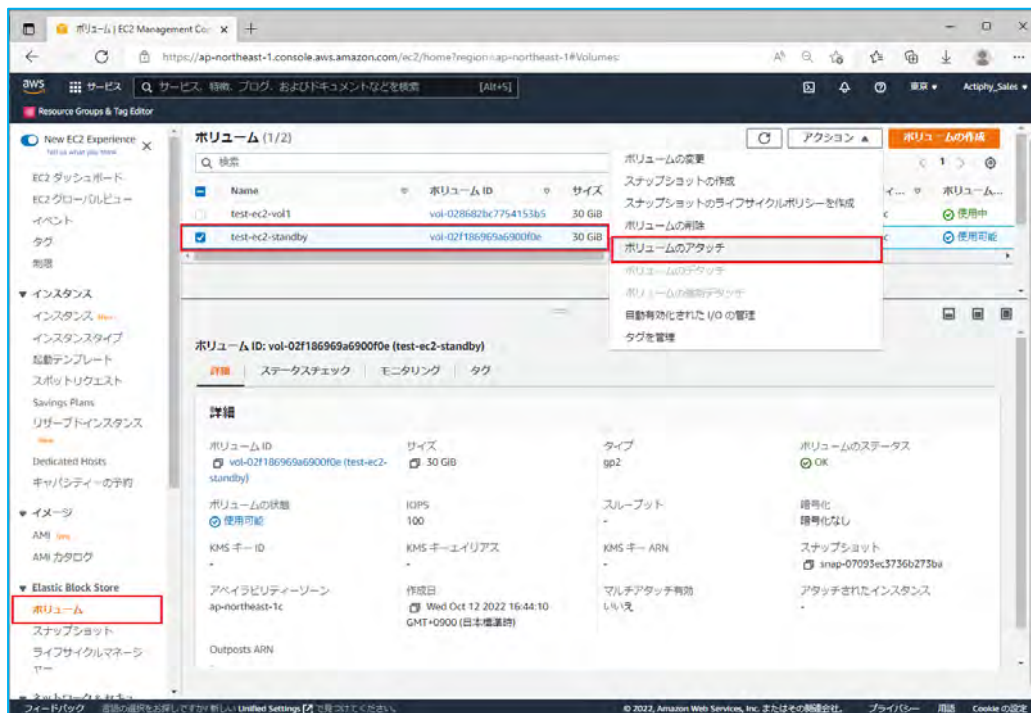
仮想スタンバイマシンの作成 (In-Cloud Standby)

6. 次に、ボリューム設定画面に切り替わったら、[アクション] のプルダウンメニューから [ボリュームのデタッチ] をクリックします。



7. スナップショットから作成したボリュームをアタッチします。

AWS マネジメントコンソールのメニューから、[EC2] → [ボリューム] を選択し、スナップショットから作成したボリュームにチェックを入れ、[アクション] のプルダウンメニューから [ボリュームのアタッチ] をクリックします。



仮想スタンバイマシンの作成 (In-Cloud Standby)

- 作成したボリュームを新規作成のインスタンスへアタッチします。デバイス名は、前項の「5」で確認したデバイス名「/dev/sda1」としてアタッチします。

ボリュームのアタッチ 情報

インスタンスにボリュームをアタッチし、通常の物理ハードディスクドライブと同じように使用します。

基本的な詳細

ボリューム ID
vol-02f186969a6900f0e (test-ec2-standby)

