

Acronis Cyber Files

9.0

管理者ガイド

索引

[

[Files Mobile Gateway] タブ 53

[Files Web サーバー] タブ 52

[ファイルリポジトリ] タブ 54

1

1 人の管理者を招待する 169

A

Acronis Access 証明書の拇印の取得 323

Acronis Cyber Files Web サーバーとゲートウェイデータベースの移行 217

Acronis Cyber Files Web サーバーのみのインストール 233, 241

Acronis Cyber Files Web サーバーまたは Acronis Cyber Files モバイルゲートウェイのいずれかで、次の手順を実行します。 228

Acronis Cyber Files Web サーバー用の追加の DNS エントリの設定 267

Acronis Cyber Files インスタンスにライセンスを付与するには 57

Acronis Cyber Files クライアント 152

Acronis Cyber Files サーバーと Acronis Cyber Files ゲートウェイの両方として機能する 2 つのサーバーで、次の手順を実行します。 226

Acronis Cyber Files サーバーのインストール 233

Acronis Cyber Files サーバーのホストとなる新しいサーバー上で 219

Acronis Cyber Files サーバーの場合 223, 265

Acronis Cyber Files サーバーの設定 241, 293

Acronis Cyber Files サーバー上 253, 259

Acronis Cyber Files での信頼されたサーバー証明書の使用 280

Acronis Cyber Files のインストール 219

Acronis Cyber Files のクラスタリング 61

Acronis Cyber Files のバックアップと復元 193

Acronis Cyber Files のマルチホーム設定 288

Acronis Cyber Files の移行 211

Acronis Cyber Files の移行は次の手順で実行します。 211

Acronis Cyber Files の管理設定の確認 221

Acronis Cyber Files の新しいバージョンへのアップグレード 62

Acronis Cyber Files の設定 236

Acronis Cyber Files の登録招待メールを生成するには 113

Acronis Cyber Files の同一サーバーの移行 210

Acronis Cyber Files の負荷分散 223

Acronis Cyber Files の要素の説明 189

Acronis Cyber Files モバイルアプリをアンインストールするには、次の操作を行います。 117

Acronis Cyber Files 設定ファイル 64

Acronis ドメインフォレスト内の Cyber Files 261

Acronis の特許取得済みの技術 344

Acronis 異なるマシン上の Cyber Files サーバーとゲートウェイサーバー 256

Acronis 同一マシン上の Cyber Files Web サーバーとゲートウェイサーバー 251

acronisaccess.cfg の編集 303

AcronisCyber Files Web サーバーの SPN の設定 268

AcronisCyber Files にログインできることを確認する 269

AcronisCyber Files のインストール 308

Active Directory グループ 336

Android Enterprise 333

Android 用 Cyber Files アプリ の自動登録 333

Apache Tomcat フォルダ 62

API で Web インターフェースをカスタマイズする 245

C

Chrome の場合 265

CMIS (Content Management Interoperability Services) ボリューム 139

CURL のインストール 245

Cyber Files データベースのバックアップ 193

Cyber Files データベースの復元 196

Cyber Files のインストール 49

D

dataディレクトリのクリーンアップ 298

E

Eメール テンプレート 182

F

Firefox の場合 264-265

H

HTTP モードでの Acronis Cyber Files の実行 302

HTTP モードの制限事項 303

I

IIS を介して証明書の要求を作成する 280

Intune に追加された iOS 用 Cyber Files アプリ 336

iOS 用 Cyber Files アプリ コンテナポリシー 333

IPv6 のセットアップ 322

IPv6 のセットアップ手順 1

 ゲートウェイのセットアップ 322

IPv6 のセットアップ手順 2

 Acronis Cyber Files Server 327

IPv6 のセットアップ手順 3

 Strict Transport Security (HSTS) 329

iTunes ライブラリでアプリのバンドル ID を検索するには 107

Ivanti AppConnect 対応 Android 用 Cyber Files アプリ 332

Ivanti チェックイン 335

Ivanti による iOS 用 Cyber Files アプリ のアクティブ化 334

Ivanti を使用した Android 用 Cyber Files アプリ 332

Ivanti を使用した iOS 用 Cyber Files アプリ 333

Ivanti (旧 MobileIron) 332

K

Kerberosドメインルックアップの設定 254, 266

Kerberos制約付き委任 276

krb5.conf ファイルの編集 260

L

LDAP 59, 180

LDAP グループ 147

LDAP プロビジョニング 41, 146

LDAP プロビジョニングを有効にする 42

M

Mac 用の 1 回限りの構成 265

Microsoft Edge および Google Chrome の場合 263

Microsoft Intune 336

Microsoft フェールオーバークラスター上での Acronis Cyber Files のアップグレード 305

Microsoft フェールオーバークラスター上での Acronis Cyber Files のインストール 308

Mobile Device Management 330

N

New Relic による Acronis Cyber Files の監視 187, 285

New Relic のインストール。New Relic による Acronis Cyber Files の監視 187

O

OneDrive for Business 139

OneDrive for Businessコンテンツへのアクセス 134

OpenSSL を介して証明書の要求を作成する 280

P

PINコードが不要な場合の基本的なURL登録リンクの使用 112

PostgreSQL 11 インストール後の「postgres」アカウントのパスワード変更 301

PostgreSQL Administrator の要件 49

PostgreSQL サーバーコンポーネントのインストール 232

PostgreSQL サーバーの移行 238

PostgreSQL データベース 63

PostgreSQL データベースおよびファイル リポジトリをホストするサーバーの場合、次の手順を実行します。 224

PostgreSQL データベースへのアクセスの構成 239

PostgreSQL のアップグレード 74

PostgreSQL のインストールと構成 232

PostgreSQL の新しいメジャーバージョンへのアップグレード 222

postgresql.conf ファイルを開き、以下の変更を加えます。 240

PostgreSQLデータベースのバックアップ 72

PostgreSQLのストリーミングレプリケーション 294

PostgreSQLの構成とスクリプトの作成 205

S

Safari の場合 265

server.xml ファイルの編集 302

SharePoint 120

SharePoint 2007、2010、2013、2016 のコンテンツへのアクセス 134

SharePoint サイトとライブラリ 138

SharePoint サイト全体またはサブサイトのデータソースの作成 138

SharePoint ライブラリのデータ ソースの作成 138

SharePoint ライブラリ内の特定のフォルダのデータ ソースの作成 139

SharePointの認証方法をサポート 134

SharePointフォローサイト 138

SharePoint設定 127

SMBまたはSharePointデータソースの使用 275

SMSの2要素認証 174

SMTP 58, 179

SPNがゲートウェイ用に正しく設定されたことを確認する 270, 274

SPN登録の確認 274

SSL バインディングの作成 322

SSO（シングルサインオン）サポートのためのブラウザの構成 256, 261-262

SSOを処理するLDAPアカウントの設定 252, 257, 267

Sync & Share 143

Sync & Share ユーザーのタイプ 158

Sync&Shareデータソース 38

T

Tomcat サーバーの接続許可 232

Tomcat/ゲートウェイ/PostgreSQL が現在稼働している元のサーバーで、次の手順を実行します。 217

Tomcatのインストール 289

W

Web インターフェースでのシングルサインオンの有効化 267

web.xml ファイルの編集 259

Windows 2012（R2）Microsoft フェールオーバークラスター上での Acronis Cyber Files のインストール 308

Windows での Tomcat ログ管理 198

Windows 証明書ストアへの証明書のインストール 281

Windows 用の 1 回限りの構成 263

あ

アーカイブされたApache Tomcatインストールの使用 291

アカウントにすべて読み取り許可を与えるには（SharePoint 2016 および SharePoint 2010 の場合） 128

アクセス権なしユーザーアカウント 160

アクセス権の構成 295

アクティブ ユーザー 122

アップグレード 62, 65

アップグレード前のデータベースのバキューム 64

アプリがインストールされ、Cyber Files サーバーに登録されました 334

アプリがインストールされていない 335

アプリケーション パスワードのリセット 156

アプリケーションのバンドル ID の確認 107

アプリケーションポリシー 93

アプリはインストールされており、Cyber Files サーバーに登録されていません 334

アプリ設定ポリシー 339

アプリ保護ポリシー 338

い

インスタンスの移行 300

インストーラの使用 29

インストーラ配布ポイントの作成 247

インストール 29, 43

インストール実行可能ファイルの使用 289

う

ウェブUIのカスタマイズ 176

ウェブインターフェイスでのシングルサインオンの有効化 255, 261

ウェブクライアントとデスクトップクライアント 42

ウェブクライアントユーザーのFile Serversなどへのアクセスの許可 40

ウェブのプレビューサーバレットの負荷分散 293

ウェブのプレビューと編集 177

お

オペレーティングシステムの一部として機能するユーザーの選択 277

オペレーティングシステム要件 43

か

カスタム ロゴの使用 176

カスタムアクセス制限 132

カスタムカラースキームの作成 245

カスタムクォータを設定するには、次の手順を実行します。 162

カスタムのようにこそメッセージを使用する 176

カラー スキームの使用 177

く

クイック スタート 29

クォータ 147

クライアントガイド 38, 42

クライアントで表示されるゲートウェイ サーバー 141

クライアントのインストール 248

クライアントの無人インストール 247

クライアント証明書認証でモバイルクライアントを使用する 275

クラスターグループ 132

クラスターグループの編集 133

クラスターグループを作成するには、次の手順を実行します。 133

グループ ポリシーを変更するには、次の操作を行います。 89

け

ゲートウェイ サーバー データベース 64

ゲートウェイ サーバーのアップグレード 68, 81

ゲートウェイ サーバーの管理 117

ゲートウェイ クラスターのアップグレード 67

ゲートウェイサーバーが Acronis Cyber Files Web サーバーとは異なるマシンに存在する場合 256, 272

ゲートウェイサーバーが Acronis Cyber Files サーバーとは異なるマシンに存在する場合 258

ゲートウェイサーバーが Acronis Cyber Files サーバーと同じマシンに存在する場合 258

ゲートウェイサーバーデータベースの復元 220

ゲートウェイサーバーのSPNの設定 253, 258, 269, 278

ゲートウェイサーバーのインストール 235

ゲートウェイサーバーのサービスを選択したユーザーアカウントとして実行する 278

ゲートウェイサーバーのデータベースのバックアップ 73, 195

ゲートウェイサーバーのデータベースの復元 197

ゲートウェイサーバーのログ 124

ゲートウェイサーバーの移行 243

ゲートウェイサーバーの検索オプション 118, 125

ゲートウェイサーバーの追加 255, 272

ゲートウェイサーバーの追加DNSエントリの構成 269

ゲートウェイサーバー構成 123

ゲートウェイサーバー上 269

ゲートウェイサーバー用に新しいライセンスを追加する必要はありません 185

ゲートウェイサービスがユーザーアカウントとして実行するように設定する 273

こ

このPostgreSQLインスタンスへのリモートアクセスを有効にするには、次の手順を実行してください
300

このヘルプの使用 26

コンセプト 85

さ

サーバー 173

サーバー ポリシー 102

サーバーの管理 167

サーバーの現在の割り当てを編集するには 141

サーバーの詳細 122

サーバーの設定 173, 233, 241

サーバーへの Acronis Cyber Files のインストール 49

サーバー側の管理登録処理 111

サービスがユーザーアカウントとして実行している 285

サービスがローカルシステムアカウントとして実行している 284

サブレットのインストールと構成 289

サポートされるオペレーティングシステム 48

サポートされるモバイルデバイス 44

サポート対象 43

サポート対象ウェブブラウザ 48

し

システム要件 48, 231, 237

シングルサインオンのトラブルシューティング 279

シングルサインオンの設定 250

シングルサインオン認証で使用するドメインアカウントの構成 265

シングルサインオン認証で使用するドメインアカウントの設定 253

す

スクリプトの作成 206

スケジュール タスクの作成 204

スタンバイサーバー上 296

ステータス 122

ストリーミングレプリケーション 294

ストリーミングレプリケーションの構成 295-296

ストリーミングレプリケーションの制御 298

すべてのマシン上のすべての Acronis Cyber Files サービスを停止します。 74

せ

セキュリティ ポリシー 90

セットアップ ウィザードの使用 55

セットアップウィザードに進む 55

そ

その他の Acronis Cyber Files サーバーの接続 241

その他のバックアップ対象ファイル 195, 218

その他のファイルとカスタマイズの復元 197

その他の構成 120, 126

その他の重要なコンポーネントのバックアップ 73

その他の要件 48

ソフトウェアの競合 223

た

- タスクが実行可能なことの確認 205
- タスクスケジューラの設定 207
- タスクの想定どおりの動作を確認 209

て

- データソースの管理 134
- データソースの作成 140
- データソースの作成と編集 136
- データソースの編集 138
- データベース バックアップ スクリプトの作成 203
- データベースのインポート 240
- データベースのバキューム 71
- データベースのバキューム処理や分析を手動で行うには、次の手順を実行します。 192
- データベースの自動バキューム 205
- データベースの自動バックアップ 203
- デスクトップ クライアントの無人設定 247
- デスクトップクライアント要件 48
- デバイスに関するデータのエクスポート 156
- デバイスの管理 155
- デバイスの登録に必要なもの 142
- デバイスポリシー 337
- デバイスを管理するには、次の操作を行います。 116
- デバイス上のファイルを参照することによるアプリケーションのバンドル ID の確認 107
- デバイス登録モード 111
- デバッグ ログ 185
- デフォルト パス 119, 126
- デフォルト ポリシーの設定 36
- デフォルトのアクセス制限 108
- デフォルト以外のロケーションへの FileStore の移動 284

デプロイサンプル 44

デモモードでアプリを試用する 37

と

ドメイン上 251, 256

トラブルシューティング 246

ね

ネットワークノードの有効化 277

ネットワーク接続 232, 237

ネットワーク要件 46

は

ハードウェア要件 231, 237

はじめに 28, 189

ふ

ファイル リポジトリ 60, 151

ファイルストアとファイルリポジトリの移行 243

ファイルストアとファイルリポジトリの設定 235

ファイルの最大サイズを設定するには、次の手順を実行します。 144

ファイルの種類のブロックリストを設定するには、次の手順を実行します。 144

ファイルリポジトリサービスのインストール 235

ファイルリポジトリのアップグレード 78

ファイル消去ポリシー 148

ファイル名検索のローカル データ ソースのインデックスを作成 119, 126

フェイルオーバーのテスト 299

フォルダ 135

フォルダおよびレジストリ エントリの作成 249

フォルダの共有 146

フォルダの同期 136

プライマリ Cyber Files サーバーのアップグレード 80

プライマリサーバー上 295

ブロックリスト 146

ブロック対象のパスのリストの作成 104

プロビジョニング済み LDAP 管理者グループ 168

プロビジョニング済みの LDAP 管理者グループを追加するには 168

ほ

ホームフォルダ 100

ポリシー 87

ポリシーの設定 90

ポリシーの変更 89

ポリシー設定の例外 104

ま

マスターゲートウェイサーバーの変更 134

マルチホームの設定 288

め

メンテナンス タスク 189

も

モバイル アクセス 36, 85

モバイル クライアントの要件 44

モバイル デバイスの登録 110

モバイルアプリのダウンロード 44

モバイルオペレーティングシステムの最小サポート要件 44

モバイルクライアント 37

ゆ

ユーザー ポリシーまたはグループ ポリシーのブロックリストを有効にするには、次の操作を実行します。 105

ユーザー ポリシーを変更するには、次の操作を行います。 90

ユーザーとそのコンテンツの完全な削除 164

ユーザーとそのコンテンツの削除 163
ユーザーとデバイス 155
ユーザーとのコンテンツの共有 38
ユーザーに管理者権限を付与するには 170
ユーザーに関するデータのエクスポート 161
ユーザーのコンピュータへのインストーラの保存 247
ユーザーの管理 158
ユーザーへの登録招待 112
ユーザー期限切れポリシー 149
ユーザー側の管理登録処理 114

ら

ライセンス 56, 184

り

リストで利用できるアプリの追加 106
リストを作成するには、次の操作を実行します。 104
リソーススペースのKerberos制約付き委任 276
リソーススペース制約付き委任の設定 271
リモート アプリケーション パスワード リセットの実行 156
リモートアクセス用PostgreSQLの構成 300
リモートゲートウェイサーバーのSPNの構成 274
リモートデータベースへの Acronis Cyber Files の接続 243
リモートワイプの実行 157

れ

レプリケーションスロットの作成 296, 298
レプリケーションユーザーの作成 295

ろ

ローカル ゲートウェイ サーバー 60
ローカルゲートウェイサーバーのSPNの構成 270

ロードバランシング 61

ロードバランス設定のアップグレード 69

ログ 171

ログの管理と消去 244

漢字

安全でない TLS バージョンを使用した Acronis Cyber Files Tomcat の実行 304

以下の手順を実行してください 301

以前のゲートウェイサーバーのすべての設定の移行 244

一般制限事項 143

運用例 191

会社のサーバーに登録するには 37

開始する前に 70, 216

外部（アドホック）ユーザーアカウント 159

外部（アドホック）ユーザーの追加 161

割り当て済みのソース 140

監査ログ 171

監視 187

管理の削除 116

管理ページのアクセス制限 167

管理ユーザー 169

管理者と権限 167

管理者の固有の権限を付与するには 170

管理者権限 170

管理対象アプリ構成（AppConfig） 330

既存の PostgreSQL サーバー上での構成 238

既存のクラスターグループにメンバーを追加するには、次の操作を実行します。 134

既知の問題 342

期限切れのユーザーアカウントのコンテンツはどうなりますか？ 150

許可されたアプリ 105

許可リスト 146

共有の制限 145

共有ファイルおよびフォルダの許可の変更 135

継続的な管理の更新 116

元のサーバーのクリーンアップ 221, 245

現在の構成に関し、次の重要な事項に注意してください。 70

古い Acronis Cyber Files サーバーの接続 243

古いバージョン用のドキュメント 343

構成ファイルのバックアップ 297

構成ファイルの復元 298

構成ユーティリティの概要 51

最小ハードウェア要件 44

最大スレッド数の構成 234, 242

災害復旧ガイドライン 189

削除されたユーザーのコンテンツの他のユーザーへの再割り当て 165

残りのすべてのノードのアップグレード 83

試用版を開始するには 56

手順 190

手順 1

 PostgreSQL をアンインストールする 74

手順 2

 新しいバージョンの PostgreSQL をインストールする 76

手順 3

 DB コンテンツをインポートする 78

重要なコンポーネントのバックアップ 62

初期シーディング 298

初期構成プロセスを進める 55

初期設定 30

小規模デプロイ 45

証明書の要求の作成 280

証明書を使用するように Cyber Files を設定する 282

詳細設定 130

新しい PostgreSQL サーバー上 240

新しい PostgreSQL サーバー上での構成 239

新しいグループ ポリシーを追加するには 88

新しいゲートウェイ サーバーの登録 120

新しいゲートウェイサーバーのインストール 235, 243

新しいサーバーの設定 220

新しいポリシーの追加 88

新しいユーザー ポリシーを追加するには 88

新しいライセンスの追加 185

新しい構成のテスト 215, 221

新機能 341

迅速な復旧プロセスの実装に必要なリソース 190

推奨 43

設定 141, 172

設定ユーティリティの使用 30, 51

選択したユーザーに必要な権限を付与する 273

全般設定 57, 123

対象のドメインのマシンにゲートウェイサーバーをインストールする 273

大規模デプロイ 46

単一ファイル共有の有効期限 145

中間証明書の使用 283

中規模デプロイ 45

著作権情報 343

追加のTomcatコネクタの構成 287

追加情報 299

通常導入のオンライン化 197

通知の設定 174

適切なデータベースに接続するようサーバーを構成する 234, 241

適切なロギングの構成 234, 242

適切な接続数のセットアップ 233

登録設定 111, 142

同一サーバーの移行プロセスの基本概要 210

同一サーバーの移行を開始する前に 210

同期・共有 38

同期ポリシー 99

特定の IPv6 アドレスの iplisten リストへの追加 323

特定のゲートウェイサーバーのカスタムアクセス制限の設定 132

内部 (LDAP) ユーザーアカウント 159

内部 (LDAP) ユーザーの追加 162

必要なすべてのサーバーの相互アクセスの確認 296

不要な監査ログの消去 63

負荷分散コンポーネントのバックアップ 72

負荷分散環境 277

負荷分散型セットアップでの Acronis Cyber Files のインストール 231

負荷分散構成への移行 236

負荷分散装置での作業 230

負荷分散装置固有の設定 236, 244

負荷分散導入のオンライン化 197

復元した Cyber Files サーバーのテスト 197

複数のウェブプレビューサーブレットのデプロイ 288

複数のデスクトップクライアントバージョンのサポート 283

複数のポートでの Acronis Cyber Files Tomcat の実行 286

別のサーバーへの Acronis Cyber Files の移行 216

別のドメインにあるゲートウェイサーバーの構成 272

補足資料 223

役割の作成 309

要件 43, 118, 125, 262, 294

利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート 119, 126

両方のシナリオの要件 289

目次

索引	2
このヘルプの使用	26
はじめに	28
クイック スタート	29
インストール	29
インストーラの使用	29
設定ユーティリティの使用	30
初期設定	30
モバイル アクセス	36
デフォルト ポリシーの設定	36
モバイルクライアント	37
クライアントガイド	38
同期・共有	38
Sync&Shareデータソース	38
LDAP プロビジョニング	41
ウェブクライアントとデスクトップクライアント	42
クライアントガイド	42
インストール	43
要件	43
オペレーティングシステム要件	43
モバイル クライアントの要件	44
最小ハードウェア要件	44
ネットワーク要件	46
デスクトップクライアント要件	48
PostgreSQL Administrator の要件	49
サーバーへの Acronis Cyber Files のインストール	49
Cyber Files のインストール	49
設定ユーティリティの使用	51
構成ユーティリティの概要	51
セットアップウィザードに進む	55
セットアップウィザードの使用	55
初期構成プロセスを進める	55
Acronis Cyber Files のクラスタリング	61
ロードバランシング	61
アップグレード	62

Acronis Cyber Files の新しいバージョンへのアップグレード	62
重要なコンポーネントのバックアップ	62
アップグレード前のデータベースのバキューム	64
アップグレード	65
ゲートウェイクラスタのアップグレード	67
ゲートウェイ サーバーのアップグレード	68
ロードバランス設定のアップグレード	69
開始する前に	70
負荷分散コンポーネントのバックアップ	72
PostgreSQL のアップグレード	74
ファイルリポジトリのアップグレード	78
プライマリ Cyber Files サーバーのアップグレード	80
ゲートウェイ サーバーのアップグレード	81
残りのすべてのノードのアップグレード	83
モバイル アクセス	85
コンセプト	85
ポリシー	87
新しいポリシーの追加	88
ポリシーの変更	89
ポリシーの設定	90
ブロック対象のパスのリストの作成	104
許可されたアプリ	105
デフォルトのアクセス制限	108
モバイル デバイスの登録	110
サーバー側の管理登録処理	111
ユーザー側の管理登録処理	114
ゲートウェイ サーバーの管理	117
ゲートウェイサーバーの検索オプション	118
SharePoint	120
新しいゲートウェイ サーバーの登録	120
サーバーの詳細	122
ゲートウェイサーバー構成	123
カスタムアクセス制限	132
クラスターグループ	132
データソースの管理	134
SharePoint 2007、2010、2013、2016 のコンテンツへのアクセス	134
OneDrive for Businessコンテンツへのアクセス	134

共有ファイルおよびフォルダの許可の変更	135
フォルダ	135
割り当て済みのソース	140
クライアントで表示されるゲートウェイ サーバー	141
設定	141
登録設定	142
デバイスの登録に必要なもの:	142
Sync & Share	143
一般制限事項	143
ファイルの種類のブロックリストを設定するには、次の手順を実行します。	144
ファイルの最大サイズを設定するには、次の手順を実行します。	144
共有の制限	145
単一ファイル共有の有効期限	145
フォルダの共有	146
許可リスト	146
ブロックリスト	146
LDAP プロビジョニング	146
LDAP グループ	147
クォータ	147
ファイル消去ポリシー	148
ユーザー期限切れポリシー	149
期限切れのユーザーアカウントのコンテンツはどうなりますか？	150
ファイル リポジトリ	151
Acronis Cyber Files クライアント	152
ユーザーとデバイス	155
デバイスの管理	155
デバイスに関するデータのエクスポート	156
リモート アプリケーション パスワード リセットの実行	156
リモートワイプの実行	157
ユーザーの管理	158
Sync & Share ユーザーのタイプ	158
外部（アドホック）ユーザーの追加	161
内部（LDAP）ユーザーの追加	162
カスタムクォータを設定するには、次の手順を実行します。	162
ユーザーとそのコンテンツの削除	163
サーバーの管理	167
サーバーの管理	167

管理者と権限	167
管理ページのアクセス制限	167
プロビジョニング済み LDAP 管理者グループ	168
管理ユーザー	169
管理者権限	170
監査ログ	171
ログ	171
設定	172
サーバー	173
サーバーの設定	173
通知の設定	174
SMSの2要素認証	174
ウェブUIのカスタマイズ	176
カスタム ロゴの使用	176
カスタムのようこそメッセージを使用する	176
カラー スキームの使用	177
ウェブのプレビューと編集	177
SMTP	179
LDAP	180
Eメール テンプレート	182
ライセンス	184
新しいライセンスの追加	185
ゲートウェイサーバー用に新しいライセンスを追加する必要はありません	185
デバッグ ログ	185
監視	187
New Relic のインストール。New Relic による Acronis Cyber Files の監視	187
New Relic による Acronis Cyber Files の監視	187
メンテナンス タスク	189
災害復旧ガイドライン	189
はじめに:	189
Acronis Cyber Files の要素の説明:	189
迅速な復旧プロセスの実装に必要なリソース	190
手順	190
運用例	191
Acronis Cyber Files のバックアップと復元	193
Cyber Files データベースのバックアップ	193

ゲートウェイサーバーのデータベースのバックアップ	195
その他のバックアップ対象ファイル	195
Cyber Files データベースの復元	196
ゲートウェイサーバーのデータベースの復元	197
その他のファイルとカスタマイズの復元	197
復元した Cyber Files サーバーのテスト	197
Windows での Tomcat ログ管理	198
データベースの自動バックアップ	203
データベース バックアップ スクリプトの作成	203
スケジュール タスクの作成	204
データベースの自動バキューム	205
PostgreSQLの構成とスクリプトの作成	205
タスクスケジューラの設定	207
Acronis Cyber Files の同一サーバーの移行	210
同一サーバーの移行を開始する前に	210
Acronis Cyber Files の移行	211
新しい構成のテスト	215
別のサーバーへの Acronis Cyber Files の移行	216
開始する前に	216
Acronis Cyber Files Web サーバーとゲートウェイデータベースの移行	217
その他のバックアップ対象ファイル	218
新しい構成のテスト	221
元のサーバーのクリーンアップ	221
PostgreSQL の新しいメジャーバージョンへのアップグレード	222
補足資料	223
ソフトウェアの競合	223
Acronis Cyber Files サーバーの場合	223
Acronis Cyber Files の負荷分散	223
負荷分散型セットアップでの Acronis Cyber Files のインストール	231
負荷分散構成への移行	236
適切なデータベースに接続するようサーバーを構成する	241
最大スレッド数の構成	242
適切なロギングの構成	242
API で Web インターフェースをカスタマイズする	245
デスクトップ クライアントの無人設定	247
シングルサインオンの設定	250
Microsoft Edge および Google Chrome の場合	263

Firefox の場合	264
Safari の場合	265
Firefox の場合	265
Chrome の場合	265
Acronis Cyber Files Web サーバー用の追加の DNS エントリの設定	267
AcronisCyber Files Web サーバーの SPN の設定	268
AcronisCyber Files にログインできることを確認する	269
ゲートウェイサーバーの追加DNSエントリの構成	269
ローカルゲートウェイサーバーのSPNの構成	270
対象のドメインのマシンにゲートウェイサーバーをインストールする	273
ゲートウェイサービスがユーザーアカウントとして実行するように設定する	273
選択したユーザーに必要な権限を付与する	273
リモートゲートウェイサーバーのSPNの構成	274
Acronis Cyber Files での信頼されたサーバー証明書の使用	280
複数のデスクトップクライアントバージョンのサポート	283
デフォルト以外のロケーションへの FileStore の移動	284
New Relic による Acronis Cyber Files の監視	285
複数のポートでの Acronis Cyber Files Tomcat の実行	286
Acronis Cyber Files のマルチホーム設定	288
複数のウェブプレビューサブリットのデプロイ	288
PostgreSQLのストリーミングレプリケーション	294
リモートアクセス用PostgreSQLの構成	300
PostgreSQL 11 インストール後の「postgres」アカウントのパスワード変更	301
HTTP モードでの Acronis Cyber Files の実行	302
安全でない TLS バージョンを使用した Acronis Cyber Files Tomcat の実行	304
Microsoft フェールオーバークラスター上での Acronis Cyber Files のアップグレード	305
Microsoft フェールオーバークラスター上での Acronis Cyber Files のインストール	308
IPv6 のセットアップ	322
Mobile Device Management	330
管理対象アプリ構成 (AppConfig)	330
Ivanti (旧 MobileIron)	332
Microsoft Intune	336
新機能	341
既知の問題	342
古いバージョン用のドキュメント	343

このヘルプの使用

このヘルプは、表示に使用しているデバイスに応じて動的に調整されます。

デスクトップデバイスとラップトップ

コンテンツに移動

デスクトップデバイスやラップトップでは、デフォルトでナビゲーションペインが展開され、[内容] タブが選択されています。これにより、トピックの階層を表示してコンテンツに移動することができます。

コンテンツの確認中にナビゲーションペインを折りたたむには、ペインの上部にあるをクリックします。

ペインが折りたたまれ、画面の左側に展開ボタン () が表示されます。

索引と用語集

索引と用語集は、左側のナビゲーションペインに個別のタブで表示されます。

検索

右上にある検索では、トピックのコンテンツのみが検索対象となります。索引と用語集を検索するには、タブを切り替えてタブ検索を使用します。

モバイル デバイス

コンテンツに移動

小型デバイスでは、デフォルトでナビゲーションペインが折りたたまれた状態で、ウェルカムページが表示されます。右上の矢印を使用して、前後のトピックに移動できます。

目次を表示するには、左上のメニューボタンをクリックし、[内容] を選択します。

索引と用語集

索引と用語集には、画面左上のメニューからアクセスできます。

検索

メイン検索では、トピックのコンテンツのみが検索対象となります。索引と用語集を検索するには、左上のメニューでタブを切り替えてタブ検索を使用します。

検索では、大文字と小文字が区別されません。

特定のフレーズを検索するには、フレーズを引用符で囲みます。複数の単語を引用符なしで検索した場合、ブール演算子のANDとして解釈されます。たとえば、"backup schedule"で検索した場合、検索結果には「backup schedule」というフレーズを含むトピックが、大文字と小文字を区別せずに表示されます。backup scheduleで検索する場合は、検索結果は「backup AND schedule」と同じになります。この場合検索結果には、「backup」と「schedule」の両方の単語を含むすべてのトピックが表示されます。ロケーションによる限定はありません。

一部の単語は検索できません。

ブール演算子を使って、検索結果を絞り込んだり、拡張したりすることができます。

- AND - 列举されたすべての単語を含むトピックのみを検索します。単語間にスペースが挿入されている場合、検索クエリを引用符で囲まない限り、常にANDと解釈されます。引用符を使用することで、フレーズを検索できます。
- OR - 列举されたいずれかの単語を含むトピックを検索します。この演算子により、検索結果が拡張されます。

ブール演算子では、大文字と小文字は区別されません。たとえば、検索クエリとしてANDやandを使用しても、検索結果に影響はありません。

はじめに

このガイドでは、Acronis Cyber Files 管理者向けのドキュメントを提供します。

Cyber Files の概要

Cyber Files は、セキュアアクセス、同期、および共有のソリューションです。このソリューションにより、エンタープライズの IT 部門はビジネス コンテンツを完全に制御でき、セキュリティの確保、コンプライアンスの遵守、BYOD の導入を実現できます。Cyber Files により、従業員は、デスクトップ、ラップトップ、タブレット、スマートフォンなど、あらゆるデバイスを使用してコンテンツに安全にアクセスし、また、同僚、顧客、パートナー、ベンダーなど社内外の承認された個人とコンテンツを共有できます。

Cyber Files の機能は、2つのカテゴリに分けることができます。

モバイルデバイスアクセス

モバイルデバイスアクセスにより、企業の IT 部門は、社内のファイルサーバー、SharePoint デバイス、および NAS デバイスへのシンプルでセキュアな管理されたアクセスをモバイルデバイスユーザーに提供できるようになります。IT 部門では、リスクを伴う消費者ベースのサービスやその他のコンプライアンス違反のサービスを従業員が利用しようとすることから生じる問題がなくなります。

IT 部門で Cyber Files を利用すれば、モバイルデバイスユーザーによるコンテンツへのアクセスをセキュリティで保護し統制しながら、業務に必要なコンテンツ、ファイル、資料へのアクセスを提供できるようになります。

注意

モバイルデバイスアクセスの詳細については、次のドキュメントを参照してください。

- [デスクトップおよびウェブクライアント](#)
 - [iOSアプリ](#)
 - [Androidアプリ](#)
-

File Sync & Share

Sync & Share 機能は、エンドユーザーによるシンプルさと効果性のニーズと、企業の IT 部門が必要とするセキュリティ、管理の容易さ、柔軟性との間でバランスを維持する業界唯一の企業向けソリューションです。

Cyber Files により、企業の IT 部門は、ファイルにアクセスできるユーザーを管理でき、ファイル共有アクティビティが組織のコンプライアンスとセキュリティの要件を満たしているかどうかを判断できるようになります。Cyber Files では、消費者ベースのソリューションでは提供されないレベルの可視性と監視が可能です。

クイック スタート

このガイドでは、Acronis Cyber Files のインストールおよび実行に関する最も簡単で迅速な方法を紹介します。設定をカスタマイズする場合、本ガイドは実用的ではありません。各コンポーネントの詳細および手順については、マニュアルの該当セクションを確認してください。

