

# Acronis Access

## インストールおよびア ップグレード ガイド



## 著作権情報

Copyright © Acronis International GmbH, 2002-2014. All rights reserved.

「Acronis」および「Acronis セキュア ゾーン」は、Acronis International GmbH の登録商標です。

「Acronis Compute with Confidence」、「Acronis Startup Recovery Manager」、「Acronis Active Restore」、「Acronis Instant Restore」、および Acronis ロゴは、Acronis International GmbH の商標です。

Linux は、Linus Torvalds の登録商標です。

VMware および VMware Ready は、VMware, Inc. の米国ならびにその他の地域における商標または登録商標です。

Windows および MS-DOS は、Microsoft Corporation の登録商標です。

ここに記載されているその他すべての商標および著作権は、それぞれの権利所有者に帰属します。

著作権所有者の明示的な許可なく本ドキュメントの実質的な修正版を配布することは禁止されています。

著作権所有者からの事前の許可がない限り、いかなる形態（紙媒体など）であっても商業目的で本ドキュメントまたはその派生物を配布することは禁止されています。

ドキュメントは、「現状のまま」で提供され、商品性に対する黙示的保証、特定の目的に対する適合性、権利を侵害していないことなどを含む明示的または黙示的な条件、言明、および保証に関する責任を負いません（免責条項の範囲が法的に無効と見なす場合を除く）。

本ソフトウェアまたはサービスにサードパーティのコードが付属している場合があります。サードパーティのライセンス条項の詳細については、ルート インストール ディレクトリにある license.txt ファイルをご参照ください。本ソフトウェアまたはサービスと共に使用するサードパーティ コードおよび関連するライセンス条項の最新の一覧については、<http://kb.acronis.com/content/7696> をご参照ください。

## Acronis の特許取得済みの技術

この製品で使用されている技術は、以下の番号の米国特許のうち 1 つ以上の保護対象です。  
7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533;  
7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064;  
7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815;  
8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137;  
8,484,427; 8,645,748; 8,732,121 および出願中特許。

## 目次

|   |            |
|---|------------|
| <b>1 インストール .....</b>   | <b>5</b>   |
| 1.1 要件 .....  | 5          |
| 1.1.1 オペレーティング システムの要件 .....  | 5          |
| 1.1.2 モバイル クライアントの要件 .....  | 5          |
| 1.1.3 推奨される最小ハードウェア構成 .....   | 6          |
| 1.1.4 ネットワーク要件 .....  | 6          |
| 1.1.5 デスクトップ クライアント要件 .....   | 7          |
| 1.2 サーバーに Acronis Access Advanced をインストールする .....                                   | 8          |
| 1.3 設定ユーティリティの使用 .....  | 10         |
| 1.4 セットアップ ウィザードの使用 .....   | 14         |
| 1.5 Acronis Access のクラスタリング .....   | 20         |
| 1.6 Acronis Access の負荷分散 .....  | 20         |
| <b>2 Microsoft フェールオーバー クラスタ上での Acronis Access のインストール.....</b>                     | <b>20</b>  |
| 2.1 Windows 2003 Microsoft フェールオーバー クラスタ上での Acronis Access<br>のインストール .....         | 21         |
| 2.2 Windows 2008 Microsoft フェールオーバー クラスタ上での Acronis Access<br>のインストール .....         | 36         |
| 2.3 Windows 2012 Microsoft フェールオーバー クラスタ上での Acronis Access<br>のインストール .....         | 50         |
| <b>3 アップグレード .....</b>  | <b>65</b>  |
| 3.1 Acronis Access の新しいバージョンへのアップグレード .....   | 65         |
| 3.2 Acronis Access Advanced へのアップグレード .....   | 66         |
| 3.3 mobilEcho バージョン 4.5 以前からのアップグレード .....  | 67         |
| 3.3.1 開始する前に .....  | 67         |
| 3.3.2 アップグレード プロセス .....  | 75         |
| 3.3.3 mobilEcho 4.5 へのダウングレード .....   | 110        |
| 3.4 activEcho バージョン 2.7 以前からのアップグレード .....  | 111        |
| 3.4.1 開始する前に .....  | 111        |
| 3.4.2 アップグレード プロセス .....  | 112        |
| 3.5 クラスタ構成のアップグレード .....  | 133        |
| <b>4 Microsoft フェールオーバー クラスタ上での Acronis Access のアップグレード....</b>                     | <b>135</b> |
| <b>5 Microsoft フェールオーバー クラスタでの mobilEcho 4.5 からのアップグレード....</b>                     | <b>138</b> |
| 5.1 Windows 2003 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis<br>Access にアップグレードする ..... | 138        |
| 5.2 Windows 2008 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis<br>Access にアップグレードする ..... | 151        |
| 5.3 Windows 2012 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis<br>Access にアップグレードする ..... | 162        |

|          |  |            |
|----------|--|------------|
| <b>6</b> | <b>クイック スタート: モバイル アクセス .....</b>        | <b>178</b> |
| 6.1      | 初期設定.....                                | 178        |
| 6.2      | 最初のゲートウェイ サーバーとデータ ソースの構成 .....          | 183        |
| 6.3      | ポリシーの設定 .....                            | 185        |
| 6.4      | Access モバイル クライアント アプリケーションのインストール ..... | 186        |
| 6.5      | クライアント管理での登録.....                        | 187        |
| <b>7</b> | <b>クイック スタート: 同期と共有 .....</b>            | <b>192</b> |
| 7.1      | 初期設定.....                                | 192        |
| 7.2      | ファイルにアクセスするためのウェブ インターフェイスの使用 .....      | 197        |
| 7.3      | デスクトップ クライアントの使用 .....                   | 202        |

# 1 インストール

## セクションの内容

|   |    |
|---|----|
| 要件 .....                                      | 5  |
| サーバーに Acronis Access Advanced をインストールする ..... | 8  |
| 設定ユーティリティの使用 .....                            | 10 |
| セットアップ ウィザードの使用 .....                         | 14 |
| Acronis Access のクラスタリング .....                 | 20 |
| Acronis Access の負荷分散 .....                    | 20 |

## 1.1 要件

Acronis Access をインストールする前に、管理者としてログインする必要があります。サーバーが次の要件を満たしていることを確認します。

### セクションの内容

|                        |   |
|------------------------|---|
| オペレーティング システムの要件 ..... | 5 |
| モバイル クライアントの要件 .....   | 5 |
| 推奨される最小ハードウェア構成 .....  | 6 |
| ネットワーク要件 .....         | 6 |
| デスクトップ クライアント要件 .....  | 7 |

### 1.1.1 オペレーティング システムの要件

#### 推奨:

Windows 2012(すべてのエディション)

Windows 2008 R2 64 ビット

#### サポート対象:

Windows 2012 R2

Windows 2012(Standard Edition および Datacenter Edition)

Windows 2008(各エディション、32/64 ビット版)

---

**注意:** テスト用にシステムをインストールして、Windows 7 以降で実行することができます。これらのデスクトップ クラスの構成は、本番環境ではサポートされません。

---

### 1.1.2 モバイル クライアントの要件

モバイル クライアント アプリケーションは、次のものと互換性があります。

#### サポートされるデバイス:

- Apple iPad 第 2 世代、第 3 世代、第 4 世代、Air、Air 2
- Apple iPad Mini 第 1 世代、第 2 世代、第 3 世代
- Apple iPhone 3GS、4、4S、5、5s、5c、6、6 Plus
- Apple iPod Touch 第 4 世代、第 5 世代
- Android のスマートフォンおよびタブレット(x86 プロセッサ アーキテクチャのデバイスはサポートされていません)

### サポートされる OS:

- iOS 6 以降
- Android 2.2 以降(x86 プロセッサ アーキテクチャのデバイスはサポートされていません)

**Acronis Access アプリケーションは次のウェブ サイトからダウンロードできます。**

- iOS の場合 <http://www.grouplogic.com/web/meappstore>
- Android の場合 <https://play.google.com/store/apps/details?id=com.grouplogic.mobilecho>

## 1.1.3 推奨される最小ハードウェア構成

**プロセッサ:** Intel/AMD

---

**注意:** Acronis Access サーバーは仮想コンピュータにインストールできます。

---

**メモリ:**

- 本番環境: 最低 8 GB。これ以上を推奨。
- 試用環境またはテスト環境: 最低 4 GB。8 GB 以上を推奨。

**ディスク領域:**

- ソフトウェアのインストールには、300 MB のディスク領域が必要です。

---

**注意:** Acronis Access インストーラを実行するための十分な領域があることを確認してください。インストーラを実行するには、1 GB の空き領域が必要です。

---

- 同期と共有機能で 사용되는ファイル リポジトリは、デフォルトでローカル コンピュータにインストールされます。
- テスト パラメータを満たすため、十分な空き領域を確保してください。50 GB 以上が推奨です。

## 1.1.4 ネットワーク要件

- 1 つの静的 IP アドレス。一部の構成では、2 つの IP アドレスが必要になることがあります。
- 任意(推奨): 上記の IP アドレスに対応する FQDN。
- Active Directory が使用される場合は、ドメイン コントローラへのネットワーク アクセス。
- 電子メール通知および招待メッセージ用の SMTP サーバーへのネットワーク アクセス。
- アドレス **127.0.0.1** は Access モバイル クライアントの内部で使用するため、VPN、MobileIron、Good Dynamics などのトンネルを経由して転送しないでください。
- Access サーバーまたはゲートウェイ サーバーが実行されているコンピュータはすべて、Windows Active Directory にバインドされていなければなりません。

HTTPS トラフィックを処理する 2 つのコンポーネントとして、ゲートウェイ サーバーと Acronis Access サーバーがあります。ゲートウェイ サーバーは、モバイル クライアントからファイルとデータ ソースの共有の両方にアクセスするのに使われます。Access サーバーは、「同期と共有」クライアントのウェブ ユーザー インターフェイスを提供すると同時に、「モバイル アクセス」と「同期と共有」の両方の管理コンソールにもなります。サーバーに 2 つの IP アドレスを割り当て、これらのアドレスに対して 2 つの別個の DNS エントリを割り当てることをお勧めします。ただし、コンポーネントごとに別ポートを使って、1 つの IP アドレスだけを使用するように、サーバーを構成することもできます。通常モバイル アクセスのみのインストールではこの 1 個の IP アドレス構成で十分ですが、同期と共有も使用する場合は 2 個の IP アドレスを使用することをお勧めします。

モバイル デバイスがファイアウォールの外部からアクセスできるようにする場合は、次のようないくつかのオプションがあります。

- **ポート 443 アクセス:** Acronis Access は暗号化された転送に HTTP を使用するため、ポート 443 で HTTPS トラフィックを許可する一般的なファイアウォール ルールに自然に適合します。ポート 443 から Acronis Access サーバーへのアクセスを許可すると、権限のある iPad クライアントをファイアウォールの内外で接続できます。希望する他のポートを使用するように、Acronis Access を設定することもできます。
- **VPN:** Access モバイル クライアントは VPN 接続を介したアクセスをサポートします。組み込みの iOS VPN クライアントとサードパーティの VPN クライアントの両方がサポートされています。Mobile Device Management (MDM) システムまたは Apple iPhone 構成ユーティリティを使用して iOS 管理プロファイルをオプションでデバイスに適用し、証明書ベースの iOS 「VPN オンデマンド」機能を構成し、Acronis Access サーバーや会社の他のリソースへのシームレスなアクセスを実現できます。
- **リバース プロキシ サーバー:** リバース プロキシ サーバーが設定されている場合は、開かれたファイアウォール ポートまたは VPN 接続がなくても iPad クライアントを接続できます。Access モバイル クライアント アプリケーションは、リバース プロキシのパススルー認証、ユーザー名/パスワード認証、Kerberos 制約付き委任認証、および証明書認証をサポートします。Access モバイル クライアント アプリケーションへの証明書追加の詳細については、「クライアント証明書の使用」の記事を参照してください。
- **Access モバイル クライアント アプリケーションでの Good Dynamics の有効化:** Access モバイル クライアント アプリケーションには、Good Dynamics プラットフォームに登録して管理する機能が用意されています。この構成では、Access モバイル クライアントとゲートウェイサーバーの間のすべてのネットワーク通信が、Good Dynamics のセキュリティで保護された通信チャネルと Good Proxy サーバーを経由して転送されます。詳細については、『Access モバイル クライアント for Good Dynamics』のマニュアル ページを参照してください。
- **MobileIron AppConnect enrolled Access Mobile Client app (MobileIron AppConnect に登録された Access モバイル クライアント):** Access モバイル クライアント アプリケーションが MobileIron の AppConnect プラットフォームに登録されている場合は、Access モバイル クライアントとゲートウェイ サーバー間のすべてのネットワーク通信を MobileIron Sentry 経由で転送できます。詳細については、『MobileIron AppConnect』のマニュアル ページを参照してください。

#### 証明書:

Acronis Access には、テスト目的の自己署名証明書が付属しており、インストールされます。本稼動時には、適切な CA 証明書を実装する必要があります。

- **注意:** 自己署名証明書を使用する際、一部のウェブ ブラウザに警告メッセージが表示されます。これらのメッセージを非表示にすると、システムを問題なく使用できます。本番環境で自己署名証明書を使用することはお勧めしません。

## 1.1.5 デスクトップ クライアント要件

#### サポートされるオペレーティング システム:

- Windows XP、Windows Vista、Windows 7、Windows 8 および Windows 8.1

**注意:** Windows XP で Acronis Access デスクトップ クライアントを使用する場合、厳しくない SSL 暗号化ルールを使用する必要があります。詳細については、「Acronis Access Tomcat SSL 暗号化の変更」を参照してください。



- Mac OS X 10.6.8 以降および 64 ビット ソフトウェアと互換性のある Mac

**注意:** Acronis Access デスクトップ クライアントをインストールする場合は、作成する同期フォルダが別のソフトウェアによる同期の対象となるフォルダに含まれないようにしてください。既知の競合のリストについては、「ソフトウェアの競合」を参照してください。

### サポート対象ウェブ ブラウザ:

- Mozilla Firefox 6 以降
- Internet Explorer 9 以降

**注意:** 安全でないバージョンである Internet Explorer 8 のサポートが必要な場合は、「Acronis Access Tomcat SSL 暗号化の変更」の内容を実行してください。Internet Explorer 8 は、サーバー管理ではサポートされません。

**注意:** Internet Explorer を使用する場合、ファイルをダウンロードするためには、[暗号化されたページをディスクに保存しない] にチェック マークが付いていない状態にしておく必要があります。この設定は、[インターネット オプション] → [詳細設定] → [セキュリティ] にあります。

- Google Chrome
- Safari 5.1.10 以降

## 1.2 サーバーに Acronis Access Advanced をインストールする

次の手順では、提供された自己署名証明書を使用して HTTPS で Acronis Access Advanced を新規インストールしてテストできます。

**注意:** アップグレード手順については、「アップグレード『65ページ』」のセクションを参照してください。

**注意:** クラスタでのインストール手順については、「クラスタでの Acronis Access のインストール『20ページ』」のセクションを参照してください。

Acronis Access のインストールは次の 3 ステップで行います。

1. Acronis Access Server インストーラのインストール。
2. Acronis Access サーバーが使用するネットワーク ポートおよび SSL 証明書の構成
3. ウェブベースのセットアップ ウィザードによる、用途に合わせたサーバーの構成

### Acronis Access のインストール

管理者としてログインしていることを確認してから Acronis Access をインストールしてください。

1. Acronis Access のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。

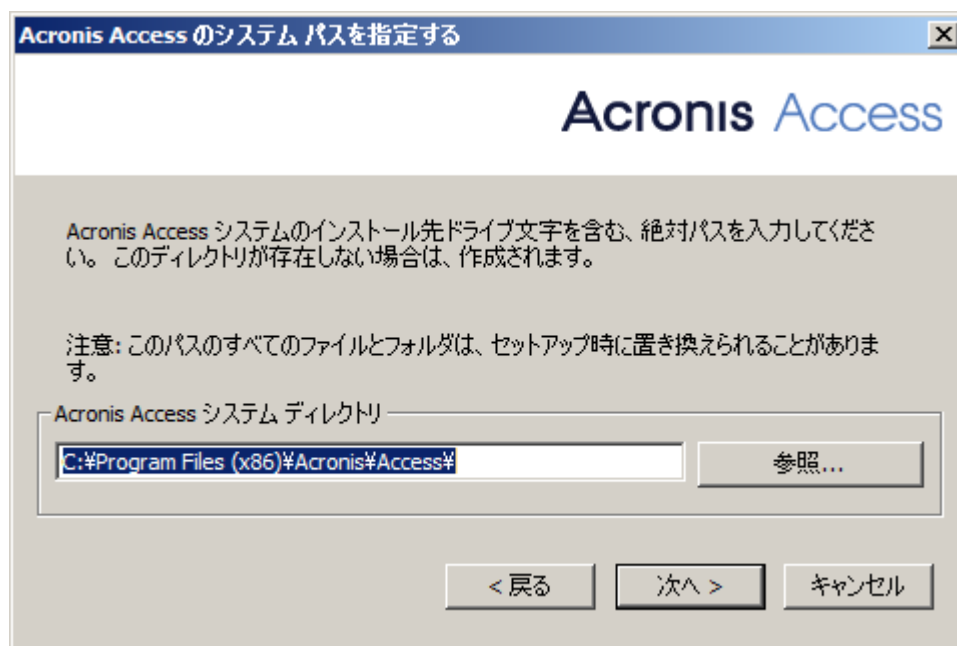




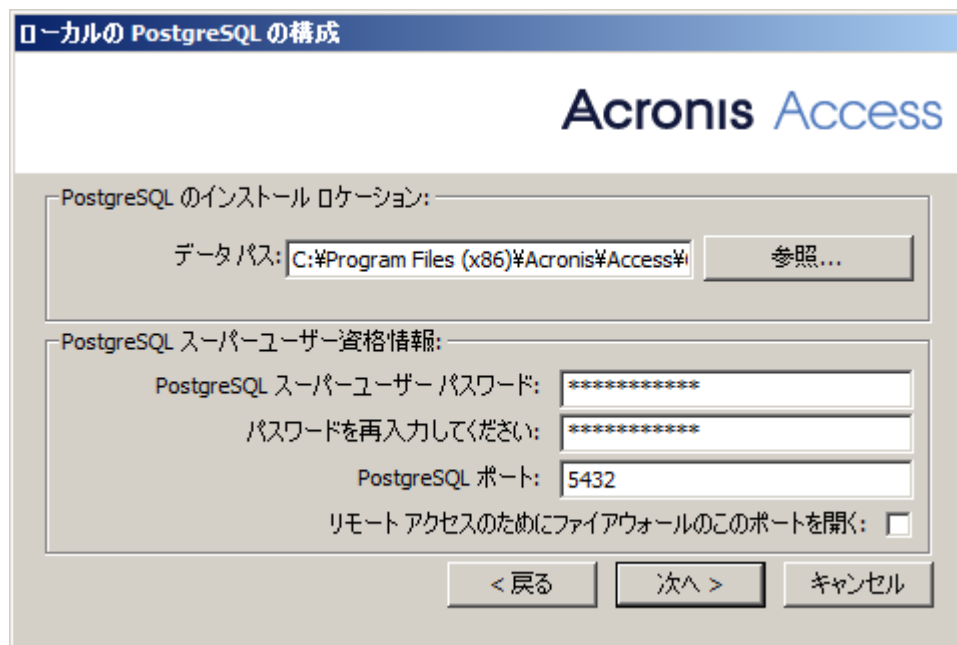
4. **[次へ]** を押して開始します。
5. 使用許諾契約を読み、承諾します。
6. **[インストール]** を押します。

**注意:** 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

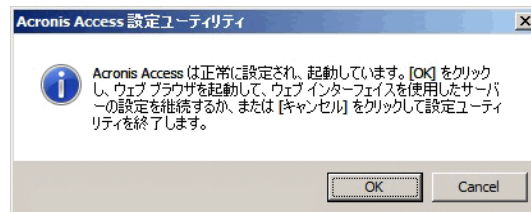
7. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、**[OK]** を押します。



8. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。



9. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。
10. Acronis Access のインストーラが完了したら、**[終了]** を押します。
11. 設定ユーティリティが自動的に起動し、インストールが完了します。



設定ユーティリティの使用方法については、「設定ユーティリティの使用『10ページ』」ページを参照してください。

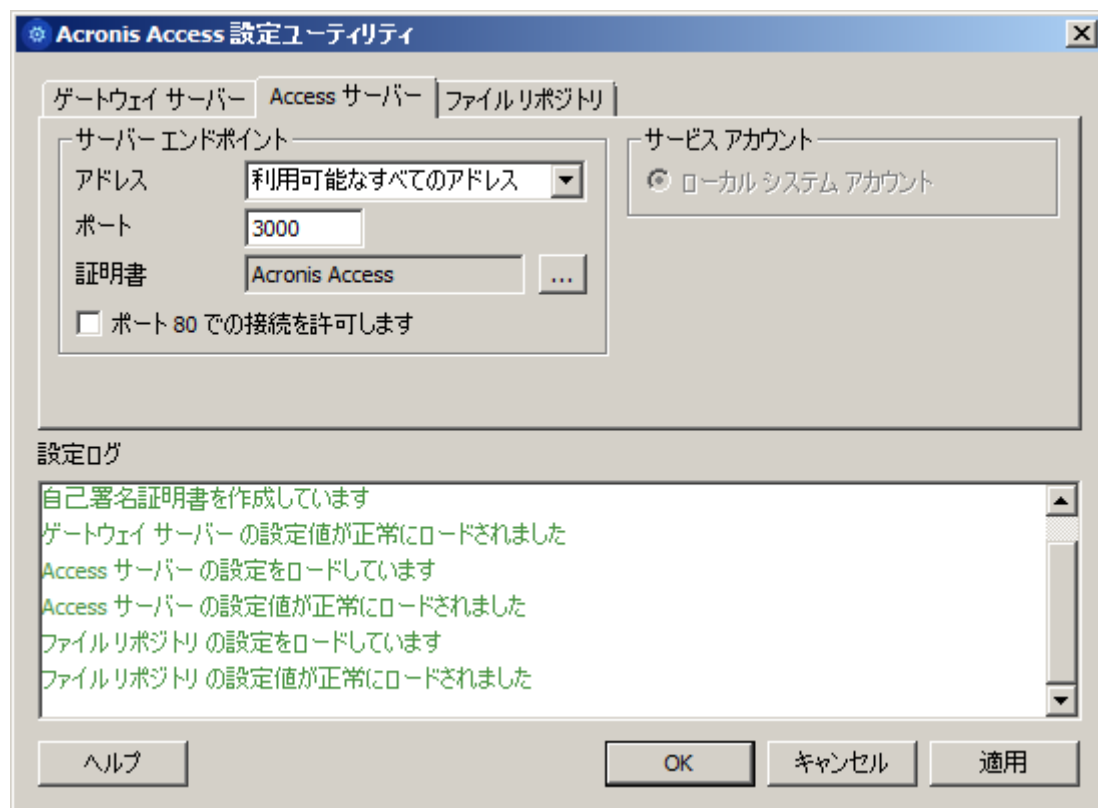
## 1.3 設定ユーティリティの使用

Acronis Access インストーラには、設定ユーティリティを付属しています。このユーティリティを使用すると、Acronis Access ゲートウェイ サーバー、ファイル リポジトリおよび Acronis Access サーバーへのアクセスを迅速簡単に設定できます。ゲートウェイ サーバーは、モバイル クライアントからファイルと共有の両方にアクセスするのに使われます。Access サーバーは、「同期と共有」クライアントのウェブ ユーザー インターフェイスを提供すると同時に、モバイル アクセスと同期と共有の両方の管理コンソールにもなります。

**注意:** Acronis Access の IP アドレス設定のベスト プラクティスに関する詳細については、「ネットワーク要件『6ページ』」セクションを参照してください。

**注意:** Microsoft Windows 証明書ストアに証明書を追加する方法については、「証明書の使用」の記事を参照してください。

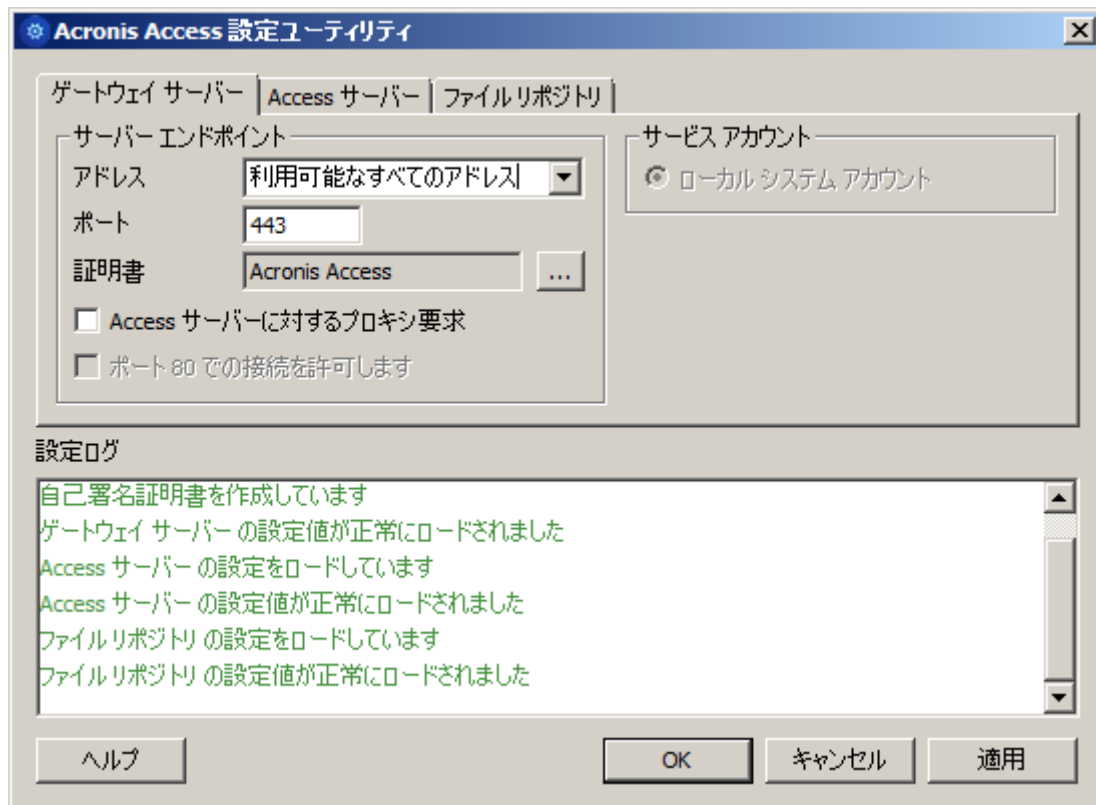
## Access サーバーの概要



Access サーバーは、「同期と共有」クライアントのウェブ ユーザー インターフェイスを提供すると同時に、モバイル アクセスと同期と共有の両方の管理コンソールにもなります。

- **アドレス:** ウェブ インターフェイスの FQDN または IP アドレス、またすべてのインターフェイスでリッスンするには **[すべてのアドレス]** を選択します。
- **ポート:** ウェブ インターフェイスのポート。
- **証明書:** ウェブ インターフェイスの証明書のパス。Microsoft Windows 証明書ストアから証明書を選択できます。
- **ポート 80 での接続を許可します:** このオプションが選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。
- **サービス アカウント:** これにより、Acronis Access サーバー サービスを別のアカウントのコンテキストで実行できます。通常のインストールでは必要ありません。

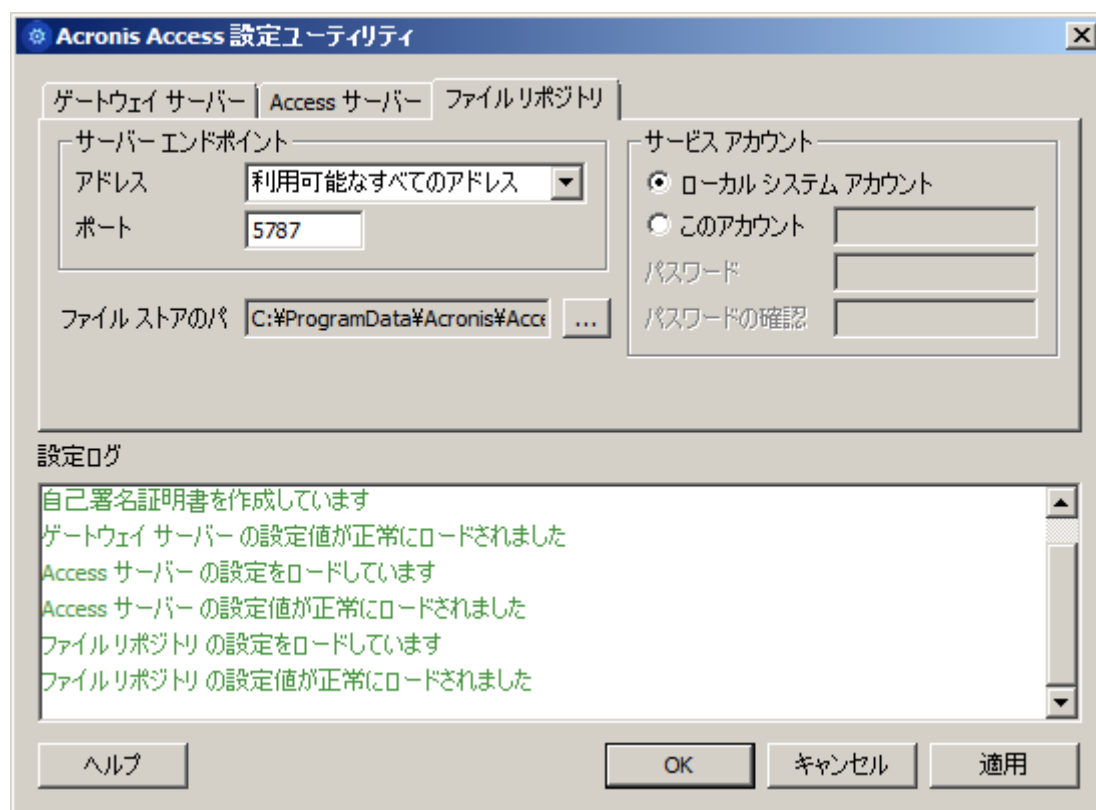
## ゲートウェイ サーバーの概要



ゲートウェイ サーバーは、モバイル クライアントからファイルと共有の両方にアクセスするのに使われます。

- **アドレス:** ゲートウェイ サーバーの FQDN または IP アドレス、またすべてのインターフェイスでリッスンするには **[すべてのアドレス]** を選択します。
- **ポート:** ゲートウェイ サーバーのポート。
- **証明書:** ゲートウェイ サーバーの証明書のパス。Microsoft Windows 証明書ストアから証明書を選択できます。
- **サービス アカウント:** これにより、ゲートウェイ サーバー サービスを別のアカウントのコンテキストで実行できます。通常のインストールでは必要ありません。
- **Access サーバーに対するプロキシ要求:** 有効になっている場合、ユーザーはゲートウェイ サーバーに接続します。このサーバーが Access サーバーのプロキシ サーバーとして機能します。これは、Access サーバーとゲートウェイ サーバーが同じコンピュータにインストールされている場合に使用できます。
- **ポート 80 での接続を許可します:** このオプションが選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。

## ファイル リポジトリの概要



ファイル リポジトリは、同期と共有機能によって使われます。同期と共有をまだ有効にしていない場合は、標準の値を受け入れます。同期と共有を使用している場合、ファイル ストアのパスとして、ストレージに使用するディスクのロケーションを指定する必要があります。ストレージに Amazon S3 を使用する計画がある場合、デフォルトの値でかまいません。

- **アドレス:** ファイル リポジトリの FQDN または IP アドレス、またすべてのインターフェイスでリッスンするには **[すべてのアドレス]** を選択します。IP または DNS アドレスを指定する場合、同じアドレスを、ウェブ インターフェイスの **[ファイル リポジトリ]** セクションにも指定する必要があります。詳しくは、「ファイル リポジトリ」の記事を参照してください。
- **ポート:** ファイル リポジトリのポート。同じポートを、ウェブ インターフェイスの **[ファイル リポジトリ]** セクションにも指定する必要があります。詳しくは、「ファイル リポジトリ」の記事を参照してください。
- **ファイル ストアのパス:** [ファイル ストア] の UNC パス。ファイル ストアのパスを変更する場合は、元のファイル ストアの場所に既に存在するファイルすべてを、新しい場所に手動でコピーする必要があります。

**注意:** ファイル ストアを別の場所に移動する場合は、新しいファイルが正しく新しい場所に移動されるようにアップロードする必要があります。また、ファイル ストアに既に存在していたファイルをダウンロードして、元の場所にあったファイルのすべてが新しい場所でもアクセス可能な状態にしておく必要があります。

- **サービス アカウント:** リポジトリのファイル ストレージがリモート ネットワーク共有にある場合、サービス アカウントがそのネットワーク共有へのアクセス許可を持つように設定する必要があります。このアカウントには、ログ ファイルを書き込むため、Repository フォルダ(例えば、C:\Program Files (x86)\Acronis\Access\File Repository\Repository) への読み取り/書き込みアクセス権限も必要です。

必要なフィールドのすべてに入力した後、[適用] または [OK] を押すと、変更を加えたサービスが再起動します。サービスが開始されてから 30～45 秒経つと、Acronis Access サーバーが利用できるようになります。この時点で、ウェブ ブラウザが自動的に起動し、Acronis Access の IP アドレスおよびポートに接続します。ログイン ページで、管理者パスワードを設定します。セットアップ ウィザード『14ページ』が表示され、そこでセットアップ プロセスを実行できます。

**注意:** 管理者パスワードを書き留めておいてください。忘れた場合にパスワードを復元することはできません。

**注意:** ネットワーク IP アドレス/ポートまたは Acronis Access コンポーネントが使用する証明書のいずれかを変更する必要がある場合、いつでも設定ユーティリティを再度実行してそれらの変更を加えることができます。自動的に必要な設定ファイルを調整し、サービスを再起動します。

## 1.4 セットアップ ウィザードの使用

ソフトウェアをインストールし、設定ユーティリティを実行してネットワーク ポートと SSL 証明書を設定した後、管理者は Acronis Access サーバーを設定する必要があります。設定ウィザードは、管理者に一連の手順を案内し、サーバーの基本的な機能が動作するようにします。

**注意:** activEcho または mobilEcho からアップグレードする場合、続行する前に「アップグレード『65ページ』」セクションをお読みください。

**注意:** 設定ユーティリティを実行した後、サーバーが最初に起動するまで 30～45 秒かかります。

設定ユーティリティで指定した IP アドレスとポートを使用して、Acronis Access のウェブ インターフェイスに移動します。デフォルトの管理者アカウントにパスワードを設定するように求めるメッセージが表示されます。

**注意:** 管理者は後から設定できます。詳細については、「サーバーの管理」セクションを参照してください。

このウィザードにより、製品の主要な機能を設定できます。

- [全般設定] では、言語、カラー スキーム、管理者通知で使用するサーバー名、ライセンス、管理者など、ウェブ インターフェイス自体の設定を行います。
- [LDAP] の設定では、製品で Active Directory の資格情報、ルール、ポリシーを使用できるようにします。
- [SMTP] の設定では、モバイル アクセス機能、および同期と共有機能の設定を行います。モバイル アクセスでは、登録招待の送信時に SMTP サーバーが使用されます。同期と共有機能は、フォルダへの招待、警告、エラーの概要を送信するために SMTP サーバーを使用します。

[初期構成] ページで見ることができるすべての設定は、構成の完了後にも確認することができます。設定の詳細については、「サーバー管理」の記事を参照してください。

## 初期構成プロセスを進める

### ライセンス

#### ライセンス

ライセンス: Access Advanced 無期限  
クライアント数: 50  
現在のライセンス取得済みクライアントの数: 2  
現在の無料クライアント数: 1

| ライセンス タイプ           | クライアント数 | 有効期限日 | プロダクト キー |
|---------------------|---------|-------|----------|
| Access Advanced 無期限 | 50      |       |          |

プロダクト キーの追加...

ライセンスの追加

☐ ライセンスの詳細と範囲については、納品書および <http://www.acronis.co.jp/company/licensing.html> で確認できることを理解しました。

#### 試用版を開始するには:

1. **[試用を開始]** を選択し、**[続行]** を押します。

#### Access サーバーにライセンスを付与するには:

1. **[プロダクト キーを入力します]** を選択します。
2. プロダクト キーを入力し、チェックボックスにマークを付けます。
3. **[保存]** を押します。

### 全般設定

#### サーバー設定

サーバー名

Acronis Access

ウェブ アドレス

<https://www.echoserver.com>

モバイル クライアント登録  
アドレス

[www.echoserver.com](http://www.echoserver.com)

カスタム ログを使用

☐

監査ログの言語

日本語



保存

1. **[サーバー名]** にサーバー名を入力します。



2. ユーザーが(http:// または https:// で始まる)ウェブ サイトにアクセスできる FQDN または IP アドレスを指定します。
3. モバイル ユーザーが登録する FQDN または IP アドレスを指定します。
4. カラー スキームを選択します。現在のオプションは、[灰色]、[紫]、[カプチーノ]、[青]、[濃紺]、および [オレンジ] です。
5. **[監査ログ]** のデフォルトの言語を選択します。現在のオプションは、[英語]、[ドイツ語]、[フランス語]、および [日本語] です。
6. **[保存]** を押します。

## SMTP

### SMTP

Acronis Access サーバーは、構成された SMTP サーバーを使用して電子メールを送信し、ファイルの共有やデバイスの登録のためにユーザーを招待したり、ユーザーや管理者にサーバー アクティビティを通知します。

SMTP サーバー アドレス

SMTP サーバー ポート

セキュリティで保護された  
接続を使用しますか？ ☒

差出人名

差出人電子メール アドレス

SMTP 認証を使用します  
か？ ☐

保存

テスト用の電子メールの送信

SMTP セットアップのスキップ

**注意:** この手順をスキップして、後で SMTP を構成することもできます。

1. SMTP サーバーの FQDN または IP アドレスを入力します。
2. サーバーの SMTP ポートを入力します。
3. SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか？]** のチェックを外します。

4. サーバーによって送信される電子メールの「差出人」行に表示されるユーザー名を入力します。
5. サーバーから送信される電子メールのアドレスを入力します。
6. SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、**[認証を使用しますか？]** をチェックし、認証情報を入力してください。
7. **[テスト用の電子メールの送信]** を押して電子メールを手順 5 で指定したテスト用の電子メールアドレスに送信します。
8. **[保存]** を押します。

## LDAP

### LDAP

組織内のユーザーにモバイル アクセス、同期アクセス、および共有アクセスを提供するために、Active Directory への LDAP 接続を使用することができます。LDAP は、管理対象外のモバイル アクセスや、同期および共有サポートに対しては不要ですが、管理対象のモバイル アクセスには必要になります。Microsoft Active Directory への LDAP 接続のみがサポートされています。

LDAP を有効にしますか？ ☒

LDAP サーバー アドレス

LDAP サーバー ポート

セキュリティで保護された  
LDAP 接続を使用します  
か？ ☐

LDAP ユーザー名

LDAP パスワード

LDAP パスワードの確認入  
力

LDAP 検索ベース

LDAP 認証のためのドメイ  
ン

例: mycompany.com。このリストに含まれるドメ  
インの電子メール アドレスを使用しているユー  
ザーは、LDAP に対して認証する必要がありま  
す。他のドメインのユーザーは、Acronis Access  
データベースに対して認証します。

+ 追加

- 削除

☐ 完全に一致している必要があります

LDAP 情報をキャッシュす  
る間隔

保存

LDAP のセットアップをスキップ

**注意:** この手順をスキップして、後で LDAP を構成することもできます。

1. **[LDAP を有効にしますか?]** をチェックします。
2. LDAP サーバーの FQDN または IP アドレスを入力します。
3. LDAP サーバーのポートを入力します。
4. LDAP サーバーとの接続に証明書を使用する場合は、**[セキュリティで保護された LDAP 接続を使用しますか?]** をチェックします。
5. LDAP の資格情報をドメインも含めて入力します (例: `acronis%hristo`)。
6. LDAP 検索ベースを入力します。
7. LDAP 認証のドメインを入力します (例えば、電子メール `joe@glilabs.com` のアカウントの LDAP 認証を有効にするには、**glilabs.com** と入力します)。
8. **[保存]** を押します。

## ローカル ゲートウェイ サーバー

### ローカル ゲートウェイ サーバー

Acronis Access のモバイル アプリケーション クライアントは、ゲートウェイ サーバーのアドレスを使用して Access サーバーに接続します。サーバーの設定によっては、デスクトップ同期クライアントおよびウェブ クライアントもこのサーバーに接続されていることがあります。ゲートウェイ サーバーは現在 **192.168.2.129:443** で動作しています。クライアントの接続設定では、接続元となるすべてのネットワークからアクセス可能な DNS アドレスを使用することが推奨されます。クライアントがプロキシ サーバーを経由して接続する場合、このアドレスはプロキシ サーバーの実際の DNS アドレスにすることができます (例: `gateway.mycompany.com`)。

クライアントがサーバーに接続するために使用するアドレス:

192.168.2.129:443

保存

スキップ

**注意:** 同じコンピュータにゲートウェイ サーバーと Acronis Access サーバーの両方をインストールする場合、ゲートウェイ サーバーが自動的に検出され、Acronis Access サーバーに管理されます。クライアントがアクセス可能なローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定するように指示するメッセージが表示されます。このアドレスは後から変更できます。

1. ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。
2. **[保存]** を押します。

## ファイル リポジトリ

1. ファイル ストア タイプを選択します。お使いのコンピュータのファイル ストアの場合、**[ファイル システム]** を、クラウドのファイル ストアの場合、**[Amazon S3]** を使います。
2. ファイル リポジトリ サービスの FQDN または IP アドレスを入力します。

**注意:** ファイル リポジトリのアドレス、ポート、およびファイル ストアのロケーションを設定するには、Acronis Access 設定ユーティリティを使用します。ファイル ストア リポジトリ エンドポイントの設定は、設定ユーティリティの **[ファイル リポジトリ]** タブの設定と一致していなければなりません。それらの設定値を表示または変更するには、AcronisAccessConfiguration.exe を実行します。通常、これはエンドポイント サーバーの **C:\Program Files (x86)\Acronis\Configuration Utility** にあります。

3. 暗号化レベルを選択します。[なし]、[AES-128]、[AES-256] から選択してください。
4. サーバーがユーザーに警告を送信する最小限の空き領域を選択してください。
5. [保存] を押します。

## 1.5 Acronis Access のクラスタリング

Acronis Access では、サードパーティのクラスタリング ソフトウェアを使用せずに、可用性の高い設定を行うことができます。設定には、Acronis Access 5.1 で導入された新しいクラスタ グループ機能を使用します。設定手順はシンプルで、Acronis Access ゲートウェイ サーバーには高い可用性がもたらされますが、ゲートウェイ サーバーは負荷が最も高いコンポーネントです。設定のすべては、Acronis Access サーバーを通して管理されます。

クラスタ グループの詳細や設定手順に関する詳細については、「クラスタ グループ」の記事を参照してください。

組み込みのクラスタ グループ機能を使用することをお勧めいたしますが、Acronis Access では Microsoft Failover Clustering もサポートされています。こちらの詳細については、「補足資料」セクションを参照してください。

## 1.6 Acronis Access の負荷分散

Acronis Access では負荷分散がサポートされています。詳細については、「Acronis Access の負荷分散」および「クラスタ グループ」の記事を参照してください。

# 2 Microsoft フェールオーバー クラスタ上での Acronis Access のインストール

---

**警告:** Acronis Access フェールオーバー クラスタリングは、5.0.3 より前のバージョンではサポートされていません。それより前のバージョンを使用している場合、何らかのクラスタの設定を続行する前に、5.0.3 以降のバージョンにアップグレードする必要があります。

---

Acronis Access をクラスタ上にインストールするには、以下のガイドが役立ちます。

### セクションの内容

|   |    |
|---|----|
| Windows 2003 Microsoft フェールオーバー クラスタ上での Acronis Access のインストール..... | 20 |
| Windows 2008 Microsoft フェールオーバー クラスタ上での Acronis Access のインストール..... | 36 |
| Windows 2012 Microsoft フェールオーバー クラスタ上での Acronis Access のインストール..... | 50 |

## 2.1 Windows 2003 Microsoft フェールオーバー クラスタ 上での Acronis Access のインストール

### Acronis Access のインストール

管理者としてログインしていることを確認してから Acronis Access をインストールしてください。

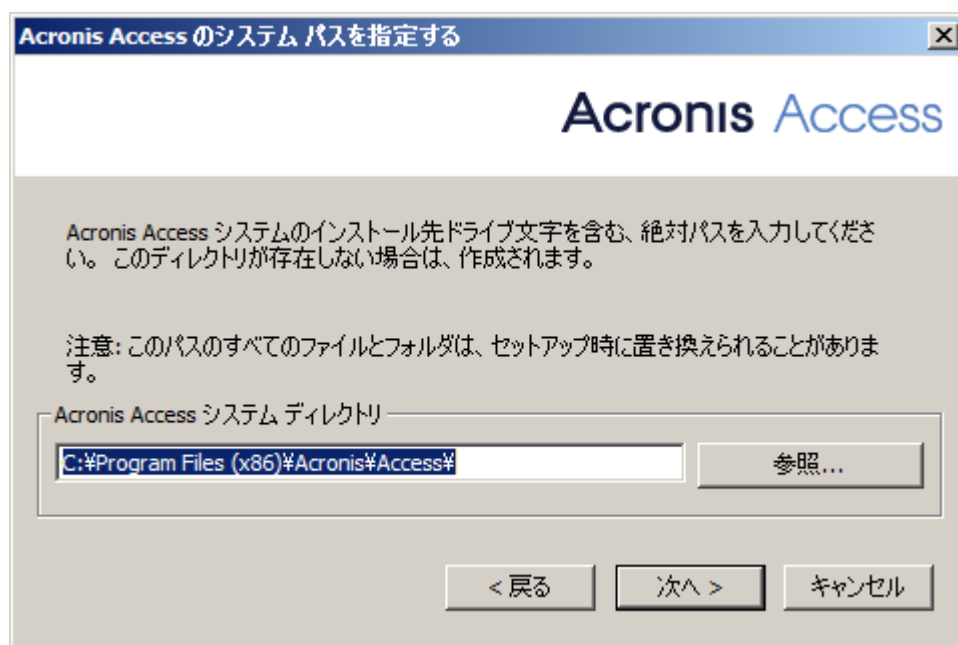
1. Acronis Access のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。



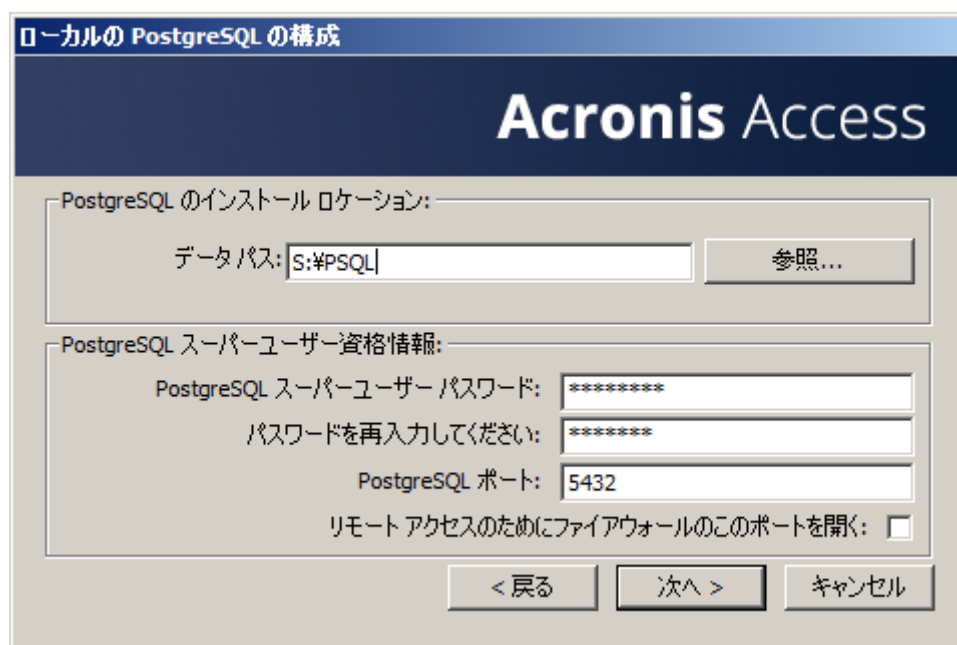
4. [次へ] を押して開始します。
5. 使用許諾契約を読み、承諾します。
6. [インストール] を押します。

**注意:** 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

7. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、[OK] を押します。



8. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。
9. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して [次へ] をクリックします。



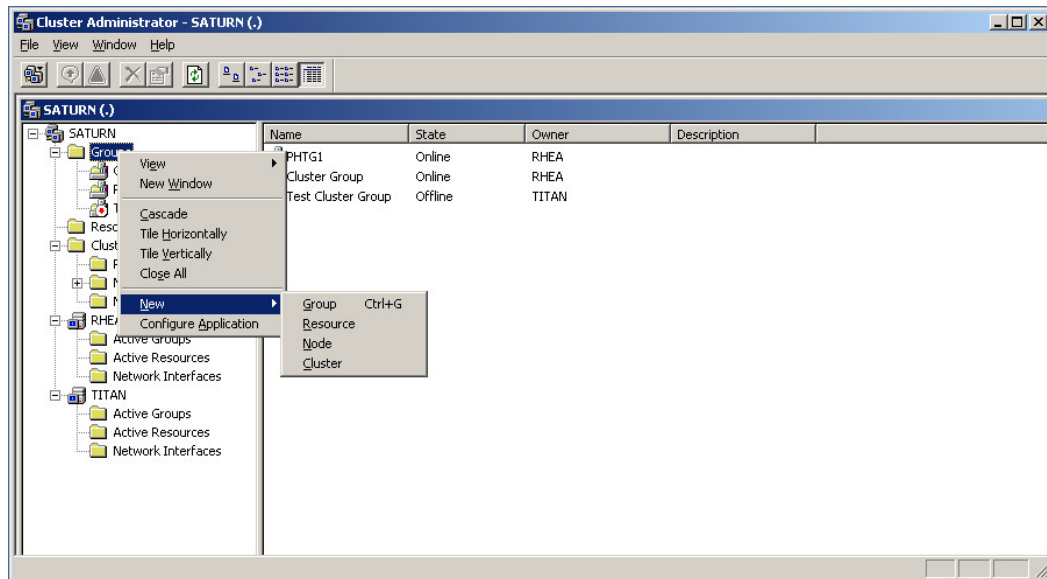
10. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、[OK] を押します。



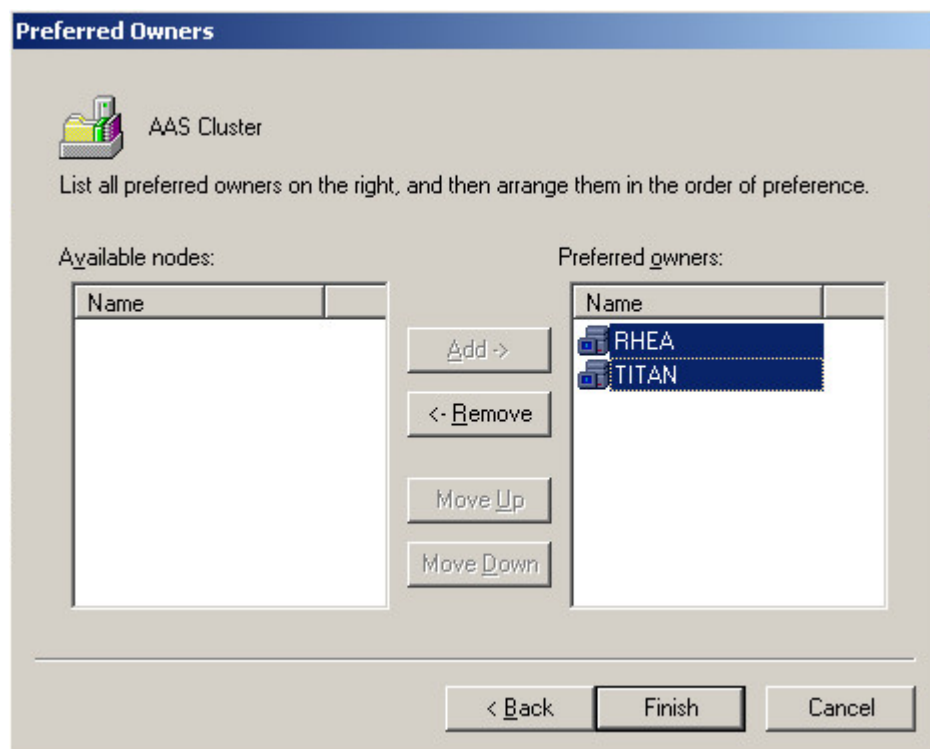
Acronis Access のインストーラが完了したら、[終了] を押します。

## クラスタ グループの作成

1. [クラスタ管理者] を開き、[グループ] を開きます。
2. [グループ] を右クリックし、[新規] および [グループ] を選択します。クラスタ グループに適切な名前を付けます（Acronis Access、AAS クラスタなど）。



3. このクラスタ グループの一部となるマシンを選択して [完了] をクリックします。



## アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\Acronis\Access\Gateway Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます(例: **database\_path: 'S:/access\_cluster/database/'**)。

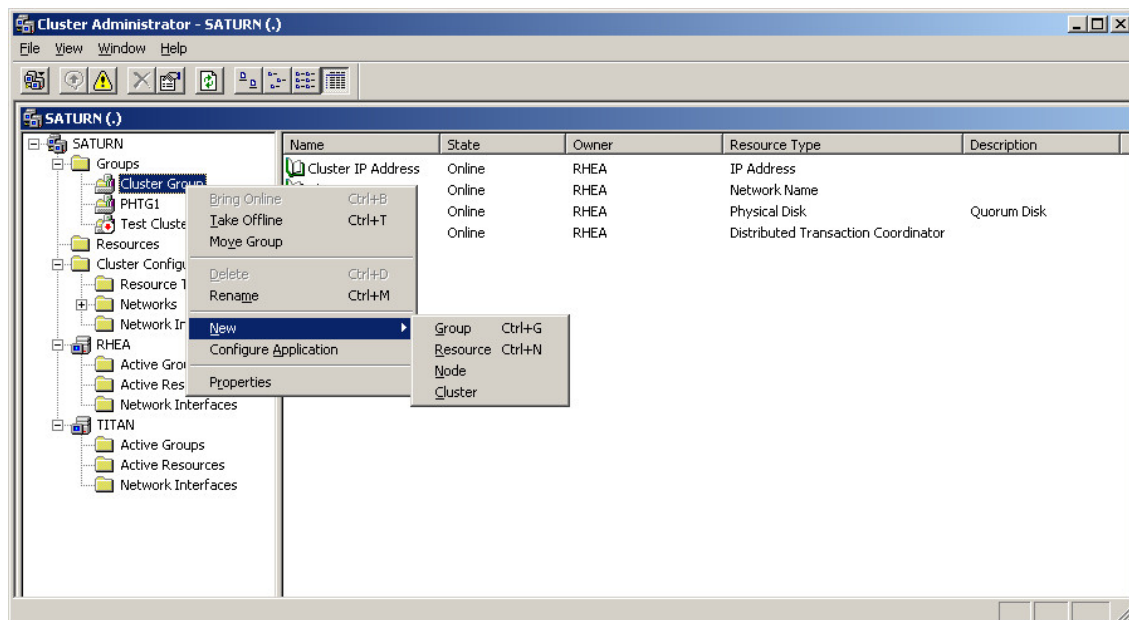
**注意:** パスの区切りにはスラッシュ (/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

## 必要なすべてのサービスを Acronis Access クラスタ グループに追加する

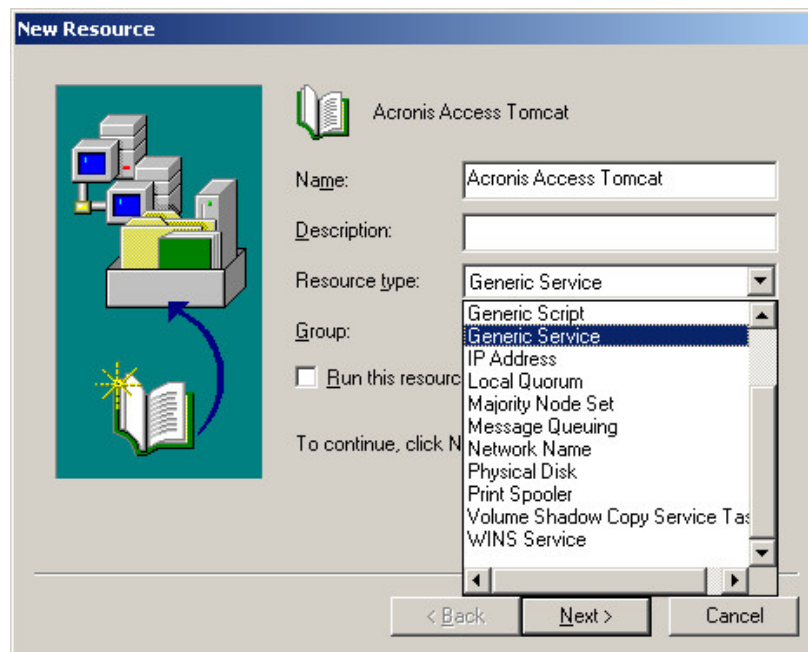
AcronisAccessGateway、AcronisAccessPostgreSQL (Acronis Access のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Acronis Access クラスタ グループを右クリックします。
2. **[新規]** を開いて **[リソース]** を選択します。

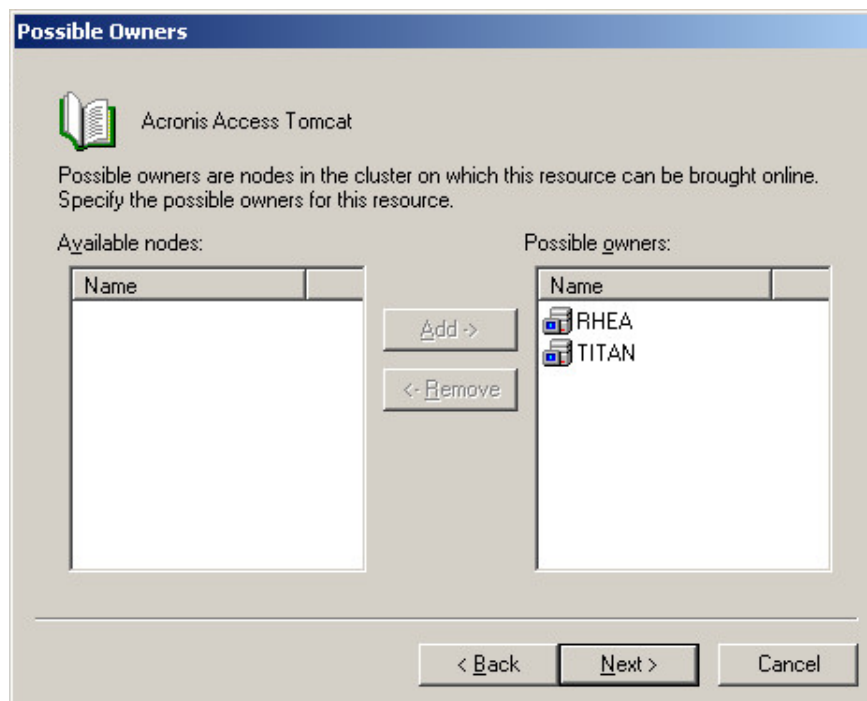


3. サービスの名前を入力し、適切なクラスタ グループを選択します。

4. [リソースの種類] ドロップダウン メニューから [汎用サービス] を選択して [次へ] をクリックします。



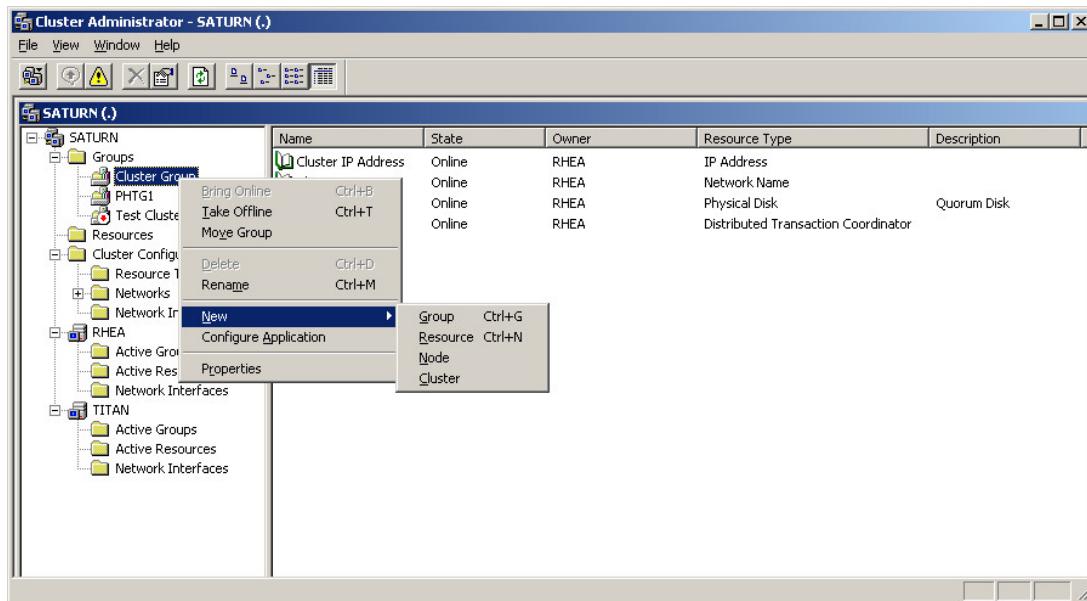
5. 2 つのノードがいずれも[使用可能な所有者] のリストに含まれていることを確認してから[次へ] をクリックします。



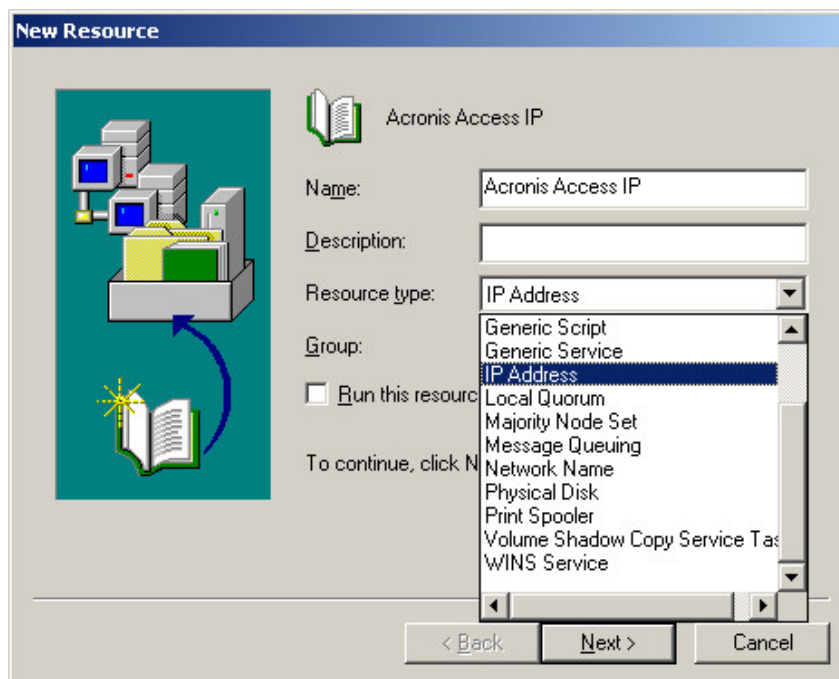
6. [次へ] をクリックして依存関係をスキップします。
7. 追加するサービスの正確なサービス名 (postgresql-x64-9.2 など) を入力して [次へ] をクリックします。
8. ここでは [次へ] を押して [レジストリ レプリケーション] ウィンドウをスキップします。
9. [完了] をクリックします。これで手順は完了です。

## クラスタ グループの IP アドレスの設定

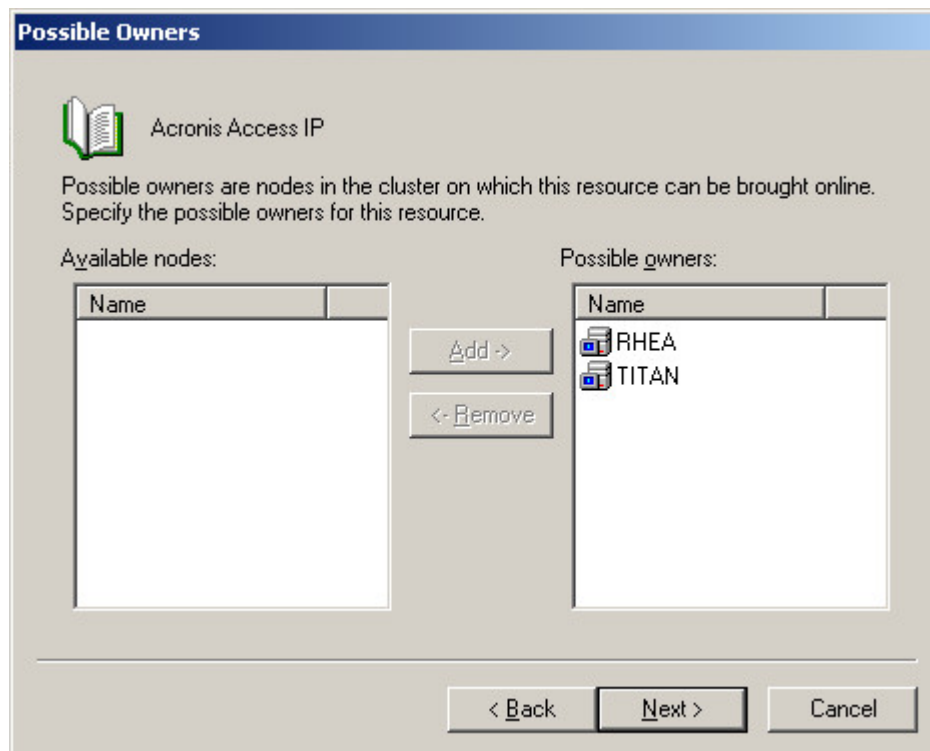
1. Acronis Access クラスタ グループを右クリックします。
2. [新規] を開いて [リソース] を選択します。



3. リソースの名前を入力し、適切なクラスタ グループを選択します。
4. [リソースの種類] ドロップダウン メニューから [IP アドレス] を選択して [次へ] をクリックします。



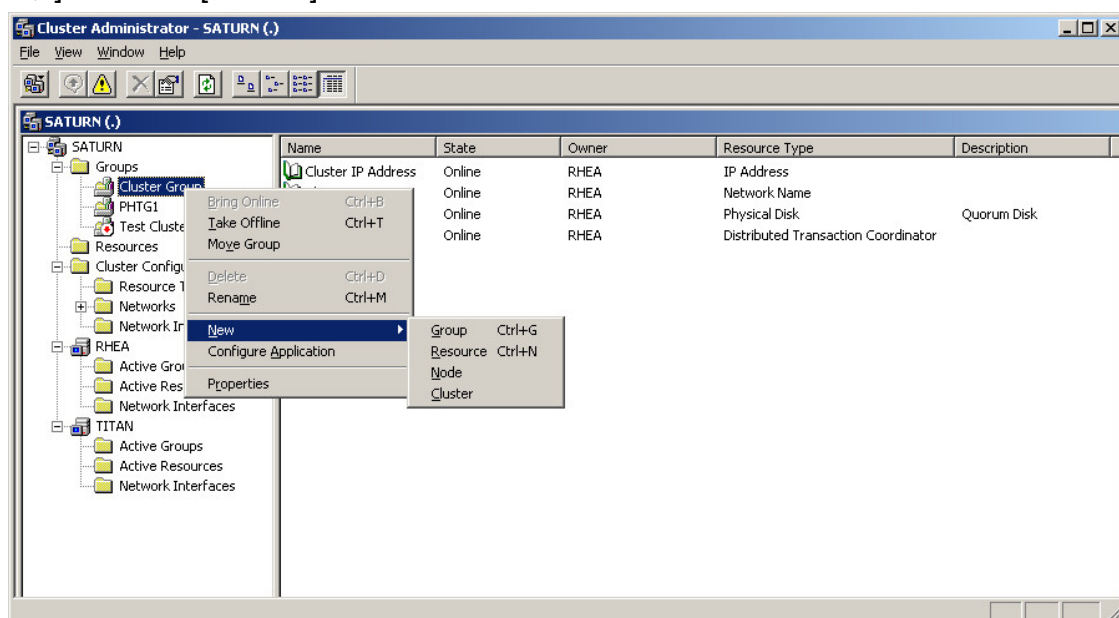
5. 2 つのノードがいずれも [使用可能な所有者] のリストに含まれていることを確認してから [次へ] をクリックします。



6. [次へ] をクリックして依存関係をスキップします。
7. このクラスタ グループで使用する IP アドレスを入力します。
8. サブネット マスクを入力して [完了] をクリックします。

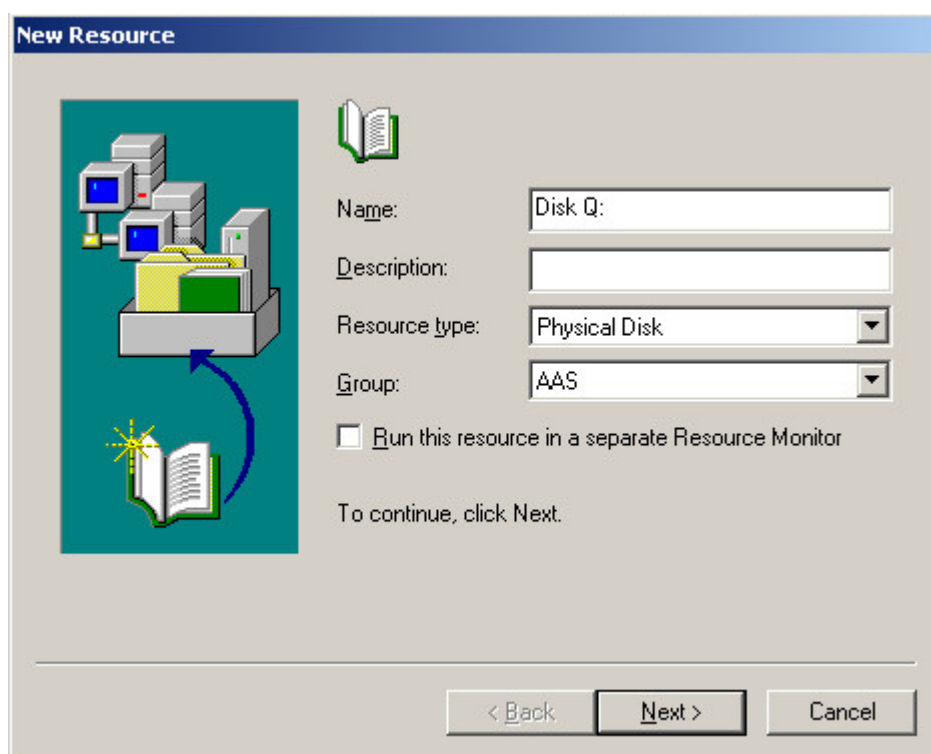
## 共有ディスクの追加

1. Acronis Access クラスタ グループを右クリックします。
2. [新規] を開いて [リソース] を選択します。



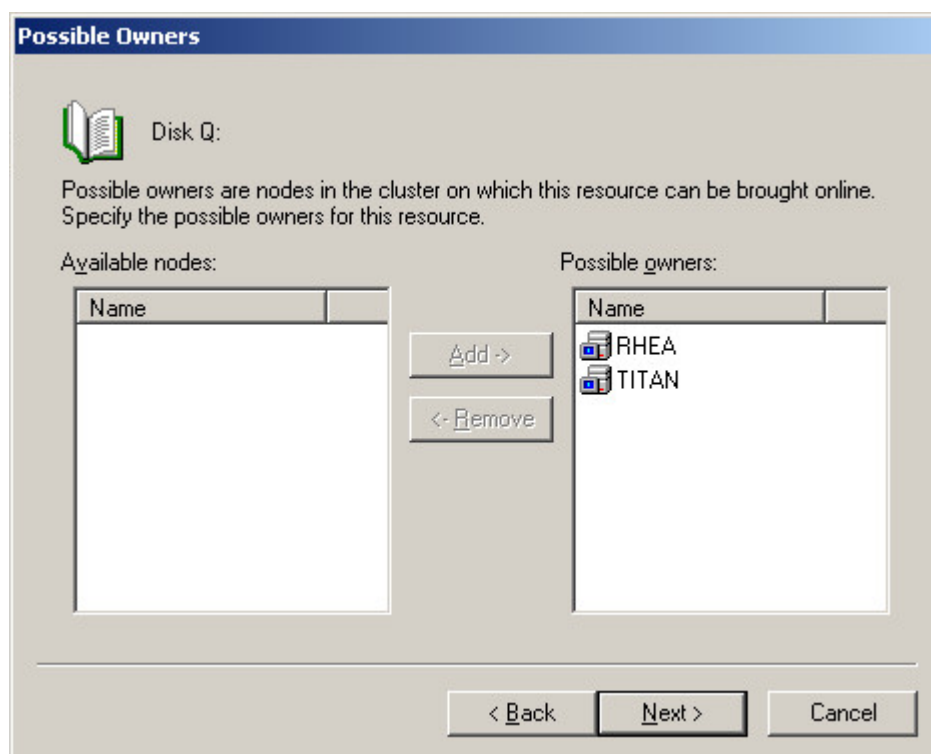
3. リソースの名前を入力し、適切なクラスタ グループを選択します。

4. [リソースの種類] ドロップダウン メニューから [物理ディスク] を選択して [次へ] をクリックします。



The 'New Resource' dialog box is shown. It has a title bar 'New Resource'. On the left is an icon of a server rack with a blue arrow pointing to a book icon. On the right, there are input fields: 'Name:' with 'Disk Q:', 'Description:', 'Resource type:' with a dropdown menu showing 'Physical Disk', and 'Group:' with a dropdown menu showing 'AAS'. Below these is a checkbox 'Run this resource in a separate Resource Monitor' which is unchecked. At the bottom, there is a text prompt 'To continue, click Next.' and three buttons: '< Back', 'Next >', and 'Cancel'.