アベイラビリティゾーン
ap-northeast-1c

インスタンス 情報
i-01ac4091f7c237dec

デバイス名 情報
/dev/sda1

Windows 用の推奨デバイス名: ルートボリュームの場合は /dev/sda1。データボリュームの場合は xvd[f-p]。

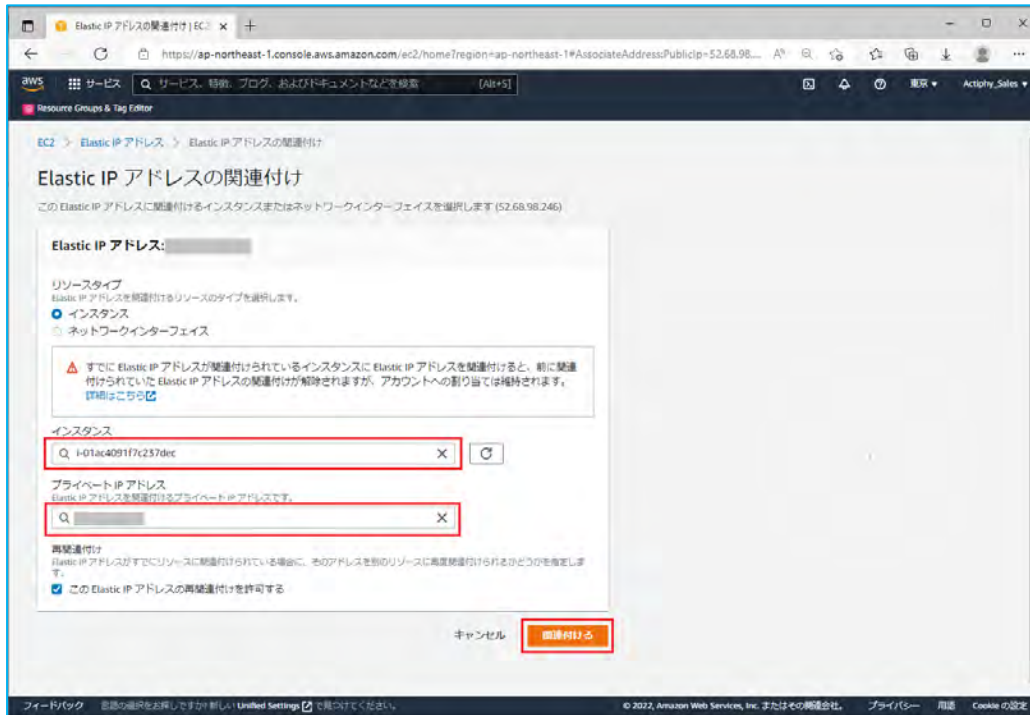
キャンセル ボリュームのアタッチ

- 既存のインスタンスについている Elastic IP を新規インスタンスに再割り当てします。
AWS マネジメントコンソールのメニューから、[EC2] → [Elastic IP] を選択し、既存のインスタンスについている Elastic IP にチェックを入れ、[アクション] のプルダウンメニューから [Elastic IP アドレスの関連付け] をクリックします。

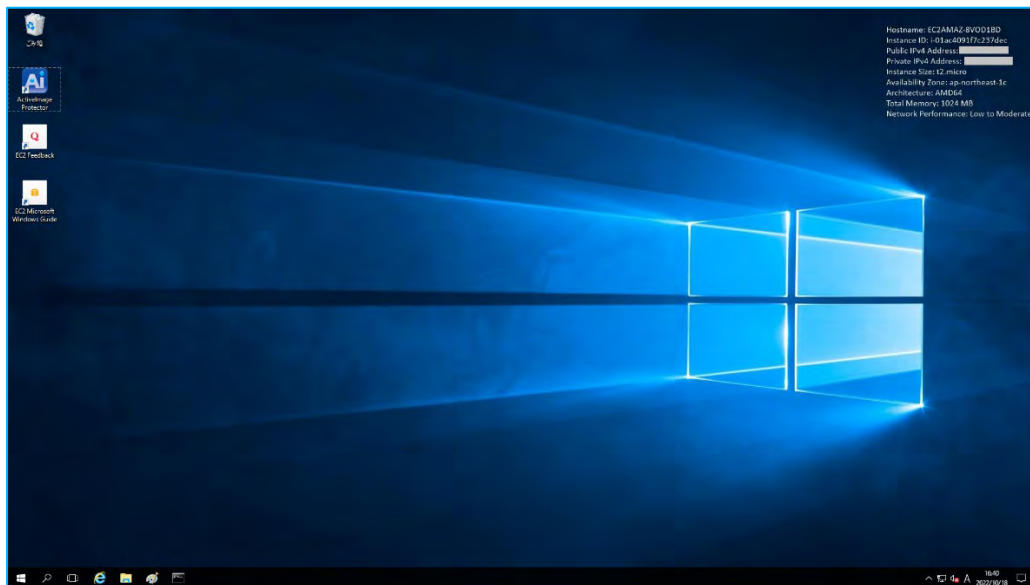
The screenshot shows the AWS Management Console interface for Elastic IP addresses. The left sidebar shows the navigation menu with 'Elastic IP' highlighted. The main content area shows a table of Elastic IP addresses. The first row, 'test-ec2', is selected. The 'Actions' dropdown menu is open, showing the option 'Associate Elastic IP address' (Elastic IP アドレスの関連付け) which is highlighted. Below the table, the details for the selected Elastic IP address are shown, including the public IP address 52.68.98.246 and the associated instance ID i-07b9a865e8e618b5.