インストール

注意

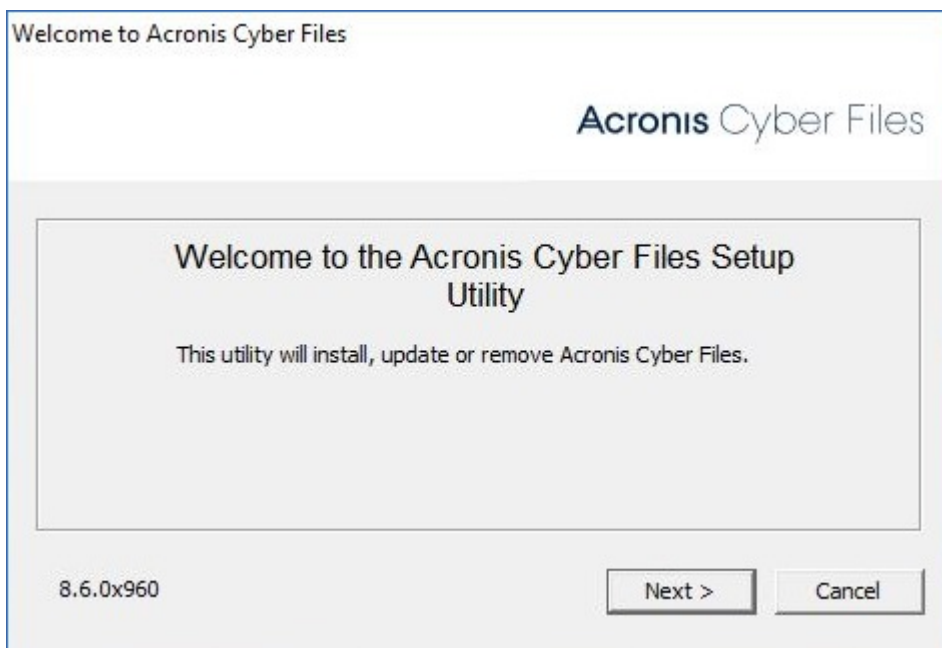
管理者としてログインしていることを確認してから Acronis Cyber Files をインストールしてください。

注意

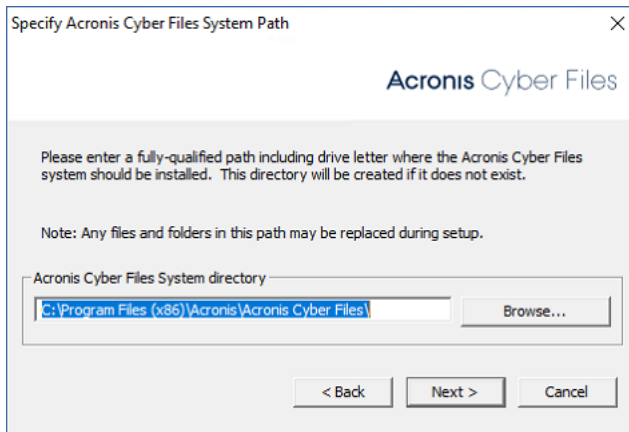
Acronis Cyber Files 8.8 はデフォルトで PostgreSQL 11 と一緒に配布されます。

インストーラの使用

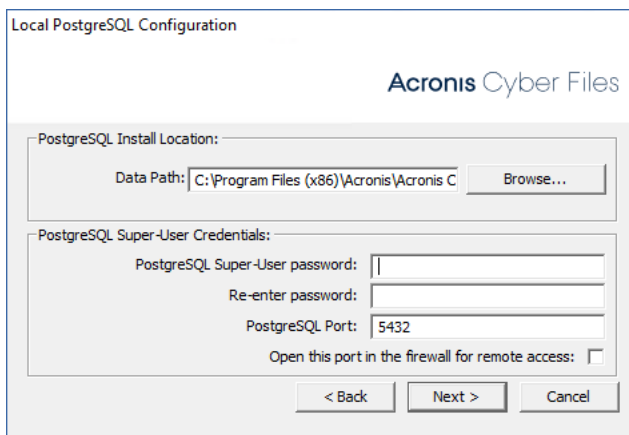
1. Acronis Cyber Files インストーラをダウンロードします。
2. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
3. 実行可能なインストーラをダブルクリックします。



4. **[次へ]** を押して開始します。
5. ライセンス契約を読み、承諾します。
6. **[インストール]** を押します。
7. Acronis Cyber Files のメインフォルダのデフォルトパスを使用する場合は、**[OK]** を押します。



8. ユーザー Postgres 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復旧に必要となります。



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] をクリックしてください。
10. Acronis Cyber Files のインストーラが完了したら、[終了] をクリックします。
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

注意

構成ユーティリティの設定内容は後で変更できます。

各タブでデフォルト値を使用し、[OK] を押して Acronis Cyber Files を起動します。

初期設定

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

構成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。

ネットワークアダプタの IP アドレスおよび目的のポートを使用して、Acronis Cyber Files の Web インターフェースに移動します。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

認証機関からの証明書ではなく、デフォルトの証明書を使用して Acronis Cyber Files を実行すると、サーバーが信頼されていないことを示すエラーが表示されます。

注意

[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](#)」の資料を参照してください。

ライセンス

試用版を開始するには:

[**トライアルを開始**] を選択し、必要な情報を入力して [**続行**] を押します。

☒ Start trial ☐ Enter license key

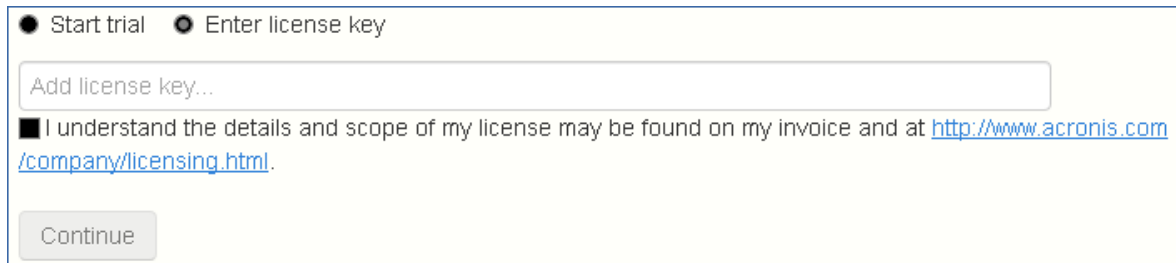
Please register to start using the trial

First Name	John
Last Name	Price
Country	United States ▼
State/province	Washington ▼
Phone	+1000-755-332-12
Select industry	Telecommunication ▼
Company	Neucott Ltd.
Email	jprice@neucott.com

Continue

Acronis Cyber Files インスタンス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、チェックボックスを選択します。



☒ Start trial ☐ Enter license key

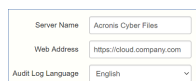
Add license key...

☒ I understand the details and scope of my license may be found on my invoice and at <http://www.acronis.com/company/licensing.html>.

Continue

3. [保存] を押します。

全般設定



Server Name: Acronis Cyber Files

Web Address: https://cloud.company.com

Audit Log Language: English

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 root DNS 名または IP アドレスを指定します。
[監査ログ] のデフォルトの言語を選択します。
3. 現在のオプションは、[英語]、[ドイツ語]、[フランス語]、[日本語]、[イタリア語]、[スペイン語]、[チェコ語]、[ロシア語]、[ポーランド語]、[韓国語]、[中国語 (繁体字)]、[中国語 (簡体字)] です。
4. [保存] を押します。

SMTP

Acronis Cyber Files

SMTP

Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to share or enroll mobile devices, as well as notify users and administrators of server activity.

SMTP Server Address: myemailserver.mycompany

SMTP Server Port: 25

Use secure connection? ☒

From Name: Acronis Cyber Files Admini...

From Email Address: adminname@mycompany.c...

Use only this address for all email notifications ☐

Use SMTP authentication? ☐

Save Send Test Email Skip SMTP Setup

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 DNS 名または 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. サーバーから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、**[SMTP 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、手順5で指定したテスト用の電子メールアドレスに電子メールを送信します。
8. **[保存]** を押します。

LDAP

LDAP

An LDAP connection to your Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Only LDAP connections to Microsoft Active Directory are supported.

Enable LDAP? ☒

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection? ☐

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

e.g. mycompany.com. Users with email addresses whose domains are in this list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.

+ Add

myldap.mydomain.com

Remove

☐ Require exact match

LDAP information caching interval

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。しかし、一部の Acronis Cyber Files 機能は構成するまで使用できません。

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 DNS 名または IP アドレスを入力します。
3. サーバーの LDAP 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、**[LDAP のセキュリティで保護された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. (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. LDAP 認証のドメインを入力します。
9. **[保存]** を押します。

ローカル ゲートウェイ サーバー

KCD をモバイルクライアント経由で動作させる場合は、ローカルゲートウェイ（管理元の Tomcat と同じマシン上にインストールされたもの）に登録する必要があります。そうすれば、ゲートウェイがこれらのリクエストをその Tomcat（管理）サーバーにプロキシします。

注意

同じコンピュータにゲートウェイサーバーと Acronis Cyber Files 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 Cyber Files 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 DNS 名または 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 DNS 名または 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

File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The file store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the [documentation](#).

File Store Type	Filesystem
File Store Repository Endpoint	http://127.0.0.1:5787
Encryption Level	AES-256

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ー上のファイルストアとして **[ファイル システム]** を使用するか、クラウド上のファイルストアとして次のオプションの任意のものを使用します。 **[Acronis Storage]**、 **[Microsoft Azure Storage]**、 **[Amazon S3]**、 **[Swift S3]**、 **[Ceph S3]**、 **[S3 と互換性のある他のストレージ]**。

注意

[S3 と互換性のある他のストレージ] オプションでこのリストに記載されていない S3 ストレージプロバイダを使用できます。しかし、すべての機能の正常な動作は保証されていません。

注意

MinIO S3 ストレージタイプがサポートされており、 **[S3 と互換性のある他のストレージ]** オプションとして設定できますが、セキュリティで保護されていない HTTP 接続経由ではサポートされません。

1. ファイル リポジトリ サービスの DNS 名または IP アドレスを入力します。

注意

Cyber Files の設定ユーティリティは、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ロケーションを設定するために使用します。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。これらの設定を表示または変更するには、AcronisAccessConfiguration.exe を実行します。それは、一般にエンドポイント サーバー上の C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility にあります。

2. 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。
3. 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。
4. [保存] を押します。

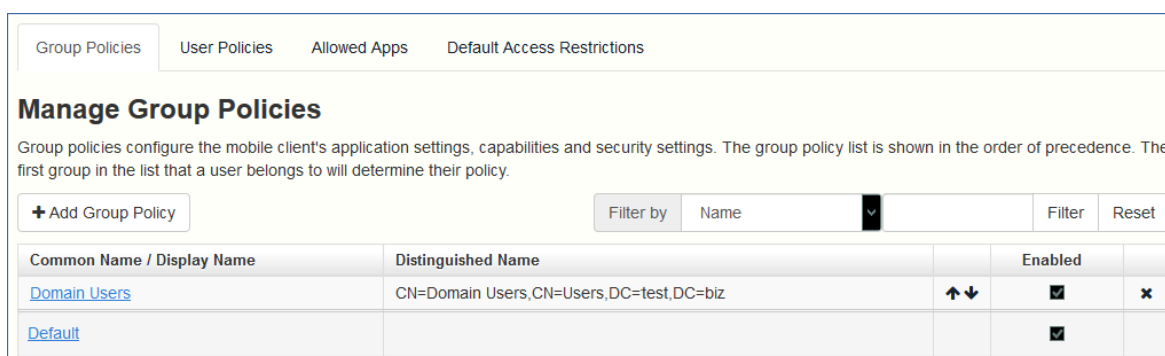
モバイル アクセス

デフォルト ポリシーの設定

Acronis Cyber Files Web サーバーの管理に登録されているすべてのモバイルクライアントでは、ユーザーポリシーまたはグループポリシーによって機能が管理および制御されます。デフォルトのポリシーは、インストール時に自動的に作成され、最も低い優先度が適用されます（最も高い優先度は個人的なユーザー ポリシーになります）。ユーザー ポリシーが適用されておらず、グループ ポリシーのメンバーにも登録されていないすべてのユーザーにデフォルト ポリシーが適用されます。デフォルト ポリシーはデフォルトで有効になっています。

デフォルト ポリシーの設定

1. Acronis Cyber Files ウェブ コンソールを開きます。
2. [モバイル アクセス] → [ポリシー] → [グループ ポリシー] に移動します。



Group Policies User Policies Allowed Apps Default Access Restrictions

Manage Group Policies

Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

+ Add Group Policy

Filter by Name Filter Reset

Common Name / Display Name	Distinguished Name	Enabled	
Domain Users	CN=Domain Users,CN=Users,DC=test,DC=biz	☒	⬆⬇⬆
Default		☒	

3. [有効] フィールドのチェックボックスがオンになっていることを確認し、[デフォルト] ポリシーをクリックします。
4. 設定を表示し、必要に応じて変更します。設定の各項目に関する詳細については、「[ポリシー](#)」セクションを参照してください。

モバイルクライアント

Acronis Cyber Files アプリを初めて実行するときに、デモモードでアプリを試用するか、会社のサーバーに接続するかを選択できます。

デモモードでアプリを試用する

デモモードでは、お勤めの会社に Acronis Cyber Files Web サーバーが用意されていない場合でも、Acronis Cyber Files アプリを試用することができます。デモモードの環境設定は試用を目的としているため、一部の機能は利用できません。

1. アプリをインストールし、起動します。
2. ようこそ画面の後に **[デモサーバーに接続する]** を選択します。
3. デモサーバーに接続されます。

注意

デモサーバーに接続されると、デモサーバー上の一部の共有フォルダおよび同期フォルダへの読み取り専用アクセス権が付与されます。これらのフォルダには、PDFや画像ファイルなどのサンプルファイルが含まれています。これらのファイルの参照、検索、表示、編集を実行したり、必要に応じて編集済みファイルをアプリ内（ローカル）に保存したりできます。

4. いつでも会社のサーバーに切り替えることができます。

会社のサーバーに登録するには

1. アプリをインストールし、起動します。
2. ようこそ画面の後に **[会社のサーバーに接続する]** を選択します。
3. 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。
4. 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。
5. 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。
6. Acronis Cyber Files モバイルアプリ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、必要な場合はそれが表示されます。

管理ポリシーで Acronis Cyber Files でのファイルの保存が制限されているか Acronis Cyber Files モバイルアプリ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。Acronis Cyber Files モバイルアプリ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。

クライアントガイド

Cyber Files クライアントの詳細については、以下のクライアントガイドドキュメントを参照してください。

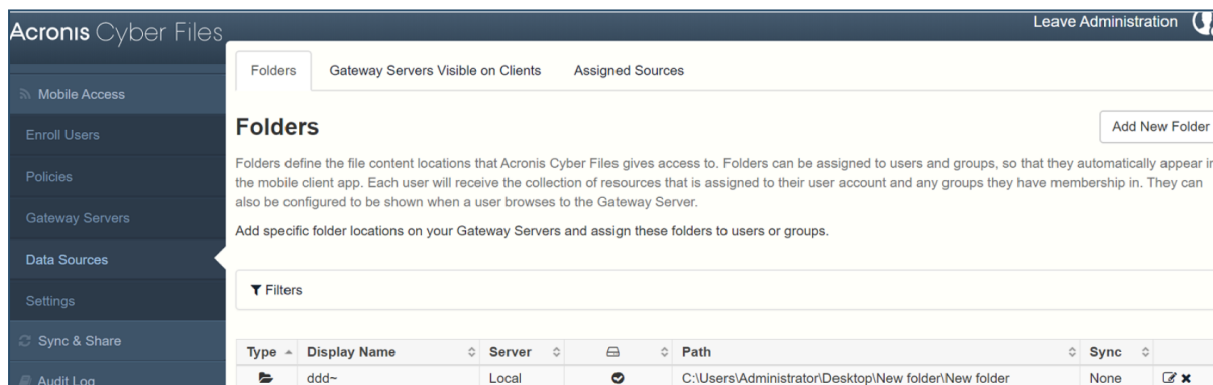
- [デスクトップおよびウェブクライアント](#)
- [iOSアプリ](#)
- [Androidアプリ](#)

同期・共有

Sync&Shareデータソース

Acronis Cyber Files をインストールして設定すると、自動的に「**Sync&Share**」という名前のデータソースが作成され、割り当てられたユーザーとグループのリストにデフォルトで **Domain Users** グループが追加されます。管理者は、このデータソースフォルダをいつでも変更または削除できます。

このデフォルトのデータソースは、**Domain Users**グループの一部として新しく作成するすべてのユーザーが使用することができ、モバイル、デスクトップ、およびウェブクライアント経由で利用できます。



ユーザーとのコンテンツの共有

既存のコンテンツを共有するには、そのコンテンツのデータソースを設定して、対象とするユーザーやグループにそのデータソースを割り当てることだけが必要です。

データソースの作成

1. Acronis Cyber Files Web インターフェースを開きます。
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. **[新しいフォルダを追加]** をクリックします。

Add New Folder

Display Name:

Select the Gateway Server to use to give access to this data source:

Data Location:

Enter the path to the local folder on this Acronis Cyber Files Gateway Server that you would like to share. (Example: "E:\Shares\Documents\"). You can include the wildcard string %USERNAME% in the path, in which case the wildcard will be replaced with the user's username.

Path:

Automatic Sync (Mobile Apps):

☐ Show When Browsing Server

Assign This Folder to a User or Group

Find User or Group that

Common Name / Display Name	Distinguished Name	Login Name
Domain Users	CN=Domain Users,CN=Users,DC=bgtest,DC=corp,DC=acronis,DC=com	Domain Users

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、Sync & Shareサーバー上を選択できます。

注意

リムーバブルメディアのフォルダを共有フォルダとして使用することはできません。別のロケーションから選択してください。

注意

Sync & Share 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 Cyber Files 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、このデータソースを表示するには、**[サーバーの参照時に表示する]**を有効にします。

注意

SharePoint のデータソースを作成する場合には、SharePoint フォローサイトの表示を有効化するオプションがあります。

12. **[保存]** ボタンをクリックします。

ウェブクライアントユーザーのFile Serversなどへのアクセスの許可

デフォルトでは、ユーザーはNAS、File Servers、およびSharePointのリソースをウェブクライアントから開くことができません。しかし、それを可能にすることは容易であり、そうすることでウェブユーザーが行えることの可能性は広がります。

1. Web インターフェースを開き、**[モバイルアクセス]** -> **[ポリシー]** に移動します。（モバイルアプリには主にポリシーが関連付けられていますが、ウェブアクセスの設定も関係することに注意してください。）
2. 変更するポリシーを選択します。新しいポリシーを何も作成していない場合は、**デフォルト**ポリシーを選択してください。

Group Policies

User Policies

Allowed Apps

Default Access Restrictions

Manage Group Policies

Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

+ Add Group Policy

Filter by Name FilterReset

Common Name / Display Name	Distinguished Name		Enabled	
Domain Users	CN=Domain Users,CN=Users,DC=test,DC=biz	↑↓	☒	✕
Default			☒	

3. **[サーバーポリシー]** タブで、**[ウェブクライアントからファイルサーバー、NAS、および SharePoint へのアクセスを許可する]** ボックスをオンにします。

Security Policy Application Policy Sync Policy Home Folders **Server Policy**

Required Login Frequency for Resources Assigned by This Policy:

☒ Once Only, Then Save for Future Sessions

☐ Once per Session

☐ For Every Connection

☐ Allow User to Add Individual Servers

☐ Allow Saved Passwords for User Configured Servers

☒ Allow File Server, NAS and SharePoint Access From the Web Client

☒ Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client

☒ Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client

☐ Allow User to Add Network Folders by UNC path or URL

Gateway Server used for access to user-configured Network Folders:

Local (192.168.2.129:3000) ▼

☐ Block access to specific network paths

Blocked Path List: ▼ Add/Edit lists Refresh lists

☐ Only Allow This Mobile Client to Connect to Servers with Third-Party Signed SSL Certificates

☒ Warn Client When Connecting to Servers with Untrusted SSL Certificates

4. デスクトップ同期を有効にするかどうかを検討し、選択したポリシーについて、サブオプション [ファイル サーバー、NAS および SharePoint のフォルダからデスクトップクライアントへの同期を許可する] および [ファイル サーバー、NAS および SharePoint のフォルダとデスクトップクライアントの双方向同期を許可する] を使用して設定してください。
5. [保存] をクリックします。

ポリシーごとの設定として実装されているので、より柔軟な設定が可能です。別のグループの設定やいくつかの個々のポリシーの設定を有効にすることもできます。

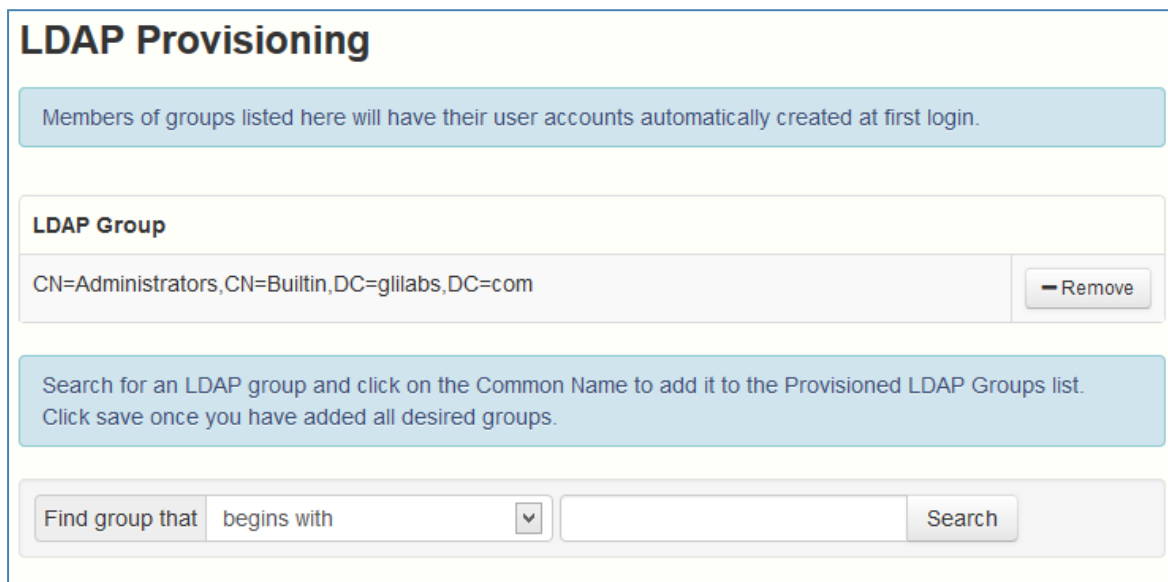
LDAP プロビジョニング

LDAP プロビジョニングを有効にすることで、管理者によるユーザーごと（またはグループごと）への招待が不要になり、ユーザーは LDAP の資格情報でログインすることができ、アカウントも自動的に作

成されるようになります。これらのアカウントはライセンス プールのライセンスから抽出されるため、特定の LDAP グループ（複数のグループも可）をプロビジョニング用に選択してください。

LDAP プロビジョニングを有効にする

1. Acronis Cyber Files ウェブ コンソールを開きます。
2. **[Sync&Share]** → **[LDAP プロビジョニング]** に移動します。



3. 1 つまたは複数の LDAP グループ名を入力します。
4. 目的のグループを選択し、**[保存]** をクリックします。

選択されたグループのユーザーは、LDAP の資格情報で Acronis Cyber Files へのログインを試行すると、Acronis Cyber Files アカウントが自動的に生成されます。

ウェブクライアントとデスクトップクライアント

- Web クライアントでは、Acronis Cyber Files の有効な資格情報を持つすべてのユーザーが、任意のブラウザからファイルやフォルダにアクセスしたり共有したりすることができます。
- デスクトップクライアントでは、サイズの大きなファイルを簡単に共有したり、ファイルを常に最新の状態に維持したりすることができます。

クライアントガイド

Cyber Files クライアントの詳細については、以下のクライアントガイドドキュメントを参照してください。

- [デスクトップおよびウェブクライアント](#)
- [iOSアプリ](#)
- [Androidアプリ](#)

インストール

要件

Acronis Cyber Files 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。

オペレーティングシステム要件

注意

Acronis Cyber Files 9.0は、Windows Server 2012およびWindows Server 2012 R2オペレーティングシステムをサポートする最後のバージョンです。

注意

Acronis Access Advanced 7.2.3 は 32 ビットオペレーティングシステムをサポートする最後のバージョンです。Acronis Cyber Files の新しいバージョンは、64 ビットオペレーティングシステムのみをサポートします。

注意

Acronis Access Advanced 7.4.x は、Windows XP および Vista をサポートする最後のバージョンです。これより新しいバージョンの Acronis Cyber Files は、これらのオペレーティングシステムからの接続をサポートしていません。

推奨:

- Windows Server 2019 Standard Edition および Datacenter Edition

サポート対象:

- Windows Server 2019 Standard Edition および Datacenter Edition
- Windows Server 2016 Standard Edition および Datacenter Edition
- Windows Server 2012 R2 Standard Edition および Datacenter Edition
- Windows Server 2012 Standard Edition および Datacenter Edition

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。

モバイル クライアントの要件

サポートされるモバイルデバイス

- Acronis Cyber Files がサポートする iOS または iPadOS のバージョンを実行する Apple ブランドのデバイス。
- Acronis Cyber Files でサポートされている Android の各バージョンを実行するデバイス（下記のとおり）。

重要

x86 ファミリーのプロセッサはサポートされていません。

モバイルオペレーティングシステムの最小サポート要件

注意

Ivanti MDM または Microsoft Intune のデプロイの場合、オペレーティングシステムのバージョンのサポートは、モバイルクライアントアプリに搭載される特定の SDK バージョンのサポートに依存します。SDK バージョンの詳細については、リンク先のリリースノートを参照してください。

- iOS または iPadOS の場合、サポートされる最小バージョンはバージョン 14 です。
これ以降のオペレーティングシステムバージョンのサポートの詳細については、[iOS 用 Acronis Cyber Files アプリのリリースノート](#)を参照してください。
- Android の場合、サポートされる最小バージョンはバージョン 7 です。
これ以降のオペレーティングシステムバージョンのサポートの詳細については、[Android 用 Acronis Cyber Files アプリのリリースノート](#)を参照してください。

モバイルアプリのダウンロード

- [iOS の場合](#)。
- [Android の場合](#)。

注意

標準、MDM Android APKは、[製品ダウンロード ページ](#)からダウンロードできます。

最小ハードウェア要件

デプロイサンプル

これらのデプロイ構成図は、すべての Acronis Cyber Files コンポーネントが同一の仮想マシンまたは物理サーバー上で実行されることを前提としています。

注意

推奨ディスク領域は、削除済みリビジョンの古いファイルがファイルリポジトリで消去されることを前提にしたものです。

注意

推奨ディスクサイズは最小構成によるものです。ユーザーが同期しているファイルのサイズおよび数によっては、ディスクサイズを増やす必要があります。

注意

Acronis Cyber Files Web サーバーは仮想マシンにインストールできます。

注意

Acronis Cyber Files 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。

注意

値は、本番環境の要件です。試用版のご利用、あるいはテスト目的での Acronis Cyber Files のインストールをお考えの場合には、テスト負荷に応じて必要に応じて小規模デプロイのハードウェア要件で始めるとよいでしょう。

小規模デプロイ

- 最大25ユーザー

注意

ここでの「ユーザー」は、**[全般設定] > [LDAP]** で Acronis Cyber Files に入力された LDAP 検索ベース内に含まれるすべてのユーザーアカウントおよびグループオブジェクトの合計です。

- CPU: Intel i7 Xeon (4コア) クラス、あるいは同等の AMD 製 CPU。
- RAM: 16GB
- ディスク領域: 100GB

中規模デプロイ

- 最大500ユーザー

注意

ここでの「ユーザー」は、**[全般設定] > [LDAP]** で Acronis Cyber Files に入力された LDAP 検索ベース内に含まれるすべてのユーザーアカウントおよびグループオブジェクトの合計です。

- CPU: Intel i7 Xeon (8コア) クラス、あるいは同等の AMD 製 CPU。
- RAM: 40GB
- ディスク領域: 2TB RAID

大規模デプロイ

- 最大2,500ユーザー

注意

ここでの「ユーザー」は、**[全般設定] > [LDAP]** で Acronis Cyber Files に入力された LDAP 検索ベース内に含まれるすべてのユーザーアカウントおよびグループオブジェクトの合計です。

- CPU: Intel i7 Xeon (16コア) クラス、あるいは同等の AMD 製 CPU。
- RAM: 64GB
- ディスク領域: 10TB RAID

注意

2,500 ユーザーを超えるデプロイでは、クラスター化されたサーバー構成を推奨します。

2,500 ユーザーを超えるデプロイについては、Acronis サポートにお問い合わせください。

注意

ワークフローとサーバー上で実行される他のアプリケーションに応じて、実際にはより多くのリソースが必要となる場合があります。

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 DNS 名。
- Active Directory (LDAP) の使用をご検討の場合の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** はモバイルアプリの内部で使用するため、VPN、MobileIron などのトンネルを経由して転送しないでください。
- Acronis Cyber Files Web 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ーはすべて、Windows Active Directory にバインドされていなければなりません。
- 管理コンソールの **[全般設定] > [Web サービス]** で設定した Acronis Cyber Files Web サーバーアドレスは、Acronis Cyber Files モバイルゲートウェイサーバーにアクセスできるようにする必要があります。

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 Cyber Files Web 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。Acronis Cyber Files Web サーバーは、Sync & Share クライアントの Web ユーザーインターフェースを提供すると同時に、モバイルアクセスと Sync & Share の両方の管理コンソールにもなります。

多くの場合、デプロイでは両方のサーバーで 1 つの IP アドレスを使用することが推奨されますが、ポートと DNS エントリは別個のものを使用してください。多くのインストールでは、このように、IP アド

レス設定は1つで十分です。特定のデプロイまたはセットアップが必要な場合には、コンポーネントごとに別個のIPアドレスを使用してサーバーを設定することがあります。

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 および 3000 へのアクセス:** Acronis Cyber Files は暗号化された転送に HTTPS を使用するため、ポート 443 および 3000 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 ルールに当然適合します。ポート 443 から Acronis Cyber Files Web サーバーへのアクセスを許可する場合、ファイアウォールで Acronis Cyber Files ゲートウェイ サービスへのポート 3000 アクセスを許可する必要があります。これにより、承認されたモバイルデバイスのクライアントアプリがファイアウォールの内外で接続できます。必要に応じて、他のポートを使用するように、サービスを構成することもできます。
- **VPN:** Acronis Cyber Files モバイルアプリは 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 Cyber Files Web 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、解放さ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。Acronis Cyber Files モバイルアプリは、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 制約付き認証委任、および証明書認証をサポートします。Acronis Cyber Files モバイルアプリへの証明書追加の詳細については、「クライアント証明書認証の使用」の記事を参照してください。
- **MobileIron AppConnect に登録されたアプリ:** Acronis Cyber Files モバイルアプリが MobileIron の AppConnect プラットフォームに登録されている場合は、Acronis Cyber Files モバイルアプリ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が MobileIron Sentry を経由して転送できます。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 Cyber Files には、テスト用の自己署名証明書が付属されており、この証明書が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している場合、一部のウェブ ブラウザでは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。本稼働環境での自己署名証明書の使用はサポートされていません。

注意

セキュリティで保護された LDAP 接続機能を有効にする場合、Acronis Cyber Files では、LDAP サーバーの完全修飾ドメイン名が、共通名 (CN) またはサブジェクト代替名 (SAN) として証明書に存在している必要があります。

デスクトップクライアント要件

システム要件

サポートされるオペレーティングシステム

- Windows 7、8、8.1、10、11

注意

デスクトップクライアント 7.4 は、Windows XP および Vista と互換性がある最後のバージョンです。Acronis Cyber Files デスクトップクライアントのより新しいバージョンを使用するには、Windows OS をアップデートしてください。Access Advanced 7.4 は Windows XP または Vista から接続が可能な最後のサーバーバージョンです。

注意

Acronis Cyber Files では 8.6 リリース以降、Windows Server 2008 R2 がサポートされなくなります ([Microsoft 公式発表リファレンス](#))。

- macOS X 10.13 から 10.15 と、64 ビットソフトウェアと互換性のある Mac
- Intel x86-64 と Apple シリコン CPU の両方が搭載された macOS 11 Big Sur と macOS 12 Monterey

注意

デスクトップクライアント 7.1.2 は、macOS X 10.6 および 10.7 と互換性がある最後のバージョンです。デスクトップクライアント 8.5 は macOS X 10.12 と互換性のある最後のバージョンです。Acronis Cyber Files デスクトップクライアントのより新しいバージョンを使用するには、macOS をアップデートしてください。

注意

Acronis Cyber Files デスクトップクライアントをインストールする際に、作成する同期フォルダが別のソフトウェアで同期されるフォルダ内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 60以降
- Microsoft Edge 25 以降
- Google Chrome 64 以降
- Safari 12 以降
- Opera 72 以降

その他の要件

インストール プロセスには次のものが必要となります。

- Acronis Cyber Files デスクトップクライアントインストーラの実行可能ファイルとそれを実行するための適切な権限。
- 使用するサーバーのアドレス（管理者またはEメールから取得）。
- サーバーのログイン資格情報（Active Directory、管理者、Eメールから取得）。

PostgreSQL Administrator の要件

Acronis Cyber Files PostgreSQL Administrator GUI アプリケーション（pgAdmin）は、PostgreSQLと一緒にインストールされます。

これには、PostgreSQL がインストールされているサーバーで実行されている次のウェブブラウザのいずれかが必要です。

- Chrome 90 以上
- Firefox 78 以上
- Edge 91 以上

サーバーへの Acronis Cyber Files のインストール

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 Cyber Files 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](#)」のセクションを参照してください。