5. 2 つのノードがいずれも [使用可能な所有者] のリストに含まれていることを確認してから [次へ] をクリックします。



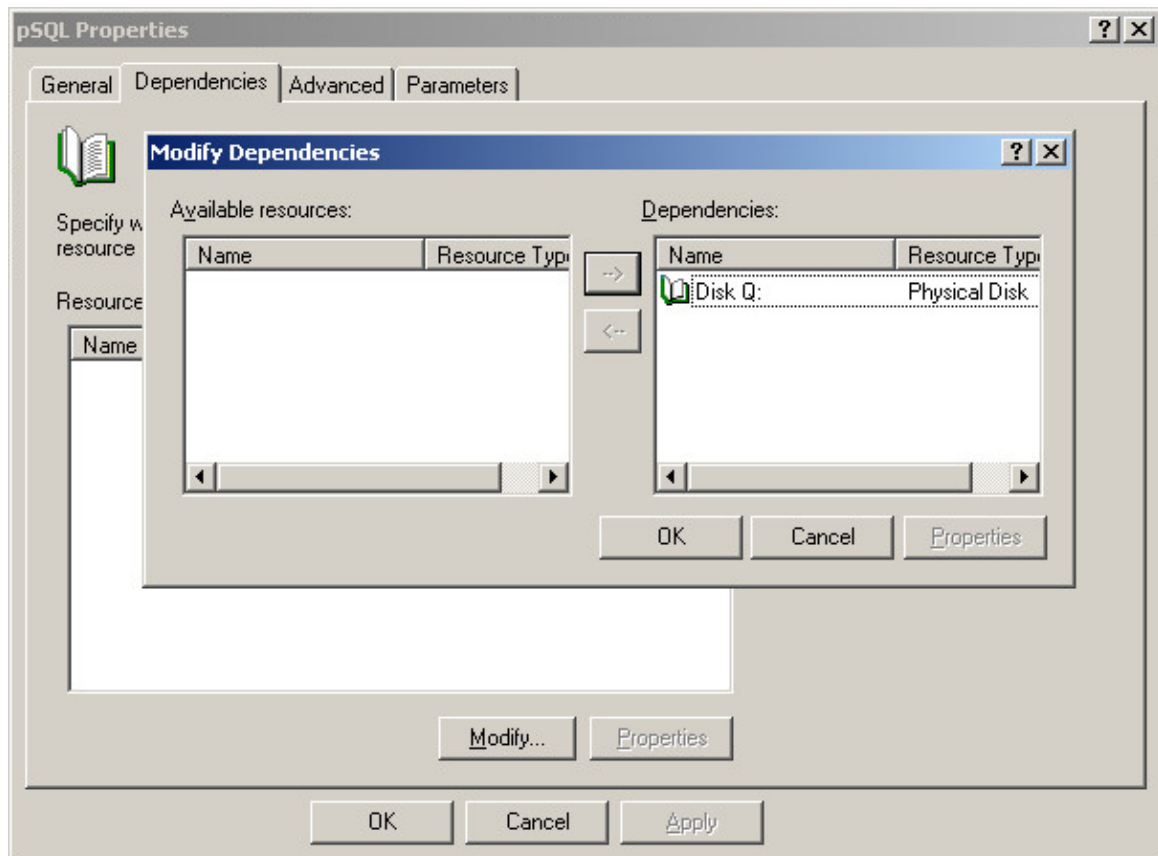
The 'Possible Owners' dialog box is shown. It has a title bar 'Possible Owners'. At the top left is an icon of a book and the text 'Disk Q:'. Below this is a paragraph: 'Possible owners are nodes in the cluster on which this resource can be brought online. Specify the possible owners for this resource.' There are two lists: 'Available nodes:' on the left and 'Possible owners:' on the right. The 'Possible owners:' list contains two entries: 'RHEA' and 'TITAN', each with a small server icon. Between the lists are two buttons: 'Add ->' and '< Remove'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. [次へ] をクリックして依存関係をスキップします。  
7. ドロップダウン メニューから使用可能なディスクを選択し、[完了] をクリックします。

## 依存関係の設定

PostgreSQL および Acronis Access ファイル リポジトリでは、次の操作を実行します。

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。
3. [変更] をクリックします。
4. 追加した共有ディスクを選択し、右側に移動します。



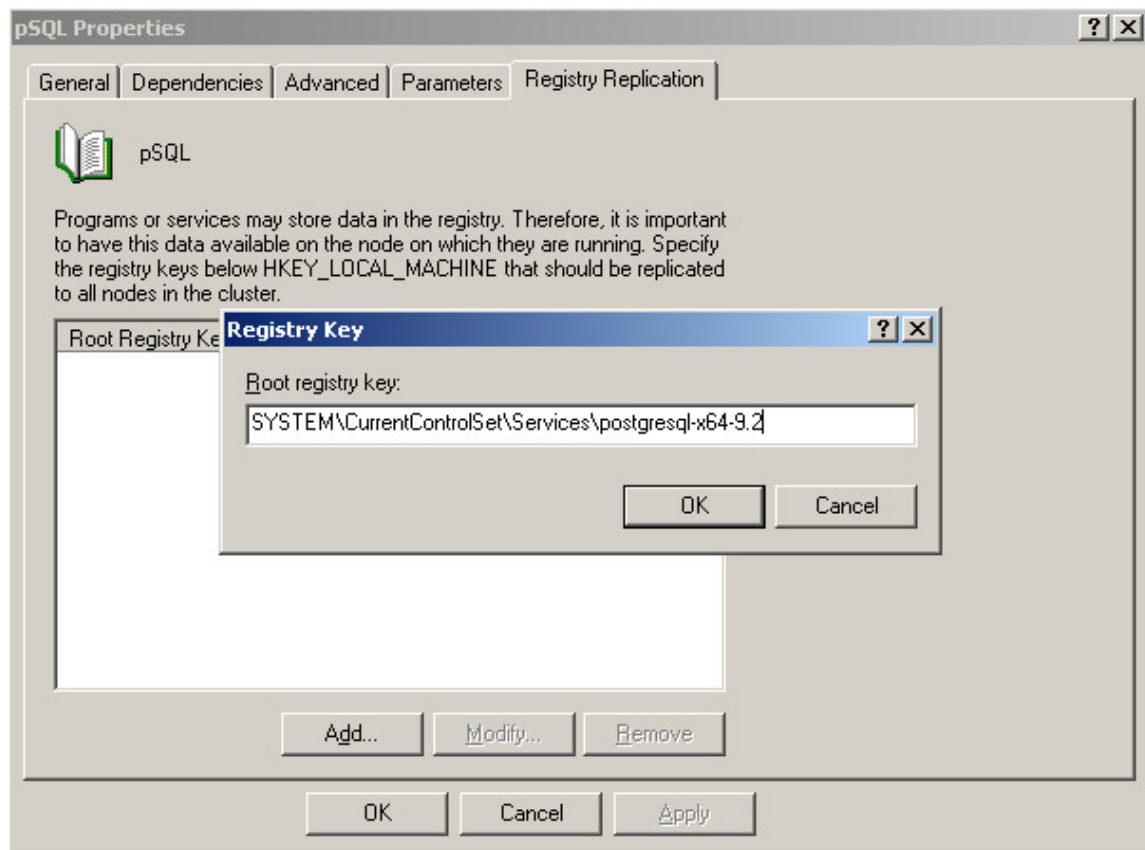
5. [OK] を押します。

PostgreSQL では、次の操作も実行します。

1. [レジストリ レプリケーション] タブをクリックします。



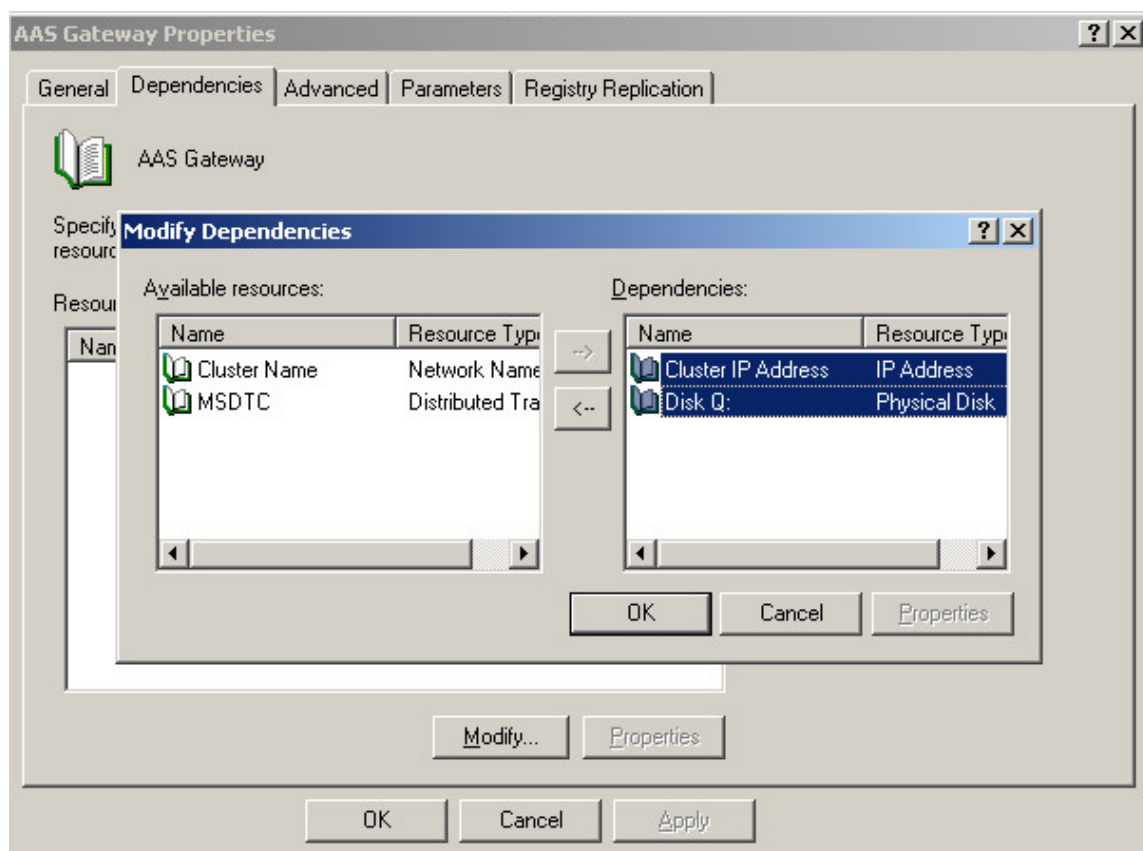
2. **[追加]** を押し、**SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\** のように入力します(旧バージョンの Acronis Access の場合、サービスが **postgresql-x64-9.2** のように異なることがあります)。



**Acronis Access ゲートウェイ サーバー サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、**[プロパティ]** を選択します。
2. **[依存関係]** タブをクリックします。
3. **[変更]** をクリックします。

4. IP アドレスと物理ディスクを選択し、右側に移動します。

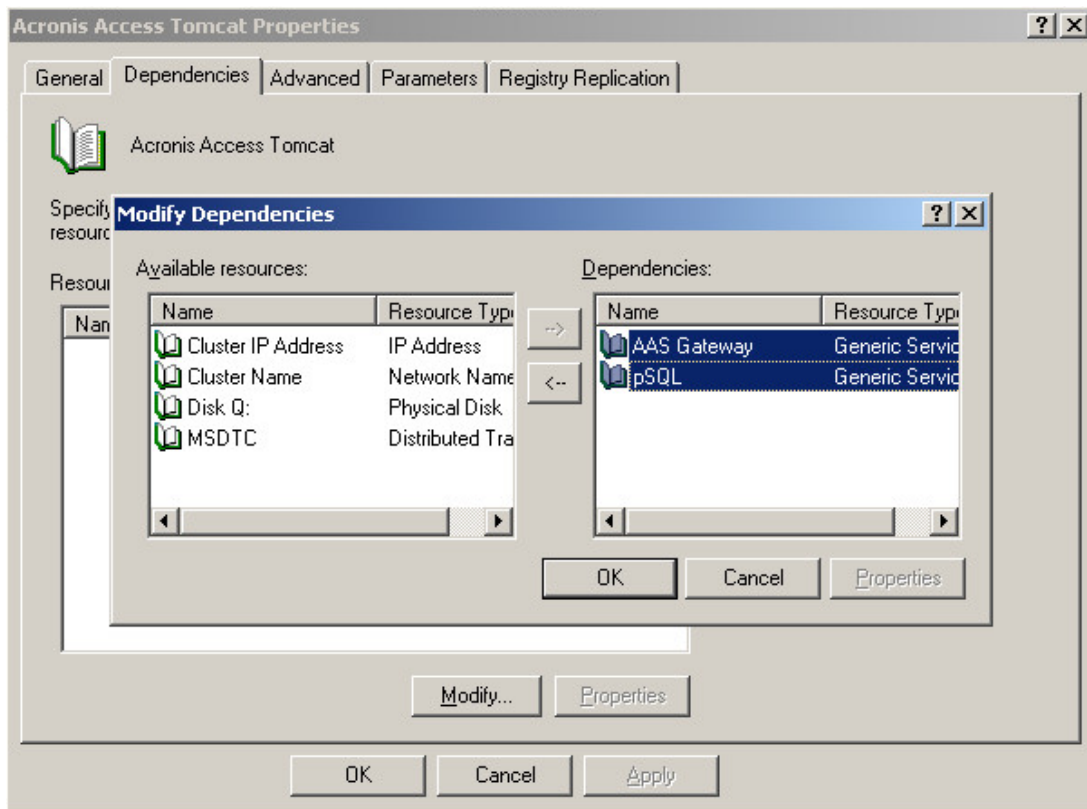


5. [OK] を押します。

**Acronis Access Tomcat サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。
3. [変更] をクリックします。

4. PostgreSQL および Acronis Access ゲートウェイ サーバーのサービスを選択し、右側に移動します。

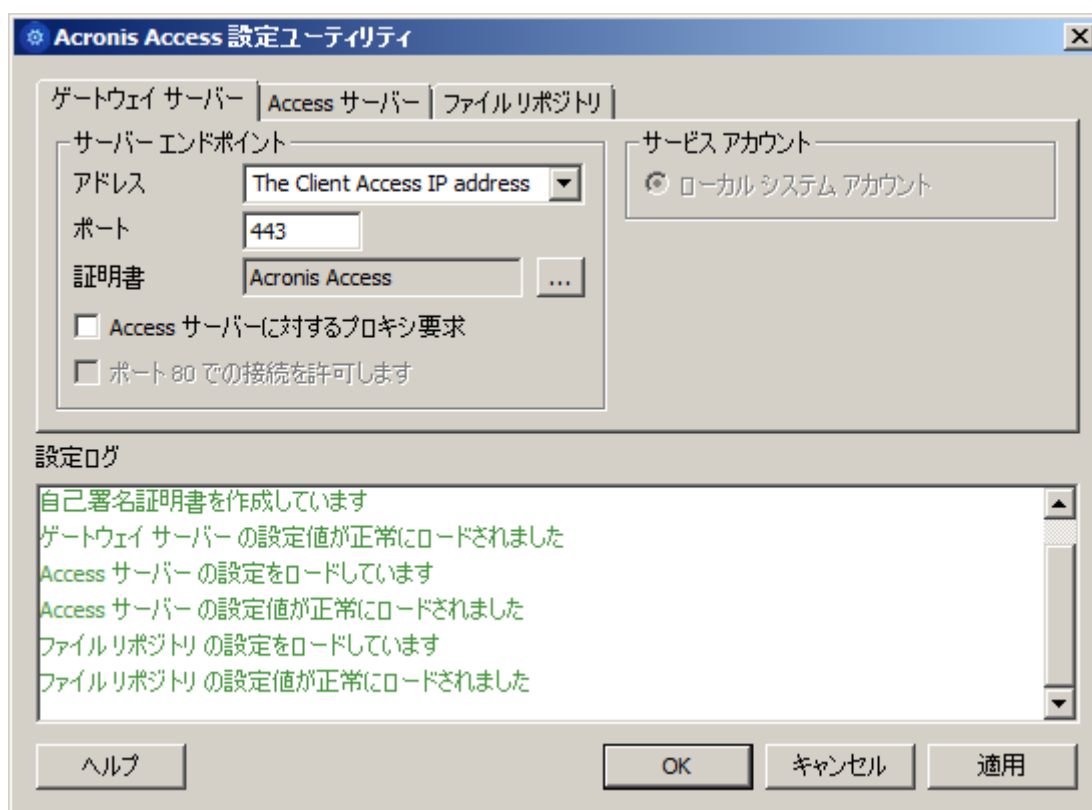


5. [OK] を押します。

## クラスタ グループをオンラインにして設定ユーティリティを使用する

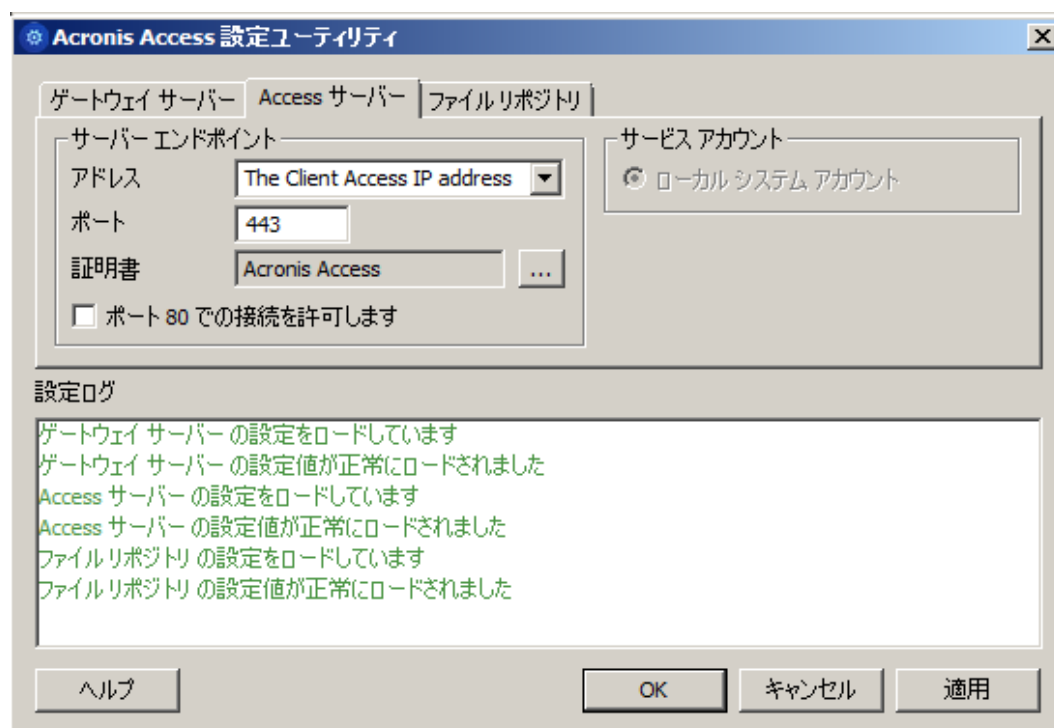
1. クラスタ グループを右クリックし、[Bring online] をクリックします。
2. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。

3. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

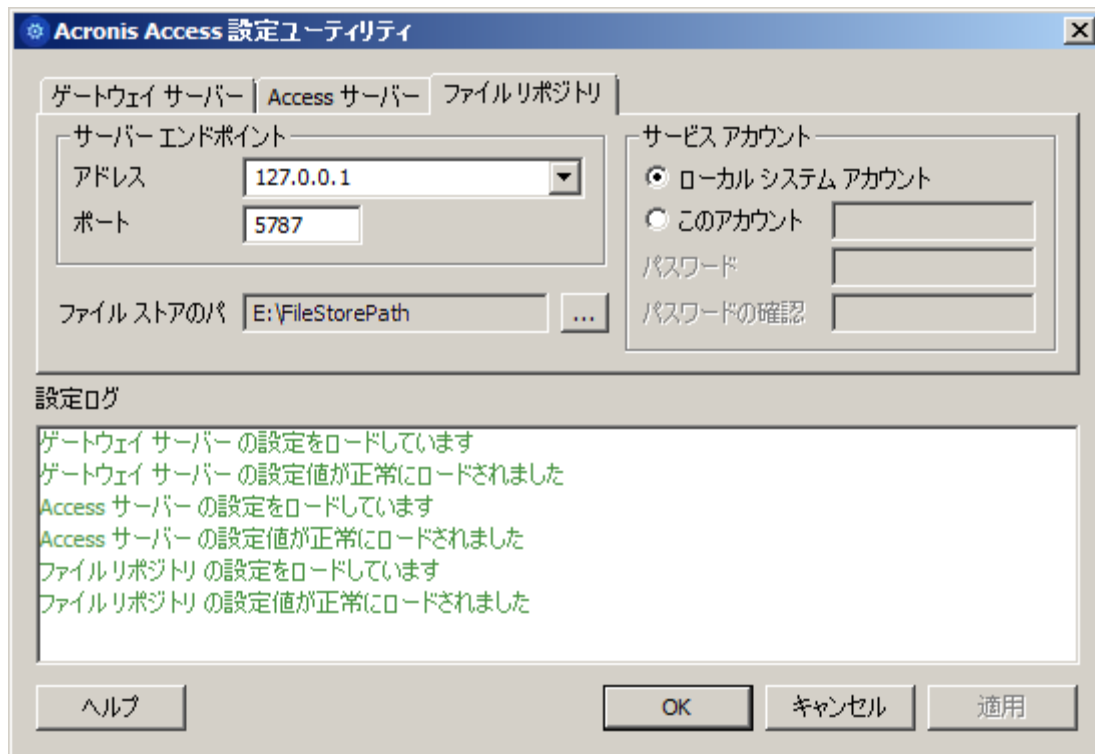


4. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



5. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



6. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Acronis Access をインストールします。ただし、今回は、デフォルトの **Postgres データ** ロケーション、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。

4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\Acronis\Access\Gateway Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます(例: **database\_path: 'S:/access\_cluster/database/')**。

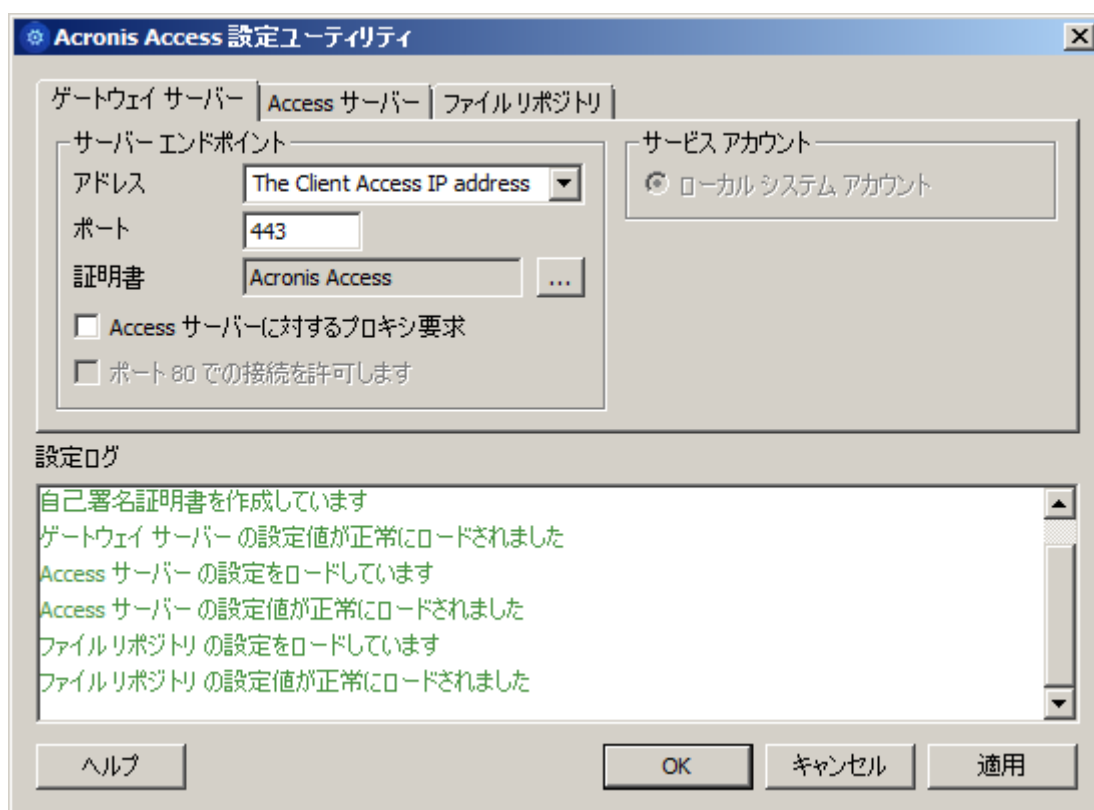
**注意:** パスの区切りにはスラッシュ(/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

**注意:** このパスは第 1 ノードで設定されているパスと同じでなければなりません。

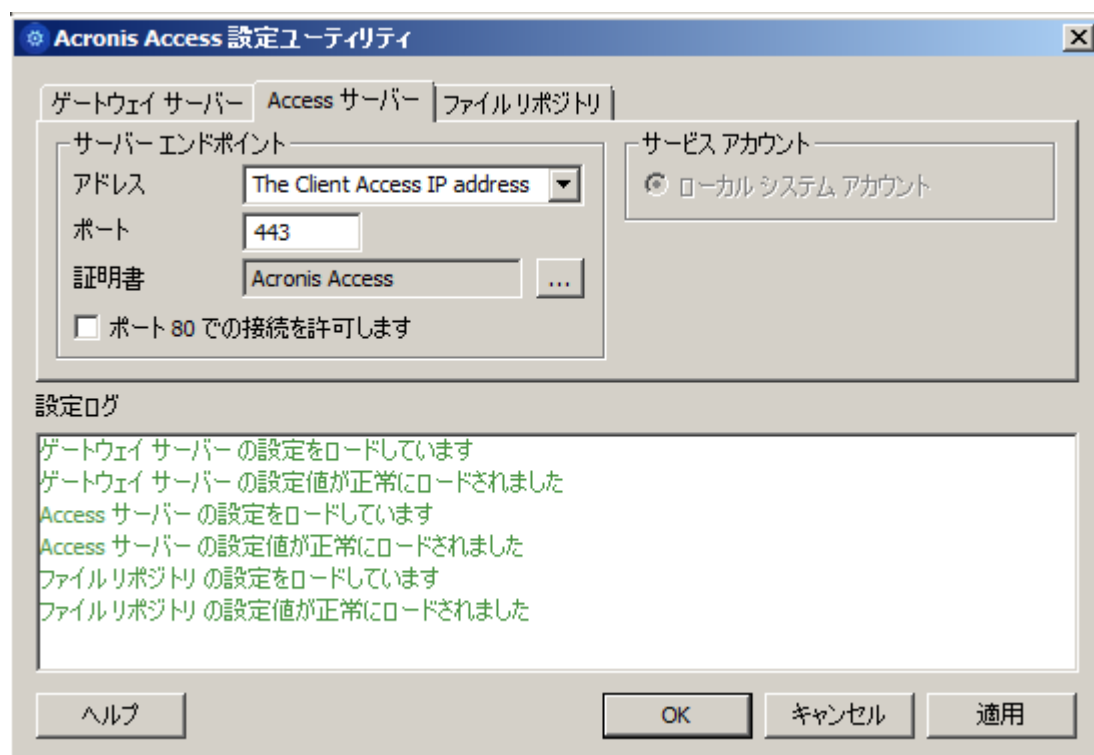
5. クラスタ グループを第 2 ノードに移動します。そのためには、クラスタ グループを右クリックして **[Move Group]** をクリックします。
6. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。

7. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

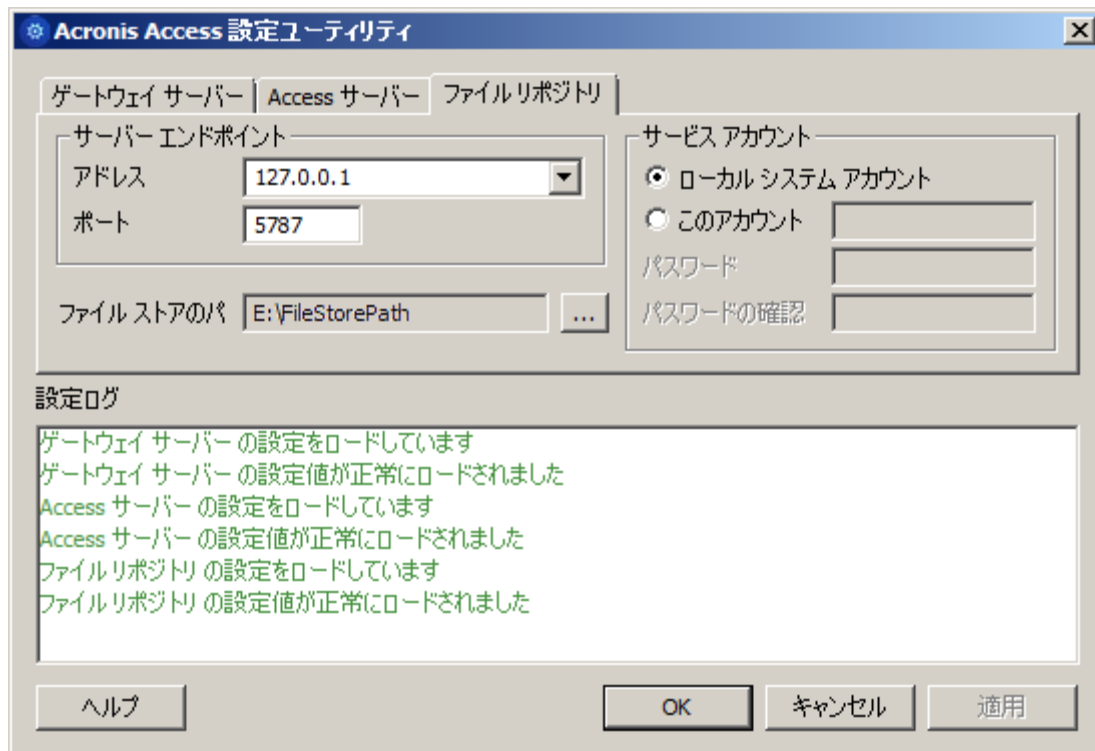


8. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



9. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



10. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 2.2 Windows 2008 Microsoft フェールオーバー クラスタ 上での Acronis Access のインストール

### Acronis Access のインストール

管理者としてログインしていることを確認してから Acronis Access をインストールしてください。

1. Acronis Access のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。



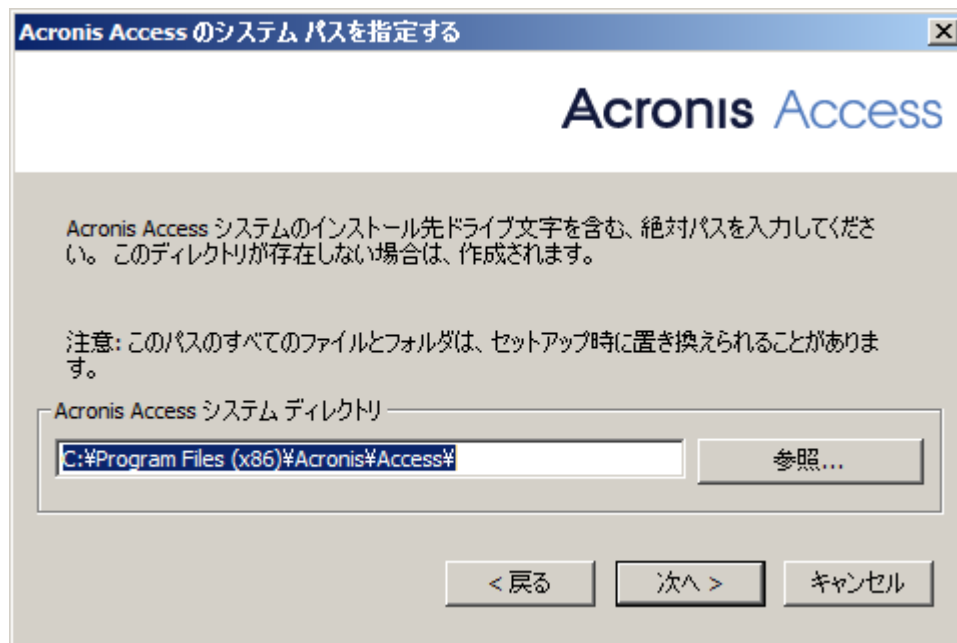
3. 実行可能なインストーラをダブルクリックします。



4. [次へ] を押して開始します。  
5. 使用許諾契約を読み、承諾します。  
6. [インストール] を押します。

注意: 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

7. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、[OK] を押します。



8. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。

9. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して **[次へ]** をクリックします。

ローカルの PostgreSQL の構成

Acronis Access

PostgreSQL のインストール ロケーション:

データパス: S:\PSQL 参照...

PostgreSQL スーパーユーザー資格情報:

PostgreSQL スーパーユーザー パスワード: \*\*\*\*\*

パスワードを再入力してください: \*\*\*\*\*

PostgreSQL ポート: 5432

リモート アクセスのためにファイアウォールのこのポートを開く: ☐

< 戻る 次へ > キャンセル

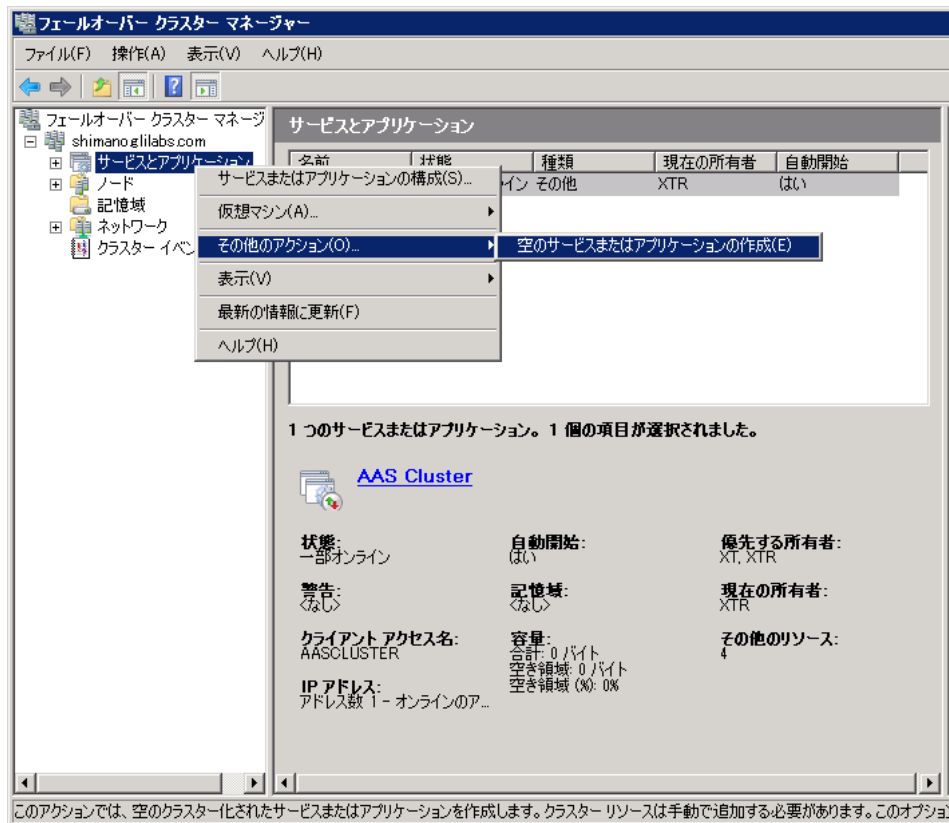
10. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。

**Acronis Access** のインストーラが完了したら、**[終了]** を押します。

### サービス グループの作成

1. **[フェールオーバー クラスタ マネージャ]** を開き、使用するクラスタを展開します。
2. **[サービスとアプリケーション]** を右クリックし、**[他の操作]** を選択します。

3. **[空のサービスまたはアプリケーションの作成]** を選択して **[次へ]** をクリックします。サービスグループに適切な名前を付けます。(Acronis Access、AAS クラスタなど)。



## アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\Acronis\Access\Gateway Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます (例: **database\_path: 'S:/access\_cluster/database/'**)。

**注意:** パスの区切りにはスラッシュ (/) を使用します。

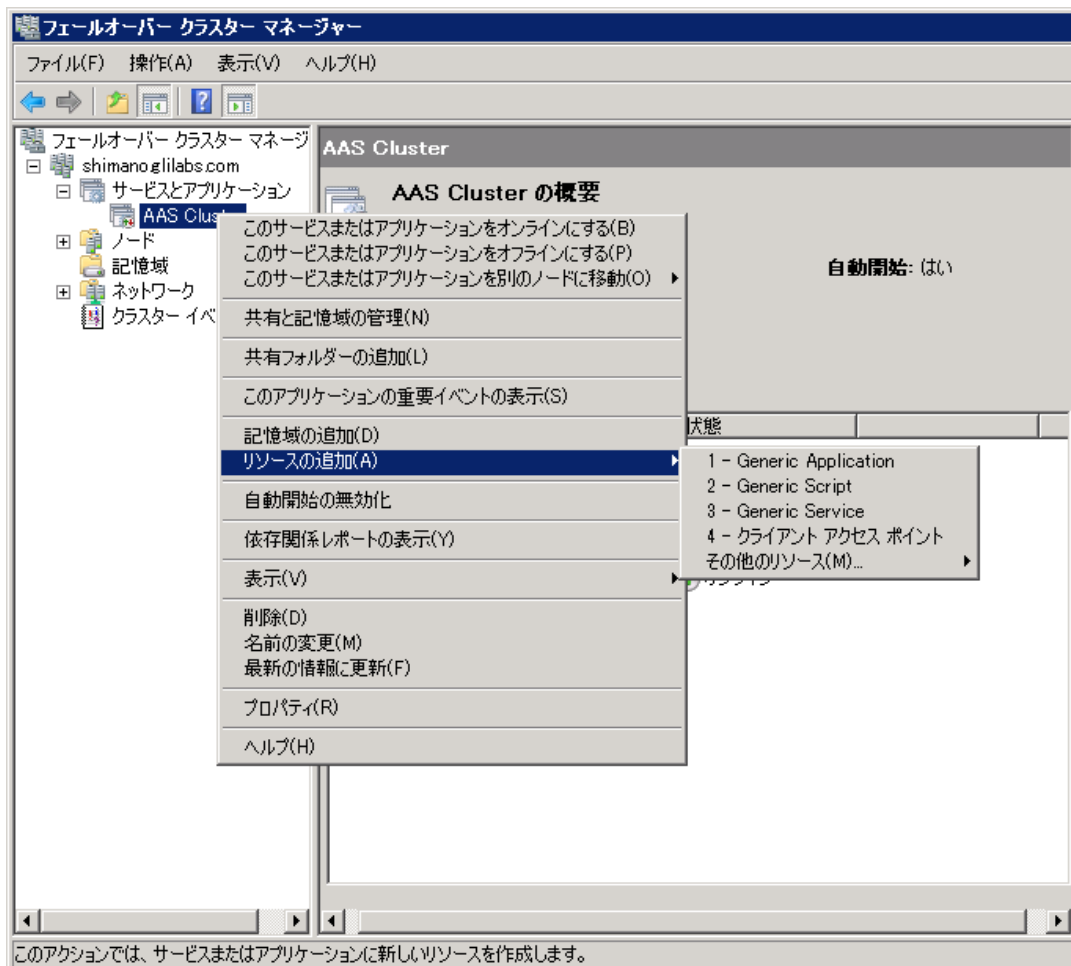
**注意:** 第 1 ノードで設定した **database.yml** をコピーして、第 2 ノードに貼り付けることができます。

## 必要なすべてのサービスを Acronis Access サービス グループに追加する

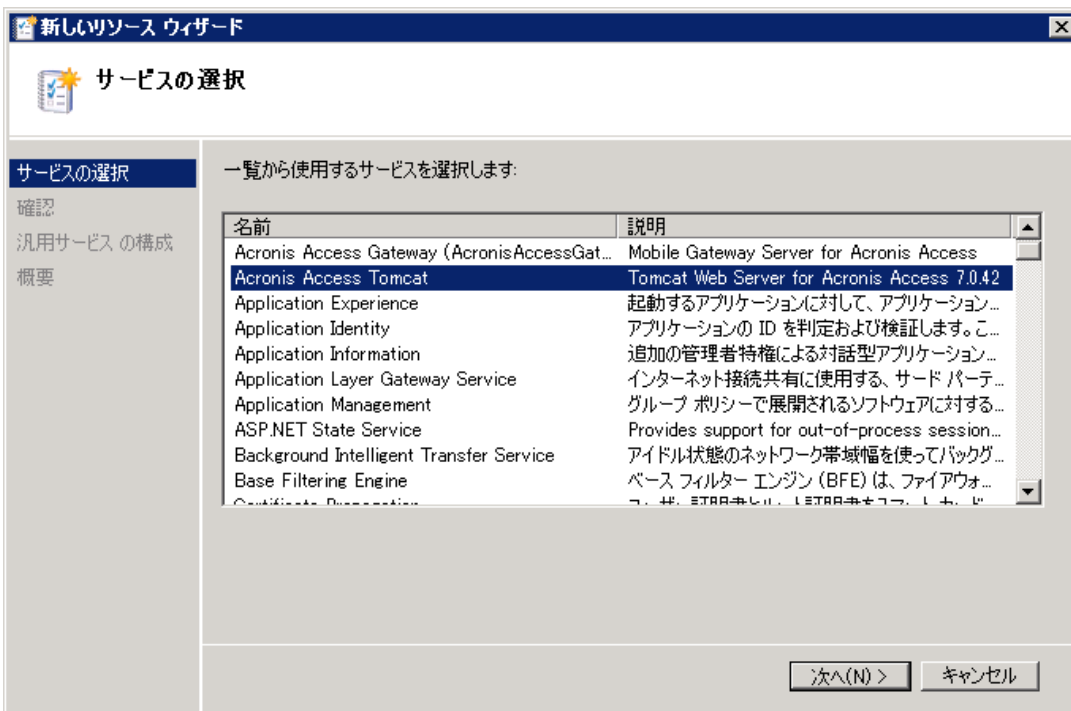
AcronisAccessGateway、AcronisAccessPostgreSQL (Acronis Access のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Acronis Access サービス グループを右クリックして、**[リソースの追加]** を選択します。

2. [汎用サービス] を選択します。



3. 適切なサービスを選択して [次へ] をクリックします。

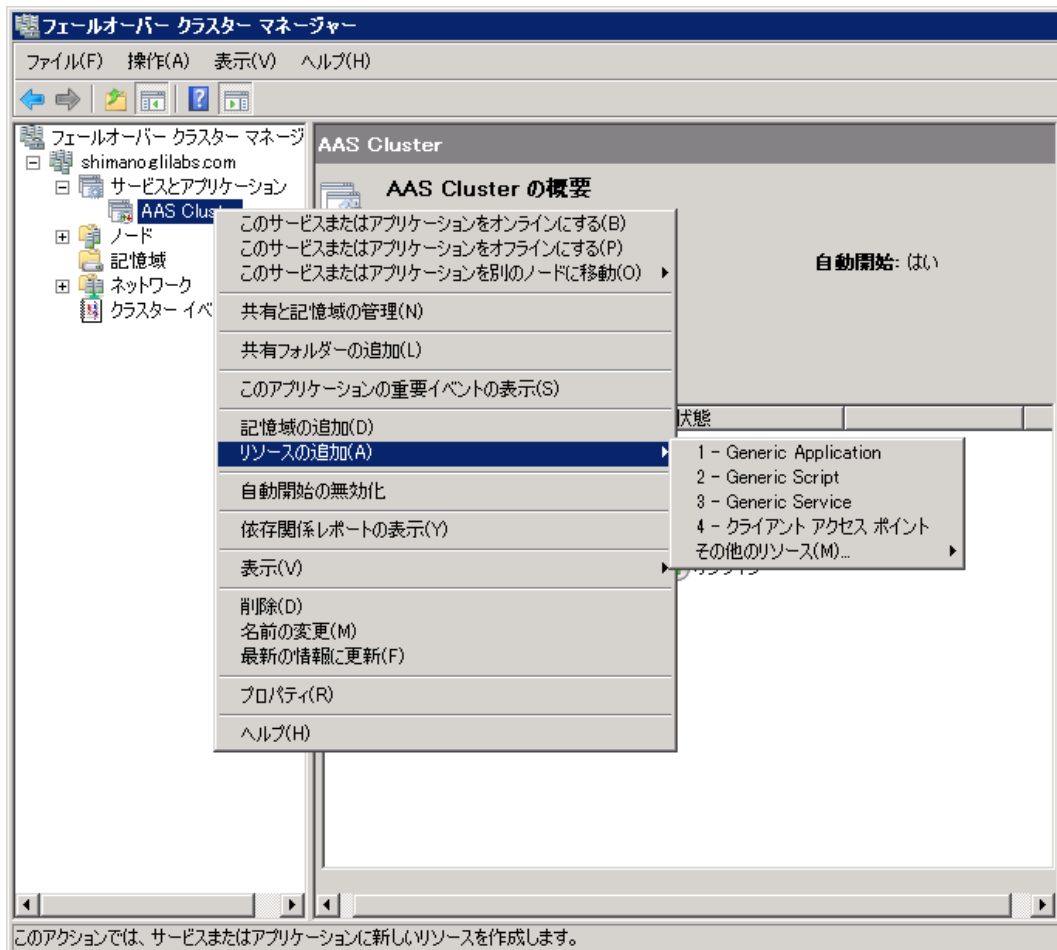


4. 確認ウィンドウで [次へ] をクリックします。

5. [レジストリ設定のレプリケート] ウィンドウで [次へ] をクリックします。
6. 概要ウィンドウで [完了] をクリックします。

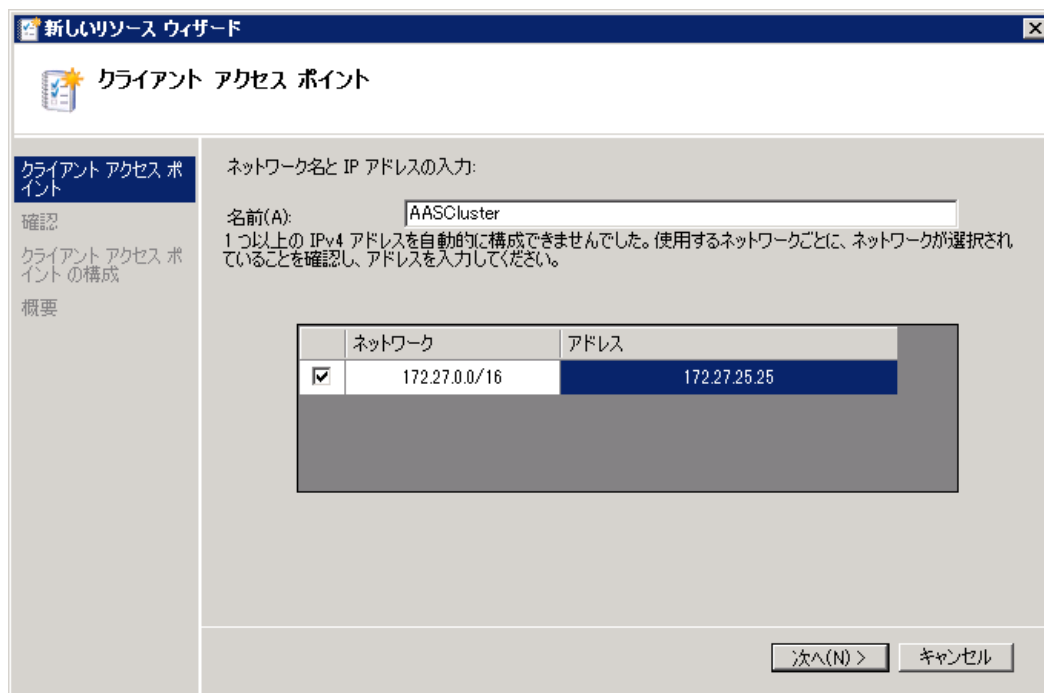
## クライアント アクセス ポイントの設定

1. Acronis Access サービス グループを右クリックして、[リソースの追加] を選択します。
2. [クライアント アクセス ポイント] を選択します。



3. このアクセス ポイントの名前を入力します。

#### 4. ネットワークを選択します。



5. IP アドレスを入力して [次へ] をクリックします。

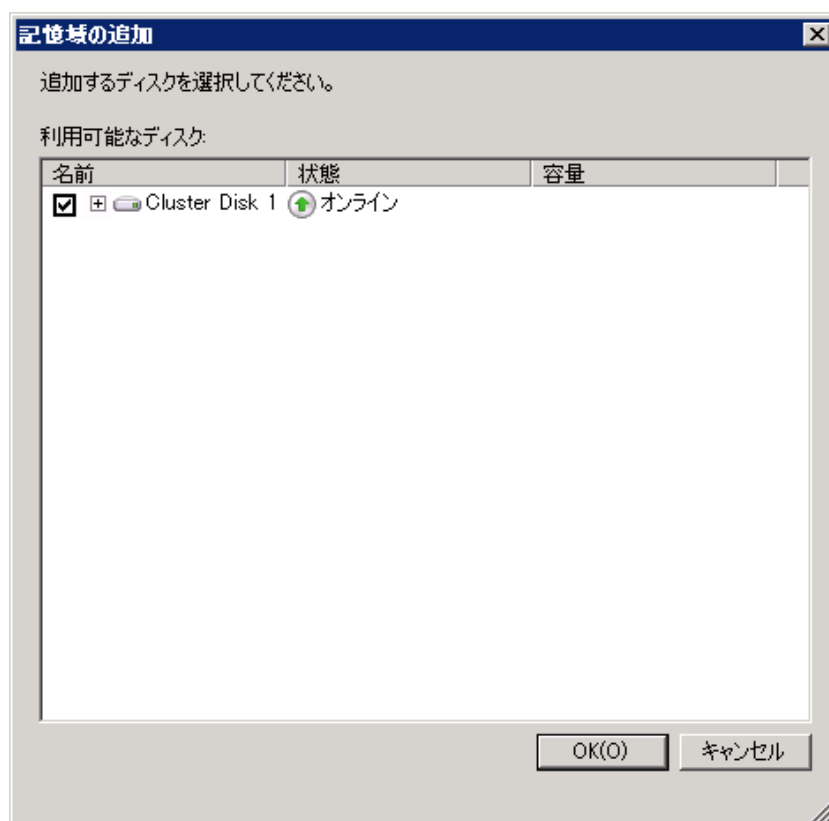
6. 確認ウィンドウで [次へ] をクリックします。

7. 概要ウィンドウで [完了] をクリックします。

### 共有ディスクの追加

1. Acronis Access サービス グループを右クリックして、[リソースの追加] を選択します。

2. 共有ドライブを選択します。



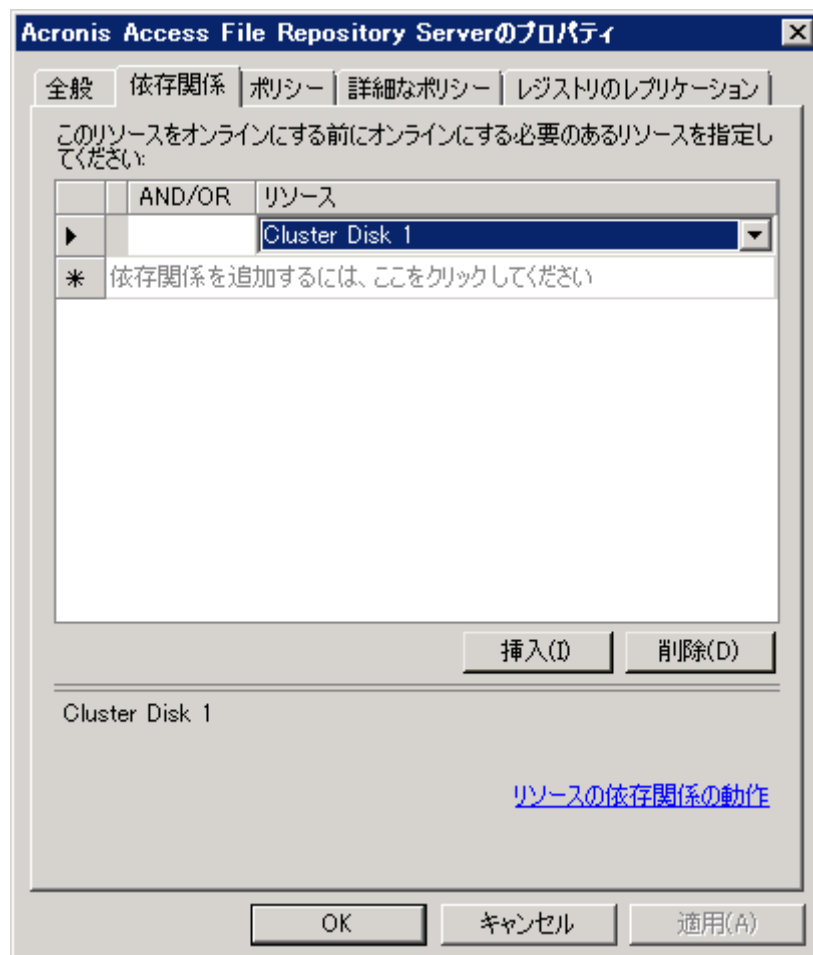
3. 確認ウィンドウで [次へ] をクリックします。
4. 概要ウィンドウで [完了] をクリックします。

## 依存関係の設定

1. Acronis Access サービス グループをダブルクリックします。

**PostgreSQL および Acronis Access ファイル リポジトリ サービスについて、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。
3. [リソース] をクリックし、追加した共有ディスクを選択します。

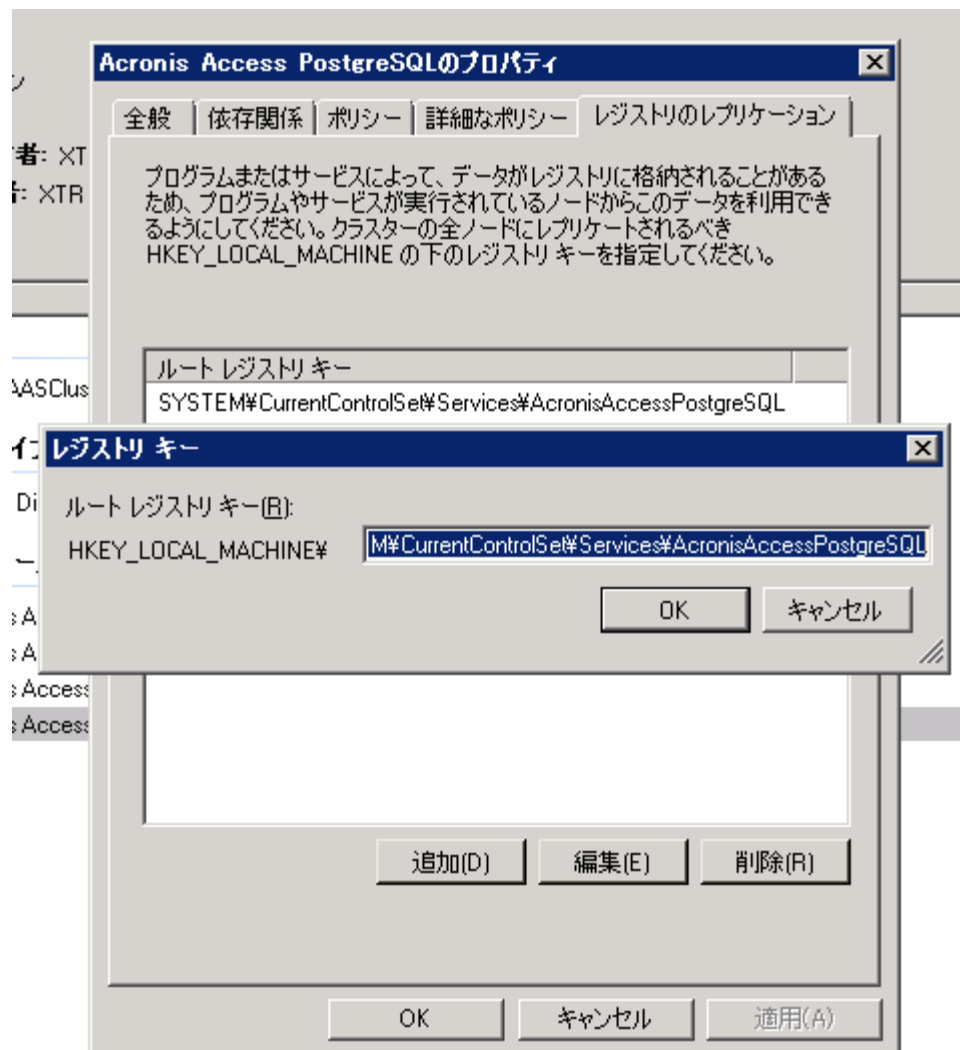


4. [適用] をクリックしてウィンドウを閉じます。

**PostgreSQL では、次の操作も実行します。**

1. [レジストリ レプリケーション] タブをクリックします。

2. **[追加]** を押し、**SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\** のように入力します (旧バージョンの Acronis Access の場合、サービスが **postgresql-x64-9.2** のように異なることがあります)。

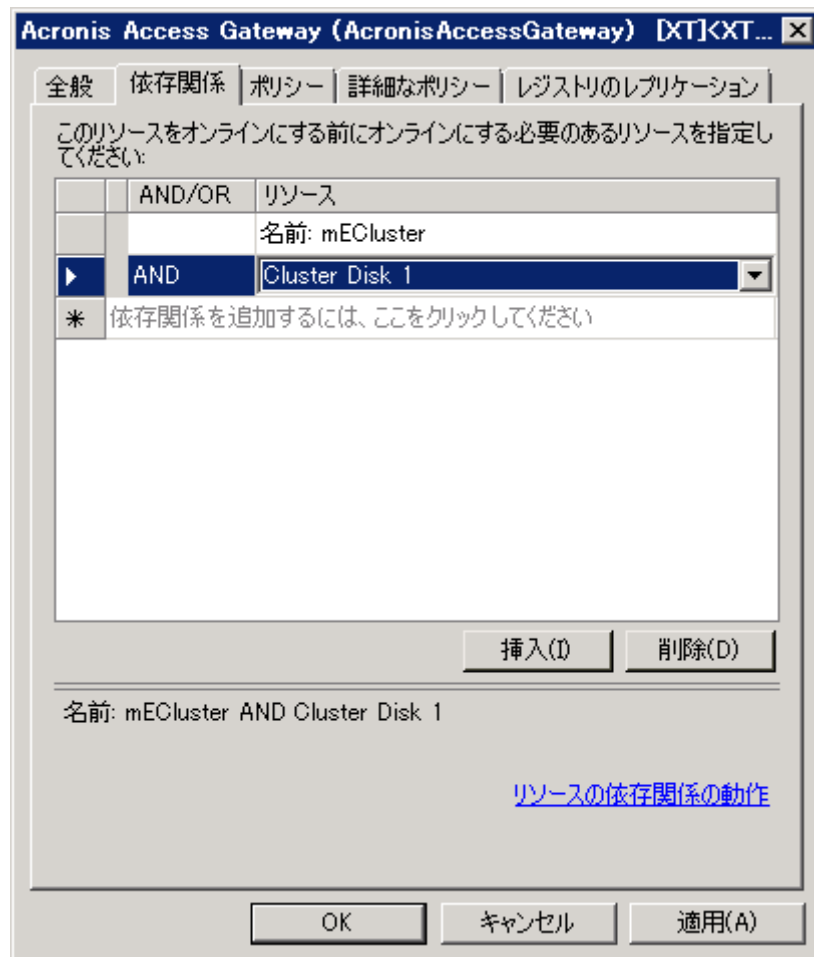


**Acronis Access ゲートウェイ サーバー サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、**[プロパティ]** を選択します。
2. **[依存関係]** タブをクリックします。



3. [リソース] をクリックしてから、追加した共有ディスク、およびネットワーク名(クライアント アクセス ポイントの名前)を選択します。

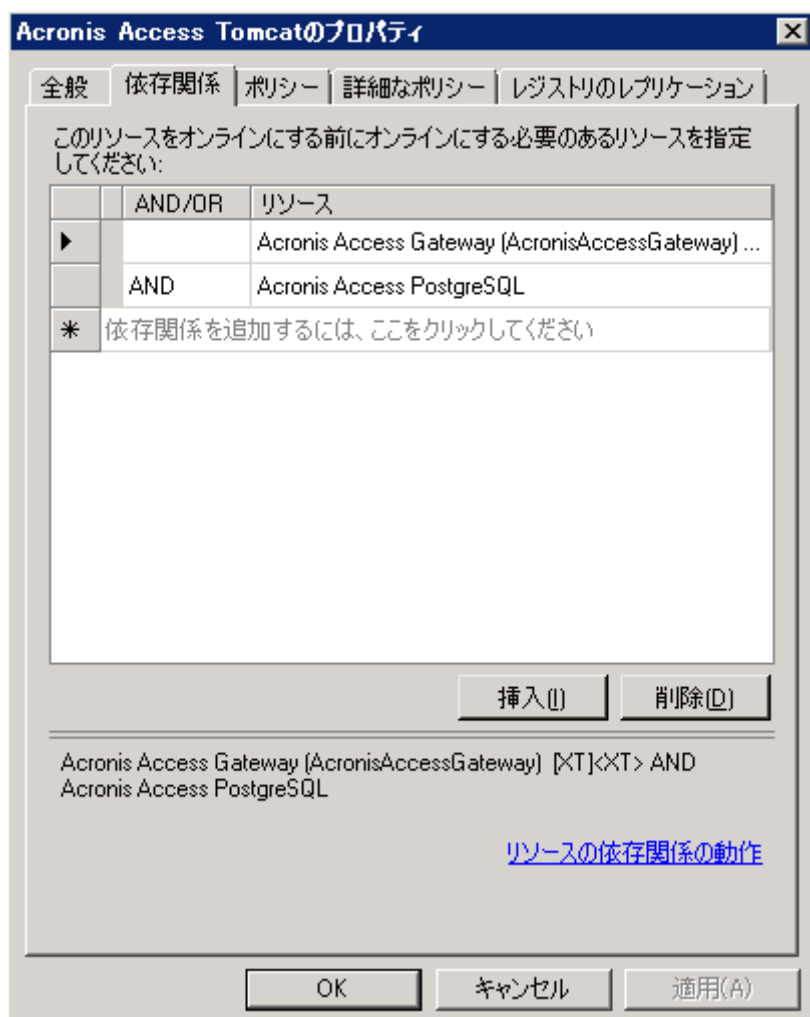


4. [適用] をクリックしてウィンドウを閉じます。

**Acronis Access Tomcat サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックし、依存関係として、PostgreSQL および Acronis Access ゲートウェイ サーバーのサービスを選択します。[適用] をクリックしてウィンドウを閉じます。



**注意:** ゲートウェイ サーバーと Access サーバーを異なる IP アドレスで実行する場合は、Acronis Access サービス グループに第 2 IP をリソースとして追加し、ネットワーク名の依存関係として設定します。

## サービス グループをオンラインにし、設定ユーティリティを使用する

1. Acronis Access サービス グループを右クリックし、[Bring this application or service group online] を押します。
2. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。

3. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**Acronis Access 設定ユーティリティ**

ゲートウェイ サーバー | **Access サーバー** | ファイルリポジトリ

サーバー エンドポイント

アドレス: The Client Access IP address

ポート: 443

証明書: Acronis Access

☐ Access サーバーに対するプロキシ要求

☐ ポート 80 での接続を許可します

サービス アカウント

☒ ローカル システム アカウント

設定ログ

自己署名証明書を作成しています  
ゲートウェイ サーバー の設定値が正常にロードされました  
Access サーバー の設定をロードしています  
Access サーバー の設定値が正常にロードされました  
ファイルリポジトリ の設定をロードしています  
ファイルリポジトリ の設定値が正常にロードされました

ヘルプ OK キャンセル 適用

4. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。

**Acronis Access 設定ユーティリティ**

ゲートウェイ サーバー | **Access サーバー** | ファイルリポジトリ

サーバー エンドポイント

アドレス: The Client Access IP address

ポート: 443

証明書: Acronis Access

☐ ポート 80 での接続を許可します

サービス アカウント

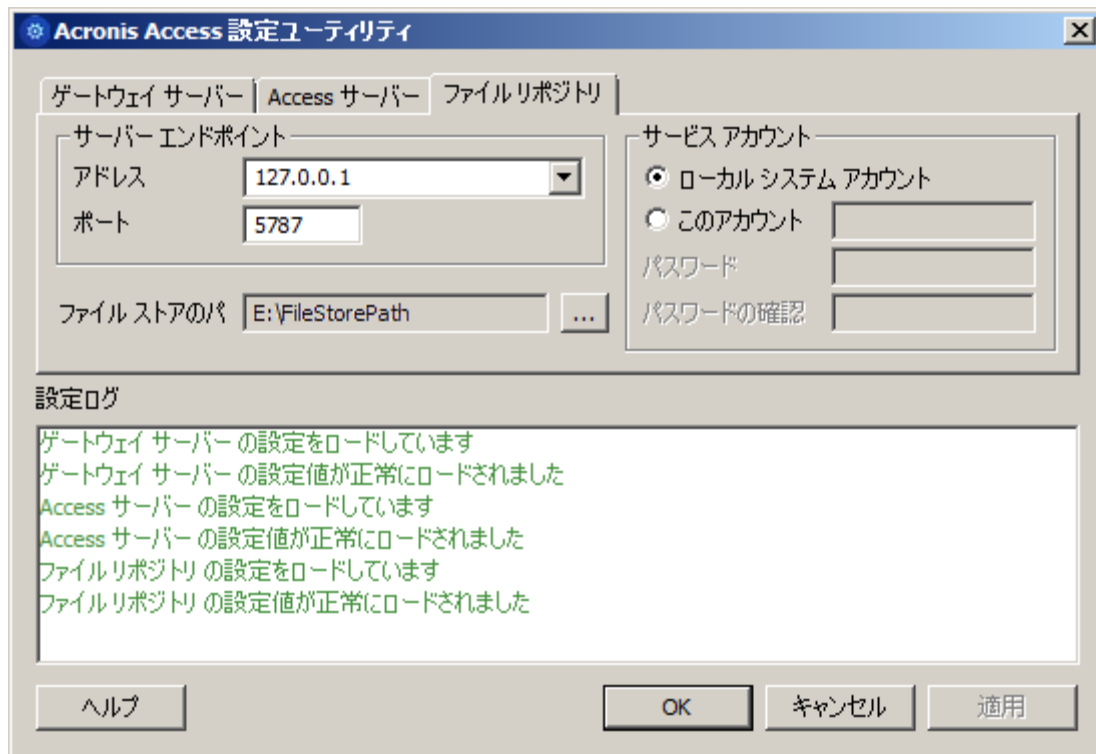
☒ ローカル システム アカウント

設定ログ

ゲートウェイ サーバー の設定をロードしています  
ゲートウェイ サーバー の設定値が正常にロードされました  
Access サーバー の設定をロードしています  
Access サーバー の設定値が正常にロードされました  
ファイルリポジトリ の設定をロードしています  
ファイルリポジトリ の設定値が正常にロードされました

ヘルプ OK キャンセル 適用

5. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



6. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Acronis Access をインストールします。ただし、今回は、デフォルトの **Postgres データ** ロケーション、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。

4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。

- a. **C:\Program Files (x86)\Acronis\Access\Gateway Server\** に移動します。
- b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
- c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます(例: **database\_path: 'S:/access\_cluster/database/')**。

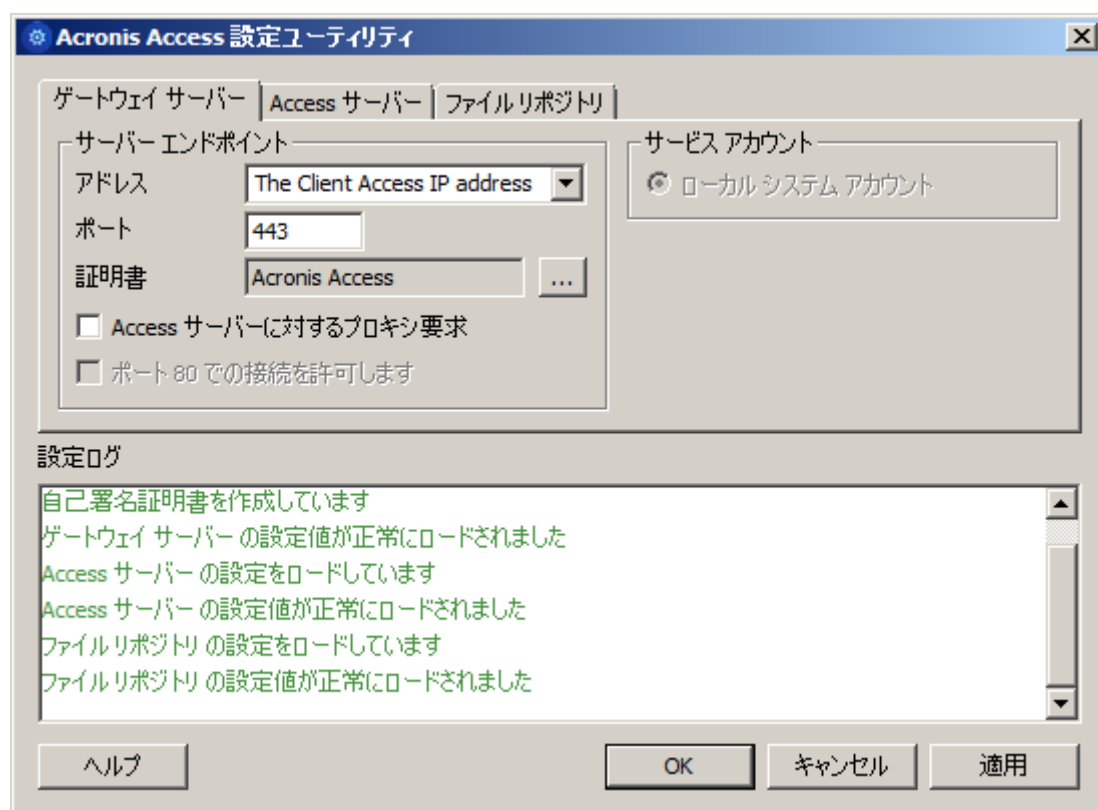
**注意:** パスの区切りにはスラッシュ(/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