仮想スタンバイマシンの作成 (In-Cloud Standby)

10. インスタンスに、新規作成したインスタンスを選択し、再関連付けにチェックを入れて、[関連付ける]をクリックします。



11. 新規作成のインスタンスを起動します。
これで、バックアップから作成したスナップショットから、新規作成のインスタンスへの復旧は完了です。



6. リモート管理コンソール

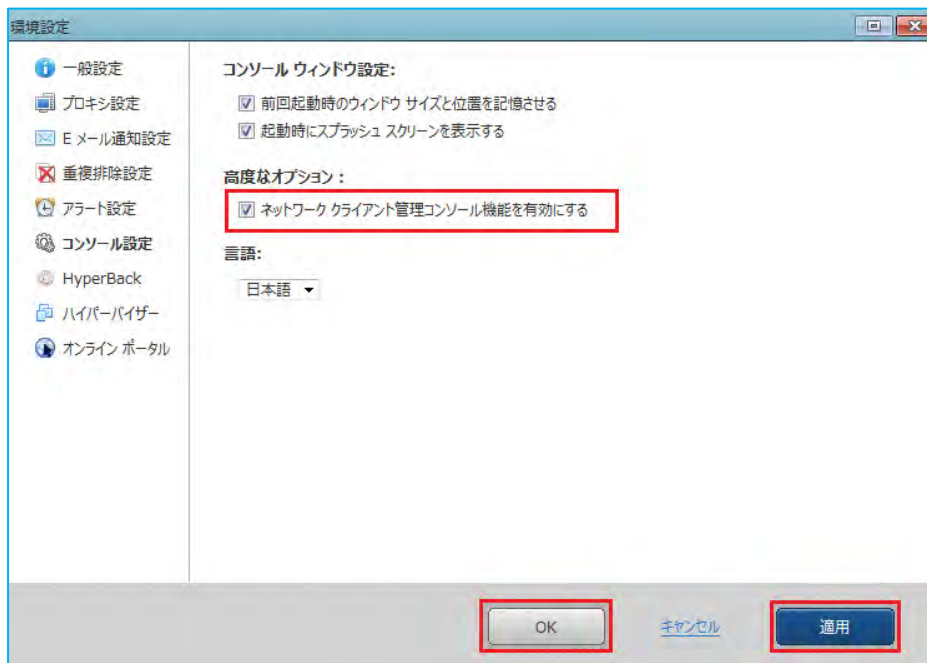
AWS EC2、および Azure のインスタンスにインストールされている ActiveImage Protector の管理をリモートで行うことができます。