注意

クラスターでのインストール手順については、「[ロードバランシング](#)」のセクションを参照してください。

Cyber Files のインストールは次の 3 ステップで行います。

1. Cyber Files Web サーバーインストーラのインストール。
2. Cyber Files Web 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

Cyber Files のインストール

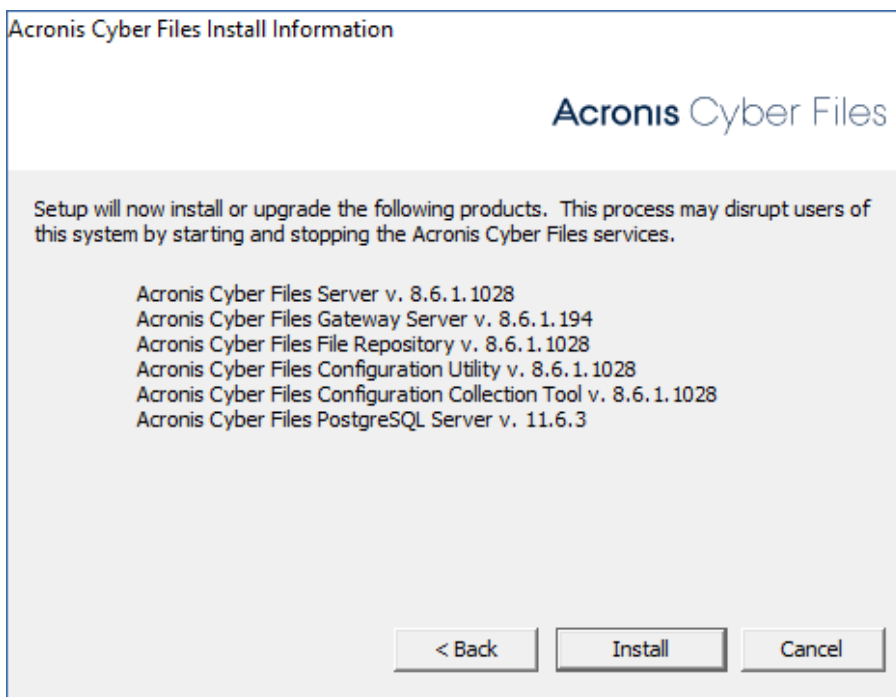
管理者としてサインインしていることを確認してから Cyber Files をインストールしてください。

1. Cyber Files インストーラをダウンロードします。
2. インストール手順が中断される可能性を避けるために、ウイルス対策ソフトウェアを無効にします。
中断すると、インストールが失敗します。
3. インストーラの実行ファイルを開きます。
4. **[次へ]** をクリックします。
5. 使用許諾契約を読み、承諾します。

6. **[インストール]** を選択します。

注意

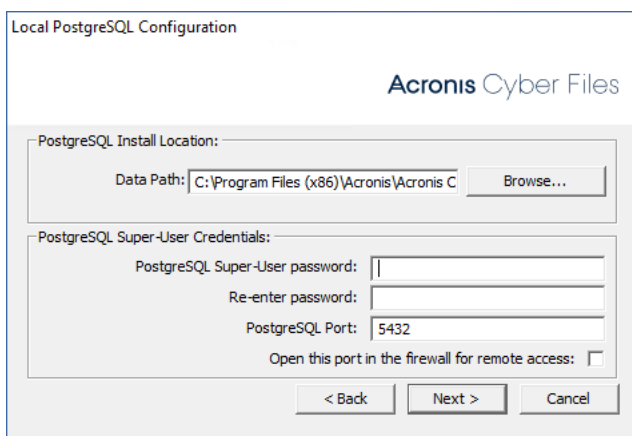
複数の Cyber Files サーバーを配置する場合や、標準構成以外でインストールを行う場合は、**[カスタムインストール]** ボタンからインストールするコンポーネントを選択することができます。



7. Cyber Files 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ます。
8. **[OK]** を選択します。
9. PostgreSQL スーパーユーザーのパスワードを指定します。

注意

PostgreSQL スーパーユーザーのパスワードにはコロン (:)、セミコロン (;)、またはアスタリスク (*) を含めることはできません。



重要

PostgreSQL スーパーユーザーのパスワードを書き留めて、安全な場所に保管します。それはデータベースのバックアップと復元に必要です。

10. **[OK]** を選択して、インストールされているコンポーネントのリストを閉じます。
11. インストーラが完了したら、**[終了]** を選択します。
12. 設定ユーティリティが自動的に起動します。

注意

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](#)を参照してください。

設定ユーティリティの使用

Acronis Cyber Files インストーラには設定ユーティリティが付属しています。このユーティリティを使用すると、Cyber Files ゲートウェイサーバー、ファイルリポジトリ、および Cyber Files Web サーバーへのアクセスをすばやく、簡単に設定できます。

注意

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](#)」セクションを参照してください。

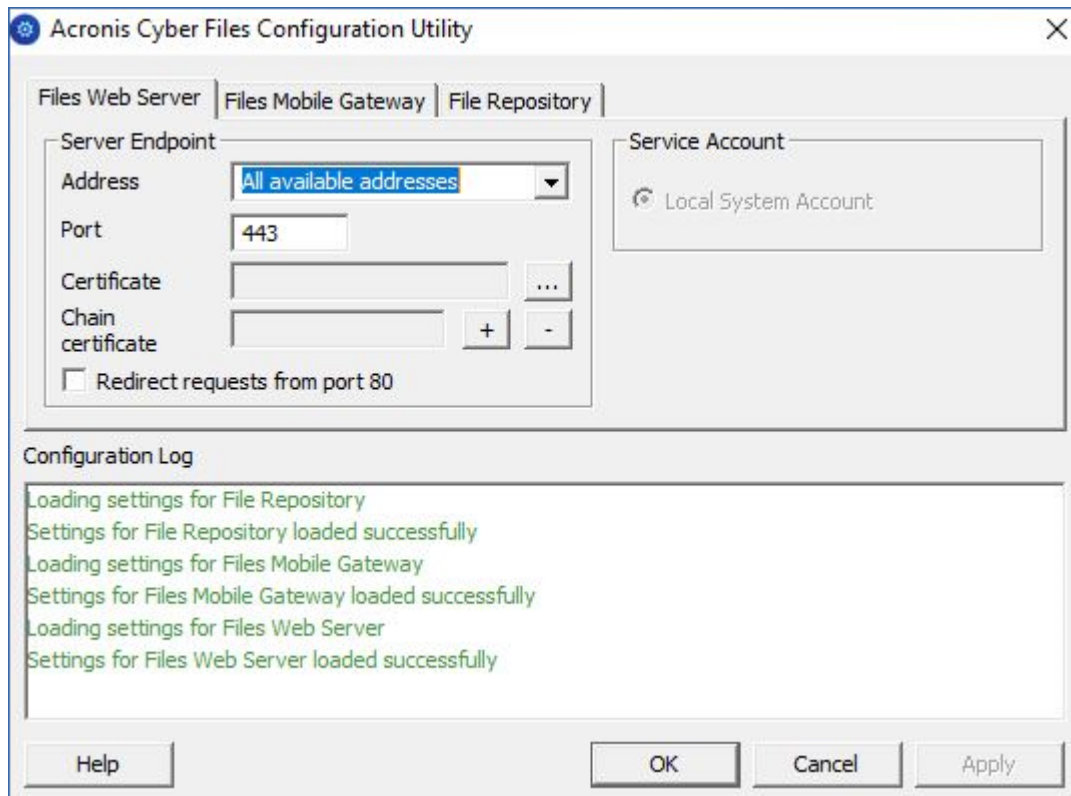
注意

Microsoft Windows 証明書ストアに証明書を追加する方法に関する詳細については、「[証明書の使用](#)」の記事を参照してください。

構成ユーティリティの概要

構成ユーティリティ内の設定は、いつでもユーティリティを起動して必要な変更を加えることによって変更できます。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。

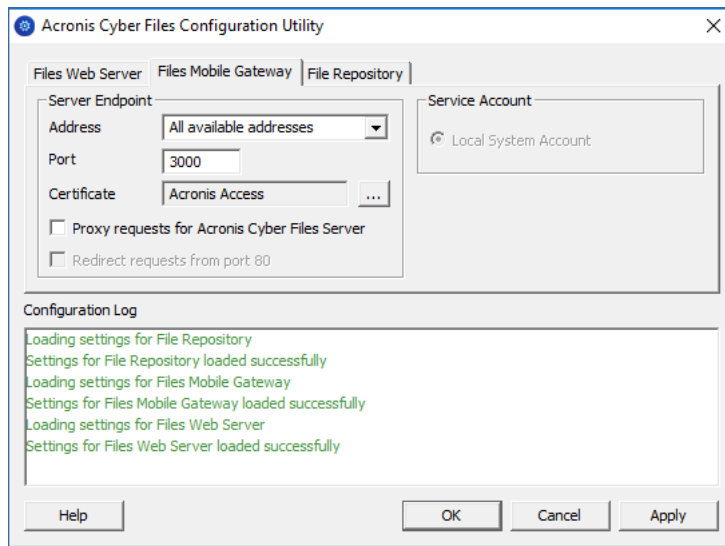
[Files Web サーバー] タブ



Cyber Files Web サーバーは、Cyber Files クライアントの Web ユーザーインターフェースを提供すると同時に、「[モバイルアクセス](#)」と「[Sync & Share](#)」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ースのIPアドレス。利用可能なすべてのインターフェー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 インターフェースのポート。
- **証明書:** ウェブ インターフェースの証明書のパス。Microsoft Windows証明書ストアから証明書を選択できます。
- **チェーン証明書:** Web インターフェースの中間証明書へのパス。Microsoft Windows 証明書ストアから 1 つを選択できます。証明機関でも中間証明書が発行されている場合にのみ、この証明書が必要になります。
- **ポート 80 での接続を許可します:** 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、このボックスをオフにしてください。
- **サービスアカウント:** Cyber Files Web 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。

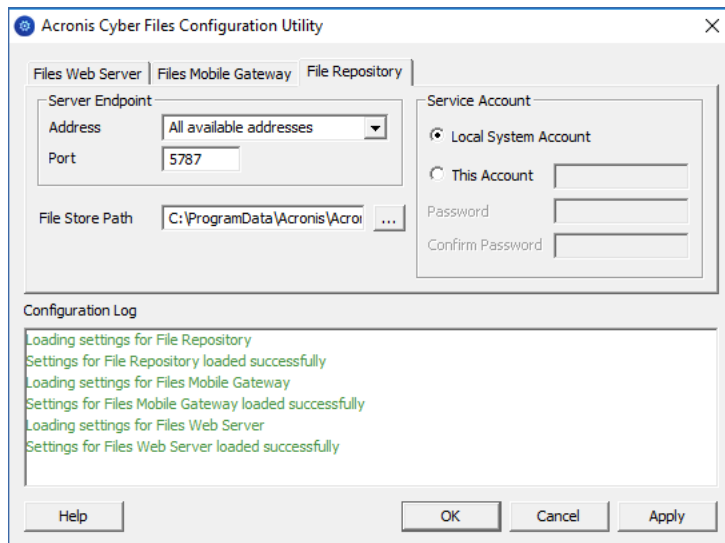
[Files Mobile Gateway] タブ



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 IP アドレス。すべてのインターフェー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:** 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。
- **Cyber Files サーバーに対するプロキシ要求:** このオプションをオンにすると、ユーザーはゲートウェイサーバーに接続され、ゲートウェイサーバーが Cyber Files サーバーのプロキシサーバーとして機能します。このオプションを使用できるのは、Cyber Files サーバーとゲートウェイサーバーが同じマシン上にインストールされている場合です。
- **ポート 80 での接続を許可します:** 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、このボックスをオフにしてください。

[ファイルリポジトリ] タブ



ファイルリポジトリは、Sync & Share機能で使します。Sync & Share をまだ有効にしていない場合は、標準値を受け入れることができます。Sync & Share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 IP アドレス。すべてのインターフェー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 Web インターフェースの **[ファイルリポジトリ]** セクションで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、Web インターフェースの **[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（たとえば、C:\Program Files (x86)\Acronis\Acronis Cyber Files\File Repository\Repository）への読み取り/書き込みアクセス権限も必要です。

注意

ローカルシステムアカウントではなく、このサービスに固有のアカウントを使用する場合は、[サービス] コントロールパネルを開き、**Cyber Files ファイルリポジトリ**サービスのプロパティを開いて、[ログオン] タブを編集してください。アカウントとパスワードは対応するフィールドに手動で入力してください。

セットアップウィザードに進む

必要なフィールドのすべてに入力した後、[適用] または [OK] を選択すると、変更を加えたサービスが再起動します。

注意

サービスが開始されてから 30～45 秒経つと、Cyber Files Web サーバーが利用できるようになります。

1. 設定ユーティリティの初期セットアップが完了すると、Web ブラウザで自動的に Cyber Files Web インターフェースが開きます。
2. ログインページで、**管理者**パスワードを設定するよう促すメッセージが表示されます。[セットアップウィザード](#)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。

重要

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。

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 Cyber Files 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

構成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。

以前のステップで管理者アカウントをセットアップしなかった場合は、ログインページで、**管理者**パスワードを設定するよう促すメッセージが表示されます。

管理者パスワードを書き留めておいてください。忘れた場合はパスワードを復元することができません。

初期構成プロセスを進める

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 Cyber Files の Web インターフェースに移動します。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

追加の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](#)」の資料を参照してください。

ライセンス

試用版を開始するには:

[**トライアルを開始**] を選択し、必要な情報を入力して [**続行**] をクリックします。

☒ Start trial ☐ Enter license key

Please register to start using the trial

First Name

Last Name

Country ▼

State/province ▼

Phone

Select industry ▼

Company

Email

Acronis Cyber Files インスタンス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、チェックボックスを選択します。

☐ Start trial ☒ Enter license key

☒ I understand the details and scope of my license may be found on my invoice and at <http://www.acronis.com/company/licensing.html>.

3. [保存] をクリックします。

全般設定

Server Name

Web Address

Audit Log Language ▼

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 root DNS 名または IP アドレスを指定します。
3. **[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]、[日本語]、[イタリア語]、[スペイン語]、[チェコ語]、[ロシア語]、[ポーランド語]、[韓国語]、[中国語 (繁体字)]、[中国語 (簡体字)] です。
4. **[保存]** をクリックします。

SMTP

The screenshot shows the 'SMTP' configuration page in the Acronis Cyber Files interface. On the left is a sidebar with navigation links: Licensing, General Settings, SMTP (selected), LDAP, Local Gateway Server, and File Repository. The main content area is titled 'SMTP' and contains a blue informational box stating: 'Acronis Cyber Files Server uses the configured SMTP server to send emails to invite users to share or enroll mobile devices, as well as notify users and administrators of server activity.' Below this are several configuration fields: 'SMTP Server Address' (myemailserver.mycompany), 'SMTP Server Port' (25), 'Use secure connection?' (checked), 'From Name' (Acronis Cyber Files Admin), 'From Email Address' (adminname@mycompany.c), 'Use only this address for all email notifications' (unchecked), and 'Use SMTP authentication?' (unchecked). At the bottom are three buttons: 'Save', 'Send Test Email', and 'Skip SMTP Setup'.

注意

この手順をスキップして、後で SMTP を設定することもできます。

1. SMTP サーバーの DNS 名または 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?]** オプションをオフにします。
4. サーバーから送信される E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 E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、**[SMTP 認証の使用]** をオンにして、資格情報を入力します。
7. **[テスト用の Eメールの送信]** をクリックして、手順 5 で指定した Eメールアドレスにテスト用の Eメールを送信します。
8. **[保存]** をクリックします。

LDAP

LDAP

An LDAP connection to your Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Only LDAP connections to Microsoft Active Directory are supported.

Enable LDAP? ☒

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection? ☐

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

e.g. mycompany.com. Users with email addresses whose domains are in this list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.

+ Add

myldap.mydomain.com

- Remove

Domains for LDAP Authentication

☐ Require exact match

LDAP information caching interval

注意

この手順をスキップして、後で LDAP を設定することもできます。ただし、一部の Acronis Cyber Files 機能は設定するまで使用できません。

1. **[LDAP を有効にしますか?]** をオンにします。
2. LDAP サーバーの DNS 名または IP アドレスを入力します。
3. サーバーの LDAP 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、**[LDAP のセキュリティで保護された接続を使用しますか?]** をオンにします。
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。

- LDAP 認証のドメインを入力します。（「joe@glilabs.com」という電子メールアカウントの LDAP 認証を有効にするには、「glilabs.com」と入力します）。
- [保存] をクリックします。

ローカル ゲートウェイ サーバー

KCD をモバイルクライアント経由で動作させる場合は、ローカルゲートウェイ（管理元の Tomcat と同じマシン上にインストールされたもの）に登録する必要があります。そうすれば、ゲートウェイがこれらのリクエストをその Tomcat（管理）サーバーにプロキシします。

注意

同じマシンにゲートウェイサーバーと Acronis Cyber Files サーバーの両方をインストールする場合、前者が自動的に検出され、後者によって管理されます。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 DNS 名または 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。

- ローカルゲートウェイサーバーの DNS 名または IP アドレスを設定します。
- [保存] をクリックします。

ファイル リポジトリ

File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The file store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the [documentation](#).

File Store Type	Filesystem
File Store Repository Endpoint	http://127.0.0.1:5787
Encryption Level	AES-256

- 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ー上のファイルストアとして [ファイルシステム] を使用するか、クラウド上のファイルストアとして次のオプションの任意のものを使用します。[Acronis Storage]、[Microsoft Azure Storage]、[Amazon S3]、[Swift S3]、[Ceph S3]、[S3 と互換性のある他のストレージ]。

注意

[S3 と互換性のある他のストレージ] オプションでこのリストに記載されていない S3 ストレージプロバイダを使用できます。しかし、すべての機能の正常な動作は保証されていません。

注意

MinIO S3 ストレージタイプがサポートされており、**[S3 と互換性のある他のストレージ]** オプションとして設定できますが、セキュリティで保護されていない HTTP 接続経由ではサポートされません。

2. ファイル リポジトリ サービスの DNS 名または IP アドレスを入力します。

注意

Acronis Cyber Files の構成ユーティリティは、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ロケーションを設定するために使用します。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。これらの設定を表示または変更するには、AcronisAccessConfiguration.exe を実行します。それは、一般にエンドポイント サーバー上の C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\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]** をクリックします。

Acronis Cyber Files のクラスタリング

Acronis Cyber Files 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、高可用性の設定を構成することができます。設定には、Acronis Access 5.1 で導入された新しいクラスターグループ機能を使用します。設定手順は簡単ですが、Acronis Cyber Files ゲートウェイサーバーは最も高い負荷がかかるコンポーネントであるため、同サーバーに高可用性を提供します。設定のすべては、Acronis Cyber Files サーバーを通して管理されます。

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

組み込みのクラスターグループ機能を使用することをお勧めしますが、Acronis Cyber Files 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。

ロードバランシング

Acronis Cyber Files ではロードバランシングがサポートされています。

注意

詳細については、[負荷分散構成での Acronis Cyber Files のインストール](#)、[負荷分散環境への移行](#)、および[クラスターグループ](#)を参照してください。

アップグレード

Acronis Cyber Files の新しいバージョンへのアップグレード

Acronis Cyber Files 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。

注意

オペレーティングシステムのインプレースアップグレードはサポートされていません。ご質問がある場合は、[Acronis Mobility テクニカルサポート](#)にお問い合わせください。

注意

Acronis Cyber Files（旧名称: Acronis Access）7.5 より前のバージョンを使用している場合は、Acronis サポート（<https://support.acronis.com/mobility/>）までお問い合わせください。

注意

アップグレードする前に、[最小ハードウェア要件](#)を確認してください。

注意

導入環境によっては、この記事で使用されている一部のパスがご使用のパスと異なる可能性があります。以前のバージョンの Acronis Cyber Files からのアップグレードやカスタムインストールにより、導入環境のフォルダ構造に影響が現れる可能性があります。

注意

Acronis Cyber Files バージョン 8.6 以降にアップグレードする場合、PostgreSQL は自動的にバージョン 11 にアップグレードされません。その方法の詳細については、「[PostgreSQL の新しいメジャーバージョンへのアップグレード](#)」を参照してください。

重要なコンポーネントのバックアップ

Apache Tomcat フォルダ

アップグレード時に、Apache Tomcat もアップグレードされ、すべての構成ファイルが置き換えられ、ログファイルが削除される場合があります。Apache Tomcat フォルダのコピーを作成することをお勧めします。これは、デフォルトで次の場所にあります: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\。

web.xml ファイルは更新する前にバックアップしておくことをお勧めします。**web.xml** ファイルはアップグレード時に上書きされます。バージョン 8.6 以降のバックアップの保存場所は

C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF<<タイムスタンプ>>.previous.web.xml です。

維持しておきたい特定の変更（**シングルサインオン**は除きます。この変更は保存されます）がある場合は、古いファイルからその変更を手動でコピーし貼り付けてください。

不要な監査ログの消去

自動ログ消去を設定していない場合は、サーバーにログがたまって、バックアッププロセスの速度が低下する可能性があります。データベースのバックアップを実行する前に、古いログをエクスポートまたは消去することをお勧めします。

PostgreSQL データベース

次の手順を実行すると、元のデータベースのテキスト表示が格納された *.sql ファイルを作成することができます。

1. コマンドプロンプトウィンドウを開き、PostgreSQLのインストールディレクトリにある 11.21\bin フォルダに移動します。

例: `cd "C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.21\bin"`

2. 現在のコマンド プロンプト ウィンドウのディレクトリを **bin** フォルダに移動したら、次のコマンドを入力してください。

```
pg_dump -U postgres -f mybackup.sql acronisaccess_production
```

ここで、mybackup.sql は、生成されたバックアップ ファイルのファイル名です。

D:\Backups\mybackup.sql のように、バックアップファイルを作成するロケーションのフルパスを含めることもできます。

注意

acronisaccess_production は Acronis Cyber Files データベースの名前に表示されるとおり正確に入力する必要があります。

3. 「Password:」という行が表示されます。Acronis Cyber Files のインストールプロセス中に設定した postgres のパスワードを入力してください。

注意

パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

4. 出力ファイルにほかのディレクトリへのフルパスが指定されていない限り、バックアップ ファイルは、デフォルトで **bin** フォルダに作成されます。

注意

PostgreSQL データベース全体のバックアップを行う場合は、次のコマンドを使用してください。

```
pg_dumpall -U postgres > alldbs.sql
```

alldbs.sql は作成されるバックアップ ファイルです。D:\Backups\alldbs.sql のようにフルパスを指定することも可能です。

このコマンドの完全な構文の詳細については、以下を参照してください。<https://www.postgresql.org/docs/11/app-pg>

注意

PostgreSQL のバックアップ手順とコマンド構文の詳細については、以下を参照してください。 <https://www.postgresql.org/>

ゲートウェイ サーバー データベース

1. Acronis Cyber Files ゲートウェイサーバーがインストールされているサーバーを参照します。
2. データベースを含むフォルダに移動します。

注意

デフォルトの場所は、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database です。

3. **mobilEcho.sqlite3** ファイルをコピーして、安全な場所に貼り付けます。

Acronis Cyber Files 設定ファイル

1. 設定ファイルが含まれる Acronis Cyber Files のインストールフォルダに移動します。

注意

デフォルトの場所は、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server です。

2. **acronisaccess.cfg** ファイルをコピーして、安全な場所に貼り付けます。

アップグレード前のデータベースのバキューム

注意

以降の手順を実行する前に、次の**推奨事項**を確認してください。

1. Acronis Cyber Files PostgreSQL 管理ツールを開きます。これは [スタート] メニューの Acronis Cyber Files フォルダにあります。[localhost] をダブルクリックして、サーバーに接続します。
2. acronisaccess_production データベースを右クリックして、[メンテナンス] を選択します。
3. [バキューム] を選択し、[分析] を [はい] に設定します。

Maintenance...

Options

Maintenance operation: VACUUM ANALYZE REINDEX CLUSTER

Vacuum

FULL: No FREEZE: No ANALYZE: Yes

Verbose Messages: Yes

Buttons: i ? Cancel OK

警告

バキューム処理には長時間がかかる場合があります。サーバーの負荷が低いときにこのプロセスを実行してください。

4. [OK] をクリックします。
5. [バキューム] プロセスが終わると、[完了] を押します。
6. PostgreSQL管理ツールを閉じます。

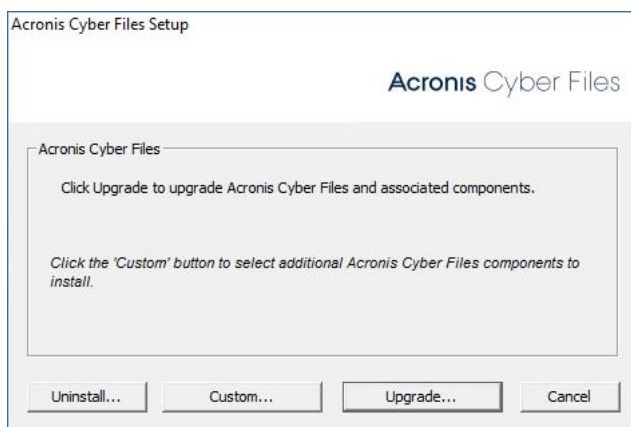
アップグレード

注意

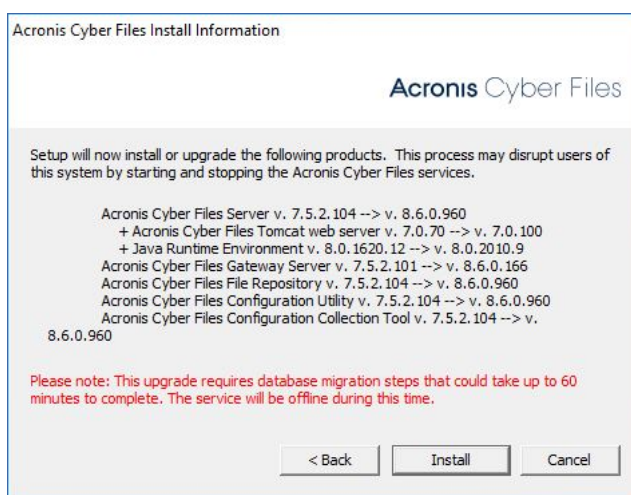
インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、操作が中断され、インストールが失敗する可能性があります。

1. 実行可能なインストーラをダブルクリックします。

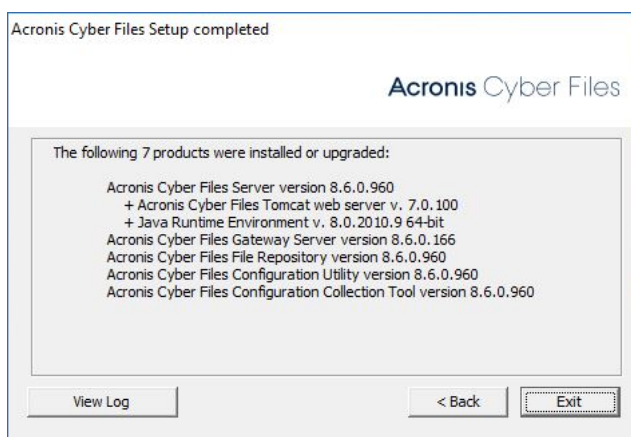
2. 次に開いた画面で、[アップグレード] をクリックします。



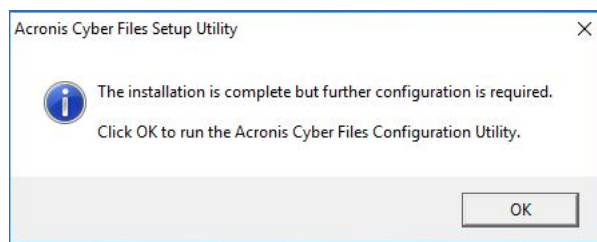
3. インストールするコンポーネントを確認して、[インストール] をクリックします。



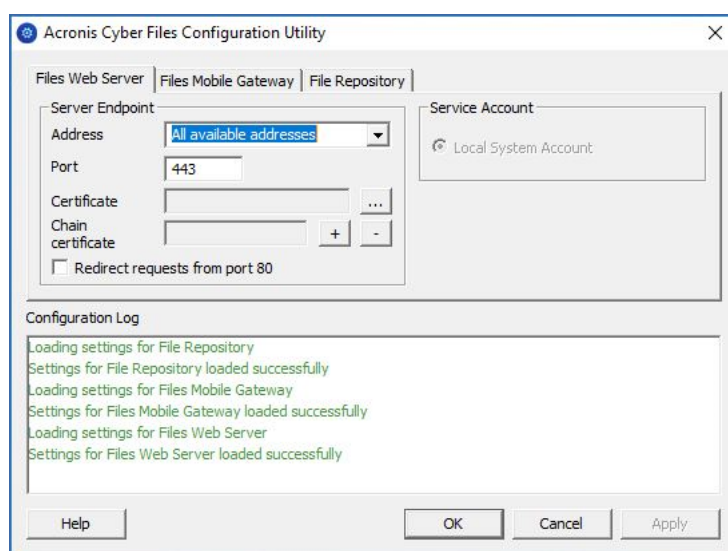
4. 既にインストールされたコンポーネントを確認して、インストーラを閉じます。



5. 次のメッセージでアップグレードの完了が確認されます。



6. 設定ユーティリティを開くように求められたら、**[OK]** をクリックします。
7. 設定ユーティリティ内の設定が正しい値であるかどうかを確認します。これらのすべてが想定どおりだった場合は、**[OK]** を押して設定ユーティリティを閉じ、Acronis Cyber Files サービスを開始します。



警告

アップグレード手順の直後にデータベース移行が実施されます。この期間中は、実際の Web サイトとそのサービスのすべてが利用できなくなります。かなりの期間アップグレードしなかったなどの理由で、この重要な処理がすべて完了するまでに 1 時間以上かかる場合があります。Web サイトがブラウザに応答を返すようになるまでは、サーバーの再起動やサービスの中断を行わないようにすることを強くお勧めします。

ゲートウェイクラスタのアップグレード

Acronis Cyber Files のクラスター構成をアップグレードするには、Acronis Cyber Files Web サーバーと [クラスターグループ](#) 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。

注意

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。

注意

Acronis Cyber Files Web サーバーのアップグレードの方法については、「[Acronis Cyber Files の新しいバージョンへのアップグレード](#)」の記事を参照してください。

ゲートウェイサーバーごとに、次のアップグレード手順を実行する必要があります。

アップグレードを実行する前に、「[バックアップ](#)」の記事を確認してから構成をバックアップしてください。

注意

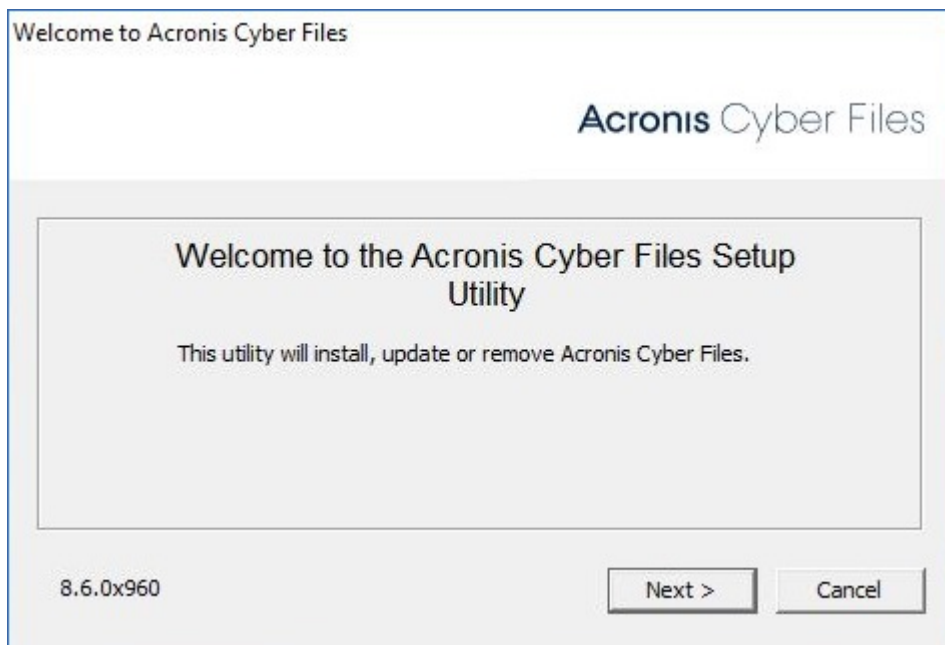
アップグレードする前に、[最小ハードウェア要件](#)を確認してください。

注意

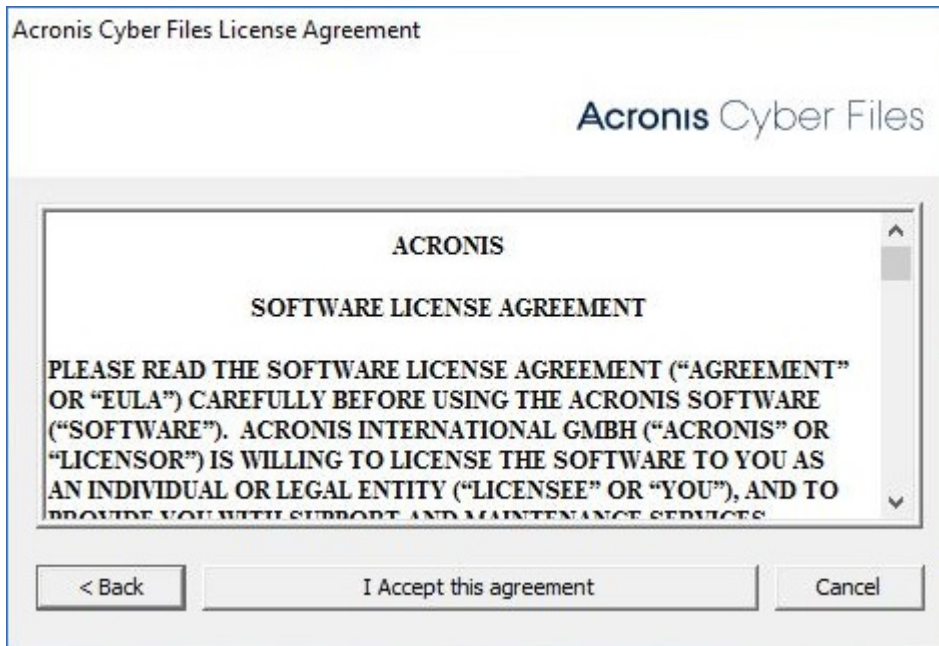
導入環境によっては、この記事で使用されている一部のパスがご使用のパスと異なる可能性があります。以前のバージョンの Acronis Cyber Files からのアップグレードやカスタムインストールにより、導入環境のフォルダ構造に影響が現れる可能性があります。