**注意:** このパスは第 1 ノードで設定されているパスと同じでなければなりません。

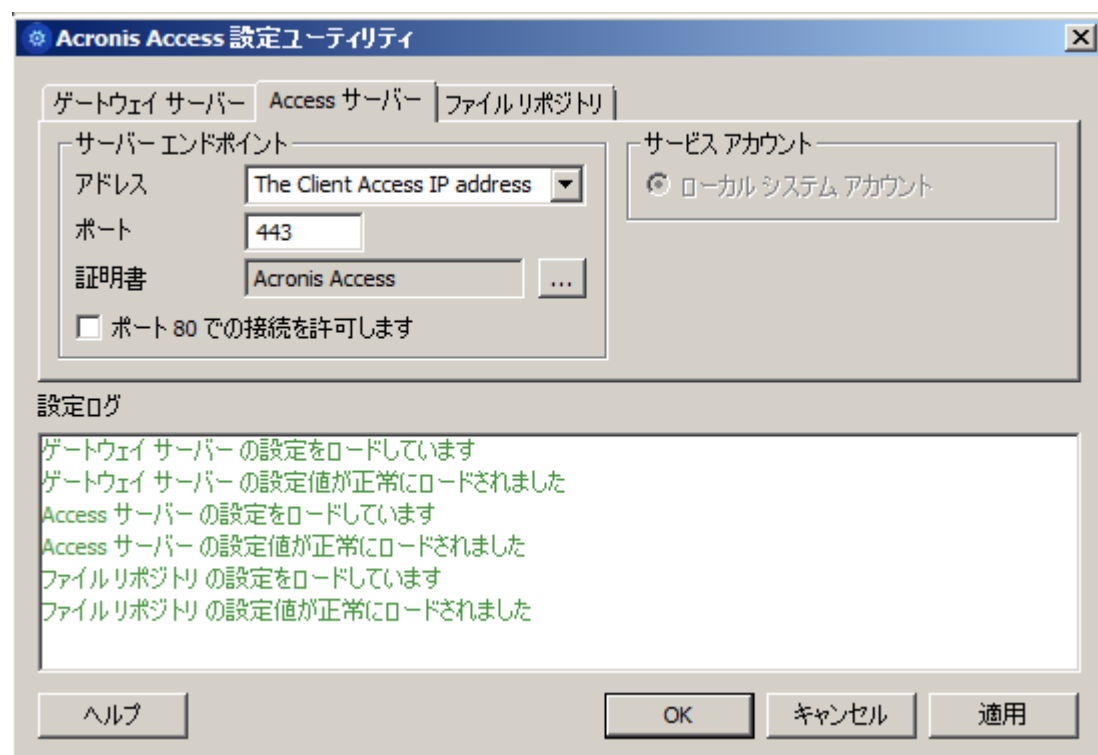
5. Acronis Access サービス グループを第 2 ノードに移動します。そのためには、そのサービス グループを右クリックして [第 2 ノードに移動] をクリックします。
6. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。

7. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

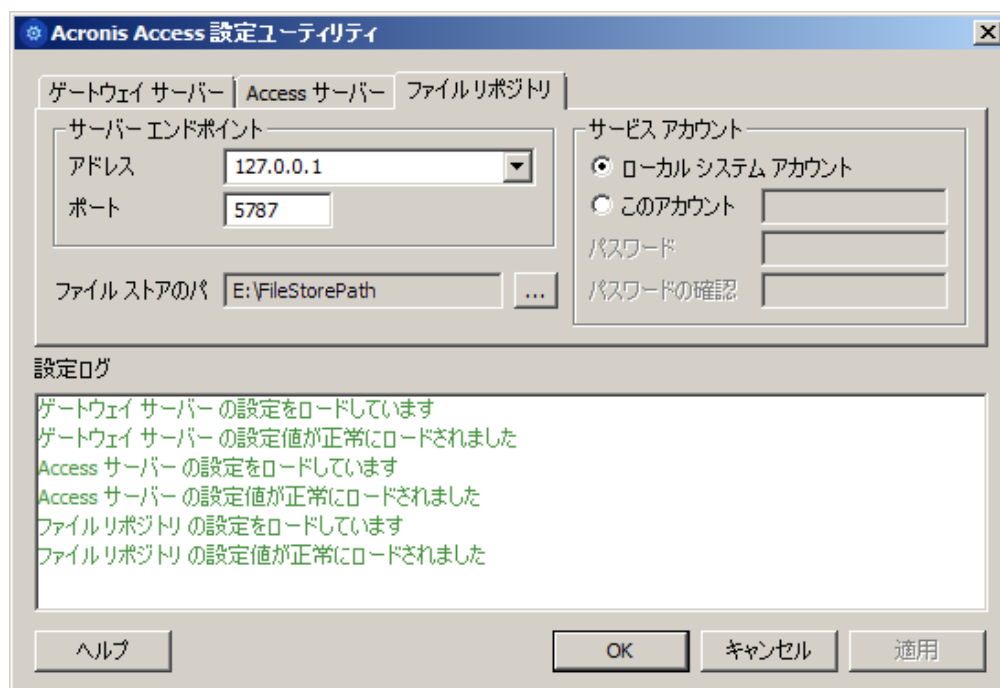


8. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



9. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



10. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 2.3 Windows 2012 Microsoft フェールオーバー クラスタ 上での Acronis Access のインストール

### Acronis Access のインストール

管理者としてログインしていることを確認してから Acronis Access をインストールしてください。

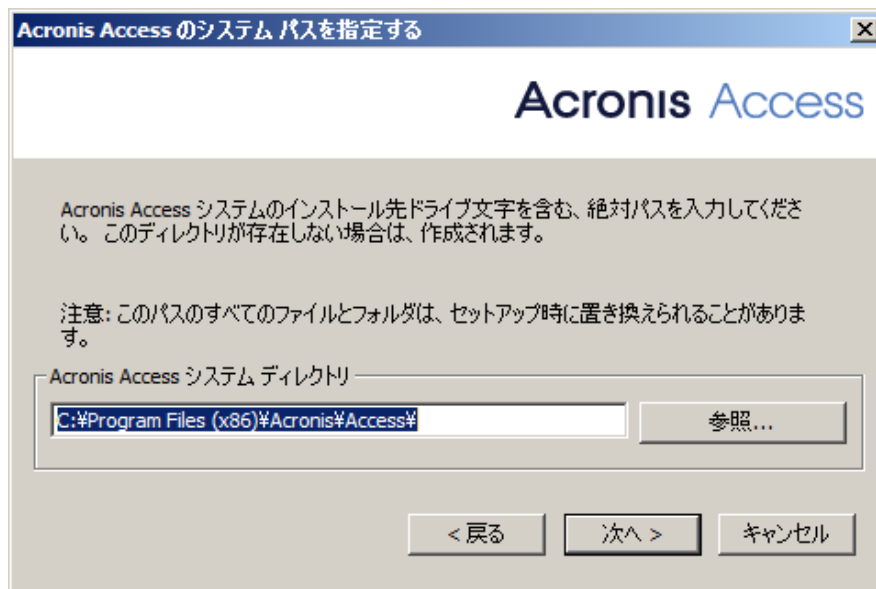
1. Acronis Access のインストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。



4. **[次へ]** を押して開始します。
5. 使用許諾契約を読み、承諾します。
6. **[インストール]** を押します。

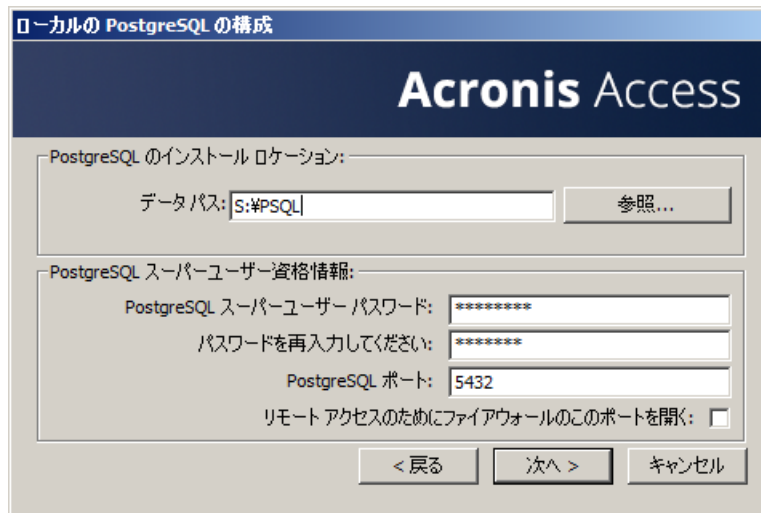
**注意:** 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

7. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、**[OK]** を押します。



8. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。

- 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して [次へ] をクリックします。

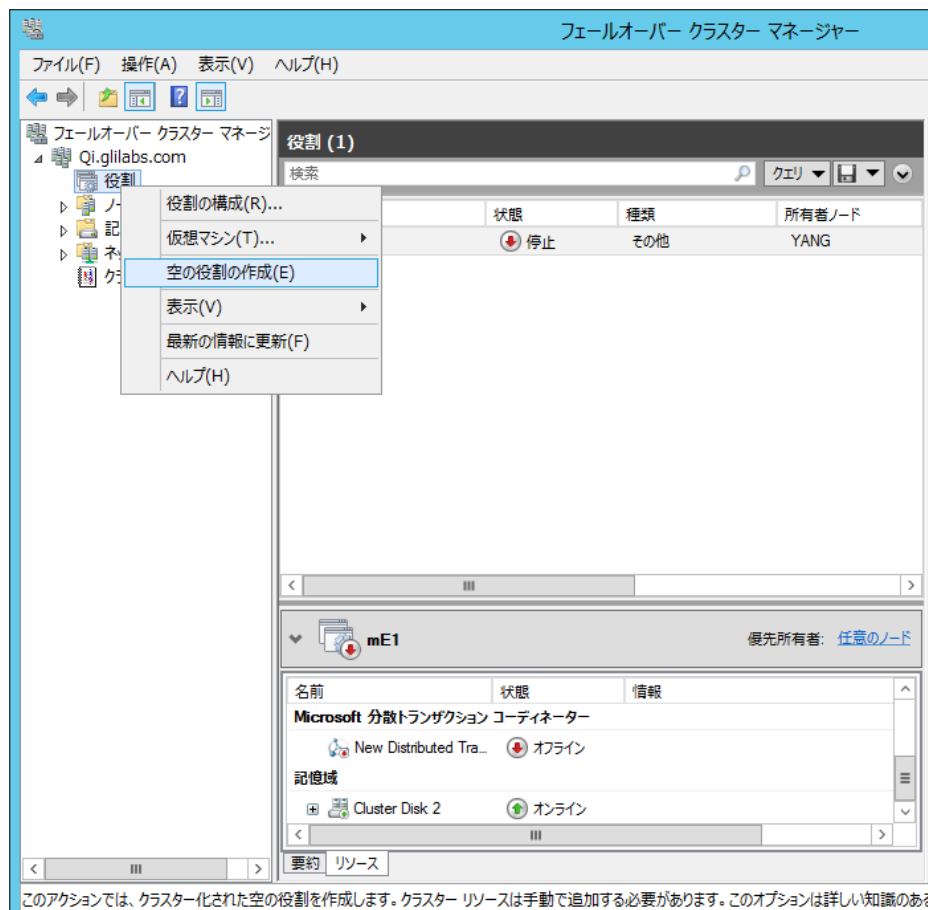


- インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、[OK] を押します。

Acronis Access のインストーラが完了したら、[終了] を押します。

## 役割の作成

- [フェールオーバー クラスタ マネージャ] を開き、[役割] を右クリックします。
- [空の役割の作成] を選択します。役割に適切な名前を付けます (Acronis Access、AAS クラスタなど)。





## アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\Acronis\Access\Gateway Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます(例: **database\_path: 'S:/access\_cluster/database/'**)。

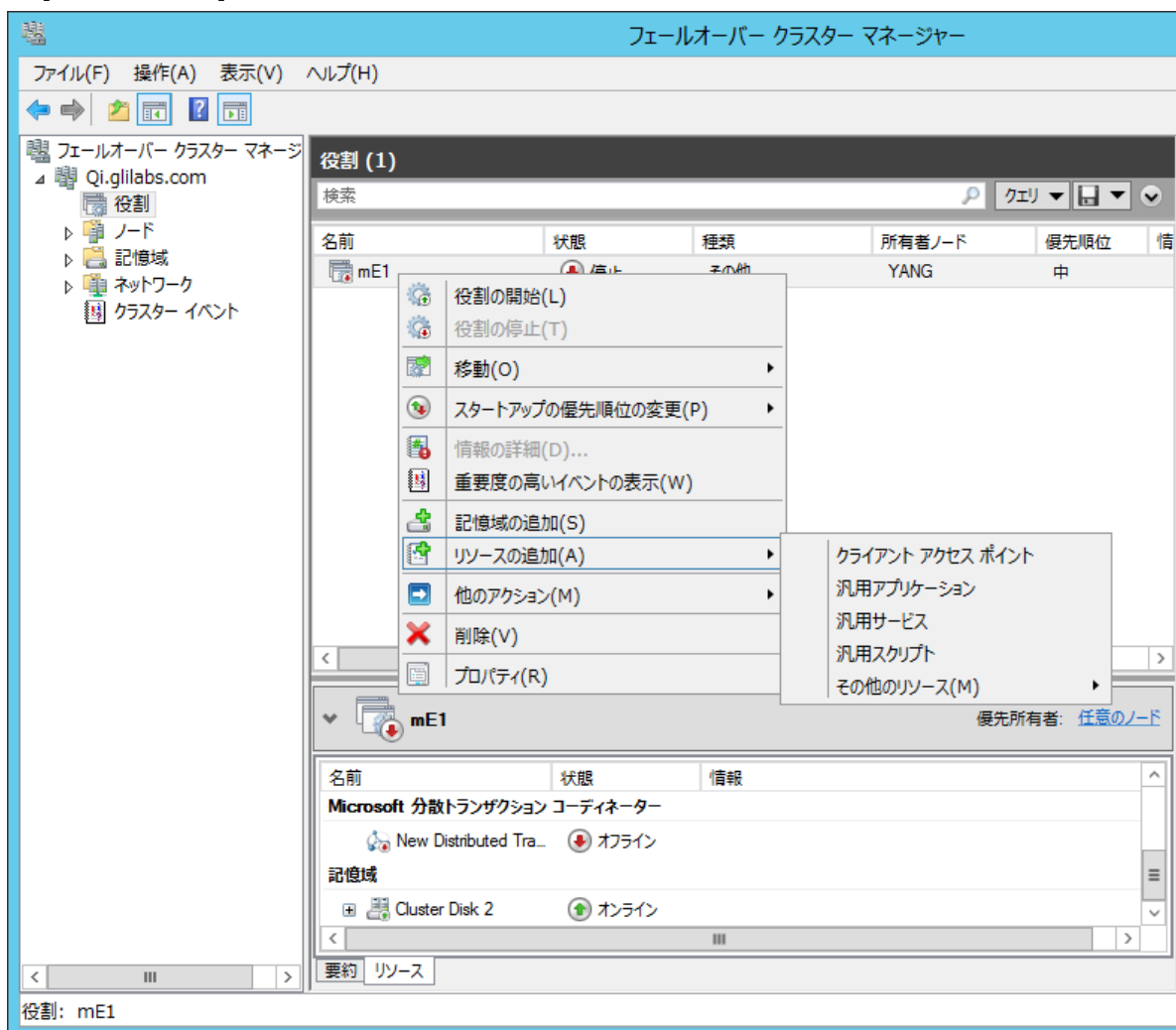
**注意:** パスの区切りにはスラッシュ (/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

## 必要なすべてのサービスを Acronis Access 役割に追加する

AcronisAccessGateway、AcronisAccessPostgreSQL (Acronis Access のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Acronis Access 役割を右クリックして、[リソースの追加] を選択します。
2. [汎用サービス] を選択します。



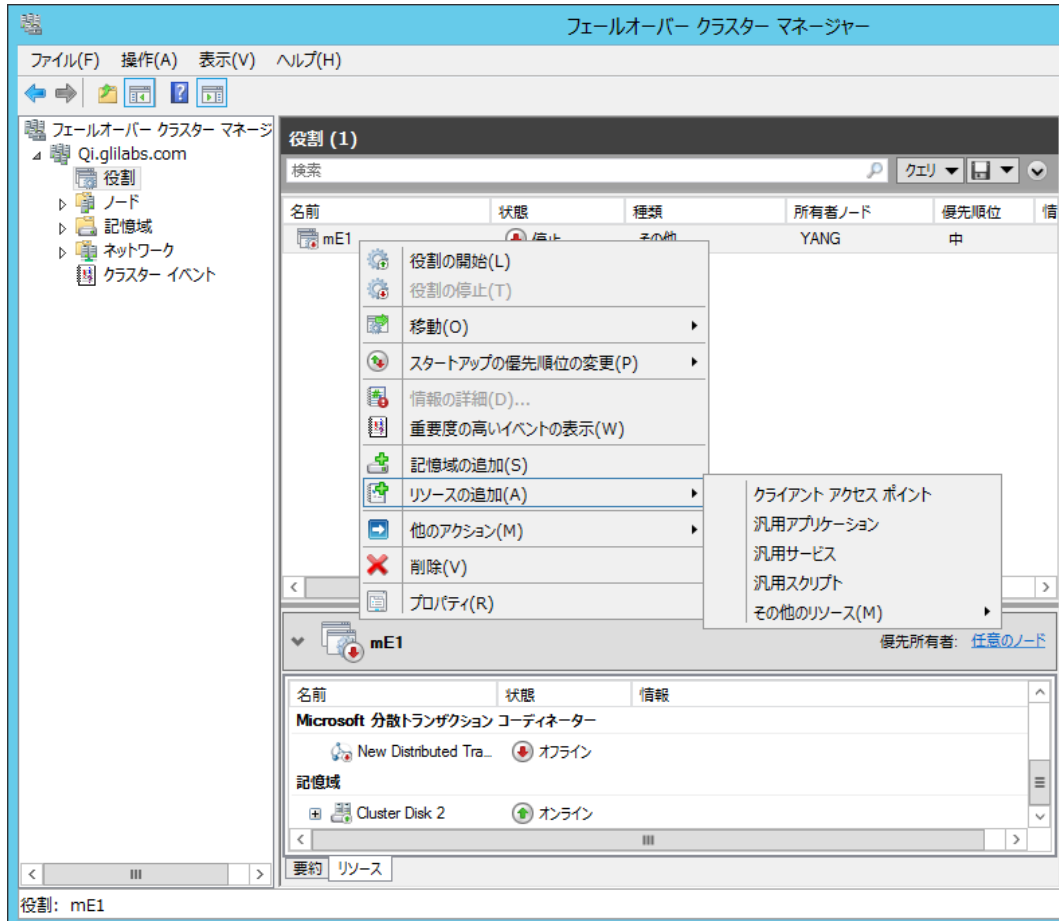
- 適切なサービスを選択して [次へ] をクリックします。



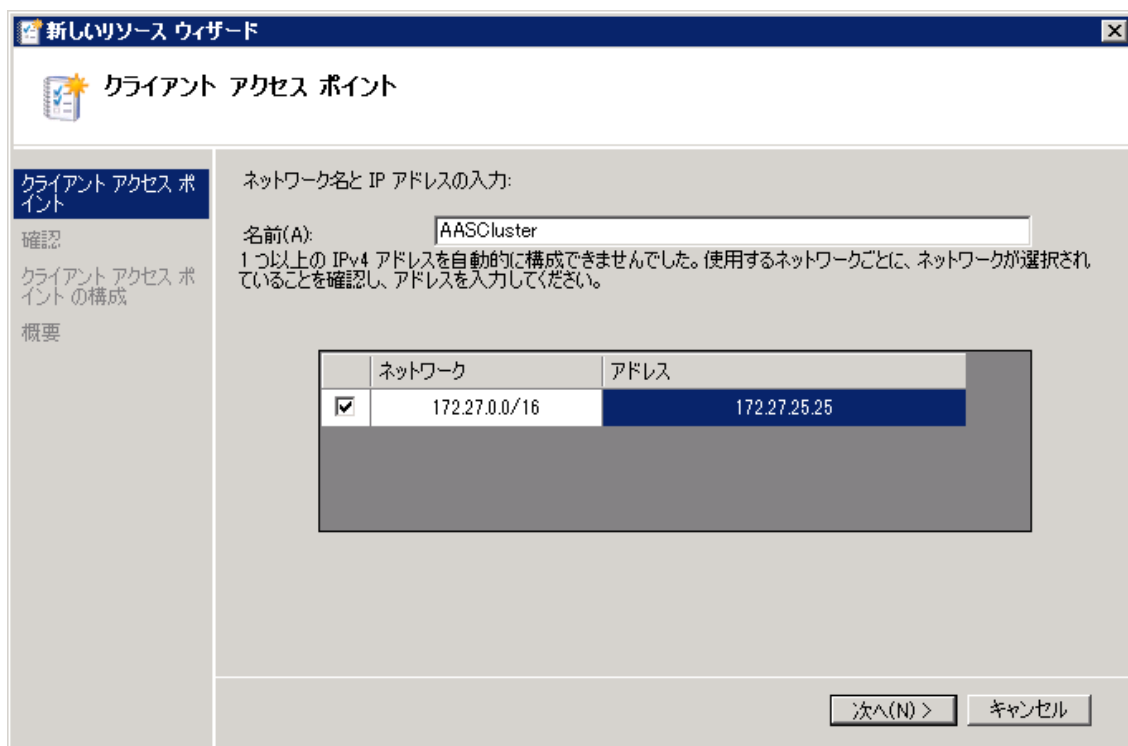
- 確認ウィンドウで [次へ] をクリックします。
- 概要ウィンドウで [完了] をクリックします。

## アクセス ポイントの設定

- Acronis Access 役割を右クリックして、[リソースの追加] を選択します。
- [クライアント アクセス ポイント] を選択します。



3. このアクセス ポイントの名前を入力します。
4. ネットワークを選択します。



新しいリソース ウィザード

クライアント アクセス ポイント

クライアント アクセス ポイント

確認

クライアント アクセス ポイント の構成

概要

ネットワーク名と IP アドレスの入力:

名前(A): AASCluster

1 つ以上の IPv4 アドレスを自動的に構成できませんでした。使用するネットワークごとに、ネットワークが選択されていることを確認し、アドレスを入力してください。

|                                     | ネットワーク        | アドレス         |
|-------------------------------------|---------------|--------------|
| <input checked="" type="checkbox"/> | 172.27.0.0/16 | 172.27.25.25 |

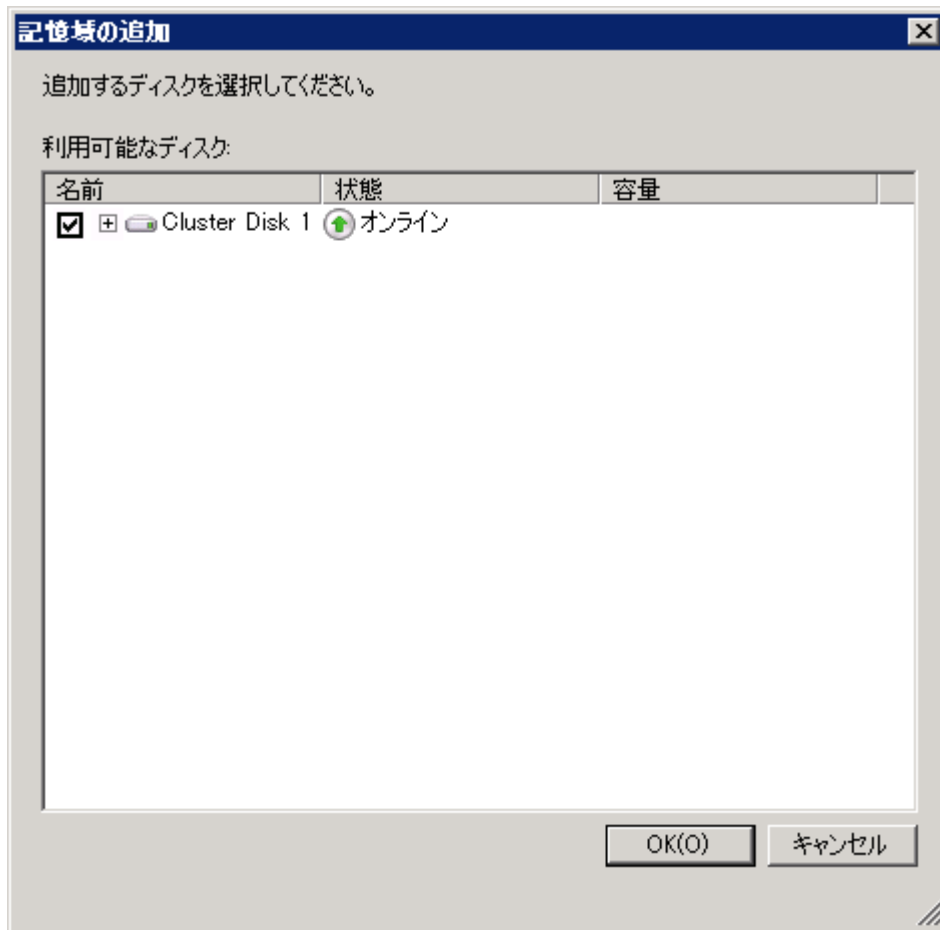
次へ(N) > キャンセル

5. IP アドレスを入力して [次へ] をクリックします。
6. 確認ウィンドウで [次へ] をクリックします。
7. 概要ウィンドウで [完了] をクリックします。

## 共有ディスクの追加

1. Acronis Access 役割を右クリックして、[ストレージの追加] を選択します。

2. 共有ドライブを選択します。



## 依存関係の設定

1. Acronis Access の役割を選択し、[リソース] タブをクリックします。

**PostgreSQL および Acronis Access ファイル リポジトリ サービスについて、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックし、追加した共有ディスクを選択します。

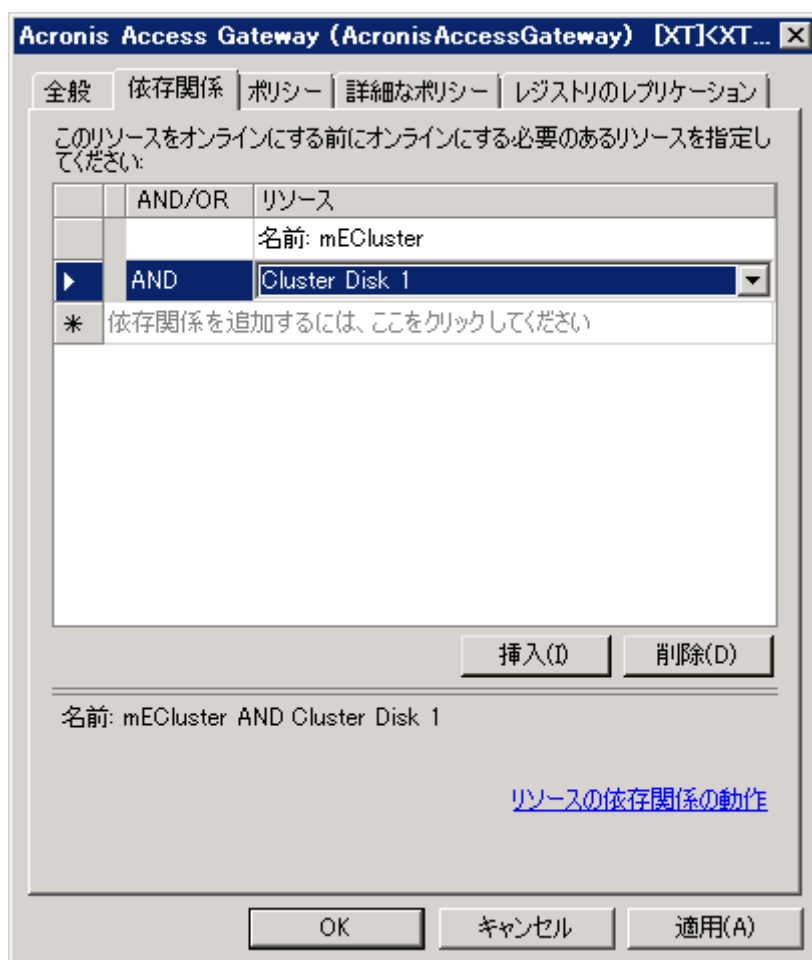


4. [適用] をクリックしてウィンドウを閉じます。

**Acronis Access ゲートウェイ サーバー サービスについて、次のことを実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックしてから、追加した共有ディスク、およびネットワーク名（クライアント アクセス ポイントの名前）を選択します。



4. [適用] をクリックしてウィンドウを閉じます。

**Acronis Access Tomcat サービスについて、次のことを実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。
3. [リソース] をクリックし、依存関係として、PostgreSQL および Acronis Access ゲートウェイ サーバーのサービスを選択します。[適用] をクリックしてウィンドウを閉じます。

**注意:** ゲートウェイ サーバーとアクセス サーバーを異なる IP アドレスで実行する場合は、第 2 IP をリソースとして Acronis Access 役割に追加し、それをネットワーク名の依存関係として設定します。



## 役割の開始と設定ユーティリティの使用

1. Acronis Access 役割を右クリックして、[役割の開始] を押します。
2. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。

3. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**Acronis Access 設定ユーティリティ**

ゲートウェイ サーバー | **Access サーバー** | ファイルリポジトリ

サーバー エンドポイント

アドレス: The Client Access IP address

ポート: 443

証明書: Acronis Access

☐ Access サーバーに対するプロキシ要求

☐ ポート 80 での接続を許可します

サービス アカウント

☒ ローカル システム アカウント

設定ログ

自己署名証明書を作成しています  
 ゲートウェイ サーバー の設定値が正常にロードされました  
 Access サーバー の設定をロードしています  
 Access サーバー の設定値が正常にロードされました  
 ファイルリポジトリ の設定をロードしています  
 ファイルリポジトリ の設定値が正常にロードされました

ヘルプ OK キャンセル 適用

4. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。

**Acronis Access 設定ユーティリティ**

ゲートウェイ サーバー | **Access サーバー** | ファイルリポジトリ

サーバー エンドポイント

アドレス: The Client Access IP address

ポート: 443

証明書: Acronis Access

☐ ポート 80 での接続を許可します

サービス アカウント

☒ ローカル システム アカウント

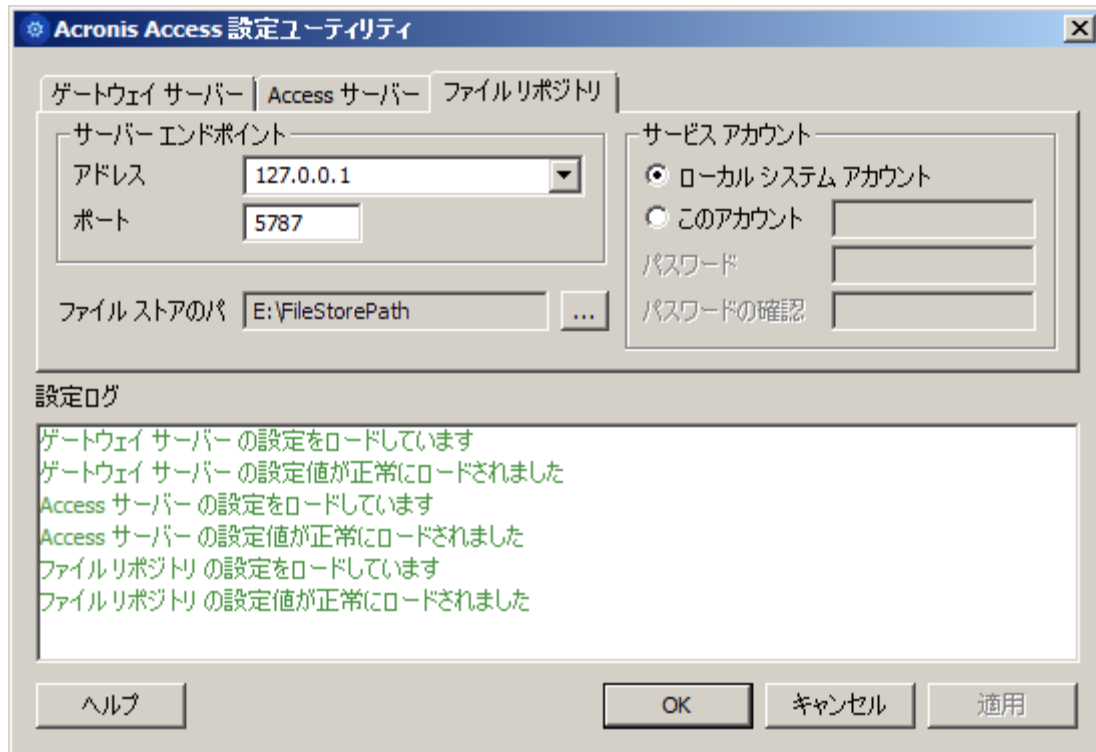
設定ログ

ゲートウェイ サーバー の設定をロードしています  
 ゲートウェイ サーバー の設定値が正常にロードされました  
 Access サーバー の設定をロードしています  
 Access サーバー の設定値が正常にロードされました  
 ファイルリポジトリ の設定をロードしています  
 ファイルリポジトリ の設定値が正常にロードされました

ヘルプ OK キャンセル 適用



5. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



6. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Acronis Access をインストールします。ただし、今回は、デフォルトの **Postgres データ** ロケーション、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。
4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\Acronis\Access\Gateway Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます (例: **database\_path: 'S:/access\_cluster/database/')**。

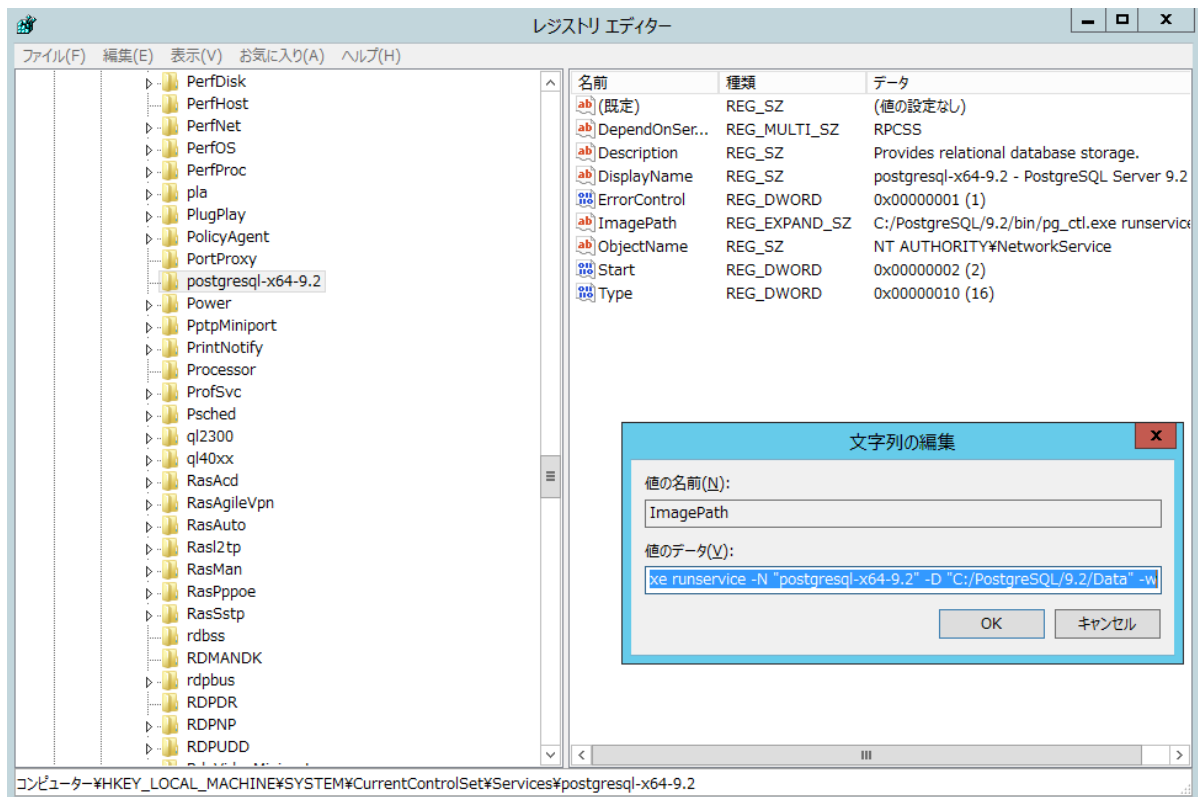
**注意:** パスの区切りにはスラッシュ (/) を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

**注意:** このパスは第 1 ノードで設定されているパスと同じでなければなりません。

PostgreSQL の場合、レジストリを手動で複製する必要があります。

1. **Regedit** を開きます。
2. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\** に移動します。
3. キー「**ImagePath**」を開き、キーの値の一部を次のように変更します: **-D "The path you selected for the PostgreSQL data location"** (例: **-D "E:/PostgreSQL/data"**)。
4. キー「**DataDirectory**」を開き、値を PostgreSQL のデータ フォルダに選択したパスに変更します(例: **E:/PostgreSQL/data**)。

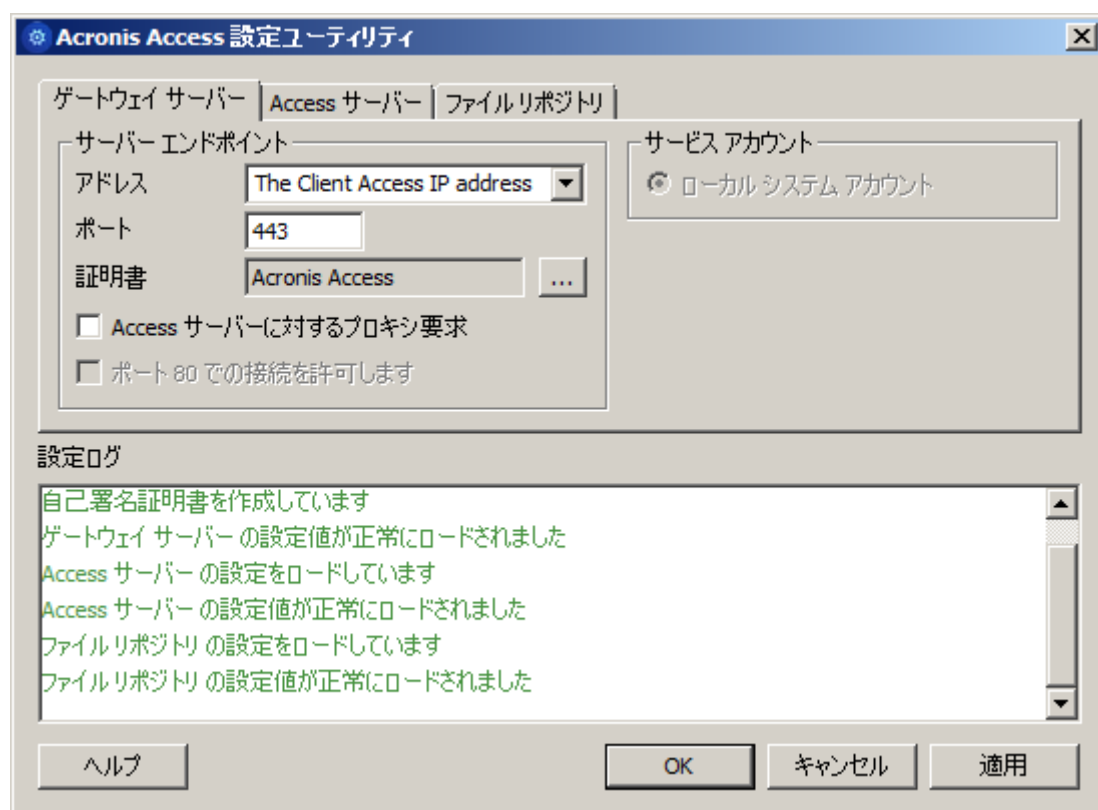


5. **Regedit** を閉じ、続けて以下のステップを実行します。
6. Acronis Access 役割を第 2 ノードに移動します。

## 第 2 ノードの設定ユーティリティの使用

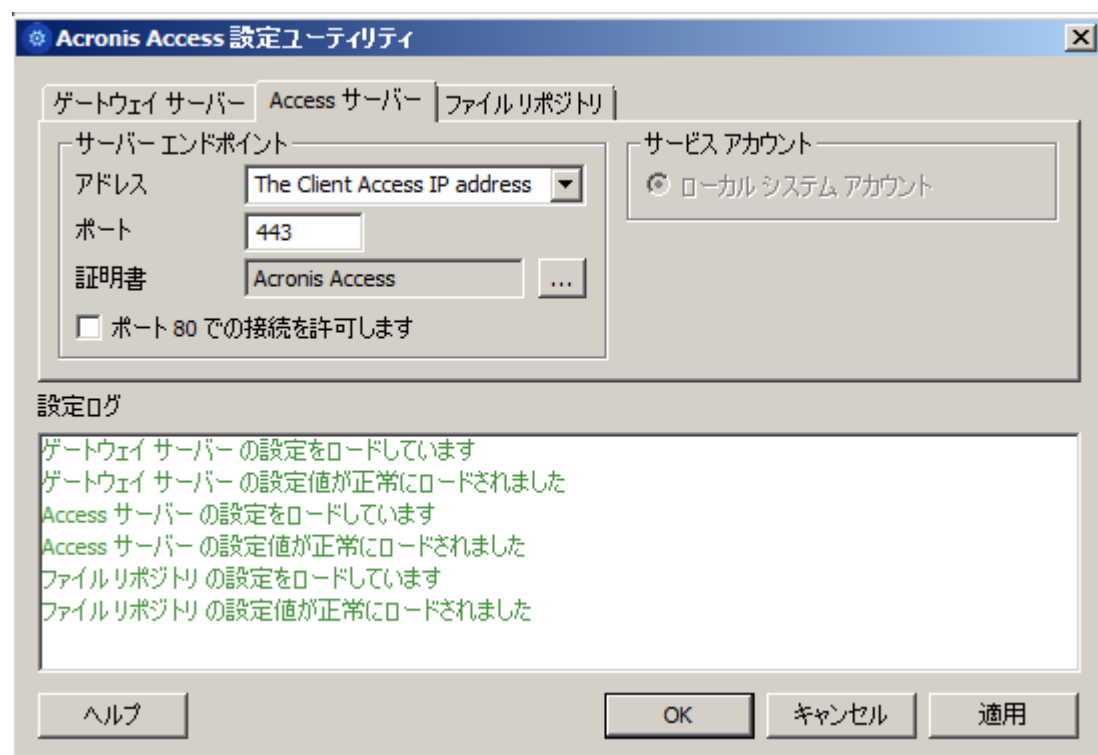
1. 設定ユーティリティを起動します。クリーン インストールの場合、通常このユーティリティは **C:\Program Files (x86)\Acronis\Access\Configuration Utility** にあります。

2. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

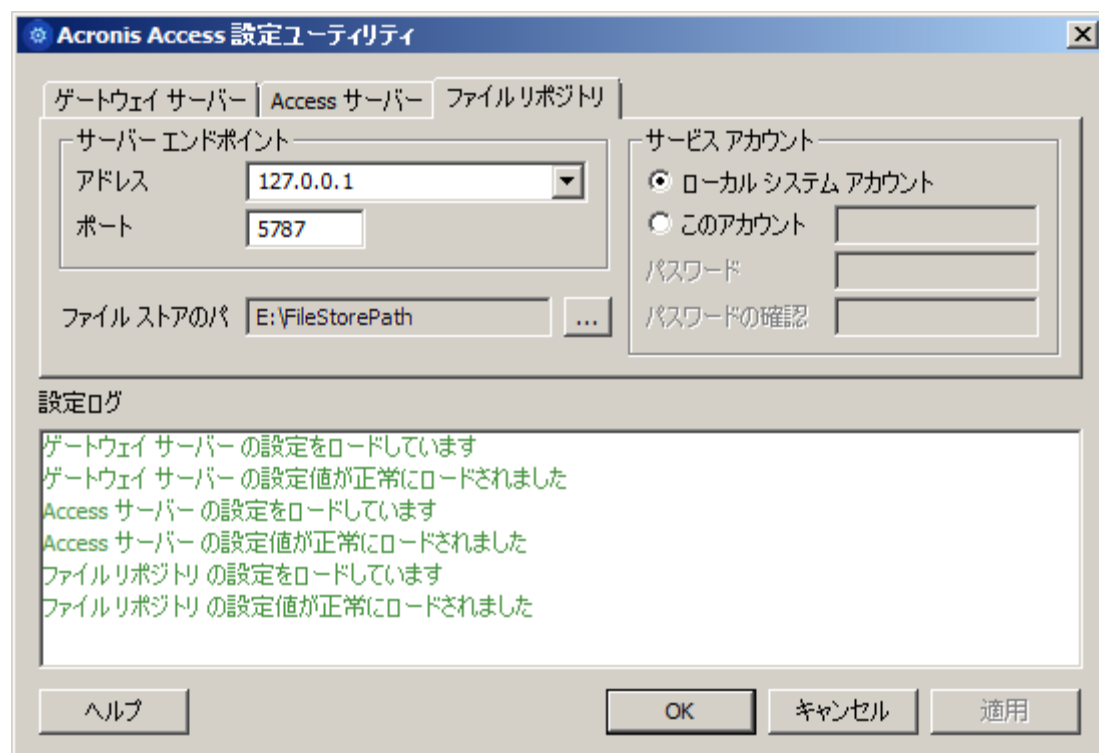


3. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



4. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



5. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 3 アップグレード

### セクションの内容

|   |     |
|---|-----|
| Acronis Access の新しいバージョンへのアップグレード ..... | 65  |
| Acronis Access Advanced へのアップグレード.....  | 66  |
| mobilEcho バージョン 4.5 以前からのアップグレード.....   | 66  |
| activEcho バージョン 2.7 以前からのアップグレード.....   | 111 |
| クラスタ構成のアップグレード .....                    | 133 |

### 3.1 Acronis Access の新しいバージョンへのアップグレード

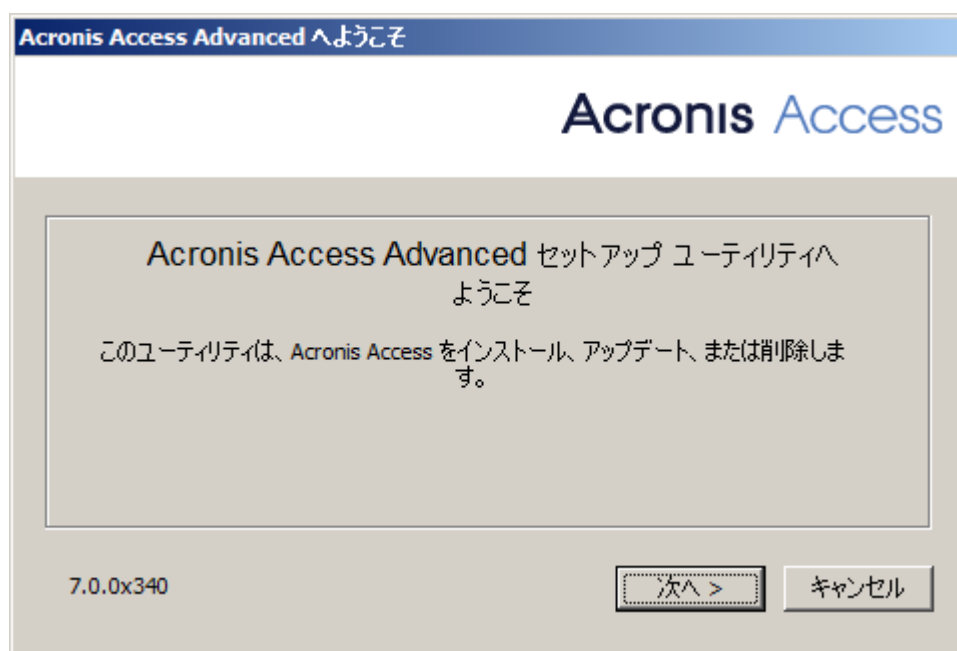
Acronis Access を以前のバージョンからアップグレードする手順は、簡単で、設定の必要もほとんどありません。

#### Apache Tomcat フォルダのバックアップ

アップグレード時に Apache Tomcat がアップグレードされ、現在の Tomcat のすべての設定ファイル およびログ ファイルが削除されます。Apache Tomcat フォルダのコピーを作成することをお勧めします。デフォルトでは、このフォルダは次の場所にあります: **C:\Program Files (x86)\Acronis\Access\Common\**。

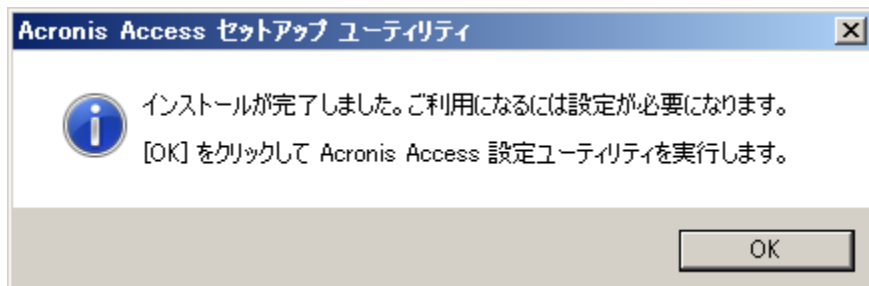
#### アップグレード

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 実行可能なインストーラをダブルクリックします。



3. [次へ] を押して開始します。
4. 使用許諾契約を読み、承諾します。

5. **[アップグレード]** を押します。
6. インストールするコンポーネントを確認して、**[インストール]** をクリックします。
7. インストールされたコンポーネントを確認して、インストーラを閉じます。
8. 設定ユーティリティを開くように求められたら、**[OK]** を押します。



9. 設定ユーティリティの設定が変更されていないことを確認します。すべての設定が希望の設定と同じであることを確認したら、**[OK]** を押して設定ユーティリティを閉じ、Acronis Access サービスを開始します。

## 3.2 Acronis Access Advanced へのアップグレード

Acronis Access サーバーを Advanced バージョンにアップグレードするために必要な操作は、Acronis Access Advanced ライセンス キーの追加だけです。

### キーを追加するには:

1. 管理者として Acronis Access ウェブ インターフェイスを開きます。
2. **[全般設定]** タブを開き、**[ライセンス]** をクリックします。
3. ライセンスを追加します。

### 新しいライセンスの追加

1. プロダクト キーをコピーします。
2. **[プロダクト キーの追加]** フィールドに貼り付けます。
3. ライセンス契約を読み、チェックボックスをオンにして同意します。
4. **[ライセンスの追加]** を押します。

## 3.3 mobilEcho バージョン 4.5 以前からのアップグレード

### セクションの内容

|                              |     |
|------------------------------|-----|
| 開始する前に.....                  | 67  |
| アップグレード プロセス .....           | 75  |
| mobilEcho 4.5 へのダウングレード..... | 110 |

### 3.3.1 開始する前に

#### アップグレード前の mobilEcho のバックアップ

既存の mobilEcho サーバーで使用されているデータ ファイルをバックアップしてください。Acronis Access インストーラによってデータ ファイルはバックアップされますが、安全のため、アップグレードを開始する前に独自のバックアップ コピーを作成することをお勧めします。

mobilEcho 4.5 以前のサーバーのバックアップと復元のプロセスについては、  
<http://docs.grouplogic.com/display/MobilEcho/mobilEcho+Server+Backup+and+Restoration>  
を参照してください。

**Acronis Access へのアップグレードに進むには、事前にご使用の mobilEcho のバージョンをバージョン 4.5 にアップグレードしてください。**

#### 設定の確認

アップグレードを続行する前に、次のことを確認してください。

- mobilEcho と activEcho の両方がインストールされていることを確認します。
- mobilEcho と activEcho が同一のコンピュータにインストールされているか、別々のコンピュータにインストールされているかを確認します。
- mobilEcho で使用されているポートを確認します。また、ファイル サーバーおよび管理サーバーのポートも確認します。
- activEcho で使用されているポートを確認します。ファイル レポジトリが同じコンピュータにあることを確認します。

#### 機能強化

Acronis Access には多数の機能強化が組み込まれており、mobilEcho サーバーの設定と管理が改善されるとともに、mobilEcho と activEcho の両製品の管理が単一のコンソールに統合されました。このガイドでは、Acronis Access へのアップグレード時に考慮する必要がある、アーキテクチャと機能の変更点を説明します。

Acronis Access では Network Reshare Path Mapping のセットアップが自動で行われるため、これをユーザー自身で行う必要はありません。しかし、ホーム ディレクトリをホストするサーバーを指す「フォルダ」データ ソースを、サーバーにつき 1 つずつ作成しなければなりません。

## アップグレードには慎重な計画が必要

Acronis Access では、mobilEcho のソフトウェア サービス、データベース/設定の場所、および管理の面で、アーキテクチャと機能が大幅に変更されています。これらの変更により、強力な新機能と統合が導入されていますが、Acronis Access へのアップグレードにあたっては注意深く検討すべき事項がいくつかあります。

mobilEcho の単一サーバーを配置する場合であれば、プロセスはきわめて簡単ですが、リバースプロキシ サーバーと負荷分散装置を使用する場合や、複数の mobilEcho サーバーがある場合、または Microsoft フェールオーバー クラスタリングを使用する場合は、このドキュメントで説明される、特定のシナリオに該当する場合のアップグレード考慮事項を理解してから実行してください。

このドキュメントでは、Acronis Access へのアップグレードを計画して安全に実行するために必要な詳細事項を説明します。固有の mobilEcho の配置をシミュレートしたテスト環境でこのアップグレードを実行してから、本番 mobilEcho サーバーをアップグレードすることを強くお勧めします。

## 負荷分散された mobilEcho サーバーと Microsoft フェールオーバー クラスタ

負荷分散装置をフロントエンドとして使用する複数の mobilEcho サーバーを配置している場合、または Microsoft フェールオーバー クラスタ上で mobilEcho を実行している場合は、Acronis Access 5.1 以降にアップグレードする必要があります。5.1 では新機能が導入され、負荷分散された一群のゲートウェイ サーバーを Acronis Access Server コンソールから自動的に管理できるようになりました。この機能を使用すれば、レジストリ設定を複製したりサーバーの更新をスクリプトで実行したりする必要がなくなります。新しいデータ ソース(ボリューム)をサーバーに追加する操作をワン ステップのプロセスとして管理コンソールから自動的に処理できます。詳しくは、「クラスタグループ」の記事を参照してください。

---

Windows フェールオーバー クラスタで mobilEcho をインストールしたりアップグレードしたりする作業は、かなり複雑なプロセスになります。mobilEcho 5.0 でアーキテクチャが変更された結果、Windows フェールオーバー クラスタで mobilEcho を実行する方法にも変更が必要になります。

クラスタでの Acronis Access のインストールについては、「クラスタ上での Acronis Access のインストール『20ページ』」の記事を参照してください。

mobilEcho クラスタを Acronis Access クラスタにアップグレードする手順については、「クラスタでの Acronis Access のアップグレード『138ページ』」の記事を参照してください。

---

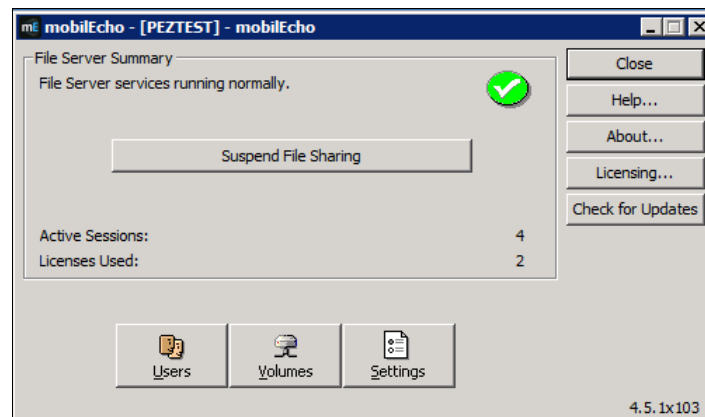
## アーキテクチャと用語の変更

mobilEcho と activEcho の両製品が統合されて、1 つの共通ソフトウェア プラットフォームになりました。両製品は引き続き別個にライセンス供与され、別個に使用することも一緒に使用することも可能ですが、インストーラと管理コンソールが共通になりました。ウェブ ベースのこの共通コンソールを Acronis Access サーバーといいます。




**mobileEcho 4.5 以前のバージョンには 2 つの管理コンソールがありました**

**mobileEcho Administrator:** この Windows プログラムは、mobileEcho クライアントで利用可能なファイル共有「ボリューム」の定義、アクティブなユーザーの監視、mobileEcho File Access Server の全般設定の構成に使用されていました。



**mobileEcho Client Management Administrator:** この Web ベースのコンソールは、mobileEcho クライアント ユーザーのオンボード、監視、リモート ワイプ、およびクライアントのセキュリティと設定ポリシーの定義に使用されていました。さらに、mobileEcho アプリに自動的に表示される mobileEcho サーバー、ネットワーク フォルダ ショートカット、および同期フォルダの割り当てにも使用されていました。

[Devices](#) | [Invitations](#) | [Groups](#) | [Users](#) | [Servers & Folders](#) | [Allowed Apps](#) | [Settings](#) | [Log out](#)



## Client Management Administrator

### Manage Group Profiles

Group profiles configure the mobileEcho client's application settings, capabilities, and the list of available servers shown to the group members. The group profile list is shown in the order of precedence. The first group in the list that a user belongs to will determine their profile.

[Add new group](#)

Filter by Name  [Filter](#)

| Common Name / Display Name | Distinguished Name                         |     | Enabled                             |                        |
|----------------------------|--|-----|-------------------------------------|------------------------|
| TestSecGroup               | CN=TestSecGroup,OU=Groups,DC=gllabs,DC=com | ↑ ↓ | <input type="checkbox"/>            | <a href="#">delete</a> |
| Marketing                  | CN=Marketing,OU=Groups,DC=gllabs,DC=com    | ↑ ↓ | <input checked="" type="checkbox"/> | <a href="#">delete</a> |
| Group1                     | CN=Group1,CN=Users,DC=gllabs,DC=com        | ↑ ↓ | <input checked="" type="checkbox"/> | <a href="#">delete</a> |
| Group2                     | CN=Group2,CN=Users,DC=gllabs,DC=com        | ↑ ↓ | <input checked="" type="checkbox"/> | <a href="#">delete</a> |
| Domain Users               | CN=Domain Users,CN=Users,DC=gllabs,DC=com  | ↑ ↓ | <input checked="" type="checkbox"/> | <a href="#">delete</a> |

Per page: [10](#) [20](#) [30](#) [50](#) [100](#)

© 2002-2013 Acronis International GmbH. All rights reserved. | [Help](#)

Acronis Access のリリースをもって、上記の 2 つの管理コンソールは Acronis Access サーバーというウェブ ベースの単一のコンソールにまとめられました。



Acronis Access サーバーは以下の役目を果たすウェブ アプリケーションです。

- mobilEcho の管理コンソール
- activEcho の管理コンソール
- activEcho のクライアント ウェブ インターフェイス

mobilEcho 製品のみを使用している場合は、Acronis Access にアップグレードすると、既存の mobilEcho Client Management Administrator ウェブ コンソール(通常は mobilEcho サーバーのポート 3000 で実行)が Acronis Access サーバー ウェブ コンソールにアップグレードされます。

mobilEcho Administrator Windows プログラムの機能は、Acronis Access サーバー ウェブ コンソールで処理されることになりました。Acronis Access にアップグレードすると、mobilEcho Administrator を使用して mobilEcho File Access Server サービスを設定することがなくなるため、mobilEcho Administrator は mobilEcho サーバーから削除されます。

## Windows レジストリに設定が保存されなくなりました

旧バージョンの mobilEcho では、mobilEcho File Access Server の設定と、設定されたボリュームが Windows レジストリに保存されていました。Acronis Access にアップグレードすると、これらの設定が内部の SQL データベースに移されます。mobilEcho ボリュームを直接 Windows レジストリに追加したり、mobilEcho のレジストリ設定をバックアップしたりするための自動プロセスを使用していた場合、代わりに SQL データベースを処理するようにプロセスを変更する必要があります。

デフォルトで、この SQL データベースはアップグレード後のサーバーの以下の場所に置かれます。

C:\Program Files (x86)\Group Logic\mobilEcho Server\database\mobilEcho.sqlite3

負荷分散された一連の mobilEcho サーバーのボリュームを管理するためにレジストリを直接編集している場合、新たに導入されるクラスタ mobilEcho サーバー管理機能のおかげで、レジストリでボリューム変更を加える必要が軽減されます。

## Acronis Access サーバーの管理

### 既存の設定

mobilEcho 4.5 以前の既存のボリューム、登録ユーザー、ポリシー、割り当て済みのサーバーとフォルダ、および許可アプリは、アップグレード処理中にすべて Acronis Access サーバーに移行されます。既存の mobilEcho クライアント ユーザーは、クライアント側の変更を一切必要とせずに引き続きサーバーに接続でき、同一のポリシーとデータ ソースを受け取ることができます。クライアント ユーザーには Acronis Access iOS クライアント アプリまたは Acronis Access Android クライアント アプリにアップグレードすることをお勧めしますが、旧バージョンのクライアント アプリには Acronis Access サーバーとの互換性があります。

### サーバー管理者の設定

Acronis Access へのアップグレード前に mobilEcho 管理者として設定されていた既存のユーザーまたはグループには、引き続き Acronis Access サーバー ウェブ コンソールへの完全な管理者権限が付与されます。Acronis Access では役割ベースの新しい管理者権限が導入され、これによって管理の機能を特定のユーザーまたはグループに制限することができます。管理者を追加または編集するには、[全般設定] メニューの [管理者] ページにアクセスしてください。

**プロビジョニング済み LDAP 管理者グループの追加**

選択済みグループ:

**管理者権限**

- ☒ 完全な管理者権限
- ☒ ユーザーを管理する
- ☒ モバイル データソースを管理する
- ☒ モバイル ポリシーを管理する
- ☒ 監査ログを表示する

LDAP グループを検索して、共通名/表示名をクリックし、[プロビジョニング済み LDAP 管理者グループ]として選択します。

次に該当するグループを検索  先頭の文字

## 電子メール テンプレート

ユーザーに送信する mobilEcho 登録招待メールに使用する電子メール テンプレートをカスタマイズした場合、Acronis Access へのアップグレード時にこの電子メール テンプレートは移行されません。電子メール テンプレート編集用の新しいインターフェイスが用意されています。Acronis Access コンソールの [全般設定] メニューで [電子メール テンプレート] ページを開き、必要に応じて電子メール テンプレートを変更しなければなりません。詳細については、「電子メール テンプレートの設定」の記事を参照してください。

**注意:** 前の mobilEcho テンプレートのコピーは、**Legacy mobilEcho files** フォルダにあります。デフォルトでは、そのロケーションは **C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files** です。ファイルの名前は、**invitation.html.erb** および **invitation.txt.erb** です。新しいテンプレートをカスタマイズする際には、これらのファイルを参考にすることができます。

Acronis Access

管理画面を開く administrator

### 電子メール テンプレート

テンプレートの保存

Acronis Access サーバーによって送信されるすべての電子メールは、カスタマイズできます。各電子メールについて、HTML とテキスト形式の電子メール テンプレートを指定する必要があります。テンプレートの本文は、**ERB, embedded Ruby** 内に記述する必要があります。デフォルトのテンプレートを確認して、テンプレートの最適なカスタマイズ方法を判断してください。

言語の選択: 日本語

電子メール テンプレートの選択: モバイル アクセスのためのユーザー登録

使用可能なパラメータ

- @invitation.email - ユーザーの電子メール アドレス
- @invitation.pin - ユーザーの PIN コード
- @invitation.display\_name - ユーザーの表示名
- @management\_server\_address - Acronis Access サーバー アドレス
- @expiration - PIN コードの有効期限日付
- @url - Acronis Access URL
- @invitation.user - ユーザー名 (ユーザー プリンシパル名)
- @app\_name - アプリ名 ("Acronis Access" または "Acronis Access for Good Dynamics")
- @is\_good - アプリケーションが Good Dynamics 用の場合は True
- @send\_ios\_instructions - 招待メールに iOS の指示が含まれる場合は True
- @send\_android\_instructions - 招待メールに Android の指示が含まれる場合は True
- @locale - このテンプレートのロケール コード

電子メールの件名: Acronis Access へようこそ

件名でパラメータを使用するには、パラメータ名を #{} で囲みます (例: #{parameter\_name})。

HTML 電子メール テンプレート

デフォルトの表示

```
<!DOCTYPE html>
<html>
<head>
<meta content="text/html; charset=UTF-8" http-equiv="Content-Type" />
</head>
<body>
<p>#{@invitation.email}</p>
</body>
```

## データ ソース/ボリューム管理

Acronis Access では、mobilEcho Administrator Windows プログラムと mobilEcho Client Management Administrator ウェブ コンソールのサーバー管理機能が統合されて単一のウェブ インターフェイスになります。その結果、ボリュームという概念が不要になりました。

新しいファイル共有または SharePoint ロケーションへのアクセス権を、1 ステップの処理でユーザーに付与できるようになりました。そのためには、[データ ソース] ページの [フォルダ] タブで [新しいフォルダの追加] をクリックします。この 1 ステップで実行する操作は次のとおりです。

1. フォルダの表示名を指定します (これがユーザーに表示されます)。
2. このデータ ソースにアクセスするために使用するゲートウェイ サーバーを選択します。
3. データ ソースの種類を選択します。ゲートウェイ サーバー上のローカル フォルダ、SMB/CIFS 共有、SharePoint サイトまたはドキュメント ライブラリ、activEcho サーバーのいずれかです。
4. 割り当て先のユーザーにこのフォルダを自動的に同期するかどうかを選択します。
5. このフォルダを mobilEcho サーバーのルートに表示するかどうかを選択します (サーバーのルートを表示することがユーザーに許可される設定の場合)。

6. このフォルダを一連の AD(Active Directory) ユーザーまたはグループに割り当てます。これで、フォルダはユーザーの mobilEcho アプリケーションに自動的に表示されるようになります。

### フォルダの編集

表示名: Demo Share

このデータソースにアクセス権を付与するために使用するゲートウェイ サーバーを選択する:

Local (192.168.1.141:443)

データのロケーション: ゲートウェイ サーバー上

この Acronis Access ゲートウェイ サーバー上で共有するローカル フォルダのパスを入力します (例: "E:\Shares\Documents\"). ワイルドカード文字列 %USERNAME% をパスに含めることができます。この場合、ワイルドカードはユーザーのユーザー名で置き換えられます。

パス: D:\Demo Share

同期: なし

☒ サーバーの参照時に表示する

☐ Salesforce.com アクティビティのログ記録を必須にする

ユーザーまたはグループにこのフォルダを割り当てる

次に該当するユーザーまたはグループを検索

先頭の文字

検索

このフォルダの割り当て先:

| 共通名 | 識別名 |
|-----|-----|
|-----|-----|

保存 キャンセル

ゲートウェイ サーバーが mobilEcho クライアント アプリケーションに自動的に表示されるように設定するには、[クライアントで表示されるゲートウェイ サーバー] タブを使用します。このページで AD ユーザーまたはグループをゲートウェイ サーバーに割り当てることができます。そうすると、それらのユーザーの mobilEcho アプリケーションには指定したサーバーのリストが表示されるようになります。それらのユーザーは、どんなフォルダであれ、[サーバーの参照時に表示する] プロパティが有効で、かつ自分がファイル アクセス許可を持っているものなら、表示して中身を参照することができます。

フォルダ

クライアントで表示されるゲートウェイ サーバー

割り当て済みのソース

クライアントで表示されるゲートウェイ サーバー

Acronis Access モバイル ユーザーが Active Directory のユーザーまたはグループによって割り当てられると、特定のゲートウェイ サーバーが、その Acronis Access モバイル ユーザーの Acronis Access モバイル アプリに表示されます。すると、これらのユーザーが、既存のファイル アクセス許可を持っているこれらのサーバー上の表示可能なデータソースを参照できるようになります。

| 表示名         | サーバー アドレス         | 割り当て先         |  |
|-------------|-------------------|---------------|--|
| Local       | 192.168.1.141:443 | Domain Admins |  |
| Main Server | 192.168.1.140:443 | Demo Users    |  |

## mobilEcho クライアント管理のアドバンス機能の使用を開始する

既存の mobilEcho サーバーで mobilEcho クライアント管理機能を設定していなかった場合は、Acronis Access のインストール プロセスに表示される手順に従って基本設定を行うことにより、そのアドバンス機能を使用し始めることができます。

初めに、Active Directory ユーザーとグループを Acronis Access サーバーで列挙できるように LDAP を設定することと、電子メールによる登録招待をユーザーに送信できるように SMTP を設定することが求められます。

この設定を実行すると、ユーザーとグループのポリシー、デバイスごとの追跡、およびその他の多くの機能を利用できるようになります。

## 新しい監査ログ オプション

Acronis Access には新しい監査ログ機能が含まれています。これにより、Acronis Access ゲートウェイ サーバーはすべてのファイル アクティビティを Acronis Access ウェブ コンソールに報告できるようになります。これらのアクティビティは統合された監査ログに保存されます。これを使用して、ユーザーが実行するすべてのファイル操作を監査できます。

デフォルトで、ゲートウェイ サーバーの監査ログは無効になっています。ゲートウェイ サーバーで監査ログを有効にするには、[ゲートウェイ サーバー] ページにアクセスし、希望のサーバーの [詳細] ボタンをクリックし、[ログ] タブで [監査ログ] オプションを選択します。

Main Server

ステータス

ログ

アクティブ ユーザー

デバッグ ログの設定は、カスタム サポート 担当者の要求があった場合のみ変更することをお勧めします。追加のデバッグ ログはサーバーで発生した問題のトラブルシューティングに役立つことがあります。  
 ログ ファイルがあるロケーションの詳細については、[ドキュメント](#) を参照してください。

☒ 監査ログ  
☐ デバッグ ログ

ログ ファイルのアーカイブ

閉じる

これでイベントが監査ログに記録されるようになります。監査ログには Acronis Access サーバーのメイン メニューからアクセスできます。



## 3.3.2 アップグレード プロセス

### Acronis Access のアップグレード プロセス

まず、アップグレードする mobilEcho 実装環境のタイプを確認します。この後のセクションでは、シナリオごとに実行手順を説明していきます。以下のようなシナリオが一般的です。

1. **単一の mobilEcho サーバー(クライアント管理なし)**
  - 1 つの Windows サーバーで mobilEcho File Access Server サービスだけを実行する環境です。
2. **単一の mobilEcho サーバー(クライアント管理あり)**
  - 1 つの Windows サーバーで mobilEcho File Access Server サービスと mobilEcho Client Management サービスの両方を実行する環境です。
3. **複数の mobilEcho サーバー(クライアント管理あり)**
  - 複数の Windows サーバーで mobilEcho File Access Server サービスを実行し、いずれか 1 つの Windows サーバーで mobilEcho Client Management サービスも実行する環境です。
4. **複数の mobilEcho サーバー(負荷分散装置をフロントエンドで使用)**
  - 1 つのスタンドアロン Windows サーバーで mobilEcho Client Management サービスを実行し、負荷分散装置をフロントエンドで使用する 2 つ以上の Windows サーバーで mobilEcho File Access Server サービスだけを実行する環境です。
5. **Windows フェールオーバー クラスタ**
  - バージョン 5.0.3 以降でサポートされます。
  - マルチノード Windows フェールオーバー クラスタの 1 つ以上のアクティブ/アクティブ仮想サーバーまたはアクティブ/パッシブ仮想サーバーで mobilEcho を実行する環境です。

### シナリオ 4(mobilEcho File Access Server のために負荷分散装置を使用する環境)に関する重要な注記

負荷分散装置をフロントエンドで使用する環境で複数の mobilEcho File Access Server を実行する場合は、ユーザーが自分のファイルにアクセスするためにどのノードにも接続できるようにするために、それぞれの mobilEcho サーバーで常に同じ mobilEcho ボリュームを設定しておく必要があります。負荷分散装置を使用する複数のサーバーで常に同じボリュームを設定しておくには、mobilEcho ボリュームの設定を複製するという方法が最も一般的です。その設定は、mobilEcho 4.5 以前ではレジストリに格納されています。

Acronis Access では、ボリュームの設定が SQL データベースに移されました。Acronis Access にアップグレードすると、新しいボリュームを mobilEcho サーバーに追加するときに使用する既存のレジストリ アップデート スクリプトが機能しなくなります。5.1 では新機能が導入され、負荷分散された一群のゲートウェイサーバーを Acronis Access Server コンソールから自動的に管理できるようになりました。この機能を使用すれば、レジストリ設定を複製したりサーバーの更新をスクリプトで実行したりする必要がなくなります。新しいデータ ソース(ボリューム)をサーバーに追加する操作をワン ステップのプロセスとして管理コンソールから自動的に処理できます。詳しくは、「クラスタ グループ」の記事を参照してください。

### シナリオ 5(Windows フェールオーバー クラスタ)に関する重要な注記

Windows フェールオーバー クラスタで mobilEcho をインストールしたりアップグレードしたりする作業は、かなり複雑なプロセスになります。mobilEcho 5.0 でアーキテクチャが変更された結果、Windows フェールオーバー クラスタで mobilEcho を実行する方法にも変更が必要になります。

クラスタでの Acronis Access のインストールについては、「クラスタ上での Acronis Access のインストール『20ページ』」の記事を参照してください。

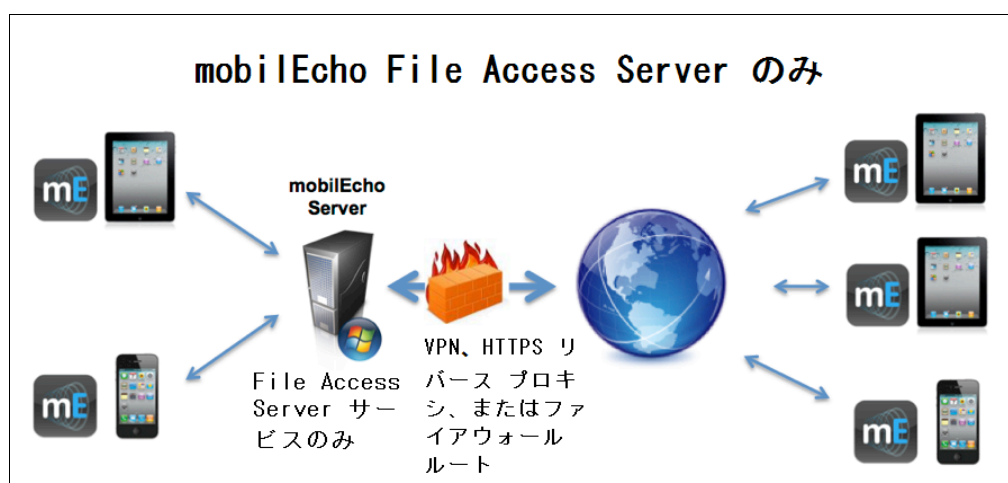
mobilEcho クラスタを Acronis Access クラスタにアップグレードする手順については、「クラスタでの Acronis Access のアップグレード『138ページ』」の記事を参照してください。

## セクションの内容

|  |     |
|--|-----|
| 単一の mobilEcho サーバー(クライアント管理設定なし)のアップグレード.....                      | 76  |
| 単一の mobilEcho サーバー(クライアント管理有効)のアップグレード.....                        | 88  |
| 複数の mobilEcho サーバー(クライアント管理あり)のアップグレード.....                        | 105 |
| クライアント管理を有効に設定した単一の mobilEcho サーバーと activEcho<br>サーバーのアップグレード..... | 110 |

### 3.3.2.1 単一の mobilEcho サーバー(クライアント管理設定なし)のアップグレード

#### シナリオ 1: 単一の mobilEcho サーバー(クライアント管理設定なし)のアップグレード



これは、1 つの Windows サーバーで mobilEcho File Access Server サービスだけを実行する環境です。このアーキテクチャでは、オプションの mobilEcho Client Management Administrator ウェブ コンソールを有効にしません。また、mobilEcho のポリシーやリモート管理機能も使用しません。ユーザーが mobilEcho を設定する場合は、自分のサーバー名、ユーザー名、パスワードを mobilEcho アプリに手動で入力します。

Acronis Access にアップグレードすると、mobilEcho File Access Server が Acronis Access ゲートウェイ サーバーにアップグレードされます。このサービスは、引き続き mobilEcho クライアントからの接続を受け入れ、ユーザーがアクセスするすべてのファイル サーバーや、NAS または SharePoint のデータ ソースへのゲートウェイの役割を果たします。

このアップグレードを実行すると、Acronis Access サーバー ウェブ コンソールもインストールされます。この新しいコンソールは、mobilEcho サーバーを管理するために以前に使用していた Windows プログラム mobilEcho Administrator に代わるものです。Acronis Access サーバー ウェブ コンソールを使用すれば、1 つの統合的なウェブ インターフェイスから mobilEcho サーバーを管理し、必要に応じて追加のクライアント管理機能を利用することも可能になります。

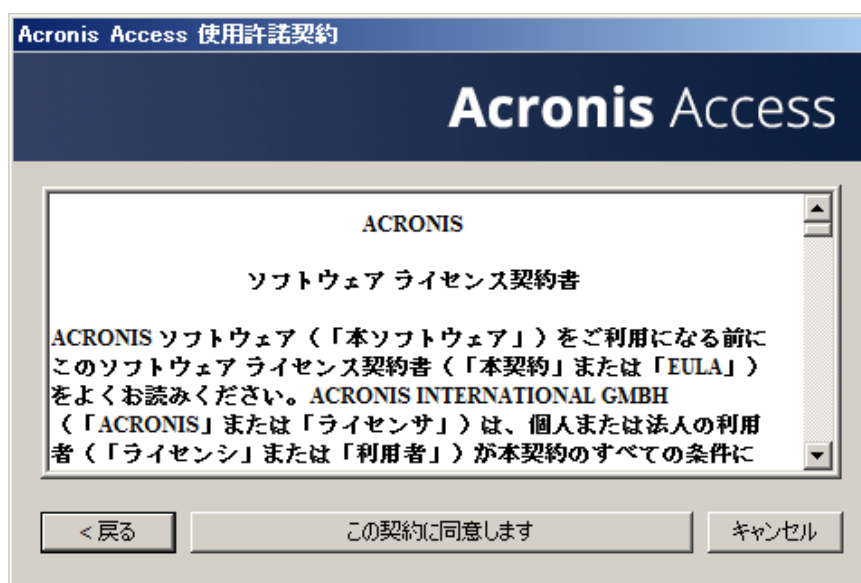


**Acronis Access へのアップグレードは次の手順で実行します。**

1. 必要なファイルすべてをバックアップします。「mobilEcho 4.5 バックアップ」や「activEcho 2.7 バックアップ」のガイドに従ってください。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. Acronis Access Server インストーラを mobilEcho サーバーにダウンロードし、インストーラを実行します。
  - a. 最新版のインストーラを入手するには、[http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598) にアクセスします。
  - b. 確認のため、インストーラをダウンロードする前に製品のプロダクト キーを入力する必要があります。
  - c. インストーラ ファイルの名前は AcronisAccessSetup.exe です。
4. [ようこそ] 画面で **[次へ]** をクリックします。

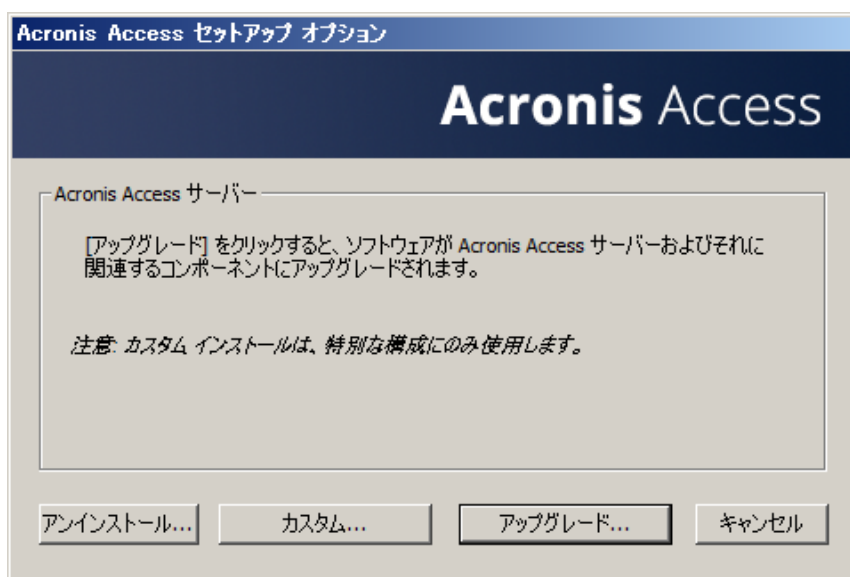


5. 使用許諾契約に同意します。



6. **[アップグレード]** オプションをクリックすると、mobilEcho File Access Server サービスが自動的に Acronis Access ゲートウェイ サーバーにアップグレードされます。アップグレード プロセスでは、Acronis Access サーバーとそれに必要なサービスもインストールされます。

**注意:** [カスタム] を選択して Acronis Access ゲートウェイ サーバーだけをインストールすることはしないでください。Acronis Access サーバーは、mobilEcho Administrator Windows プログラムに取って代わる新しいウェブ コンソールです。mobilEcho サーバーを管理するにはこのコンソールが必要です。これをインストールしないと、mobilEcho の設定を変更したり、新規ファイル共有へのアクセス権を付与したりすることができません。



7. Acronis Access コンポーネントのインストール先となるインストール ロケーションを選択します。既存の mobilEcho サーバーをアップグレードする場合、既存のインストール ロケーションがデフォルトのパスになります。デフォルトのインストール パスを変更しないことをお勧めします。



8. Acronis Access サーバーでは設定を保存するために PostgreSQL データベースが使用されます。このデータベースは必須であり、自動的にインストールされます。

**注意:** 「postgres」管理アカウント用のスーパーユーザー パスワードを入力し、確認のために再度入力します。必ずこのパスワードを安全な場所に記録してください。

**注意:** PostgreSQL のインストール場所もポートも変更しないことをお勧めします。

PostgreSQL の構成

## Acronis Access

PostgreSQL のインストール ロケーション:

ベース パス:  参照...