1. ActiveImage Protector を起動します。

Windows スタートメニューから [Actiphy] → [ActiveImage Protector] をクリックします。

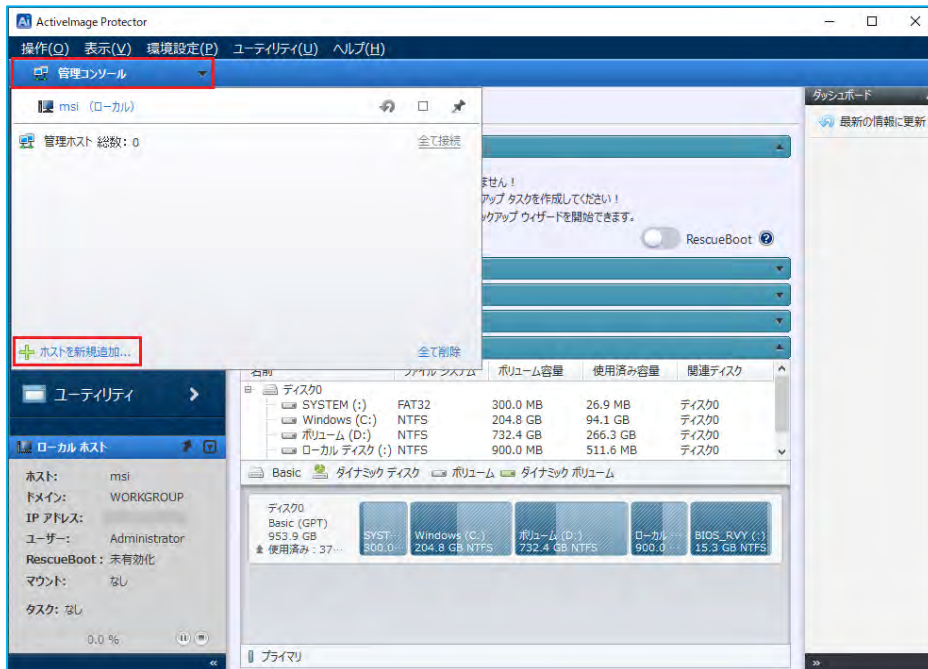
2. 最初に、リモート管理コンソールを使用するためには、ActiveImage Protector の管理コンソールのメニューから、[環境設定] → [コンソール設定] → [ネットワーク クライアント管理コンソール機能を有効にする] にチェックを入れ、[適用] をクリックします。[OK] をクリックしてダッシュボードに戻ります。
また、インスタンスのセキュリティ設定で以下のポートを開放します。（AWS では、セキュリティポリシーのインバウンドルールに追加します。）

- ・TCP ポート 48236
- ・UDP ポート 48238
- ・UDP ポート 48239

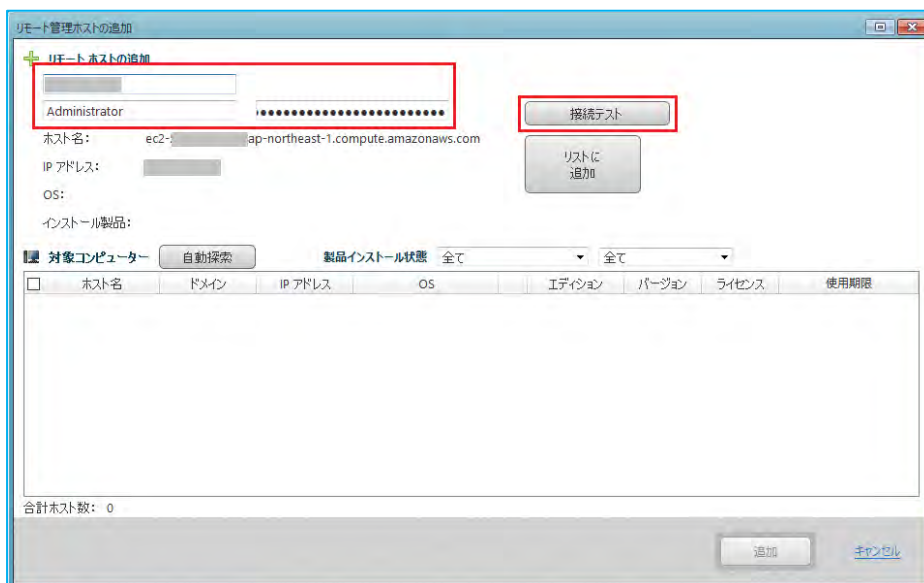


リモート管理コンソール

3. コンソール左上にある「管理コンソール」から操作を行います。リモート管理を行うためには、最初にホストリストを作成します。「ホストを新規追加...」をクリックします。