ゲートウェイ サーバーのアップグレード

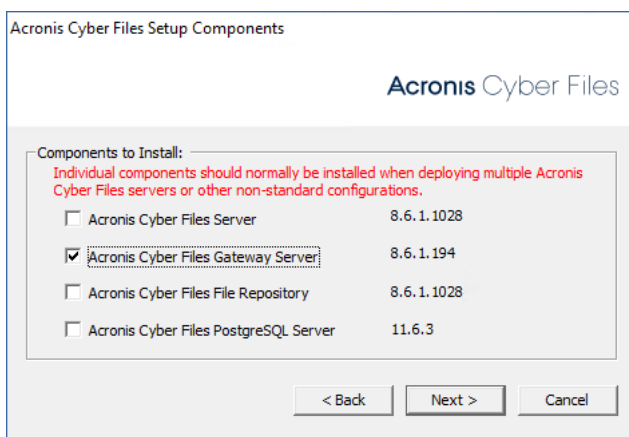
1. 対象のサーバーで Acronis Cyber Files インストーラを実行します。
2. **[ようこそ]** 画面で **[次へ]** をクリックします。



3. 使用許諾契約を読み、承諾します。



4. **[カスタム]** を選択します。
5. **[Acronis Cyber Files 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]** をクリックします。
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。
8. **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]** をクリックします。

ロードバランス設定のアップグレード

このガイドでは、Acronis Cyber Files のロードバランシング、およびそのコンポーネントすべての配置について説明します。

アップグレードを実行する前に、「**バックアップ**」の記事を確認してから構成をバックアップしてください。

注意

アップグレードする前に、[最小ハードウェア要件](#)を確認してください。

注意

導入環境によっては、この記事で使用されている一部のパスがご使用のパスと異なる可能性があります。以前のバージョンの Acronis Cyber Files からのアップグレードやカスタムインストールにより、導入環境のフォルダ構造に影響が現れる可能性があります。

開始する前に

警告

Acronis Cyber Files では、各リリースに組み込まれているバージョンより新しいバージョンの Tomcat、Java、および PostgreSQL はサポートされません。特定のバージョンに関する情報が必要な場合は、[アクロニス サポートセンター](#)までご連絡ください。

注意

本番環境外でのテストアップグレードの実行を強くお勧めします。

このページに記載されているすべてのパスは、デフォルトの場所を示しています。アップグレードまたはカスタムインストールを行った場合には、パスが異なっている場合があります。その場合には、プログラム実行可能フォルダへの正しいパスを見つけるために、Windows サービスの [サービス名] エントリを使用してください。

現在の構成に関し、次の重要な事項に注意してください。

- Acronis Cyber Files サーバーと PostgreSQL サーバーが同じマシン上に存在しますか？
- PostgreSQLがどのポートで実行されていますか？
- 現在インストールされているPostgreSQLのロケールは何ですか？これを確かめるには、PostgreSQL 管理ツールを開いて `acronisaccess_production` データベースをクリックします。右側の [プロパティ] に、[エンコーディング] と [文字の種類] が表示されます。

警告

新しくインストールした PostgreSQL でも [エンコーディング] と [文字の種類] が同じになっていることを確認してください。同じでない場合、正常にアップグレードできません。

- PostgreSQL を実行しているマシンの IP や DNS 名は何ですか？
- 現在のサーバーのPostgreSQLバージョン番号は何ですか？これを確かめるには、メインの PostgreSQL フォルダ内のフォルダ名を調べるのが最も簡単です（デフォルトで `C:\Program Files (x86)\Acronis\Cyber Files\Common\PostgreSQL`）。内側のフォルダ名は PostgreSQL のメジャーバージョン番号（9.2、9.3、9.4 など）です。
- Access や Files Advanced などの古いバージョンの製品から Acronis Cyber Files にアップグレードしたお客様は、ディレクトリのパスが異なる可能性がありますのでご注意ください。次の例を参考にしてください。

- C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL
- C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL
- C:\Program Files\PostgreSQL\
- ファイルシステムについての必要なアクセス許可がすべて設定されていることを確認します。

プライマリとして機能する Acronis Cyber Files Web サーバーマシンの 1 つを選択します。このマシンは、最初にアップグレードされ、変更/設定が PostgreSQL データベースに移行されるという意味においてのみ**プライマリ**ノードです。非常に大きなデータベースの場合は、これらの移行に数分かかることがあります。

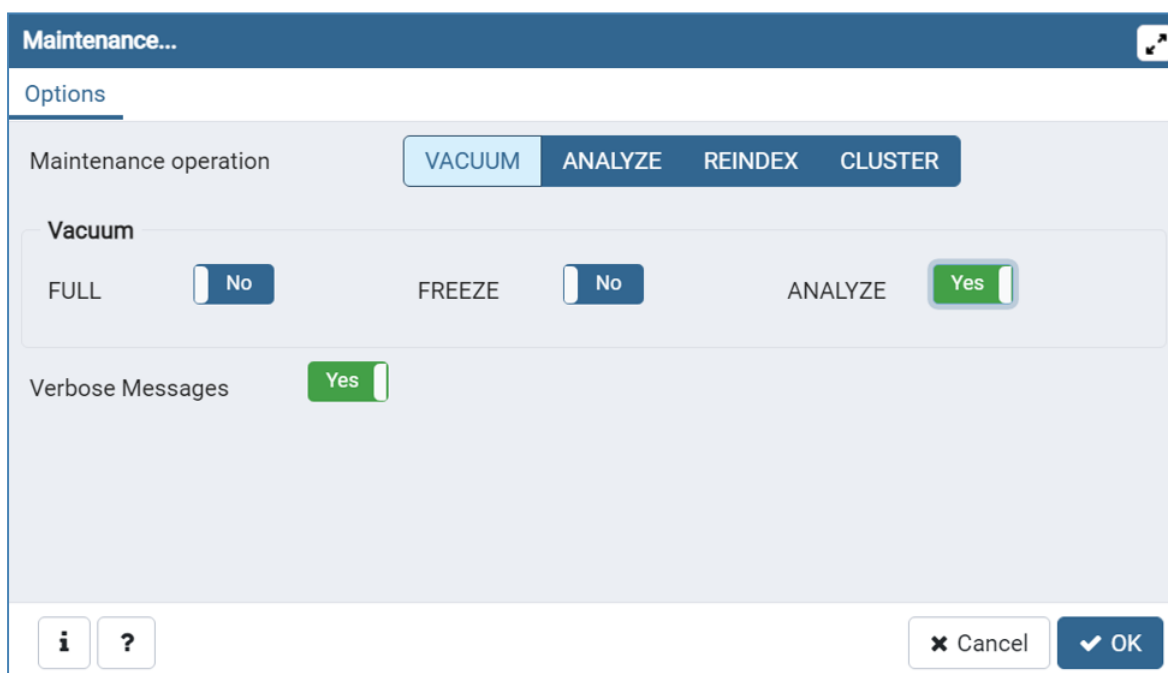
警告

プライマリサーバーがアップグレードされ、Web インターフェースにログインしてそのサーバーを試すことができるようになるまで、他の Tomcat サーバーをアップグレードしないでください。

データベースのバキューム

これにより、データベースを最適化することでバックアップと復元のプロセスが高速化されます。

1. Acronis Cyber Files PostgreSQL 管理ツールを開きます。これは [スタート] メニューの Acronis Cyber Files フォルダにあります。**[localhost]** をダブルクリックして、サーバーに接続します。
2. acronisaccess_production データベースを右クリックして、**[メンテナンス]** を選択します。
3. **[バキューム]** を選択し、**[分析]** を **[はい]** に設定します。



警告

バキューム処理には長時間がかかる場合があります。サーバーの負荷が低いときにこのプロセスを実行してください。

4. **[OK]** をクリックします。

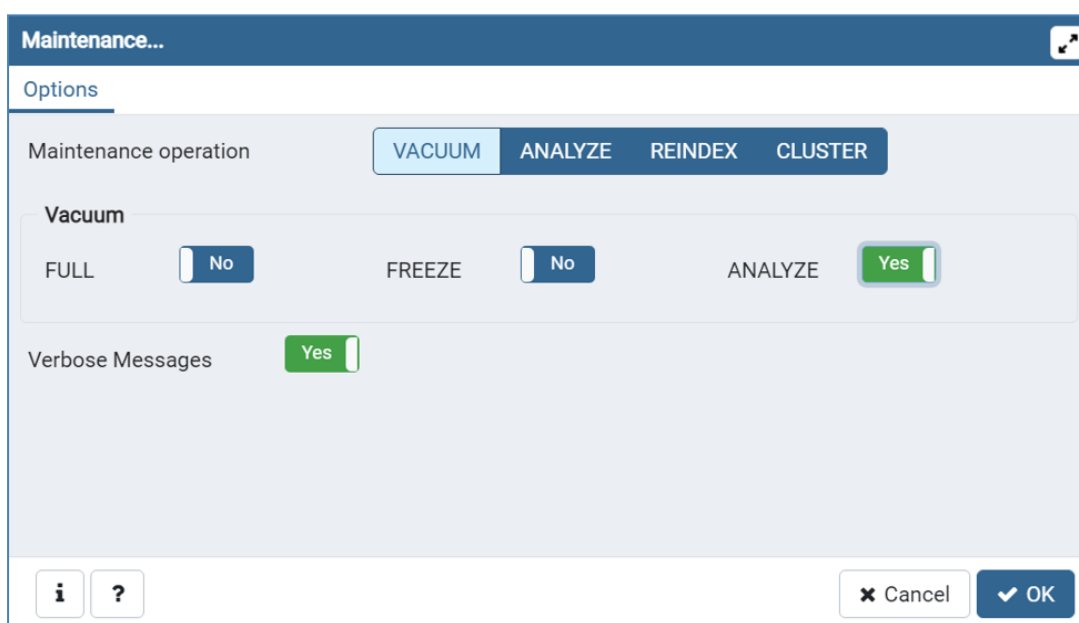
5. [バキューム] プロセスが終わると、[完了] を押します。
6. PostgreSQL管理ツールを閉じます。

負荷分散コンポーネントのバックアップ

バックアップと復元の手順の詳細については、『[Acronis Cyber Files のバックアップと復元](#)』の記事を参照してください。

PostgreSQLデータベースのバックアップ

1. すべての Acronis Cyber Files Tomcat サービスを停止します。
2. Acronis Cyber Files PostgreSQL 管理ツールを開きます。これは Windows の [スタート] メニューの Acronis Cyber Files フォルダにあります。データベースサーバーに接続します。postgres ユーザーのパスワード入力を求められる場合があります。
3. [データベース]を展開し、acronisaccess_productionデータベースを右クリックします。
4. [メンテナンス] を選択します。
5. [バキューム] を選択し、[分析] を [はい] に設定します。



6. [OK] をクリックします。
7. データベース、[スキーマ]、[Public]の順に展開します。[テーブル]セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
8. PostgreSQL Administrator ツールを閉じ、管理者特権でのコマンドプロンプトを開きます。
9. このコマンドプロンプトで、PostgreSQLのbinディレクトリに移動します。
例:cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"

注意

カスタムインストールまたは古いインストールを使用する場合には PostgreSQL bin フォルダを指すようにパスを編集する必要があります (例: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\)

1. コマンド `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql` を入力します。
 - バックアップのファイル名は `alldbs.sql` になります。これは、PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を `--file D:\Backups\alldbs.sql` のように変更します。
 - デフォルト以外のポートを使用している場合は、5432 を正しいポート番号に変更します。
 - デフォルトの PSQL 管理者アカウント `postgres` を使用していない場合は、上記コマンド内の `postgres` をご使用の管理者アカウント名に変更してください。
 - この手順では、`postgres` ユーザーのパスワードを何回か入力するように求められます。そのたびにパスワードを入力してEnterキーを押してください。

注意

パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

2. バックアップファイルを安全な場所にコピーします。
3. PostgreSQL自体はアップグレードされないため、Postgresサービスはシャットダウンしないでください。

その他の重要なコンポーネントのバックアップ

1. Tomcatの**conf**フォルダと**logs**フォルダをバックアップします。デフォルトの場所: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\

注意

<バージョン> は Acronis Cyber Files Tomcat インスタンスの正しいバージョンに置き換えて、\apache-tomcat.70.0.70\ のようにしてください。

2. **acronisaccess.cfg** ファイルをバックアップします。デフォルトの場所: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server
3. デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\ に配置されるすべての **web.xml** ファイルをバックアップします。
4. **newrelic.yml** ファイルをバックアップします。このファイルの場所は保存した場所に依存します。New Relic監視を使用していない場合は、このステップをスキップできます。

ゲートウェイサーバーのデータベースのバックアップ

1. すべての Acronis Cyber Files ゲートウェイサービスをオフにします。
2. デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database のゲートウェイデータベースフォルダに移動します。

3. **mobileEcho.sqlite3**ファイルのバックアップを作成します。
4. ゲートウェイサーバーごとにこれらのステップを繰り返します。

すべてのマシン上のすべての Acronis Cyber Files サービスを停止します。

アップグレード前にすべての Acronis Cyber Files Tomcat サービスを停止することが不可欠です。実行したままにする必要がある PostgreSQL サービスを除いて、他のすべての Acronis Cyber Files サービスも停止することをお勧めします。

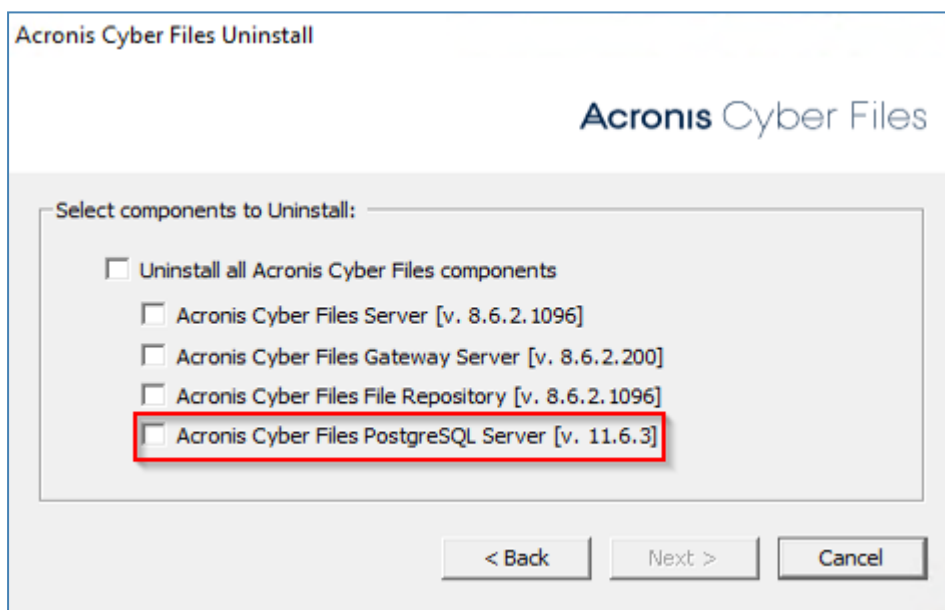
PostgreSQL のアップグレード

手順 1: PostgreSQL をアンインストールする

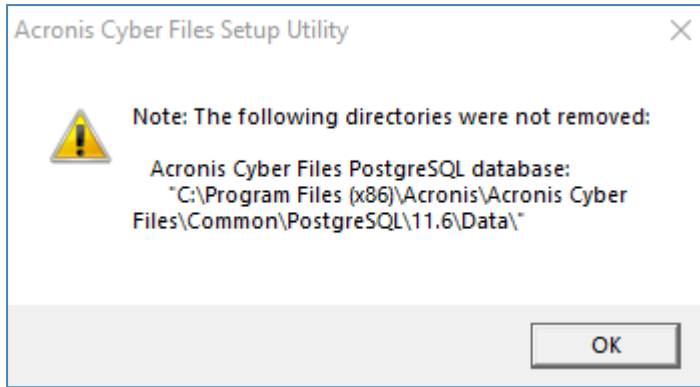
古い Acronis Cyber Files サーバーのインストーラを起動します。

[ようこそ] 画面で **[次へ]** をクリックします。

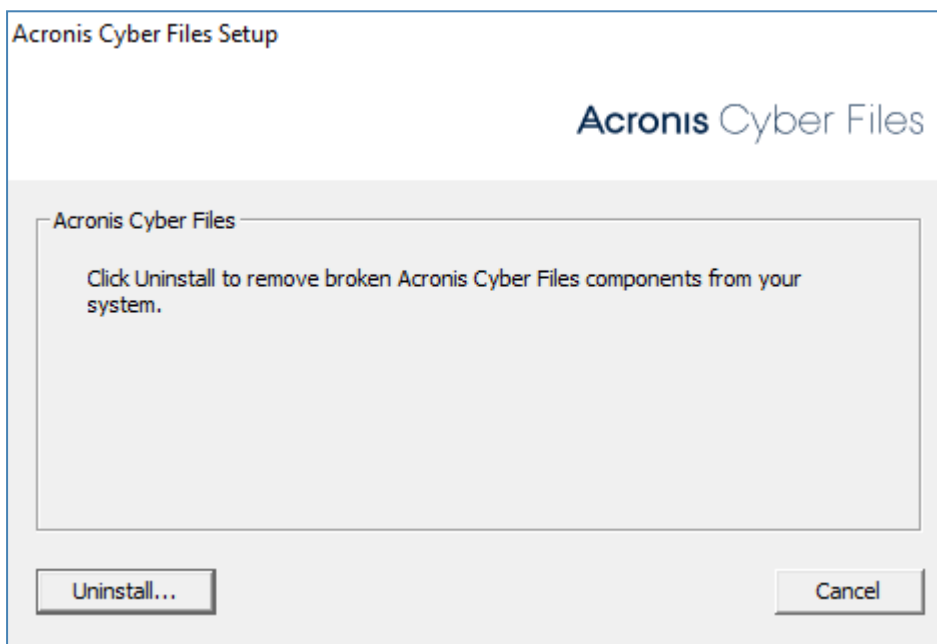
1. 内容を読んで **[OK]** をクリックし、エンドユーザーライセンス契約 (EULA) を受け入れます。
2. **[アンインストール]** をクリックします。
3. [Acronis Cyber Files PostgreSQL サーバー] のみを選択して、**[次へ]** をクリックします。



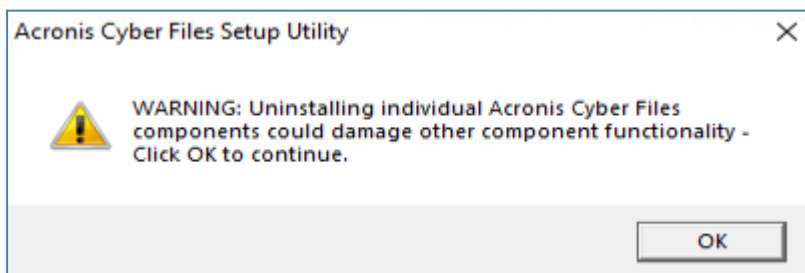
4. アンインストールが完了したら、次の警告ダイアログが表示されます。



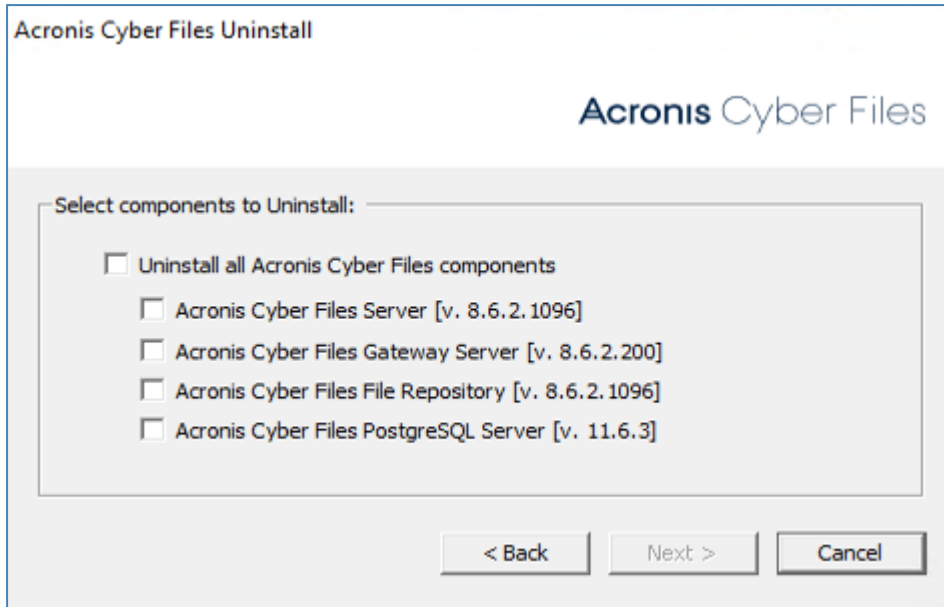
5. **[OK]** をクリックします。
次のウィンドウが表示されます。



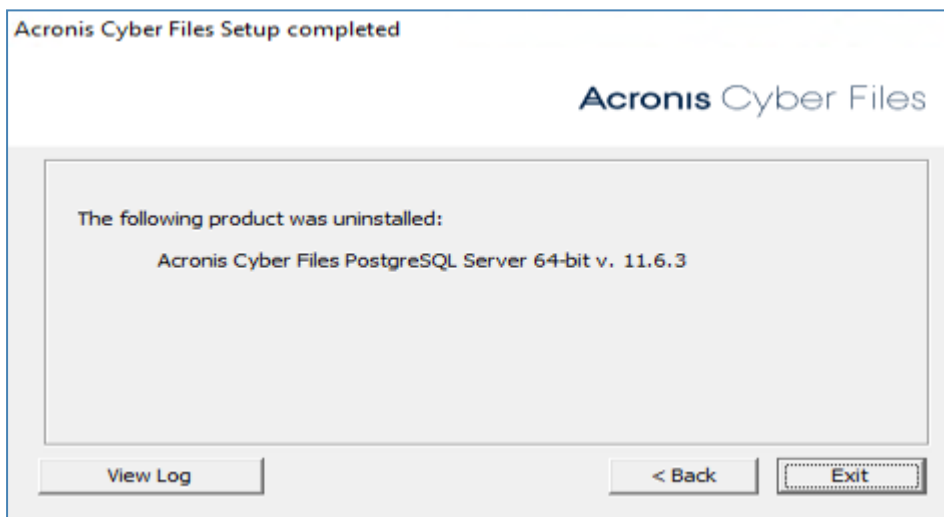
6. **[アンインストール...]** をクリックします。.
次の警告ダイアログが表示されます。



7. **[OK]** をクリックします。
Acronis Cyber Files のアンインストールの初期ウィンドウが再度表示されます。



8. [キャンセル] をクリックします。
次の確認ウィンドウが表示されます。



9. [終了] をクリックします。
10. サーバマシンを再起動します。
11. C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common に移動し、手順 6 に従って PostgreSQL フォルダを削除します。

注意

アンインストールが完了したら、Windows サービスのリストに **AcronisAccessPostgreSQL** が表示されなくなります。

手順 2: 新しいバージョンの PostgreSQL をインストールする

新しいバージョンの PostgreSQL をインストールするには、次の手順を実行します。

1. **[サービス]** コントロールパネルを開いて、Acronis Cyber Files Tomcat サービスを停止します。
2. 新しい Acronis Cyber Files サーバーのインストーラを起動します。

注意

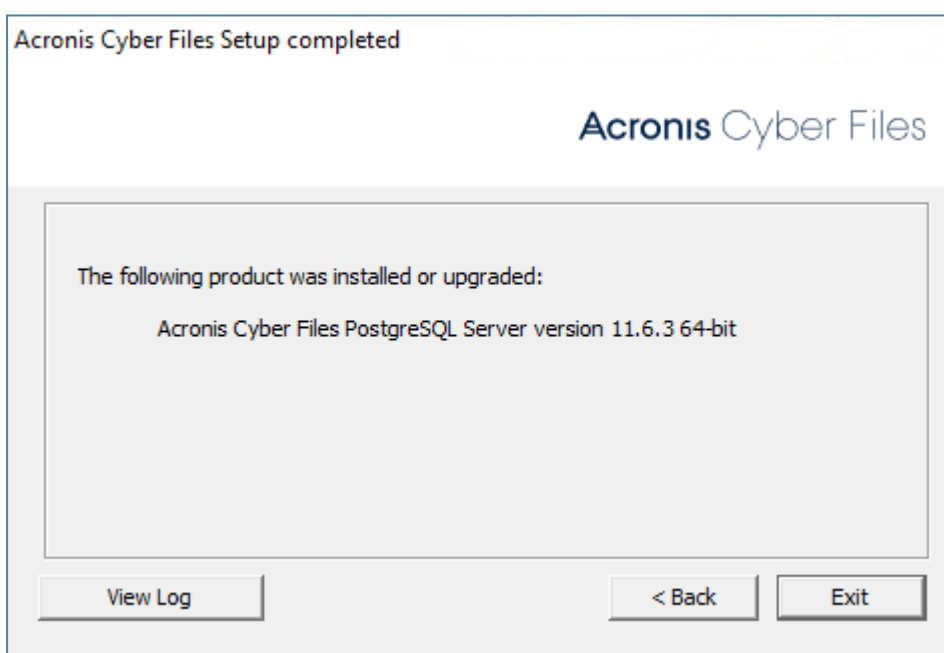
最新バージョンの Acronis Cyber Files サーバーのインストーラは、
<https://www.acronis.com/products/file-sync-and-share-downloads/> からダウンロードするか、
テクニカルサポート (<https://support.acronis.com/mobility>) にお問い合わせください。

3. [ようこそ] 画面で **[次へ]** をクリックします。
4. 内容を読んで **[OK]** をクリックし、エンドユーザーライセンス契約 (EULA) を受け入れます。
5. **[カスタム]** をクリックします。
6. [Acronis Cyber Files PostgreSQL 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. DB をインストールするデフォルトの場所を確認して、**[次へ]** をクリックします。
8. DB パスワードを設定して、**[次へ]** をクリックします。
9. **[インストール]** をクリックして、PostgreSQL DB のインストールを開始します。

注意

このプロセスにかかる時間は、サーバーのリソースにより異なります。

インストールが完了すると、次のウィンドウが表示されます。



10. **[終了]** をクリックします。

注意

インストールが完了したら、Windows サービスのリストに **AcronisAccessPostgreSQL** が再度表示されるようになります。

手順 3: DB コンテンツをインポートする

DB コンテンツをインポートするには、次の手順を実行します。

1. Acronis Cyber Files PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続して、**[データベース]** を選択します。
2. `acronisaccess_production` という名前のデータベースがあることを確認します。
3. データベースを右クリックして、**[更新]** をクリックします。
4. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。

注意

データベースにテーブルがある場合は、データベースを右クリックして、名前を `oldacronisaccess_production` に変更します。

最後に、**[データベース]** に移動して右クリックし、`acronisaccess_production` という名前の新しいデータベースを作成します。

5. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
6. コマンドプロンプトで、PostgreSQL bin ディレクトリに移動します。
例: `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
7. データベースのバックアップファイル `alldbs.sql` (またはユーザーが付けたファイル名) を **bin** ディレクトリにコピーします。
8. コマンドプロンプトで、次のコマンドを実行します: `psql -U postgres -f alldbs.sql`
9. `postgres` パスワードを求められたら入力します。

注意

復元処理には時間がかかる場合があります。この時間はデータベースのサイズにより異なります。

10. 復元が完了したら、コマンドプロンプトのウィンドウを閉じます。
11. **Acronis Cyber Files PostgreSQL Administrator** をもう一度開き、ローカルデータベースサーバーに接続します。
12. **[データベース]** を選択します。
13. `acronisaccess_production` データベースを開き、**[スキーマ]**、**[Public]** の順に展開します。**テーブル** の数が元のサーバーと同じであることを確認します。
14. データベースサービス Acronis Cyber Files PostgreSQL サーバーを開始します。

ファイルリポジトリのアップグレード

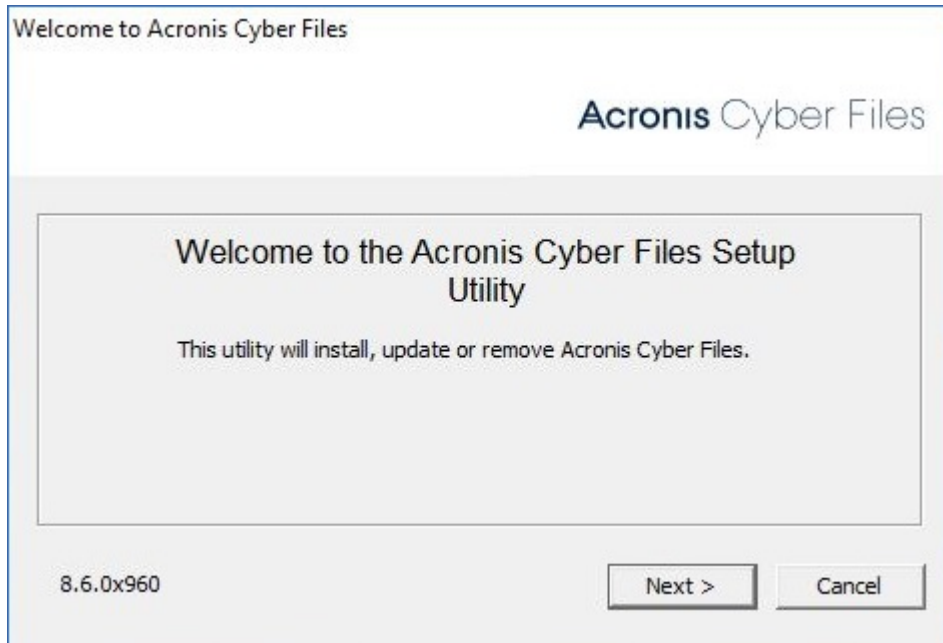
どこに存在するかに関係なく、まずファイルリポジトリをアップグレードします。

1. Acronis Cyber Files インストーラをファイルリポジトリコンポーネントが存在するコンピューターにコピーして実行します。

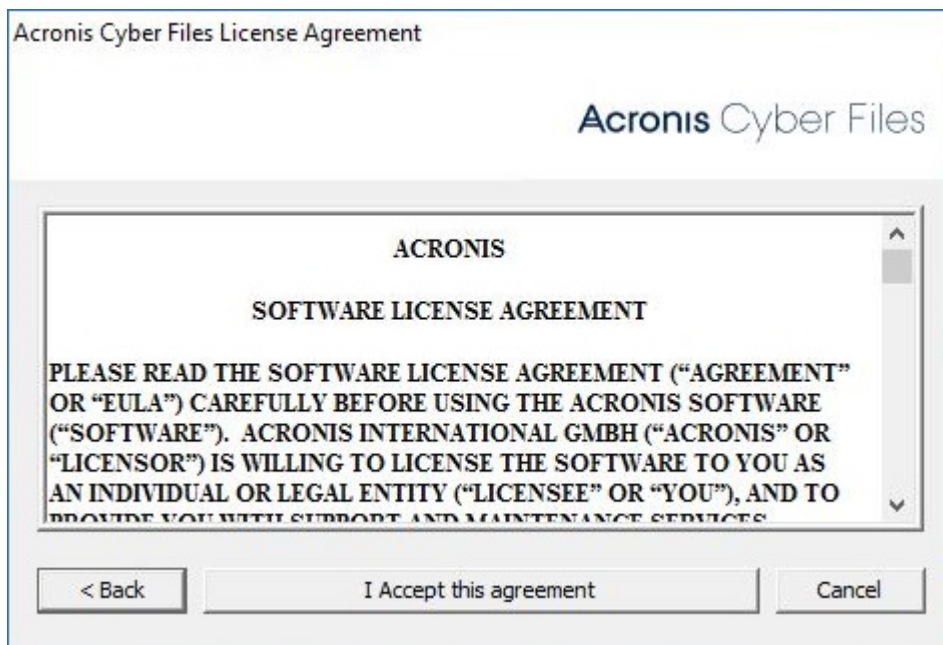
注意

複数のファイルリポジトリサービスを使用している場合は、他のコンポーネントに進む前に、すべてのリポジトリに対してこれらのステップを繰り返します。

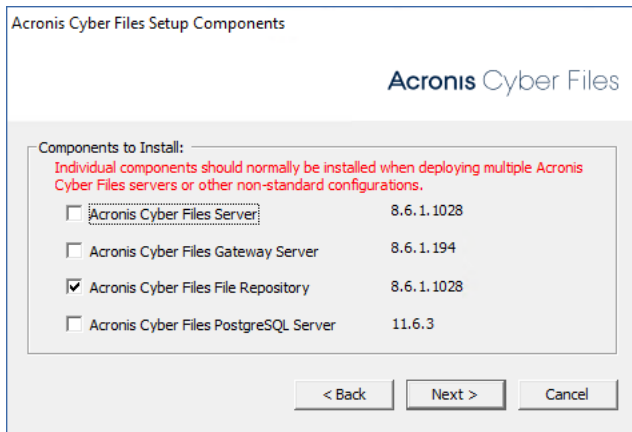
2. ようこそ画面で、[次へ] をクリックします。



3. 使用許諾契約に同意します。



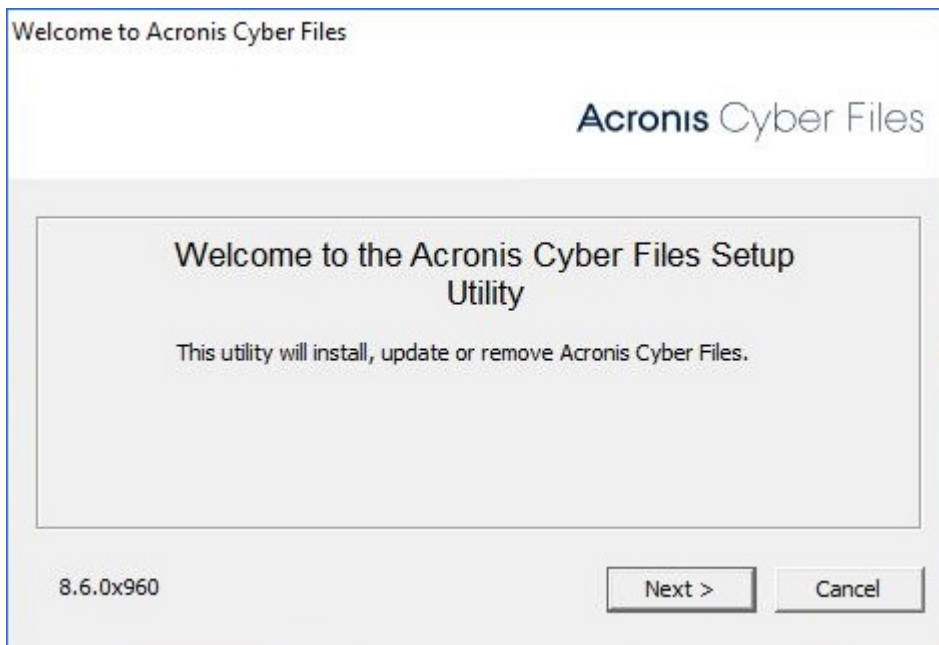
4. [カスタム...] を選択して、アップグレードする Acronis < PRODUCT_NAME > ファイルリポジトリのみを選択します。