データ パス:  参照...

PostgreSQL スーパーユーザー資格情報: (必要な場合は作成されます)

PostgreSQL スーパーユーザー パスワード:

パスワードを再入力してください:

PostgreSQL ポート:

< 戻る
次へ >
キャンセル

9. インストールおよびアップグレードするサービスを確認します。それから **【インストール】** をクリックして、アップグレードを開始します。

Acronis Access のインストールに関する警告

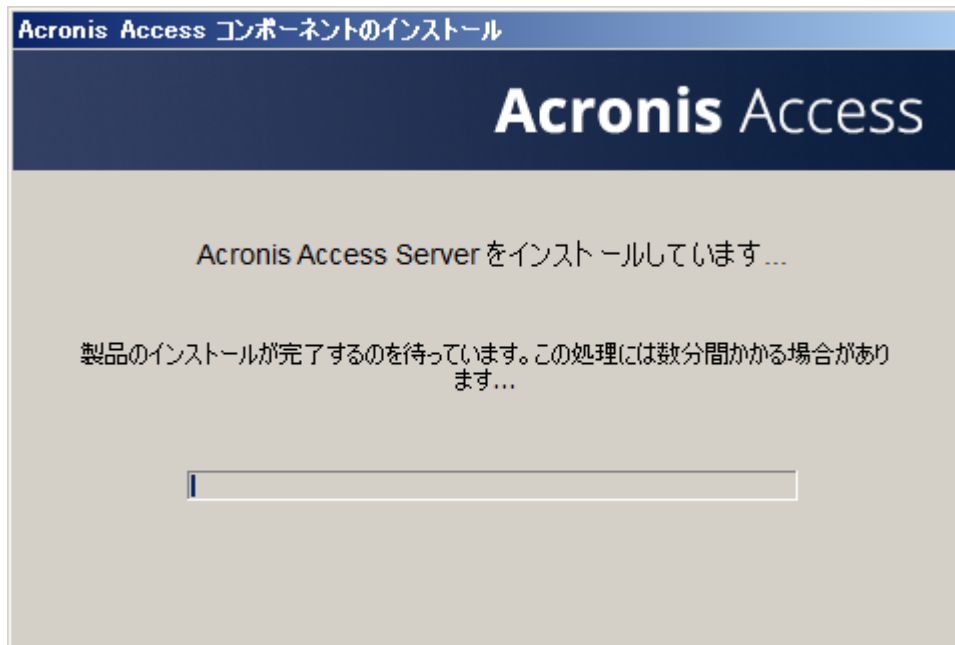
## Acronis Access

セットアップにより、以下の製品がインストールまたはアップグレードされます。この処理により、Acronis Access が起動または停止され、このシステムのユーザーの作業が中断される可能性があります。

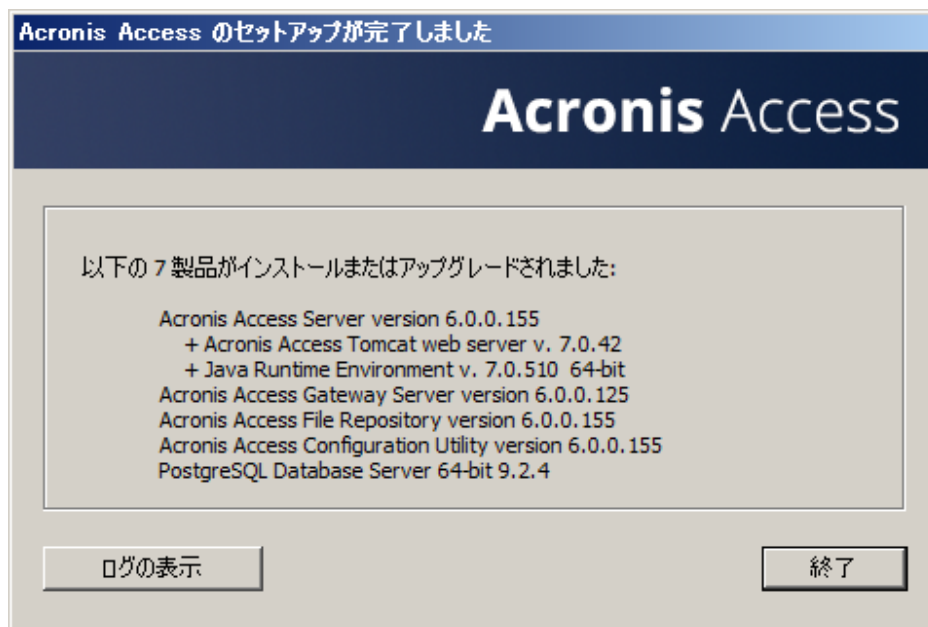
Acronis Access Server v. 6.0.0.155  
 + Acronis Access Tomcat web server v. 7.0.42  
 + Java Runtime Environment v. 7.0.510  
 Acronis Access Gateway Server v. 4.5.2.103 --> v. 6.0.0.125  
 Acronis Access File Repository v. 6.0.0.155  
 Acronis Access Configuration Utility v. 6.0.0.155  
 PostgreSQL Database Server v. 9.2.4

< 戻る
インストール
キャンセル

**注意:** 必要なすべてのコンポーネントが順に自動的にインストールされます。これにはサーバーに応じて 5～15 分かかります。将来のアップグレードのインストールはより高速になります。



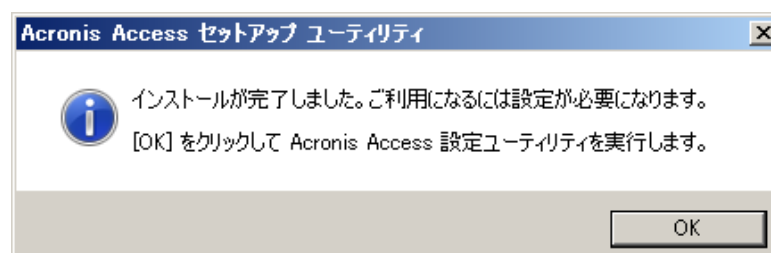
10. インストールが完了すると、インストールされたコンポーネントの要約が表示されます。続行するには、**[終了]** をクリックします。



11. 必要なすべてのソフトウェアはアップグレード処理のこの時点ですべてインストール済みですが、次に、使用するネットワーク インターフェイス、ポート、および証明書を設定する必要があります。

**重要:** この設定ステップに進まないと、mobilEcho サーバーは機能しません。このステップは必須です。

インストーラを終了すると、Acronis Access 設定ユーティリティを実行するよう促すプロンプトが表示されます。続行するには、**[OK]** をクリックしてください。



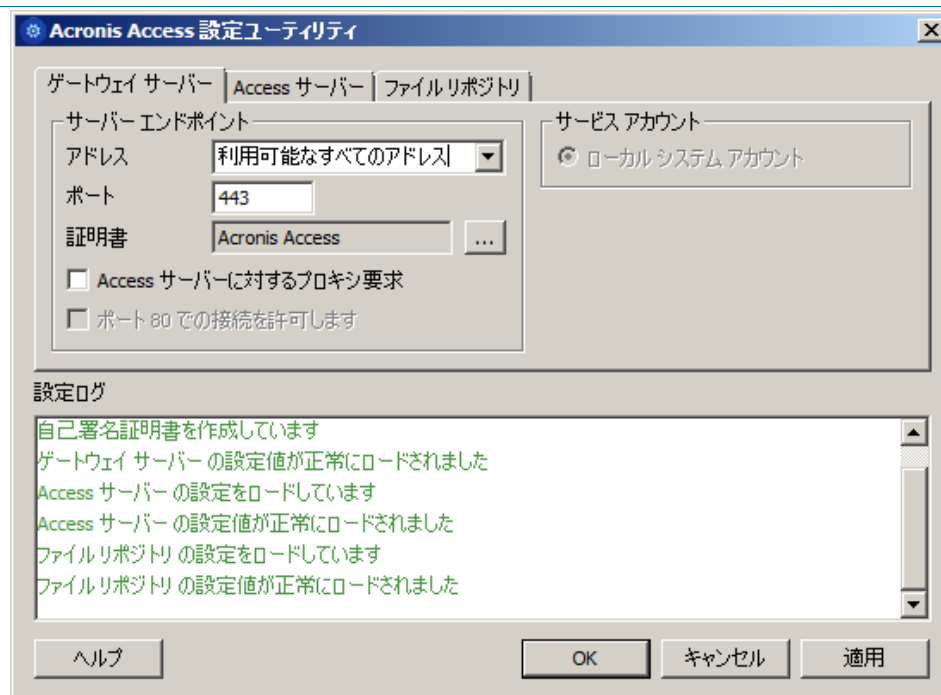
誤ってこのステップを飛ばしてしまった場合、あるいは後でネットワーク インターフェイス、ポート、または証明書を変更しなければならなくなった場合は、設定ユーティリティをいつでも手動で実行できます。

アップグレード済みの mobilEcho サーバーにおいて、ユーティリティのデフォルト位置は以下のとおりです。

**C:\Program Files (x86)\Group Logic\Configuration Utility\AcronisAccessConfiguration.exe**

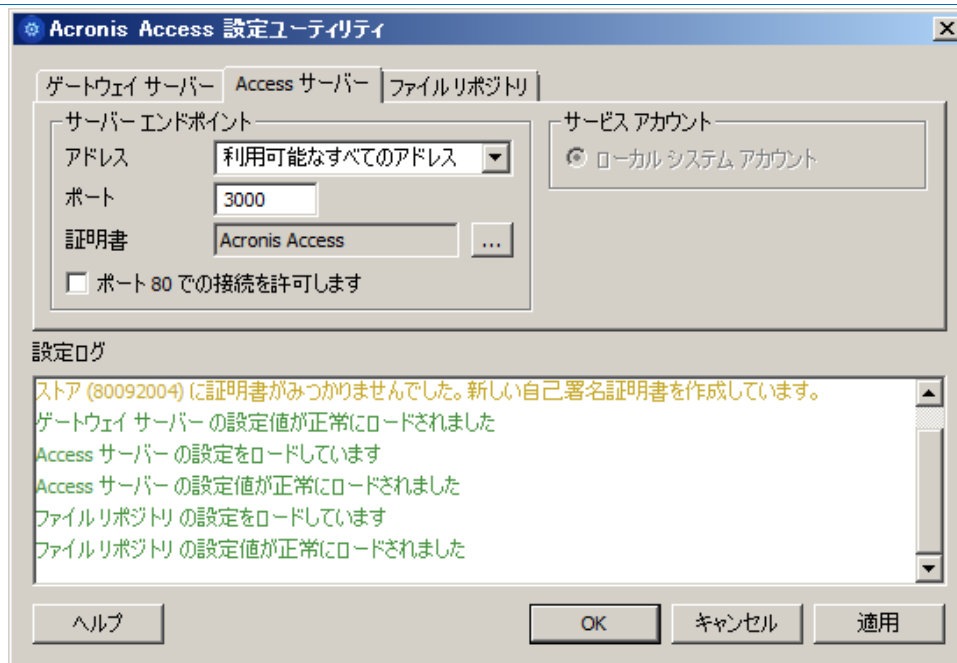
12. Acronis Access ゲートウェイ サーバーのネットワーク アドレス、ポート、および証明書を設定するには、設定ユーティリティ内で [ゲートウェイ サーバー] タブを使用します。Acronis Access ゲートウェイ サーバーは mobilEcho クライアントの接続先となる主要な mobilEcho サービスであり、ファイル サーバー、NAS、および SharePoint サーバーへのアクセス権はここから付与されます。Acronis Access より前、このサービスは mobilEcho File Access Server という名前でした。

**注意:** 既存の設定は保持されます。これらの設定が mobilEcho File Access Server の既存の設定と一致することを確認してください。通常、このサービスはすべての有効なネットワーク アドレスのポート 443 で実行されます。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。



13. [Access サーバー] タブを使用して、Acronis Access サーバーのネットワーク アドレス、ポート、証明書を設定します。Acronis Access サーバーは、サーバー管理とリモート クライアント管理のすべての作業を実行するためのウェブ コンソールです。このコンソールは、Windows プログラム mobilEcho Administrator の代わりに使用する必須コンポーネントです。

**注意:** Access サーバーの設定を確認してください。デフォルトの設定をお勧めします。通常、このウェブ コンソールはすべての有効なネットワーク アドレスのポート 3000 で実行されます。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。



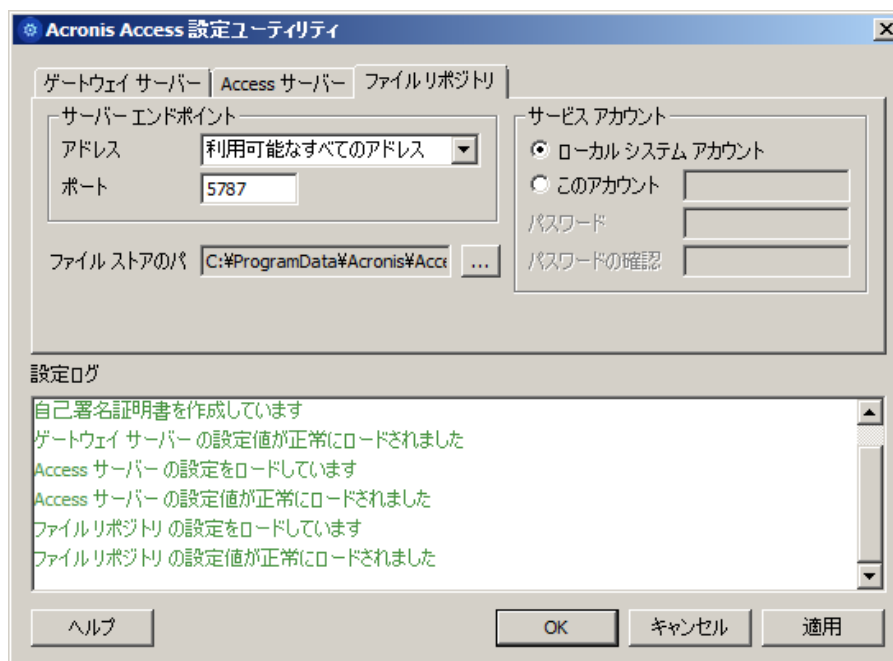
14. Acronis Access Server では、ファイル リポジトリの場所を選択しなければなりません。mobilEcho だけを使用する場合、このファイル リポジトリに何かを格納することはありませんが、それでも場所の設定は必要です。

このリポジトリは、Acronis の activEcho のファイル同期機能とファイル共有機能で使います。これらの機能がまだインストールされていないサーバーをアップグレードした場合、これらの機能は有効になりませんが、必要に応じて後から有効にすることができます。

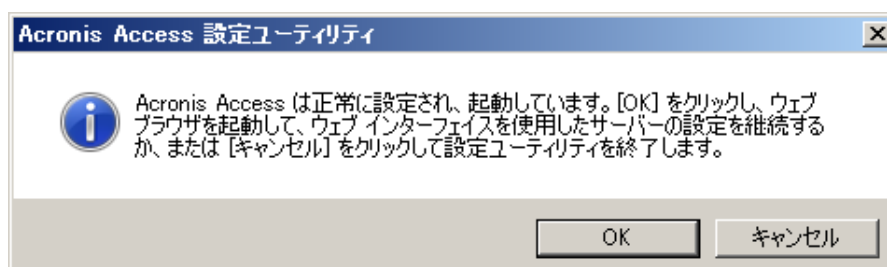
ファイル リポジトリのデフォルトの場所は、以下のとおりです。

**C:\ProgramData\Acronis\Access\FileStore**

後から activEcho を試してみようと思う場合は、C: ドライブではなくデータ ドライブにある場所を選択することもできます。この場所もインストール後に変更できます。



15. **[OK]** をクリックして設定ユーティリティを終了し、設定を適用します。
16. その後、Acronis Access Server ウェブ コンソールに初めてログインすることによって、この設定作業を完了できます。表示される画面で **[OK]** をクリックしてウェブ ブラウザを起動すると、設定が完了します。



### Acronis Access で必要な初期設定:

1. 上記の手順を実行すると、Acronis Access Server のウェブ コンソールが自動的に表示されます。各種サービスが起動してウェブ ページの初回のロードが完了するまでに、30 秒程度の時間がかかることがあります。
2. ウェブ ページが自動的にロードされない場合は、ウェブ ブラウザを開いて、設定ユーティリティで選択した Access Server の HTTPS アドレスとポートを指定してください。
  - a. たとえば、https://mobilecho.mycompany.com:3000 または https://localhost:3000 のように指定します。

**注意:** SMTP、全般設定、LDAP の各ページにある設定のほとんどは、常に mobilEcho のシステムから提示されます。

3. Acronis Access Server では、ローカル管理者アカウントを作成する必要があります。このローカル管理者アカウントのパスワードを入力して、確認のために再度入力してください。





- a. このローカル管理者アカウントのユーザー名は administrator です。
  - b. このローカル管理者のパスワードを安全な場所に保管しておいてください。他の管理ユーザーを設定するまでは、管理者としてログインするためにそのパスワードが必要になります。
  - c. サーバーを設定したら、サーバーの管理者としての役割を果たす追加の Active Directory ユーザー/グループを設定できるようになります。
4. この時点で、残りの設定プロセスを進めていくための設定ウィザードが表示されます。
  5. ライセンス
    - a) 新しいタイプのライセンスの入力を求めるメッセージが表示されるか、古い mobilEcho ライセンスの使用を続けることになります。
  6. SMTP の設定

**Acronis Access** administrator

### SMTP

Acronis Access サーバーは、構成された SMTP サーバーを使用して電子メールを送信し、ファイルの共有やデバイスの登録のためにユーザーを招待したり、ユーザーや管理者にサーバー アクティビティを通知したりします。

SMTP サーバー アドレス

SMTP サーバー ポート

セキュリティで保護された接続を使用しますか? ☒

差出人名

差出人電子メール アドレス

SMTP 認証を使用しますか? ☐

- a. Access Server でアラートやクライアント登録招待の電子メールを送信するために使用する SMTP の設定を定義するための画面が表示されます。
  - b. テスト用の電子メールを送信して設定内容を確認するためのオプションもあります。
7. LDAP の設定



- a. Acronis Access Server では、ポリシーやデータ ソースの割り当て先にするユーザーやグループを Active Directory で検索するときに、LDAP 接続が必要になります。
  - b. ネットワーク上にある Active Directory サーバーの LDAP 情報を入力してください。マルチドメイン ネットワークがある場合は、ポート 3268 または 3269 (SSL 接続の場合) のグローバル カタログ サーバーを指定する必要があります。各フィールドの詳細を説明したツールチップが表示されます。
  - c. サーバーから LDAP への要求を実行するときに使用する LDAP のユーザー名とパスワードを設定しなければなりません。
  - d. 入力した LDAP の設定値を保存するときに、その設定値がテストされます。
8. ローカル ゲートウェイ サーバー: クライアント接続アドレス

- a. mobilEcho ゲートウェイ サーバーは、管理作業のために Acronis Access サーバー ウェブ コンソールに自動的に関連付けられます。デフォルトでは、IP アドレスに基づいてこの接続が行われますが、後から変更することも可能です。

- b. この手順では、mobilEcho クライアントからこの mobilEcho サーバーに接続するためのネットワーク アドレスを入力する必要があります。通常は DNS アドレスであり、このサーバーの DNS アドレスを指定できますが、このサーバーにアクセスするためのプロキシ サーバーのアドレスも使用できます。
9. 初期設定はこれで完了です。
  - a. **[設定の完了]** をクリックして次に進みます。

## mobilEcho ゲートウェイ サーバーの操作

ゲートウェイ サーバーは、この設定プロセスで自動的に登録され、[ゲートウェイ サーバー] リストに表示されます。そのリストで、設定を変更したり、詳細情報や状況を表示したりすることができます。

フォルダ

クライアントで表示されるゲートウェイ サーバー

割り当て済みのソース

### クライアントで表示されるゲートウェイ サーバー

Acronis Access モバイル ユーザーが Active Directory のユーザーまたはグループによって割り当てられると、特定のゲートウェイ サーバーが、その Acronis Access モバイル ユーザーの Acronis Access モバイル アプリに表示されます。すると、これらのユーザーが、既存のファイル アクセス許可を持っているこれらのサーバー上の表示可能なデータソースを参照できるようになります。

| 表示名         | サーバー アドレス       | 割り当て先          |  |
|-------------|-----------------|----------------|--|
| Local       | 192.168.1.141   | TG, Demo Users |  |
| Main Server | rrt.gillabs.com | Domain Admins  |  |

登録が済んだ時点で、Acronis Access へのアップグレード前に mobilEcho ゲートウェイ サーバーに存在していたボリュームが [データ ソース] ページのフォルダ リストにインポートされています。

フォルダ

クライアントで表示されるゲートウェイ サーバー

レガシー データソース

割り当て済みのソース

新しいフォルダを追加

### フォルダ

フォルダは、Acronis Access がアクセス権を付与するファイル コンテンツの場所を定義します。フォルダはユーザーおよびグループに割り当てることができるので、モバイル クライアント アプリに自動的に表示されます。各ユーザーは、ユーザー アカウントおよびメンバーであるグループに割り当てられた一連のリソースを受け取ります。また、ユーザーがゲートウェイ サーバーを参照する場合に、これらを表示するようにも設定できます。

ゲートウェイ サーバーで特定のフォルダのロケーションを追加し、これらのフォルダをユーザーまたはグループに割り当てます。

| タイプ | 表示名            | サーバー  | パス                                     | 同期 |  |
|-----|----------------|-------|--|----|--|
|     | test folder    | Local | D:\testfolder                          | なし |  |
|     | Access         | Local | https://192.168.1.141:3000             | なし |  |
|     | Thousand Files | Local | \\vega\test files\10000 files          | なし |  |
|     | SharePoint     | Local | http://sharepoint2010.gillabs.com:2229 | なし |  |

mobilEcho 5.0 には「ボリューム」がなくなりました。ボリュームを使用してデータ ソースを共有する代わりに、フォルダを作成するようになりました。これらのフォルダには [サーバーの参照時に表示する] というオプションのプロパティがあります。このオプションを有効にすると、ユーザーが mobilEcho アプリでゲートウェイ サーバーのルートを参照したときに、mobilEcho 4.5 以前でボリュームが表示されていたのとまったく同様に、フォルダが表示されます。

フォルダの編集

表示名: test folder

このデータソースにアクセス権を付与するために使用するゲートウェイ サーバーを選択する:

Local (192.168.1.141)

データのロケーション: ゲートウェイ サーバー上

この Acronis Access ゲートウェイ サーバー上で共有するローカル フォルダのパスを入力します (例: "E:\Shares\Documents\").  
ワイルドカード文字列 %USERNAME% をパスに含めることができます。この場合、ワイルドカードはユーザーのユーザー名で置き換えられます。

パス: D:\testfolder

同期: なし

☒ サーバーの参照時に表示する  
☐ Salesforce.com アクティビティのログ記録を必須にする

ユーザーまたはグループにこのフォルダを割り当てる

次に該当するユーザーまたはグループを検索

先頭の文字

検索

このフォルダの割り当て先:

| 共通名 | 識別名 |
|-----|-----|
|     |     |

保存

キャンセル

mobilEcho 4.5 以前のサーバーにあったボリュームはすべて、[サーバーの参照時に表示する] プロパティが有効に設定されたフォルダとして Acronis Access コンソールにインポートされます。したがって、ユーザーが mobilEcho ゲートウェイ サーバーのルートを参照するときには、これらのフォルダが引き続き表示されます。後から追加したフォルダについては、この設定を有効にすることにより、ボリュームと類似の方法で動作するように構成できます。先進的なクライアント管理機能を使用し始めることもできます。例えば、割り当て先の Active Directory ユーザーまたはグループのリスト用の mobilEcho クライアント アプリに自動で表示されるフォルダを追加する機能などです。

以下に示すとおり、ゲートウェイ サーバーの登録後、この mobilEcho 4.5 サーバーの 4 つの既存のボリュームが [フォルダ] リストにインポートされ、mobilEcho アプリからサーバーを参照するときに引き続き表示されます。

フォルダ

クライアントで表示されるゲートウェイ サーバー

レガシー データソース

割り当て済みのソース

新しいフォルダを追加

フォルダ

フォルダは、Acronis Access がアクセス権を付与するファイル コンテンツの場所を定義します。フォルダはユーザーおよびグループに割り当てることができるので、モバイル クライアント アプリに自動的に表示されます。各ユーザーは、ユーザー アカウントおよびメンバーであるグループに割り当てられた一連のリソースを受け取ります。また、ユーザーがゲートウェイ サーバーを参照する場合に、これらを表示するようにも設定できます。

ゲートウェイ サーバーで特定のフォルダのロケーションを追加し、これらのフォルダをユーザーまたはグループに割り当てます。

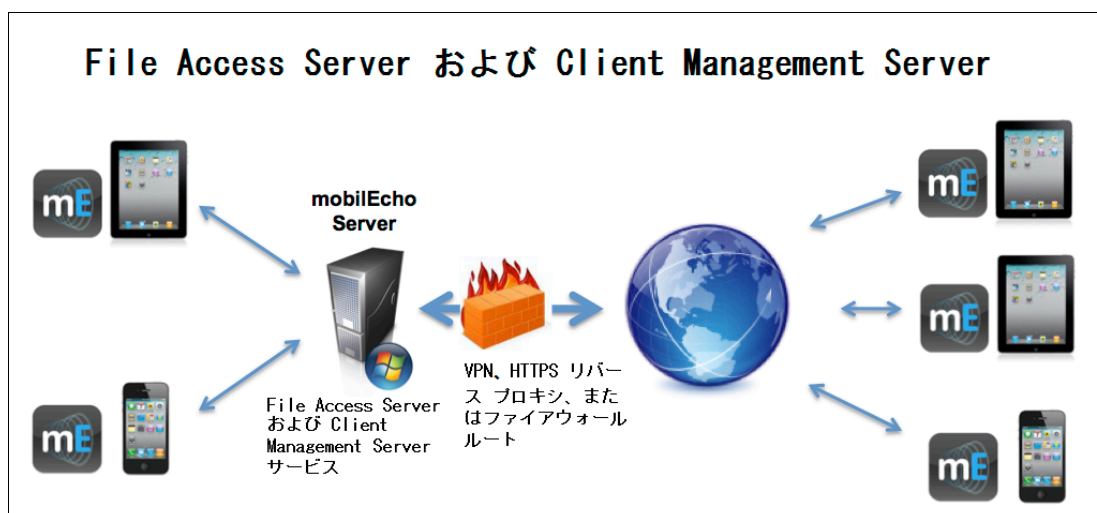
| タイプ   | 表示名            | サーバー  | パス                                       | 同期 |   |
|---|----------------|-------|--|----|---|
|  | test folder    | Local | D:\testfolder                            | なし |   |
|  | Access         | Local | https://192.168.1.141:3000               | なし |   |
|  | Thousand Files | Local | \\vega\test files\10000 files            | なし |   |
|  | SharePoint     | Local | http://sharepoint2010.gillilabs.com:2229 | なし |   |

この時点で、クライアント ポリシーを作成して使用し、そのポリシーによってユーザーを管理するためにユーザーを正式にサーバーに登録する作業を開始できます。すべてのユーザーに適用されるデフォルトのポリシーを有効にして設定することも、Active Directory のユーザーとグループに基づいてカスタム ポリシーを追加することも可能です。

ポリシーの設定が済んだ後に、[ユーザーの登録] ページから登録招待電子メールをユーザーに送信すれば、ユーザーが管理対象ユーザーとして自分を登録できるようになります。

### 3.3.2.2 単一の mobilEcho サーバー(クライアント管理有効)のアップグレード

#### シナリオ 2 - 単一の mobilEcho サーバー(クライアント管理有効)のアップグレード



これは、1 つの Windows サーバーで mobilEcho 4.5 以前を実行する環境です。このサーバーでは、必須の mobilEcho File Access Server サービスが稼働し、オプションの mobilEcho Client Management Server サービスも有効になっています。

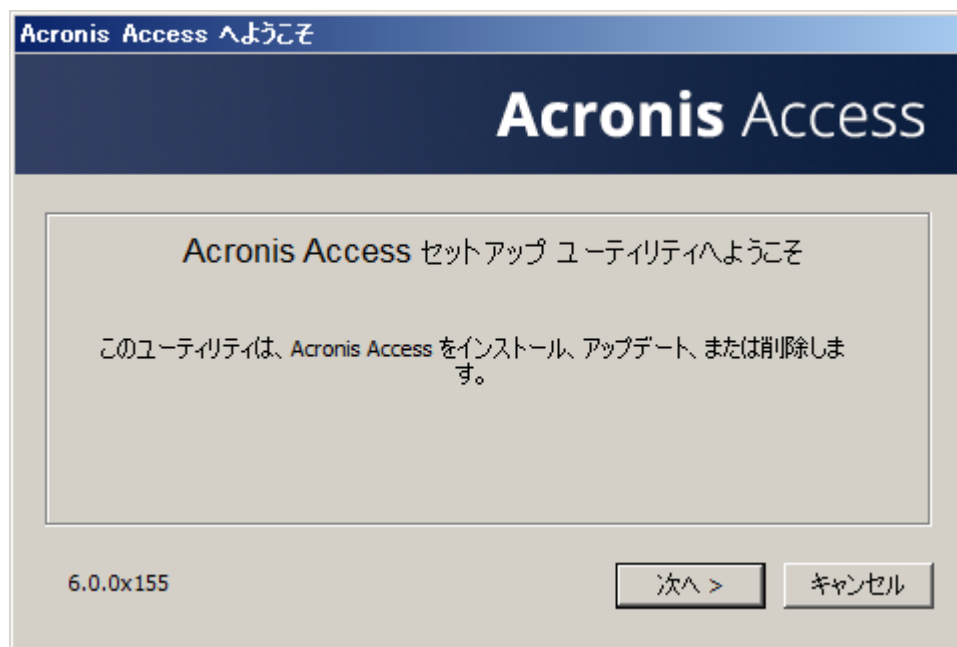
Acronis Access にアップグレードすると、mobilEcho File Access Server が Acronis Access ゲートウェイ サーバーにアップグレードされます。このサービスは、引き続き mobilEcho クライアント

からの接続を受け入れ、ユーザーがアクセスするすべてのファイル サーバーや、NAS または SharePoint のデータ ソースへのゲートウェイの役割を果たします。

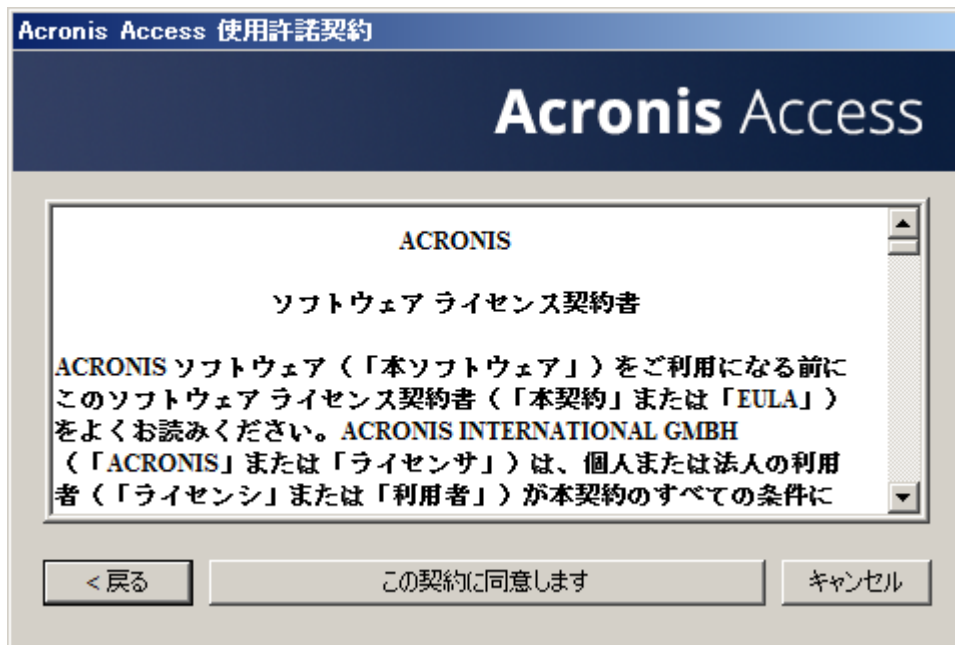
mobilEcho Client Management Administrator ウェブ コンソールは Acronis Access サーバー ウェブ コンソールにアップグレードされます。この新しいウェブ コンソールを使用すれば、1 つの共通のウェブ インターフェイスから mobilEcho のサーバーとクライアントを管理できます。

#### Acronis Access のアップグレードは次の手順で実行します。

1. 必要なファイルすべてをバックアップします。「mobilEcho 4.5 バックアップ」や「activEcho 2.7 バックアップ」のガイドに従ってください。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. Acronis Access Server インストーラを mobilEcho サーバーにダウンロードし、インストーラを実行します。
  - a. 最新版のインストーラを入手するには、[http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598) にアクセスします。
  - b. 確認のため、インストーラをダウンロードする前に製品のプロダクト キーを入力する必要があります。
  - c. インストーラ ファイルの名前は AcronisAccessSetup.exe です。
4. [ようこそ] 画面で **[次へ]** をクリックします。

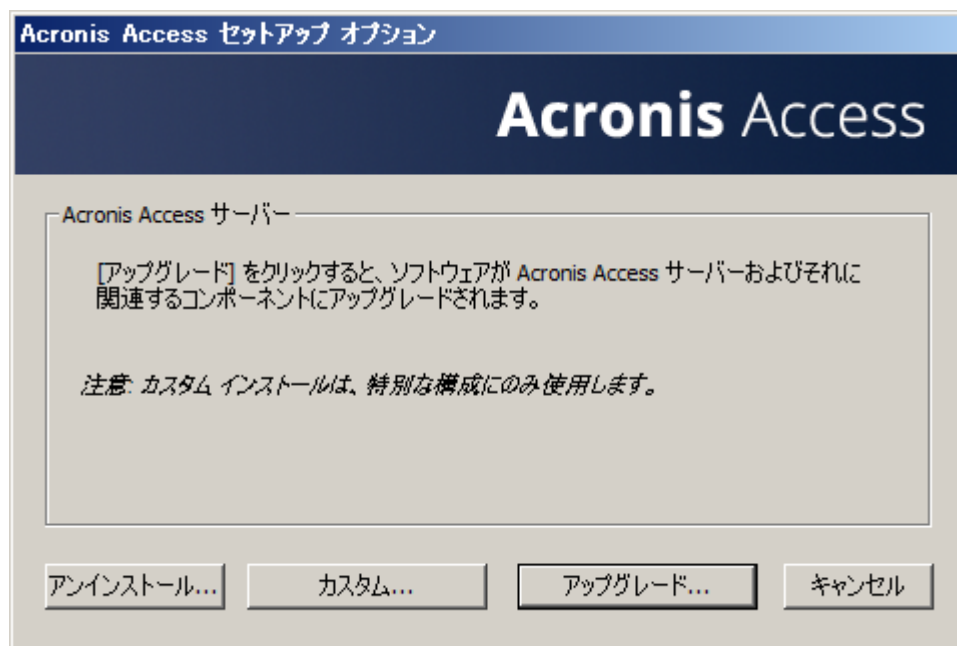


5. 使用許諾契約に同意します。



6. **[アップグレード]** オプションをクリックすると、mobilEcho File Access Server サービスが自動的に Acronis Access ゲートウェイ サーバーにアップグレードされます。アップグレード プロセスでは、Acronis Access サーバーとそれに必要なサービスもインストールされます。

**注意:** **[カスタム]** を選択して Acronis Access ゲートウェイ サーバーだけをインストールすることはいけません。Acronis Access サーバーは、mobilEcho Administrator Windows プログラムに取って代わる新しいウェブ コンソールです。mobilEcho サーバーを管理するにはこのコンソールが必要です。これをインストールしないと、mobilEcho の設定を変更したり、新規ファイル共有へのアクセス権を付与したりすることができません。





7. Acronis Access コンポーネントのインストール先となるインストール ロケーションを選択します。既存の mobilEcho サーバーをアップグレードする場合、既存のインストール ロケーションがデフォルトのパスになります。デフォルトのインストール パスを変更しないことをお勧めします。

ターゲットパスの選択

## Acronis Access

Acronis Access Server  
C:\Program Files (x86)\Group Logic\Access Server\ 参照...

Acronis Access File Repository  
C:\Program Files (x86)\Group Logic\File Repository\ 参照...

Acronis Access Configuration Utility  
C:\Program Files (x86)\Group Logic\Configuration Utility\ 参照...

< 戻る 次へ > キャンセル

8. Acronis Access サーバーでは設定を保存するために PostgreSQL データベースが使用されます。このデータベースは必須であり、自動的にインストールされます。

**注意:** 「postgres」管理アカウント用のスーパーユーザー パスワードを入力し、確認のために再度入力します。必ずこのパスワードを安全な場所に記録してください。

**注意:** PostgreSQL のインストール場所もポートも変更しないことをお勧めします。

PostgreSQL の構成

## Acronis Access

PostgreSQL のインストール ロケーション:

ベースパス: C:\PostgreSQL\9.2\ 参照...

データパス: C:\PostgreSQL\9.2\Data\ 参照...

PostgreSQL スーパーユーザー資格情報: (必要な場合は作成されます)

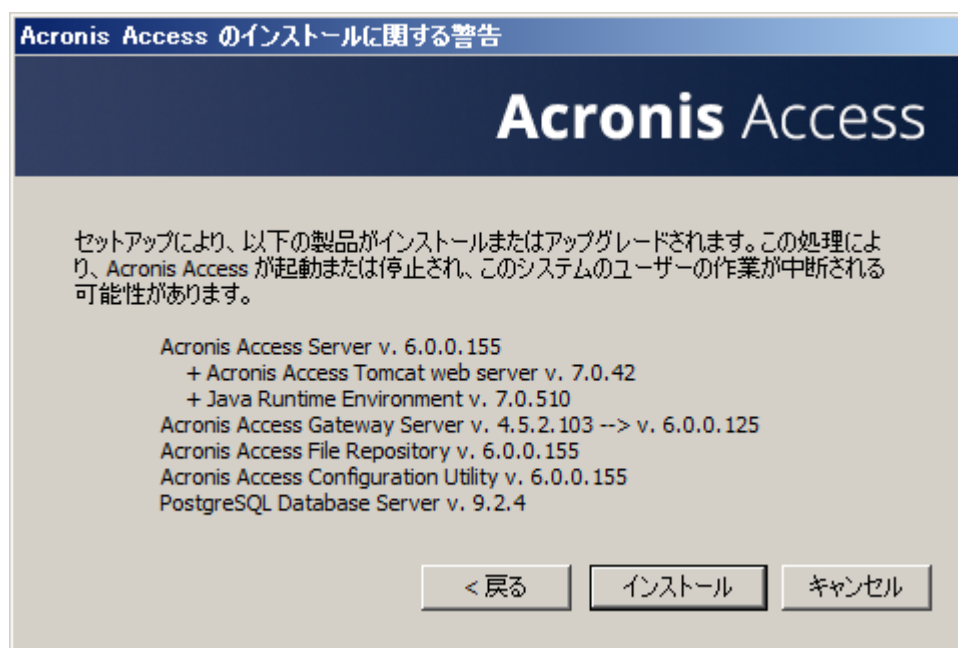
PostgreSQL スーパーユーザー パスワード: \*\*\*\*\*

パスワードを再入力してください: \*\*\*\*\*

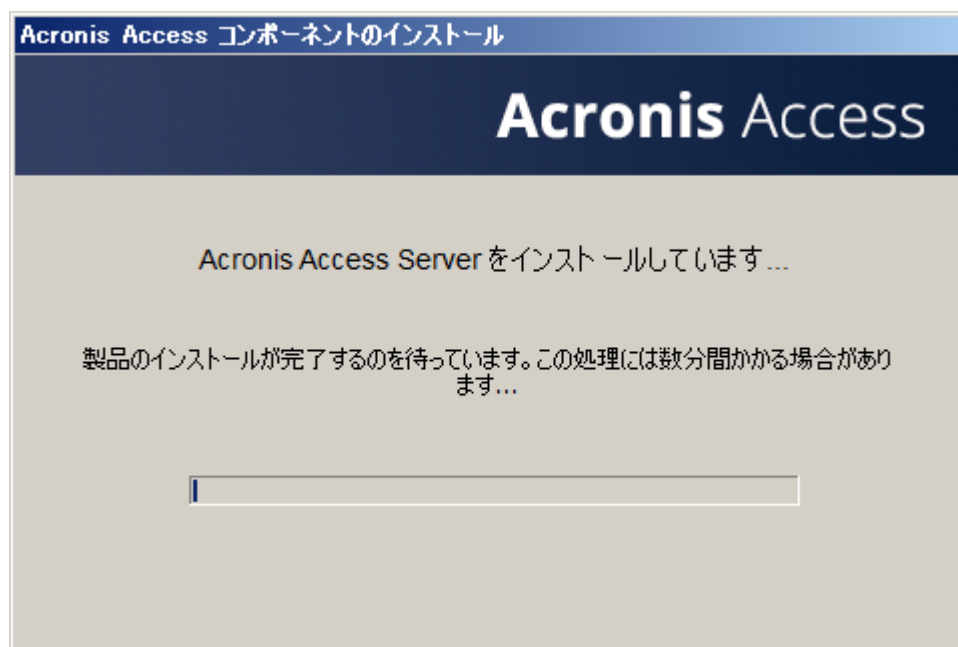
PostgreSQL ポート: 5432

< 戻る 次へ > キャンセル

9. インストールおよびアップグレードするサービスを確認します。それから **【インストール】** をクリックして、アップグレードを開始します。



**注意:** 必要なすべてのコンポーネントが順に自動的にインストールされます。これにはサーバーに応じて 5～15 分かかります。将来のアップグレードのインストールはより高速になります。





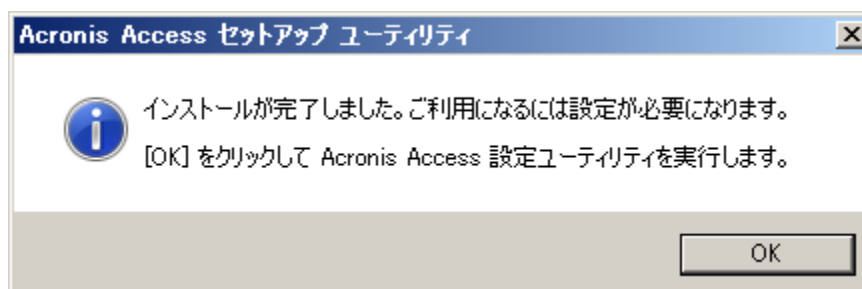
10. インストールが完了すると、インストールされたコンポーネントの要約が表示されます。続行するには、**[終了]** をクリックします。



11. 必要なすべてのソフトウェアはアップグレード処理のこの時点ですべてインストール済みですが、次に、使用するネットワーク インターフェイス、ポート、および証明書を設定する必要があります。

**重要:** この設定ステップに進まないと、mobilEcho サーバーは機能しません。このステップは必須です。

インストーラを終了すると、Acronis Access 設定ユーティリティを実行するよう促すプロンプトが表示されます。続行するには、**[OK]** をクリックしてください。



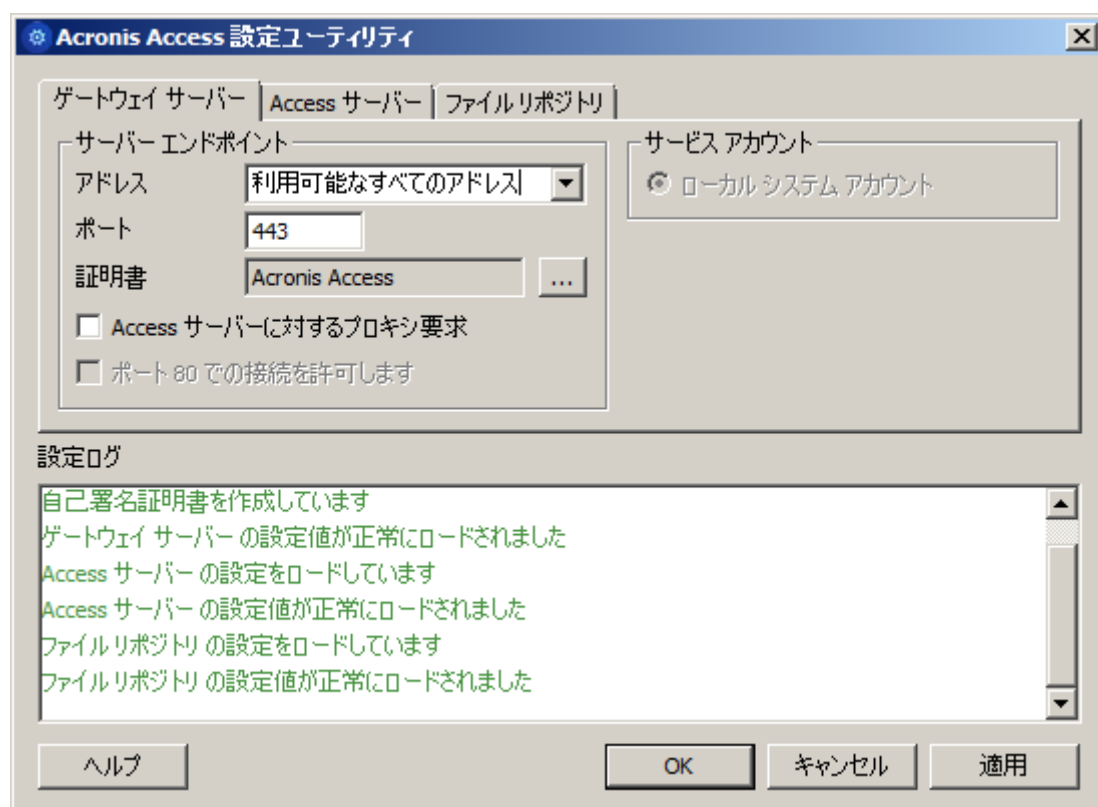
誤ってこのステップを飛ばしてしまった場合、あるいは後でネットワーク インターフェイス、ポート、または証明書を変更しなければならなくなった場合は、設定ユーティリティをいつでも手動で実行できます。

アップグレード済みの mobilEcho サーバーにおいて、ユーティリティのデフォルト位置は以下のとおりです。

**C:\Program Files (x86)\Group Logic\Configuration Utility\AcronisAccessConfiguration.exe**

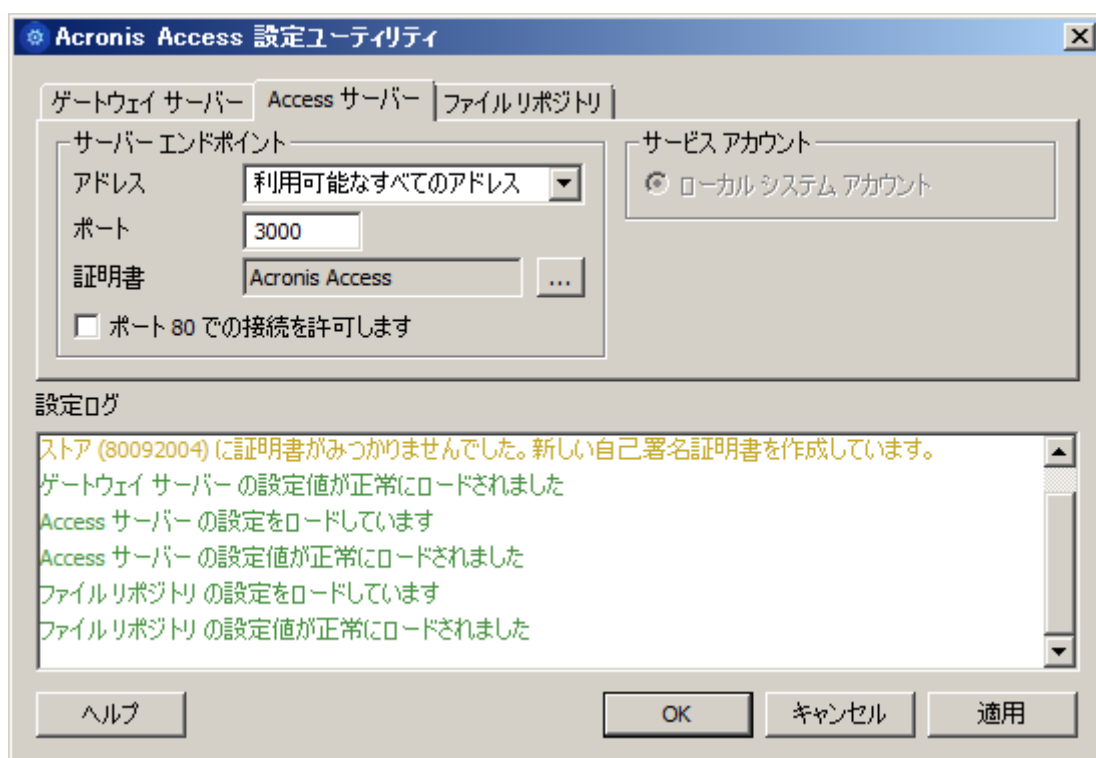
12. Acronis Access ゲートウェイ サーバーのネットワーク アドレス、ポート、および証明書を設定するには、設定ユーティリティ内で [ゲートウェイ サーバー] タブを使用します。Acronis Access ゲートウェイ サーバーは mobilEcho クライアントの接続先となる主要な mobilEcho サービスであり、ファイル サーバー、NAS、および SharePoint サーバーへのアクセス権はここから付与されます。Acronis Access より前、このサービスは mobilEcho File Access Server という名前でした。

**注意:** 既存の設定は保持されます。これらの設定が mobilEcho File Access Server の既存の設定と一致することを確認してください。通常、このサービスはすべての有効なネットワーク アドレスのポート 443 で実行されます。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。



13. [Access Server] タブを使用して、Acronis Access サーバーのネットワーク アドレス、ポート、証明書を設定します。Acronis Access サーバーは、mobilEcho Client Management Server ウェブ コンソールの後継になるウェブ コンソールです。

**注意:** mobilEcho Client Management Server の既存の設定と同じ設定になっていることを確認してください。通常、このウェブ コンソールはすべての有効なネットワーク アドレスのポート 3000 で実行されます。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。



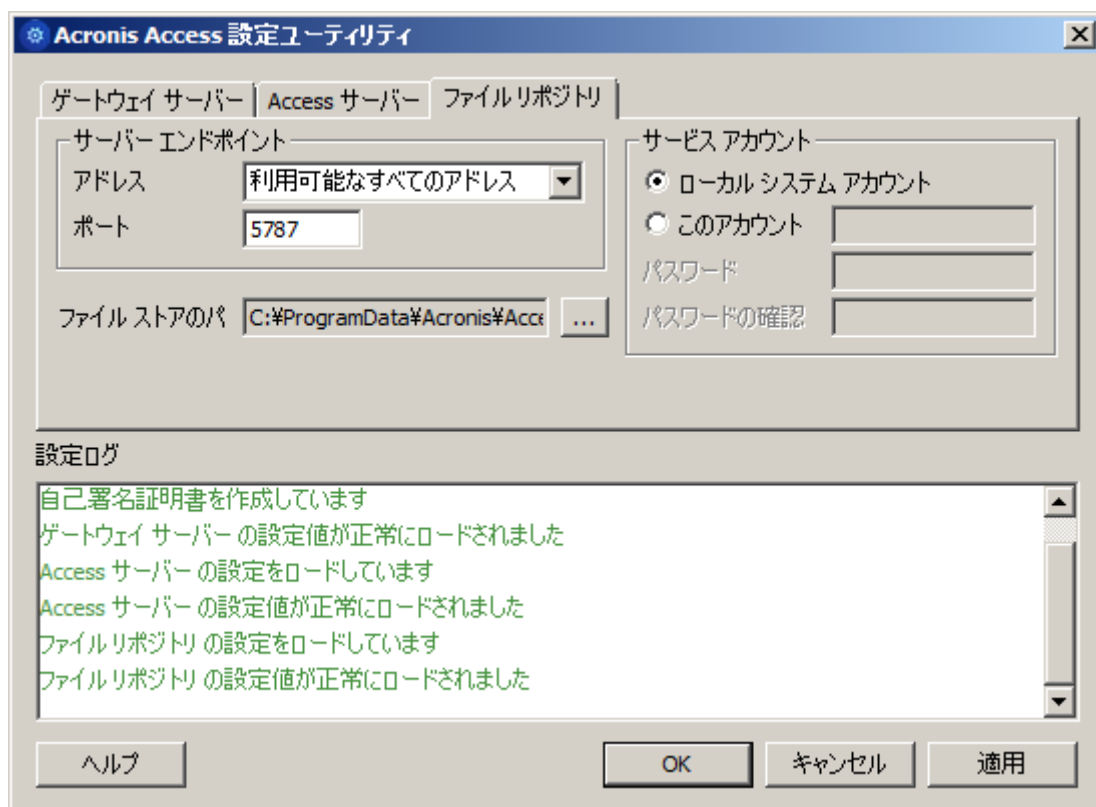
14. Acronis Access Server では、ファイル リポジトリの場所を選択しなければなりません。mobilEcho だけを使用する場合、このファイル リポジトリに何かを格納することはありませんが、それでも場所の設定は必要です。

このリポジトリは、Acronis の activEcho のファイル同期機能とファイル共有機能で使われます。これらの機能がまだインストールされていないサーバーをアップグレードした場合、これらの機能は有効になりませんが、必要に応じて後から有効にすることができます。

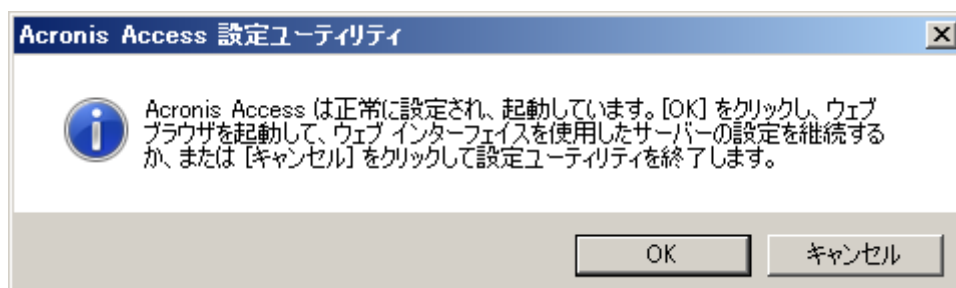
ファイル リポジトリのデフォルトの場所は、以下のとおりです。

**C:\ProgramData\Acronis\Access\FileStore**

後から activEcho を試してみようと思う場合は、C: ドライブではなくデータ ドライブにある場所を選択することもできます。この場所もインストール後に変更できます。



15. **[OK]** をクリックして設定ユーティリティを終了し、設定を適用します。
16. その後、Acronis Access Server ウェブ コンソールに初めてログインすることによって、この設定作業を完了できます。表示される画面で **[OK]** をクリックしてウェブ ブラウザを起動すると、設定が完了します。



#### Acronis Access で必要な初期設定:

1. 上記の手順を実行すると、Acronis Access Server のウェブ コンソールが自動的に表示されます。各種サービスが起動してウェブ ページの初回のロードが完了するまでに、30 秒程度の時間がかかることがあります。
2. ウェブ ページが自動的にロードされない場合は、ウェブ ブラウザを開いて、設定ユーティリティで選択した Access Server の HTTPS アドレスとポートを指定してください。
  - a. たとえば、https://mobilecho.mycompany.com:3000 または https://localhost:3000 のように指定します。

**注意:** SMTP、全般設定、LDAP の各ページにある設定のほとんどは、常に mobilEcho のシステムから提示されます。

3. Acronis Access Server では、ローカル管理者アカウントを作成する必要があります。このローカル管理者アカウントのパスワードを入力して、確認のために再度入力してください。



- a. このローカル管理者アカウントのユーザー名は administrator です。
  - b. このローカル管理者のパスワードを安全な場所に保管しておいてください。他の管理ユーザーを設定するまでは、管理者としてログインするためにそのパスワードが必要になります。
  - c. サーバーを設定したら、サーバーの管理者としての役割を果たす追加の Active Directory ユーザー/グループを設定できるようになります。
4. この時点で、残りの設定プロセスを進めていくための設定ウィザードが表示されます。
  5. ライセンス
    - a) 新しいタイプのライセンスの入力を求めるメッセージが表示されるか、古い mobilEcho ライセンスの使用を続けることになります。
  6. SMTP の設定

**Acronis Access** administrator

**SMTP**

Acronis Access サーバーは、構成された SMTP サーバーを使用して電子メールを送信し、ファイルの共有やデバイスの登録のためにユーザーを招待したり、ユーザーや管理者にサーバー アクティビティを通知したりします。

SMTP サーバー アドレス

SMTP サーバー ポート

セキュリティで保護された接続を使用しますか？ ☒

差出人名

差出人電子メール アドレス

SMTP 認証を使用しますか？ ☐

- Access Server でアラートやクライアント登録招待の電子メールを送信するために使用する SMTP の設定を定義するための画面が表示されます。
- テスト用の電子メールを送信して設定内容を確認するためのオプションもあります。

## 7. LDAP の設定

**Acronis Access** administrator

**LDAP**

組織内のユーザーにモバイル アクセスを提供するためにディレクトリ サービスを使用することができます。管理対象のモバイル アクセスには LDAP が必要です。

LDAP を有効にしますか？ ☒

LDAP サーバー アドレス

LDAP サーバー ポート

セキュリティで保護された LDAP 接続を使用しますか？ ☐

LDAP ユーザー名

LDAP パスワード

LDAP パスワードの確認入力

LDAP 検索ベース

LDAP 認証のためのドメイン

- Acronis Access Server では、ポリシーやデータ ソースの割り当て先にするユーザーやグループを Active Directory で検索するときに、LDAP 接続が必要になります。

- b. ネットワーク上にある Active Directory サーバーの LDAP 情報を入力してください。マルチドメイン ネットワークがある場合は、ポート 3268 または 3269 (SSL 接続の場合) のグローバル カタログ サーバーを指定する必要があります。各フィールドの詳細を説明したツールチップが表示されます。
  - c. サーバーから LDAP への要求を実行するときに使用する LDAP のユーザー名とパスワードを設定しなければなりません。
  - d. 入力した LDAP の設定値を保存するときに、その設定値がテストされます。
8. 初期設定はこれで完了です。
- a. **[設定の完了]** をクリックして次に進みます。

## **mobilEcho ゲートウェイ サーバーの登録**


mobilEcho クライアント管理サービスが設定されていた既存の mobilEcho 4.5 以前のサーバーをアップグレードすると、[サーバーとフォルダ] ページで設定されていたすべてのサーバーが Acronis Access ゲートウェイ サーバーのリストにインポートされます。

これらのゲートウェイ サーバーは、初期状態ではレガシー ゲートウェイ サーバーとしてインポートされます。これはつまり、Acronis Access ウェブ コンソールで管理するための登録がまだなされていないサーバーという意味です。Acronis Access へのアップグレード後にこれらのゲートウェイ サーバーを管理するには、この登録作業が必要になります。

これらのサーバーを管理対象として登録するには、まずこれらのサーバーを Acronis Access にアップグレードしなければなりません。アップグレードするまでは、Windows プログラムの mobilEcho Administrator を使用してこれらのサーバーを引き続き管理できます。

以下の例では、mobilEcho 4.5 の [サーバーとフォルダ] ページにあった 2 つのサーバーが [ゲートウェイ サーバー] ページに表示されています。

[Devices](#) | [Invitations](#) | [Groups](#) | [Users](#) | [Servers & Folders](#) | [Allowed Apps](#) | [Settings](#) | [Log out](#)



## Client Management Administrator

### Servers and Folders

mobilEcho servers and folders can be assigned to users and groups, so that they automatically appear in the mobilEcho client app. Servers and folders can be assigned to any user and group, independent of mobilEcho management profiles. Each user will receive the collection of resources that is assigned to their user account and any groups they have membership in.

#### Servers

Add your mobilEcho file servers here. In order to configure a shared folder below, the server that folder resides on must first be added to this list.