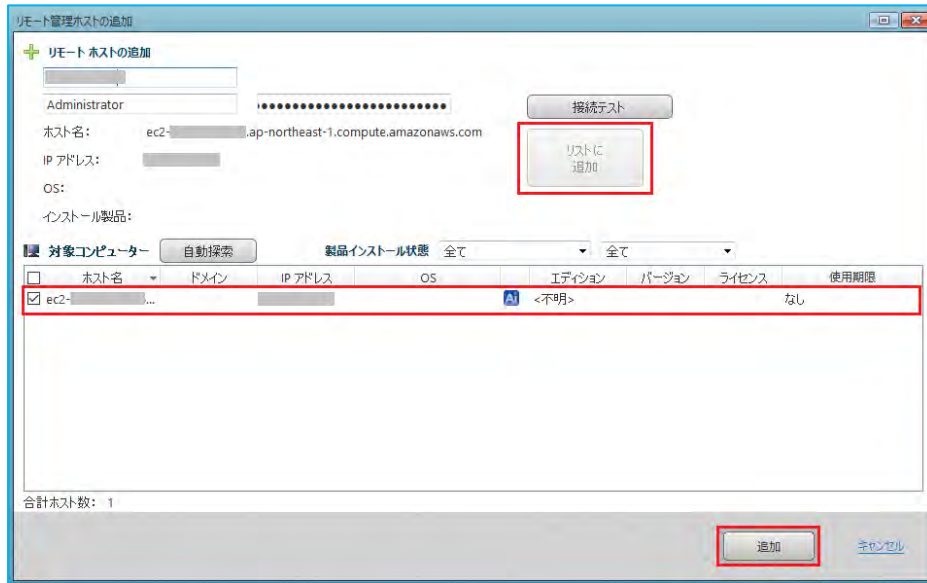


4. リストに追加するホストを指定します。指定方法は「自動検索」と「手動設定」の2つがあります。ここでの設定例として、「リモートホストの追加」から「クラウドのインスタンスのIPアドレス」、「管理者ユーザー名」、「パスワード」を入力し、「接続テスト」をクリックします。接続テストに成功すると「ホスト名」、「IP アドレス」が表示されます。