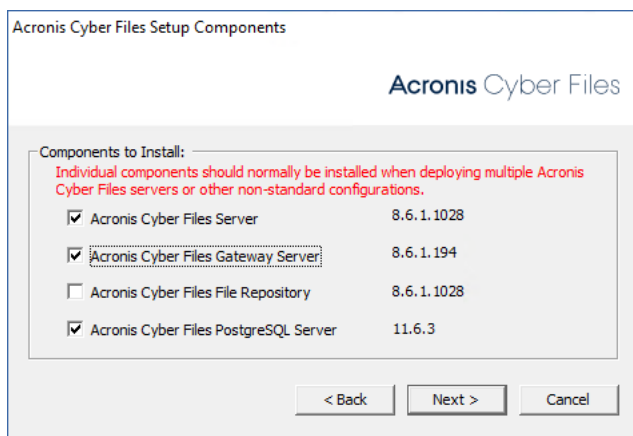
5. [次へ] をクリックして、インストールの内容を確認し、[インストール] をクリックします。
6. アップグレードが完了したら、[終了] をクリックします。設定ユーティリティが起動したら、[OK] をクリックします。
7. 対応するマシン上の**プライマリ** Acronis Cyber Files Web サーバーをアップグレードして続行します。

プライマリ Cyber Files サーバーのアップグレード

1. Acronis Cyber Files Advanced インストーラを **プライマリ** Acronis Cyber Files Web サーバー マシンにコピーします。
2. **プライマリ** ノードで、Acronis Cyber Files インストーラを開始します。



3. ようこそ画面で [次へ] をクリックしてから、[カスタム] をクリックします。これにより、他のインストールを必要とせず、既にコンピュータにインストール済みの必要なサービスのみをアップグレードすることができます。
4. アップグレードする Acronis Cyber Files サービスを選択します。Acronis Cyber Files Web サーバーと既にコンピューター上に存在するすべてのコンポーネントだけを選択します。



5. **[インストール]** をクリックしてインストーラを終了し、**設定ユーティリティ**を起動します。

注意

設定ユーティリティの設定を変更しないでください！設定を変更すると、構成に問題が生じる可能性があります。

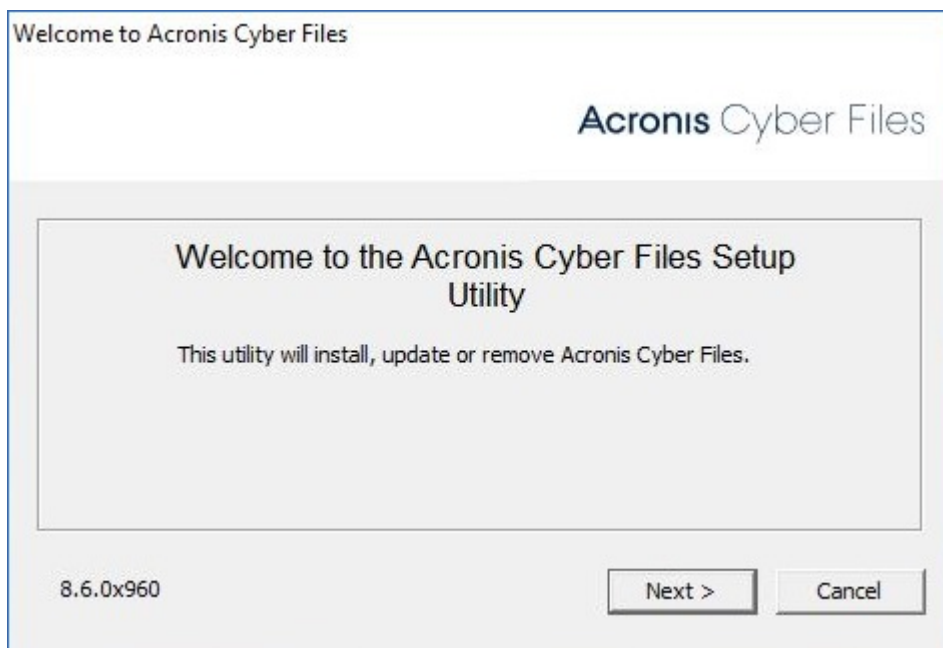
6. 設定ユーティリティですべての必要なサービスを開始して、データベース移行が終了したら、**プライマリ**サーバーで Acronis Cyber Files Web インターフェースが想定どおりに動作することを確認します。Web ブラウザが自動的に起動して、Acronis Cyber Files サーバーのログイン画面が表示されます。
7. 管理者としてログインし、設定が同じで、変更や問題がないことを確認します。
8. 他のコンポーネントのアップデート中は、Acronis Cyber Files のこのインスタンスを実行したままにします。

警告

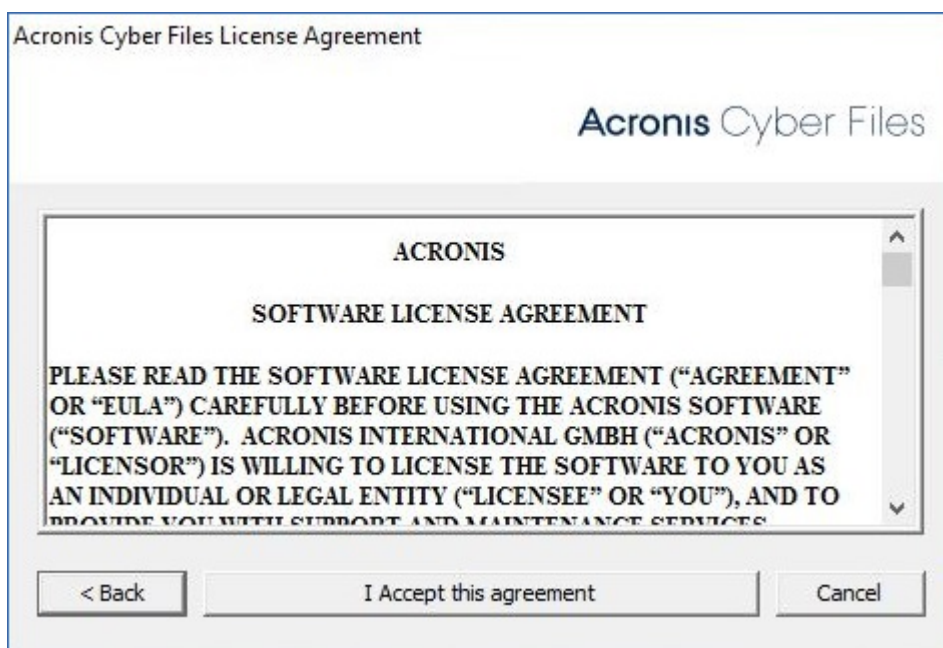
プライマリ Tomcat サーバーが実行され、正しく動作していることを確認するまでは、他の Acronis Cyber Files Tomcat サーバーをアップグレードまたは開始しないでください。

ゲートウェイ サーバーのアップグレード

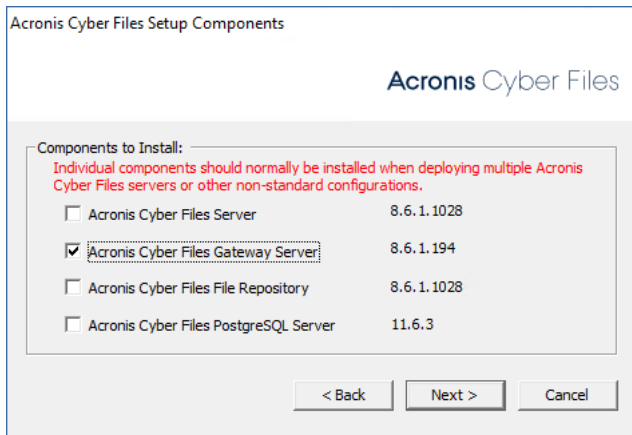
1. Acronis Cyber Files インストーラをゲートウェイサーバーのみを含むコンピューターにコピーして実行します。
2. ようこそ画面で、**[次へ]** をクリックします。



3. 使用許諾契約に同意します。



4. [カスタム...] を選択して、アップグレードする Acronis Cyber Files ゲートウェイサーバーのみを選択します。

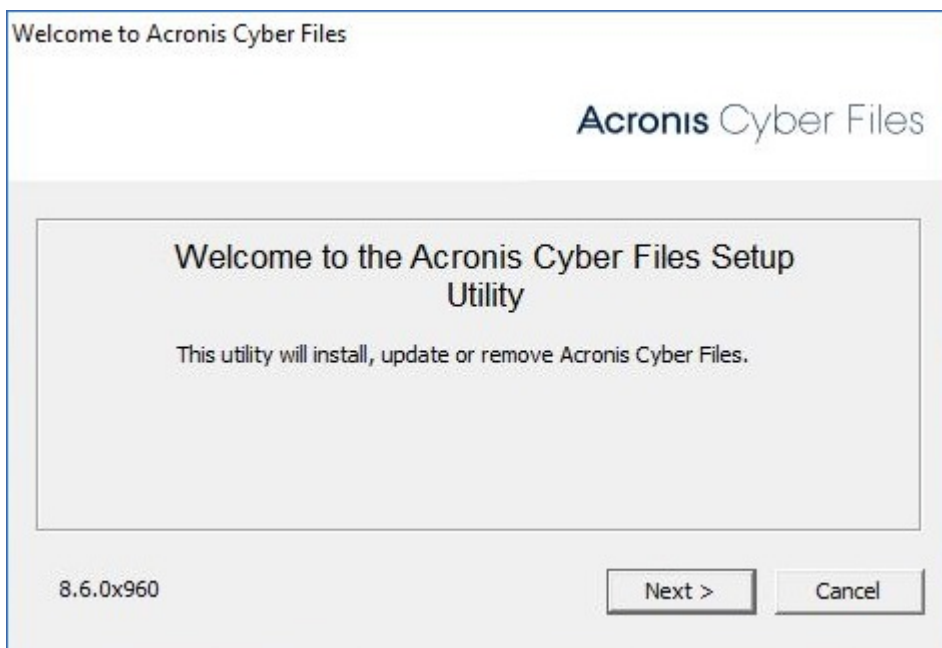


5. **[次へ]** をクリックして、インストールの内容を確認し、**[インストール]** をクリックします。
6. アップグレードが完了したら、**[終了]** をクリックします。設定ユーティリティが起動したら、**[OK]** をクリックします。

残りのすべてのノードのアップグレード

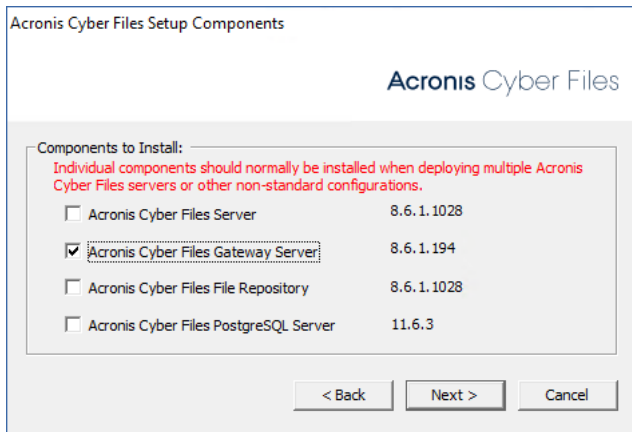
プライマリ Acronis Cyber Files ノード、すべてのファイル・リポジトリ・サーバー、およびすべてのゲートウェイサーバーのアップデートに成功したら、残りの Acronis Cyber Files サーバーのアップグレードに進みます。

1. アップグレード対象のノードに Acronis Cyber Files インストーラをコピーして実行します。

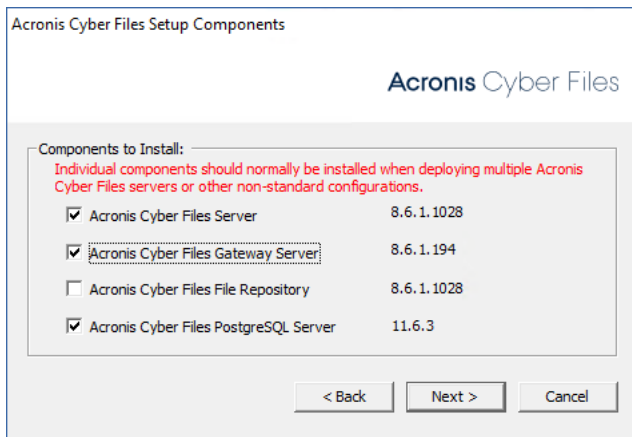


2. ようこそ画面で **[次へ]** をクリックしてから、**[カスタム]** をクリックします。これにより、他のインストールを必要とせず、既にコンピュータにインストール済みの必要なサービスのみをアップグレードすることができます。
3. アップグレードする Acronis Cyber Files サービスを選択します。既にコンピュータに存在するサービスのみを選択します。

例: インストールされたゲートウェイサーバーが1台のみである場合には、インストーラではゲートウェイサーバーコンポーネントのみを選択します。



例: ゲートウェイサーバーと Acronis Cyber Files サーバーが存在する場合は、両方を選択します。



4. **[インストール]** をクリックしてインストーラを終了し、**設定ユーティリティ**を起動します。

注意

設定ユーティリティの設定を変更しないでください。設定を変更すると、構成に問題が生じる可能性があります。

5. 設定ユーティリティですべての必要なサービスを開始した後に、このノードで Acronis Cyber Files コンポーネントが期待どおり動作することを確認します。

モバイル アクセス

このセクションの Web インターフェースには、モバイル デバイス ユーザーに影響を与えるすべての設定と構成が含まれています。

コンセプト

Acronis Cyber Files モバイルクライアントは、サードパーティのサービスを使用せずにサーバーに直接接続するため、管理者が常に管理できます。Acronis Cyber Files サーバーは、既存のファイルサーバーと同じネットワークにインストールが可能で、iPad、iPhone、または Android デバイスからそのサーバー上のファイルにアクセスできます。これらのファイルは通常、PC で Windows ファイル共有機能を使用して既に利用できるようになっているファイルや、Mac で Files Connect サーバーを使用して既に利用できるようになっているファイルと同じです。

クライアントは Active Directory のユーザーアカウントを使用して Acronis Cyber Files サーバーにアクセスします。Acronis Cyber Files 内で追加のアカウントを設定する必要はありません。AD 以外のユーザーにアクセス権を付与する必要がある場合に備えて、Acronis Cyber Files アプリは、Acronis Cyber Files が実行されている Windows サーバー上で構成されたローカルコンピューターアカウントを使用したファイルアクセスもサポートします。後に説明するクライアント管理機能には AD のユーザー アカウントが必要です。

導入の最小構成は、Acronis Cyber Files のデフォルトのインストールを実行する 1 台の Windows サーバーで構成されます。このデフォルトのインストールには、Acronis Cyber Files サーバーコンポーネントとローカル Acronis Cyber Files ゲートウェイサーバーが含まれます。このシナリオでは、Acronis Cyber Files ユーザーがこの 1 台のファイルサーバーに接続でき、モバイルデバイスでのクライアント管理が可能になります。クライアント管理が不要な場合、データソースをローカルゲートウェイサーバーにセットアップでき、Acronis Cyber Files モバイルクライアントはこれらのデータソースにアクセスできますが、ユーザーがそのアプリケーション設定を管理します。

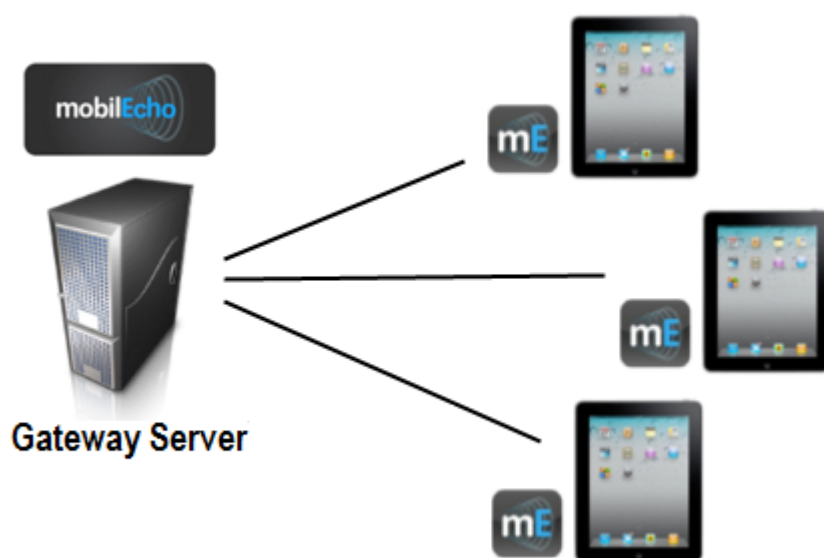


図 1. 単一の Acronis Cyber Files サーバーとローカルゲートウェイサーバー

任意の数のゲートウェイサーバーを後でネットワークに追加して、Cyber Files クライアントからのアクセスを設定できます。

注意

Acronis Cyber Files のインストールの詳細は、本書の「[インストール](#)」セクションに記載されています。ゲートウェイサーバーとデータソースの構成は、「[モバイル アクセス](#)」のセクションで説明しています。

モバイルクライアントをリモート管理する場合、Acronis Cyber Files Management を使用して、Active Directory のユーザーまたはグループごとにポリシーを作成することができます。Acronis Cyber Files サーバーが 1 台だけ必要であり、ポリシーによって以下が可能になります。

- 一般的なアプリケーションの設定を構成する
- クライアント アプリケーションに表示されるサーバー、フォルダ、ホーム ディレクトリを割り当てる
- ファイルで実行できる操作を制限する
- Acronis Cyber Files ファイルを開くことができる他のサードパーティアプリを制限する
- セキュリティ要件（サーバー ログインの頻度、アプリケーション ロック パスワードなど）を設定する
- デバイスにファイルを保存する機能を無効にする
- Acronis Cyber Files ファイルを iTunes バックアップに含める機能を無効にする
- ユーザーのアプリケーション ロック パスワードをリモートからリセットする
- モバイルアプリのローカルデータと設定のリモートワイプを実行する
- その他の多くの設定およびセキュリティ オプション

一般的なネットワーク使用クライアント管理では、Acronis Cyber Files サーバーと Acronis Cyber Files ゲートウェイサーバーコンポーネントがインストールされた 1 台のサーバーと、ファイルサーバーとして機能する複数の追加のゲートウェイサーバーが含まれます。このシナリオでは、すべてのモバイルクライアントが、Acronis Cyber Files サーバーで管理されるように構成され、Acronis Cyber Files アプリケーションが起動されるたびにこのサーバーに接続して、設定変更をチェックし、必要な場合にはアプリケーションロックパスワードのリセットやリモートワイプコマンドを受け入れます。

Acronis Cyber Files クライアントには、クライアントの管理ポリシーで、サーバーのリスト、共有ボリューム内の特定のフォルダ、およびホームディレクトリを割り当てることができます。これらのリソースは、Acronis Cyber Files アプリに自動的に表示され、クライアントアプリはファイルアクセスの必要性に応じてこれらのサーバーに直接接続します。

注意

クライアント管理の有効化と構成の詳細は、本書の「[ポリシー](#)」セクションと「[モバイル デバイスの管理](#)」セクションに記載されています。

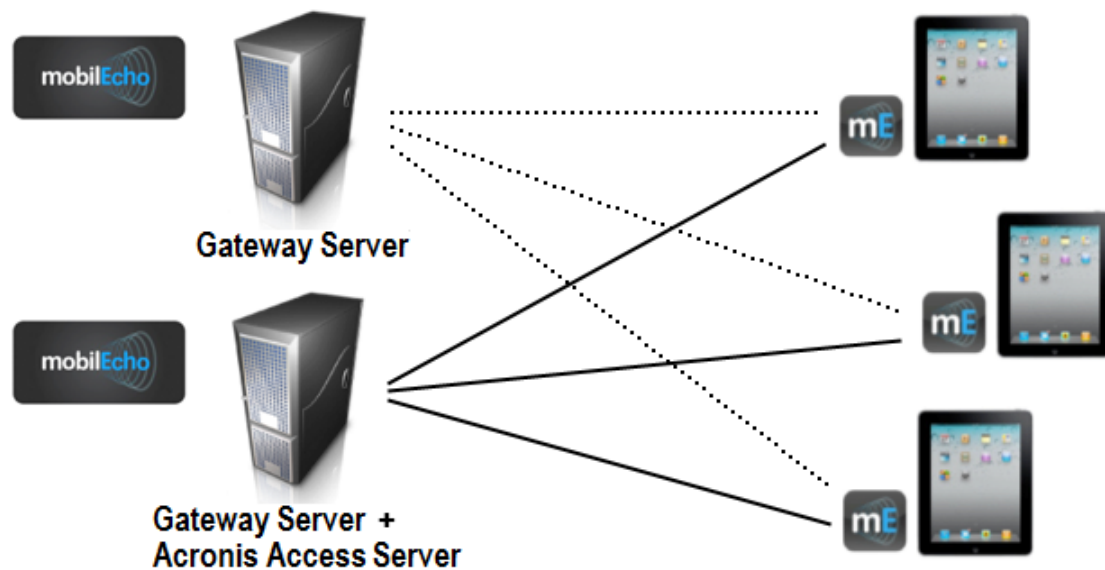


図 2.1 1 台のゲートウェイサーバー、1 台のゲートウェイサーバー + Acronis Cyber Files サーバー

ポリシー

Acronis Cyber Files では、Active Directory のグループにポリシーを割り当てることができます。グループポリシーは通常、ほとんどすべてのクライアント管理要件を満たします。グループポリシーのリストは優先順位順に表示され、リスト内の一番上のグループの優先順位が最も高くなります。ユーザーが Acronis Cyber Files サーバーに接続したときには、ユーザーがメンバーになっている最も優先順位が高い 1 つのグループポリシーによって設定が決定されます。

ユーザーポリシーはグループポリシーより優先順位が高いため、ユーザーが属するグループとは無関係に、ユーザーに特定の設定を実行されたときにユーザーポリシーを使用します。ユーザーポリシーは、グループポリシーより優先されます。

注意

グループの管理に関するヒント:

すべて、またはほとんどのユーザーに同じポリシー設定を適用する場合、**[デフォルト]** グループポリシーを使用できます。グループポリシーのメンバーではなく、明示的なユーザーポリシーがないすべてのユーザーは、**[デフォルト]** グループのメンバーになります。デフォルトでは、**[デフォルト]** グループが有効になっています。特定のユーザーのグループによる Acronis Cyber Files 管理へのアクセスを拒否する場合、それらのユーザーがどの設定済みグループポリシーのメンバーにもなっていないことを確認します。ユーザーアカウントがいずれかのグループポリシーと一致しない限り、それらのユーザーは Acronis Cyber Files クライアント管理への登録を拒否されます。

Group Policies
User Policies
Allowed Apps
Default Access Restrictions

Manage Group Policies

Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

+ Add Group Policy
Filter by
Name
Filter
Reset

Common Name / Display Name	Distinguished Name		Enabled	
Domain Users	CN=Domain Users,CN=Users,DC=test,DC=biz	↑ ↓	☒	×
Default			☒	

新しいポリシーの追加

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。

Acronis Cyber Files
Leave Administration

Group Policies
User Policies
Allowed Apps
Default Access Restrictions

Manage Group Policies

Group policies configure the mobile client's application settings, capabilities and security settings. The group policy list is shown in the order of precedence. The first group in the list that a user belongs to will determine their policy.

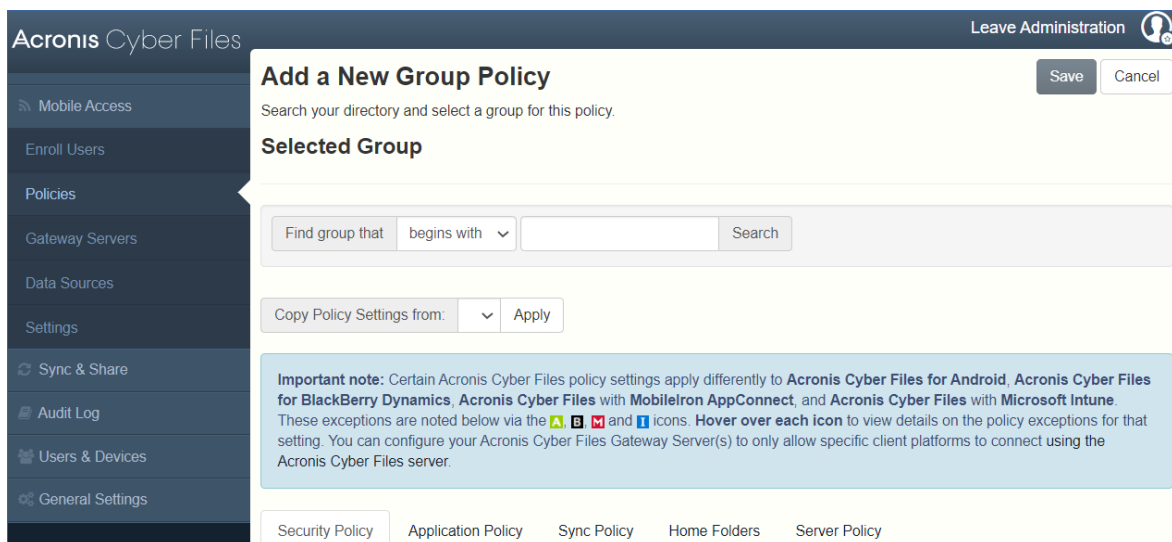
+ Add Group Policy
Filter by
Name
Filter
Reset

Common Name / Display Name	Distinguished Name		Enabled	
Default			☒	

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] ページが開きます。



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。

ポリシーの変更

既存のポリシーをいつでも変更することができます。ポリシーの変更は、関連するモバイルアプリユーザーが次にモバイルアプリを起動したときにユーザーに適用されます。

注意

接続要件

Acronis Cyber Files クライアントが、プロファイルの更新、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 Cyber Files 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 Cyber Files 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 に接続する必要もあります。

グループポリシーを変更するには、次の操作を行います。

1. トップメニューバーの **[グループポリシー]** オプションをクリックします。
2. 変更するグループをクリックします。
3. **[グループポリシーの編集]** ページで必要な変更を加え、**[保存]** を押します。
4. ポリシーを一時的に無効にするには、目的のグループの **[有効]** 列のチェックボックスをオフにします。この変更は即座に有効になります。
5. グループの優先順位を変更するには、**[Manage Group Profiles]** リストで上向きまたは下向きの矢印をクリックします。これにより、プロファイルのレベルが 1 つ上または下に移動します。

ユーザー ポリシーを変更するには、次の操作を行います。

1. [ユーザー ポリシー] タブを選択します。
2. 変更するユーザーをクリックします。
3. [ユーザー ポリシーの編集] ページで必要な変更を加え、[保存] を押します。
4. ポリシーを一時的に無効にするには、目的のユーザーの [有効] 列のチェックボックスをオフにします。すぐに無効化されます。

ポリシーの設定

セキュリティ ポリシー

Security Policy	Application Policy	Sync Policy	Home Folders	Server Policy
App Password Creation: ⓘ ⓘ ⓘ ☒ Optional ☐ Disabled ☐ Required App Will Lock: Immediately upon exit ▼ ☐ Allow User to Change This Setting Minimum Password Length: 0 Minimum Number of Complex Characters (such as \$,&,!): 0 ☐ Require One or More Letter Characters ☐ Mobile client app will be wiped after 10 ▼ failed app password attempts				
☐ Wipe or Lock After Loss of Contact Mobile client app will be locked ▼ after 30 days of failing to contact this client's Acronis Cyber Files server ☐ Warn user starting 5 days beforehand				
App Crash Reporting: ⓘ ☒ Never send reports ☐ Allow user to choose to send reports ☐ Always send reports				
☒ Allow iTunes and iCloud to Back up Locally Stored Acronis Cyber Files Files ⓘ ⓘ ☐ User Can Remove Mobile Client from Management ☐ Wipe All Acronis Cyber Files Data on Removal				

- **アプリのパスワードの作成:** モバイルアプリケーションにロックパスワードを設定して、そのパスワードを最初に入力しなければアプリケーションを起動できないようにすることができます。
 - **オプション:** この設定は、アプリケーション ロック パスワードの設定をユーザーに強制しませんが、必要な場合にアプリケーションの **[設定]** メニューからパスワードを設定できます。
 - **無効:** この設定は、アプリの **[設定]** メニューからアプリケーション ロック パスワードを設定する機能を無効にします。これは、共有されているモバイルデバイスで、ユーザーがアプリケーションパスワードを設定して他のユーザーが使用できないようにモバイルアプリをロックすることを防ぐ場合に役に立ちます。
 - **必須:** この設定は、ユーザーがアプリケーション ロック パスワードを設定していない場合に、設定を強制します。オプションのアプリケーション パスワードの複雑さの要件およびパスワード試行失敗による消去の設定は、**[アプリのパスワードの作成]** を **[必須]** に設定した場合のみ適用されます。
 - **アプリのロックのタイミグ:** アプリケーション パスワードの入力が免除される期間を設定します。ユーザーがデバイス上で Acronis Cyber Files モバイルアプリから別のアプリケーションに切り替えた後、この猶予期間が切れる前にこのモバイルアプリに戻る場合は、アプリケーションロック パスワードを入力する必要がなくなります。パスワードを毎回入力することを必須にするには、**[終了時]** を選択します。ユーザーがモバイルアプリの設定で **[アプリのロックのタイミグ]** 設定を変更できるようにする場合は、**[ユーザーが設定を変更できるようにする]** を選択します。
 - **最短パスワード長:** アプリケーション ロック パスワードとして許可される最小文字数。
 - **最低限含めなければならない文字の種類の数:** アプリケーション ロック パスワードに必要な文字および数字以外の文字の最小数。
 - **1 つ以上の文字が必要:** アプリケーション パスワード内に 1 つ以上の文字が含まれるようにします。
 - **アプリのパスワードの試行を X 回失敗した場合、モバイル クライアント アプリをワイプする:** このオプションを有効にすると、指定した回数連続してアプリケーション パスワードの入力に失敗した場合に モバイルアプリの設定とデータが消去されます。
- **接続がない場合にワイプまたはロックする:** 一定の日数にわたり Acronis Cyber Files サーバーへの接続が行われなかった場合に、モバイルアプリを自動的にワイプまたはロックするには、この設定を有効にします。

警告

何らかの理由でアプリがサーバーへの認証に失敗した場合、サーバーが到達可能であったとしても、サーバーに接続しているとはみなされません。

- 後でロックされたクライアントがサーバーに正常に接続した場合、自動的にロック解除されます。
- クライアントが消去された場合、モバイルアプリに保存されているすべてのローカルファイルとクライアント管理ポリシーが削除され、すべての設定がデフォルトにリセットされます。消去されたクライアントがゲートウェイサーバーにアクセスするには、管理に再登録する必要があります。
- **このクライアントの Acronis Cyber Files サーバーへのアクセスに X 日間失敗したらモバイルクライアント アプリをロックする/ワイプする:** 指定された日数の間にクライアントがこの Acronis Cyber Files サーバーに接続しない場合のデフォルトの操作を設定します。

- **[] 日前からユーザーに警告:** モバイルアプリでは、「接続がない」ためにワイプまたはロックが行われる日が近づいたときに、オプションでユーザーに警告することができます。これにより、ネットワーク接続を再び確立し、モバイルアプリが Acronis Cyber Files サーバーに接続して、ロックまたはワイプを防ぐ機会を防ぐ機会をユーザーに与えることができます。
- **アプリのクラッシュレポート:** モバイルアプリがクラッシュした場合に、レポートを Acronis に送信します。個人データや識別情報は送信されません。
 - **レポートを送信しない**
 - **レポート送信を許可する**
 - **常にレポート送信する**
- **iTunes と iCloud でローカルに保存された Acronis Cyber Files ファイルをバックアップできるようにする:** この設定が無効になっている場合、モバイルアプリは iTunes または iCloud でファイルをバックアップできません。これにより、Acronis Cyber Files のセキュリティで保護されたデバイスのストレージ内のファイルがバックアップにコピーされなくなります。
- **ユーザーがモバイルクライアントを管理から削除できる:** Acronis Cyber Files ユーザーが Acronis Cyber Files 内の自分の管理ポリシーをアンインストールできるようにする場合はこの設定を有効にします。このオプションを設定することで、アプリケーションの完全な機能が戻り、ポリシーによって変更された構成を復元することができます。
 - **削除されたときにすべての Acronis Cyber Files:** ユーザーによるポリシーの削除が有効になっている場合に、このオプションを選択できます。有効になっている場合、プロファイルが管理から削除された場合に、モバイルアプリケーション内にローカルで保存されているすべてのデータが消去されます。これにより、管理されていないクライアント上に会社のデータが存在しないようにすることができます。

アプリケーションポリシー

Security Policy	Application Policy	Sync Policy	Home Folders	Server Policy
☒ Require Confirmation When Deleting Files ☒ Allow User to Change This Setting				
☐ Set the Default File Action A Default Action: Show Action Menu ☐ Allow User to Change This Setting				
☒ Allow Files to be Stored on This Device ☒ Allow User to Store Files in the 'My Files' On-Device Folder ☒ Cache Recently Accessed Files on the Device Maximum Cache Size: 100 MB ☒ Allow User to Change This Setting				
☒ Content in My Files and File Inbox Expires after 21 days ☐ Block the download of files and folders larger than 0 MB ⓘ				

- **ファイルを削除するときに確認を必須にする:** 有効にすると、ユーザーはファイルを削除するたびに、確認を求められます。ユーザーがこの設定を後で変更できるようにするには、**[ユーザーが設定を変更できるようにする]**を選択します。
- **デフォルトのファイル操作を設定する:** これは、ユーザーがモバイルアプリケーションでファイルをタップしたときの操作を決定するオプションです。この設定がされていない場合、**[操作メニュー]**メニューがクライアントアプリケーションのデフォルトとして使用されます。ユーザーがこの設定を後で変更できるようにするには、**[ユーザーが設定を変更できるようにする]**を選択します。
- **このデバイスにファイルを保存できるようにする:** この設定はデフォルトで有効になっています。有効の場合、ファイルをデバイス上（Cyber Files のサンドボックス化されたストレージ内）に残すことができます。ファイルをローカルに保存するための機能（マイ ファイルフォルダ、同期フォルダ、最近アクセスしたファイルのキャッシュ）を有効または無効にするには、追加のポリシー設定が必要です。このオプションが無効な場合、デバイスにはファイルが保存されません。これにより、デバイ

スの紛失や盗難の際、会社のデータがデバイスに残っていないことを保証できます。この設定が無効な場合、ユーザーはファイルを保存または同期してオフラインで使用する、ファイルをキャッシュしてパフォーマンスを向上させること、[他のアプリで開く] 機能を使用して、別のアプリケーションから Cyber Files モバイルクライアントにファイルを送信することができません。

- **ユーザーがデバイスの [マイ ファイル] フォルダにファイルを保存できるようにする:** 有効にすると、ファイルを [マイ ファイル] フォルダにコピーして、オフラインでアクセス、編集することができます。これは Cyber Files のデバイス上にあるストレージサンドボックス内の汎用ストレージエリアです。
- **最近アクセスしたファイルをデバイスにキャッシュする:** 有効にした場合、サーバー上のファイルのうち最近アクセスしたものが、デバイス上のローカル キャッシュに保存されます。これにより、アクセスしたファイルが変更されていない場合に、パフォーマンスと帯域幅の節約が実現します。 **最大キャッシュ サイズ**を指定し、ユーザーがこの設定をオプションで変更できるようにすることもできます。
- **[マイファイル] と [ファイル受信トレイ] のコンテンツは、X日後に有効期限が切れます:** このオプションが有効の場合、設定した日数が経過すると、[マイファイル] 内のファイルがデバイスから削除されます。
- **X MB より大きいファイルおよびフォルダのダウンロードをブロックする:** このオプションを有効にすると、設定された容量より大きいファイルやフォルダは、モバイルアプリでダウンロードされなくなります。

許可

Allow

These settings can be used to disable certain Acronis Cyber Files mobile client application features and capabilities. All copy, create, move, rename, and delete settings apply to files or folders located on Gateway Servers. Files in Acronis Cyber Files's local **My Files** folder are stored on the device and are not affected. All other settings apply to any files in the app, both server-based and locally stored.