Add new server

| mobilEcho Server       | Display Name      |                        |
|------------------------|-------------------|------------------------|
| bgu2008.gililabs.com   | Z BGU2008         | <a href="#">delete</a> |
| devtest.grouplogix.com | Department Server | <a href="#">delete</a> |





mobileEcho 4.5 Client Management Administrator で設定されていたすべての既存のフォルダは、まず [データ ソース] ページの [レガシー データ ソース] タブに移されます。関連するゲートウェイ サーバーを Acronis Access にアップグレードするまでは、引き続きこのページでフォルダの追加や変更の操作を実行できます。ゲートウェイ サーバーを Acronis Access にアップグレードし、この Acronis Access サーバーで管理されるように登録すると、そのゲートウェイ サーバーに関連付けられたフォルダが、[データ ソース] ページのメインの [フォルダ] タブに移動します。

**注意:** どの mobileEcho Gateway Server も、1 つの Acronis Access コンソールだけで管理できます (複数のコンソールから管理することはできません)。mobileEcho Client Management Server (現在の名称: Acronis Access サーバー) が複数ある場合は、Acronis Access Server ごとに固有のゲートウェイ サーバーを実装する必要があります。



このシナリオでは、1 つの Windows サーバーで Acronis Access コンソールとゲートウェイ サーバーを実行するので、[ゲートウェイ サーバー] ページに表示されるサーバーは 1 つだけになります。このサーバーを管理するには、登録が必要です。

1. Acronis Access Server でそのゲートウェイ サーバーのメニュー ボタンをクリックして、[登録] を選択します。



|   |       |               |      |   |    |
|---|-------|---------------|------|---|----|
|   | Local | 192.168.1.141 | レガシー | 0 | 詳細 |
| <div> <div>アドレスの編集</div> <div>登録</div> <div>削除</div> </div> |       |               |      |   |    |

- 登録対象のサーバーの既存のネットワーク アドレスでそのサーバーに直接アクセスできるかどうかを確認するための画面が表示されます。通常、既存のアドレスは、モバイル デバイスのユーザーがゲートウェイ サーバーにアクセスするために使用するネットワーク アドレスになっているので、プロキシ サーバーや負荷分散装置のアドレスになっている可能性があります。

**注意:** その場合は、このダイアログで **[いいえ]** を選択し、Acronis Access サーバーからこのゲートウェイ サーバーへの直接的なネットワーク アクセスをするための代替ネットワーク アドレスを入力する必要があります。

サーバー 'Local' の登録

このゲートウェイ サーバーのクライアント向けアドレスは 192.168.1.141 です。このサーバーは Acronis Access ウェブ コンソールから管理されます。192.168.1.141 が、負荷分散装置またはリバース プロキシ サーバーをポイントしている場合、代替管理アドレスを設定する必要がある場合があります。192.168.1.141 は、この個別のゲートウェイ サーバーに直接アクセスするために使用できるアドレスですか？

- その後、登録ダイアログが表示されます。

サーバー 'Demo Share' の登録

名前:

Demo Share

管理とクライアント 接続のアドレス:

https:// sda.gililabs.com:4430

☐ クライアント 接続に代替アドレスを使用

管理キー:

MCGE-KAW4-NR92

☒ 自己署名証明書を使用した Acronis Access サーバーからの接続を許可

Save

キャンセル

**注意:** ゲートウェイ サーバーで自己署名 SSL 証明書を使用する場合は、[自己署名した証明書を使用した Acronis Access サーバーからの接続を許可] を有効にする必要があります。

**注意:** このリモート サーバーとの組み合わせを有効にするために、管理キーを入力することも必要です。この目的は、管理作業のための関係を検証し、セキュリティを確保することです。

- ゲートウェイ サーバーから管理キーを取得するには、ウェブ ブラウザの新しいウィンドウまたはタブを開いて、ゲートウェイ サーバーの HTTPS アドレスを指定します。[管理

とクライアント接続のアドレス] フィールドに表示されるアドレスと同じアドレスを入力してください。

**Acronis  
Access**

管理

この Acronis Access Gateway Serverを設定するには、Acronis Access Management Server に登録する必要があります。登録するには、Management Server の [ゲートウェイ サーバー] セクションにアクセスし、次のキーを使用して新しいゲートウェイ サーバーを登録します。

**CH3H-M6V9-MNAZ**

**注意:** セキュリティ上の理由から、この操作は、ゲートウェイ サーバーが実際に稼動している Windows サーバーのウェブ ブラウザから実行する必要があります。リモート ウェブ ブラウザから管理キーを表示することはできません。

5. 12 桁の管理キー(ダッシュを含む)を登録フォームに入力して、**[保存]** をクリックします。

**注意:** サーバーを登録すると、[ゲートウェイ サーバー] リストに登録済みのサーバーとして表示され、そのサーバーの設定を変更したり、詳細情報や状況を表示したりすることが可能になります。

**ゲートウェイ サーバー**
+ ゲートウェイ サーバーの追加
+ クラスタグループの追加

| タイプ | 名前          | アドレス             | バージョン | ステータス | アクティブ セッション |      |
|-----|-------------|------------------|-------|-------|-------------|------|
| ☰   | Main Server | rrt.gllilabs.com |       | レガシー  | 0           | ① 詳細 |
| ☰   | Local       | 192.168.1.141    |       | 🟢     | 0           | ① 詳細 |

① 詳細  
 ✎ 編集  
 🔒 アクセス制限  
 ✖ 削除

登録が済むと、Acronis Access へのアップグレード前に mobilEcho ゲートウェイ サーバーに存在していたボリュームが [データ ソース] ページのフォルダ リストにインポートされます。

**Acronis  
Access**

administrator

フォルダ
クライアントで表示されるゲートウェイ サーバー
レガシー データソース
割り当て済みのソース

**フォルダ**

フォルダは、Acronis Access がアクセス権を付与するファイル コンテンツの場所を定義します。フォルダはユーザーおよびグループに割り当てることができるので、モバイル クライアント アプリに自動的に表示されます。各ユーザーは、ユーザー アカウントおよびメンバーであるグループに割り当てられた一連のリソースを受け取ります。また、ユーザーがゲートウェイ サーバーを参照する場合に、これらを表示するようにも設定できます。

ゲートウェイ サーバーで特定のフォルダのロケーションを追加し、これらのフォルダをユーザーまたはグループに割り当てます。

| タイプ | 表示名            | サーバー  | パス                                      | 同期 |     |
|-----|----------------|-------|---|----|-----|
| 📁   | test folder    | Local | D:\testfolder                           | なし | ✎ ✖ |
| 🔑   | Access         | Local | https://192.168.1.141:3000              | なし | ✎ ✖ |
| 📁   | Thousand Files | Local | \\vega\test files\10000 files           | なし | ✎ ✖ |
| 📁   | SharePoint     | Local | http://sharepoint2010.gllilabs.com:2229 | なし | ✎ ✖ |

mobilEcho 5.0 には「ボリューム」がなくなりました。ボリュームを使用してデータソースを共有する代わりに、フォルダを作成するようになりました。これらのフォルダには [サーバーの参照時に表示する] というオプションのプロパティがあります。このオプションを有効にすると、ユーザーが mobilEcho アプリでゲートウェイサーバーのルートを参照したときに、mobilEcho 4.5 以前でボリュームが表示されていたのとまったく同様に、フォルダが表示されます。

フォルダの編集

表示名: test folder

このデータソースにアクセス権を付与するために使用するゲートウェイサーバーを選択する:

Local (192.168.1.141)

データのロケーション: ゲートウェイサーバー上

この Acronis Access ゲートウェイサーバー上で共有するローカルフォルダのパスを入力します (例: "E:\Shares\Documents\").  
 ワイルドカード文字列 %USERNAME% をパスに含めることができます。この場合、ワイルドカードはユーザーのユーザー名で置き換えられます。

パス: D:\testfolder

同期: なし

☒ サーバーの参照時に表示する  
☐ Salesforce.com アクティビティのログ記録を必須にする

ユーザーまたはグループにこのフォルダを割り当てる
 

次に該当するユーザーまたはグループを検索
 先頭の文字
 検索

このフォルダの割り当て先:

| 共通名 | 識別名 |
|-----|-----|
|     |     |

保存

キャンセル

mobilEcho 4.5 以前のサーバーにあったボリュームはすべて、[サーバーの参照時に表示する] プロパティが有効に設定されたフォルダとして Acronis Access コンソールにインポートされます。したがって、ユーザーが mobilEcho ゲートウェイサーバーのルートを参照するときには、これらのフォルダが引き続き表示されます。後から追加したフォルダについては、この設定を有効にすることにより、ボリュームと類似の方法で動作するように構成できます。先進的なクライアント管理機能を使用し始めることもできます。例えば、割り当て先の Active Directory ユーザーまたはグループのリスト用の mobilEcho クライアント アプリに自動で表示されるフォルダを追加する機能などです。

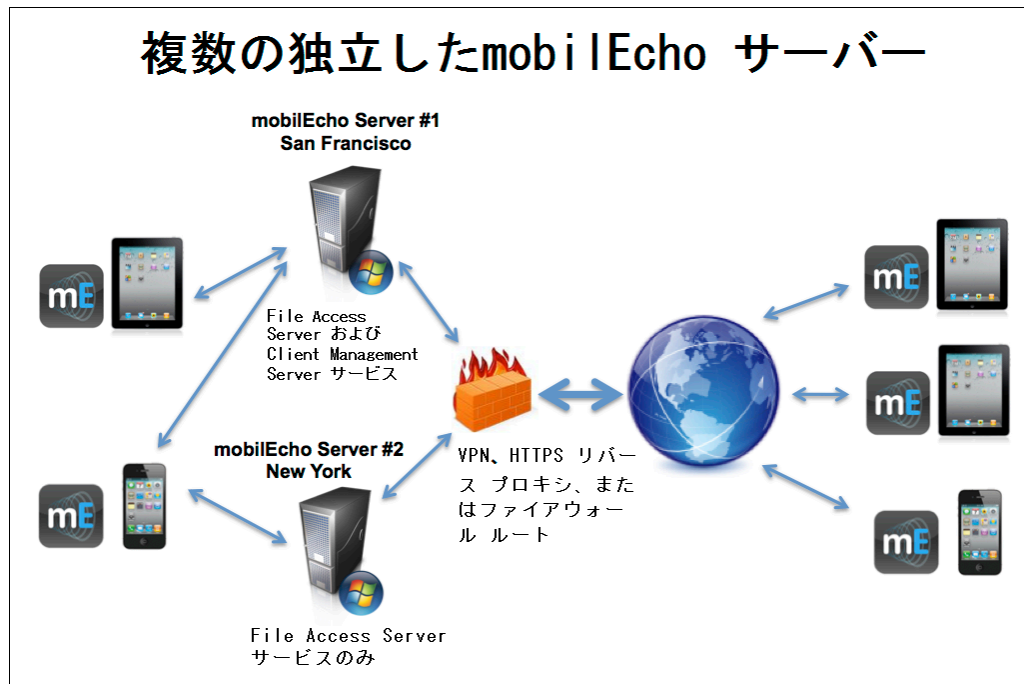
以下に示すとおり、ゲートウェイ サーバーの登録後、この mobilEcho 4.5 サーバーの 4 つの既存のボリュームが [フォルダ] リストにインポートされ、mobilEcho アプリからサーバーを参照するときに引き続き表示されます。

| フォルダ  |                |       |   |    |            |
|---|----------------|-------|---|----|------------|
| クライアントで表示されるゲートウェイ サーバー    レガシー データソース    割り当て済みのソース  |                |       |   |    |            |
| <b>フォルダ</b>   |                |       |   |    | 新しいフォルダを追加 |
| <p>フォルダは、Acronis Access がアクセス権を付与するファイル コンテンツの場所を定義します。フォルダはユーザーおよびグループに割り当てることができるので、モバイル クライアント アプリに自動的に表示されます。各ユーザーは、ユーザー アカウントおよびメンバーであるグループに割り当てられた一連のリソースを受け取ります。また、ユーザーがゲートウェイ サーバーを参照する場合に、これらを表示するようにも設定できます。</p> <p>ゲートウェイ サーバーで特定のフォルダのロケーションを追加し、これらのフォルダをユーザーまたはグループに割り当てます。</p> |                |       |   |    |            |
| タイプ   | 表示名            | サーバー  | パス                                      | 同期 |            |
| test folder   | test folder    | Local | D:\testfolder                           | なし |            |
| Access  | Access         | Local | https://192.168.1.141:3000              | なし |            |
| Thousand Files  | Thousand Files | Local | \\vega\test files\10000 files           | なし |            |
| SharePoint  | SharePoint     | Local | http://sharepoint2010.gililabs.com:2229 | なし |            |



### 3.3.2.3 複数の mobilEcho サーバー(クライアント管理あり)のアップグレード

#### シナリオ 3: 複数の mobilEcho サーバー(クライアント管理あり)のアップグレード



これは、複数の Windows サーバーで mobilEcho 4.5 以前を実行する環境です。1 つのサーバーで、必須の mobilEcho File Access Server サービスが稼動し、オプションの mobilEcho クライアント管理サーバー サービスが有効になっています。その他のサーバーでは、mobilEcho File Access Server だけを実行します。

Acronis Access にアップグレードすると、mobilEcho File Access Server が Acronis Access ゲートウェイ サーバーにアップグレードされます。このサービスは、引き続き mobilEcho クライアントからの接続を受け入れ、ユーザーがアクセスするすべてのファイル サーバーや、NAS または SharePoint のデータ ソースへのゲートウェイの役割を果たします。

mobilEcho クライアント管理サーバーを実行するサーバーの mobilEcho Client Management Administrator ウェブ コンソールは、Acronis Access サーバー ウェブ コンソールにアップグレードされます。アップグレード後は、mobilEcho File Access Server を管理するために、それぞれのサーバーで Windows プログラム mobilEcho Administrator を使用することはありません。この新しいウェブ コンソールを使用すれば、1 つの統合的なウェブ インターフェイスから mobilEcho のすべてのサーバーとクライアントを管理できます。

**Acronis Access のアップグレードは次の手順で実行します。**

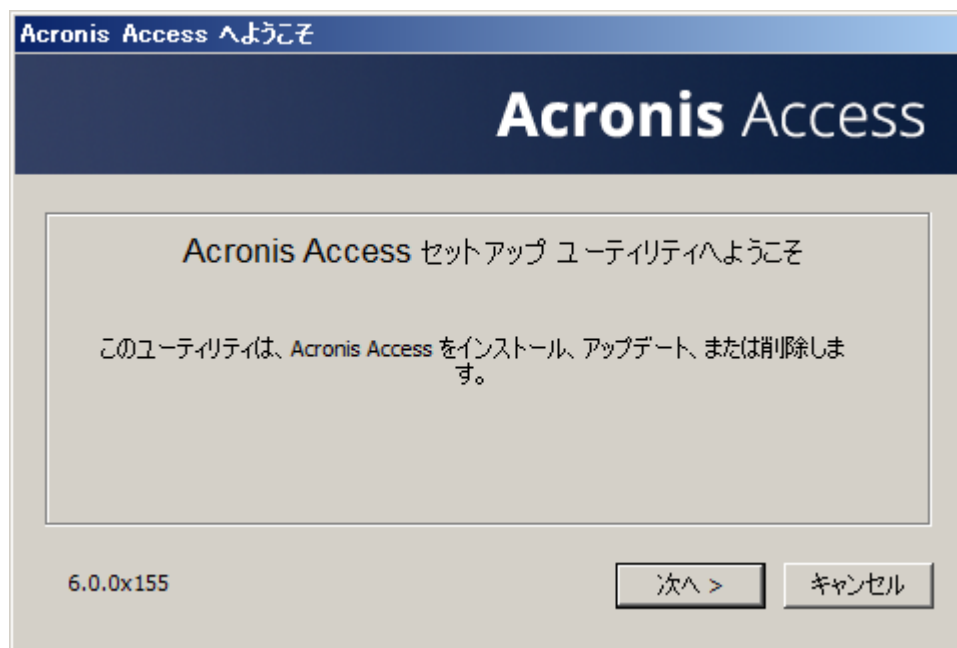
**mobilEcho Client Management Server を実行する Windows サーバーで、以下の手順を実行します。**

1. シナリオ 2 の手順を実行して、mobilEcho Client Management Server を実行する Windows サーバーをアップグレードします。これは、mobilEcho Client Management Administrator ウェブ コンソールにログインするときの接続先になっていたサーバーです。

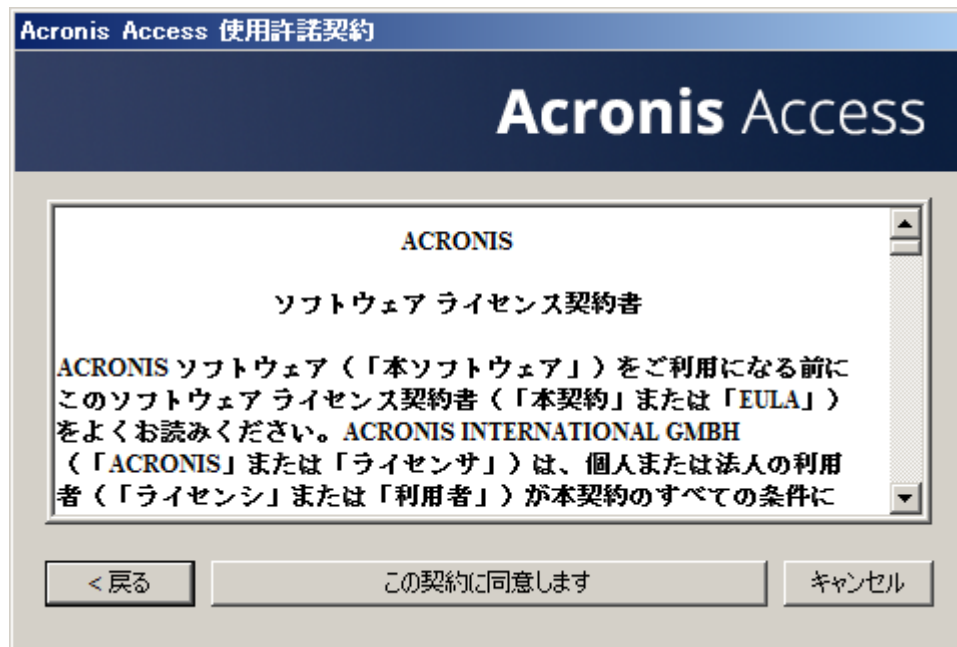
2. このアップグレードが完了すると、機能の豊富な Acronis Access サーバー ウェブ コンソールを使用できるようになり、その Windows サーバーにある mobilEcho File Access Server (現在の名称 Acronis Access ゲートウェイ サーバー)が管理対象として登録されます。さらに、[Acronis Access Gateway Server] ページでは、その他のサーバーがレガシー サーバーとして表示されます。以下の例では、アップグレード済みのサーバー「BGU2008」が登録済みになっている一方で、まだアップグレードしていないサーバー「Department Server」は未登録になっています。
3. 次に、mobilEcho File Access Server だけを実行する他のサーバーをそれぞれアップグレードします。以下の手順を実行してください。

**mobilEcho File Access Server だけを実行するそれぞれの Windows サーバーで、以下の手順を実行します。**

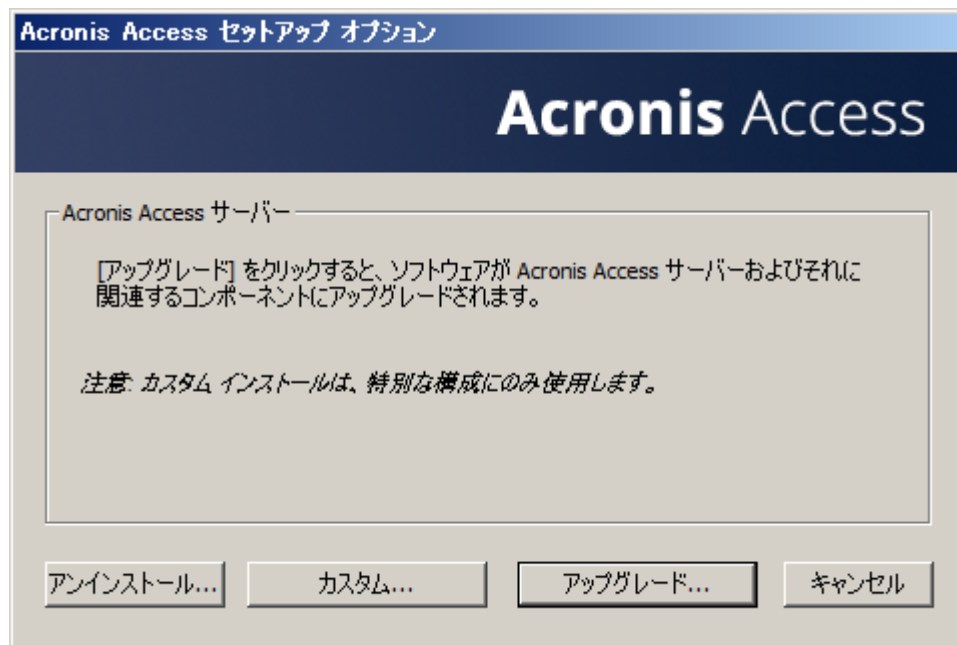
1. 必要なファイルすべてをバックアップします。「mobilEcho 4.5 バックアップ」や「activEcho 2.7 バックアップ」のガイドに従ってください。
2. 対象のサーバーで Acronis Access インストーラを実行します。
3. [ようこそ] 画面で **[次へ]** をクリックします。



4. 使用許諾契約を読み、承諾します。

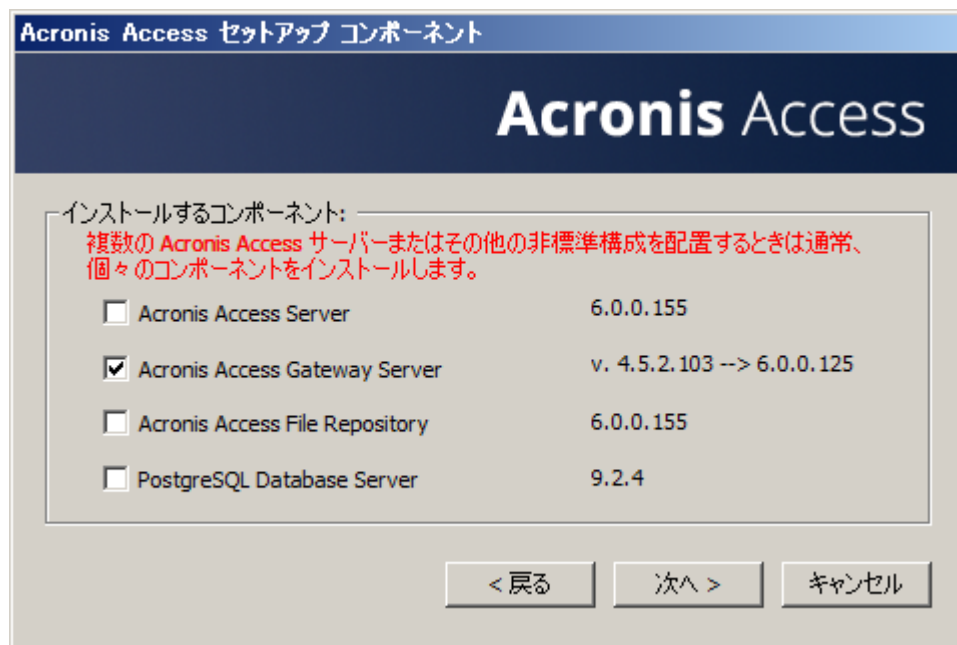


5. [カスタム] をクリックします。



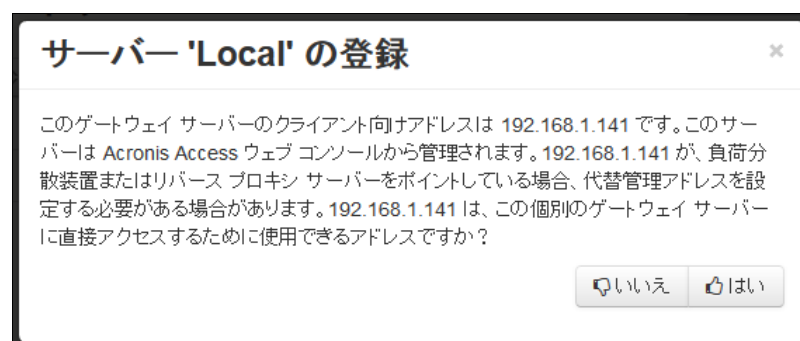
6. [Acronis Access ゲートウェイ サーバー] コンポーネントのみを選択して、[次へ] をクリックします。





7. 残りのインストール手順と設定ユーティリティの手順は、既に取り上げた内容と同じですが、ここでは設定ユーティリティで Access Server とファイル リポジトリを設定する必要はありません。
8. Acronis Access サーバー コンソールはインストールされていないので、設定ユーティリティのプロセスが完了したら、ウェブ コンソールに関する追加の設定は必要ありません。
9. フル インストールを実行した最初のサーバーの Acronis Access サーバー コンソールに戻ってください。[ゲートウェイ サーバー] ページを開き、Acronis Access にアップグレードした追加のゲートウェイ サーバーのメニュー ボタンをクリックして、[登録] を選択します。
10. 登録対象のサーバーの既存のネットワーク アドレスでそのサーバーに直接アクセスできるかどうかを確認するための画面が表示されます。通常、既存のアドレスは、モバイル デバイスのユーザーがゲートウェイ サーバーにアクセスするために使用するネットワーク アドレスになっているので、プロキシ サーバーや負荷分散装置のアドレスになっている可能性があります。

**注意:** その場合は、このダイアログで [いいえ] を選択し、Acronis Access サーバーからこのゲートウェイ サーバーへの直接的なネットワーク アクセスを取得するための代替ネットワーク アドレスを入力する必要があります。



11. その後、登録ダイアログが表示されます。



**注意:** ゲートウェイ サーバーで自己署名 SSL 証明書を使用する場合は、[自己署名証明書を使用した Acronis Access サーバーからの接続を許可] を有効にする必要があります。

**注意:** このリモート サーバーとの組み合わせを有効にするために、管理キーを入力することも必要です。この目的は、管理作業のための関係を検証し、セキュリティを確保することです。

12. このゲートウェイ サーバーから管理キーを取得するには、登録する実際の Windows サーバーでウェブ ブラウザの新しいウィンドウまたはタブを開いて、ゲートウェイ サーバーの HTTPS アドレスを指定します。[管理とクライアント接続のアドレス] フィールドに表示されるアドレスと同じアドレスを入力してください。

**注意:** セキュリティ上の理由から、この操作は、ゲートウェイ サーバーが実際に稼働している Windows サーバーのウェブ ブラウザから実行する必要があります。リモート ウェブ ブラウザから管理キーを表示することはできません。

13. 12 桁の管理キー(ダッシュを含む)を登録フォームに入力して、**[保存]** をクリックします。

**注意:** サーバーを登録すると、[ゲートウェイ サーバー] リストに登録済みのサーバーとして表示され、そのサーバーの設定を変更したり、詳細情報や状況を表示したりすることが可能になります。

**注意:** 登録が済むと、Acronis Access へのアップグレード前にこの mobilEcho ゲートウェイ サーバーに存在していたボリュームが [データ ソース] ページのフォルダ リストにインポートされます。その後の動作は、前のアップグレード シナリオで取り上げた内容のとおりです。

14. このゲートウェイ サーバーのすべての管理作業は、Acronis Access サーバー ウェブ コンソールから実行できます。[データ ソース] ページで新しいフォルダを作成すると、有効なゲートウェイ サーバーのリストにこのゲートウェイ サーバーが表示され、その新しいフォルダにアクセスできるようになります。

15. アップグレードして登録するゲートウェイ サーバーがまだある場合は、ここで取り上げた手順を繰り返してください。

### 3.3.2.4 クライアント管理を有効に設定した単一の mobilEcho サーバーと activEcho サーバーのアップグレード

この手順については、「activEcho サーバーと mobilEcho Client Management Server のアップグレード『117ページ』」の記事を参照してください。

## 3.3.3 mobilEcho 4.5 へのダウングレード

Acronis Access の mobilEcho 4.5 へのダウングレードは複雑な手順であるため、やむを得ない場合以外は行わないでください。正しいバックアップを作成して、安全な場所に保管してください。

### Acronis Access の mobilEcho 4.5 へのダウングレード

**警告:** 手順全体が完了するまで mobilEcho Administrator にライセンスを追加しないでください。この手順の実行中にレジストリを編集しないでください。

この手順を正しく実行するには、Acronis Access のアップグレードが成功していなければなりません。

1. 開始する前に、ファイル **settings\_backup** とフォルダ **Legacy mobilEcho files** のバックアップを取ります。

**注意:** ファイルは **C:\Program Files (x86)\Group Logic\mobilEcho Server** にあり、フォルダのパスは **C:\Program Files (x86)\Group Logic\Access Server\Legacy mobilEcho files** です。

2. mobilEcho 4.5 インストーラと Acronis Access インストーラをダウンロードします。
3. Acronis Access のインストーラを実行します。
4. [ようこそ] 画面で **[次へ]** をクリックします。
5. 使用許諾契約に同意します。
6. **[アンインストール]** をクリックしてダウングレードの手順を開始します。
7. 警告のポップアップで **[OK]** をクリックします。
8. **[すべての Acronis Access コンポーネントのアンインストール]** を選択します。
9. 選択されているコンポーネントを確認し、**[アンインストール]** をクリックします。
10. PostgreSQL のアンインストールのポップアップで **[はい]** をクリックします。一部のファイルと設定は残されます。
11. アンインストールされた内容すべてを確認し、**[終了]** をクリックします。
12. mobilEcho 4.5 インストーラを実行します。
13. 使用許諾契約を読んで同意してから、**[次へ]** をクリックします。
14. 前に mobilEcho をインストールしたフォルダを選択します。デフォルトのままだった場合は、今回もそのデフォルトを使用できます。
15. **[インストール]** をクリックして、mobilEcho 4.5 のインストールを開始します。インストールが完了したら、**[Launch the File Server Administrator]** (File Server Administrator を起動)を選択解除して、**[完了]** をクリックします。
16. バックアップした **settings\_backup** ファイルを実行します。
17. バックアップした **Legacy mobilEcho files** フォルダを開きます。

- a. ファイル `invitation.html.erb` と `invitation.txt.erb` を、`C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\app\views\user_mailer` にコピーします。
- b. ファイル `mobilEcho_manager` を `C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI` にコピーします。
- c. ファイル `production.sqlite3` を `C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db` にコピーします。
- d. `priority.txt` という第 4 のファイルがある場合は、それを `C:\Program Files (x86)\Group Logic\mobilEcho Server\Management` にコピーします。**Management** フォルダは手動で作成する必要があります。

---

**注意:** まず古いファイルを削除してから新しいファイルをコピーすることを強くお勧めします。

---

18. **mobilEcho File Access** サービスを開始し、**mobilEcho Management** サービスを開始します。

---

**注意:** ユーザーおよびグループのすべてのプロファイルを手動で再び有効にする必要があります。

---

## 3.4 activEcho バージョン 2.7 以前からのアップグレード

### セクションの内容

|                    |     |
|--------------------|-----|
| 開始する前に.....        | 111 |
| アップグレード プロセス ..... | 112 |

### 3.4.1 開始する前に

#### アップグレード前の activEcho のバックアップ

既存の activEcho サーバーによって使用されているデータ ファイルをバックアップしてください。

activEcho 2.7 以前のサーバーのバックアップと復元のプロセスについては、<http://docs.grouplogic.com/display/ActivEcho/Maintenance+Tasks> を参照してください。

---

**注意:** アップグレードすると、activEcho ウェブ インターフェイスのすべてのカスタマイズが失われます。

---

**Acronis Access** にアップグレードするには、事前にご使用の **activEcho** のバージョンをバージョン 2.7 にアップデートしてください。

#### アップグレード前の Tomcat のバックアップ

アップグレード時に Apache Tomcat がアップグレードされ、現在の Tomcat のすべての設定ファイル、証明書、およびログ ファイルが削除されます。Apache Tomcat フォルダのコピーを作成することをお勧めします。デフォルトでは、このフォルダは次の場所にあります: **C:\Program Files (x86)\Group Logic\Common**。

### 設定の確認

アップグレードを続行する前に、次のことを確認してください。

- mobilEcho と activEcho の両方がインストールされていることを確認します。

- mobilEcho と activEcho が同一のコンピュータにインストールされているか、別々のコンピュータにインストールされているかを確認します。
- mobilEcho で使用されているポートを確認します。また、ファイル サーバーおよび管理サーバーのポートも確認します。
- activEcho で使用されているポートを確認します。ファイル レポジトリが同じコンピュータにあることを確認します。

## 3.4.2 アップグレード プロセス

### activEcho 5.0 のアップグレード プロセス

まず、アップグレードする activEcho 実装環境のタイプを確認します。この後のセクションでは、シナリオごとに実行手順を説明していきます。以下のようなシナリオが一般的です。

1. **単一 activEcho サーバー(mobilEcho Client Management Server なし)**
  - 1 つの Windows サーバーで activEcho Server だけを実行する環境です。
2. **単一 activEcho サーバー(mobilEcho Client Management Server あり)**
  - 1 つの Windows サーバーで activEcho Server と mobilEcho Client Management Server/File Server サービスの両方を実行する環境です。
3. **activEcho Server と mobilEcho Client Management Server を別々のサーバーで実行する環境**
  - 1 つの Windows サーバーで activEcho Server を実行し、別のサーバーで mobilEcho Client Management サービスを実行する環境です。

#### セクションの内容

|   |     |
|---|-----|
| 単一 activEcho サーバー(mobilEcho Client Management Server なし)のアップグレード..... | 112 |
| activEcho サーバーと mobilEcho Client Management Server のアップグレード.....      | 117 |
| 別サーバーの mobilEcho クライアント管理サーバーを使用する activEcho<br>サーバーのアップグレード.....     | 124 |

### 3.4.2.1 単一 activEcho サーバー(mobilEcho Client Management Server なし)のアップグレード

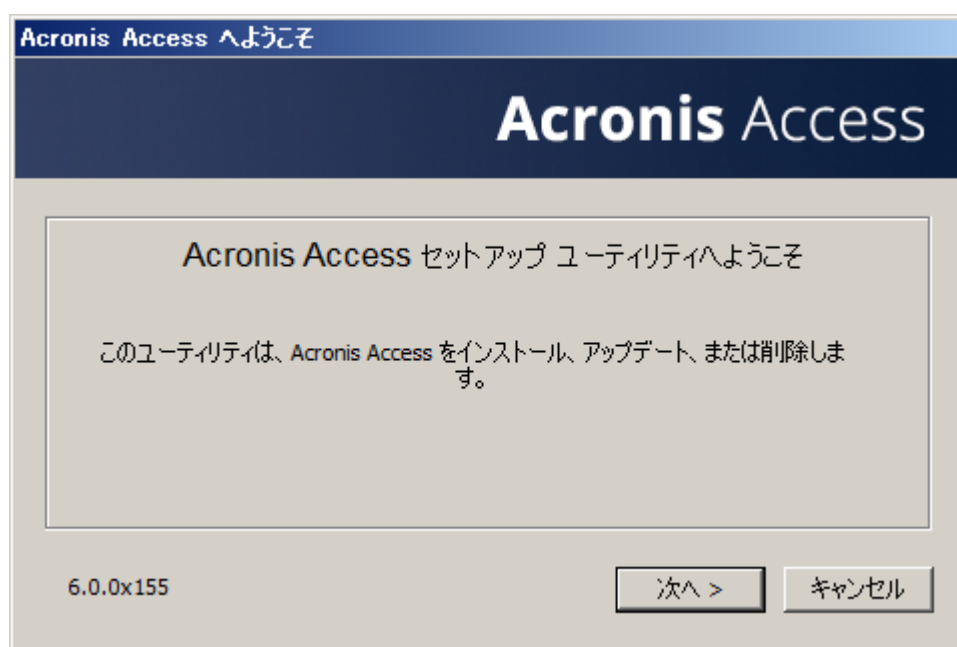
#### シナリオ 1 - 単一 activEcho サーバー(mobilEcho Client Management Server なし)のアップグレード

これは、1 つの Windows サーバーで activEcho Server だけを実行する環境です。この手順によって、activEcho Server を Acronis Access Server ウェブ コンソールにアップグレードします。この新しいコンソールには、activEcho のすべての機能が含まれており、さらにいくつかの機能が追加されています。Acronis Access サーバー ウェブ コンソールを使用すれば、1 つの共通のウェブ インターフェイスから activEcho と mobilEcho の両方を管理できます。

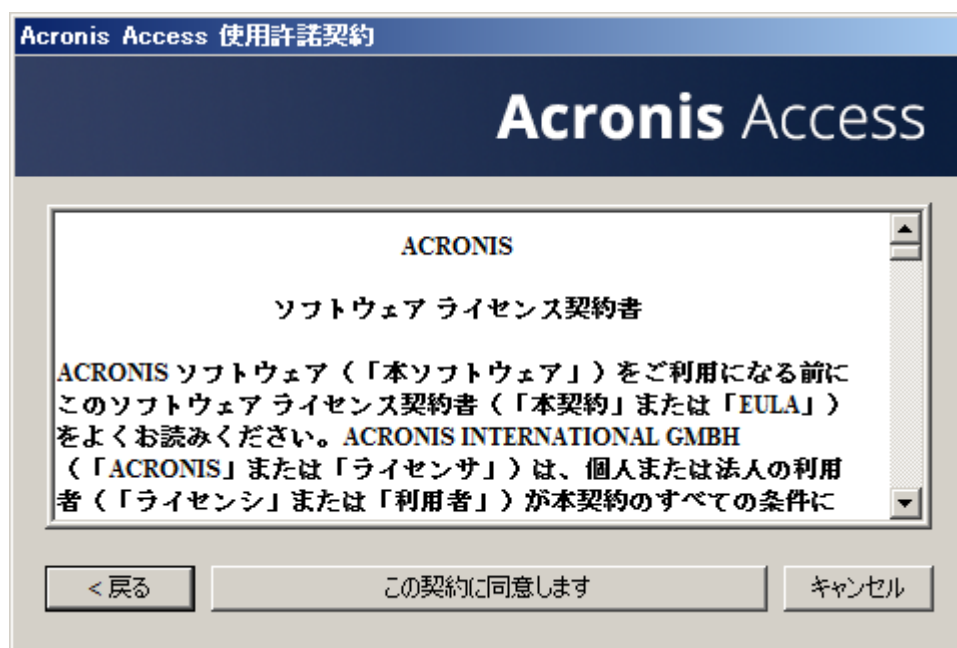
**activEcho のアップグレードを実行するには、次のように操作します。**

1. 必要なファイルすべてをバックアップします。「mobilEcho 4.5 バックアップ」や「activEcho 2.7 バックアップ」のガイドに従ってください。

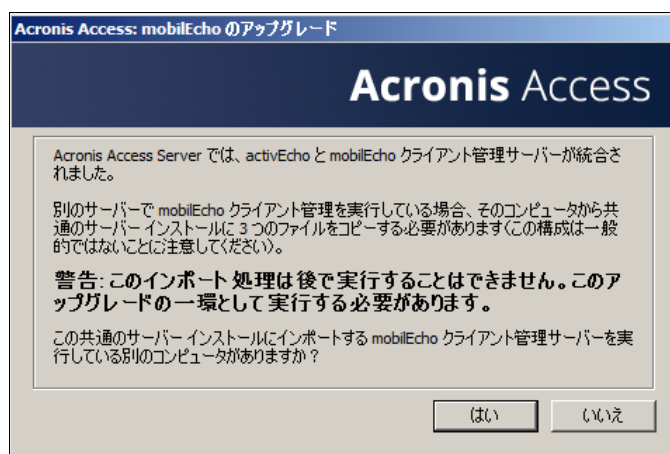
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. Acronis Access Server インストーラを activEcho サーバーにダウンロードし、インストーラを実行します。
  - a. 最新版のインストーラを入手するには、[http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598) にアクセスします。
  - b. 確認のため、インストーラをダウンロードする前に製品のプロダクト キーを入力する必要があります。
  - c. インストーラ ファイルの名前は AcronisAccessSetup.exe です。
4. [ようこそ] 画面で [次へ] をクリックします。



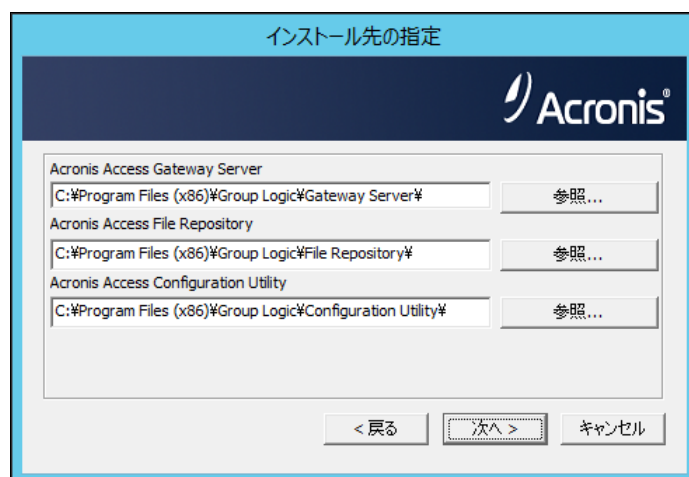
5. 使用許諾契約に同意します。



6. **[アップグレード]** をクリックすると、activEcho Server が新しい Acronis Access Server に自動的にアップグレードされます。このアップグレード プロセスでは、ゲートウェイ サーバーとそのサーバーに必要な各種サービスもインストールされます。
7. リモート mobilEcho Server に関する画面が表示されます。mobilEcho Client Management Server がいない場合は、**[いいえ]** をクリックします。mobilEcho Client Management Server がある場合は、「mobilEcho クライアント管理サーバーを使用する activEcho サーバーのアップグレード『117ページ』」または「別サーバーの mobilEcho クライアント管理サーバーを使用する activEcho サーバーのアップグレード『124ページ』」の記事を参照してください。そこでは、mobilEcho のインストールを伴うアップグレードについて説明されています。



8. Acronis Access コンポーネントのインストール先となるインストール ロケーションを選択します。既存の activEcho サーバーをアップグレードする場合、デフォルトのインストール パスは既存のインストール ロケーションになります。デフォルトのインストール パスを変更しないことをお勧めします。**[次へ]** をクリックします。

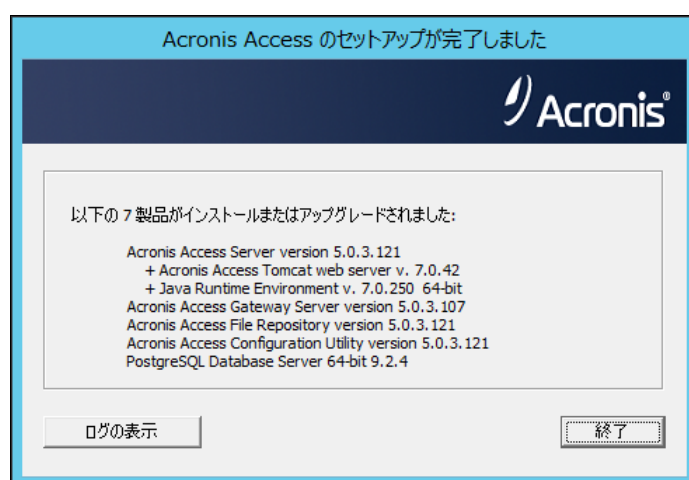




9. インストールおよびアップグレードするサービスを確認します。

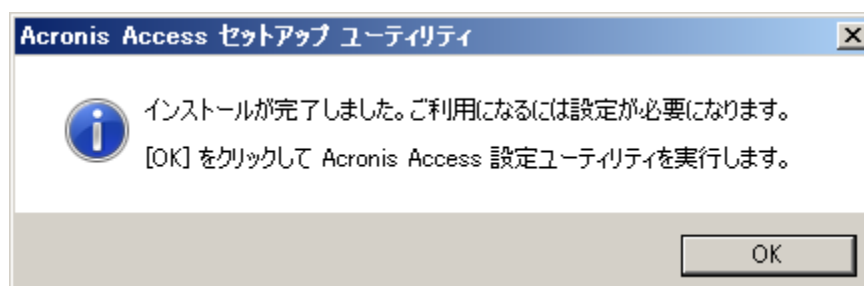


10. [インストール] を押して、アップグレードを開始します。インストールが完了すると、インストールされたコンポーネントの概要が表示されます。[終了] を押します。



**注意:** 必要なすべてのコンポーネントが順に自動的にインストールされます。これにはサーバーに応じて 5～15 分かかります。その後のアップグレードはより速く完了します。

11. 必要なすべてのソフトウェアはアップグレード処理のこの時点ですべてインストール済みですが、次に、使用するネットワーク インターフェイス、ポート、および証明書を設定する必要があります。このステップは必須です。インストーラを終了すると、Acronis Access 設定ユーティリティを実行するよう促すプロンプトが表示されます。続行するには、[OK] をクリックしてください。

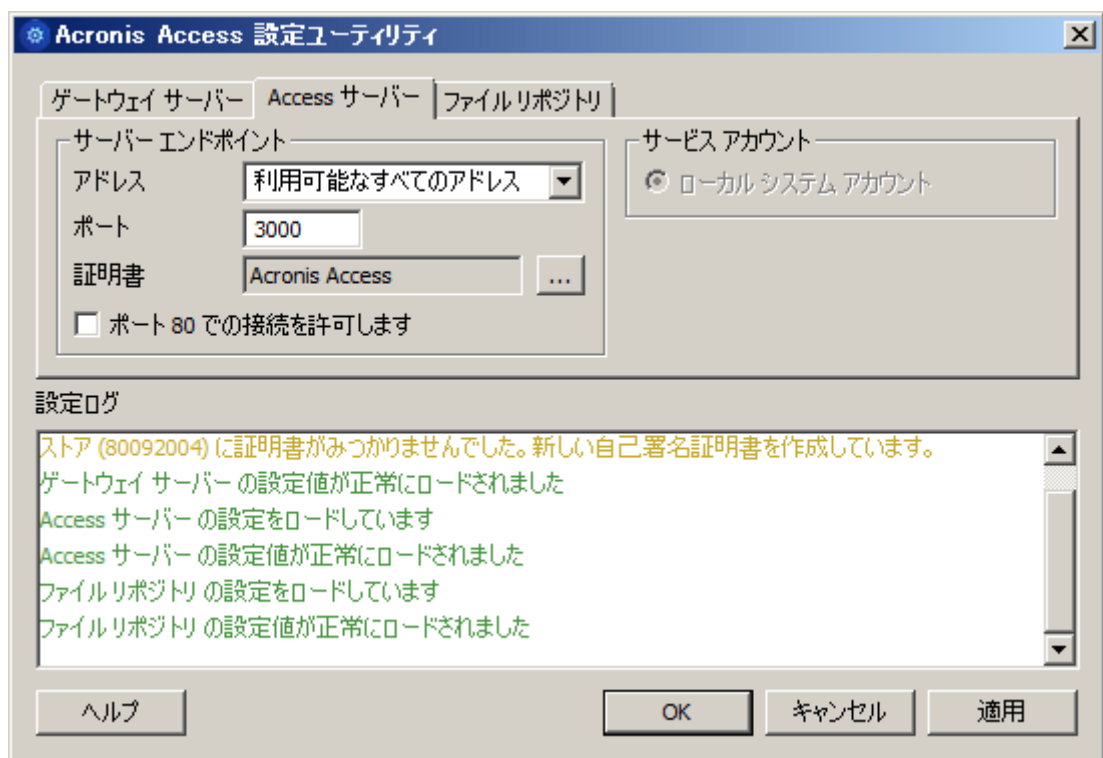


12. Acronis Access Gateway Server のネットワーク アドレス、ポート、および証明書を設定するには、設定ユーティリティ内で [ゲートウェイ サーバー] タブを使用します。Acronis Access Gateway Server は mobilEcho クライアントの接続先となる主要な Acronis Access サービスであり、ファイル サーバー、NAS、および SharePoint サーバーへのアクセス権はここから付与されます。

**注意:** 既存の設定は保持されます。これらの設定が mobilEcho File Access Server の既存の設定と一致することを確認してください。通常、このサービスは、すべての有効なネットワーク アドレスのポート 443 で実行されます。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。

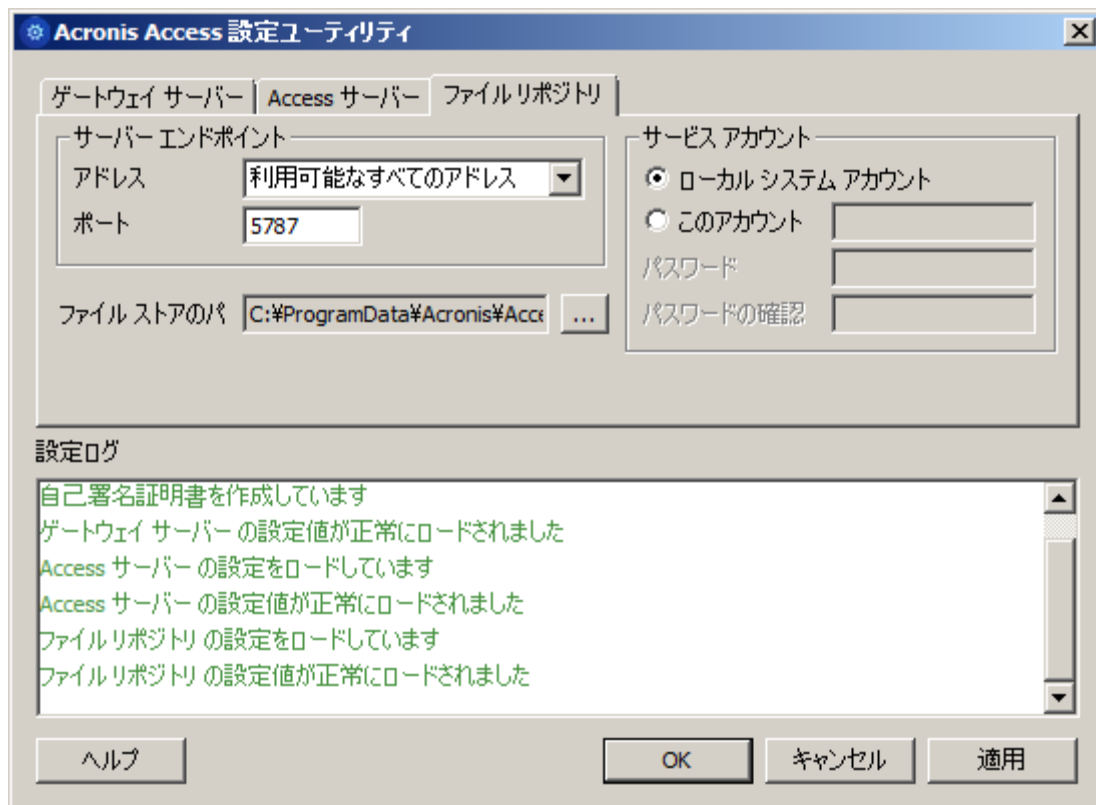
13. [Access Server] タブを使用して、Acronis Access Server のネットワーク アドレス、ポート、証明書を設定します。Acronis Access Server は、すべての同期および共有機能と activEcho ユーザーを設定したり、サーバー管理とリモート クライアント管理のすべての作業を実行したりするためのウェブ コンソールです。また、これはウェブ クライアントにアクセスするためにユーザーが使用するコンソールでもあります。

**注意:** Access Server の設定を確認してください。デフォルトの設定をお勧めします。通常、このウェブ コンソールは、ポート 3000 で有効になっているすべてのネットワーク アドレスで動作します。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。

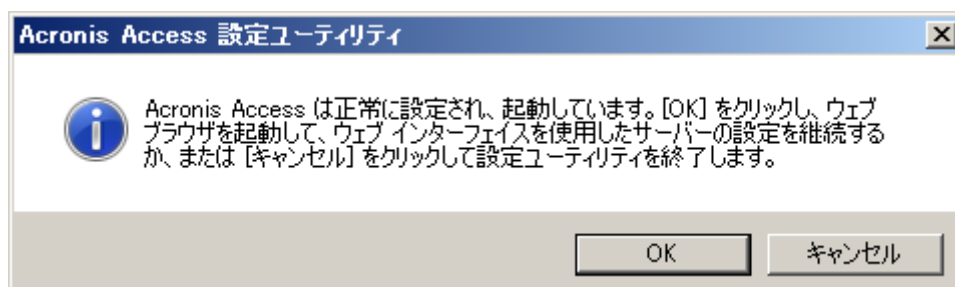


**注意:** Acronis Access Server では、ファイル リポジトリの場所を選択しなければなりません。このリポジトリは、Acronis の activEcho のファイル同期機能とファイル共有機能で使用します。





14. [OK] をクリックして設定ユーティリティを終了し、設定を適用します。
15. その後、Acronis Access Server ウェブ コンソールに初めてログインすることによって、この設定作業を完了できます。表示される画面で [OK] をクリックしてウェブ ブラウザを起動すると、設定が完了します。



### 3.4.2.2 activEcho サーバーと mobilEcho Client Management Server のアップグレード

#### シナリオ 2 - activEcho サーバーと mobilEcho Client Management Server のアップグレード

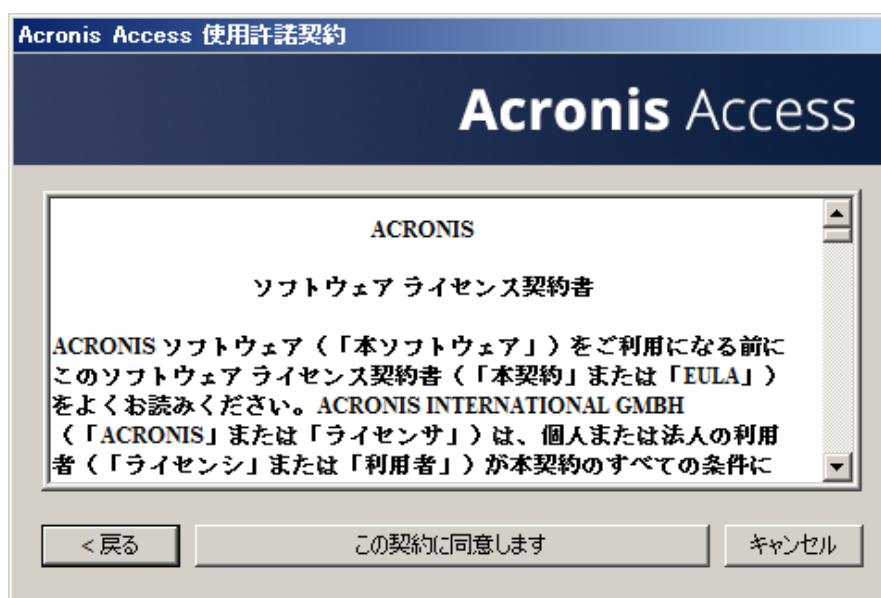
これは、1 つの Windows サーバーで activEcho Server と mobilEcho File Server と mobilEcho Management Server を実行するシナリオです。この手順では、activEcho サーバーと mobilEcho クライアント管理サーバーを統一 Acronis Access サーバー ウェブ コンソールにアップグレードします。以前 mobilEcho サーバーの管理に使用されていた mobilEcho Administrator Windows プログラムも新しいコンソールに置き換えられます。Acronis Access サーバー ウェブ コンソールを使用すれば、1 つの共通のウェブ インターフェイスから activEcho と mobilEcho の両方を管理できます。

**activEcho のアップグレードを実行するには、次のように操作します。**

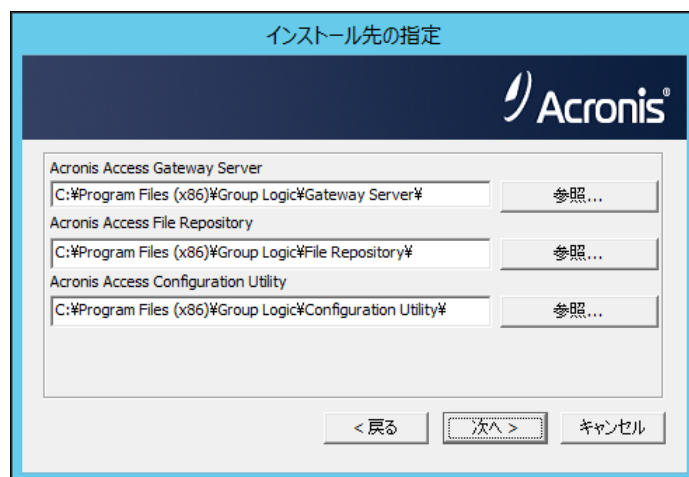
1. 必要なファイルすべてをバックアップします。「mobilEcho 4.5 バックアップ」や「activEcho 2.7 バックアップ」のガイドに従ってください。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. Acronis Access Server インストーラを activEcho サーバーにダウンロードし、インストーラを実行します。
  - a. 最新版のインストーラを入手するには、[http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598) にアクセスします。
  - b. 確認のため、インストーラをダウンロードする前に製品のプロダクト キーを入力する必要があります。
  - c. インストーラ ファイルの名前は AcronisAccessSetup.exe です。
4. [ようこそ] 画面で **[次へ]** をクリックします。



5. 使用許諾契約に同意します。



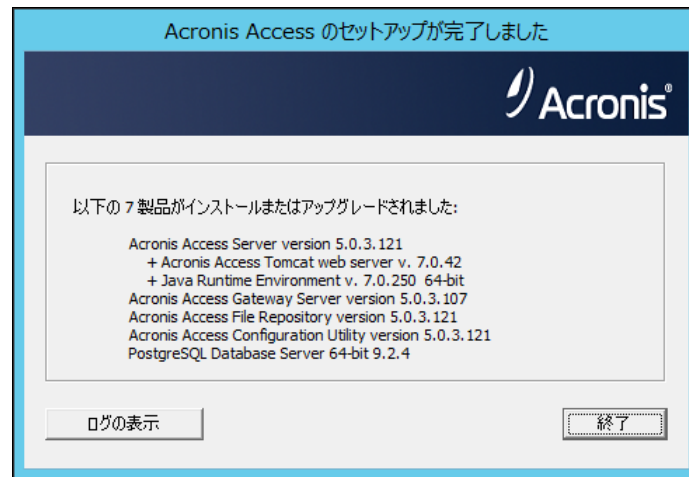
6. **[アップグレード]** をクリックすると、activEcho Server と mobilEcho Client Management Server が新しい Acronis Access Server に自動的にアップグレードされます。このアップグレード プロセスでは、ゲートウェイ サーバーとそのサーバーに必要な各種サービスもインストールされます。File Server もある場合は、新しいゲートウェイ サーバーがインストールされるのではなく、その File Server がインストーラにより新しいゲートウェイ サーバーにアップグレードされます。
7. Acronis Access コンポーネントのインストール先となるインストール ロケーションを選択します。既存の activEcho サーバーをアップグレードする場合、デフォルトのインストール パスは既存のインストール ロケーションになります。デフォルトのインストール パスを変更しないことをお勧めします。**[次へ]** をクリックします。



8. インストールおよびアップグレードするサービスを確認します。

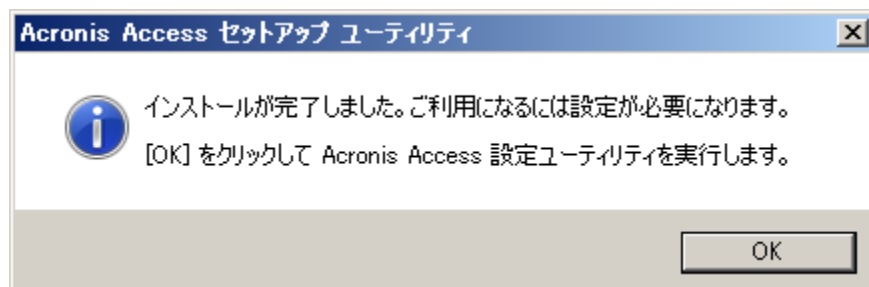


9. **[インストール]** を押して、アップグレードを開始します。インストールが完了すると、インストールされたコンポーネントの概要が表示されます。**[終了]** を押します。



**注意:** 必要なすべてのコンポーネントが順に自動的にインストールされます。これにはサーバーに応じて 5～15 分かかります。その後のアップグレードはより速く完了します。

10. 必要なすべてのソフトウェアはアップグレード処理のこの時点ですべてインストール済みですが、次に、使用するネットワーク インターフェイス、ポート、および証明書を設定する必要があります。このステップは必須です。インストーラを終了すると、Acronis Access 設定ユーティリティを実行するよう促すプロンプトが表示されます。続行するには、**[OK]** をクリックしてください。

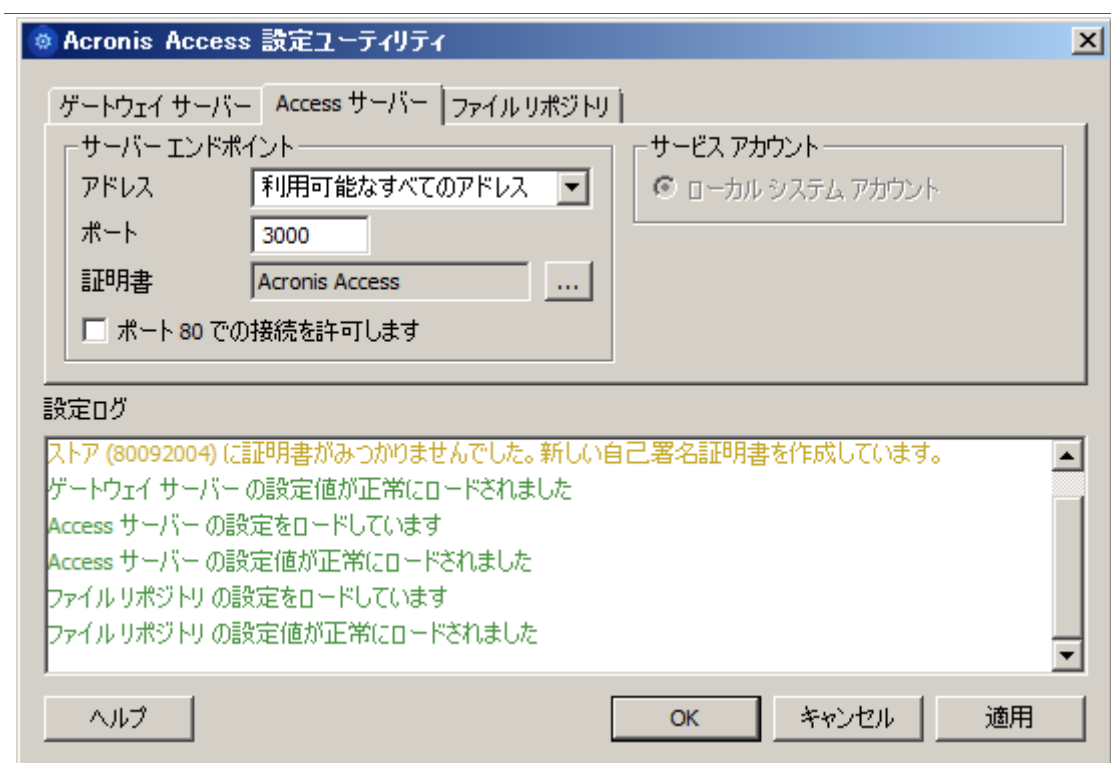


11. Acronis Access Gateway Server のネットワーク アドレス、ポート、および証明書を設定するには、設定ユーティリティ内で **[ゲートウェイ サーバー]** タブを使用します。Acronis Access Gateway Server は mobilEcho クライアントの接続先となる主要な Acronis Access サービスであり、ファイル サーバー、NAS、および SharePoint サーバーへのアクセス権はここから付与されます。

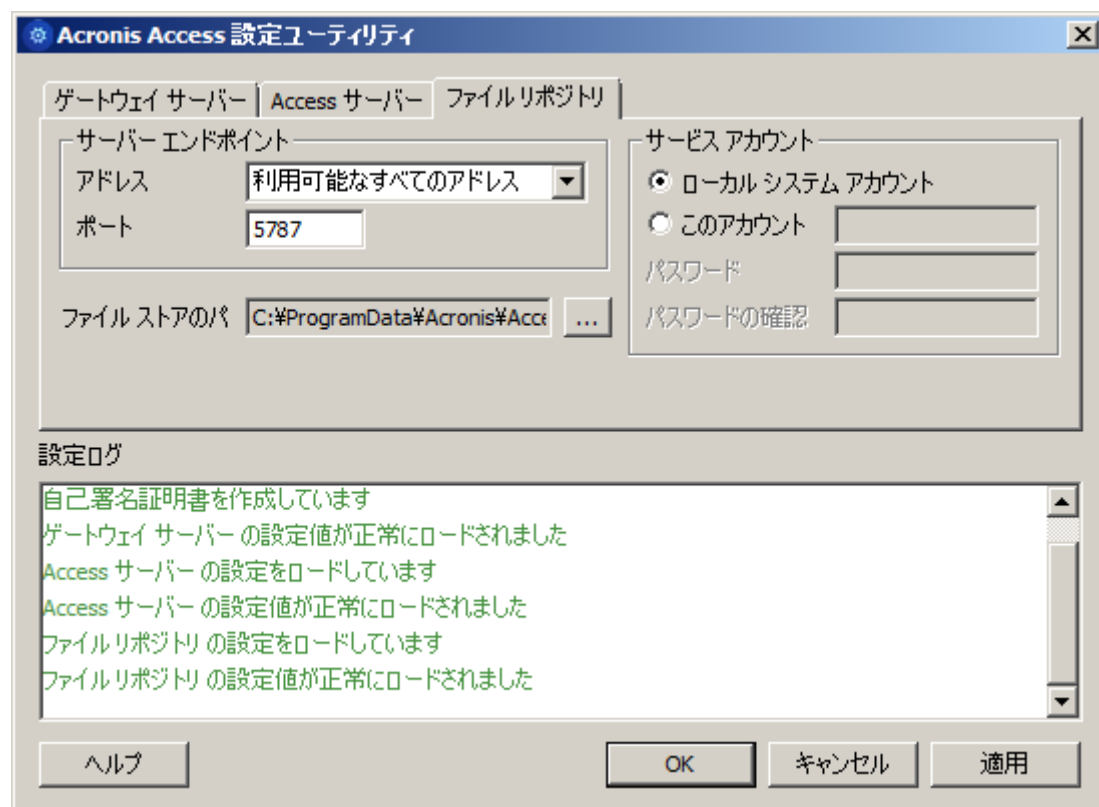
**注意:** 既存の設定は保持されます。これらの設定が mobilEcho File Access Server の既存の設定と一致することを確認してください。通常、このサービスは、すべての有効なネットワーク アドレスのポート 443 で実行されます。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。

12. **[Access Server]** タブを使用して、Acronis Access Server のネットワーク アドレス、ポート、証明書を設定します。Acronis Access Server は、すべての同期および共有機能と activEcho ユーザーを設定したり、サーバー管理とリモート クライアント管理のすべての作業を実行したりするためのウェブ コンソールです。また、これはウェブ クライアントにアクセスするためにユーザーが使用するコンソールでもあります。

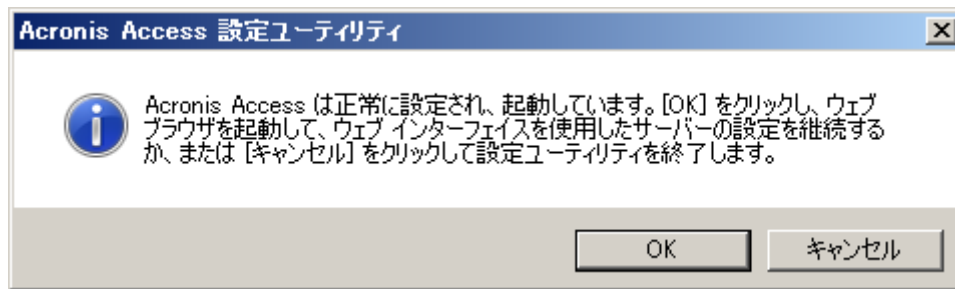
**注意:** Access Server の設定を確認してください。デフォルトの設定をお勧めします。通常、このウェブ コンソールは、ポート 3000 で有効になっているすべてのネットワーク アドレスで動作します。既存の SSL サーバー ID 証明書があれば、その証明書が自動的に選択されます。既存の SSL サーバー ID 証明書がない場合は、自己署名証明書が生成されます。



**注意:** Acronis Access Server では、ファイル リポジトリの場所を選択しなければなりません。このリポジトリは、Acronis の activEcho のファイル同期機能とファイル共有機能で使われます。



13. **[OK]** をクリックして設定ユーティリティを終了し、設定を適用します。
14. その後、Acronis Access Server ウェブ コンソールに初めてログインすることによって、この設定作業を完了できます。表示される画面で **[OK]** をクリックしてウェブ ブラウザを起動すると、設定が完了します。



## ゲートウェイの登録

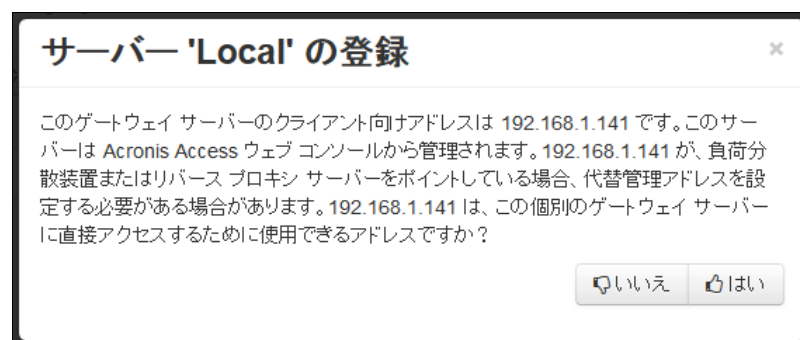
このシナリオでは、1 つの Windows サーバーで Acronis Access コンソールとゲートウェイ サーバーを実行するので、[ゲートウェイ サーバー] ページに表示されるサーバーは 1 つだけになります。このサーバーを管理するには、登録が必要です。

1. Acronis Access Server でそのゲートウェイ サーバーのメニュー ボタンをクリックして、**[登録]** を選択します。



2. 登録対象のサーバーの既存のネットワーク アドレスでそのサーバーに直接アクセスできるかどうかを確認するための画面が表示されます。通常、既存のアドレスは、モバイル デバイスのユーザーがゲートウェイ サーバーにアクセスするために使用するネットワーク アドレスになっているので、プロキシ サーバーや負荷分散装置のアドレスになっている可能性があります。

**注意:** その場合は、このダイアログで **[いいえ]** を選択し、Acronis Access サーバーからこのゲートウェイ サーバーへの直接的なネットワーク アクセスをするための代替ネットワーク アドレスを入力する必要があります。



3. その後、登録ダイアログが表示されます。

**サーバー 'Demo Share' の登録**

名前:

管理とクライアント接続のアドレス:

☐ クライアント接続に代替アドレスを使用

管理キー:

☒ 自己署名証明書を使用した Acronis Access サーバーからの接続を許可

**Save** **キャンセル**

**注意:** ゲートウェイ サーバーで自己署名 SSL 証明書を使用する場合は、[自己署名した証明書を使用した Acronis Access サーバーからの接続を許可] を有効にする必要があります。

**注意:** このリモート サーバーとの組み合わせを有効にするために、管理キーを入力することも必要です。この目的は、管理作業のための関係を検証し、セキュリティを確保することです。

4. ゲートウェイ サーバーから管理キーを取得するには、ウェブ ブラウザの新しいウィンドウまたはタブを開いて、ゲートウェイ サーバーの HTTPS アドレスを指定します。[管理とクライアント接続のアドレス] フィールドに表示されるアドレスと同じアドレスを入力してください。

**Acronis Access**

**管理**

この Acronis Access Gateway Serverを設定するには、Acronis Access Management Server に登録する必要があります。登録するには、Management Server の [ゲートウェイ サーバー] セクションにアクセスし、次のキーを使用して新しいゲートウェイ サーバーを登録します。

**CH3H-M6V9-MNAZ**

**注意:** セキュリティ上の理由から、この操作は、ゲートウェイ サーバーが実際に稼動している Windows サーバーのウェブ ブラウザから実行する必要があります。リモート ウェブ ブラウザから管理キーを表示することはできません。

5. 12 桁の管理キー(ダッシュを含む)を登録フォームに入力して、**[保存]** をクリックします。

**注意:** サーバーを登録すると、[ゲートウェイ サーバー] リストに登録済みのサーバーとして表示され、そのサーバーの設定を変更したり、詳細情報や状況を表示したりすることが可能になります。

| ゲートウェイ サーバー |             |                   |       |       |             |  | + ゲートウェイ サーバーの追加 | + クラスターグループの追加 |
|-------------|-------------|-------------------|-------|-------|-------------|--|------------------|----------------|
| タイプ         | 名前          | アドレス              | バージョン | ステータス | アクティブ セッション |  |                  |                |
| ☐           | Main Server | rrt.gillilabs.com |       | レガシー  | 0           |  | 詳細               |                |
| ☐           | Local       | 192.168.1.141     |       | 🟢     | 0           |  | 詳細               |                |

詳細  
 編集  
 アクセス制限  
 削除



### 3.4.2.3 別サーバーの mobilEcho クライアント管理サーバーを使用する activEcho サーバーのアップグレード

#### シナリオ 3 - 別サーバーの mobilEcho クライアント管理サーバーを使用する activEcho サーバーのアップグレード

**警告:** このシナリオでは、activEcho サーバーと mobilEcho サーバーは別個のままにして、各サーバーを個別にアップグレードすることを推奨します。activEcho サーバーのアップグレードの説明については、「mobilEcho クライアント管理サーバーを使用しない単一の activEcho サーバーのアップグレード『112ページ』」のガイドに従い、mobilEcho サーバーのアップグレードの説明については、「クライアント管理を有効に設定した単一の mobilEcho サーバーのアップグレード『88ページ』」のガイドに従ってください。

このシナリオでは、2 台(またはそれ以上)の Windows Server があり、一方は activEcho サーバーのみが稼働し、他方は mobilEcho ファイル サーバーと管理サーバーが稼働しているものとします。この手順では、activEcho サーバーと mobilEcho クライアント管理サーバーを統一 Acronis Access サーバー ウェブ コンソールにアップグレードします。以前 mobilEcho サーバーの管理に使用されていた mobilEcho Administrator Windows プログラムも新しいコンソールに置き換えられます。Acronis Access サーバー ウェブ コンソールを使用すれば、1 つの共通のウェブ インターフェイスから activEcho と mobilEcho の両方を管理できます。

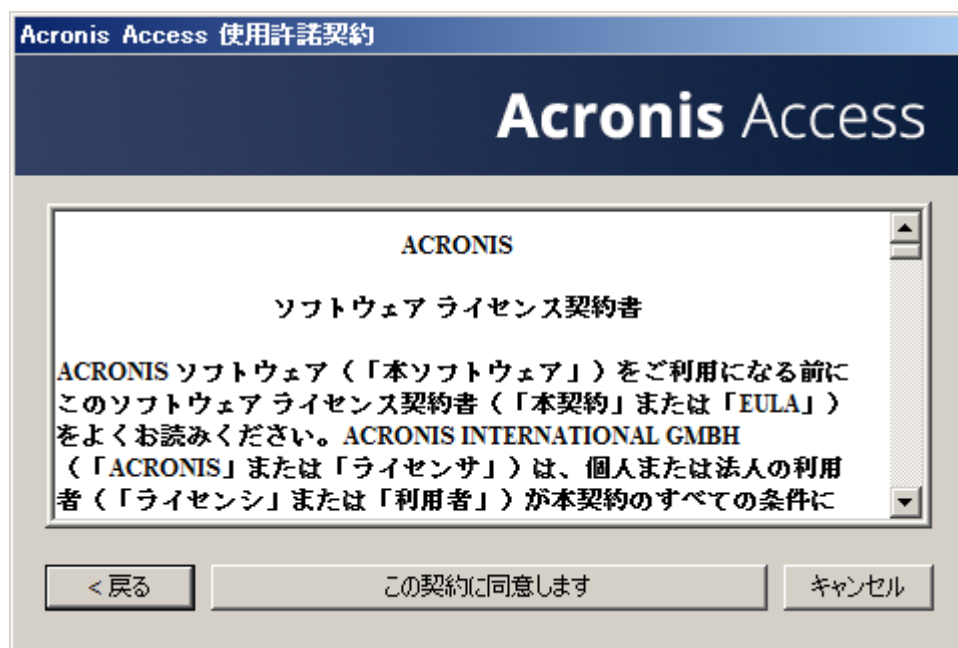
#### Acronis Access サーバーへのアップグレードを実行する手順:

1. 必要なファイルすべてをバックアップします。「mobilEcho 4.5 バックアップ」や「activEcho 2.7 バックアップ」のガイドに従ってください。
2. mobilEcho が稼働しているサーバーの現在の IP アドレスを書き出し、そのコンピュータに別の IP アドレスを与えます(新しい IP アドレスも必要になります)。
3. activEcho が稼働しているサーバーで、mobilEcho が稼働するサーバーの IP アドレスを別個のネットワーク アダプタに追加します。
4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. Acronis Access Server インストーラを activEcho サーバーにダウンロードし、インストーラを実行します。
  - a. 最新版のインストーラを入手するには、[http://support.grouplogic.com/?page\\_id=3598](http://support.grouplogic.com/?page_id=3598) にアクセスします。
  - b. 確認のため、インストーラをダウンロードする前に製品のプロダクト キーを入力する必要があります。
  - c. インストーラ ファイルの名前は AcronisAccessSetup.exe です。
6. [ようこそ] 画面で **[次へ]** をクリックします。

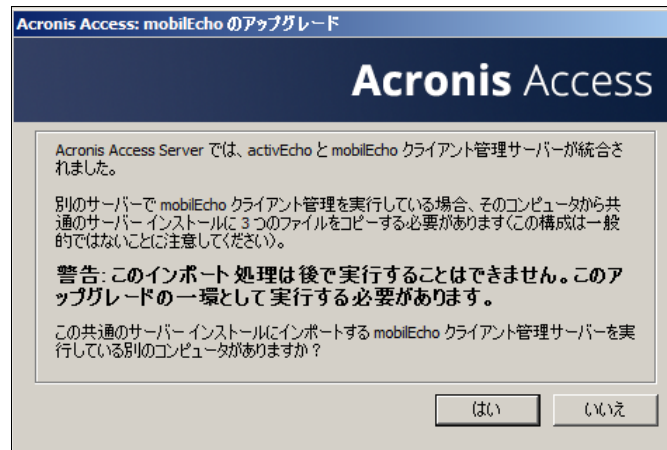




7. 使用許諾契約に同意します。



8. **[アップグレード]** をクリックすると、activEcho Server が新しい Acronis Access Server に自動的にアップグレードされます。このアップグレード プロセスでは、ゲートウェイ サーバーとそのサーバーで必要な各種サービスもインストールされます。
9. mobilEcho クライアント管理サーバーを使用している場合、**[はい]** をクリックします。mobilEcho クライアント管理サーバーを使用していない場合、mobilEcho の実行環境が存在しない場合のアップグレードに関する最初の記事に進みます。



10. mobilEcho クライアント管理サーバーが稼働しているサーバーで、**production.sqlite3**、**mobilEcho\_manager.cfg**、**priority.txt** (このファイルは存在しない可能性があります) の 3 つのファイルを見つけ、アップグレードを開始したマシンにそれらをコピーします。コピー先フォルダは、現在のコンピュータのダイアログに示されているフォルダ ロケーションです。このパスは、インストールごとに異なります (C:\¥Users¥Administrator¥AppData¥Local¥Temp¥Acronis Access Installer¥ など)。これらのファイルがすべてコピーされたら、[OK] を押して続行します。



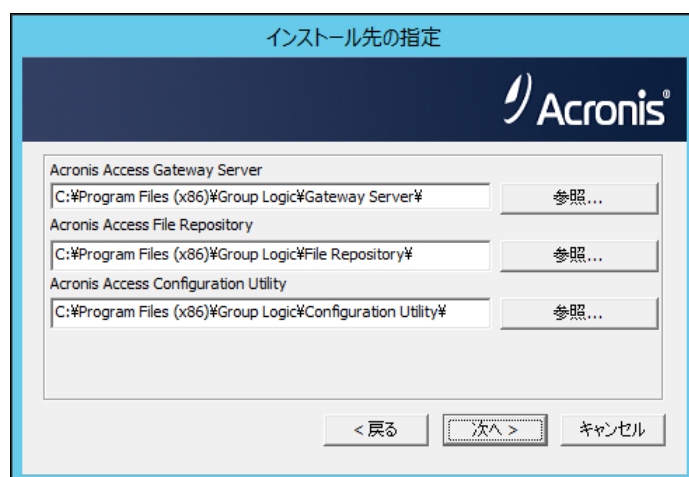
注意: これらのファイルは通常次の場所にあります。

**C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db\production.sqlite3**

**C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\mobilEcho\_manager.cfg**

**C:\Program Files (x86)\Group Logic\mobilEcho Server\Management\priority.txt**

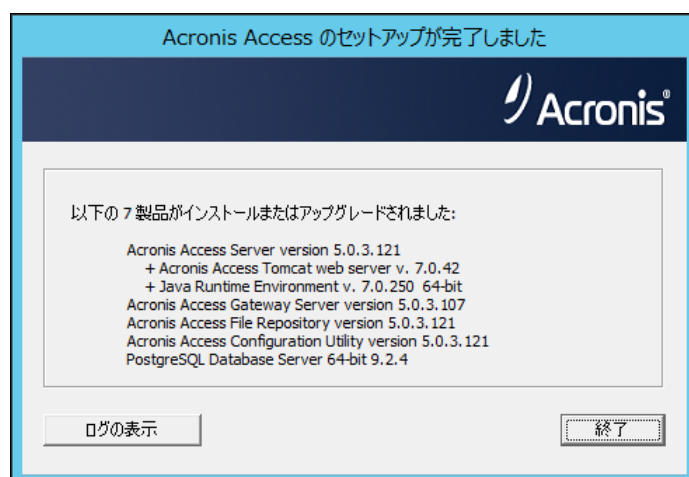
11. Acronis Access コンポーネントのインストール先となるインストール ロケーションを選択します。既存の activEcho サーバーをアップグレードする場合、デフォルトのインストール パスは既存のインストール ロケーションになります。デフォルトのインストール パスを変更しないことをお勧めします。[次へ] をクリックします。



12. インストールおよびアップグレードするサービスを確認します。

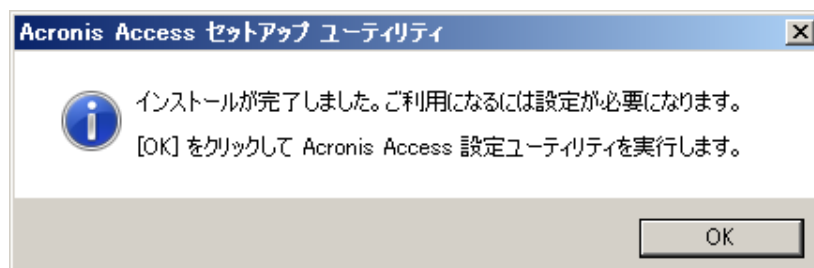


13. [インストール] を押して、アップグレードを開始します。インストールが完了すると、インストールされたコンポーネントの概要が表示されます。[終了] を押します。



**注意:** 必要なすべてのコンポーネントが順に自動的にインストールされます。これにはサーバーに応じて 5～15 分かかります。その後のアップグレードはより速く完了します。

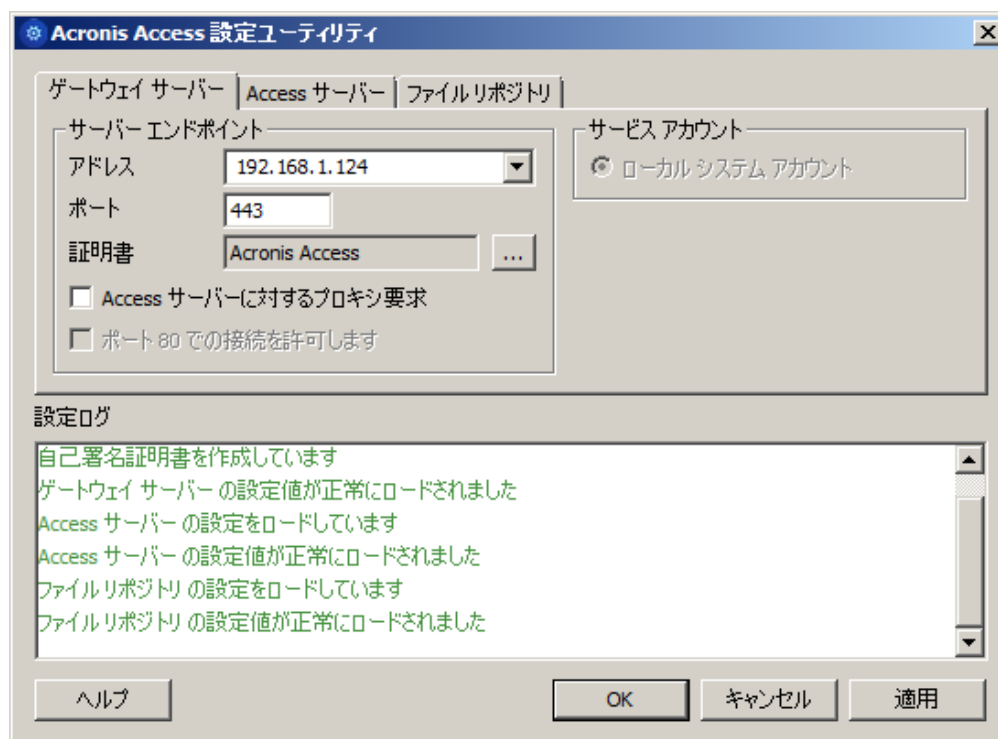
14. 必要なすべてのソフトウェアはアップグレード処理のこの時点ですべてインストール済みですが、次に、使用するネットワーク インターフェイス、ポート、および証明書を設定する必要があります。このステップは必須です。インストーラを終了すると、Acronis Access 設定ユーティリティを実行するよう促すプロンプトが表示されます。続行するには、**[OK]** をクリックしてください。



## 設定ユーティリティの使用

### [ゲートウェイ サーバー] タブでの作業

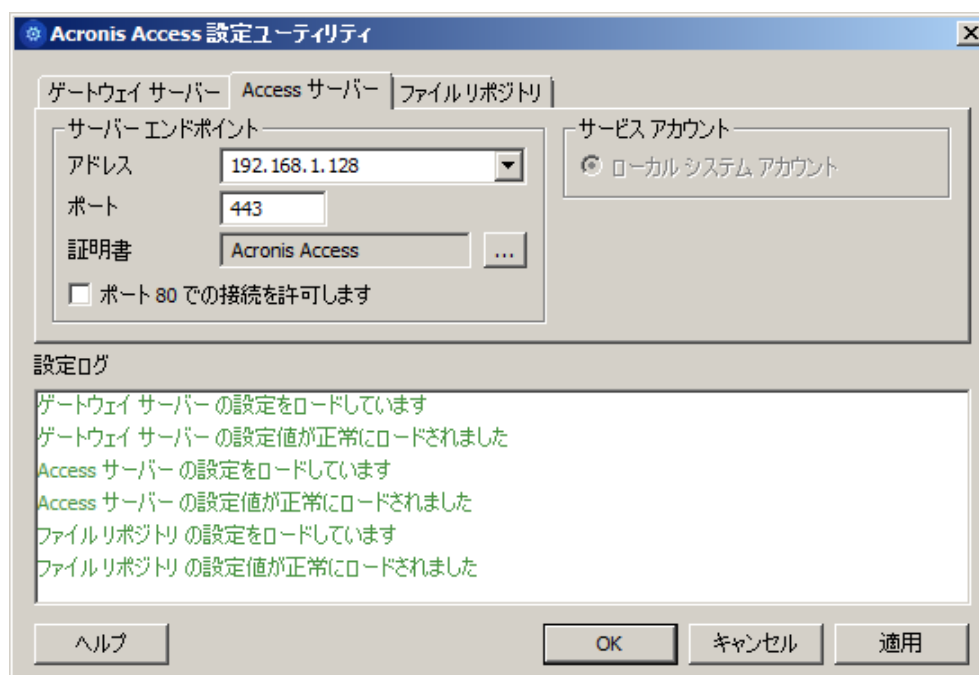
1. **[アドレス]** フィールドに、mobilEcho が稼働していたサーバーの IP アドレスを入力します。これは最初書き出したアドレスです。
2. **[ポート]** フィールドに、mobilEcho ファイル サーバーが使用していたポート番号を入力します。
3. mobilEcho ファイル サーバー用に使用していた証明書を追加します。



### [Access サーバー] での作業

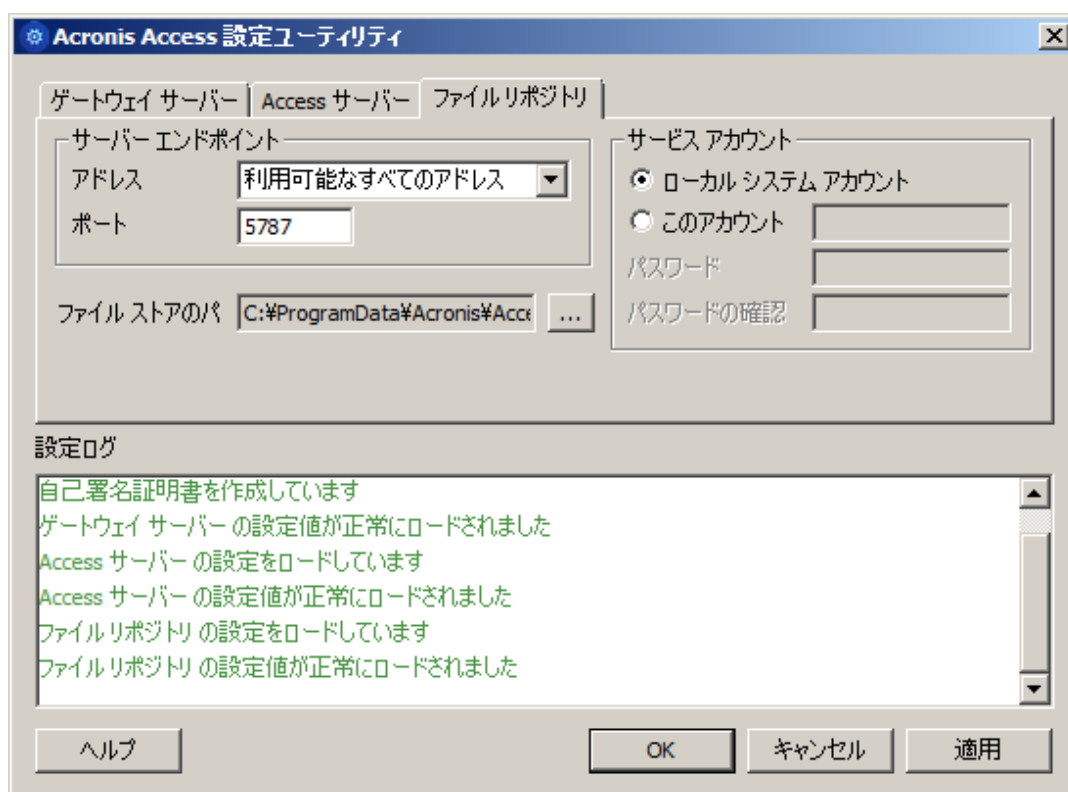
1. **[アドレス]** フィールドに、今まで activEcho サーバーで使用していた IP アドレスを入力します。これはデフォルトになっているはずです。
2. **[ポート]** フィールドに、今まで activEcho サーバーで使用していたポート番号を入力します。これはデフォルトになっているはずです。

3. activEcho サーバー用に使用していた証明書を追加します。



#### [ファイル リポジトリ] タブでの作業

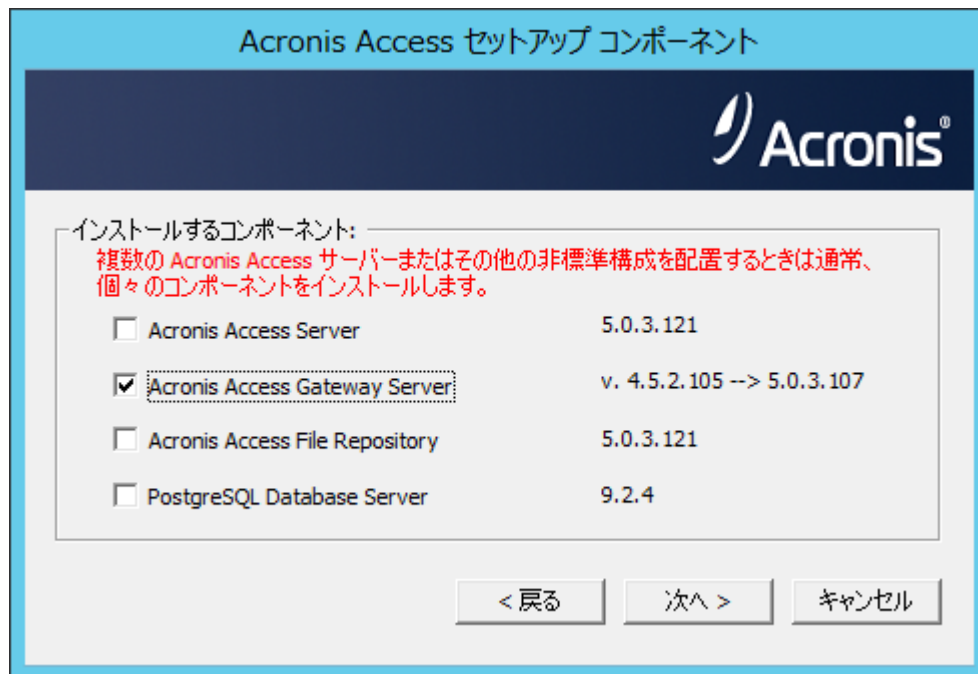
1. **[アドレス]** フィールドに、リポジトリ サービスの IP アドレスまたは FQDN を入力します。これはデフォルトになっているはずです。
2. **[ポート]** フィールドに、リポジトリ サービスのポート番号を入力します。これはデフォルトになっているはずです。
3. FileStore フォルダへのパスを選択します。これはデフォルトになっているはずです。



必要な設定をすべて終えたら、[OK] をクリックして設定ユーティリティを終了します。

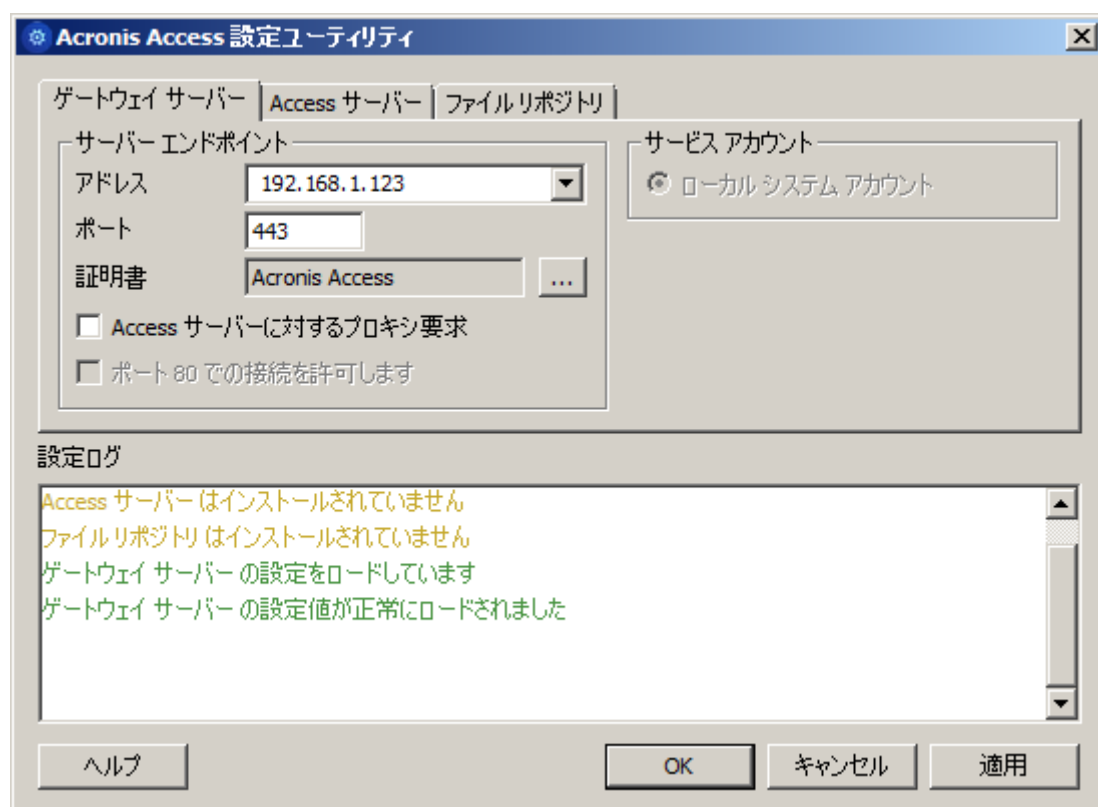
## ローカル ゲートウェイ サーバーの設定

1. Acronis Access インストーラをコピーして、mobilEcho を使用しているサーバー上に置きます。
2. mobilEcho Management Server サービスを停止します。
3. インストーラを実行し、ようこそ画面で **[次へ]** をクリックします。
4. ライセンス契約を読み、承諾します。
5. **[カスタム]** をクリックします。
6. **[ゲートウェイ サーバー]** コンポーネントのみを選択して、**[次へ]** をクリックします。

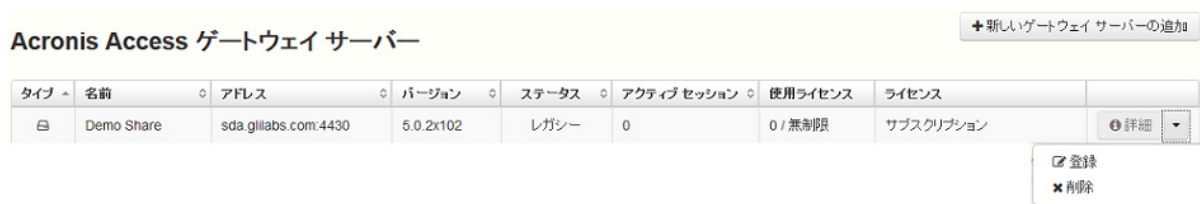


7. インストール パスを確認してから **[次へ]** をクリックします。これはデフォルトになっているはずです。
8. インストールするコンポーネントを確認して、**[インストール]** をクリックします。
9. インストールが完了したら、インストーラを終了して設定ユーティリティを起動します（自動的に起動しない場合、通常は **C:\Program Files (x86)\Group Logic\Configuration Utility** にあります）。
10. **[アドレス]** フィールドで、mobilEcho をホストしているマシンに割り当てた新しい IP アドレスを指定します。

11. **[ポート]** フィールドで、以前 mobilEcho ファイル サーバーが使用していたポート番号を指定します(これはデフォルトになっているはずです)。



12. **[OK]** をクリックすると、設定が完了します。ユーティリティを終了します。
13. Acronis Access ウェブ インターフェイスを開いてログインします。
14. **[モバイル アクセス]** タブを展開して、**[ゲートウェイ サーバー]** ページを開きます。
15. ステータスが **[レガシー]** になっているゲートウェイ サーバーを見つけて、そのゲートウェイのド롭ダウン メニューを開いて、**[登録]** を選択します。



16. ダイアログが表示されたら、[はい] を押します。



17. [管理とクライアント接続のアドレス] フィールドに、アップグレードした Gateway Server の IP アドレスを入力します。これは、以前 mobilEcho をホストしていたマシンに割り当てた新しい IP アドレスです。

**サーバー 'AWR' の登録**

名前:

管理とクライアント接続のアドレス:

☐ クライアント接続に代替アドレスを使用

管理キー:  
 ⓘ

☒ 自己署名証明書を使用した Acronis Access サーバーからの接続を許可

18. [管理キー] フィールドに、ゲートウェイ サーバーのキーを入力します。キーを取得するには、ブラウザでゲートウェイの IP アドレスを開きます（例: https://192.168.1.1）。この操作は、以前 mobilEcho をインストールしていたマシンで行う必要があります。
19. [保存] をクリックしてゲートウェイを登録します。

## ローカル ゲートウェイ サーバーの登録

[ゲートウェイ サーバー] ページで次の操作を行います。

1. [ゲートウェイ サーバーの追加] ボタンを押します。



2. 新しいゲートウェイ サーバーの表示名を入力します。
3. ゲートウェイの IP アドレスを入力します。これは、以前 mobilEcho サーバーで使用されていた IP アドレス(最初に書き出した IP)です。
4. ゲートウェイの管理キーを入力します。キーを取得するには、ブラウザでゲートウェイの IP アドレスを開きます(例: <https://192.168.1.1>)。この操作は、現在 Acronis Access Server をホストしているマシンで行う必要があります。

## 新しいゲートウェイ サーバーの追加

×

表示名:

管理のアドレス: ⓘ

☐ クライアント接続に代替アドレスを使用 ⓘ

管理キー: ⓘ

☒ 自己署名証明書を使用した Acronis Access サーバーからの接続を許可 ⓘ

保存

キャンセル

5. **[保存]** をクリックしてゲートウェイを登録します。

## 3.5 クラスタ構成のアップグレード

Acronis Access のクラスタ構成をアップグレードするには、Acronis Access サーバーとクラスタグループのゲートウェイ サーバーの両方をアップグレードする必要があります。Access サーバーのアップグレードの方法については、「Acronis Access の新しいバージョンへのアップグレード『65ページ』」の記事を参照してください。各ゲートウェイでは、次の手順を実行してください。

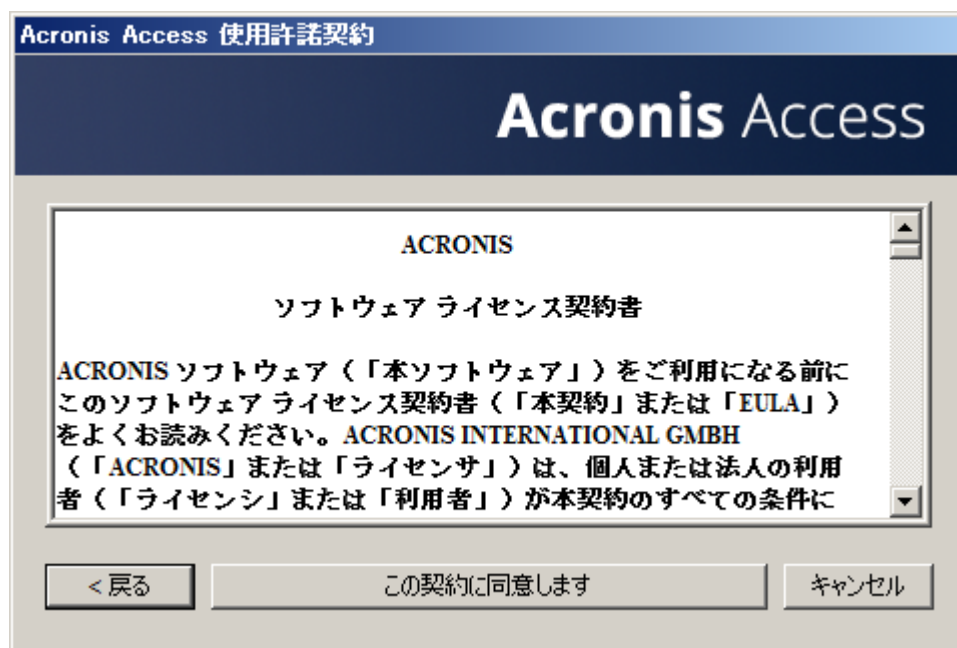
Microsoft Failover Clustering 構成のアップグレードの詳細については、「補足資料」セクションを参照してください。

## ゲートウェイ サーバーのアップグレード

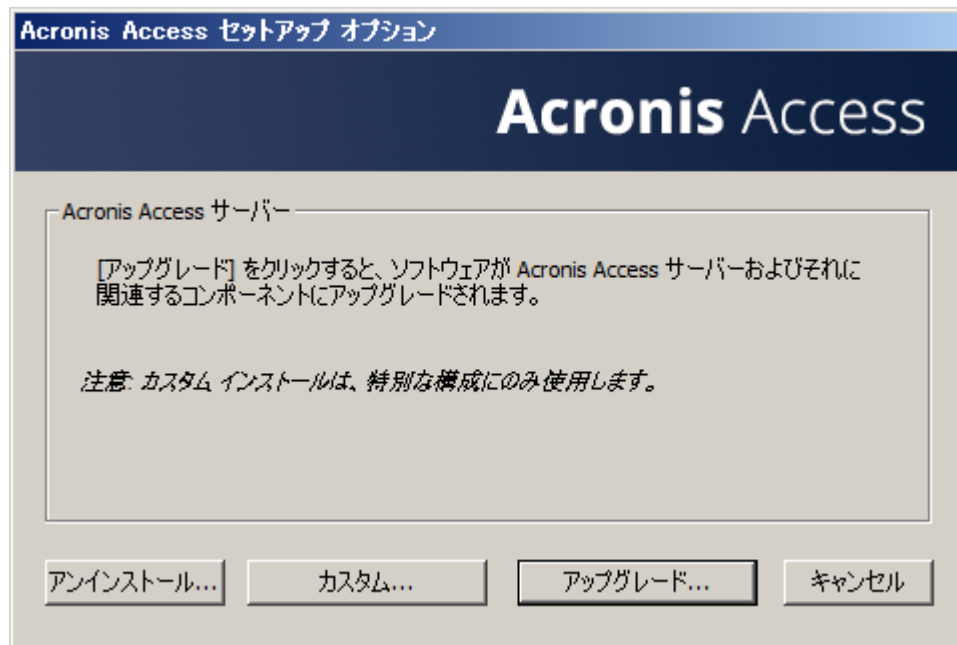
1. 対象のサーバーで Acronis Access インストーラを実行します。
2. [ようこそ] 画面で [次へ] をクリックします。



3. 使用許諾契約を読み、承諾します。



4. [カスタム] をクリックします。



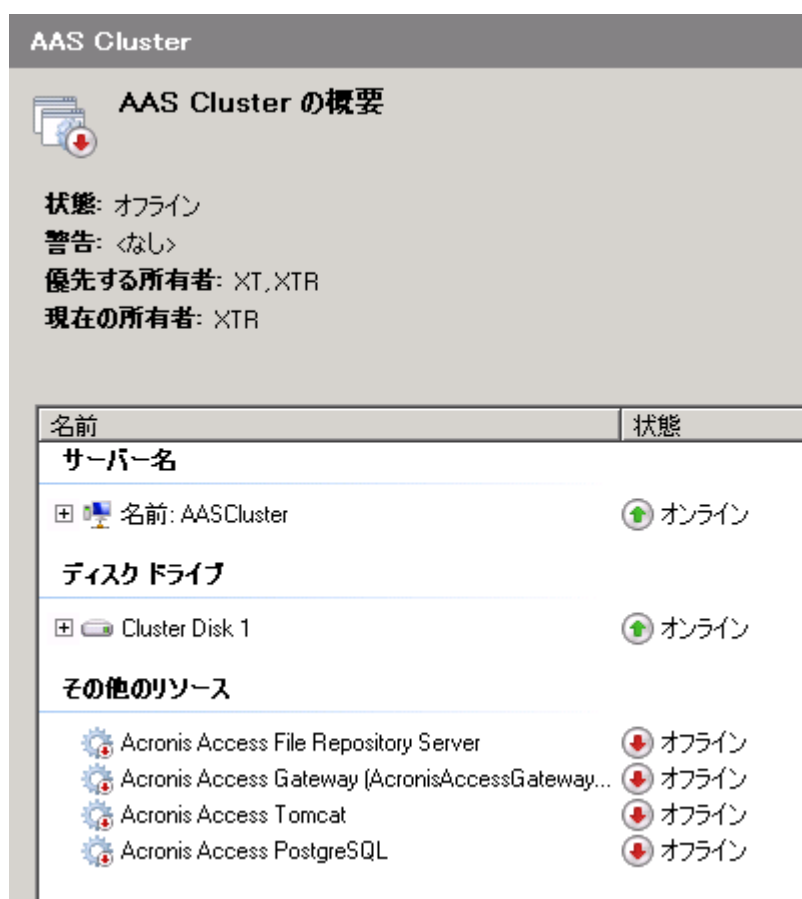
5. **[Acronis Access ゲートウェイ サーバー]** コンポーネントのみを選択して、**[次へ]** をクリックします。
6. コンポーネントを確認し、**[インストール]** を押します。
7. インストールの完了後、概要を確認してからインストーラを閉じます。設定ユーティリティを開くように求められたら、設定ユーティリティを開き、ゲートウェイ サーバーの以前の設定がすべて保持されていることを確認します。必要に応じて変更を加え、**[OK]** を押します。

## 4 Microsoft フェールオーバー クラスタ上での Acronis Access のアップグレード

Acronis Access Server クラスタを Acronis Access のさらに新しいバージョンにアップグレードするには、次のステップが役立ちます。

1. アクティブ ノードに移動します。
2. **[Cluster Administrator]/[フェイルオーバー クラスタ管理]** を開きます。

3. Acronis Access のサービスをすべて停止します(**postgres-some-version** も含む)。共有ディスクがオンラインでなければなりません。

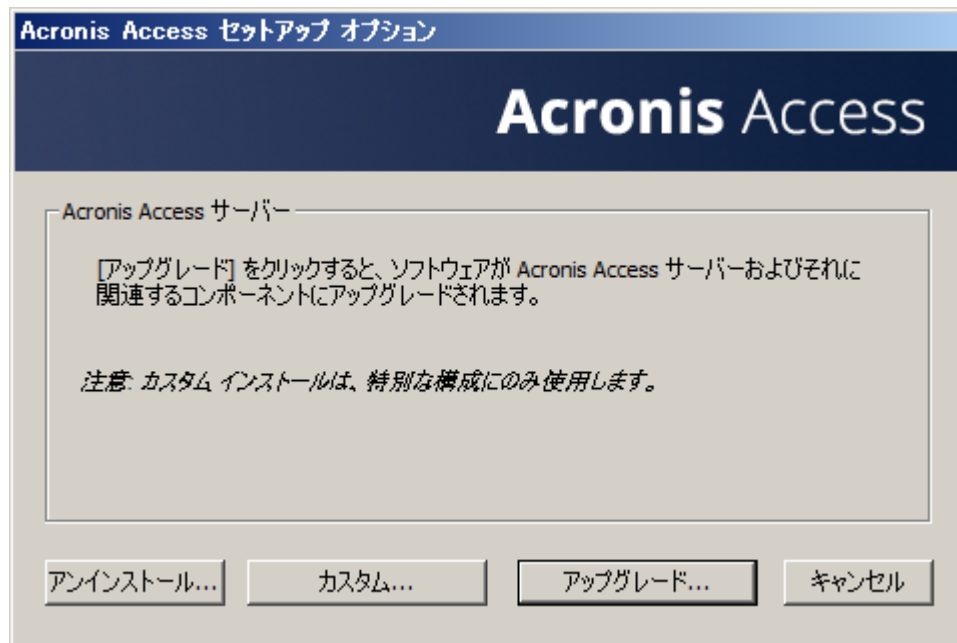


4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. 実行可能なインストーラをダブルクリックします。

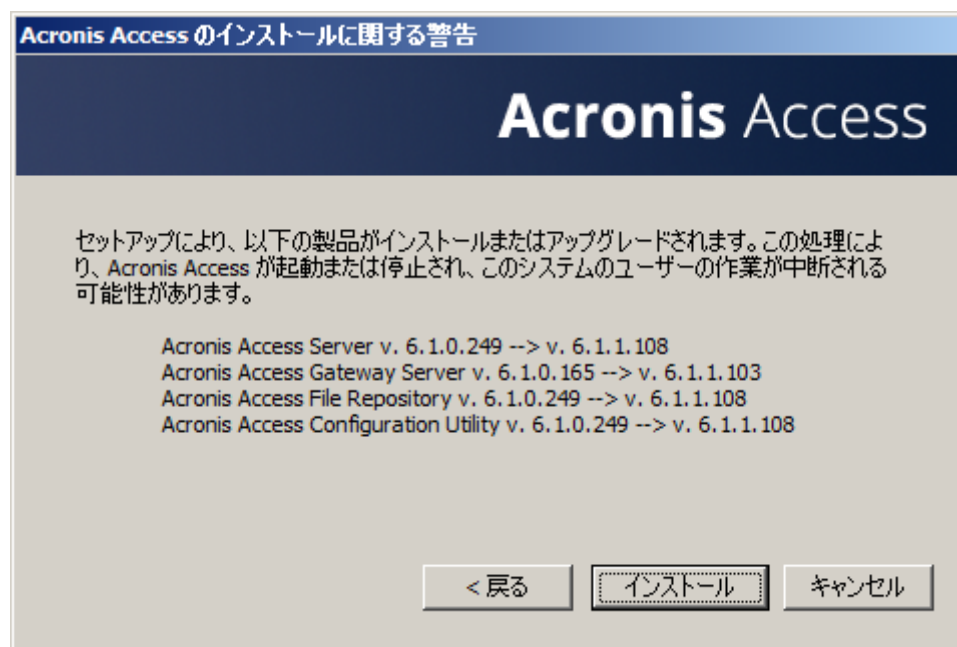


6. [次へ] を押して開始します。

7. 使用許諾契約を読み、承諾します。
8. **[アップグレード]** を押します。



9. インストールするコンポーネントを確認して、**[インストール]** をクリックします。



10. **postgres** スーパー ユーザーのパスワードを入力して、**[次へ]** を押します。
11. インストールが終了したら、**[終了]** を押してインストーラを閉じます。

**警告:** クラスタ グループをオンラインにしないでください。

12. クラスタ グループを第 2 のノードに移動します。
13. 第 2 のノード上で、同じインストール手順を実行します。
14. Acronis Access のサービスをすべてオンラインにします。

## 5 Microsoft フェールオーバー クラスタでの mobilEcho 4.5 からのアップグレード

**警告:** Acronis Access フェールオーバー クラスタリングは、5.0.3 より前のバージョンではサポートされていません。それより前のバージョンを使用している場合、何らかのクラスタの設定を続行する前に、5.0.3 以降のバージョンにアップグレードする必要があります。

以下のガイド情報は、mobilEcho から Acronis Access にクラスタをアップグレードする作業についてのものです。

### セクションの内容

|   |     |
|---|-----|
| Windows 2003 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis Access にアップグレードする..... | 138 |
| Windows 2008 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis Access にアップグレードする..... | 151 |
| Windows 2012 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis Access にアップグレードする..... | 162 |

### 5.1 Windows 2003 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis Access にアップグレードする

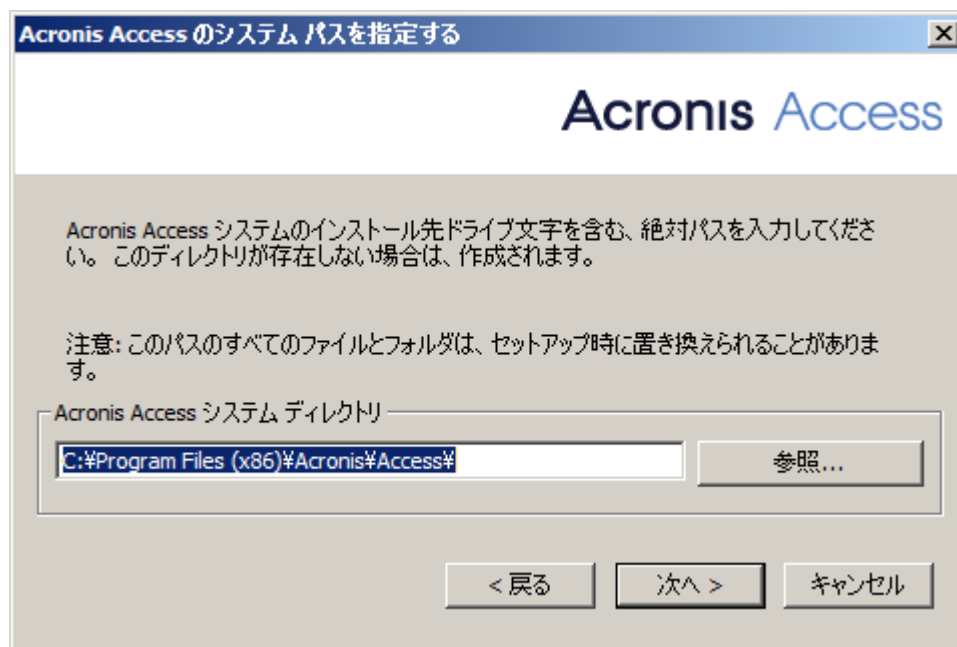
1. **[Cluster Administrator]** を開き、サービス グループをダブルクリックします。
2. mobilEcho サービスのリソースを削除します。  
**注意:** クラスタ グループ全体をオフラインにしないでください。mobilEcho サービス リソースだけを削除してください。
3. アクティブ ノードでインストーラを起動します。
4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. 実行可能なインストーラをダブルクリックします。



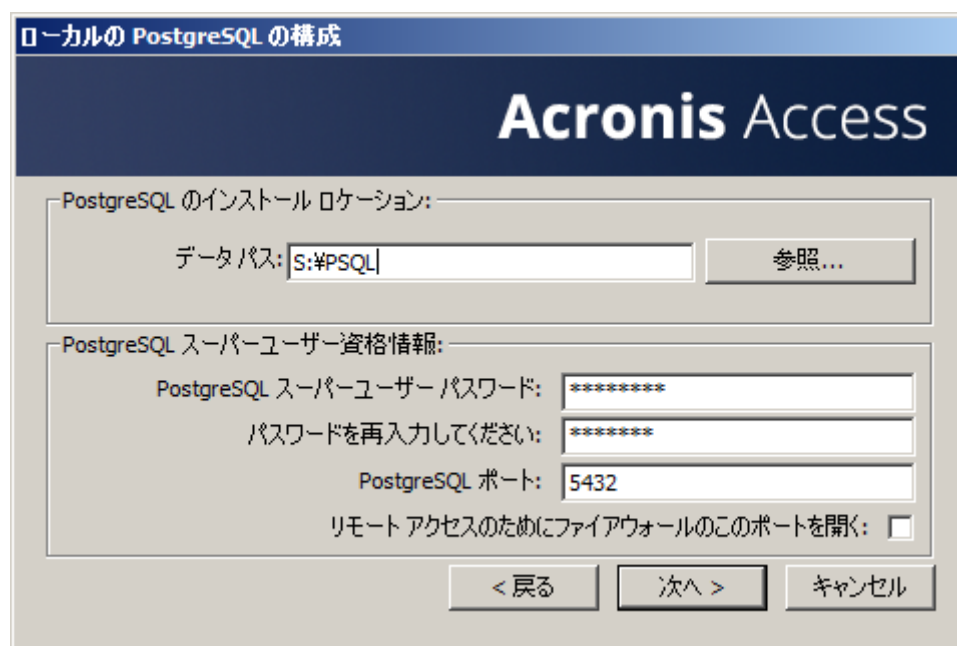
6. **[次へ]** を押して開始します。
7. 使用許諾契約を読み、承諾します。
8. **[インストール]** を押します。

**注意:** 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

9. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、**[OK]** を押します。



10. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。
11. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して**[次へ]**をクリックします。



12. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、**[OK]** を押します。
13. Acronis Access のインストーラが完了したら、**[終了]** を押します。共有ディスクに移動し、**production.sqlite3**、**mobilEcho\_manager.cfg**、**priority.txt** (これは存在しない場合があります) の 3 つのファイルを見つけてコピーしてから、それらを Acronis Access インストールディレクトリに貼り付けて既存のファイルを置き換えます。

---

**注意:** 置き換える元のファイルは、一般に次の場所にあるはずです。

**C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db\production.sqlite3**

**C:\Program Files (x86)\Group Logic\mobilEcho  
Server\ManagementUI\mobilEcho\_manager.cfg**

**C:\Program Files (x86)\Group Logic\mobilEcho Server\Management\priority.txt**

---

## アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\Group Logic\mobilEcho Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます (**database\_path: 'S:/mobilEcho\_cluster/database/'** など)。

---

**注意:** パスの区切りにはスラッシュ (/) を使用します。

**注意:** 第 1 ノードで設定した **database.yml** をコピーして、第 2 ノードに貼り付けることができます。

---

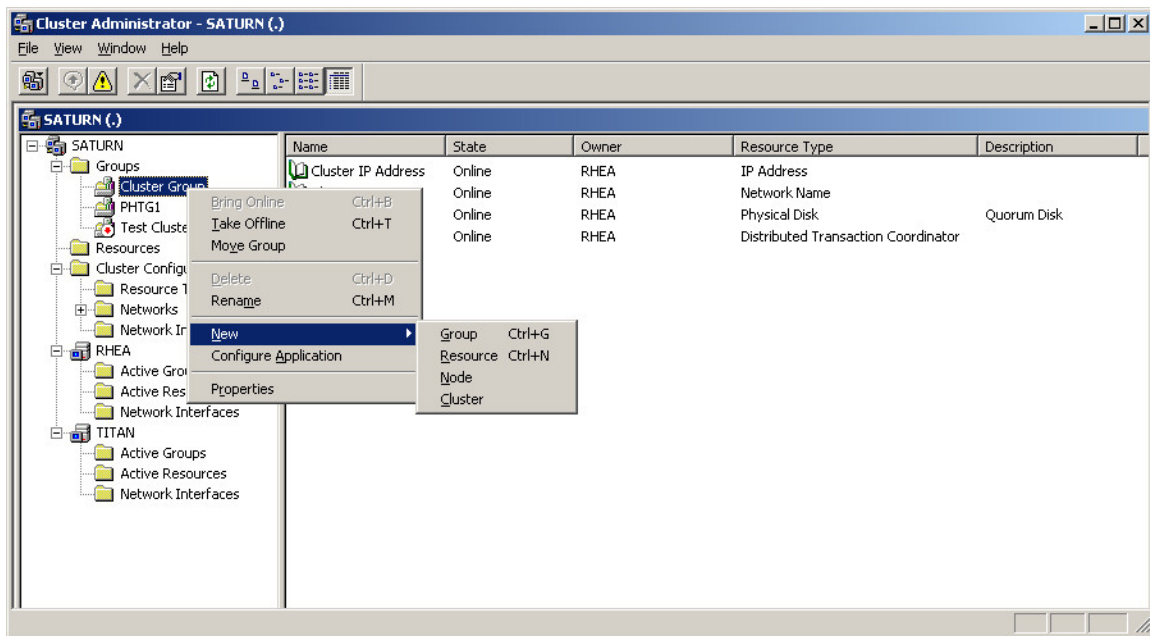
## 必要なすべてのサービスを Acronis Access クラスタ グループに追加する

AcronisAccessGateway、AcronisAccessPostgreSQL (Acronis Access のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

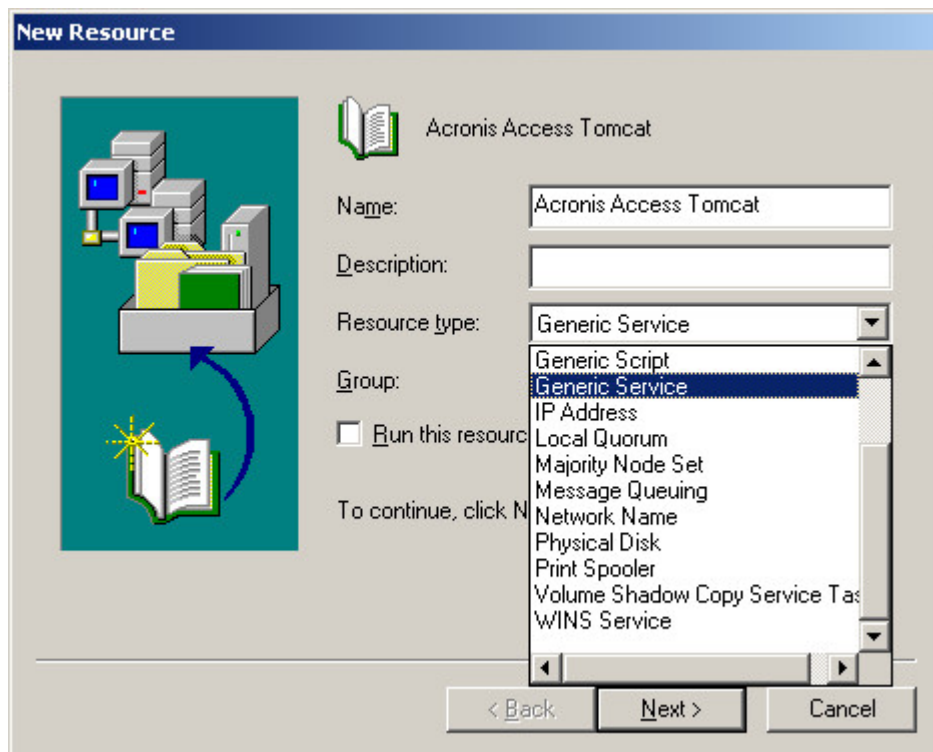
1. Acronis Access クラスタ グループを右クリックします。



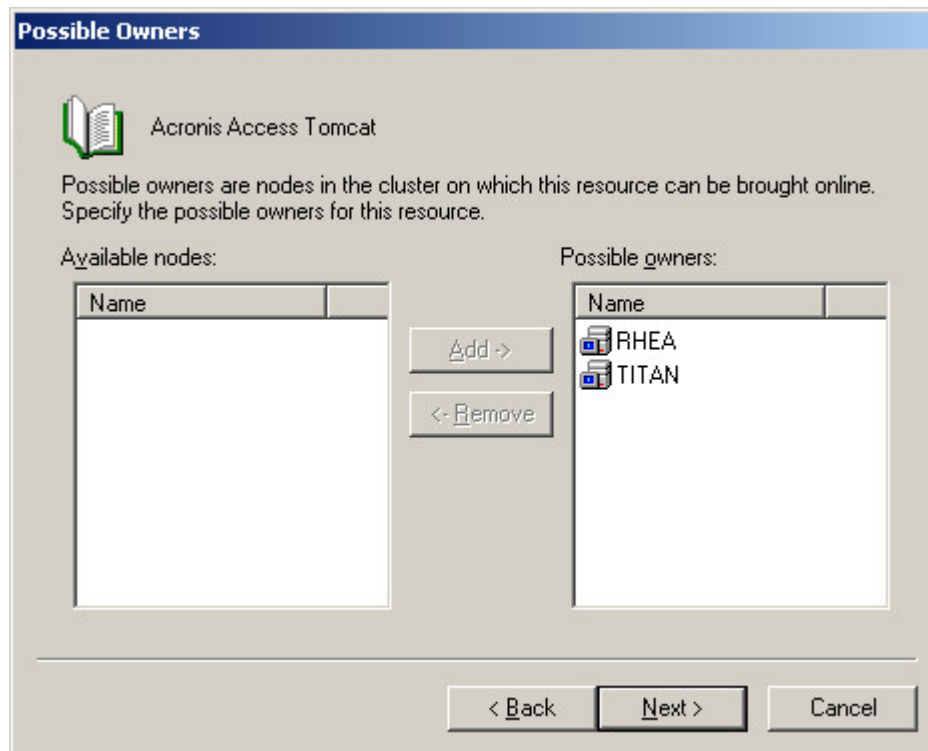
2. [新規] を開いて [リソース] を選択します。



3. サービスの名前を入力し、適切なクラスターグループを選択します。
4. [リソースの種類] ドロップダウンメニューから [汎用サービス] を選択して [次へ] をクリックします。



5. 2 つのノードがいずれも **[使用可能な所有者]** のリストに含まれていることを確認してから **[次へ]** をクリックします。



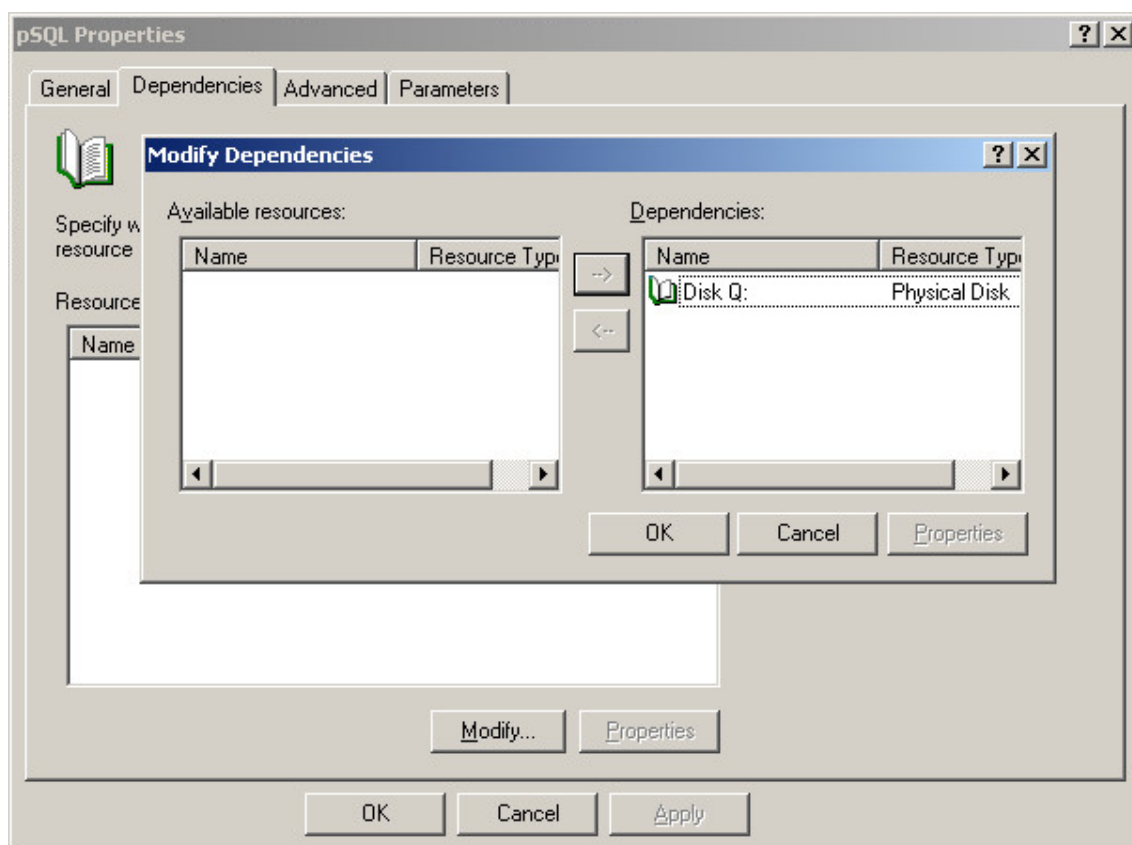
6. **[次へ]** をクリックして依存関係をスキップします。
7. 追加するサービスの正確なサービス名 (postgresql-x64-9.2 など) を入力して **[次へ]** をクリックします。
8. ここでは **[次へ]** を押して **[レジストリ レプリケーション]** ウィンドウをスキップします。
9. **[完了]** をクリックします。これで手順は完了です。

## 依存関係の設定

**PostgreSQL および Acronis Access ファイル リポジトリでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、**[プロパティ]** を選択します。
2. **[依存関係]** タブをクリックします。
3. **[変更]** をクリックします。

4. 追加した共有ディスクを選択し、右側に移動します。

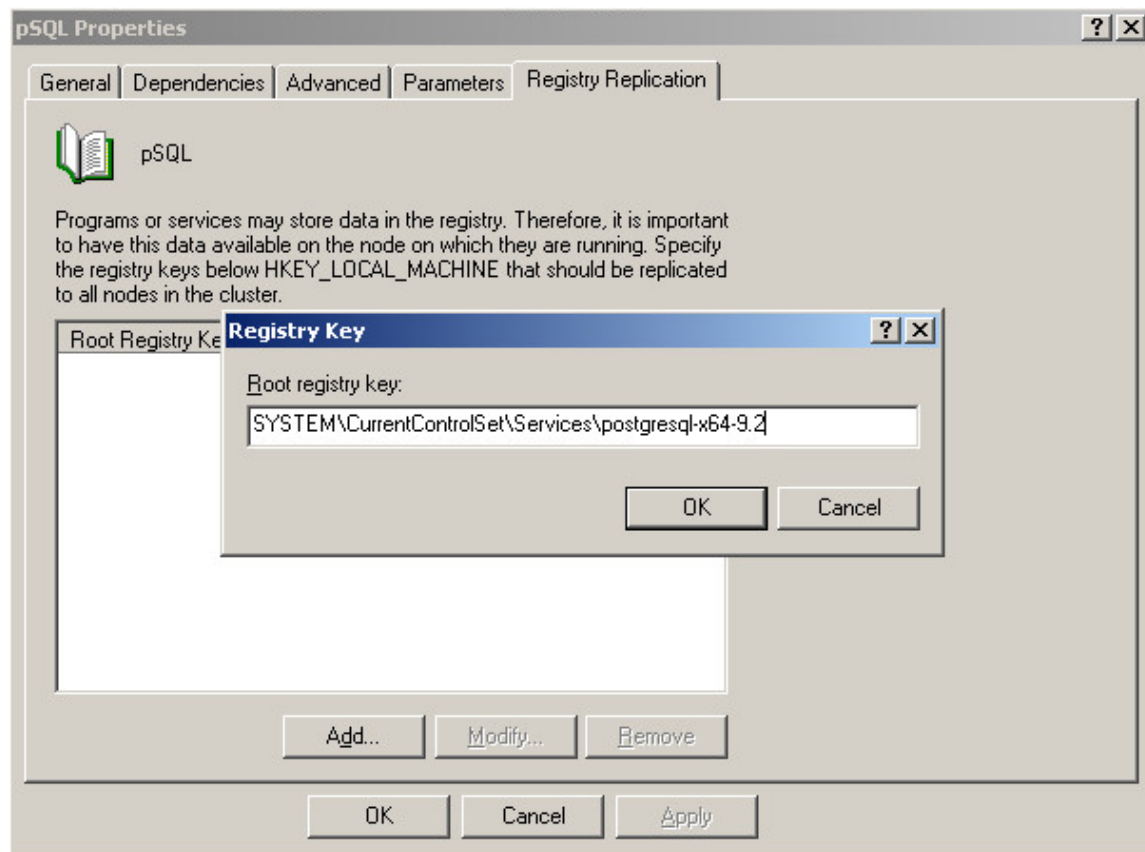


5. [OK] を押します。

**PostgreSQL** では、次の操作も実行します。

1. [レジストリ レプリケーション] タブをクリックします。

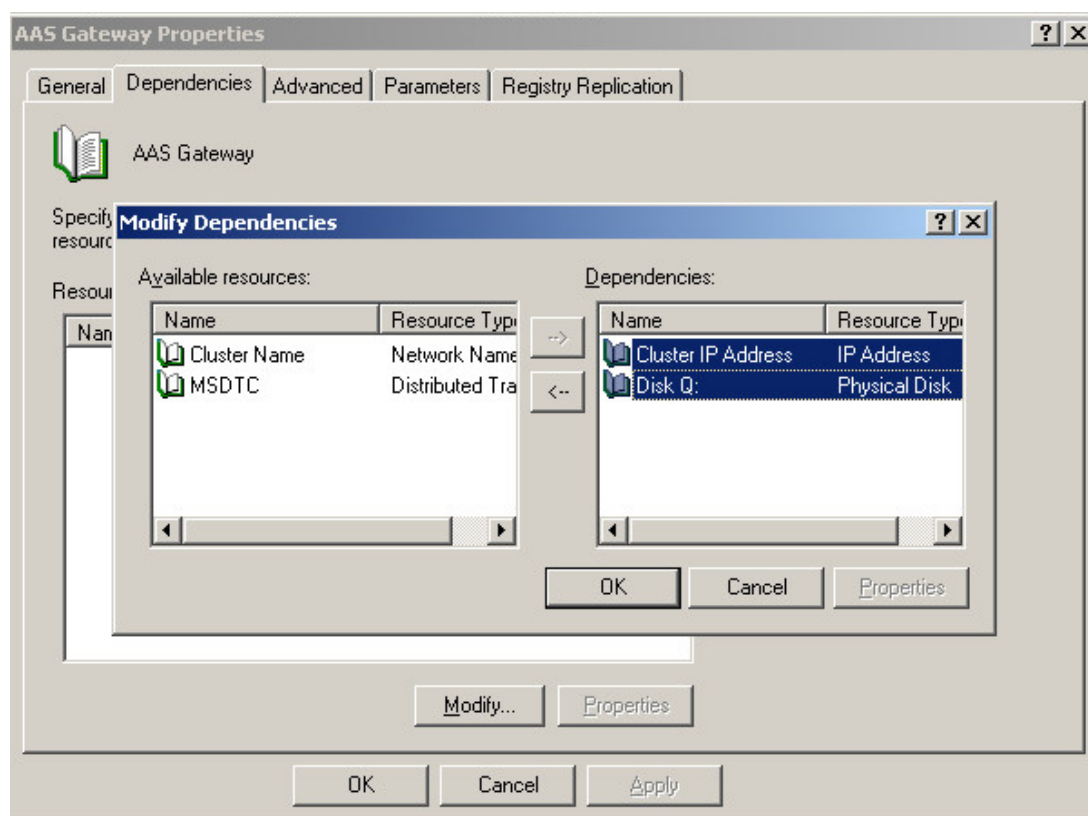
2. **[追加]** を押し、**SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\** のように入力します (旧バージョンの Acronis Access の場合、サービスが **postgresql-x64-9.2** のように異なることがあります)。



**Acronis Access ゲートウェイ サーバー サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、**[プロパティ]** を選択します。
2. **[依存関係]** タブをクリックします。
3. **[変更]** をクリックします。

4. IP アドレスと物理ディスクを選択し、右側に移動します。

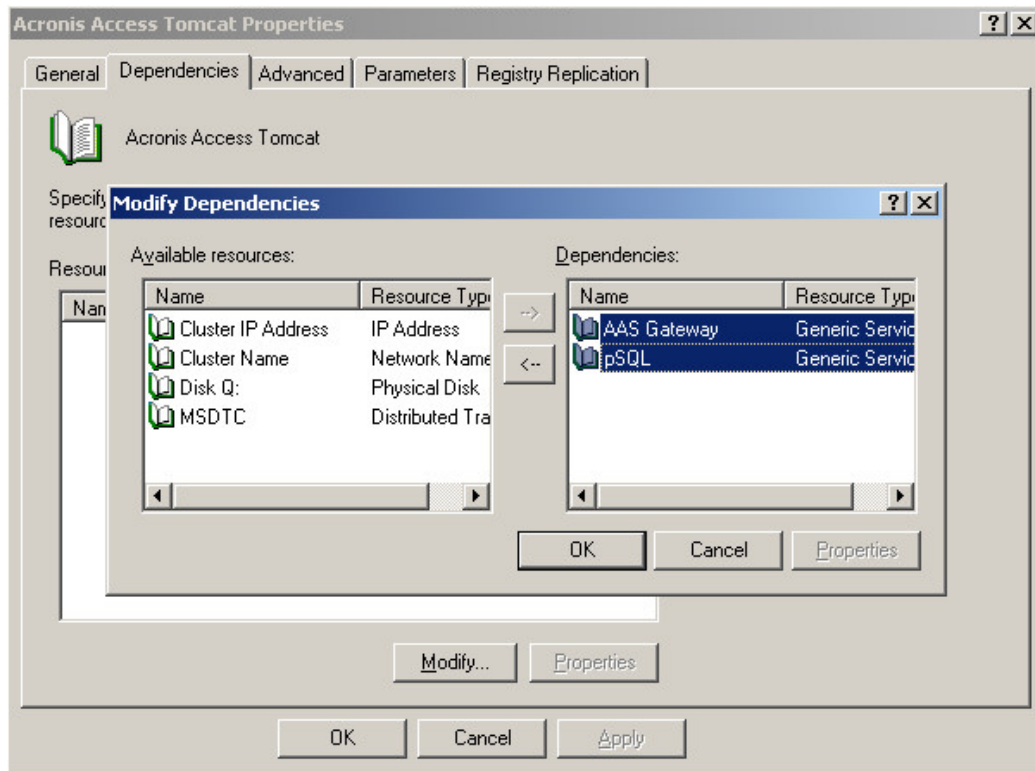


5. [OK] を押します。

**Acronis Access Tomcat サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。
3. [変更] をクリックします。

4. PostgreSQL および Acronis Access ゲートウェイ サーバーのサービスを選択し、右側に移動します。

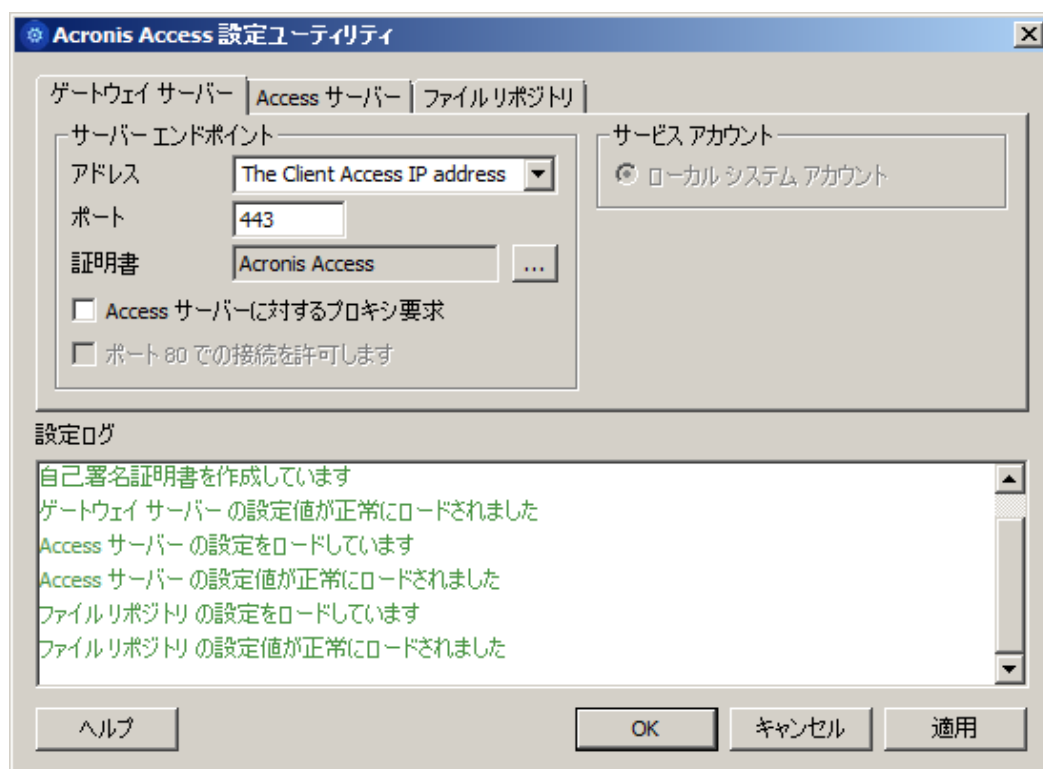


5. [OK] を押します。

### クラスタ グループをオンラインにして設定ユーティリティを使用する

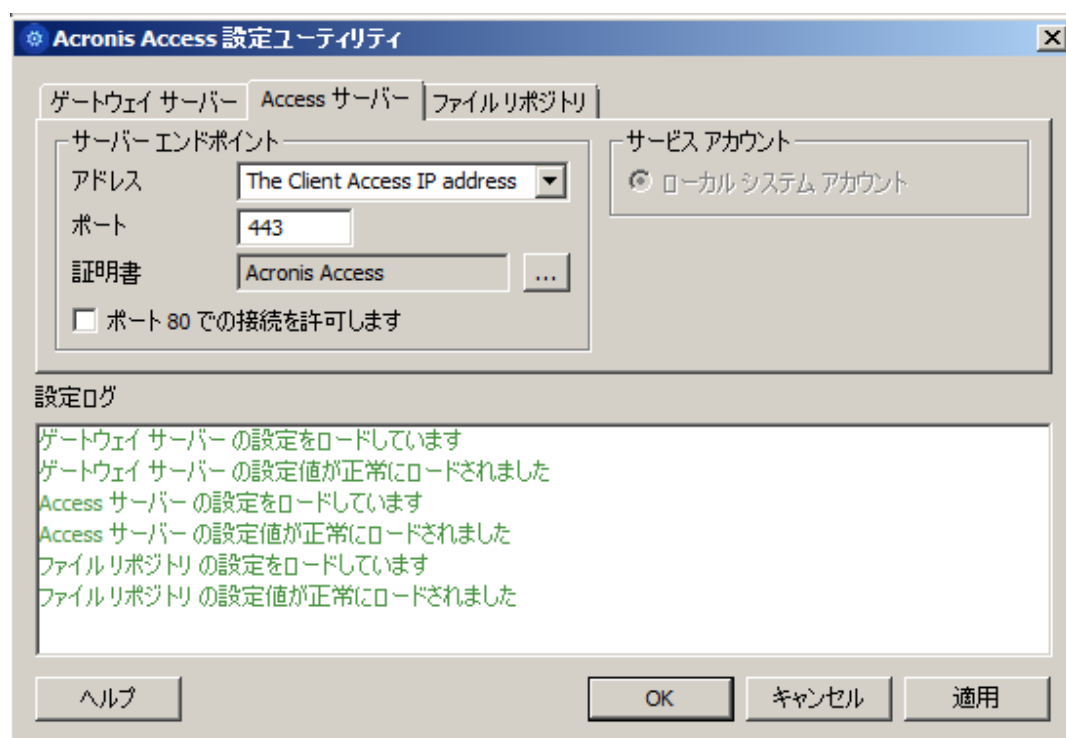
1. クラスタ グループを右クリックし、[Bring online] をクリックします。
2. 設定ユーティリティを起動します。mobilEcho からのアップグレードの場合、通常これは **C:\Program Files (x86)\GroupLogic\Configuration Utility** にあります。

3. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

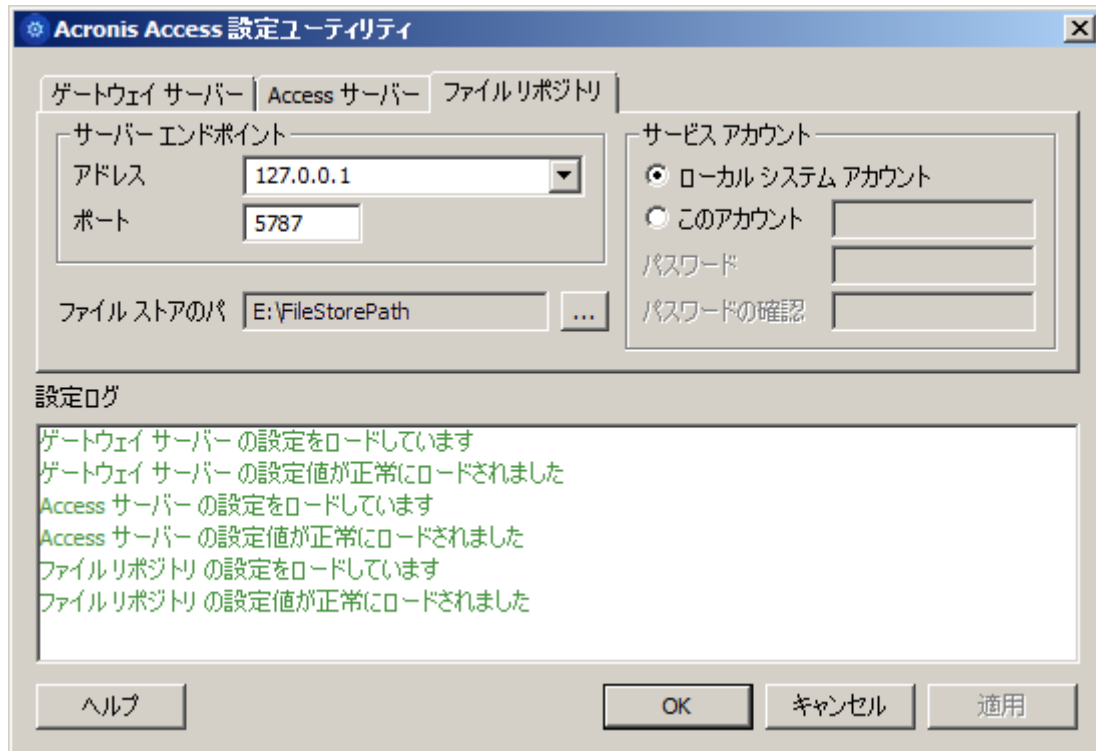


4. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



5. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



6. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Acronis Access をインストールします。ただし、今回は、デフォルトの **Postgres データ ロケーション**、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。
4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。

- a. **C:\Program Files (x86)\GroupLogic\mobilEcho Server\** に移動します。
- b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
- c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます (**database\_path: 'S:/mobilEcho\_cluster/database/'** など)。