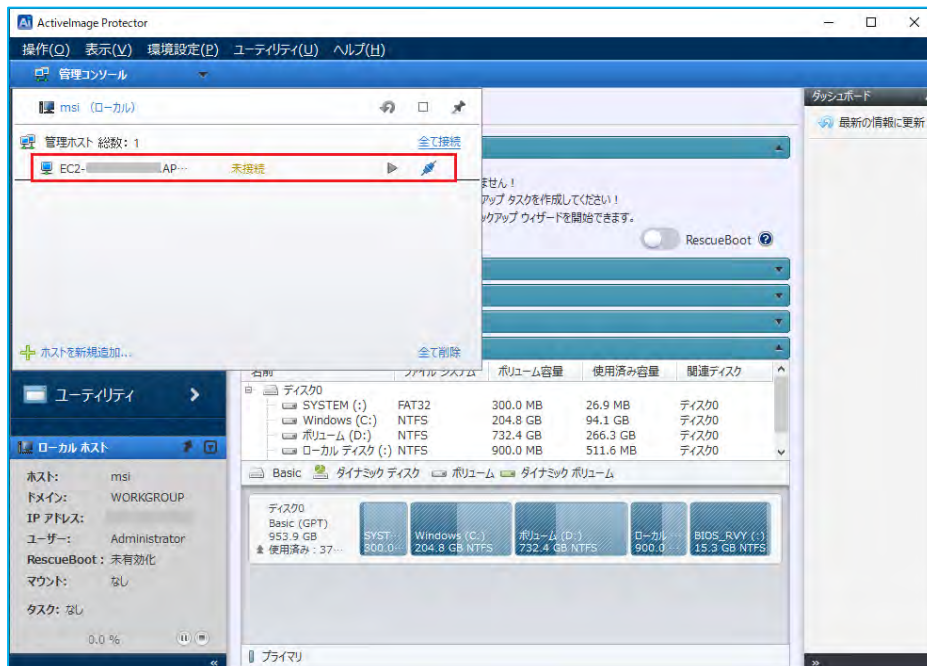


リモート管理コンソール

5. 次に、[リストに追加] をクリックすると、[対象コンピューター] のリストに追加されますので、[追加] をクリックして管理対象コンピューターに登録します。

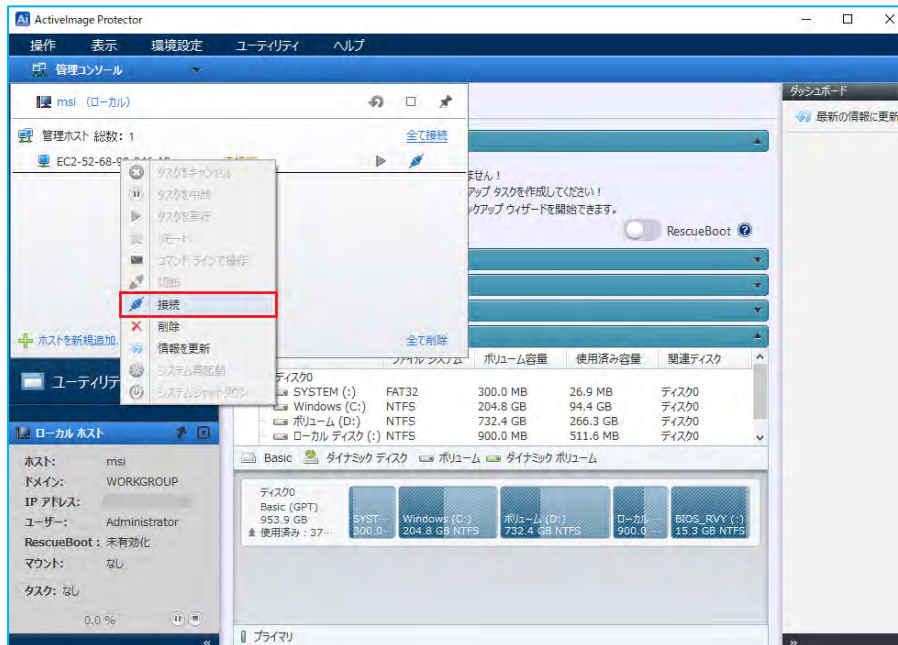


6. 管理対象ホストとして、リモートホストが追加されます。

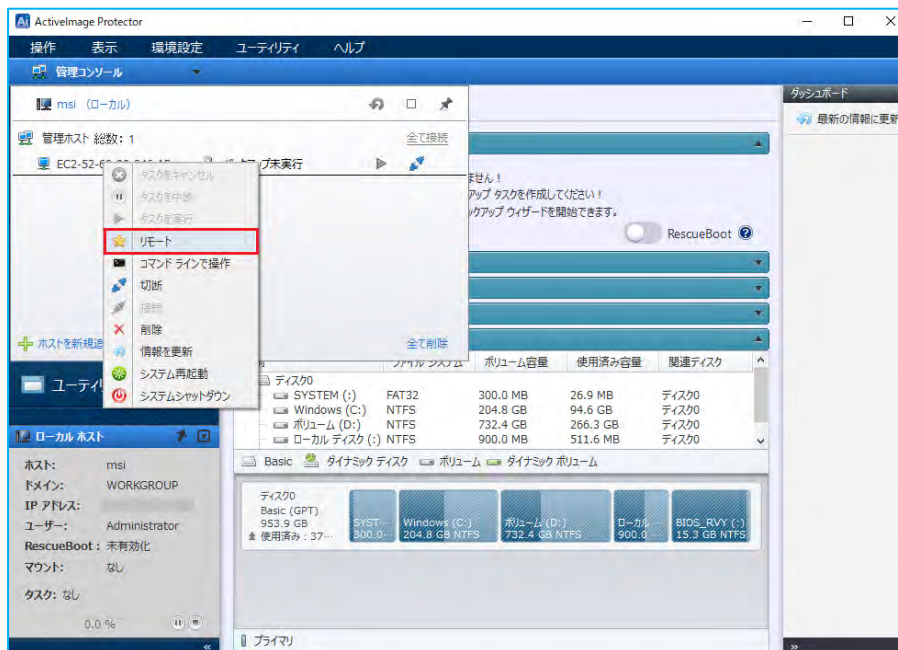


リモート管理コンソール

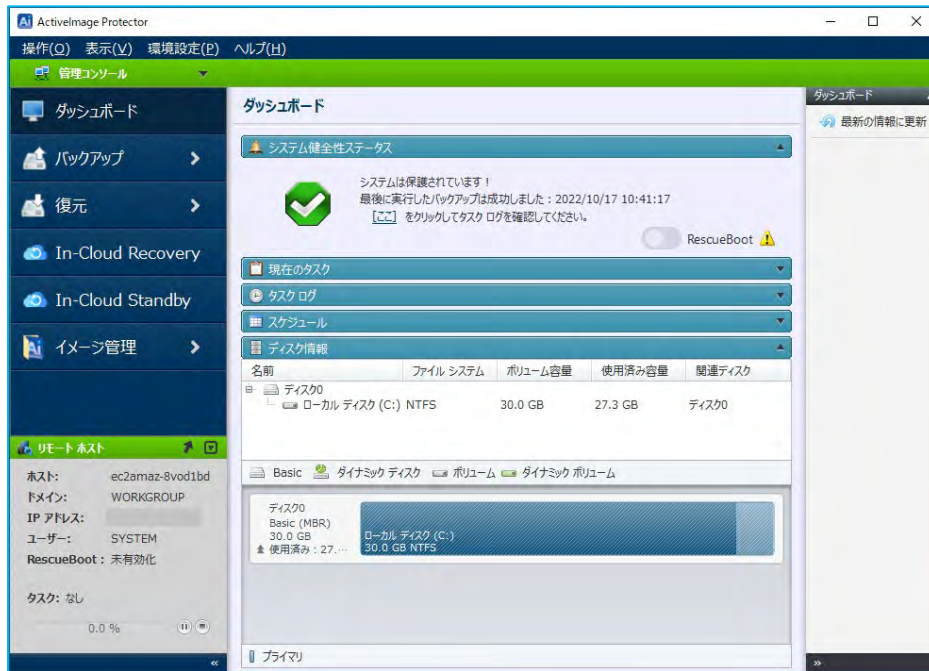
7. ホストリストからホストを選択し、右クリックすると、以下のようなコンテキストメニューが表示されます。ここから、[接続] をクリックします。



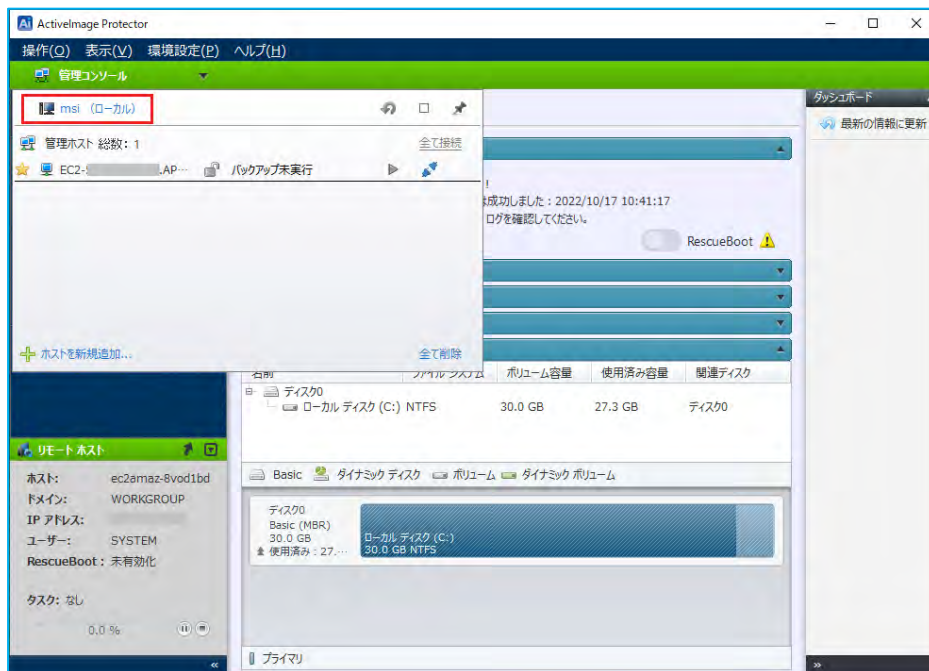
8. ホストリストからホストを選択し、右クリックメニューから [リモート] をクリックするとエージェントにリモート接続できます。



9. 接続に成功すると、ステータスバーの色が緑になります。バックアップスケジュールの作成や復元、イメージ管理などの各種操作、ログ等の閲覧ができます。



10. ローカルホスト名をダブルクリックするとリモートホストへの接続が解除されます。



7. 参考情報

アクティファイの Web サイト

製品情報の他、各種資料やサポート情報、アップデートなど、総合的にご案内しています。

<https://www.actiphy.com>

ActiveImage Protector の FAQ

サポート情報のデータベースです。

<https://jpkb.actiphy.com/>

ActiveImage Protector に関するお問い合わせ先：

株式会社 アクティファイ

営業本部

E-mail: sales@actiphy.com

TEL: 03-5256-0877

FAX: 03-5256-0878

© 2024Actiphy, Inc. 無断複写・転載を禁止します。

本ソフトウェアと付属ドキュメントは株式会社アクティファイに所有権および著作権があります

本ガイド中のその他のブランド名及び製品名は、それぞれ帰属する所有者の商標または登録商標です。