Only file and folder operation settings apply to Mobile Access data sources accessed via the Acronis Cyber Files web client interface. Acronis Cyber Files Desktop Clients will not be permitted to two-way sync folders in Mobile Access data sources if the policy does not grant full access for file and folder operations.

File Operations

☒ File Copies / Creation

☒ File Deletes

☒ File Moves

☒ File Renames

Folder Operations

☒ Folder Copies

☒ Folder Deletes

☒ Folder Moves

☒ Folder Renames

☒ Adding New Folders

☒ Bookmarking Folders

'mobileEcho' File Links

☒ Emailing 'mobileEcho' File Links

☒ Opening 'mobileEcho' File Links

Hyperlinks in Documents

☒ Allow Opening Hyperlinks in Documents

☒ Allow User to Change These Settings

Open Into:

☒ Inline Browser

☐ Default Browser

☐ MobileIron Web@Work

☐ BlackBerry Access

Data Leakage Protection

☒ Opening Acronis Cyber Files in Other Applications

App Allowlist/Blocklist:

☒ Allow use of Document Provider

☒ Sending Files to Acronis Cyber Files from Other Apps

☒ Importing Files from camera/photo library

☒ Emailing Files from Acronis Cyber Files

☒ Printing Files from Acronis Cyber Files

☒ Copying Content from Opened Files

File Editing

☒ Editing & Creation of Office Files

☐ Editing of password protected files

☒ Editing & Creation of Text Files

PDF Editing & Annotation

☐ Allow PDF Editing

☒ Allow PDF Annotation

☒ Allow Creation of Empty PDF Files

☐ Apply custom PDF view settings

☐ Allow User to Change These Settings

☐ Fit to Width

☐ Night Mode

Scroll Direction:

Page Transitions:

Page Display Mode:

Thumbnails:

これらの設定を使用して特定の Mobile アプリケーションの機能を無効にすることができます。コピー、作成、移動、名前の変更、および削除のすべての設定は、ゲートウェイサーバーに置かれているファイルまたはフォルダに適用されます。モバイルクライアントのローカルの [マイファイル] フォルダ内にあるファイルはデバイスに保存され、影響を受けません。他のすべての設定は、サーバーベースか

クライアント上にローカルに保存されているかを問わず、Cyber Files のすべてのファイルに適用されます。

ファイルの操作

- **ファイルのコピー/作成:** このオプションを無効にすると、ユーザーは他のアプリケーションや iPad 写真ライブラリからゲートウェイ サーバーにファイルを保存できません。また、ゲートウェイ サーバーに新しいファイルやフォルダをコピーまたは作成することもできません。この設定は、クライアントにファイルの作成を許可する NTFS アクセス権よりも優先されます。
- **ファイルの削除:** このオプションを無効にすると、ゲートウェイ サーバーからファイルを削除できなくなります。この設定は、クライアントにファイルの削除を許可する NTFS アクセス権よりも優先されます。
- **ファイルの移動:** このオプションを無効にすると、ユーザーは、ゲートウェイ サーバー上のあるロケーションから別のロケーションへ、またはゲートウェイサーバーからモバイルアプリケーションのローカル [マイ ファイル] ストレージへファイルを移動することができません。この設定は、クライアントにファイルまたはフォルダの移動を許可する NTFS アクセス権よりも優先されます。
- **ファイル名の変更:** このオプションを無効にすると、ゲートウェイ サーバーのファイルの名前が変更できなくなります。この設定は、クライアントにファイル名の変更を許可する NTFS アクセス権よりも優先されます。

フォルダの操作

- **フォルダのコピー:** このオプションを無効にすると、ユーザーはゲートウェイ サーバーでフォルダをコピーしたり、ゲートウェイ サーバーにフォルダをコピーすることができません。この設定は、クライアントにフォルダの作成を許可する NTFS アクセス権よりも優先されます。この設定を有効にするには、[ファイルのコピー/作成] を有効にする必要があります。
- **フォルダの削除:** このオプションを無効にすると、ゲートウェイ サーバーからフォルダを削除できなくなります。この設定は、クライアントにファイルまたはフォルダの削除を許可する NTFS アクセス権よりも優先されます。
- **フォルダの移動:** このオプションを無効にすると、ゲートウェイサーバー上のあるロケーションから別のロケーションへ、またはゲートウェイサーバーから Acronis Cyber Files モバイルアプリケーションのローカル [マイ ファイル] ストレージへフォルダを移動することができません。この設定は、クライアントにファイルまたはフォルダの移動を許可する NTFS アクセス権よりも優先されます。この設定を有効にするには、[フォルダのコピー] を有効にする必要があります。
- **フォルダ名の変更:** このオプションを無効にすると、ゲートウェイ サーバーのフォルダの名前を変更できなくなります。この設定は、クライアントにフォルダ名の変更を許可する NTFS アクセス権よりも優先されます。
- **新しいフォルダを追加:** このオプションを無効にすると、ユーザーはゲートウェイ サーバーで新しい空のフォルダを作成できません。
- **フォルダのブックマーク:** このオプションを無効にすると、ユーザーはデバイス上またはサーバー上の Acronis Cyber Files フォルダにすばやくアクセスするためのブックマークを登録することができなくなります。

'mobilEcho' ファイルのリンク

- **'mobilEcho' ファイルのリンクを電子メールで送信する:** このオプションを無効にすると、ユーザーは Acronis Cyber Files ファイルまたはフォルダへの mobilEcho:// URL を、他の Acronis Cyber Files ユーザーに送信できません。このようなリンクは、受信者が Acronis Cyber Files モバイルクライアントをインストールしており、サーバーを構成しているデバイス、またはリンクロケーションへのアクセス権を持つフォルダを割り当てたデバイスで開いた場合のみ正常に動作します。また、このユーザーには、アイテムを読み取るための、ファイル/フォルダレベルのアクセス権も必要です。
- **'mobilEcho' ファイルのリンクを開く:** このオプションを無効にすると、ユーザーは Acronis Cyber Files ファイルまたはフォルダへの mobilEcho:// URL を開くことができなくなります。

ドキュメント内のハイパーリンク

- **ドキュメント内のハイパーリンクの参照を許可する:** 有効にすると、ドキュメント内にあるすべてのハイパーリンクを開くことができます。
 - **ユーザーが設定を変更できるようにする:** 有効にすると、設定に基づいて機能を有効化、無効化できます。
 他のアプリで開く:
 - **インラインブラウザ:** ハイパーリンクが Acronis Cyber Files アプリで直接開かれます。
 - **デフォルトのブラウザ:** ハイパーリンクがデバイスで選択されたデフォルトのブラウザで開かれます。
 - **MobileIron Web@Work:** ハイパーリンクは、MobileIron Web@Workアプリで開かれます。

データ漏えいの防止

- **Acronis Cyber Files ファイルを別のアプリケーションで開く:** このオプションを無効にすると、モバイルアプリケーションに **[他のアプリで開く]** ボタンは表示されず、Acronis Cyber Files のファイルを別のアプリケーションで開くことは許可されません。別のアプリケーションで開かれたファイルは、そのアプリケーションのデータ ストレージ エリアにコピーされ、Acronis Cyber Files では制御できなくなります。
 - **アプリの許可リスト/ブロックリスト:** デバイスで Acronis Cyber Files ファイルを開くことのできるサードパーティアプリケーションを制限するために、あらかじめ定義されている許可リストまたはブロックリストを選択します。許可リストまたはブロックリストを作成するには、トップメニューバーの **[許可されたアプリ]** をクリックします。
- **ドキュメントプロバイダの使用を許可する:** モバイルデバイスが Acronis Cyber Files のドキュメントプロバイダ拡張機能を使用できるようにします。ドキュメントプロバイダ拡張機能は、以下のように特定の設定の影響を受ける場合があります。
 - a. クライアントが古いサーバーで管理される場合、**[Acronis Cyber Files ファイルを別のアプリケーションで開く]** が無効に設定されるか、有効な許可リスト/ブロックリストがある限り、ドキュメントプロバイダ拡張機能は有効になります。
 - b. クライアントが新しいサーバー（バージョン 7.3.1 以降）で管理され、**[ドキュメントプロバイダの使用を許可]** が有効に設定されている場合、**[Acronis Cyber Files ファイルを別のアプリケーションで開く]** が無効に設定されるか、有効な許可リスト/ブロックリストがある場合でも、ユーザーは他のアプリとファイルを共有することができます。特別にブロックされたファイルも含む。

c. **[ドキュメントプロバイダの使用を許可]** が有効に設定されているものの、ファイルの作成が無効である場合には、ドキュメントプロバイダ拡張は機能しますが、ユーザーは他のアプリから Acronis Cyber Files データソースにファイルを保存することができません。

- **他のアプリケーションから Acronis Cyber Files にファイルを送信する:** このオプションを無効にすると、モバイルアプリケーションは、別のアプリケーションの **[他のアプリで開く]** 機能から送信されたファイルを受け入れなくなります。
- **カメラまたは写真ライブラリからファイルをインポートする:** 有効にすると、ユーザーは写真およびビデオをデバイスの写真ライブラリから Acronis Cyber Files に直接インポートできます。
- **Acronis Cyber Files からファイルを電子メールで送信する:** このオプションを無効にすると、モバイルアプリケーションに **[ファイルを電子メールで送信]** ボタンが表示されなくなります。したがって、Acronis Cyber Files からファイルを Eメールで送信することができなくなります。

注意

Android プラットフォームには、無効にできる組み込みの Eメールアプリや機能がありません。そのため、Eメールにファイルを移動できないようにするには、**[他のアプリケーションで Acronis Cyber Files ファイルを開く]** を無効にする必要があります。

- **Acronis Cyber Files からファイルを印刷する:** このオプションが無効である場合、モバイルアプリケーションには **[印刷]** ボタンは表示されず、Acronis Cyber Files のファイルを印刷することはできません。
- **開いているファイルからテキストをコピーする:** このオプションを無効にすると、ユーザーは、Access モバイル クライアントで開いている文書からテキストを選択してコピー/貼り付け操作を行うことができなくなります。これにより、別のアプリケーションへのデータのコピーを防ぐことができます。

警告

MobileIron ポリシー がアクティブな場合、その Allow Copy/Paste To 設定の方が、この設定よりも優先されます。

ファイルの編集

- **Office ファイルの編集と作成:** このオプションを無効にすると、統合されている Polaris エディタで文書を編集できなくなります。
 - **パスワードで保護されたファイルの編集:** このオプションを無効にすると、ユーザーはパスワードで保護されたファイルを編集できなくなります。
- **テキストファイルの編集と作成:** このオプションを無効にすると、ユーザーは組み込みのテキストエディタを使用して .txt ファイルを編集できなくなります。

PDF の編集と注釈

- **PDF の編集を許可:** この設定が有効な場合、ユーザーはページの新規作成、ファイルの複製、コピーと貼り付け、並べ替え、回転、削除、選択したページのサブセットからの新しいドキュメントの作成など、多くの PDF 編集機能を利用できるようになります。
- **PDF の注釈を使用できるようにする:** このオプションを無効にすると、モバイルアプリで PDF に注釈を付けることができなくなります。

- **空のPDFファイルの作成を許可する:** 有効にすると、注釈作成用の空のPDFファイルを作成できます。
- **PDFのカスタム表示設定を適用する:** このオプションを有効にすると、すべてのユーザーおよびすべてのPDFに、すべてのサブ設定が適用されます。
 - **ユーザーが設定を変更できるようにする:** 有効にすると、ユーザーは自分のPDF表示設定を変更できるようになります。
 - **[スクロール方向]:** ページの移動方法（縦にスクロールするか横にスクロールするか）を選択できます。
 - **[ページトランジション]:** トランジションの視覚効果を選択できます。**[スライド]:** 単にページが変更されます。**[スクロール]:** ページが1つに繋がっているかのようにスクロールされます。**[カール]:** ページが本のようにめくられます。
 - **[ページ表示]:** 表示モード（1ページずつ、または2ページずつ）を選択できます。
 - **サムネイル:** PDFページのサムネイルのサイズを設定します。**[小]、[大]、[なし]** から選択できます。
 - **[検索モード]:** 組み込みのPDFビューアによって提供される検索結果の表示形式を設定します。3種類の検索結果の表示形式があります。
 - **[シンプル]:** 結果がハイライト表示され、矢印アイコンを使ってスクロールできます。
 - **[詳細]:** すべての結果がドロップダウンリストに表示され、タップして参照できます。
 - **[ダイナミック]:** 検索結果表示形式をiPhoneでは**[シンプル]**に設定し、iPadでは**[詳細]**に設定します。
 - **[ハイパーリンクハイライト]:** ハイパーリンクをハイライト表示するための色を選択できます。**[無効]**を選択してハイライトを無効にすることもできます。
 - **[幅に合わせる]:** 有効にすると、デバイス画面の幅に合わせてページのサイズが変更されます。
 - **[ナイトモード]:** 有効にすると、薄暗い場所での表示が快適になるように、デバイスでナイトモードカラスキームが使用されます。

同期ポリシー

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

☒ Allow User to Create Sync Folders

The following features are not supported by older mobile client apps. Please see this knowledge base article for details on the mobile client apps that support these features.

☐ Only Allow 1-way Sync Folders to be Created ⓘ

Default Sync Folder Type

2-way ⓘ

Client is Prompted to Confirm before Synced Files are Downloaded:

Always

☒ Allow User to Change This Setting

☐ Only Allow File Syncing While Device Is on WiFi Networks

☒ Allow User to Change This Setting

Auto-Sync Interval:

On App Launch Only

☒ Allow User to Change This Setting

☐ Only Allow File Auto-Syncing While Device is on WiFi Networks

☐ Prevent device from sleeping during file sync ⓘ

☒ Allow User to Change This Setting

- **ユーザーに同期フォルダの作成を許可:** ユーザーが独自の同期フォルダを作成することを許可します。
 - **一方向同期フォルダのみ作成を許可する:** ユーザーは一方向同期フォルダのみ作成できます。
 - **デフォルトの同期フォルダタイプ:** デフォルトの同期フォルダタイプとして、一方向または双方向のいずれかを設定します。
- **同期ファイルがダウンロードされる前にクライアントに確認を求めるメッセージを表示:** 同期されたフォルダ内のファイルをダウンロードする前にユーザーが確認する必要がある状況の条件を選択します。オプションは、[常に]、[携帯ネットワーク使用時のみ]、[なし] です。[ユーザーが設定を変更できるようにする] が有効な場合、クライアントは確認オプションを変更できます。
- **デバイスが WiFi ネットワークに接続されている場合のみファイルの同期を許可する:** このオプションを有効にすると、Acronis Cyber Files では携帯接続を介したファイルの同期が許可されません。[ユーザーが設定を変更できるようにする] が有効な場合、クライアントは WiFi ネットワーク上にある間、自動ファイル同期を有効または無効にできます。
- **自動同期間隔:** このオプションが有効になっている場合、Acronis Cyber Files は自動同期を実行しないか、アプリ起動時のみに実行するか、いくつかの時間間隔で実行します。
 - **ユーザーが設定を変更できるようにする:** このオプションが有効になっている場合は、ユーザーは Acronis Cyber Files モバイルアプリから時間間隔を変更できます。

- **デバイスが WiFi ネットワークに接続されている場合のみファイルの自動同期を許可する:** このオプションが有効になっている場合、ユーザーが WiFi に接続していなければ自動同期は行われません。
- **ファイル同期中のデバイスのスリープを許可しない:** この設定を有効にした場合、ファイル同期の実行中にロックやスリープが起こりません。[ユーザーが設定を変更できるようにする] が有効な場合、クライアントは確認オプションを変更できます。

ホームフォルダ

- **ユーザーのホームフォルダを表示する:** このオプションを選択すると、ユーザーの個人用ホームディレクトリが Mobile アプリに表示されます。
- **クライアントに表示する表示名:** モバイルアプリでのホームフォルダ項目の表示名を設定します。パスの一部としてワイルドカード文字列 %USERNAME% を含めることが可能です。ワイルドカードは、ユーザーのメインの個人フォルダ名に置き換えられます。%USERNAME% は大文字で指定する必要があります。

注意

その他のデータソースタイプでは、%USERNAME% ワイルドカードを使用してユーザーのユーザー名を表示することはできません。Active Directoryで割り当てられたホームフォルダのみで使用できます。

- **Active Directory で割り当てられたホームフォルダ:** モバイルアプリで表示されるホーム フォルダから、AD アカウント プロファイルで定義されたサーバー/フォルダのパスにユーザーが接続されます。
ホーム フォルダには、選択したゲートウェイを介してアクセスすることができます。
- **カスタム ホーム ディレクトリのパス:** モバイルアプリで表示されるホームフォルダから、この設定で定義されたサーバーおよびパスにユーザーが接続されます。
パスの一部としてワイルドカード文字列 %USERNAME% を含めることが可能です。ワイルドカードは、ユーザーのメインの個人フォルダ名に置き換えられます。 %USERNAME% は大文字で指定する必要があります。
- **モバイルクライアントへの同期:** このオプションにより、ホームディレクトリの同期の種類が選択されます。

注意

このオプションは、ユーザーのホームフォルダとデスクトップクライアントとの同期機能には影響しません。

サーバー ポリシー

Security Policy	Application Policy	Sync Policy	Home Folders	Server Policy
Required Login Frequency for Resources Assigned by This Policy: ☒ Once Only, Then Save for Future Sessions ☐ Once per Session ☐ For Every Connection				
☐ Allow User to Add Individual Servers ☐ Allow Saved Passwords for User Configured Servers				
☒ Allow File Server, NAS and SharePoint Access From the Web Client ☒ Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client ☒ Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client				
☐ Allow User to Add Network Folders by UNC path or URL Gateway Server used for access to user-configured Network Folders: Local (192.168.2.129:3000) ▼ ☐ Block access to specific network paths Blocked Path List: ▼ Add/Edit lists Refresh lists				
☐ Only Allow This Mobile Client to Connect to Servers with Third-Party Signed SSL Certificates				
☒ Warn Client When Connecting to Servers with Untrusted SSL Certificates				

- **このポリシーによって割り当てられるリソースの必要なログイン頻度:** このポリシーによって割り当てられたサーバーにユーザーがログインする必要がある頻度を設定します。
 - **1 回のみ、将来のセッション用に保存する:** ユーザーは管理サーバーに最初に登録するときにパスワードを入力します。このパスワードは保存され、その後に開始するすべてのファイルサーバーへの接続で使用されます。
 - **セッションごと:** Acronis Cyber Files モバイルの起動後、ユーザーは、最初のサーバーに接続するときにパスワードの入力が求められます。ユーザーは、Acronis Cyber Files モバイルアプリケーションから移動するまで、パスワードを再入力せずに追加のサーバーに接続することができま

す。。Acronis Cyber Files モバイルを終了してから再び起動した場合は、時間の長さにかかわらずパスワードをもう一度入力して最初のサーバーに接続する必要があります。

- **接続するたび**: ユーザーは、サーバーに接続するたびにパスワードを入力する必要があります。
- **ユーザーによる個別のサーバーの追加を許可**: このオプションを有効にすると、ユーザーは、Acronis Cyber Files モバイル アプリケーション内から、サーバーの DNS 名または IP アドレスを持っていれば、手動でサーバーを追加できます。ユーザーに、ポリシーの**割り当てられたサーバー**のみを利用できるようにする場合は、このオプションを無効のままにします。
 - **ユーザーが設定したサーバーに接続するためのパスワードを保存できるようにする**: ユーザーが個別のサーバーの追加を許可されている場合、このサブオプションでそれらのサーバーに対するパスワードを保存できるようにするかどうかを決定します。
- **ウェブ クライアントからファイル サーバー、NAS、および SharePoint へのアクセスを許可する**: 有効にした場合、ウェブ クライアントは、モバイル データ ソースの表示とアクセスも実行できるようになります。
 - **ファイル サーバー、NAS および SharePoint のフォルダからデスクトップ クライアントへの同期を許可する**: このオプションが有効な場合、デスクトップ クライアントでは **[ネットワーク]** のコンテンツへの一方向同期が可能になります。
 - **ファイル サーバー、NAS および SharePoint のフォルダとデスクトップ クライアントの双方向同期を許可する**: このオプションが有効な場合、デスクトップ クライアントでは **[ネットワーク]** のコンテンツとの双方向同期が可能になります。

注意

デスクトップクライアントで **[ネットワーク]** のコンテンツとの双方向同期を有効にするには、**[アプリケーション ポリシー]** タブでファイルとフォルダの操作の**作成**（フォルダの**追加**）、**コピー**、**削除**、**移動**、および**名前の変更**を事前に許可しておく必要があります。

- **ユーザーが UNC パスまたは URL を指定してネットワーク フォルダを追加できるようにする**: このオプションが有効な場合、モバイルクライアント ユーザーは、ネットワーク フォルダおよび SharePoint サイトのうち、自分に割り当てられているのではないもの、または既存のデータソースではアクセスできないものを追加してアクセスすることが可能になります。選択するゲートウェイサーバーには、それらの SMB 共有または SharePoint サイトへのアクセス権が付与されていなければなりません。
 - **特定のネットワーク パスへのアクセスをブロックする**: 有効にすると、ユーザーによる自己プロビジョニングが許可されていないネットワーク パスのブロックリストを管理者が作成して使用できるようになります。
- **このモバイルクライアントのみがサードパーティ署名済み SSL 証明書を使用してサーバーに接続できるようにする**: このオプションが有効な場合、Access Mobile Client Acronis Cyber Files モバイルのみが、サードパーティの署名済み SSL 証明書を使用したサーバーへの接続を許可されます。

注意

管理サーバーにサードパーティの証明書がない場合、クライアントは初期設定の後に管理サーバーに接続できません。このオプションを有効にする場合は、すべてのゲートウェイサーバーにサードパーティの証明書があることを確認してください。

- **信頼されていない SSL 証明書を使用してサーバーに接続するときにクライアントに警告する:** ユーザーが自己署名証明書を使用するサーバーに頻繁に接続する場合は、これらのサーバーに接続するときに表示されるクライアント側の警告ダイアログ メッセージを無効にすることができます。
- **サーバーからの応答がない場合のクライアント タイムアウト:** このオプションは、サーバーが応答しない場合のクライアント ログイン接続のタイムアウトを設定します。クライアントのデータ接続速度が特に遅い場合、またはゲートウェイ サーバーに接続する前に VPN オンデマンド ソリューションを利用して接続を確立している場合、このタイムアウトをデフォルトの 30 秒より長い値に設定することができます。クライアントが Acronis Cyber Files モバイルアプリを使用してこの値を変更できるようにするには、**[ユーザーが設定を変更できるようにする]** をオンにします。

ポリシー設定の例外

Acronis Cyber Files mobile for Android アプリと **Acronis Cyber Files mobile with Mobile Iron AppConnect** アプリを実行している場合は、モバイルアプリへの Acronis Cyber Files 管理ポリシーの適用方法にいくつかの例外があります。Android の場合、いくつかの機能がまだサポートされていないため、関連するポリシーは適用されません。MobileIron の場合、いくつかの標準的な Acronis Cyber Files ポリシー機能が MobileIron AppConnect プラットフォームによって異なります。これらの例外については、Acronis Cyber Files ポリシー設定のページを参照してください。Android ロゴと MobileIron ロゴの上にマウスのポインタを移動すると、個別のポリシーの例外に関する詳細が表示されます。

ブロック対象のパスのリストの作成

ブロックリストを作成して、ユーザーによるモバイル デバイスからの自己プロビジョニングを不可にするパスを指定できます。これらのリストはユーザー ポリシーまたはグループ ポリシーに割り当てる必要があります。自己プロビジョニングのパスに対してのみ有効です。リストを作成して適切なユーザー、グループ、またはその両方に割り当てたら、適用するユーザー ポリシーまたはグループ ポリシーの **[特定のネットワーク パスへのアクセスをブロックする]** をそれぞれ有効にする必要があります。

リストを作成するには、次の操作を実行します。

1. 管理者としてウェブ インターフェイスを開きます。
2. **ポリシー** ページを開きます。
3. 目的のユーザー ポリシーまたはグループ ポリシーをクリックします。
4. **[サーバー ポリシー]** タブを開きます。
5. **[特定のネットワーク パスへのアクセスをブロックする]** チェックボックスをオンにします。

注意

ブロックリストをユーザーポリシーまたはグループポリシーに割り当てるたびに、この手順を実行する必要があります。

6. **[リストの追加/編集]** を押します。
7. **[ブロック対象のパスのリスト]** ページで **[リストの追加]** を押します。
8. このリストの名前を入力します。

9. ブロックリストに含めるパスまたはパスのリストを入力します。各エントリは、新しい行に入力する必要があります。
10. [ユーザーまたはグループに適用する] タブを開きます。
11. 目的のユーザーまたはグループにリストを割り当てます。
12. [保存] を押します。

ユーザー ポリシーまたはグループ ポリシーのブロックリストを有効にするには、次の操作を実行します。

1. 管理者としてウェブ インターフェイスを開きます。
2. [ポリシー](#) ページを開きます。
3. 目的のユーザー ポリシーまたはグループ ポリシーをクリックします。
4. [サーバー ポリシー] タブを開きます。
5. [特定のネットワーク パスへのアクセスをブロックする] チェックボックスをオンにします。

注意

ブロックリストをユーザーポリシーまたはグループポリシーに割り当てるたびに、この手順を実行する必要があります。

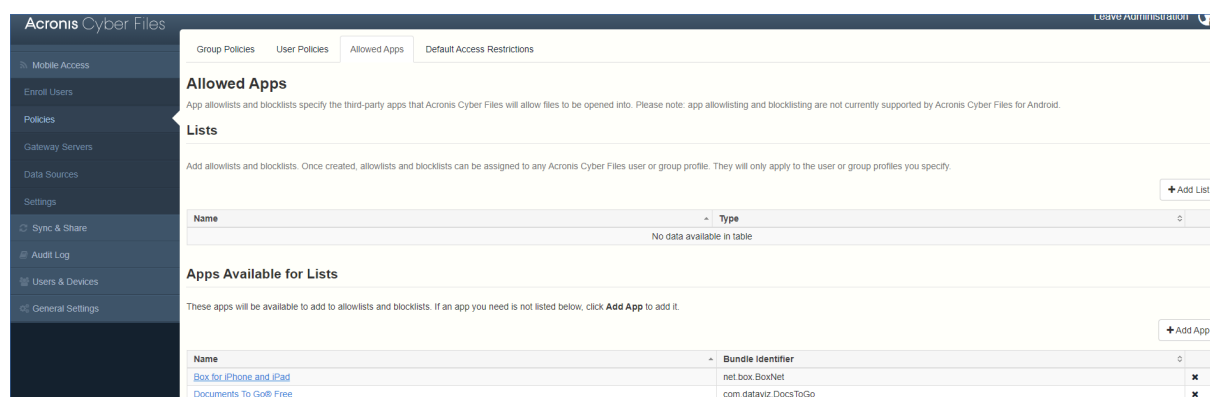
6. ドロップダウン メニューから目的のリストを選択します。

注意

[リストの更新] を押すと、ドロップダウンメニュー内のオプションが更新されます。

7. [保存] を押すと、ポリシーを保存して終了します。

許可されたアプリ



Allowed Apps

App allowlists and blocklists specify the third-party apps that Acronis Cyber Files will allow files to be opened into. Please note: app allowlisting and blocklisting are not currently supported by Acronis Cyber Files for Android.

Lists

Add allowlists and blocklists. Once created, allowlists and blocklists can be assigned to any Acronis Cyber Files user or group profile. They will only apply to the user or group profiles you specify.

Name	Type
No data available in table	

Apps Available for Lists

These apps will be available to add to allowlists and blocklists. If an app you need is not listed below, click **Add App** to add it.

Name	Bundle Identifier
Box for iPhone and iPad	net.box.BoxNet
Documents To Go® Free	com.dataviz.DocsToGo

Acronis Cyber Files Client Management を使用すると、モバイルデバイス上の他のアプリでファイルを開く Acronis Cyber Files モバイルの機能を制限する許可リストまたはブロックリストを作成することができます。これらを使用して、Acronis Cyber Files モバイルを介してアクセスできるファイルが、セキュリティで保護された信頼済みアプリでのみ開かれるようにすることができます。

許可リスト – Acronis Cyber Files ファイルを開くことを許可されるアプリケーションのリストを指定できます。他のすべてのアプリケーションはアクセスを拒否されます。

ブロックリスト: Acronis Cyber Files ファイルを開くことを許可されないアプリケーションのリストを指定できます。他のすべてのアプリケーションはアクセスを許可されます。

Acronis Cyber Files が特定のアプリを識別するには、そのアプリの**バンドル ID** を認識している必要があります。一般的なアプリとそれらのバンドル ID のリストは、デフォルトで Acronis Cyber Files Web インターフェースに含まれています。許可リストまたはブロックリストに必要なアプリケーションが含まれていない場合、リストに追加する必要があります。

注意

アプリの許可リストとブロックリストは、Acronis Cyber Files mobile for Android では現在サポートされていません。

リスト

許可リストとブロックリストを追加します。作成した許可リストおよびブロックリストは、任意の Acronis Cyber Files ユーザー ポリシーまたはグループ ポリシーに割り当てることができます。リストは、指定したユーザー ポリシーまたはグループ ポリシーにのみ適用されます。

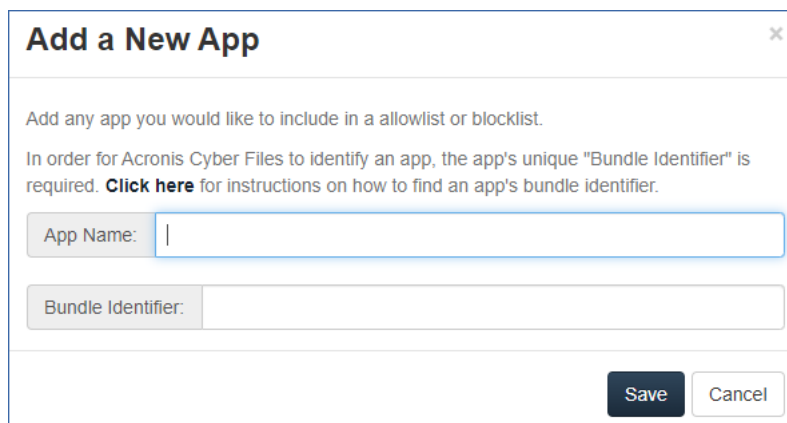
- **名前**: 管理者が設定したリストの名前を表示します。
- **タイプ**: リストのタイプを表示します（許可リスト/ブロックリスト）
- **リストの追加**: [新しい許可リストまたはブロックリストの追加] メニューを開きます。

リストで使用できるアプリの追加

許可リストまたはブロックリストに含めるアプリケーションを追加するには、次の操作を実行します。

1. トップメニューバーの **[許可されたアプリ]** をクリックします。
2. **[リストで使用できるアプリ]** セクションで **[アプリの追加]** をクリックします。
3. **アプリケーション名**を入力します。これには、App Store に表示されるアプリケーションの名前または選択した代替の名前を入力できます。
4. アプリケーションの**バンドル ID**を入力します。これは、目的のアプリケーション バンドル ID と正確に一致している必要があります。一致していないと許可リストまたはブロックリストに追加されません。
5. **[保存]** をクリックします。

バンドル ID は、デバイスでファイルを参照して確認できます。また、iTunes ライブラリで表示することもできます。



アプリケーションのバンドル ID の確認

デバイス上のファイルを参照することによるアプリケーションのバンドル ID の確認

デバイスのストレージの内容を閲覧できるソフトウェアを使用すると、デバイス上のアプリを特定し、その**バンドルID**を確認できます。このために使用できるアプリのひとつに [iExplorer](#) があります。

1. USB でデバイスをコンピュータに接続し、iExplorer または同様のユーティリティを起動します。
2. デバイスの Apps フォルダを開き、必要なアプリケーションを見つけます。
3. アプリケーションのフォルダを開き、**iTunesMetadata.plist** ファイルを見つけます。
4. この PLIST ファイルをテキスト エディタで開きます。
5. リスト内で **softwareVersionBundleId** キーを見つけます。
6. その下にある**文字列**値が、Acronis Cyber Files で入力する必要があるアプリケーションのバンドル ID の値です。通常、これらの値は「**com.companyname.appname**」という形式になっています。

iTunes ライブラリでアプリのバンドル ID を検索するには

デバイスと iTunes が同期されており、目的のアプリがデバイス上にあるか、または iTunes からダウンロードされたものである場合、そのアプリはコンピュータのハードドライブに配置されます。**バンドル ID**を見つけるには、まずハードドライブでこのアプリを探し、アプリの中を確認します。

1. iTunes ライブラリに移動し、**Mobile Applications** フォルダを開きます。
2. Mac では、通常、ホーム ディレクトリの ~/Music/iTunes/Mobile Applications/ にあります。
3. Windows 7 PC では、通常、C:\Users\username\My Music\iTunes\Mobile Applications/ にあります。
4. デバイスにアプリをインストールしたばかりの場合は、iTunes の同期を実行してから、次の手順に進んでください。
5. **Mobile Applications** フォルダで必要なアプリを見つけます。
6. このファイルを複製し、拡張子を .ZIP に変更します。
7. 新しく作成されたこの ZIP ファイルを解凍すると、アプリケーション名の付いたフォルダが作成されます。
8. このフォルダの中には、**iTunesMetadata.plist** という名前のファイルがあります。

9. この PLIST ファイルをテキスト エディタで開きます。
10. リスト内で **softwareVersionBundled** キーを見つけます。
11. その下にある**文字列**値が、Acronis Cyber Files で入力する必要があるアプリケーションのバンドル ID の値です。通常、これらの値は「**com.companyname.appname**」という形式になっています。

デフォルトのアクセス制限

このセクションでは、管理サーバーと接続されるクライアントに制限を設定することができます。このような制限は、ゲートウェイ サーバーに対するデフォルトの制限にもなります。

注意

ゲートウェイサーバーに対するカスタムアクセス制限の設定の詳細については、「ゲートウェイサーバーの管理」セクションの「[ゲートウェイサーバーの編集](#)」の記事を参照してください。

The screenshot displays the 'Default Access Restrictions' configuration interface. At the top, there are tabs for 'Group Policies', 'User Policies', 'Allowed Apps', and 'Default Access Restrictions'. Below the tabs, a header reads 'Default Access Restrictions'. A descriptive text block states: 'Configure the client enrollment status, client app types, and authentication methods that can be used to connect to any Gateway Servers configured to use these default settings, and to connect to this Acronis Cyber Files server.'