**注意:** パスの区切りにはスラッシュ (/) を使用します。

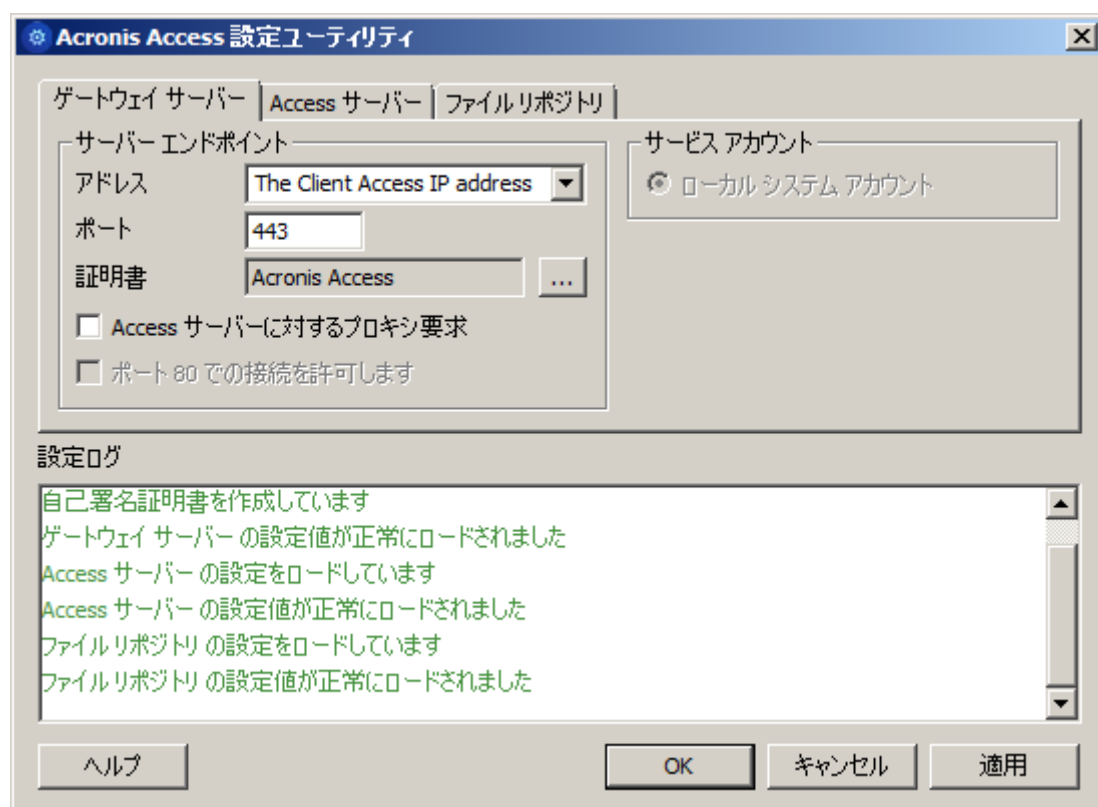
**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

**注意:** このパスは第 1 ノードで設定されているパスと同じでなければなりません。

5. クラスタ グループを第 2 ノードに移動します。そのためには、クラスタ グループを右クリックして **[Move Group]** をクリックします。
6. 設定ユーティリティを起動します。mobilEcho からのアップグレードの場合、通常これは **C:\Program Files (x86)\GroupLogic\Configuration Utility** にあります。

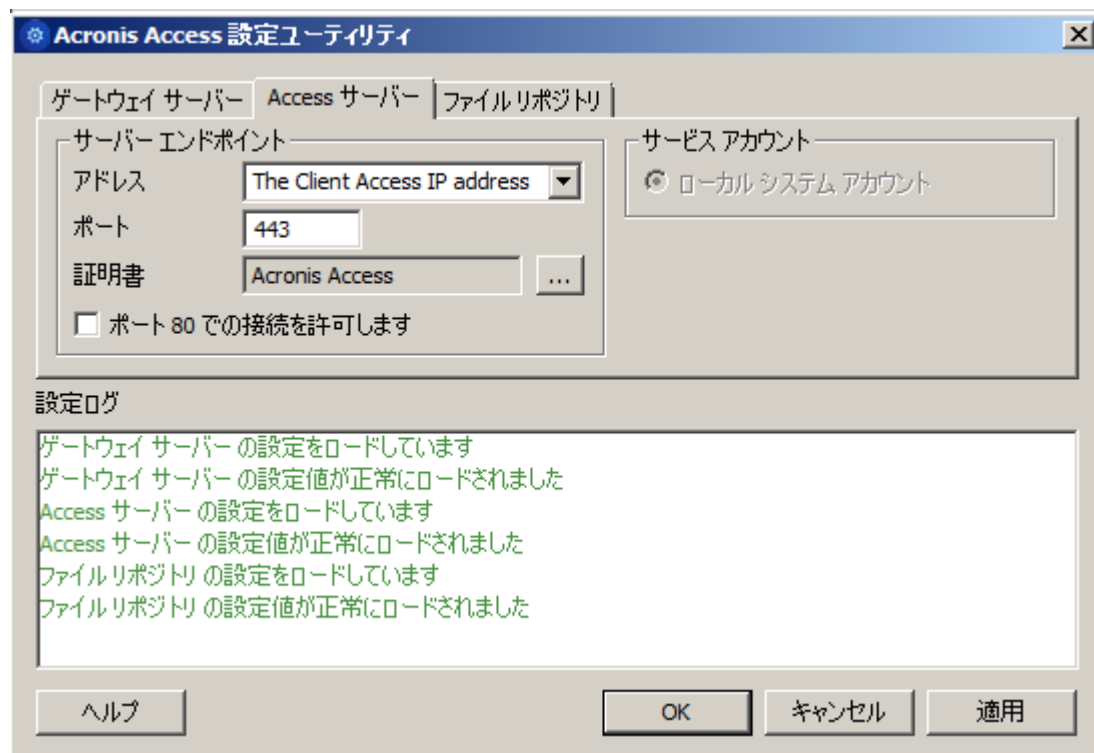


7. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリッスンするように設定します。

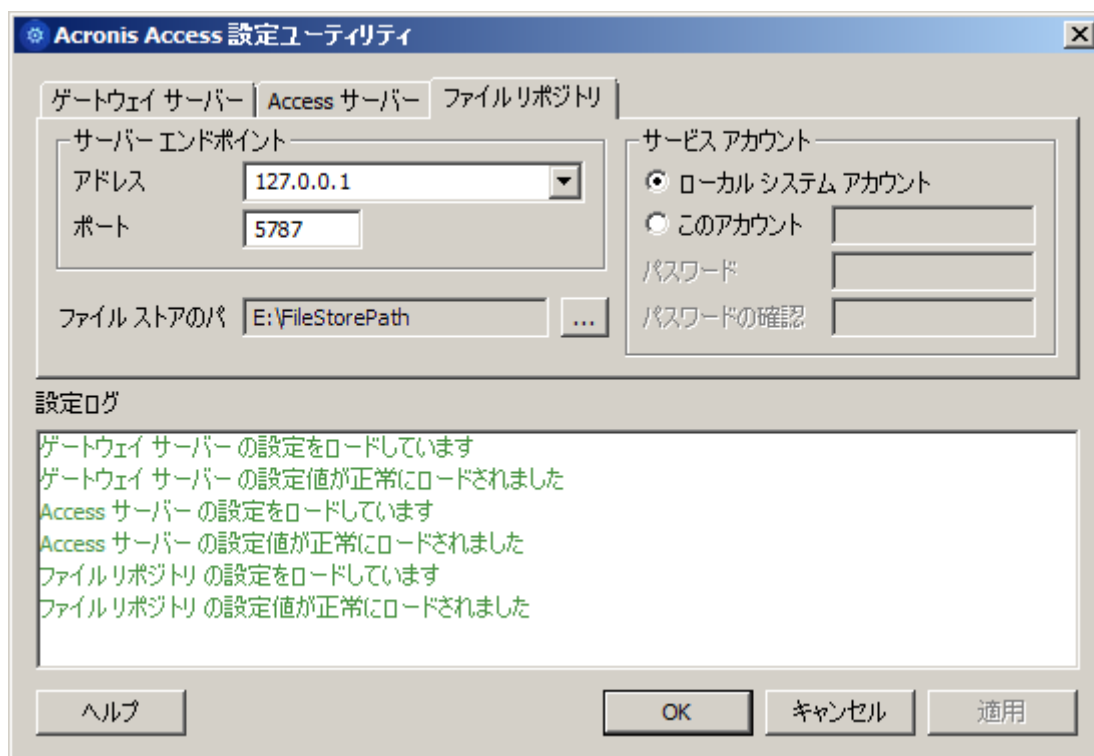


8. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリッスンするように設定します。

注意: [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリッスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリッスンする別のプログラムがある場合は、このボックスをオンにしないでください。



9. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



10. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 5.2 Windows 2008 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis Access にアップグレードする

1. [フェールオーバー クラスタ マネージャ] を開き、サービス グループをダブルクリックします。
2. mobilEcho サービスのリソースを削除します。

**注意:** クラスタ グループ全体をオフラインにしないでください。mobilEcho サービス リソースだけを削除してください。

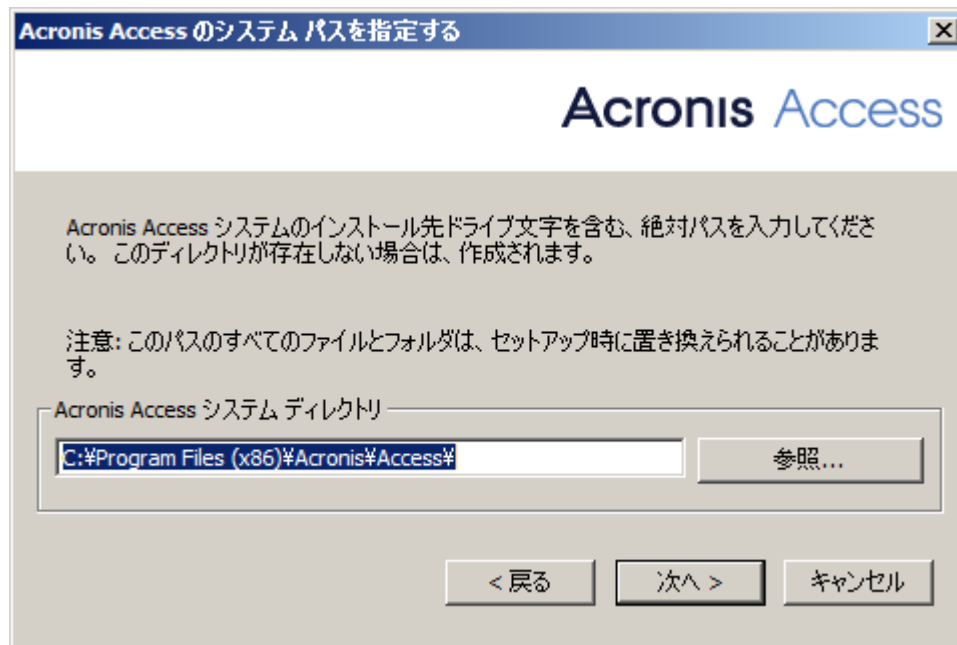
3. アクティブ ノードでインストーラを起動します。
4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. 実行可能なインストーラをダブルクリックします。



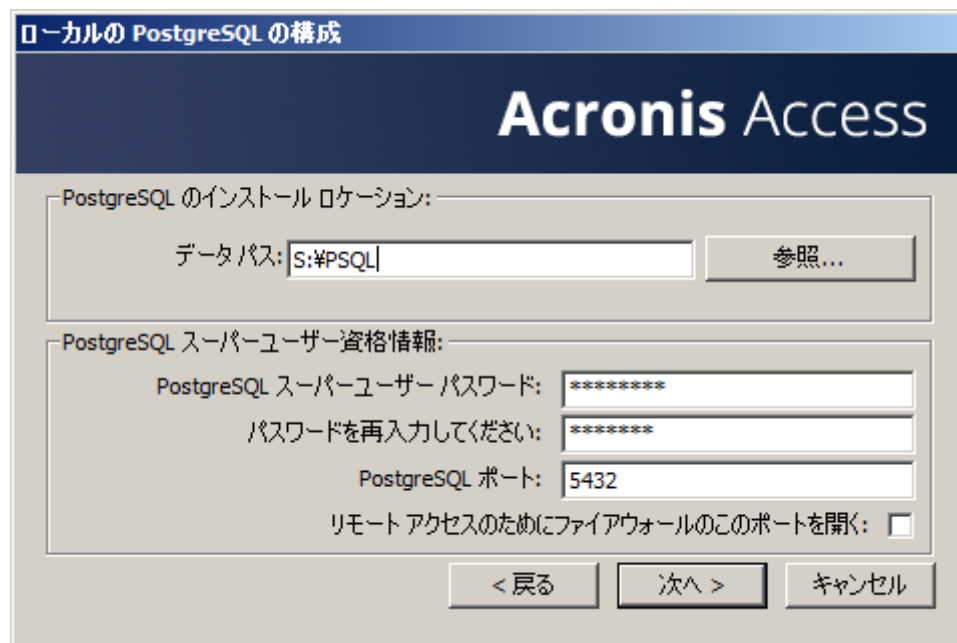
6. [次へ] を押して開始します。
7. 使用許諾契約を読み、承諾します。
8. [インストール] を押します。

**注意:** 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、[カスタム インストール] ボタンからインストールするコンポーネントを選択することができます。

9. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、[OK] を押します。



10. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。
11. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して [次へ] をクリックします。



12. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、[OK] を押します。
13. Acronis Access のインストーラが完了したら、[終了] を押します。共有ディスクに移動し、**production.sqlite3**、**mobilEcho\_manager.cfg**、**priority.txt** (これは存在しない場合があります) の 3 つのファイルを見つけてコピーしてから、それらを Acronis Access インストールディレクトリに貼り付けて既存のファイルを置き換えます。

**注意:** 置き換える元のファイルは、一般に次の場所にあるはずです。

**C:\Program Files (x86)\Group Logic\mobilEcho Server\ManagementUI\db\production.sqlite3**

C:\Program Files (x86)\Group Logic\mobilEcho  
Server\ManagementUI\mobilEcho\_manager.cfg

C:\Program Files (x86)\Group Logic\mobilEcho Server\Management\priority.txt

## アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. C:\Program Files (x86)\GroupLogic\mobilEcho Server\ に移動します。
  - b. database.yml ファイルを見つけ、テキスト エディタで開きます。
  - c. database\_path: './database/' の行を見つけ、./database/ を、使用するパスに置き換えます(database\_path: 'S:/mobilEcho\_cluster/database/' など)。

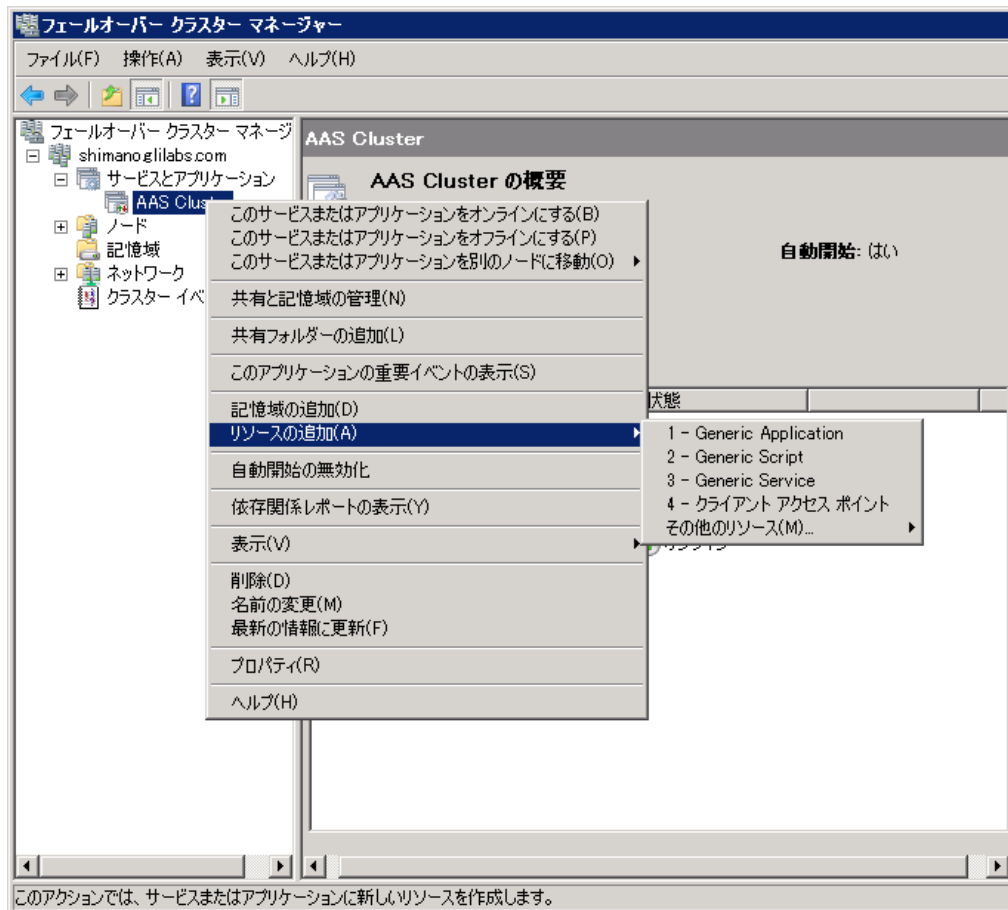
**注意:** パスの区切りにはスラッシュ(/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

## 必要なすべてのサービスを Acronis Access サービス グループに追加する

AcronisAccessGateway、AcronisAccessPostgreSQL (Acronis Access のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Acronis Access サービス グループを右クリックして、[リソースの追加] を選択します。
2. [汎用サービス] を選択します。



3. 適切なサービスを選択して [次へ] をクリックします。



4. 確認ウィンドウで [次へ] をクリックします。
5. [レジストリ設定のレプリケート] ウィンドウで [次へ] をクリックします。
6. 概要ウィンドウで [完了] をクリックします。

## 依存関係の設定

1. Acronis Access サービス グループをダブルクリックします。

**PostgreSQL および Acronis Access ファイル リポジトリ サービスについて、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックし、追加した共有ディスクを選択します。

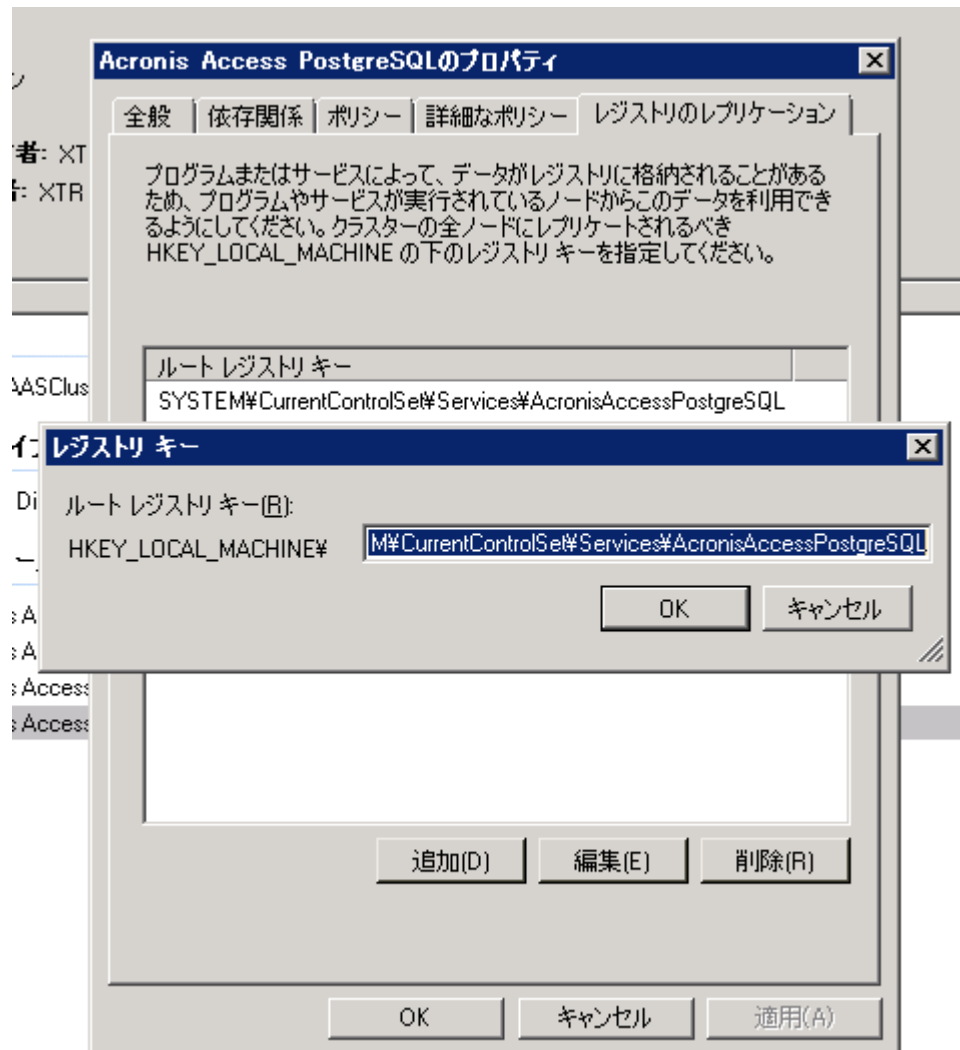


4. [適用] をクリックしてウィンドウを閉じます。

PostgreSQL では、次の操作も実行します。

1. [レジストリ レプリケーション] タブをクリックします。

2. **[追加]** を押し、**SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\** のように入力します (旧バージョンの Acronis Access の場合、サービスが **postgresql-x64-9.2** のように異なることがあります)。

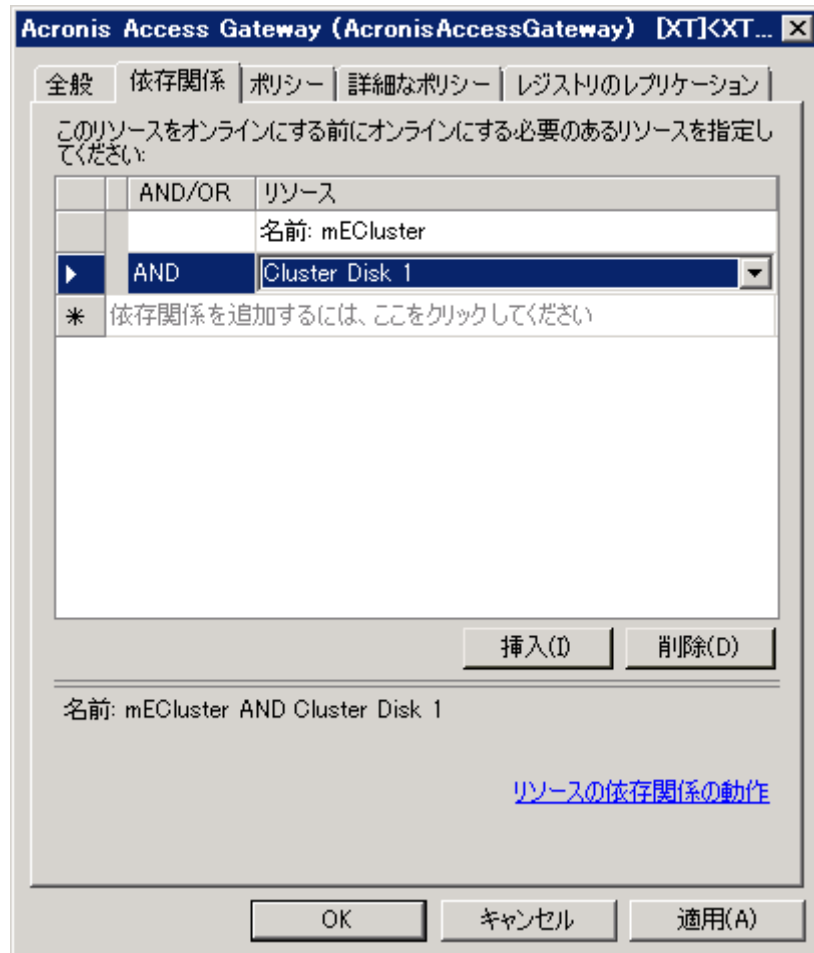


**Acronis Access ゲートウェイ サーバー サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、**[プロパティ]** を選択します。
2. **[依存関係]** タブをクリックします。



3. [リソース] をクリックしてから、追加した共有ディスク、およびネットワーク名(クライアント アクセス ポイントの名前)を選択します。

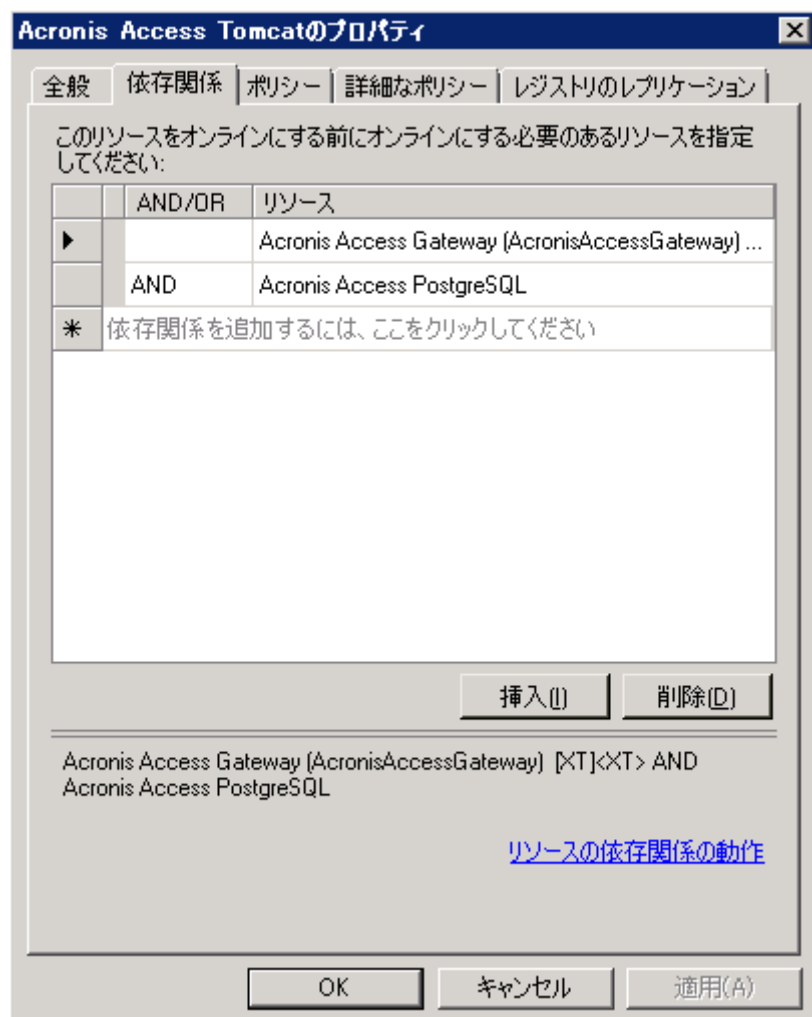


4. [適用] をクリックしてウィンドウを閉じます。

**Acronis Access Tomcat サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックし、依存関係として、PostgreSQL および Acronis Access ゲートウェイ サーバーのサービスを選択します。[適用] をクリックしてウィンドウを閉じます。

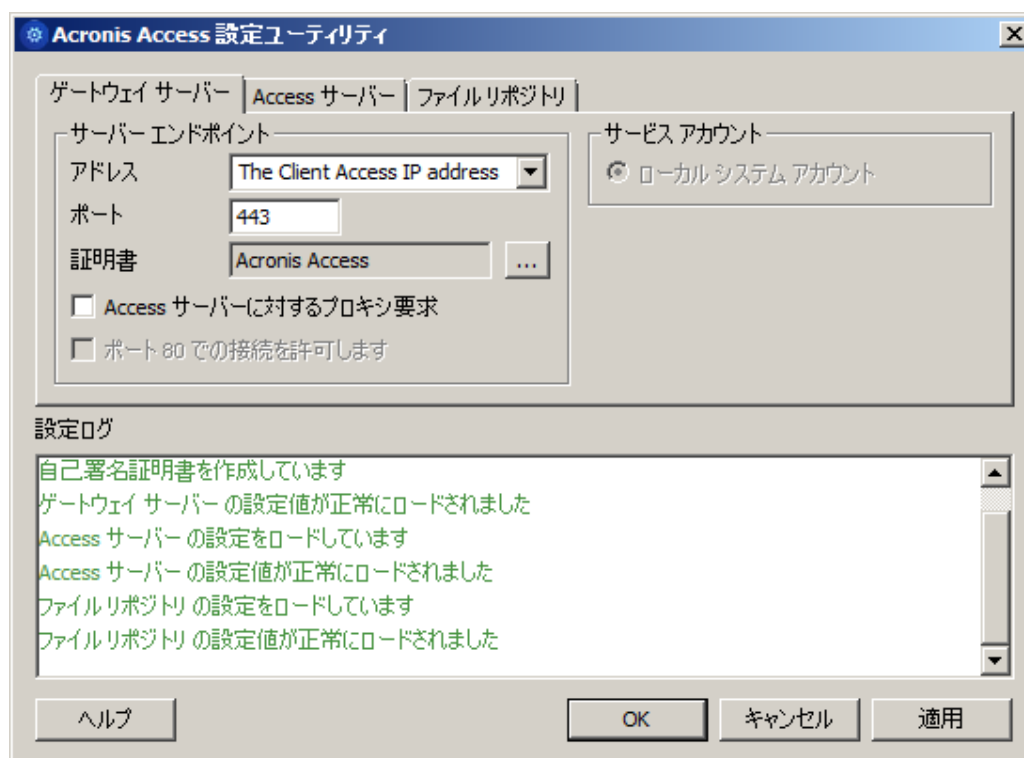


**注意:** ゲートウェイ サーバーと Access サーバーを異なる IP アドレスで実行する場合は、Acronis Access サービス グループに第 2 IP をリソースとして追加し、ネットワーク名の依存関係として設定します。

## サービス グループをオンラインにし、設定ユーティリティを使用する

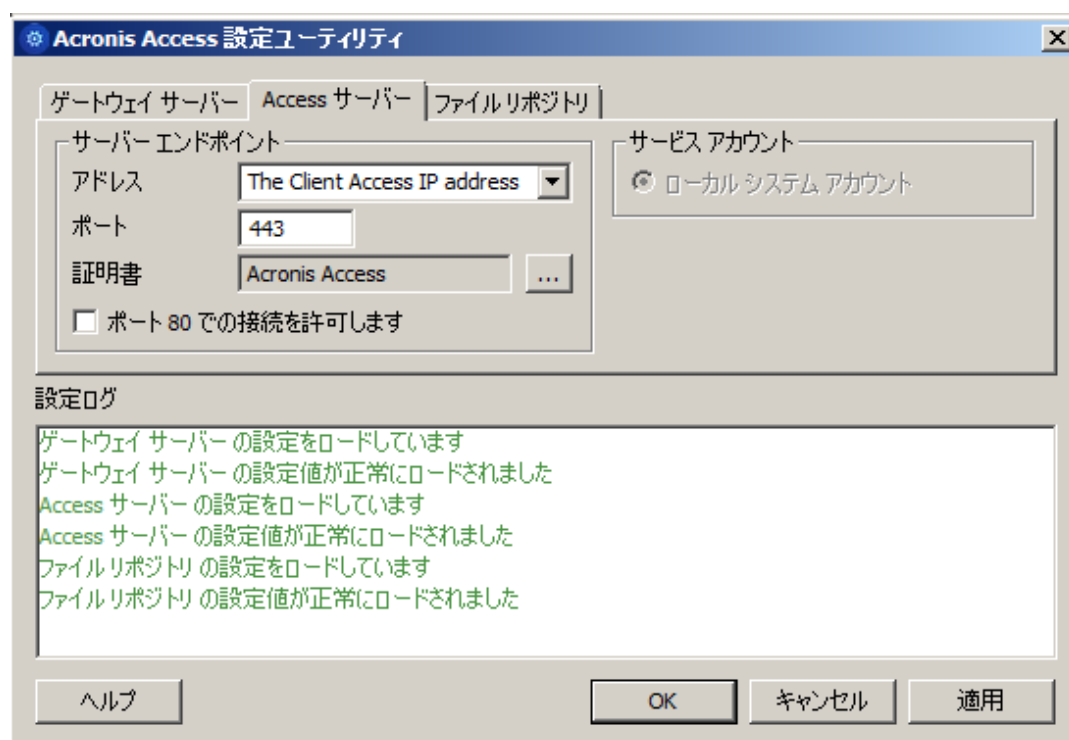
1. Acronis Access サービス グループを右クリックし、[Bring this application or service group online] を押します。
2. 設定ユーティリティを起動します。mobilEcho からのアップグレードの場合、通常これは **C:\Program Files (x86)\GroupLogic\Configuration Utility** にあります。

3. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

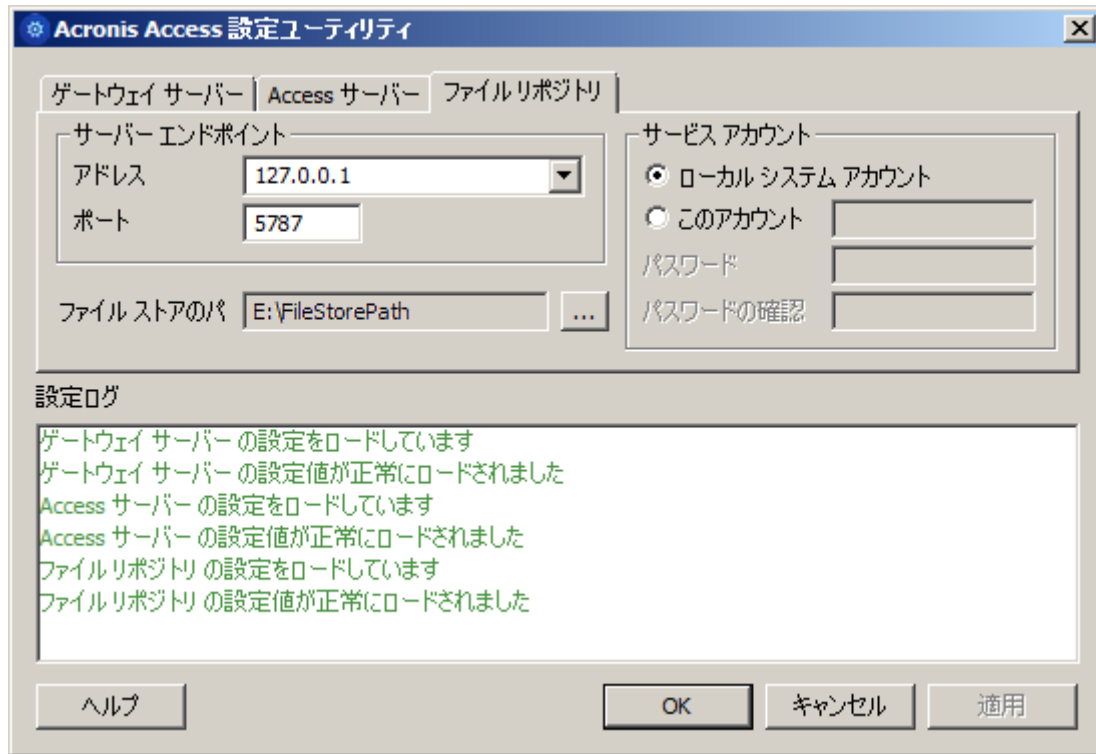


4. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



5. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



6. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Acronis Access をインストールします。ただし、今回は、デフォルトの **Postgres データ ロケーション**、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。

3. インストールを実行します。
4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。

- a. **C:\Program Files (x86)\GroupLogic\mobileEcho Server\** に移動します。
- b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
- c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます(**database\_path: 'S:/mobileEcho\_cluster/database/'** など)。

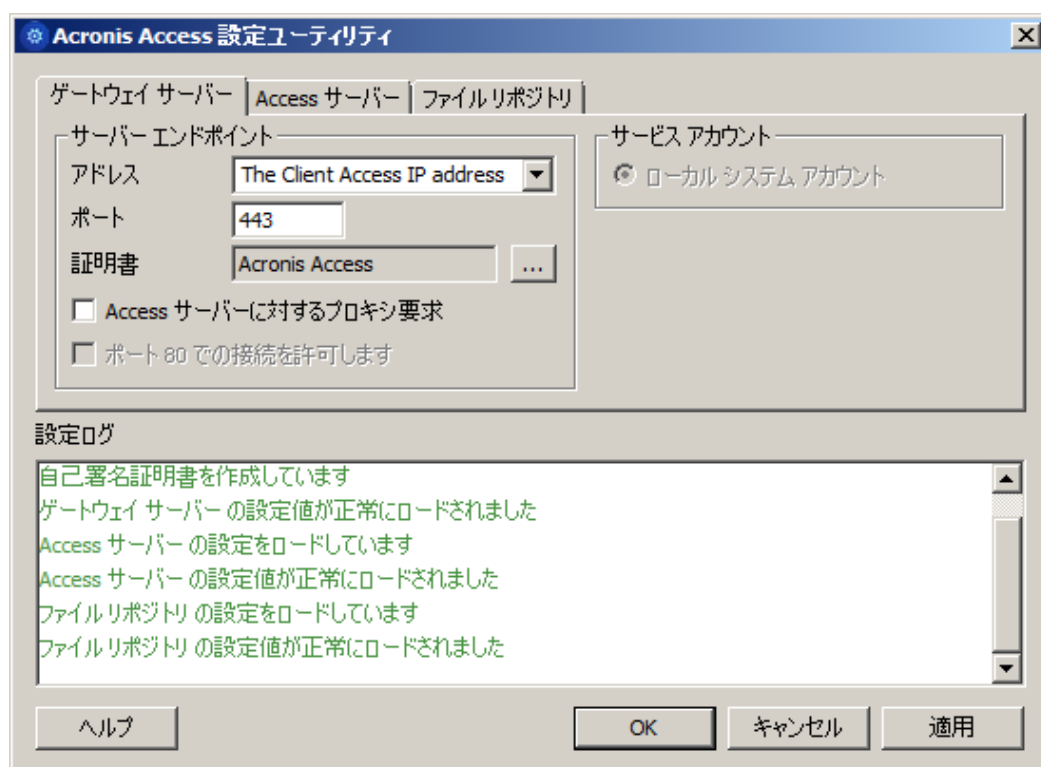
**注意:** パスの区切りにはスラッシュ (/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

**注意:** このパスは第 1 ノードで設定されているパスと同じでなければなりません。

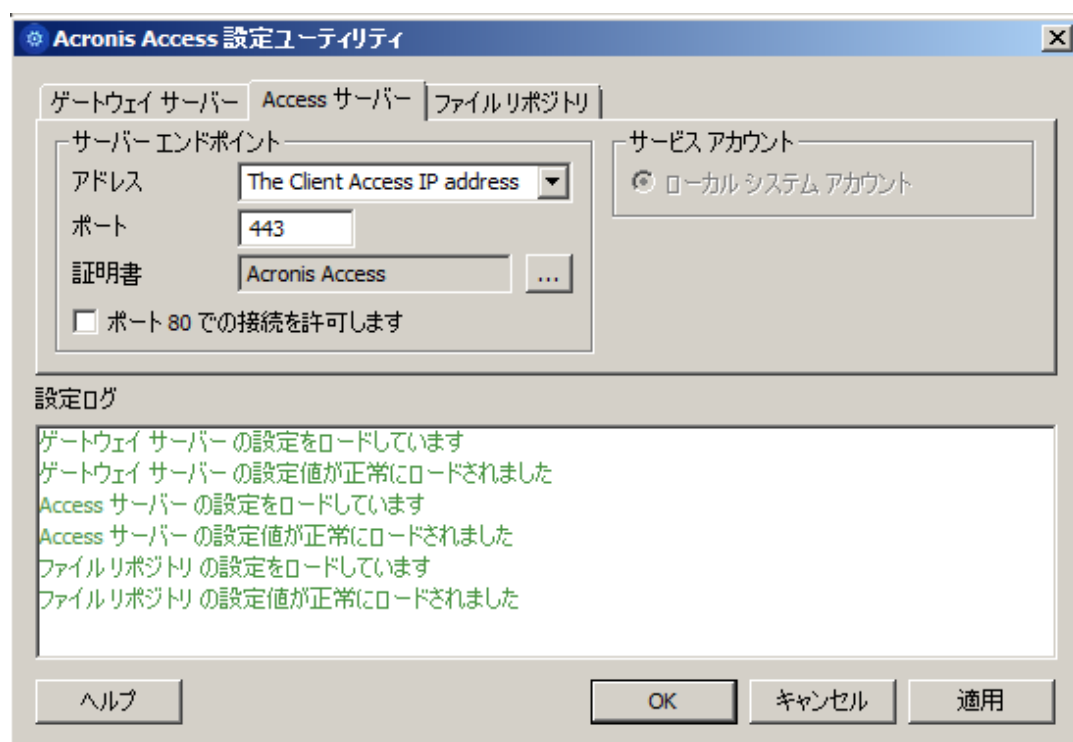
5. Acronis Access サービス グループを第 2 ノードに移動します。そのためには、そのサービス グループを右クリックして [第 2 ノードに移動] をクリックします。
6. 設定ユーティリティを起動します。mobileEcho からのアップグレードの場合、通常これは **C:\Program Files (x86)\GroupLogic\Configuration Utility** にあります。

7. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

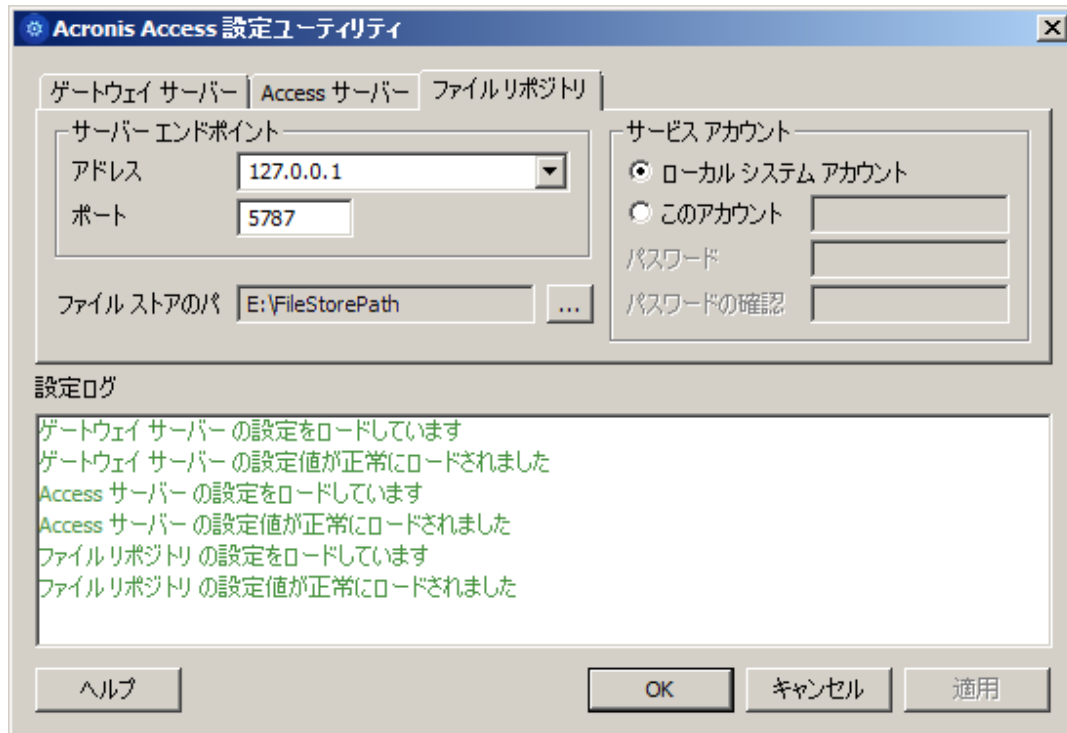


8. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



9. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



10. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 5.3 Windows 2012 フェールオーバー クラスタ上の mobilEcho サーバーを Acronis Access にアップグレードする

1. [フェールオーバー クラスタ マネージャ] を開き、サービス グループをダブルクリックします。
2. mobilEcho サービスのリソースを削除します。

**注意:** クラスタ グループ全体をオフラインにしないでください。mobilEcho サービス リソースだけを削除してください。

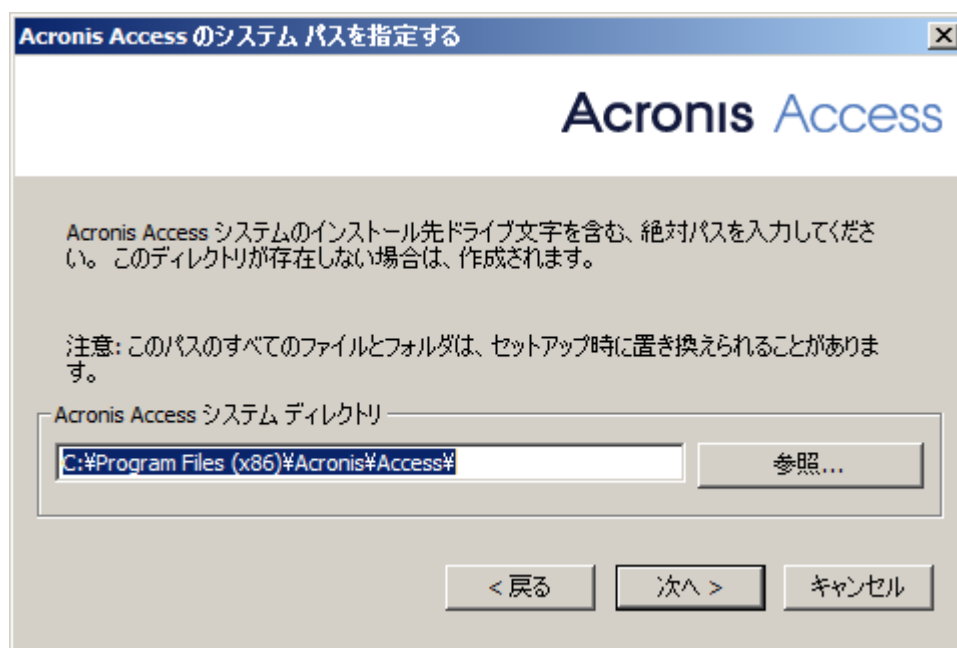
3. アクティブ ノードでインストーラを起動します。
4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. 実行可能なインストーラをダブルクリックします。



6. **[次へ]** を押して開始します。
7. 使用許諾契約を読み、承諾します。
8. **[インストール]** を押します。

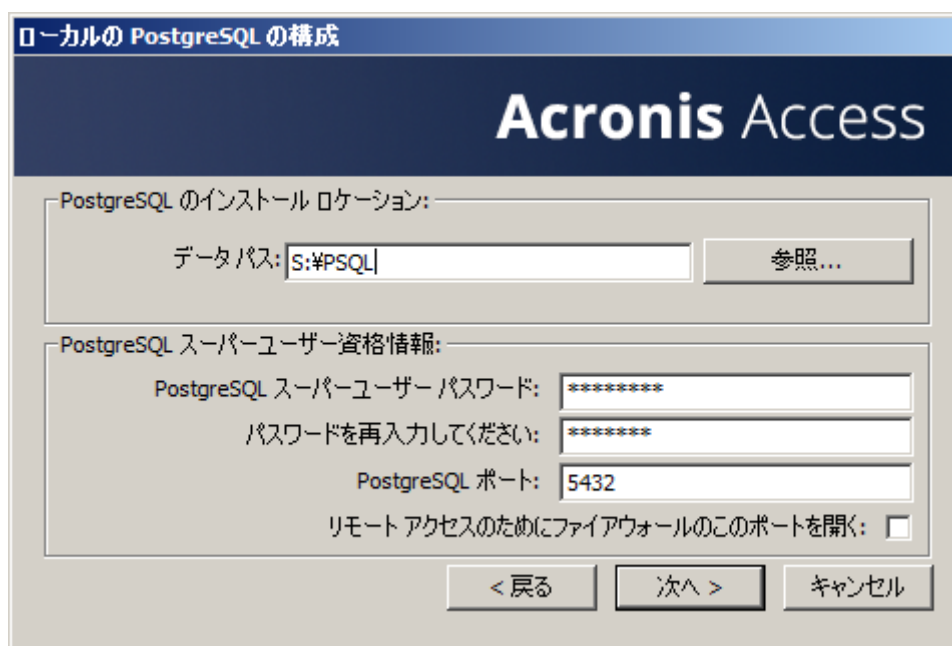
**注意:** 複数の Acronis Access サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタム インストール]** ボタンからインストールするコンポーネントを選択することができます。

9. Acronis Access メイン フォルダのデフォルト パスを使用するか新しいパスを選択し、**[OK]** を押します。



10. Postgres ユーザーのパスワードを設定し、書き留めておきます。このパスワードは、データベースのバックアップとリカバリに必要です。

11. 共有ディスクのうち **Postgres データ** フォルダのためのロケーションを選択して [次へ] をクリックします。



12. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、[OK] を押します。
13. Acronis Access のインストーラが完了したら、[終了] を押します。共有ディスクに移動し、**production.sqlite3**、**mobilecho\_manager.cfg**、**priority.txt** (これは存在しない場合があります) の 3 つのファイルを見つけてコピーしてから、それらを Acronis Access インストールディレクトリに貼り付けて既存のファイルを置き換えます。

**注意:** 置き換える元のファイルは、一般に次の場所にあるはずです。

C:\Program Files (x86)\Group Logic\mobilecho Server\ManagementUI\db\production.sqlite3

C:\Program Files (x86)\Group Logic\mobilecho  
Server\ManagementUI\mobilecho\_manager.cfg

C:\Program Files (x86)\Group Logic\mobilecho Server\Management\priority.txt

## アクティブ ノードでの設定

1. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. C:\Program Files (x86)\GroupLogic\mobilecho Server\ に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます (**database\_path: 'S:/mobilecho\_cluster/database/'** など)。

**注意:** パスの区切りにはスラッシュ (/) を使用します。

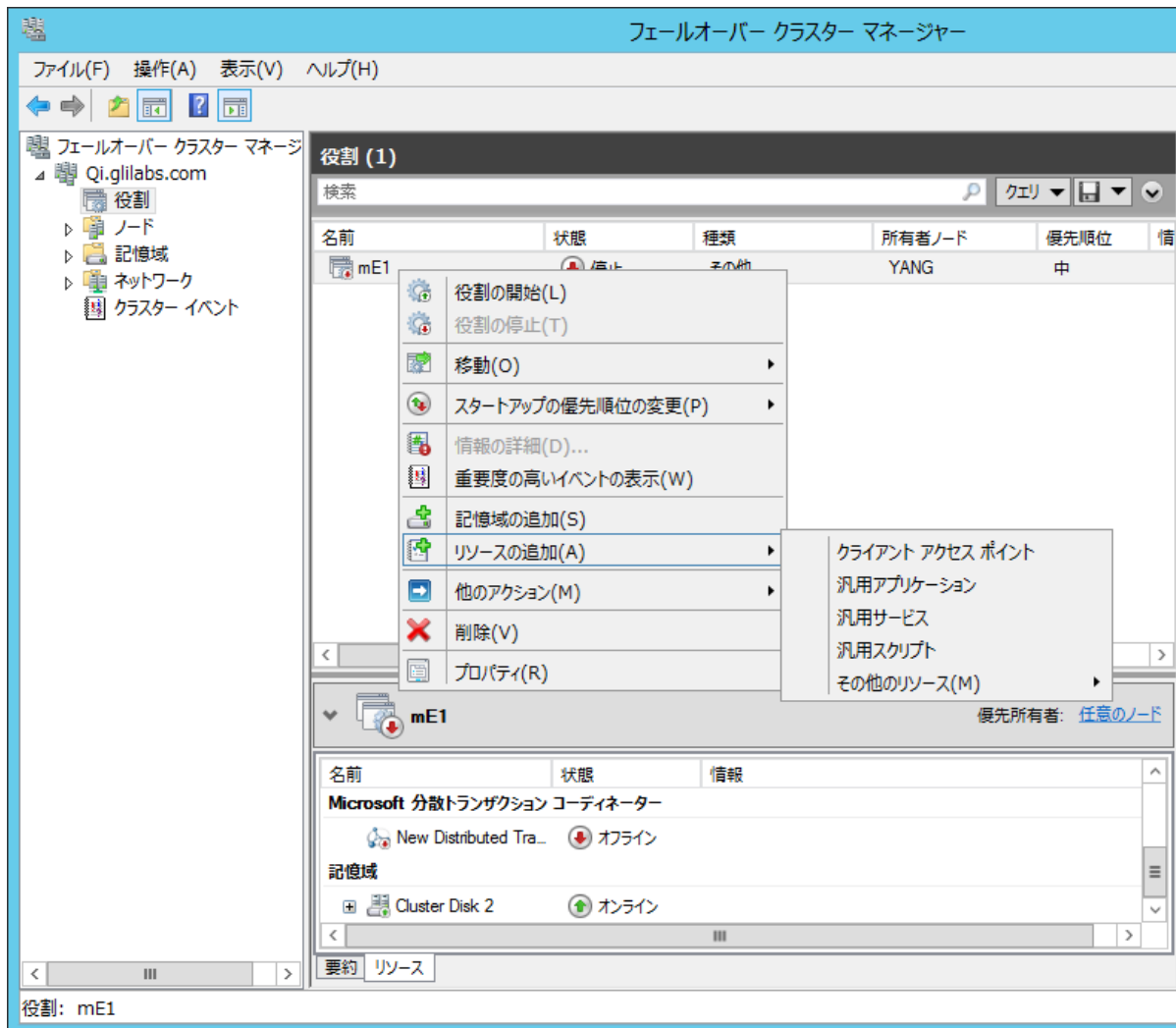
**注意:** 第 1 ノードで設定した **database.yml** をコピーして、第 2 ノードに貼り付けることができます。



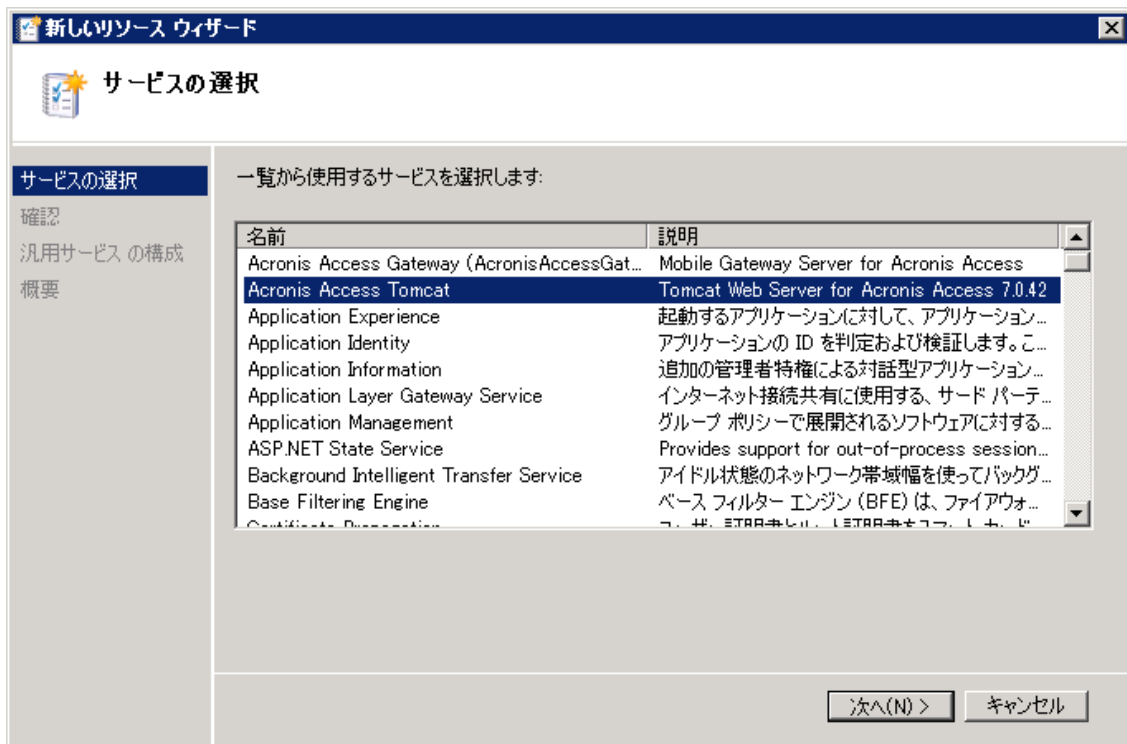
## 必要なすべてのサービスを Acronis Access の役割に追加する

AcronisAccessGateway、AcronisAccessPostgreSQL (Acronis Access のバージョンに応じて異なる)、AcronisAccessRepository、および AcronisAccessTomcat の各サービスについて、以下の手順を実行します。

1. Acronis Access 役割を右クリックして、[リソースの追加] を選択します。
2. [汎用サービス] を選択します。



- 適切なサービスを選択して [次へ] をクリックします。

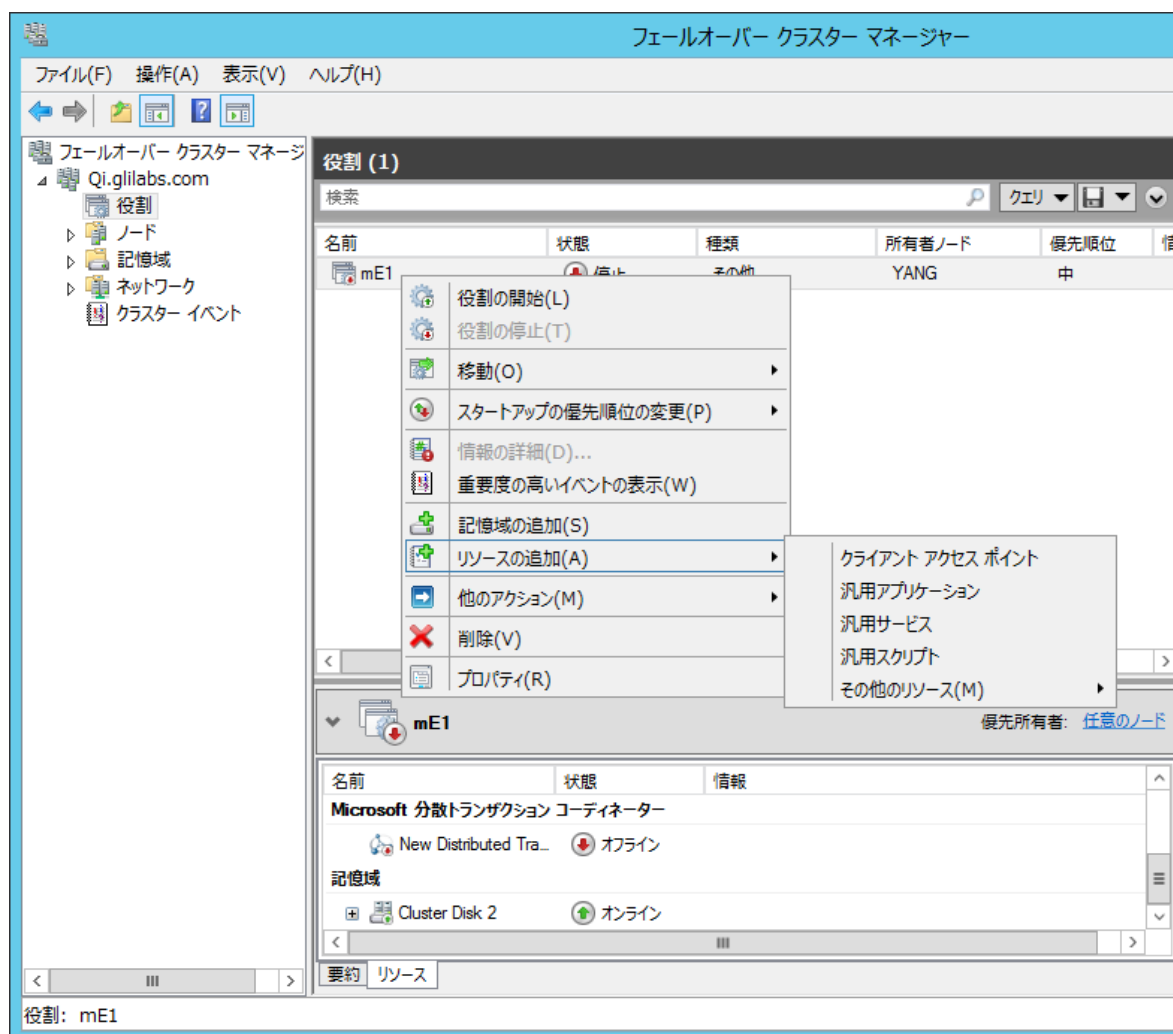


- 確認ウィンドウで [次へ] をクリックします。
- 概要ウィンドウで [完了] をクリックします。

## アクセス ポイントの設定

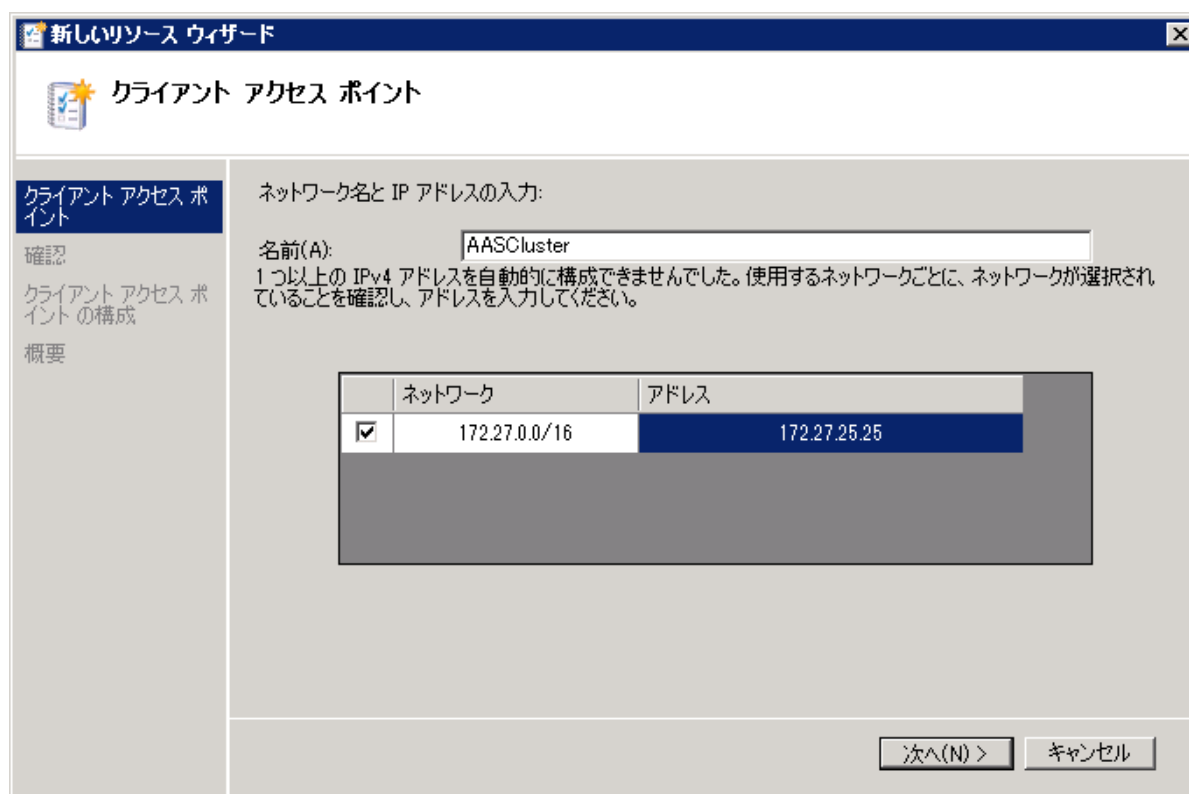
- Acronis Access 役割を右クリックして、[リソースの追加] を選択します。

2. [クライアント アクセス ポイント] を選択します。



3. このアクセス ポイントの名前を入力します。

4. ネットワークを選択します。



新しいリソース ウィザード

クライアント アクセス ポイント

クライアント アクセス ポイント

確認

クライアント アクセス ポイント の構成

概要

ネットワーク名と IP アドレスの入力:

名前(A): AASCluster

1 つ以上の IPv4 アドレスを自動的に構成できませんでした。使用するネットワークごとに、ネットワークが選択されていることを確認し、アドレスを入力してください。

|                                     | ネットワーク        | アドレス         |
|-------------------------------------|---------------|--------------|
| <input checked="" type="checkbox"/> | 172.27.0.0/16 | 172.27.25.25 |

次へ(N) > キャンセル

5. IP アドレスを入力して [次へ] をクリックします。

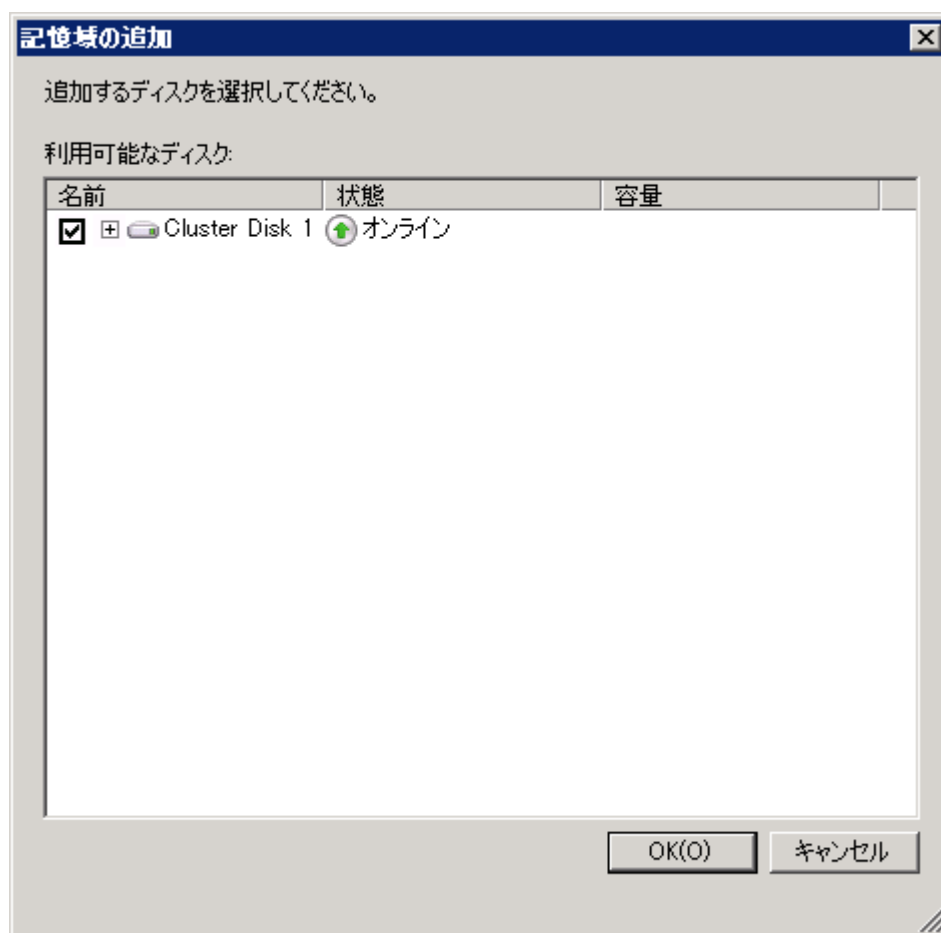
6. 確認ウィンドウで [次へ] をクリックします。

7. 概要ウィンドウで [完了] をクリックします。

## 共有ディスクの追加

1. Acronis Access の役割を右クリックして、[ストレージの追加] を選択します。

2. 共有ドライブを選択します。



## 依存関係の設定

1. Acronis Access の役割を選択し、[リソース] タブをクリックします。

**PostgreSQL および Acronis Access ファイル リポジトリ サービスについて、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックし、追加した共有ディスクを選択します。

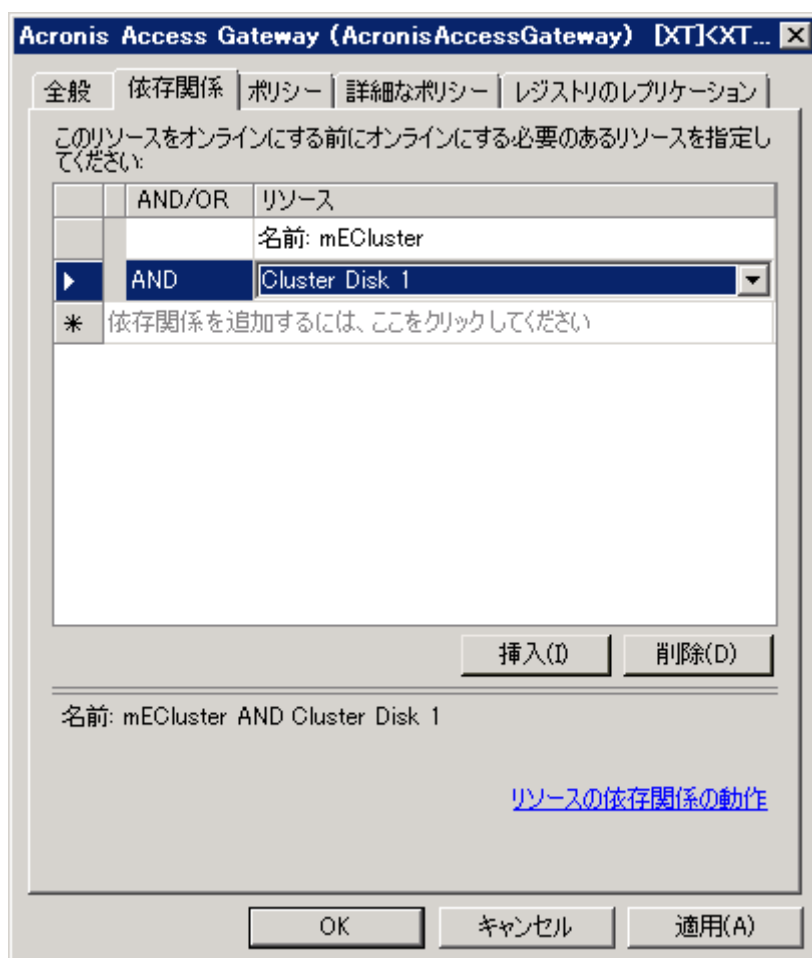


4. [適用] をクリックしてウィンドウを閉じます。

**Acronis Access ゲートウェイ サーバー サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。

3. [リソース] をクリックしてから、追加した共有ディスク、およびネットワーク名(クライアント アクセス ポイントの名前)を選択します。

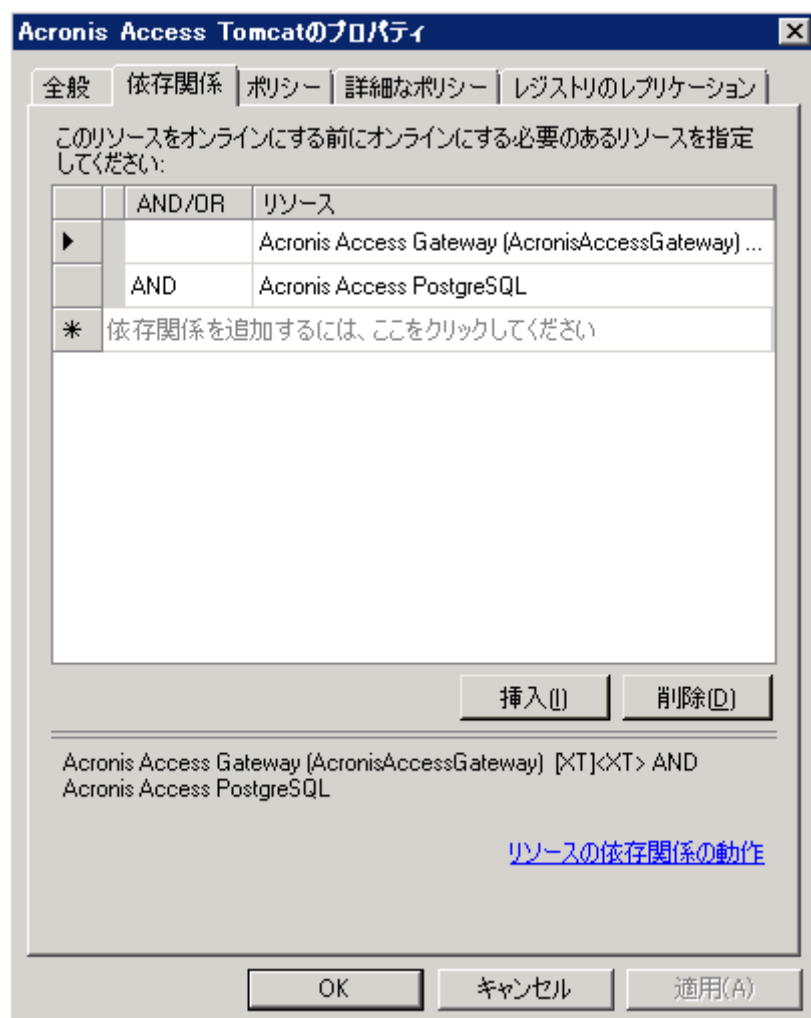


4. [適用] をクリックしてウィンドウを閉じます。

**Acronis Access Tomcat サービスでは、次の操作を実行します。**

1. 適切なサービスを右クリックし、[プロパティ] を選択します。
2. [依存関係] タブをクリックします。
3. [リソース] をクリックし、依存関係として、PostgreSQL および Acronis Access ゲートウェイ サーバーのサービスを選択します。[適用] をクリックしてウィンドウを閉じます。