The configuration options are as follows:

- ☐ Require that client is enrolled with an Acronis Cyber Files server
- ☒ Allow Client Certificate Authentication
- ☒ Allow Username/Password Authentication
- ☒ Allow Smart Card Authentication
- ☒ Allow Acronis Cyber Files **Android** clients to access this server
 - ☒ Allow standard **Android** client
 - ☒ Allow **BlackBerry Dynamics** managed **Android** client
 - ☒ Allow **AppConnect** managed **Android** client
- ☒ Allow Acronis Cyber Files **iOS** clients to access this server
 - ☒ Allow standard **iOS** client
 - ☒ Allow '**iOS Managed App**' **iOS** client
 - ☒ Allow **BlackBerry Dynamics** managed **iOS** client
 - ☒ Allow **Intune** managed **iOS** client
 - ☒ Allow **AppConnect** managed **iOS** client
- ☒ Allow Acronis Cyber Files **Windows Mobile** clients to access this server
 - ☒ Allow **Windows Phone** client
 - ☒ Allow **Windows Tablet / Desktop** client

クライアントの登録状態、クライアントアプリのタイプ、および認証方法を構成します。認証方法は、この Acronis Cyber Files サーバーと、デフォルトのアクセス制限を使うように構成された任意のゲートウェイサーバーの接続に使うことができます。

- **クライアントに Acronis Cyber Files サーバーへの登録を要求:** このオプションをオンにすると、このサーバーに接続しているすべての Acronis Cyber Files モバイルクライアントは、[対象の Acronis Cyber Files サーバー] の下に一覧表示される Acronis Cyber Files サーバーによって管理される必要があります。このオプションによって、サーバーにアクセスするすべてのクライアントに、必要な設定とセキュリティオプションが反映されます。入力するサーバー名は、モバイルアプリで設定した管理サーバー名と同じである必要があります。名前の一部を使用して、たとえばドメイン内の複数のクライアント管理サーバーを許可することもできます。名前の一部を使用する場合、ワイルドカードを使用する必要はありません。

- **クライアント証明書認証を許可:** このオプションをオフにすると、証明書を使った接続ができなくなり、クライアントのユーザー名とパスワード、またはスマートカードを使って接続できるようになります。
- **ユーザー名/パスワード認証を許可:** このオプションをオフにすると、ユーザー名とパスワードを使った接続ができなくなり、クライアントの証明書、またはスマートカードを使って接続できるようになります。
- **スマートカード認証を許可:** このオプションをオフにすると、スマートカードを使った接続ができなくなり、クライアントのユーザー名とパスワード、または証明書を使って接続できるようになります。
- **Acronis Cyber Files Android クライアントにこのサーバーへのアクセスを許可:** このオプションをオフにすると、Android デバイスから Acronis Cyber Files サーバーへの接続ができなくなり、管理にアクセスすることもできません。このオプションをオンにすると、以下のオプションでクライアントの接続条件を細かく設定することができます。
 - **標準 Android クライアントを許可:** このオプションをオンにすると、標準の Android Acronis Cyber Files クライアントアプリを実行しているユーザーにこの Acronis Cyber Files サーバーへの接続を許可します。Android ユーザーにこの Acronis Cyber Files サーバーへのアクセスを許可しない場合、この設定をオフにします。
 - **AppConnect が管理する Android クライアントを許可:** このオプションをオンにすると、Acronis Cyber Files クライアントを MobileIron に登録された Android ユーザーに、この Acronis Cyber Files サーバーへのアクセスを許可します。MobileIron に登録された Android ユーザーにこの Acronis Cyber Files サーバーへのアクセスを許可しない場合、この設定をオフにします。
- **Acronis Cyber Files iOS クライアントにこのサーバーへのアクセスを許可:** このオプションをオフにすると、iOS デバイスから Acronis Cyber Files サーバーへの接続ができなくなり、管理にアクセスすることもできません。このオプションをオンにすると、以下のオプションでクライアントの接続条件を細かく設定することができます。
 - **標準 iOS クライアントを許可:** このオプションをオンにすると、標準の iOS Acronis Cyber Files モバイルアプリを実行しているユーザーにこの Acronis Cyber Files サーバーへの接続を許可します。iOS ユーザーにこの Acronis Cyber Files サーバーへのアクセスを許可しない場合、この設定をオフにします。
 - **「iOS 管理対象アプリ」iOS クライアントを許可:** このオプションをオンにすると、Acronis Cyber Files 管理対象 iOS アプリを実行しているユーザーに、この Acronis Cyber Files サーバーへの接続を許可します。この状態にするには、クライアントがパラメータを 1 つ以上含む [管理対象アプリ](#) [セッションの設定](#)を受け取る必要があります。管理対象 iOS ユーザーにこの Acronis Cyber Files サーバーへのアクセスを許可しない場合、この設定をオフにします。
 - **Intune が管理する iOS クライアントを許可:** このオプションをオンにすると、iOS の Acronis Cyber Files モバイルクライアントである Intune が管理するクライアントを使用しているユーザーに、この Acronis Cyber Files サーバーへの接続を許可します。Intune が管理するユーザーにこの Acronis Cyber Files サーバーへのアクセスを許可しない場合は、この設定をオフにします。
 - **AppConnect が管理する iOS クライアントを許可:** このオプションをオンにすると、Acronis Cyber Files モバイルクライアントを MobileIron に登録した iOS ユーザーが、この Acronis Cyber Files サーバーにアクセスすることを許可します。MobileIron に登録された iOS ユーザーにこの Acronis Cyber Files サーバーへのアクセスを許可しない場合、この設定をオフにします。

モバイル デバイスの登録

Acronis Cyber Files モバイルアプリの使用開始にあたり、ユーザーは iTunes または Google Play のうち該当する App Store からアプリをインストールする必要があります。会社がクライアント管理を使用している場合、ユーザーも Acronis Cyber Files サーバーでデバイスに Acronis Cyber Files モバイルアプリを登録する必要があります。登録を行うと、モバイルクライアントの構成、セキュリティ設定、および機能が、Acronis Cyber Files のユーザーポリシーまたはグループポリシーによって制御されるようになります。

次のようなモバイルアプリケーションの設定と機能が管理ポリシーによって制御されます。

- Acronis Cyber Files アプリケーション ロック パスワードを必須にする
- アプリのパスワードの複雑性に関する要件
- Acronis Cyber Files アプリを管理から除外する機能
- Acronis Cyber Files アプリからのファイルの電子メール送信および印刷を許可する
- ファイルをデバイスに保存することを許可する
- Acronis Cyber Files アプリのデバイス上のファイルを iTunes バックアップに含めることを許可する
- 他のアプリケーションから Acronis Cyber Files へのファイルの送信を許可する
- 他のアプリケーションで Acronis Cyber Files ファイルを開くことを許可する
- Acronis Cyber Files ファイルを開くことができる他のアプリケーションを制限する
- PDF 注釈を許可する
- ファイルやフォルダの作成、名前の変更、および削除を許可する
- ファイルの移動を許可する
- 削除するときの確認を必須にする
- サーバー、フォルダ、ホームディレクトリを割り当てて Acronis Cyber Files アプリに自動的に表示されるようにする
- 割り当てられたフォルダを設定してサーバーとの一方向または双方向同期を実行できるようにする

サーバー側の管理登録処理

Acronis Cyber Files

Mobile Access

Enroll Users

Policies

Gateway Servers

Data Sources

Settings

Sync & Share

Audit Log

Enrollment Settings

Mobile Client Enrollment Address: myserver.mycompany.com

☐ Allow mobile clients restored to new devices to auto-enroll without PIN

☒ Use user principal name (UPN) for authentication to Gateway Servers ⓘ

Device Enrollment Requires:

☒ A PIN number + Active Directory username and password

☐ Active Directory username and password only

Save

1. Acronis Cyber Files Web インターフェースを開きます。
2. 管理者としてログインします。
3. **[モバイル アクセス]** タブを選択します。
4. **[設定]** タブを開きます。
5. デバイス登録要件を選択します

登録設定

モバイルクライアントを新しいデバイスに復元した場合でも、PIN コードなしで自動登録されるようにする: この設定を有効にすると、以前のバージョンの Acronis Cyber Files モバイルによって管理されていたユーザーが PIN コードを使用せずに新しいサーバーに登録できるようになります。

ユーザー プリンシパル名 (UPN) を使用したゲートウェイ サーバーの認証: この設定を有効にすると、ユーザーは UPN (例: user@company.com) を使用してゲートウェイ サーバーに対する認証を行います。無効にした場合は、ユーザーはドメイン名とユーザー名の組み合わせ (例: domain/user) を使用して認証を行います。

デバイス登録モード

Acronis Cyber Files には、2 つのデバイス登録モードオプションがあります。このモードは、すべてのクライアント登録で使用されます。要件に適したオプションを選択する必要があります。

- **PIN コード + Active Directory のユーザー名とパスワード:** ユーザーは、自分の Acronis Cyber Files アプリをアクティブ化して Acronis Cyber Files サーバーにアクセスするために、有効期限が設定されたワンタイム PIN コードと有効な Active Directory ユーザー名およびパスワードの入力が求められます。このオプションを使用する場合、ユーザーは、IT 管理者によって発行された PIN コードを受け取った後に 1 台のデバイスのみ登録することができます。このオプションは、2 つの要素によるデ

バイス登録でセキュリティを強化する必要がある場合に推奨されます。

- **Active Directory のユーザー名とパスワードのみ:** ユーザーは Active Directory のユーザー名とパスワードのみを使用して Acronis Cyber Files アプリをアクティブ化することができます。このオプションを使用すると、ユーザーが今後いつでも 1 台以上のデバイスを登録することができます。ユーザーには、Acronis Cyber Files サーバーの名前、または Acronis Cyber Files サーバーをポイントする URL のみを提供する必要があります。この情報は、Web サイトに掲示したり電子メールで送信したりできるので、多数のユーザーへの Acronis Cyber Files のロールアウトを簡素化することができます。このオプションは、2 つの要素による登録が不要な環境および学生用の導入など多くのユーザーがいつでも Acronis Cyber Files にアクセスする必要がある環境に推奨されます。

ユーザーへの登録招待

ユーザーは通常、Acronis Cyber Files Administrator から送信される電子メールによって、Acronis Cyber Files サーバーでの登録に招待されます。ユーザーが必要とする場合は、設定可能な日数だけ有効なワンタイム PIN コードをこの電子メールに含めます。この PIN コードを使用して、1 つのデバイスでのみ Mobile アプリに登録することができます。ユーザーが複数のデバイスを持っている場合は、アクセスが必要なデバイスごとに招待メールを受け取る必要があります。この電子メールには、Mobile アプリを初めてインストールする必要がある場合のために、App Store 内の Mobile アプリへのリンクが含まれています。さらに、2 つ目のリンクが含まれており、デバイスでこのリンクをタップすると Acronis Cyber Files モバイルが開き、Acronis Cyber Files サーバーの名前、固有の登録 PIN コード、およびユーザーのユーザー名を使用して、クライアントの登録が自動的に完了します。このリンクを使用すると、ユーザーがアカウントのパスワードを入力するだけでクライアントの登録が完了します。

- 登録招待メールが生成されると、招待されるユーザーが **[登録招待メール]** ページに表示されます。自動電子メール以外の方法で伝える必要がある場合のために、各ユーザーの PIN コードが一覧表示されます。
- ユーザーがワンタイム PIN コードを使用して Acronis Cyber Files モバイルに正常に登録すると、そのユーザーはこのリストに表示されなくなります。
- ユーザーの招待 PIN コードを無効にするには、**[削除]** をクリックしてリストから削除します。

Enrollment Invitations

Send Enrollment Invitation Export

Send an enrollment invitation to invite mobilEcho clients to enroll with this Acronis Access server. This invitation will include their unique, required PIN number, instructions, and a shortcut to begin the enrollment process. If you choose to give your users their PIN number by other means, they can also initiate the enrollment process from the mobilEcho client Settings menu or by opening this URL while on their device: [mobilEcho://https://myaccessserver/enroll](https://myaccessserver/enroll)

Filter by Username Filter Reset

Username	Display Name	Email Address	Distinguished Name	Expires	PIN	
hristo	Hristo Ilchev	hristo@gliilabs.com	CN=GLI,CN=Users,DC=gliilabs,DC=com	2013-10-24 06:28:09	VKJ3X9ZJ	✕

PINコードが不要な場合の基本的なURL登録リンクの使用

クライアントの登録に PIN コードを必要としないようにサーバーが設定されている場合、モバイル デバイスでタップしたときに登録処理を自動的に開始する標準の URL をユーザーに提供することができます。

管理サーバーの登録URLを判別するには、[モバイルアクセス] タブを開き、[ユーザーの登録] タブを開きます。URL はこのページに表示されます。

注意

2 つのモードの詳細については、「[設定](#)」セクションを参照してください。

Acronis Cyber Files の登録招待メールを生成するには:

1. [モバイルアクセス] タブを開き、[ユーザーの登録] タブを開きます。
2. [登録招待メールを送信する] ボタンをクリックします。
3. Active Directory のユーザー名もしくはグループ名を入力し、[検索] をクリックします。グループを選択した場合に [追加] を押すと、[招待するユーザー] リストのグループに各電子メール アドレスが表示されます。これにより、グループ内のすべてのメンバを一括招待することができます。オプションで、招待を送信する前に 1 人または複数のグループ メンバを削除することができます。[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. 最初のユーザーまたはグループを追加したら、新しい検索を実行し、さらにユーザーまたはグループをリストに追加することができます。
5. 招待するユーザーのリストを確認します。リストから任意のユーザーを削除することができます。
6. ユーザーのアカウントに E メールアドレスが関連付けられていない場合は、[電子メールアドレス] 列に **[電子メールアドレスが割り当てられていません。ここをクリックして編集してください]** と表示されます。これらのエントリのいずれかをクリックして、そのユーザーの代わりの E メールアドレスを手動で入力することができます。**[電子メールアドレスが割り当てられていません]** と表示されても、それらのユーザーの PIN コードが生成され、[ユーザーの登録] ページに表示されます。それらのユーザーが Acronis Cyber Files モバイルに登録するには、その前にこの PIN コードを別の方法でユーザーに伝える必要があります。

注意

登録 PIN コードを手動でユーザーに伝える場合は、**[指定したアドレスを使用して登録招待メールを各ユーザーに送信する]** チェックボックスをオフにします。各 PIN コードは、**[登録招待メール]** ページに表示されます。

7. [招待の期限が切れるまでの日数] フィールドで、招待の有効期間の日数を選択します。
8. 招待リストで各ユーザーに送信する PIN コードの数を選択します。これは、ユーザーが 2、3 台のデバイスを持っている場合に使用できます。ユーザーは、固有のワンタイム PIN コードが含まれる個別の電子メールを受信します。

注意

Acronis Cyber Files ライセンスを使用すると、ライセンスを付与される各ユーザーが最大 3 台のデバイスをアクティブ化することができます。3 台を超える各デバイスについては、ライセンス上の新規ユーザーとして追加できます。

9. ユーザーがダウンロードしてデバイスにインストールできるようにする Acronis Cyber Files モバイルのバージョンを選択します。iOS、Android、または両方を選択できます。

10. **[送信]** をクリックします。

注意

送信時にエラーメッセージが表示された場合は、[全般設定]にある[SMTP]タブのSMTP設定が適切であることを確認してください。また、**セキュリティで保護された接続**を使っている場合、自分が使用している証明書が、SMTPサーバーのホスト名と一致していることを確認します。

ユーザー側の管理登録処理

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 Acronis Cyber Files モバイルをインストールするためのリンク。
- Mobile アプリを起動し、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、Acronis Cyber Files モバイルをインストールし、登録情報を入力します。

モバイルアプリ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 Cyber Files 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。これらの資格情報は、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 Cyber Files 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. をまだインストールしていない場合は、IT 管理者から送信された電子メールを開き、「**Acronis Cyber Files 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 Cyber Files 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。

注意

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。

注意

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. Acronis Cyber Files モバイルアプリ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 Cyber Files でのファイルの保存が制限されているか Acronis Cyber Files モバイルアプリ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。Acronis Cyber Files モバイルアプリ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 Cyber Files アプリを開きます。
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. Acronis Cyber Files モバイルアプリ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 Cyber Files でのファイルの保存が制限されているか Acronis Cyber Files モバイルアプリ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。Acronis Cyber Files モバイルアプリ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、Acronis Cyber Files モバイルは、アプリ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。

注意

接続要件

Acronis Cyber Files クライアントが、プロファイルの更新、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 Cyber Files 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 Cyber Files 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 に接続する必要もあります。

管理の削除

Acronis Cyber Files モバイル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）
- Mobile アプリケーションを削除する

Acronis Cyber Files の管理ポリシーの設定によっては、Acronis Cyber Files モバイル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 Acronis Cyber Files モバイル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。ファイルを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]** をタップすることによって Acronis Cyber Files を管理から削除することを確認します。

注意

Acronis Cyber Files ポリシー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、Mobile 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、Acronis Cyber Files モバイルの既存のデータと設定がすべて消去されます。アプリケーションを再インストールすると、設定がデフォルトに戻ります。

Acronis Cyber Files モバイルアプリをアンインストールするには、次の操作を行います。

iOSの場合:

1. Mobile アプリ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. Mobile 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。

Androidの場合:

注意

Android デバイスのソフトウェアにはさまざまな種類があるため、設定は若干異なる場合があります。

1. **[アプリ]** メニューを開き、**[編集/削除]** を選択します。
2. Acronis Cyber Files アプリを探し、選択します。
3. **[削除]** を押します。

ゲートウェイ サーバーの管理

Acronis Cyber Files ゲートウェイサーバーは、ファイルサーバー、SharePoint リポジトリ、および Sync & Share ボリュームにあるファイルとフォルダについて、それらへのアクセスと操作を処理する Acronis Cyber Files モバイルアプリから参照されるサーバーです。ゲートウェイ サーバーは、モバイルクライアントにとって、ファイルへの「ゲートウェイ」となります。

Acronis Cyber Files サーバーは、1 つ以上のゲートウェイサーバーの管理と構成を、同じ管理コンソールから実行することができます。管理下に置かれているゲートウェイ サーバーは、**[モバイル アクセス]** メニューの **[ゲートウェイ サーバー]** セクションに表示されます。

- **タイプ:** ゲートウェイのタイプを表示します。現在、**[サーバー]** タイプのみ選択できます。
- **名前:** ゲートウェイの作成時に与えられた表示名。
- **アドレス:** ゲートウェイの FQDN または IP アドレス。
- **バージョン:** Acronis Cyber Files ゲートウェイサーバーのバージョンを表示します。
- **ステータス:** サーバーがオンラインかオフラインかを表示します。
- **アクティブ セッション:** このゲートウェイ サーバーに対して現在アクティブなセッションの数。
- **使用ライセンス:** 使用済みのライセンスの数と、使用可能なライセンスの数。
- **ライセンス:** ゲートウェイ サーバーに使われているライセンスの現在のタイプを表示します。

[新しいゲートウェイサーバーの追加] ボタンを使用して、[新しいゲートウェイサーバーを登録](#)することができます。

各ゲートウェイサーバーの **[操作]** メニューから、管理者は次のことを行えます。

- サーバーとそのパフォーマンスの詳細を取得する。
- その構成を編集する。
- サーバーのアクセス制限を変更する。
- サーバーのライセンスを変更する。
- サーバーを削除する。

警告

データソースのブックマークは、それが存在するゲートウェイサーバーを削除すると、不可逆的に失われます。サーバーに関連するデータソースを Cyber Files Server 管理コンソールに追加しなおしても、この操作を元に戻すことはできません。

注意

ゲートウェイサーバーは、Windows の HTTP.sys サービスを使用して、マシン上の関係する Windows 設定を適用します。これには、TLS 暗号化セキュリティを管理する Microsoft Secure Channel (schannel) の設定が含まれます。

ゲートウェイサーバー サービス セキュリティを変更したいお客様は、IIS Crypto などの Acronis 以外のツールを使用して、これらの Windows 設定を管理する必要があります。

ゲートウェイサーバーの検索オプション

要件

Acronis Cyber Files は、**Windows Search** を使用して、ネットワークデータソース内の検索を可能にしています。**Windows Search** は、Windows Server に組み込まれた機能ですが、デフォルトでは有効になっていません。

オンにするには、次の操作を実行します。

- サーバーマネージャで **ファイルサービス** 役割を追加/インストールします。
- **Windows Search サービス** が稼働していることを確認してください。

注意

上記要件が満たされない場合は、ネットワークデータソースで検索を実行できません。

また、以下に対する検索もサポートされません。

- NAS ファイルサーバー、CMIS、および SharePoint のデータロケーション。ただし、SMB/CIFS ファイルサーバーに対するサポートはあります。
- ファイルサーバーのルート (//server)。動作するのは (//server/share) 内部の実際の共有だけです。
- ゲートウェイマシン上のサービスアカウントが、リモート共有をホストしているコンピューターへのアクセス権 (Windows のアクセス許可) を持っていない場合。これを確認するには、管理サービスアカウントを使ってゲートウェイサービスを実行してみてください。

以下の場合、**[検索]** フィールドが無効になります。

- 何らかの理由で検索できない
- インデックス付きのディレクトリが空である

ファイル名検索のローカル データ ソースのインデックスを作成

ネットワークデータソースでの検索は、Acronis Cyber Files ゲートウェイサーバーと Windows Search インデックスに依存しています。Windows Search インデックスが必要なボリュームに対して有効で、インデックス付けが終わっている場合は、ディープ検索とコンテンツ検索の両方をそこで実行できます。

デフォルトでは、インデックス検索がすべてのゲートウェイ サーバーで有効です。インデックス検索は、ゲートウェイの **[サーバーの編集]** ダイアログでゲートウェイサーバーごとに無効または有効にすることができます。

1. Acronis Cyber Files 管理コンソールを開きます。
2. **[モバイル アクセス]** > **[ゲートウェイ サーバー]** > **[編集]** > **[検索]** に移動します。
3. 以下をオンにします。
 - **[ファイル名検索のローカル データ ソースのインデックスを作成]** チェックボックス
 - オプションで、**[利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート]** チェックボックス

デフォルト パス

デフォルトで、スタンドアロンサーバーでは、Acronis Cyber Files が Acronis Cyber Files ゲートウェイサーバー アプリケーション フォルダ内の **[Search Indexes]** ディレクトリにインデックスファイルを保存します。別の場所にインデックス ファイルを保存する場合は、新しいフォルダのパスを入力します。

利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート

共有フォルダのコンテンツ検索のサポートはデフォルトで有効になっており、このオプションを使用してオン/オフを切り替えることができます。コンテンツ検索は、ゲートウェイサーバーごとに有効または無効にすることができます。

Windows Search で必要なデータソースをインデックス化するように設定するには、スタートバーの **[Windows Search]** アイコンを右クリックし、**[Windows Search のオプション]** を選択します。

Windows の Reshare で Windows のコンテンツ検索を実行できますが、リモート マシンはゲートウェイサーバーと同じドメインに参加している必要があります。

注意

Windows の Reshare でコンテンツ検索を使用する場合は、データソースのボリュームパスはホスト名か完全な修飾子名にする必要があります。IP アドレスは Windows Search ではサポートされていません。

その他の構成

コンテンツ検索インデックス化は、特定のファイルタイプのコンテンツのみをインデックス化するように設定できます。

1. ゲートウェイサーバーをホストしているサーバーで、[コントロール パネル] -> [インデックスのオプション] を開きます。
2. [詳細設定] を選択して、[ファイルの種類] タブを開きます。
3. コンテンツ検索を有効/無効にするファイルの種類 (doc や txt) を探します。
4. 必要なファイルの種類を選択して、[このファイルのインデックスの作成方法] で、このファイルの種類コンテンツ検索を有効にする場合は [プロパティとファイルのコンテンツのインデックスを作成する] を、無効にする場合は [プロパティのみインデックスを作成する] を選択します。必要なすべてのファイルの種類に対してこのステップを繰り返します。

SharePoint

これらの認証情報の入力是一般的な SharePoint のサポートでは任意ですが、サイト コレクションを列挙するには必須です。たとえば、<http://sharepoint.example.com> および <http://sharepoint.example.com/SeparateCollection> という 2 つのサイト コレクションがあるとします。資格情報を入力しないと、<http://sharepoint.example.com> をポイントするボリュームを作成する場合、ボリュームを列挙するときに SeparateCollection というフォルダが表示されません。アカウントには、ウェブ アプリケーションに対するすべて読み取りアクセスが必要です。

新しいゲートウェイ サーバーの登録

管理ウェブ アプリケーションと同じコンピュータで実行しているゲートウェイ サーバーの自動登録を例外として、ゲートウェイ サーバーの登録は、複数の手順からなる、手動プロセスです。

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. **設定ユーティリティ**の設定に基づいて:
 - a. [利用可能なすべてのアドレス] を選択した場合は、https://localhost:3000/gateway_admin を開きます。
 - b. 特定の IP アドレスを選択した場合は、https://<特定の IP アドレス>:3000/gateway_admin を開きます。

注意

デフォルトのポート番号は、3000 です。デフォルトのポートを変更した場合は、localhost または IP アドレスの後ろにポート番号を追加します。

3. [管理キー] を書き留めます。

Administration

In order to configure this Acronis Cyber Files Gateway Server, it needs to be registered with an Acronis Cyber Files Management Server. To do this, visit the Gateway Servers section on the Management Server to register a new Gateway Server using the following key:

FCHW-WX7R-ZHPR

4. Acronis Cyber Files Web インターフェースを開きます。
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]** ボタンをクリックします。

Add New Gateway Server

Display Name:

Address for administration: ⓘ

☐ Use alternate address for client connections ⓘ

Administration Key: ⓘ

☒ Allow connections from Acronis Access servers using self-signed certificates ⓘ

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 DNS 名または 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、**[クライアント接続用に別のアドレスを使用する]** 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 DNS 名または 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 Cyber Files 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]** ボタンをクリックします。

ゲートウェイ サーバーを登録した後、このゲートウェイ サーバーにカスタムのアクセス制限を設定できます。この点に関する詳細については、「**ゲートウェイ サーバーの編集**」セクションを参照してください。

サーバーの詳細

ゲートウェイ サーバーの [詳細] ページを開くと、特定のサーバーとそのユーザーに関する多くの有用な情報が得られます。

ステータス

Status	Logging	Active Users
Display Name	Local	
Address for administration	192.168.1.128:443	
Address for client connections	192.168.1.128:443	
Operating System	Microsoft Windows Server 2008 R2 Enterprise Edition (build 7600), 64-bit	
Gateway Server version	5.0.0x365	
Status	Online	
Last Contact	2013-10-15 03:29:21	
Active Sessions	2	
Licenses Used	2 of Unlimited	
License type	activEcho + mobilEcho Trial	
Expiration Date	2013-11-04, 20 days remaining	

[ステータス] セクションでは、ゲートウェイ サーバー自体に関する情報が得られます。オペレーティング システム、ライセンスの種類、使用されているライセンスの数、ゲートウェイ サーバーのバージョンなどの情報です。

アクティブ ユーザー

Status

Logging

Active Users



User	Location	Device	Model	OS	mobilEcho Version	Policy	Idle Time
frank	192.168.11.29:49202			iOS	4.5.1.115	Frank	02:06:44
hristo	192.168.11.29:49211	айПад	iPad 2 (GSM)	iOS	5.0.0.127		02:03:57

現在、ゲートウェイ サーバーでアクティブなすべてのユーザーの表が表示されます。

- **ユーザー:** ユーザーの Active Directory 名（フル）を表示します。
- **ロケーション:** デバイスの IP アドレスを表示します。

- **デバイス:** ユーザーが設定したデバイス名を表示します。
- **モデル:** デバイスのタイプ/モデルを表示します。
- **OS:** デバイスのオペレーティングシステムを表示します。
- **クライアントのバージョン:** デバイスにインストールされている Acronis Cyber Files アプリのバージョンを表示します。
- **ポリシー:** デバイスが使用するアカウントのポリシーを表示します。
- **アイドル時間:** ユーザーがゲートウェイに接続した状態で経過した時間を表示します。

ゲートウェイサーバー構成

ゲートウェイサーバーの構成を変更するには、設定メニューに入力する必要があります。

1. **[モバイルアクセス]** → **[ゲートウェイサーバー]** タブに移動します。
2. 必要なサーバーの **[詳細]** の横にある矢印をクリックします。
3. **[編集]** を選択します。

全般設定

- **表示名:** ゲートウェイサーバーの表示名を設定します。この名前はあくまでも表示用であり、サーバーを区別しやすいようにするために使用されます。
- **管理用のアドレス:** Acronis Cyber Files サーバーとモバイルクライアントがアクセス可能なゲートウェイサーバーのデフォルトアドレスを設定します。IP アドレスではなく、DNS アドレスを使用することをおすすめします。

注意

これは、**[クライアント接続に代替アドレスを使用]** が有効にされていない限り、モバイルクライアントがゲートウェイサーバーに接続する際のデフォルトアドレスです。

- **クライアント接続に代替アドレスを使用:** 有効にすると、モバイルクライアントがゲートウェイサーバーに接続する際に使用するアドレスを上書きできます。

注意

この設定は、負荷分散装置または何らかのプロキシ（MobileIron など）経由でプロキシゲートウェイサーバーに接続する特定の構成のみで使用してください。通常の導入環境では、この設定を有効にする必要はありません。

- **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] が有効にした場合、このアドレスが、モバイルクライアントでゲートウェイサーバーに接続するために使用するアドレスになります。IP アドレスではなく、DNS アドレスを使用することをおすすめします。

ゲートウェイサーバーのログ

[ログ] セクションでは、この特定のゲートウェイサーバーのログイベントを監査ログに表示するかどうかを制御でき、またこのサーバーのデバッグ ログを有効にできます。

The screenshot shows a dialog box titled "Edit Server: Local" with a close button (X) in the top right corner. Below the title bar are five tabs: "General Settings", "Logging", "Search", "SharePoint", and "Advanced". The "Logging" tab is selected. Inside the dialog, there is a light blue informational box with the following text: "It is recommended that the Debug Logging setting only be changed at the request of a customer support representative. Additional debug logging can be useful in troubleshooting problems on the server." Below this, it says "Please consult the [documentation](#) for more information on where log files are located." Underneath the informational box are two checkboxes: "Audit Logging" (checked) and "Debug Logging" (unchecked). To the right of these checkboxes is a button labeled "Archive Log File". At the bottom right of the dialog are three buttons: "OK", "Apply", and "Cancel".