**注意:** ゲートウェイ サーバーとアクセス サーバーを異なる IP アドレスで実行する場合は、第 2 IP をリソースとして Acronis Access 役割に追加し、それをネットワーク名の依存関係として設定します。

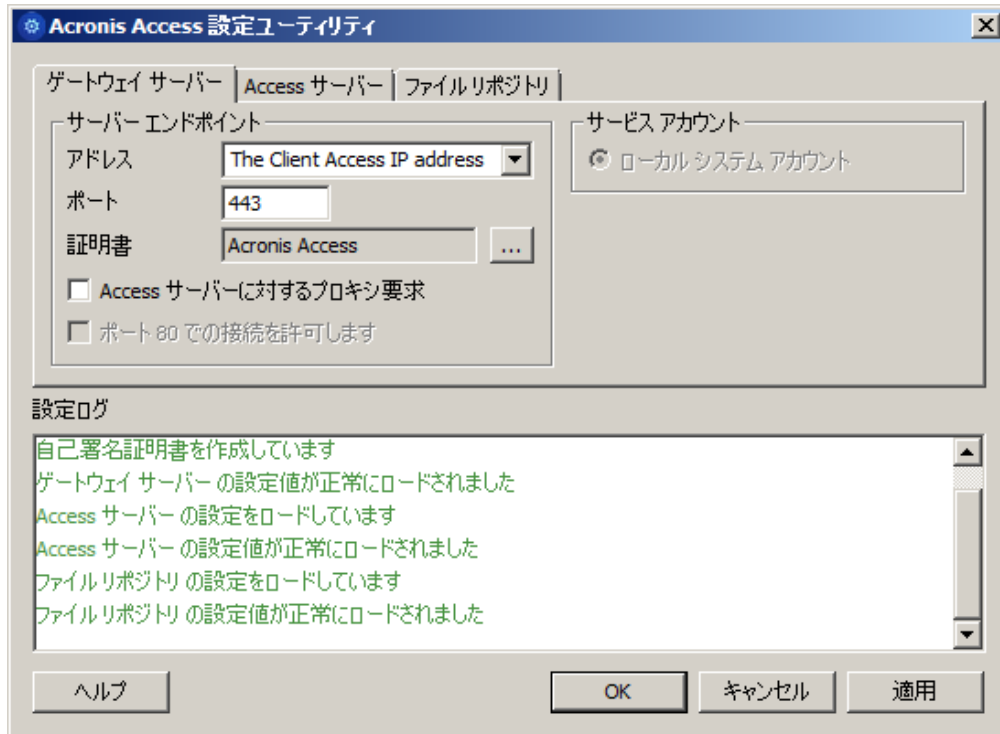


## 役割の開始と設定ユーティリティの使用

1. Acronis Access の役割を右クリックして、**[役割の開始]** を押します。
2. 設定ユーティリティを起動します。mobilEcho からのアップグレードの場合、通常これは **C:\Program Files (x86)\GroupLogic\Configuration Utility** にあります。

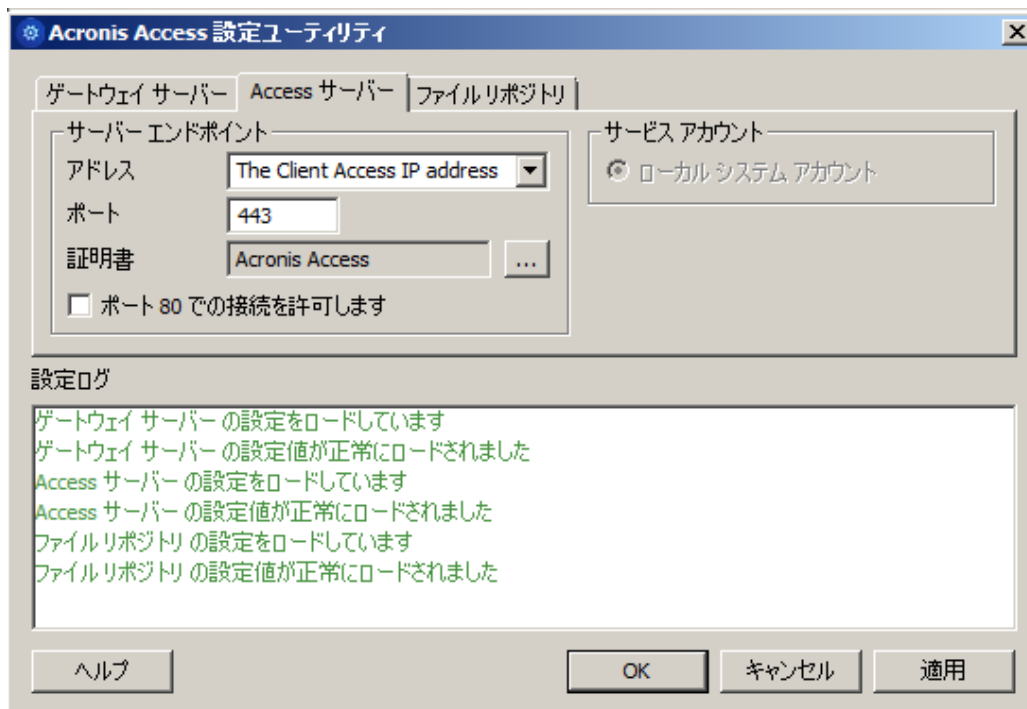


3. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

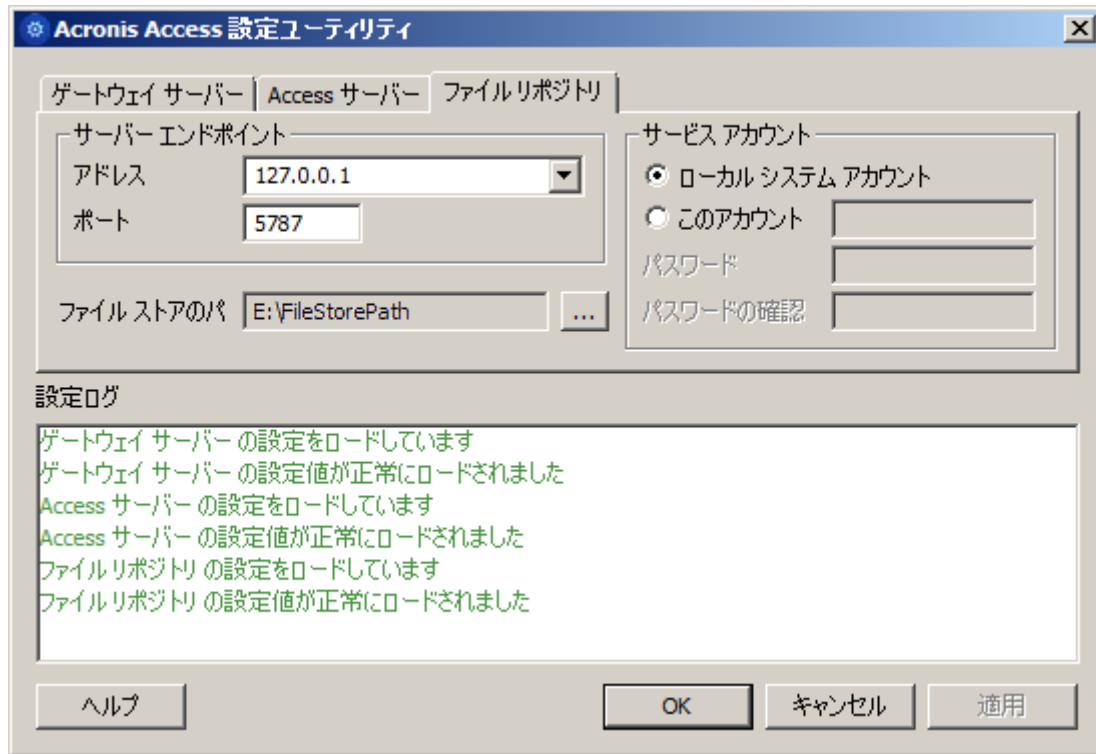


4. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



5. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



6. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 第 2 ノードでのインストールおよび設定

1. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
2. 第 2 ノードに Acronis Access をインストールします。ただし、今回は、デフォルトの **Postgres データ** ロケーション、および第 1 ノードと同じ postgres ユーザー パスワードを使用します。
3. インストールを実行します。
4. ゲートウェイ サーバーのデータベースが共有ディスク上のロケーションとなるように設定します。
  - a. **C:\Program Files (x86)\GroupLogic\mobilEcho Server\** に移動します。
  - b. **database.yml** ファイルを見つけ、テキスト エディタで開きます。
  - c. **database\_path: './database/'** の行を見つけ、**./database/** を、使用するパスに置き換えます (**database\_path: 'S:/mobilEcho\_cluster/database/'** など)。

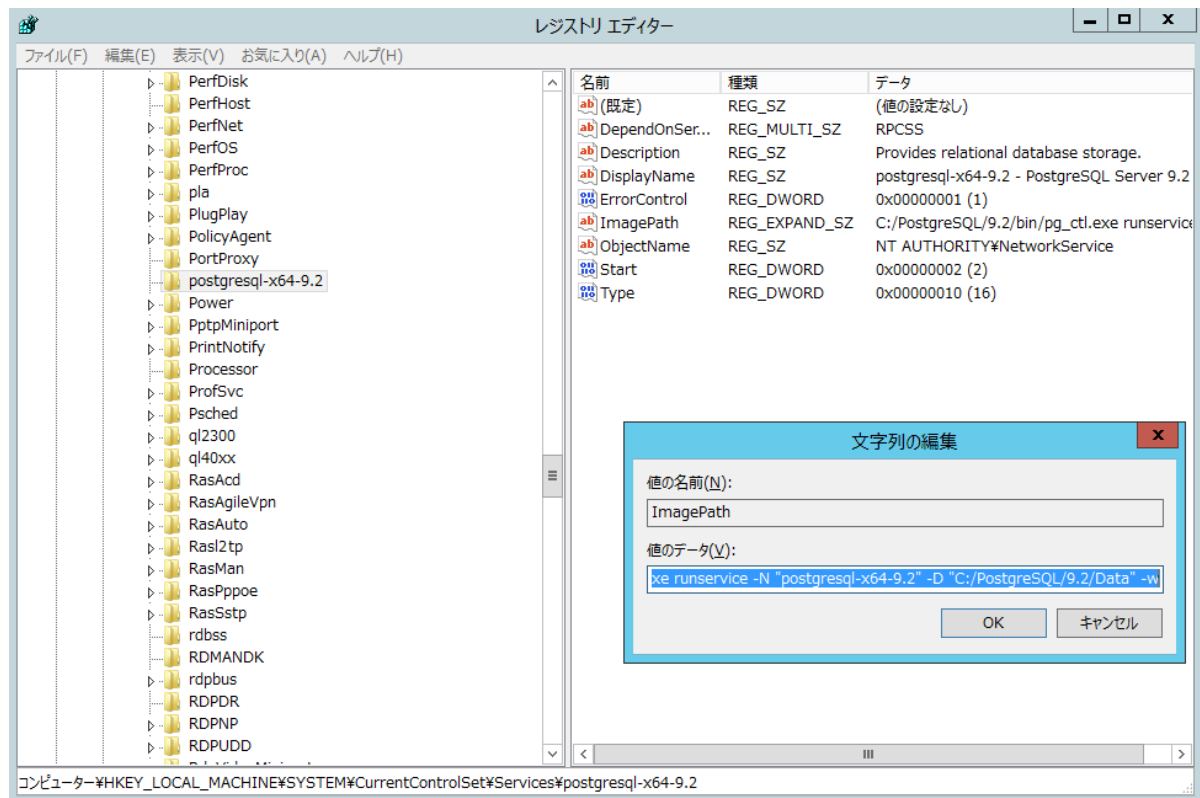
**注意:** パスの区切りにはスラッシュ (/)を使用します。

**注意:** 第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

**注意:** このパスは第 1 ノードで設定されているパスと同じでなければなりません。

PostgreSQL の場合、レジストリを手動で複製する必要があります。

1. **Regedit** を開きます。
2. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL\** に移動します。
3. キー「**ImagePath**」を開き、キーの値の一部を次のように変更します: **-D "The path you selected for the PostgreSQL data location"** (例: **-D "E:/PostgreSQL/data"**)。
4. キー「**DataDirectory**」を開き、値を PostgreSQL のデータ フォルダに選択したパスに変更します (例: **E:/PostgreSQL/data**)。

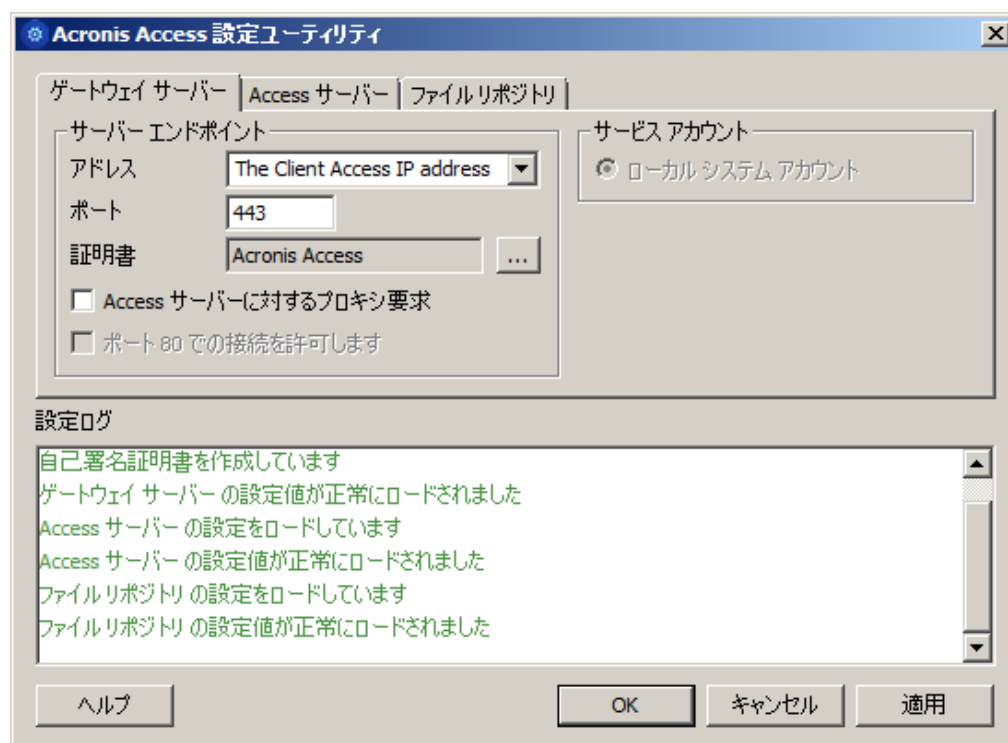


5. **Regedit** を閉じ、続けて以下のステップを実行します。
6. Acronis Access の役割を第 2 ノードに移動します。

## 第 2 ノードの設定ユーティリティの使用

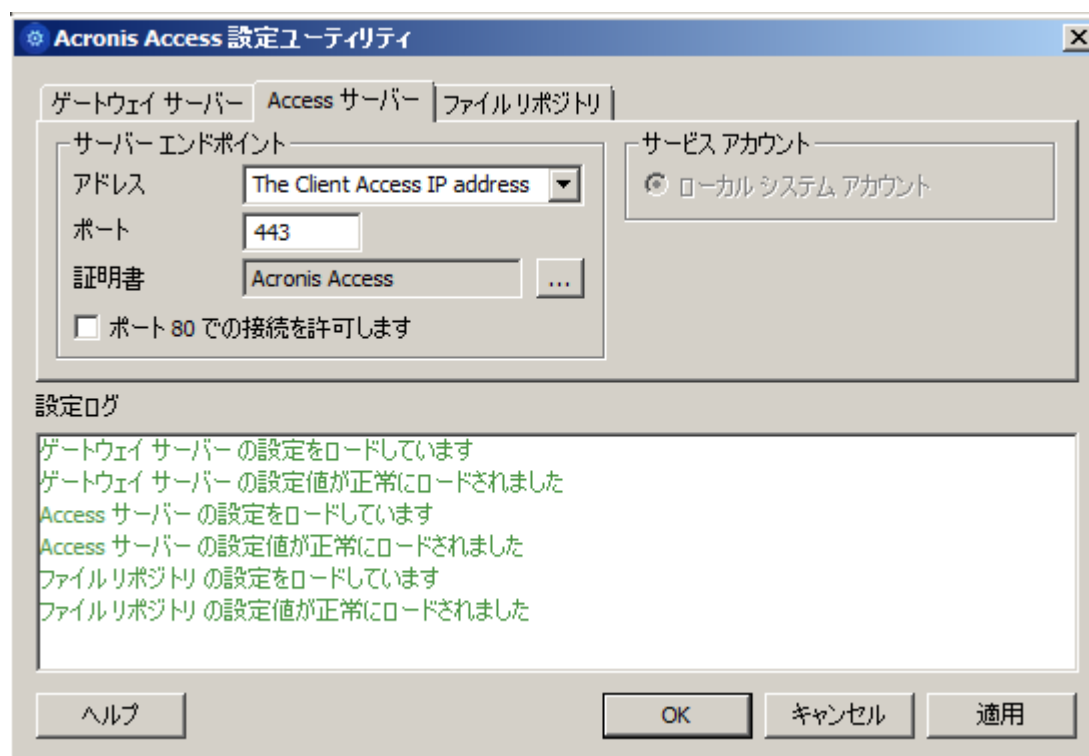
1. 設定ユーティリティを起動します。mobilEcho からのアップグレードの場合、通常これは **C:\Program Files (x86)\GroupLogic\Configuration Utility** にあります。

2. Acronis Access ゲートウェイ サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

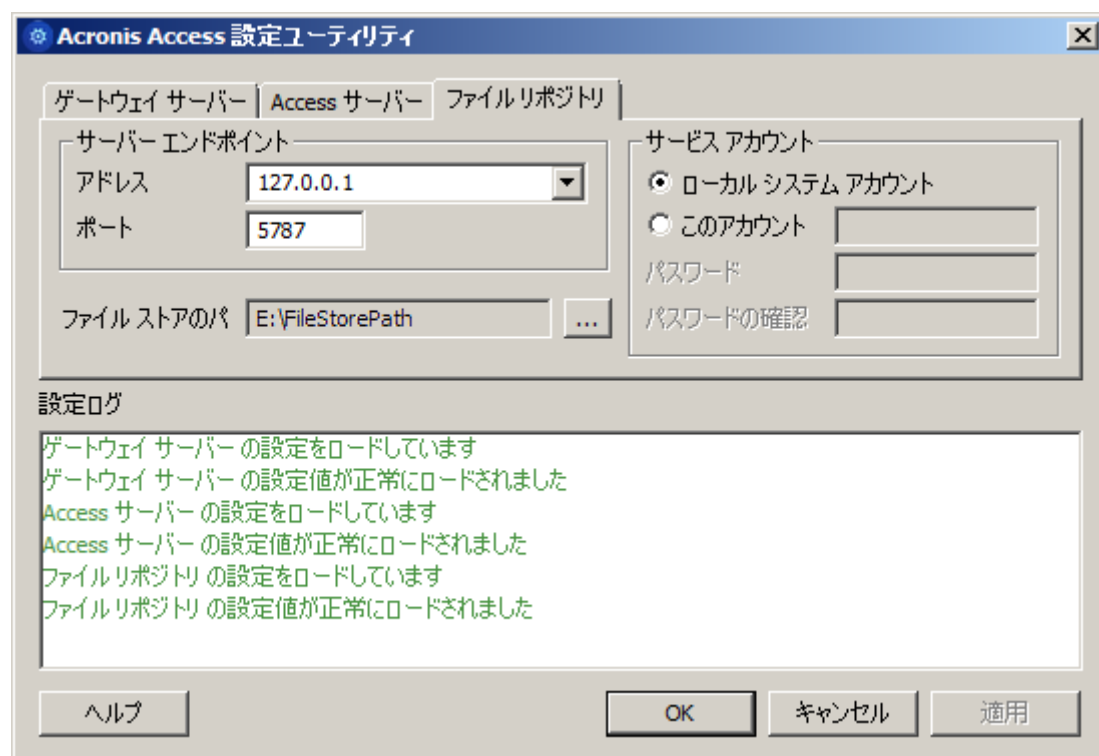


3. Acronis Access サーバー サービスが、IP アドレス上で Acronis Access サービス グループをリスンするように設定します。

**注意:** [ポート 80 での接続を許可します] が選択されている場合、Tomcat は、セキュアでないポート 80 で着信トラフィックをリスンし、それを上記で指定された HTTPS ポートにリダイレクトします。ポート 80 上でリスンする別のプログラムがある場合は、このボックスをオンにしないでください。



4. Acronis Access ファイル リポジトリが localhost 上でリッスンするように設定し、FileStore へのパスが共有ディスク上になるように変更します。このパスは、2 つのノードで同じにする必要があります。



5. [OK] をクリックすると、設定が完了し、サービスが再起動します。

## 6 クイック スタート: モバイル アクセス

このガイドでは、ゲートウェイ サーバーの設定、データ ソースの追加、および Access モバイル クライアント アプリケーションのインストールに不可欠な手順について説明します。Acronis Access ゲートウェイ サーバーと Client Management コンポーネントの構成に関する詳細については、「ゲートウェイ サーバーの管理」と「モバイル アクセス」のセクションを参照してください。

### セクションの内容

|  |     |
|--|-----|
| 初期設定 .....                               | 178 |
| 最初のゲートウェイ サーバーとデータ ソースの構成 .....          | 182 |
| ポリシーの設定 .....                            | 185 |
| Access モバイル クライアント アプリケーションのインストール ..... | 186 |
| クライアント管理での登録 .....                       | 187 |

### 6.1 初期設定

Acronis Access のインストールと構成をまだ行っていない場合は、それを実行します。詳細については、「インストール 『5ページ』」セクションと「設定ユーティリティ 『10ページ』」セクションを参照してください。

ウェブ インターフェイスを初めて開いたときに、デフォルト管理者アカウントのパスワードを設定する必要があり、ログイン後に**セットアップ ウィザード**が表示されます。

---

**警告:** 管理者パスワードを忘れることがないようにしてください。サポート部門でそのパスワードを復元することはできません。

**注意:** 構成ユーティリティからの起動後、アプリケーションが使用可能になるまでに 30 から 45 秒かかることがあります。

---

上記の手順が完了すると、下記に示されている初期構成を進める準備が整います。

## サーバー設定

|                       |   |
|-----------------------|---|
| サーバー名                 | <input type="text" value="Acronis Access"/>             |
| ウェブ アドレス              | <input type="text" value="https://www.echoserver.com"/> |
| モバイル クライアント登録<br>アドレス | <input type="text" value="www.echoserver.com"/>         |
| カスタム ログを使用            | <input type="checkbox"/>                                |
| 監査ログの言語               | <input type="text" value="日本語"/> ▼                      |

保存

1. [サーバー名] にサーバー名を入力します。
2. ユーザーが(http:// または https:// で始まる)ウェブ サイトにアクセスできるFQDN または IP アドレスを指定します。
3. モバイル ユーザーが登録する FQDN または IP アドレスを指定します。
4. カラー スキームを選択します。現在のオプションは、[灰色]、[紫]、[カプチーノ]、[青]、[濃紺]、および [オレンジ] です。
5. **[監査ログ]** のデフォルトの言語を選択します。現在のオプションは、[英語]、[ドイツ語]、[フランス語]、および [日本語] です。
6. **[保存]** を押します。

## SMTP

### SMTP

Acronis Access サーバーは、構成された SMTP サーバーを使用して電子メールを送信し、ファイルの共有やデバイスの登録のためにユーザーを招待したり、ユーザーや管理者にサーバー アクティビティを通知します。

SMTP サーバー アドレス

myemailserver.mycompany.com

SMTP サーバー ポート

25

セキュリティで保護された  
接続を使用しますか？



差出人名

Access Administrator

差出人電子メール アドレス

adminname@mycompany.com

SMTP 認証を使用します  
か？



保存

テスト用の電子メールの送信

SMTP セットアップのスキップ

**注意:** この手順をスキップして、後で SMTP を構成することもできます。

1. SMTP サーバーの FQDN または IP アドレスを入力します。
2. サーバーの SMTP ポートを入力します。
3. SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか？]** のチェックを外します。
4. サーバーによって送信される電子メールの「差出人」行に表示されるユーザー名を入力します。
5. サーバーから送信される電子メールのアドレスを入力します。
6. SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、**[認証を使用しますか？]** をチェックし、認証情報を入力してください。
7. **[テスト用の電子メールの送信]** を押して電子メールを手順 5 で指定したテスト用の電子メール アドレスに送信します。
8. **[保存]** を押します。



## LDAP

### LDAP

組織内のユーザーにモバイル アクセス、同期アクセス、および共有アクセスを提供するために、Active Directory への LDAP 接続を使用することができます。LDAP は、管理対象外のモバイル アクセスや、同期および共有サポートに対しては不要ですが、管理対象のモバイル アクセスには必要になります。Microsoft Active Directory への LDAP 接続のみがサポートされています。

LDAP を有効にしますか？ ☒

LDAP サーバー アドレス

LDAP サーバー ポート

セキュリティで保護された  
LDAP 接続を使用します  
か？ ☐

LDAP ユーザー名

LDAP パスワード

LDAP パスワードの確認入  
力

LDAP 検索ベース

LDAP 認証のためのドメイ  
ン

例: mycompany.com. このリストに含まれるドメインの電子メール アドレスを使用しているユーザーは、LDAP に対して認証する必要があります。他のドメインのユーザーは、Acronis Access データベースに対して認証します。

+ 追加

- 削除

☐ 完全に一致している必要があります

LDAP 情報をキャッシュす  
る間隔

保存

LDAP のセットアップをスキップ

---

**注意:** この手順をスキップして、後で LDAP を構成することもできます。

---

1. **[LDAP を有効にしますか?]** をチェックします。
2. LDAP サーバーの FQDN または IP アドレスを入力します。
3. LDAP サーバーのポートを入力します。
4. LDAP サーバーとの接続に証明書を使用する場合は、**[セキュリティで保護された LDAP 接続を使用しますか?]** をチェックします。
5. LDAP の資格情報をドメインも含めて入力します (例: `acronis%hristo`)。
6. LDAP 検索ベースを入力します。
7. LDAP 認証のドメインを入力します (例えば、電子メール `joe@glilabs.com` のアカウントの LDAP 認証を有効にするには、**glilabs.com** と入力します)。
8. **[保存]** を押します。

## ローカル ゲートウェイ サーバー

### ローカル ゲートウェイ サーバー

Acronis Access のモバイル アプリケーション クライアントは、ゲートウェイ サーバーのアドレスを使用して Access サーバーに接続します。サーバーの設定によっては、デスクトップ同期クライアントおよびウェブ クライアントもこのサーバーに接続されていることがあります。ゲートウェイ サーバーは現在 **192.168.2.129:443** で動作しています。クライアントの接続設定では、接続元となるすべてのネットワークからアクセス可能な DNS アドレスを使用することが推奨されます。クライアントがプロキシ サーバーを経由して接続する場合、このアドレスはプロキシ サーバーの実際の DNS アドレスにすることができます (例: `gateway.mycompany.com`)。

クライアントがサーバーに接続するために使用するアドレス:

192.168.2.129:443

保存

スキップ

---

**注意:** 同じコンピュータにゲートウェイ サーバーと Acronis Access サーバーの両方をインストールする場合、ゲートウェイ サーバーが自動的に検出され、Acronis Access サーバーに管理されます。クライアントがアクセス可能なローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定するように指示するメッセージが表示されます。このアドレスは後から変更できます。

---

1. ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。
2. **[保存]** を押します。

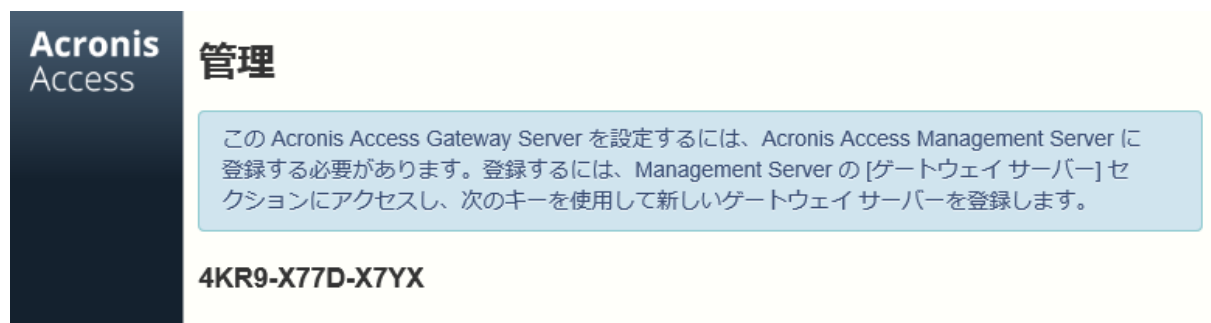
## 6.2 最初のゲートウェイ サーバーとデータ ソースの構成

### 新しいゲートウェイ サーバーの登録:

1. ゲートウェイ サービスがインストールされているコンピュータを参照します。
2. **https://localhost/gateway\_admin** を開きます。

注意: デフォルトのポート番号は、443 です。デフォルトのポートを変更した場合は、「localhost」の後ろにポート番号を追加してください。

3. **【管理キー】** を書き留めます。



4. Acronis Access ウェブ インターフェイスを開きます。
5. **【モバイル アクセス】** タブを選択します。
6. **【ゲートウェイ サーバー】** ページを開きます。
7. **【新しいゲートウェイ サーバーの追加】** ボタンを押します。

### 新しいゲートウェイ サーバーの追加

表示名:

Marketing Gateway

管理のアドレス: ⓘ

https:// 192.168.1.72

☐ クライアント接続に代替アドレスを使用 ⓘ

管理キー: ⓘ

4KR9-X77D-X7YX

☒ 自己署名証明書を使用した Acronis Access サーバーからの接続を許可 ⓘ

8. ゲートウェイ サーバーの表示名を入力します。
9. ゲートウェイ サーバーの FQDN または IP アドレスを入力します。

**注意:** リバース プロキシ サーバーまたはロードバランサを経由してモバイル クライアントをゲートウェイに接続する場合、**[クライアント接続に代替アドレスを使用]** を有効にして、リバース プロキシ サーバーまたはロードバランサの FQDN または IP アドレスを入力してください。

10. **[管理キー]** を入力します。
11. 必要に応じて、**[自己署名した証明書を使用した Acronis Access サーバーからの接続を許可]** を有効にして、自己署名した証明書を使用することで、このゲートウェイに接続することができます。
12. **[保存]** ボタンを押します。

**注記:** ゲートウェイ サーバーが 1 つ以上あることを確認してください。

## データ ソースの作成

### 新しいフォルダを追加

表示名:

このデータソースにアクセス権を付与するために使用するゲートウェイ サーバーを選択する:

Local (192.168.2.129:443)

データのロケーション:

この Acronis Access ゲートウェイ サーバー上で共有するローカル フォルダのパスを入力します (例: "E:\Shares\Documents\"). ワイルドカード文字列 %USERNAME% をパスに含めることができます。この場合、ワイルドカードはユーザーのユーザー名で置き換えられます。

パス:

同期:

☒ サーバーの参照時に表示する

☐ Salesforce.com アクティビティのログ記録を必須にする **A G**

### ユーザーまたはグループにこのフォルダを割り当てる

次に該当するユーザーまたはグループを検索

検索

データ ソースを作成する手順は、次のとおりです。

1. Acronis Access ウェブ インターフェイスを開きます。
2. **[モバイル アクセス]** タブを選択します。
3. **[データ ソース]** タブを開きます。
4. **[フォルダ]** に移動します。
5. **[新しいフォルダの追加]** ボタンを押します。
6. フォルダの表示名を入力します。
7. フォルダへのアクセスを提供するゲートウェイ サーバーを選択します。
8. データのロケーションを選択します。ロケーションとして、実際のゲートウェイ サーバー、他の SMB サーバー、SharePoint サイトまたはライブラリ、同期と共有サーバー上を選択できます。

**注意:** 同期と共有を選択するときは、必ずサーバーのフル パスをポート番号と共に入力してください(例: <https://mycompany.com:3000>)。

9. ロケーションの選択に基づき、フォルダ、サーバー、サイトまたはライブラリへのパスを入力します。
10. フォルダの同期タイプを選択します。
11. Acronis Access モバイル クライアントがゲートウェイ サーバーを参照した場合に、このデータソースが表示されるようにするには **[サーバーの参照時に表示する]** を有効にします。
12. フォルダを Salesforce アクティビティ ログが必要な場合に選択します。
13. フォルダを割り当てるユーザーやグループを参照し選択します。
14. **[保存]** ボタンをクリックします。

## 6.3 ポリシーの設定

クライアント管理にユーザーを登録するには、ユーザー ポリシーまたはグループ ポリシーを設定する必要があります。ポリシーの詳細については、「ユーザーおよびグループ ポリシー」の記事を参照してください。

新しいグループ ポリシーを追加するには

1. **[グループ ポリシー]** タブを選択します。
2. 新しいグループ ポリシーを追加するには、**[新しいポリシーの追加]** ボタンをクリックします。これにより、**[新しいグループ ポリシーの追加]** ページが表示されます。

新しいグループ ポリシーの追加

保存 キャンセル

ディレクトリを検索し、このポリシーのグループを選択します。

選択されたグループ:

次に該当するグループを検索

先頭の文字

domain ad

検索

共通名/表示名

識別名

Domain Admins

CN=Domain Admins,CN=Users,DC=giliabs,DC=com

ポリシーの設定のコピー元:

適用

重要な注意事項: Acronis Access ポリシー設定には、Acronis Access for Android、Acronis Access for Good Dynamics および Acronis Access with MobileIron AppConnect に対して異なる方法で適用されるものがあります。これらの例外には、、、および  アイコンを表示しています。各アイコンの上にマウスを移動すると、ポリシー設定に関する例外の詳細が表示されます。特定のクライアント プラットフォームのみが Acronis Access サーバーの使用 接続できるように Acronis Access Gateway サーバーを設定することができます。

セキュリティ ポリシー

アプリケーション ポリシー

同期ポリシー

ホーム フォルダ

サーバー ポリシー

3. **[次に該当するグループを検索]** フィールドに、ポリシーを作成する対象の Active Directory グループ名の一部または全部を入力します。**[先頭の文字]** または **[含まれる文字]** 検索を Active Directory グループに対して実行できます。**[先頭の文字]** の検索は、**[含まれる文字]** の検索よりも短時間で完了します。
4. **[検索]** をクリックし、表示される結果でグループ名を見つけてクリックします。
5. **[セキュリティ]**、**[アプリケーション]**、**[同期]**、**[ホーム フォルダ]**、および **[サーバー]** の各タブで必要な設定をしてから **[保存]** をクリックします。

## 新しいユーザー ポリシーを追加するには

1. **[ユーザー ポリシー]** タブを選択します。
2. 新しいユーザー ポリシーを追加するには、**[新しいポリシーの追加]** ボタンをクリックします。これにより、**[新しいユーザー ポリシーの追加]** ページが表示されます。

**新しいユーザー ポリシーの追加** 保存 キャンセル

ディレクトリを検索し、このポリシーのユーザーを選択します。

**選択されたユーザー:**

| 次に該当するユーザーを検索 | 先頭の文字                                 | 検索     |
|---------------|---------------------------------------|--------|
| 共通名/表示名       | 識別名                                   | ログイン名  |
| hristo        | CN=hristo,CN=Users,DC=gililabs,DC=com | hristo |

ポリシーの設定のコピー元: 適用

**重要な注意事項:** Acronis Access ポリシー設定には、Acronis Access for Android、Acronis Access for Good Dynamics および Acronis Access with MobileIron AppConnect に対して異なる方法で適用されるものがあります。これらの例外には、、、および  アイコンを表示しています。各アイコンの上にマウスを移動すると、ポリシー設定に関する例外の詳細が表示されます。特定のクライアント プラットフォームのみが Acronis Access サーバーの使用 接続できるように Acronis Access Gateway サーバーを設定することができます。

**セキュリティ ポリシー**   **アプリケーション ポリシー**   **同期ポリシー**   **ホーム フォルダ**   **サーバー ポリシー**

3. **[ユーザーの検索]** フィールドに、ポリシーを作成する対象の Active Directory ユーザー名の一部または全部を入力します。**[先頭の文字]** または **[含まれる文字]** 検索を Active Directory ユーザーに対して実行できます。**[先頭の文字]** の検索は、**[含まれる文字]** の検索よりも短時間で完了します。
4. **[検索]** をクリックし、表示される結果でユーザー名を見つけてクリックします。
5. **[セキュリティ]**、**[アプリケーション]**、**[同期]**、**[ホーム フォルダ]**、および **[サーバー]** の各タブで必要な設定をしてから **[保存]** をクリックします。

## 6.4 Access モバイル クライアント アプリケーションのインストール

1. Apple または Android のアプリ ストアで Acronis Access を参照します。
  - iOS デバイスの場合、Apple App Store にアクセスして Acronis Access を検索するか、リンク <http://www.grouplogics.com/web/meappstore> にアクセスします。
  - Android デバイスの場合、Google Play ストアにアクセスして Acronis Access を検索するか、リンク <https://play.google.com/store/apps/details?id=com.grouplogics.mobilecho> にアクセスします。
2. Access モバイル クライアント アプリケーションをインストールし、タップして起動します。
3. ようこそ画面で **[続行]** をタップします。

- iOS では「+」アイコンをタップし、サーバーを追加します。
  - Android では **[設定]** メニューを開き、**[サーバーを追加]** をタップします。
4. Acronis Access サーバーまたはゲートウェイ サーバーをインストールしたサーバーのサーバー名または IP アドレスを入力します。サーバー リストに表示されるこのサーバーの表示名を任意で入力できます。
  5. ゲートウェイ サーバーにアクセスできるユーザーのユーザー名を入力します。  
<RPRODUCT\_NAME> は標準の NTFS アクセス権を使用してアクセスを規制します。
  6. パスワードを保存する場合は、**[パスワードの保存]** をオンに切り替えてから、パスワードを入力し、確認のためにもう一度入力します。
  7. **[保存]** をタップしてサーバーの設定を確定します。
  8. 左側のペインに一覧表示されるサーバーをタップして接続し、使用可能なボリュームを参照します。
  9. Access モバイル クライアント アプリケーションの設定と機能の詳細については、「モバイル クライアント」のページを参照してください。

## 6.5 クライアント管理での登録

モバイル アクセスを有効にして Acronis Access をインストールした後は、以下の 2 つの方法で Access モバイル クライアントを使用できます。

組織が Access モバイル クライアントのアクセスおよび設定を集中管理している場合、Acronis Access へのアクセス権を IT 部門に要求する必要があります。アクセス権が付与されたら、登録用電子メールを受け取ることになります。その電子メールには、Access モバイル クライアントの使用を開始するために必要な情報および手順が示されています。

Access モバイル クライアントが集中管理されずに Acronis Access サーバーへのアクセスが許可されている場合、Acronis Access サーバー名、ユーザー名、およびパスワードを入力するだけで使用を開始できます。

管理登録招待メールを送信した各ユーザーは、次の情報が含まれる電子メールを受け取ります。

- Apple App Store から Access モバイル クライアントをインストールするためのリンク
- Access モバイル クライアント アプリケーションを起動し、登録処理を自動化するために使用するリンク
- ワンタイム PIN コード
- 管理サーバーのアドレス



- 電子メールの指示に従って、Access モバイル クライアントをインストールし、登録情報を入力します。

From: Access Administrator <pam@glilabs.com>  
Subject: Acronis Access へようこそ  
Date: February 12, 2014 9:57:12 AM

[Hide](#)

pam@glilabs.com

会社によって提供されているモバイル ファイル管理アプリケーション Acronis Access へのアクセス権が付与されました。

この電子メールには、Acronis Access アプリケーションのセットアップ手順が記載されています。以下の PIN コードは、1 台のデバイスで Acronis Access をアクティブにするために使用できます。これらの手順を完了する前に、ネットワークへのアクセスがあることを確認してください。

1. Acronis Access アプリをまだインストールしていない場合、今すぐインストールしてください。

Acronis Access for iOS をインストールするにはここをタップしてください (iPad、iPhone、iPod Touch)  
Acronis Access for Android をインストールするにはここをタップしてください

2. 登録プロセスを次の手順で行います。

iOS の場合:

1. このリンクをタップして登録を自動的に開始するか、次の手順を実行して手動で登録してください。
2. Acronis Access アプリを起動して、ようこそ画面で [今すぐ登録] をタップします。
3. ようこそ画面が表示されない場合は、[設定] アイコン、[登録] ボタンの順にタップします。
4. 以下の情報を入力します。

Android の場合:

1. このリンクをタップして登録を自動的に開始するか、次の手順を実行して手動で登録してください。
2. Acronis Access アプリを起動して、デバイスで [メニュー] ボタンをタップします。
3. [設定] を選択して、[今すぐ登録] をタップします。
4. 以下の情報を入力します。

PIN: PEMA77NC

サーバー アドレス: 192.168.1.72:3000

ユーザー名: pam@glilabs.com

パスワード: 会社のパスワードを入力

登録 PIN は 2014/02/22 16:31:17 に期限切れになります。

3. [登録] ボタンをタップします。

4. セキュリティ ポリシーで要求されている場合、アプリケーション ロック パスワードの作成を指示するプロンプトが表示されます。このパスワードは、Acronis Access アプリを起動するときに入力する必要があります。

これらの手順を完了すると、利用可能なサーバーとフォルダが Acronis Access に表示されます。

Acronis Access の使い方については、『Acronis Access Client ユーザー ガイド』を参照してください。

これ以上のサポートについては、IT 部門にお問い合わせください。

Access モバイル クライアントが既にインストールされていて、デバイスでこの電子メールを表示している間にユーザーが [自動的に登録を開始するにはこのリンクをタップ...] オプションをタップした場合、Acronis Access が自動的に起動し、登録フォームが表示されます。ユーザーのサーバーアドレス、PIN コード、およびユーザー名もこの URL でエンコードされているため、登録フォーム内のこれらのフィールドは自動的に入力されます。この時点で、ユーザーがパスワードを入力するだけで登録処理が完了します。

必要なユーザー名とパスワードは、ユーザーの Active Directory のユーザー名とパスワードです。これらのログイン情報は、ゲートウェイ サーバーへのアクセスのために適切なユーザーまたはグループの管理ポリシーを照合するのに使用され、また、Acronis Access サーバー ログインのためのログイン情報を保存するため (管理ポリシーで許可されている場合) に使用されます。

管理ポリシーでアプリケーション ロック パスワードが必須になっている場合は、パスワードを入力するように要求するメッセージが表示されます。この初期パスワードの設定時および将来のアプリケーション ロック パスワードの変更時には、ポリシーで設定されているすべてのパスワードの複雑さの要件を満たす必要があります。

デバイスにローカルでファイルを保存することがポリシーで制限されている場合は、既存のファイルが削除されることを示す警告が表示され、削除する前に操作する必要があるファイルがある場合は、管理設定処理をキャンセルすることができます。



## 管理に登録するには

### 登録用電子メールを使った自動登録

1. IT 管理者から送信された電子メールを開き、Acronis Access をまだインストールしていない場合は「**Acronis Access をインストールするにはここをクリック**」というリンクをクリックします。
2. Acronis Access がインストールされたら、デバイスで招待メールに戻り、電子メールの手順 2 の「**自動的に登録を開始するにはこのリンクをクリック**」をタップします。
3. 登録フォームが表示されます。招待メール内のリンクを使用して登録処理を開始する場合は、サーバーのアドレス、PIN コード、およびユーザー名は自動的に入力されます。

---

**注記:** サーバーで PIN コードが不要な場合は、登録フォームに表示されません。

---

4. パスワードを入力し、**[今すぐ登録]** をタップして続行します。

---

**注記:** ユーザー名とパスワードは会社の標準のユーザー名とパスワードです。これは、コンピュータまたは電子メールにログインするために使用するパスワードと同じ場合があります。

---

5. フォーム全体に入力した後で、**[登録]** ボタンをタップします。
6. 社内のサーバーの設定によっては、管理サーバーのセキュリティ証明書が信頼されていないことを示す警告が表示されることがあります。この警告を受け入れて続行するには、**[常に続行]** をクリックします。
7. Access モバイル クライアント アプリケーションのアプリケーション ロック パスワードが必要な場合は、パスワードを設定するように要求されます。パスワードの複雑性の要件が適用されている場合があります、必要な場合はそれが表示されます。
8. 管理ポリシーで Acronis Access でのファイルの保存が制限されているか Access モバイル クライアント アプリケーション内で個別のサーバーを追加する機能が無効にされている場合、確認ウィンドウが表示されることがあります。Access モバイル クライアント アプリケーションでローカルに保存したファイルがある場合は、**[マイ ファイル]** ローカル ファイル ストレージ内のファイルが削除されることを確認するように要求するメッセージが表示されます。**[いいえ]** を選択すると、管理登録処理がキャンセルされ、ファイルは変更されずに残ります。

### 手動登録

1. Acronis Access アプリケーションを開きます。
2. **[設定]** を開きます。
3. **[登録]** をタップします。
4. サーバーのアドレス、PIN コード(必要な場合)、ユーザー名、パスワードを入力します。
5. フォーム全体に入力した後で、**[登録]** ボタンをタップします。
6. 社内のサーバーの設定によっては、管理サーバーのセキュリティ証明書が信頼されていないことを示す警告が表示されることがあります。この警告を受け入れて続行するには、**[常に続行]** をクリックします。
7. Access モバイル クライアント アプリケーションのアプリケーション ロック パスワードが必要な場合は、パスワードを設定するように要求されます。パスワードの複雑性の要件が適用されている場合があります、必要な場合はそれが表示されます。

管理ポリシーで Acronis Access でのファイルの保存が制限されているか Access モバイル クライアント アプリケーション内で個別のサーバーを追加する機能が無効にされている場合、確認ウィンドウが表示されることがあります。Access モバイル クライアント アプリケーションでローカルに保存したファイルがある場合は、**[マイ ファイル]** ローカル ファイル ストレージ内のファイルが削除

されることを確認するように要求するメッセージが表示されます。[いいえ] を選択すると、管理登録処理がキャンセルされ、ファイルは変更されずに残ります。

## 継続的な管理の更新

初期管理設定の後、Access モバイル クライアントは、アプリケーションが起動されるたびに管理サーバーに接続しようとします。設定変更、サーバーまたはフォルダの割り当ての変更、アプリケーション ロック パスワードのリセット、またはリモート ワイプは、そのときにクライアントに受け入れられます。

---

### 接続要件

Acronis Access クライアントが、プロファイルのアップデート、リモート パスワードのリセット、およびリモート ワイプの指示を受け取るには、Acronis Access サーバーへのネットワーク アクセスが必要です。クライアントが、Acronis Access にアクセスする前に VPN に接続する必要がある場合は、管理コマンドを受け付ける前に VPN に接続する必要があります。

---

## 管理の削除

Access モバイル クライアントを管理から削除する場合、次の 2 つのオプションを使用できます。

- [管理を使用] オプションをオフにする(ポリシーで許可されている場合)
- Access モバイル クライアント アプリケーションを削除する

Acronis Access の管理ポリシーの設定によっては、Access モバイル クライアントを管理から削除する権限が与えられている場合があります。削除すると、通常は社内のファイル サーバーにアクセスできなくなります。この操作が許可されている場合、以下の手順に従ってデバイスを非管理にします。

デバイスを管理するには、次の操作を行います。

1. [設定] メニューをタップします。
2. [管理を使用] オプションをオフにします。
3. デバイスを管理から削除するときに Access モバイル クライアントのデータが必ず消去されるように、プロファイルで指定されている場合があります。消去したくない場合はこの時点で処理をキャンセルできます。
4. 確認ウィンドウで **[はい]** をタップして Acronis Access を管理から削除することを確認します。

---

**注意:** Acronis Access 管理プロファイルでクライアントを非管理にすることが許可されていない場合は、[設定] メニューに [管理を使用] オプションが表示されません。この場合、デバイスを管理から削除するには、Access モバイル クライアント アプリケーションをアンインストールする必要があります。アプリケーションをアンインストールすると、Access モバイル クライアントの既存のデータと設定がすべて消去され、再インストール後にデフォルトのアプリケーションの設定に戻ります。

---

**Access モバイル クライアント アプリケーションをアンインストールするには、次の操作を行います。**

1. Access モバイル クライアント アプリケーションのアイコンが揺れ始めるまでアイコンを指で押し続けます。
2. Access モバイル クライアント アプリケーションの **[X]** ボタンをタップし、アンインストール処理を確認します。

Access モバイル クライアント アプリケーションを再インストールするには、  
<http://www.grouplogic.com/web/meappstore> にアクセスします。

## 7 クイック スタート: 同期と共有

このガイドでは、同期と共有の設定、ウェブ インターフェイスを使ったファイルへのアクセス、および Acronis Access デスクトップ クライアントの使用に関する基本的な手順について説明します。これらのコンポーネントの構成に関する詳細については、「同期と共有」と「デスクトップ クライアント」のセクションを参照してください。

### セクションの内容

|                                     |     |
|-------------------------------------|-----|
| 初期設定 .....                          | 192 |
| ファイルにアクセスするためのウェブ インターフェイスの使用 ..... | 197 |
| デスクトップ クライアントの使用 .....              | 202 |

### 7.1 初期設定

Acronis Access のインストールと構成をまだ行っていない場合は、それを実行します。詳細については、「インストール 『5ページ』」セクションと「設定ユーティリティ 『10ページ』」セクションを参照してください。

ウェブ インターフェイスを初めて開いたときに、デフォルト管理者アカウントのパスワードを設定する必要があり、ログイン後に**セットアップ ウィザード**が表示されます。

**警告:** 管理者パスワードを忘れることがないようにしてください。サポート部門でそのパスワードを復元することはできません。

**注意:** 構成ユーティリティからの起動後、アプリケーションが使用可能になるまでに 30 から 45 秒かかることがあります。

上記の手順が完了すると、下記に示されている初期構成を進める準備が整います。

### 全般設定

#### サーバー設定

|                       |   |
|-----------------------|---|
| サーバー名                 | <input type="text" value="Acronis Access"/>             |
| ウェブ アドレス              | <input type="text" value="https://www.echoserver.com"/> |
| モバイル クライアント登録<br>アドレス | <input type="text" value="www.echoserver.com"/>         |
| カスタム ログを使用            | <input type="checkbox"/>                                |
| 監査ログの言語               | <input type="text" value="日本語"/> ▼                      |

保存

1. [サーバー名] にサーバー名を入力します。
2. ユーザーが(http:// または https:// で始まる)ウェブ サイトにアクセスできる FQDN または IP アドレスを指定します。
3. モバイル ユーザーが登録する FQDN または IP アドレスを指定します。
4. カラー スキームを選択します。現在のオプションは、[灰色]、[紫]、[カプチーノ]、[青]、[濃紺]、および [オレンジ] です。
5. **[監査ログ]** のデフォルトの言語を選択します。現在のオプションは、[英語]、[ドイツ語]、[フランス語]、および [日本語] です。
6. **[保存]** を押します。

## SMTP

### SMTP

Acronis Access サーバーは、構成された SMTP サーバーを使用して電子メールを送信し、ファイルの共有やデバイスの登録のためにユーザーを招待したり、ユーザーや管理者にサーバー アクティビティを通知します。

SMTP サーバー アドレス

myemailserver.mycompany.com

SMTP サーバー ポート

25

セキュリティで保護された  
接続を使用しますか？



差出人名

Access Administrator

差出人電子メール アドレス

adminname@mycompany.com

SMTP 認証を使用します  
か？



保存

テスト用の電子メールの送信

SMTP セットアップのスキップ

**注意:** この手順をスキップして、後で SMTP を構成することもできます。

1. SMTP サーバーの FQDN または IP アドレスを入力します。
2. サーバーの SMTP ポートを入力します。
3. SMTP サーバーの証明書を使用しない場合は、**[セキュリティで保護された接続を使用しますか?]** のチェックを外します。
4. サーバーによって送信される電子メールの「差出人」行に表示されるユーザー名を入力します。
5. サーバーから送信される電子メールのアドレスを入力します。
6. SMTP サーバーでユーザー名やパスワードの認証を使用している場合は、**[認証を使用しますか?]** をチェックし、認証情報を入力してください。
7. **[テスト用の電子メールの送信]** を押して電子メールを手順 5 で指定したテスト用の電子メールアドレスに送信します。
8. **[保存]** を押します。

## LDAP

### LDAP

組織内のユーザーにモバイル アクセス、同期アクセス、および共有アクセスを提供するために、Active Directory への LDAP 接続を使用することができます。LDAP は、管理対象外のモバイル アクセスや、同期および共有サポートに対しては不要ですが、管理対象のモバイル アクセスには必要になります。Microsoft Active Directory への LDAP 接続のみがサポートされています。

LDAP を有効にしますか？ ☒

LDAP サーバー アドレス

LDAP サーバー ポート

セキュリティで保護された  
LDAP 接続を使用します  
か？ ☐

LDAP ユーザー名

LDAP パスワード

LDAP パスワードの確認入  
力

LDAP 検索ベース

LDAP 認証のためのドメイ  
ン

例: mycompany.com。このリストに含まれるドメインの電子メール アドレスを使用しているユーザーは、LDAP に対して認証する必要があります。他のドメインのユーザーは、Acronis Access データベースに対して認証します。

☐ 完全に一致している必要があります

LDAP 情報をキャッシュす  
る間隔

---

**注意:** この手順をスキップして、後で LDAP を構成することもできます。

---

1. **[LDAP を有効にしますか?]** をチェックします。
2. LDAP サーバーの FQDN または IP アドレスを入力します。
3. LDAP サーバーのポートを入力します。
4. LDAP サーバーとの接続に証明書を使用する場合は、**[セキュリティで保護された LDAP 接続を使用しますか?]** をチェックします。
5. LDAP の資格情報をドメインも含めて入力します (例: `acronis%hristo`)。
6. LDAP 検索ベースを入力します。
7. LDAP 認証のドメインを入力します (例えば、電子メール `joe@glilabs.com` のアカウントの LDAP 認証を有効にするには、**glilabs.com** と入力します)。
8. **[保存]** を押します。

## ローカル ゲートウェイ サーバー

### ローカル ゲートウェイ サーバー

Acronis Access のモバイル アプリケーション クライアントは、ゲートウェイ サーバーのアドレスを使用して Access サーバーに接続します。サーバーの設定によっては、デスクトップ同期クライアントおよびウェブ クライアントもこのサーバーに接続されていることがあります。ゲートウェイ サーバーは現在 **192.168.2.129:443** で動作しています。クライアントの接続設定では、接続元となるすべてのネットワークからアクセス可能な DNS アドレスを使用することが推奨されます。クライアントがプロキシ サーバーを経由して接続する場合、このアドレスはプロキシ サーバーの実際の DNS アドレスにすることができます (例: `gateway.mycompany.com`)。

クライアントがサーバーに接続するために使用するアドレス:

192.168.2.129:443

保存

スキップ

---

**注意:** 同じコンピュータにゲートウェイ サーバーと Acronis Access サーバーの両方をインストールする場合、ゲートウェイ サーバーが自動的に検出され、Acronis Access サーバーに管理されます。クライアントがアクセス可能なローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定するように指示するメッセージが表示されます。このアドレスは後から変更できます。

---

1. ローカル ゲートウェイ サーバーの FQDN または IP アドレスを設定します。
2. **[保存]** を押します。



## 7.2 ファイルにアクセスするためのウェブ インターフェイスの使用

### セクションの内容

.....199

1. ウェブ ブラウザを起動して `https://myserver` `https://myserver` に移動します。この **myserver** は Acronis Access サーバーが稼動しているコンピュータの URL または IP アドレスのことです。



The screenshot shows the 'Acronis Access' logo at the top, with 'ADVANCED' in a box below it. The main heading is 'Acronis Access へようこそ' (Welcome to Acronis Access). Below this is the instruction '管理者の初期パスワードを設定してください。' (Please set the administrator's initial password.). There are two input fields: the first is labeled 'パスワード' (Password) and the second is labeled 'パスワードの確認入力' (Confirm password). Both fields have a key icon to the left. At the bottom is a blue button labeled 'パスワードの設定' (Set password).

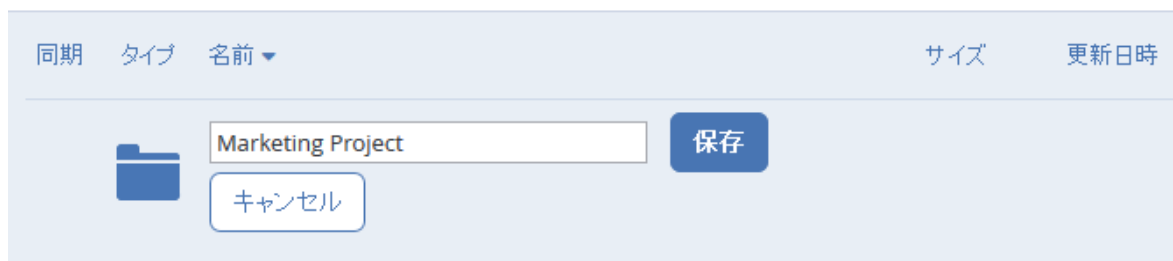
2. 資格情報を指定してログインします。
  - a. Acronis Access サーバーをインストールした直後の場合、インストール プロセス後に設定したパスワードを指定して**管理者**としてログインします。ウェブ インターフェイスを初めて開いた場合は、ここでパスワードを設定するよう要求されます。
  - b. Acronis Access に招待する電子メールを受信した場合は、この時点で**自分のパスワード**を設定するか、Active Directory の資格情報を使用してログインする必要があります。
  - c. 認証およびユーザー アカウント プロビジョニングに Active Directory を使用するように Acronis Access サーバーを設定した場合は、有効なネットワーク資格情報を使用してログインできます。

**注意:** デフォルトの管理者としてログインした場合、ウェブ クライアントへのアクセス権限はありません。デフォルトの管理者以外のアカウントを使用する必要があります。

## フォルダの作成

1. **[フォルダの作成]** ボタンをクリックし、新しいフォルダの名前を入力します。この例では **Marketing Project** を使用します。
2. **[保存]** ボタンを押します。

同期および共有





## ファイルのアップロード

1. 新しいフォルダの名前をクリックしてそのフォルダに移動します。
2. **[ファイルのアップロード]** ボタンをクリックして **[ファイルの追加...]** ボタンをクリックし、コンピュータからファイルを 1 つまたは複数選択します。

ファイルのアップロード



|   |                         |         |   |
|---|-------------------------|---------|---|
|  | AAS7.0bookid_rtm        | 0.00 MB |  |
|  | Acronis Access 7.0.xlsx | 0.01 MB |  |

複数ファイルの選択

完了

3. ユーザーがいるフォルダにファイルがアップロードされます。**[完了]** を押します。

ファイルをアップロードする別の方法は、ファイルをウェブ ページにドラッグ アンド ドロップすることです。

## ファイルのアップロード



アップロードするファイルを選択してください。同時に複数のファイルを選択できます。また、ファイルをここにドラッグ アンド ドロップしてアップロードを開始することもできます。

ファイルの選択

キャンセル

ファイルまたはフォルダをクリックすると、実行できる操作が右のサイドバーに表示されます。



ダウンロード



リビジョン



名前の変更



コピー



移動



電子メールリンク



リンクを取得



削除

## ファイルのダウンロード

ファイルをダウンロードする場合は、ファイル名をクリックします。ファイル名またはフォルダ名の右側の行をクリックし、サイドバーで **[ダウンロード]** を押すことで、ファイルをダウンロードすることもできます。

**注意:** Internet Explorer を使用する場合、ファイルをダウンロードするためには、[暗号化されたページをディスクに保存しない] にチェック マークが付いていない状態にしておく必要があります。この設定は、[インターネット オプション] ' [詳細設定] ' [セキュリティ] にあります。

### ファイルまたはフォルダのコピー

ファイルやフォルダをコピーする場合は、次の操作を実行します。

1. ファイル名またはフォルダ名の右側の行をクリックし、[コピー] を選択します。
2. 新しいライトボックスで、ファイルの貼り付け先のフォルダに移動して [コピー] を押します。

### ファイルまたはフォルダの移動

1. ファイル名またはフォルダ名の右側の行でクリックし、[移動] を選択します。
2. 新しいライトボックスで、ファイルの移動先のフォルダに移動して [移動] を押します。

### フォルダの共有

**注意:** 他のユーザーから共有されたファイルやフォルダを別のユーザーと共有する場合、別のユーザーをその共有に招待するための権限が必要です。別のユーザーを招待する権限がない場合、ファイルとフォルダを他のユーザーと共有することはできません。右のサイドバーの [共有] オプションも表示されません。

同僚や取引先とフォルダを共有するには、次の操作を実行します。

1. フォルダが置かれている場所に応じて、[同期および共有] または [ネットワーク] をクリックします。管理ポリシーによっては、[ネットワーク] タブにアクセスできない場合があります。
2. 共有するフォルダをクリックして、サイドバーから [共有] を選択します。



3. **[共有]** ライトボックスに、電子メール アドレスと適切なテキスト メッセージを入力します。送信者の情報とアクセス手順を含む電子メールが生成され、受信者に送信されます。

## Marketing Project に招待する



メンバーをこのフォルダに招待

frank.burton@glilabs.com

メッセージ(オプション)

Frank, this is the project we are working on. Please make any changes to the included documents as needed.

- ☐ 編集と削除を許可  
☐ 他のメンバーを招待することを許可  
☐ 他のメンバーがこの共有を閲覧することを許可

招待メールの言語 **日本語** ▾

フォルダの共有

キャンセル

**注意:** **[編集と削除を許可]** チェック ボックスを無効にした場合、招待されたユーザーは、共有フォルダに含まれるドキュメントのダウンロードと読み取りしか実行できません。

### 単一ファイルの共有

**注意:** 他のユーザーから共有されたファイルやフォルダを別のユーザーと共有する場合、別のユーザーをその共有に招待するための権限が必要です。別のユーザーを招待する権限がない場合、ファイルとフォルダを他のユーザーと共有することはできません。右のサイドバーの **[共有]** オプションも表示されません。

1. Acronis Access ウェブ インターフェイスを開きます。
2. 管理者アカウントでログインしていた場合、右上隅から **[管理画面を閉じる]** を押します。
3. 目的のファイルを見つけ、ファイル名の隣の行をクリックします。
  - a) **電子メールでのリンクの送信**
    - a. サイドバーから **[リンクの送信]** を選択します。
    - b. 目的の有効期限と、招待に使用する言語を入力します。
    - c. ダウンロード リンクを送信する、ユーザーの電子メール アドレスを入力します。
    - d. **[送信]** を押します。
  - b) **その他の方法でのリンクの送信**
    - a. サイドバーから **[リンクを取得]** を選択します。
    - b. 目的の有効期限と、招待に使用する言語を入力します。
    - c. **[リンクをコピー]** を押します。
    - d. 希望する方法でリンクを共有します。

## 電子メール通知の登録

自分が共有しているフォルダに対して電子メール通知アラートを申し込むことができます。

1. 通知を登録するには、その共有フォルダに移動し、サイドバーで **[通知]** をクリックします。
2. 通知に関する条件を選択し、**[保存]** を押します。

### 通知の管理



デフォルトの通知

共有の通知をカスタマイズ

間隔(分単位)

☐ ファイルがダウンロードされたときに通知する

☐ ファイルおよびフォルダが追加されたときに通知する

☐ ファイルおよびフォルダがアップデートされたときに通知する

☐ ファイルおよびフォルダが削除されたときに通知する

☐ ユーザーが招待または削除されたときに通知する

☐ エラーが発生したときに通知する

保存

すべての共有に適用する

閉じる

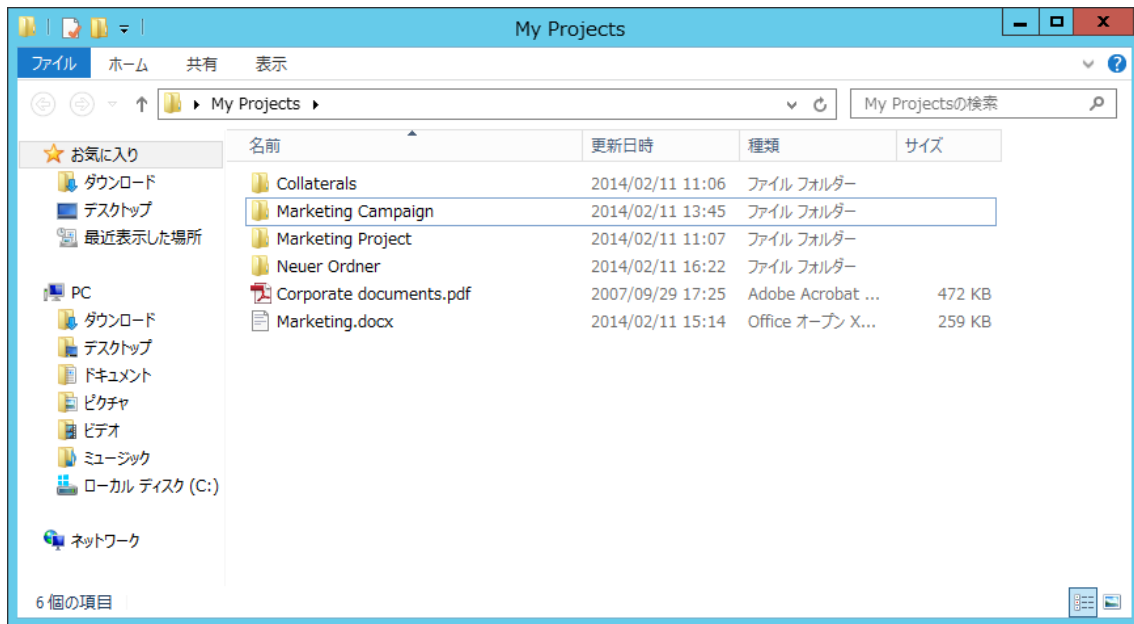
## 7.3 デスクトップ クライアントの使用

### 初期設定

**注意:** Acronis Access デスクトップ クライアントをまだインストールしていない場合は、「クライアントのインストールと設定」のガイドに従ってインストールできます。

1. 構成プロセス中に、同期するために選択したフォルダを開きます。これは通常のフォルダなので、Sync Folder と呼ぶ代わりに、より一般的な名前を使用してください。この例では、**My Projects** という名前を付けました。
2. **Marketing Campaign** という名前のフォルダを **My Projects** 内に作成します。
3. テキスト ドキュメントを **My Projects** 内に作成してテキストを入力し、保存してから閉じます。

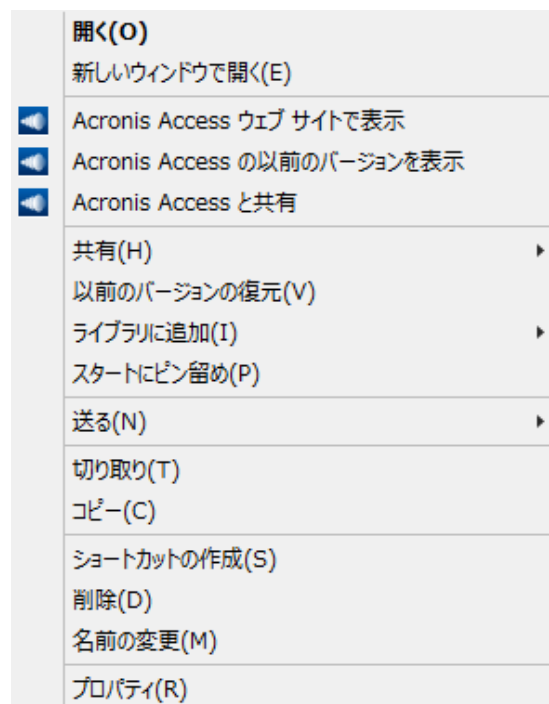
4. **Collaterals** という名前を使用し、**My Projects** 内に別のフォルダを作成します。



5. コンピュータからファイルをコピーし、そのフォルダにファイルを配置します。
6. ここで、フォルダを同僚と共有します。これは、Windows Explorer もしくは他のウェブ ブラウザを使用することで実行できます。Windows Explorer を使用してデスクトップからコンテンツを共有するには、手順 7 を実行します。他のウェブ ブラウザを使用してコンテンツを共有するには、手順 8 を実行します。

**注意:** この記事の最後に記載されている方法で、単一ファイルのみを共有することもできます。

7. これをデスクトップから直接行う場合は、**Marketing Campaign** フォルダを選択します。
- このフォルダを右クリックします。
  - コンテキスト メニューから **[Acronis Access と共有]** を選択します。



- c. ウェブ ブラウザが起動され、招待ダイアログが表示されます。
- d. 電子メール アドレスと適切なテキスト メッセージを [招待] ダイアログに入力します。

### Marketing Project に招待する



メンバーをこのフォルダに招待

frank.burton@glilabs.com

メッセージ(オプション)

Frank, this is the project we are working on. Please make any changes to the included documents as needed.

☐ 編集と削除を許可  
☐ 他のメンバーを招待することを許可  
☐ 他のメンバーがこの共有を閲覧することを許可

招待メールの言語 **日本語** ▼

フォルダの共有

キャンセル

**ウェブ ブラウザを使用する場合は、次の操作を実行します。**

1. <https://server.com/> <https://server.com/> を開きます。**server.com** は Acronis Access サーバーのアドレスを示します。ユーザー名とパスワードの資格情報を使用してログインしてください。
2. フォルダが置かれている場所に応じて、[同期および共有] または [ネットワーク] をクリックします。管理ポリシーによっては、[ネットワーク] タブにアクセスできない場合があります。



3. 共有するフォルダをクリックして、サイドバーから **[共有]** を選択します。



4. **[共有]** ライトボックスに、電子メール アドレスと適切なテキスト メッセージを入力します。送信者の情報とアクセス手順を含む電子メールが生成され、受信者に送信されます。

### Marketing Project に招待する



メンバーをこのフォルダに招待

frank.burton@glilabs.com

メッセージ(オプション)

Frank, this is the project we are working on. Please make any changes to the included documents as needed.

☐ 編集と削除を許可

☐ 他のメンバーを招待することを許可

☐ 他のメンバーがこの共有を閲覧することを許可

招待メールの言語 **日本語** ▼

フォルダの共有

キャンセル

**注意:** **[編集と削除を許可]** チェック ボックスを無効にした場合、招待されたユーザーは、共有フォルダに含まれるドキュメントのダウンロードと読み取りしか実行できません。

他のユーザーの招待に使用された方法に関係なく、受信者は、内部 (Active Directory) ユーザーであるか外部ユーザーであるかに応じて 1 通、または 2 通の電子メールを受信します。

- a. 外部ユーザーの場合、最初の電子メール (件名: 「**Acronis Access** に招待されました」) には、個人用パスワードを設定するためのリンクが含まれます。
- b. 2 通目の電子メール (件名: 「**Marketing Campaign** へのアクセス権が付与されました」) には、送信者のメッセージおよび共有ファイルにアクセスするためのリンクが含まれます。

招待されたユーザーがリンクをクリックしてシステムにアクセスし、必要に応じてパスワードを設定すると、送信者とその同僚は **Marketing Campaign** フォルダのファイルへのアクセスを共有します。

Access デスクトップ クライアントについて同僚に説明し、コンピュータ間でファイルを自動的に同期できるようにしてください。

1. **注意:** Mac OS X と Windows ではパスの最大の長さが異なるため、クロス プラットフォーム展開では同期エラーが発生することがあります。Windows では、「**C:\mysharefolder\**」の部分も含めたパス全体に、合計 260 文字 (MAX\_PATH) という OS 制限がかかります。このため、Windows の場合、ファイル名の最大の長さは、260 - (共有フォルダのパスの長さ) - 1 (NULL ターミネータ) です。

たとえば、ユーザーが C:\my\_shared\_documents を共有していて、C:\my\_shared\_documents\this\_is\_a\_folder\ にファイルをダウンロードしようとしている場合、そのサブディレクトリのファイル名の最大の長さは、260 - 40 - 1 = 219 文字になります。Mac OS X の制限は 1024 文字です。