特定のゲートウェイ サーバーに対して監査ログを有効にするには:

1. ウェブ インターフェイスを開きます。
2. 管理者としてログインします。
3. [モバイル アクセス] タブを選択します。
4. [ゲートウェイ サーバー] タブを開きます。
5. [監査ログ] を有効にするサーバーを検索します。
6. [詳細] ボタンをクリックします。
7. [ログ] セクションで、[監査ログ] をオンにします。
8. [保存] ボタンをクリックします。

特定のゲートウェイ サーバーに対してデバッグ ログを有効にするには:

注意

デバッグログのデフォルトのロケーションは C:\Program Files (x86)\Acronis\Access\Gateway Server\Logs\AcronisAccessGateway です。

1. ウェブ インターフェイスを開きます。
2. 管理者としてログインします。
3. **[モバイル アクセス]** タブを選択します。
4. **[ゲートウェイ サーバー]** タブを開きます。
5. **[デバッグログ] を有効にするサーバーを検索します。**
6. **[詳細]** ボタンをクリックします。
7. **[ログ]** セクションで、**[デバッグログ]** をオンにします。
8. **[保存]** ボタンをクリックします。

ゲートウェイサーバーの検索オプション

要件

Acronis Cyber Files は、**Windows Search** を使用して、ネットワークデータソース内の検索を可能にしています。**Windows Search** は、Windows Server に組み込まれた機能ですが、デフォルトでは有効になっていません。

オンにするには、次の操作を実行します。

- サーバーマネージャで **ファイルサービス** 役割を追加/インストールします。
- **Windows Search サービス** が稼働していることを確認してください。

注意

上記要件が満たされない場合は、ネットワークデータソースで検索を実行できません。

また、以下に対する検索もサポートされません。

- NAS ファイルサーバー、CMIS、および SharePoint のデータロケーション。ただし、SMB/CIFS ファイルサーバーに対するサポートはあります。
- ファイルサーバーのルート (//server)。動作するのは (//server/share) 内部の実際の共有だけです。
- ゲートウェイマシン上のサービスアカウントが、リモート共有をホストしているコンピューターへのアクセス権 (Windows のアクセス許可) を持っていない場合。これを確認するには、管理サービスアカウントを使ってゲートウェイサービスを実行してみてください。

以下の場合は、**[検索]** フィールドが無効になります。

- 何らかの理由で検索できない
- インデックス付きのディレクトリが空である

ファイル名検索のローカル データ ソースのインデックスを作成

ネットワークデータソースでの検索は、Acronis Cyber Files ゲートウェイサーバーと Windows Search インデックスに依存しています。Windows Search インデックスが必要なボリュームに対して有効で、インデックス付けが終わっている場合は、ディープ検索とコンテンツ検索の両方をそこで実行できます。

デフォルトでは、インデックス検索がすべてのゲートウェイ サーバーで有効です。インデックス検索は、ゲートウェイの **[サーバーの編集]** ダイアログでゲートウェイサーバーごとに無効または有効にすることができます。

1. Acronis Cyber Files 管理コンソールを開きます。
2. **[モバイル アクセス]** > **[ゲートウェイ サーバー]** > **[編集]** > **[検索]** に移動します。
3. 以下をオンにします。
 - **[ファイル名検索のローカル データ ソースのインデックスを作成]** チェックボックス
 - オプションで、**[利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート]** チェックボックス

デフォルト パス

デフォルトで、スタンドアロンサーバーでは、Acronis Cyber Files が Acronis Cyber Files ゲートウェイサーバー アプリケーション フォルダ内の **[Search Indexes]** ディレクトリにインデックスファイルを保存します。別の場所にインデックス ファイルを保存する場合は、新しいフォルダのパスを入力します。

利用可能な場合、Microsoft Windows Search を使用してコンテンツ検索をサポート

共有フォルダのコンテンツ検索のサポートはデフォルトで有効になっており、このオプションを使用してオン/オフを切り替えることができます。コンテンツ検索は、ゲートウェイサーバーごとに有効または無効にすることができます。

Windows Search で必要なデータソースをインデックス化するように設定するには、スタートバーの **[Windows Search]** アイコンを右クリックし、**[Windows Search のオプション]** を選択します。

Windows の Reshare で Windows のコンテンツ検索を実行できますが、リモート マシンはゲートウェイサーバーと同じドメインに参加している必要があります。

注意

Windows の Reshare でコンテンツ検索を使用する場合は、データソースのボリュームパスはホスト名か完全な修飾子名にする必要があります。IP アドレスは Windows Search ではサポートされていません。

その他の構成

コンテンツ検索インデックス化は、特定のファイルタイプのコンテンツのみをインデックス化するように設定できます。

1. ゲートウェイサーバーをホストしているサーバーで、**[コントロール パネル]** -> **[インデックスのオプション]** を開きます。

2. [詳細設定] を選択して、[ファイルの種類] タブを開きます。
3. コンテンツ検索を有効/無効にするファイルの種類 (doc や txt) を探します。
4. 必要なファイルの種類を選択して、[このファイルのインデックスの作成方法] で、このファイルの種類コンテンツ検索を有効にする場合は [プロパティとファイルのコンテンツのインデックスを作成する] を、無効にする場合は [プロパティのみインデックスを作成する] を選択します。必要なすべてのファイルの種類に対してこのステップを繰り返します。

SharePoint設定

The screenshot shows a dialog box titled "Edit Server: Local" with a close button (X) in the top right corner. It has five tabs: "General Settings", "Logging", "Search", "SharePoint" (which is selected), and "Advanced". Below the tabs, there is a text instruction: "Required to enumerate SharePoint site collections. Account must have Full Read privileges. If Kerberos is used, enter the user principal name (e.g. account@example.com) into the account field and leave the domain field empty." Below this instruction are four input fields: "Domain" (empty), "Username" (empty), "Password" (containing "Password..."), and "Password Confirmation" (containing "Confirm password..."). At the bottom right, there are three buttons: "OK", "Apply", and "Cancel".

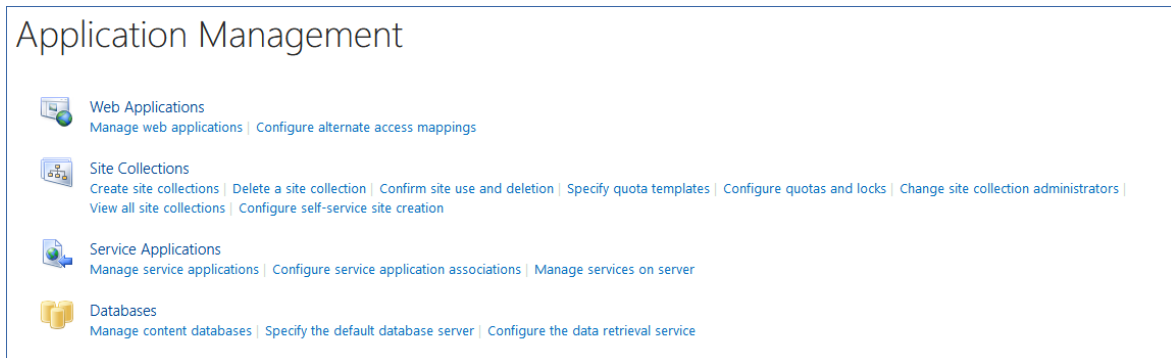
これらの資格情報の入力是一般的な SharePoint のサポートでは任意ですが、サイト コレクションを列挙するには必須です。たとえば、次の2つのサイトコレクションがあるとします。

- `http://sharepoint.example.com` と
`http://sharepoint.example.com/SeparateCollection.`

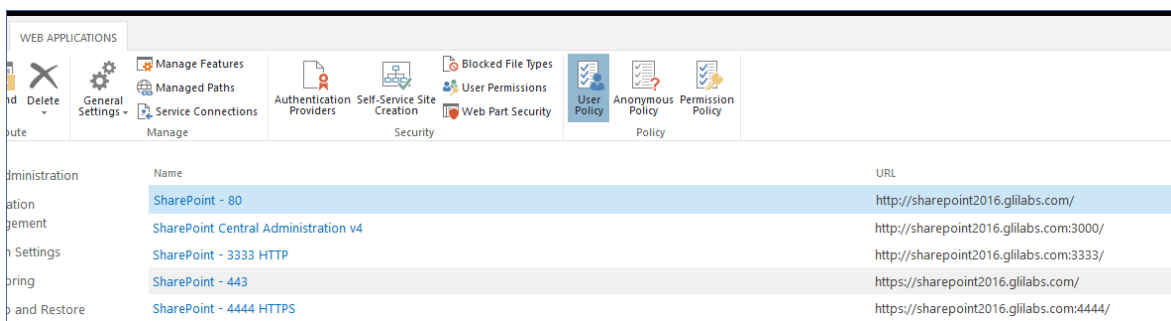
資格情報を入力しないと、**`http://sharepoint.example.com`**をポイントするボリュームを作成する場合、ボリュームを列挙するときに**SeparateCollection**というフォルダが表示されません。アカウントには、ウェブアプリケーションに対する**すべて読み取り**アクセスが必要です。

アカウントにすべて読み取り許可を与えるには（SharePoint 2016 および SharePoint 2010 の場合）：

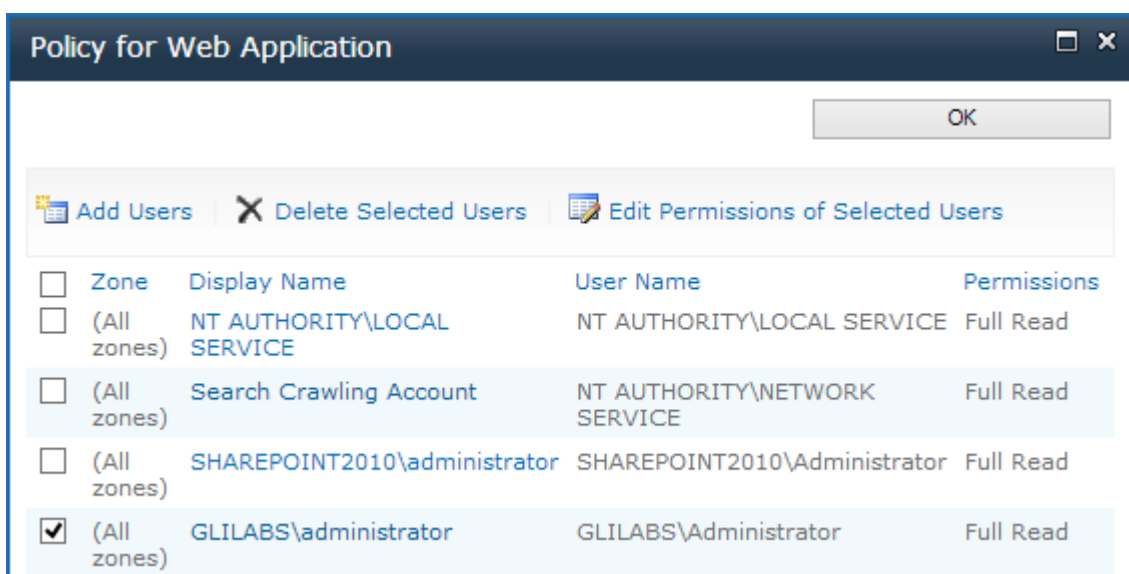
1. [SharePointのサーバー管理] を開きます。
2. [アプリケーション構成の管理] をクリックします。



3. [Webアプリケーション] で [Webアプリケーションの管理] をクリックします。
4. ウェブ アプリケーションをリストから選択し、[ユーザー ポリシー] をクリックします。



5. 権限を与えるユーザーのチェックボックスをオンにして、[選択したユーザーの権限の編集] をクリックします。ユーザーがリストに表示されない場合は、[ユーザーの追加] をクリックしてそのユーザーを追加できます。



6. [アクセス許可ポリシー レベル] セクションから [すべて読み取り - すべてに読み取り専用のアクセス権を持ちます] のチェックボックスをオンにします。

Policy for Web Application

Zone

The security policy will apply to requests made through the specified zone.

Zone:

(All zones)

Choose Users

You can enter user names or group names. Separate with semi-colons.

Users:

administrator

Choose Permissions

Choose the permissions you want these users to have.

Permissions:

☐ Full Control - Has full control.

☒ Full Read - Has full read-only access.

☐ Deny Write - Has no write access.

☐ Deny All - Has no access.

Choose System Settings

System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes made by a system account will be recorded as made by the system instead of the actual user account.

☐ Account operates as System

< Back

Finish

7. [保存] ボタンをクリックします。

詳細設定

Edit Server: Local

General Settings | Logging | Search | SharePoint | **Advanced**

It is recommended that these settings only be changed at the request of a customer support representative.

☐ Hide inaccessible items

☐ Hide inaccessible items on reshares ⓘ

☒ Hide inaccessible SharePoint sites

☐ Minimum Android client version

☒ Minimum iOS client version

2.0.0.282

☒ Use Kerberos for SharePoint Authentication

☐ Allow connections to SharePoint servers using self-signed certificates

☒ Allow connections to Acronis Cyber Files servers using self-signed certificates

☒ Accept self-signed certificates from this Gateway Server ⓘ

☐ Show hidden SMB Shares

☒ Use user principal name (UPN) for authentication with SharePoint Servers ⓘ

☐ Perform Negotiate/Kerberos authentication in user-mode ⓘ

Client session timeout in minutes

15

OK

Apply

Cancel

注意

これらの設定は、カスタマー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。

- **アクセスできない項目を非表示にする:** 有効にしている場合、ユーザーに読み取り許可がないファイルおよびフォルダは表示されません。
- **再共有上のアクセスできない項目を非表示にする:** 有効にしている場合、ユーザーに読み取り許可がない Network Reshare 上にあるファイルおよびフォルダは表示されません。

注意

この機能を有効にすると、フォルダの閲覧中に大きな悪影響が生じる可能性があります。

- **アクセスできない SharePoint サイトを非表示にする:** 有効にしている場合、ユーザーに必要な許可がない SharePoint サイトは表示されません。
- **最小 Android クライアント バージョン:** 有効にしている場合、このゲートウェイ サーバーに接続しているユーザーには、Acronis Cyber Files Android クライアント アプリのこれ以降のバージョンが要求されます。

- **最小 iOS クライアント バージョン:** 有効にしている場合、このゲートウェイ サーバーに接続しているユーザーには、Acronis Cyber Files iOS クライアント アプリのこれ以降のバージョンが要求されます。
- **SharePoint 認証に Kerberos を使用する:** SharePoint サーバーで Kerberos 認証が必要な場合、この設定を有効にする必要があります。また、ゲートウェイ サーバー ソフトウェアを実行している 1 台または複数の Windows サーバーの Active Directory コンピューター オブジェクトをアップデートする必要があります。Acronis Cyber Files Windows サーバーには、ユーザーの代理として SharePoint サーバーに委任認証情報を提示する許可を与える必要があります。Acronis Cyber Files Windows サーバーによる Kerberos 委任の実行を有効にするには、次のことを実行します。
 1. **[Active Directory ユーザーとコンピューター]** で、ゲートウェイ サーバーがインストールされている 1 台または複数の Windows サーバーを探します。それらのサーバーは、通常、**Computers** フォルダにあります。
 2. Windows サーバーの **[プロパティ]** ウィンドウを開き、**[委任]** タブを選択します。
 3. **[指定されたサービスへの委任でのみこのコンピューターを信頼する]** を選択します。
 4. **[任意の認証プロトコルを使う]** を選択します。これは SharePoint サーバーとのネゴシエーションに必要です。
 5. ここで、ユーザーが Acronis Cyber Files を使用してアクセスできるようにする SharePoint サーバーを追加する必要があります。SharePoint 実装が複数の負荷分散ノードで構成されている場合、許可を受けたコンピューターのリストに各 SharePoint/Windows ノードを追加する必要があります。**[追加...]** をクリックして、AD 内でこれらの Windows コンピューターを検索し、追加します。追加するたびに、「http」サービス タイプのみを選択します。

注意

これらの変更が AD を介して伝播し、適用されて、クライアントの接続性をテストできるようになるまで、15~20 分お待ちください。変更はすぐには反映されません。

- **自己署名した証明書を使用した SharePoint サーバーへの接続を許可:** 有効にしている場合、自己署名した証明書を使用して、このゲートウェイから SharePoint サーバーへの接続を許可します。
- **ゲートウェイサーバーからの自己署名証明書を承認:** 有効にすると、このゲートウェイサーバーが自己署名証明書を使用している場合でも、この Acronis Cyber Files サーバーをこのゲートウェイに接続できます。
- **自己署名証明書を使用した Acronis Cyber Files サーバーへの接続を許可:** 有効にすると、Acronis Cyber Files サーバーが自己署名証明書を使用している場合でも、このゲートウェイ サーバーから Acronis Cyber Files サーバーへの接続を許可します。
- **非表示の SMB 共有の表示:** 有効にしている場合、非表示のシステム SMB 共有をユーザーに表示します。
- **クライアント セッション タイムアウト (分単位):** 非アクティブなユーザーがゲートウェイ サーバーから排除されるまでの時間を設定します。
- **ユーザー プリンシパル名 (UPN) を使用した SharePoint サーバーの認証:** 有効にすると、ユーザーは各自のユーザー プリンシパル名 (例: hristo@glilabs.com) を通じて SharePoint サーバーへの認証を行います。有効にしていない場合は、ドメインとユーザー名の組み合わせ (例: glilabs/hristo) を使用して認証を行います。

- **ユーザーモードでネゴシエート/Kerberos 認証を実行:** 有効にすると、ゲートウェイサーバーは、接続しているユーザーの Kerberos チケットを使用して、データソースに対して認証を行います。これは、Kerberos（シングルサインオンや負荷分散など）を必要とする構成でのみ使用されます。

カスタムアクセス制限

[ポリシー] セクションのデフォルトアクセス制限セットを使用するか、ゲートウェイサーバーごとにカスタムアクセス制限を設定できます。

特定のゲートウェイサーバーのカスタムアクセス制限の設定

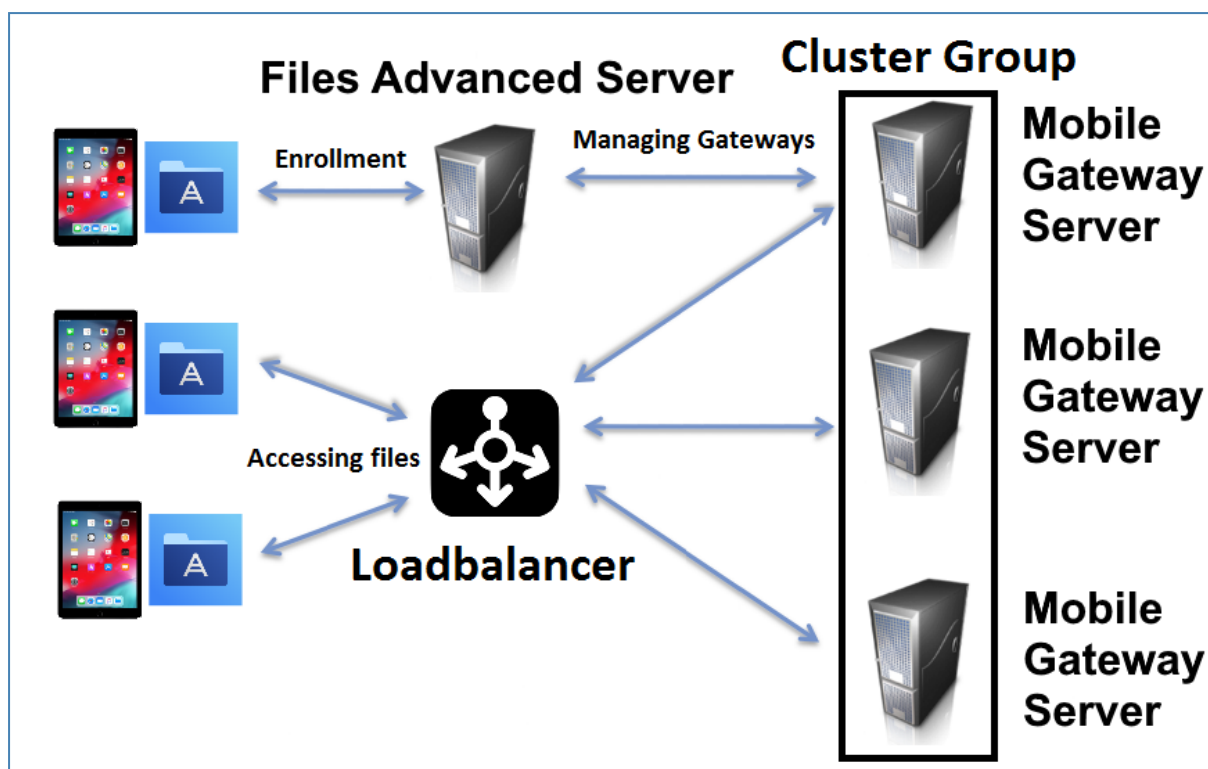
1. **[モバイルアクセス]** → **[ゲートウェイサーバー]** タブに移動します。
2. 必要なサーバーの **[詳細]** の横にある矢印をクリックします。
3. **[アクセス制限]** を選択します。
4. **[カスタム設定の使用]** タブを開きます。
5. このゲートウェイサーバーに適用する、特定のアクセス制限を選択します。
6. **[適用]** を押します。

クラスターグループ

Acronis Cyber Files では、ゲートウェイサーバーのクラスターグループを作成できます。

クラスターグループは、同じ構成を共有する複数のゲートウェイサーバーの集まりです。このグループにより、グループ内のすべてのゲートウェイを一度に制御することができ、各ゲートウェイ上で個別に同じ設定をする必要がなくなります。通常、モバイルクライアントに高可用性とスケーラビリティを提供するため、これらのサーバーは**負荷分散装置**の背後に配置されます。

クラスター化されたゲートウェイ設定の場合、負荷分散装置、2 つ以上のゲートウェイ、および Acronis Cyber Files サーバーが必要になります。すべてのゲートウェイサーバーは、Acronis Cyber Files Web インターフェースでクラスターグループに追加し、負荷分散装置の背後に配置する必要があります。Acronis Cyber Files サーバーは、管理サーバー、およびモバイルクライアントがクライアント管理に登録するサーバーとして機能します。このサーバーでは、ポリシー、デバイス、および設定のすべてが管理されます。一方、ゲートウェイでは、ファイル共有へのアクセスが提供されます。



クラスターグループを作成するには、次の手順を実行します。

続行する前に、各ゲートウェイ上で正しい**管理のアドレス**が設定済みであることを確認してください。これは、ゲートウェイ サーバーの DNS アドレスまたは IP アドレスです。

1. Acronis Cyber Files Web インターフェースを開きます。
2. **[モバイル アクセス]** タブを選択します。
3. **[ゲートウェイ サーバー]** ページを開きます。
4. **[クラスターグループの追加]** ボタンをクリックします。
5. グループの表示名を入力します。
6. 負荷分散装置のFQDNまたはIPアドレスを入力します。
7. 必要に応じて、Acronis Cyber Files サーバー接続に別のアドレスを選択することもできます。選択する場合は、チェックボックスをオンにして、アドレスを入力します。
8. グループに含めるそれぞれのゲートウェイのチェックボックスにマークを付けます。
9. グループの設定を制御するゲートウェイを選択します。そのゲートウェイ上の既存の設定のすべて（割り当てられているデータ ソースは含まれますが、管理のアドレスは含まれません）が、グループ内の各ゲートウェイにコピーされます。
10. **[作成]** をクリックします。

クラスターグループの編集:

クラスターグループの編集作業は、標準的なゲートウェイを編集する作業と違いはありません。詳細については、「**ゲートウェイサーバーの編集**」の資料を参照してください。

既存のクラスターグループにメンバーを追加するには、次の操作を実行します。

1. Web インターフェースを開き、**[モバイルアクセス]**→**[ゲートウェイサーバー]**に移動します。
2. 目的のクラスターグループの操作メニューを開き、選択可能な操作から**[クラスターメンバーの追加]**を選択します。
3. リストから目的のゲートウェイサーバーを選択し、**[追加]**を押します。

マスターゲートウェイサーバーの変更:

1. Web インターフェースを開き、**[モバイルアクセス]**→**[ゲートウェイサーバー]**に移動します。
2. 目的のクラスターグループを展開します。
3. マスターに昇格させるゲートウェイサーバーを見つけます。
4. **[操作]** ボタンをクリックして、**[グループマスターにする]**を選択します。

データソースの管理

Acronis Cyber Files ユーザーがアクセスできるように、Windows サーバー、CMIS システム、またはリモート SMB/CIFS ファイル共有上に存在する NTFS ディレクトリを共有することができます。ユーザーが接続すると、これらのディレクトリがファイル共有ボリュームとして表示されます。

SharePoint 2007、2010、2013、2016 のコンテンツへのアクセス

Acronis Cyber Files を使用すると、SharePoint 2007、2010、2013、および 2016 サーバーのドキュメントライブラリ内に存在するファイルにアクセスできます。Acronis Cyber Files SharePoint データソースは、SharePoint サーバー全体、特定の SharePoint サイトまたはサブサイト、特定のドキュメントライブラリを指し示すことができます。これらのファイルに対しては、従来のファイルサーバーや NAS ストレージに存在するファイルとまったく同様に、プレビュー、PDF 注釈、編集、および同期を行うことができます。また Acronis Cyber Files では、SharePoint ファイルの**チェックアウト**と**チェックイン**もサポートされます。

SharePointの認証方法をサポート

Acronis Cyber Files は NTLMv1、NTLMv2、クレームベース、Kerberos を使用したクライアント認証が可能な SharePoint サーバーをサポートしています。SharePoint サーバーが Kerberos 認証を要求する場合、Windows サーバー、または Acronis Cyber Files サーバーソフトウェアが実行されているサーバーの Active Directory コンピューターオブジェクトをアップデートする必要があります。Acronis Cyber Files Windows サーバーには、ユーザーの代理として SharePoint サーバーに委任認証情報を提示する許可を与える必要があります。

OneDrive for Businessコンテンツへのアクセス

Acronis Cyber Files をセットアップして、ユーザーが SharePoint データソース経由で自分個人の OneDrive for Business コンテンツにアクセスできるようにすることができます。いくつかの要件と制限

があります。

共有ファイルおよびフォルダの許可の変更

Acronis Cyber Files は、既存の Windows のユーザーアカウントとパスワードを使用します。Acronis Cyber Files では Windows NTFS 許可が実行されるため、通常は Windows に組み込まれているツールを使って、ディレクトリとファイルの許可を調整してください。標準の Windows ツールは、セキュリティ ポリシーを設定するための最も柔軟な手段です。

Acronis Cyber Files データソース（別の SMB/CIFS ファイルサーバーに存在する）は、ゲートウェイサーバーからセカンダリサーバーまたは NAS への SMB/CIFS 接続によってアクセスされます。この場合、セカンダリサーバーへのアクセスは、Acronis Cyber Files クライアントの 1 つにログインしているユーザーのコンテキストで実行されます。ユーザーがセカンダリサーバー上のファイルにアクセスできるようにするには、ユーザーのアカウントに、それらのファイルにアクセスするための「Windows 共有のアクセス許可」と NTFS セキュリティ許可の両方が必要です。

SharePoint サーバーに存在するファイルへの許可は、SharePoint サーバーで設定されている SharePoint のアクセス許可に従って管理されます。ユーザーは、ウェブブラウザを使用して SharePoint ドキュメントライブラリにアクセスする際に受け取るものと同じ許可を Acronis Cyber Files を介して受け取ります。

フォルダ

フォルダに対して Acronis Cyber Files のユーザーポリシーおよびグループポリシーを割り当てることができ、これにより、ユーザーの Acronis Cyber Files アプリにフォルダが自動的に表示されるようになります。ゲートウェイサーバー、リモート共有、CMIS ボリューム、さらには SharePoint Library であっても、そこにある任意のフォルダにポイントするように、フォルダを設定できます。そうすることでユーザーは、そのフォルダまで場所を探しながら移動する必要はなくなり、サーバー、共有ボリューム名、およびフォルダへのパスを正確に知らなくても、自分にとって重要なフォルダに直接アクセスできるようになります。

フォルダは、リムーバブルメディア上にあるのでない限り、種類を問わず Acronis Cyber Files がアクセスを提供するコンテンツすべてをポイントできます。これにより、Acronis Cyber Files 管理内で既に構成されているゲートウェイサーバー内でのロケーションが参照されます。ロケーションには、ローカルのファイル共有ボリューム、他のファイルサーバーや NAS 上のファイルへのアクセスを提供する

「Network Reshare」ボリューム、DFS 共有、CMIS ボリューム、SharePoint ボリュームなどがあります。

注意

DFS のデータソースを作成する場合は、次の方法でフルパスを DFS に追加する必要があります：

¥¥company.com¥namespace¥share

注意

Acronis Cyber Files をクリーンインストールする際、Sync & Share を有効にしているゲートウェイサーバーが存在する場合は、Sync & Share のデータソースが自動的に作成されます。初期設定の **[サーバー]** セクションで設定した URL をポイントします。モバイル ユーザーはこのフォルダを使用して、Sync & Share のファイルおよびフォルダにアクセスできるようになります。

フォルダの同期

オプションで、フォルダをクライアント デバイスに同期するように設定できます。Acronis Cyber Files フォルダ同期オプションは次のとおりです。

注意

この設定は、デスクトップクライアントに影響しません。

- **なし:** フォルダは、Acronis Cyber Files アプリにネットワーク ベースのリソースとして表示され、ゲートウェイサーバーとまったく同じようにアクセスおよび操作できます。
- **一方向:** このフォルダは、Acronis Cyber Files アプリに、ローカルフォルダとして表示されます。フォルダの内容全体がサーバーからデバイスへ同期され、サーバー上のファイルの追加、変更、または削除が発生した場合、最新の状態が反映されます。このフォルダは、サーバー ベースのファイルにローカルまたはオフラインでアクセスするためのものであり、ユーザーに対しては読み取り専用フォルダとして表示されます。
- **双方向:** このフォルダは、Acronis Cyber Files アプリに、ローカルフォルダとして表示されます。最初に、フォルダの内容全体がサーバーからデバイスへ同期されます。デバイスがサーバーのどちらかでこのフォルダ内のファイルが追加、変更、または削除されると、その変更内容が対応するサーバーまたはデバイスにも同期されます。

データソースの作成と編集

データ ソースの作成

1. Acronis Cyber Files Web インターフェースを開きます。
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. **[新しいフォルダを追加]** をクリックします。

Add New Folder

Display Name:

Select the Gateway Server to use to give access to this data source:

Data Location:

Enter the path to the local folder on this Acronis Cyber Files Gateway Server that you would like to share. (Example: "E:\Shares\Documents\"). You can include the wildcard string %USERNAME% in the path, in which case the wildcard will be replaced with the user's username.

Path:

Automatic Sync (Mobile Apps):

☐ Show When Browsing Server

Assign This Folder to a User or Group

Find User or Group that

Common Name / Display Name	Distinguished Name	Login Name
Domain Users	CN=Domain Users,CN=Users,DC=bgtest,DC=corp,DC=acronis,DC=com	Domain Users

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、Sync & Shareサーバー上を選択できます。

注意

リムーバブルメディアのフォルダを共有フォルダとして使用することはできません。別のロケーションから選択してください。

注意

Sync & Share 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 Cyber Files 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、このデータソースを表示するには、**[サーバーの参照時に表示する]**を有効にします。

注意

SharePoint のデータソースを作成する場合には、SharePoint フォローサイトの表示を有効化するオプションがあります。

12. **[保存]** ボタンをクリックします。

データソースの編集

1. **[データソース]** セクションを開いて、編集するデータソースを見つけます。
2. テーブルの右側にデータソース用に表示される **[鉛筆]** アイコンをクリックします。
3. 目的のパラメータを変更し、**[保存]** を押します。

SharePoint サイトとライブラリ

データソースを作成することで、Acronis Cyber Files モバイルユーザーは SharePoint のサイトおよびライブラリに簡単にアクセスできるようになります。SharePoint のデータソースを作成する方法は 2 つあり、SharePoint の設定により異なります。

注意

URL を入力する際には、そのルートがデフォルトのサイトコレクションであることを必ず確認してください。

SharePoint サイト全体またはサブサイトのデータソースの作成

SharePoint サイト または **サブサイト** のデータ ソースを作成する場合、入力するのは **URL** フィールドのみです。SharePoint のサイトまたはサブサイトのアドレスを入力してください。（

e.g. `https://sharepoint.mycompany.com:43222`

e.g. `https://sharepoint.mycompany.com:43222/subsite name`）

SharePoint フォローサイト

SharePoint フォローサイトは、サイトのデータソースを作成する際に有効化できます。これは [フォローサイトを表示する] チェックボックスで行います。有効化した場合、サイトをフォローするすべてのユーザー側で、Acronis Cyber Files にフォルダ「フォローサイト」が表示されます。このフォルダには、当該サイトからのアクセス許可があるリソースが含まれます。

注意

SharePoint フォローサイトは同期されません。

注意

パスの一部としてワイルドカード文字列 `%USERNAME%` を含めることが可能です。ワイルドカードは、ユーザーのメインの個人フォルダ名に置き換えられます。`%USERNAME%` は大文字で指定する必要があります。

また、URL の一部としてワイルドカード文字列 `%USERNAME%` を含めることもできます。

SharePoint ライブラリのデータ ソースの作成

SharePoint ライブラリのデータ ソースを作成する場合、**[URL]** と **[ドキュメントライブラリ名]** の両方のフィールドに入力する必要があります。URL フィールドには SharePoint のサイトまたはサブサイトのアドレスを入力し、**[ドキュメント ライブラリ名]** フィールドにはライブラリ名を入力します。

URL の例: https://sharepoint.mycompany.com:43222

ドキュメント ライブラリ名の例: My Library

SharePoint ライブラリ内の特定のフォルダのデータ ソースの作成

SharePoint ライブラリ内の特定のフォルダのデータソースを作成する場合、すべてのフィールドを入力する必要があります。URL フィールドには SharePoint のサイトまたはサブサイトのアドレスを入力し、[ドキュメント ライブラリ名] にはライブラリ名を入力しますおよび [サブパス] フィールドには、目的のフォルダの名前を入力します。

URL の例: https://sharepoint.mycompany.com:43222

ドキュメント ライブラリ名の例: Marketing Library

サブパスの例: Sales Report

注意

サブパスで SharePoint リソースにポイントするデータソースを作成する場合、**[サーバーの参照時に表示する]** オプションを有効にすることはできません。

Acronis Cyber Files モバイルでは、NTLM 認証、Kerberos 制約付き委任認証、クレームベース認証、および SharePoint 365 認証がサポートされています。SharePoint の設定によっては、データ ソースへの接続に使用するゲートウェイ サーバーで追加設定が必要になる場合があります。詳細については、[ゲートウェイサーバーの編集](#)の記事を参照してください。

CMIS (Content Management Interoperability Services) ポリリューム

サポートされているCMISポリリュームは、**Alfresco (CMIS)** ポリリュームと**Documentum (CMIS)** ポリリュームです。また、**[汎用CMIS (AtomPub)]** オプションで、**AtomPub**プロトコルが使用されている他のCMISベンダの使用を試みることもできます。このオプションは、ベンダによって機能する場合と機能しない場合があります、Acronisではサポートされていません。

低速のネットワークでタイムアウトの発生を少なくするために、CMISポリリュームをホストしているマシンにゲートウェイサーバーを配置することをお勧めします。

注意

CMIS ポリリュームには、フォルダをコピーできないという制限があります。

OneDrive for Business

OneDrive for Business は SharePoint ベースなので、Acronis Cyber Files に SharePoint データソースを作成することによって、そのコンテンツにアクセスできます。その場合でも、いくつかの制限があります。

- データソースがユーザーのメインの個人フォルダのワイルドカードをポイントしている**必要があります**。サブフォルダをポイントするデータソースを作成することはできませんが、サブフォルダへはメインフォルダからアクセスおよび参照可能です。
- ゲートウェイサーバーがアプリに手動で追加された場合は、このように設定したデータソースを使用することはできません。データソースはポリシーで割り当てる必要があります。

- Active Directory では Federated AD Services を使用するか、Azure AD を指定する必要があります。
- 各ユーザーは自分のOneDriveデータのみ表示することができ、Microsoftポータル経由で共有されてアクセス可能であっても、他のユーザーのデータにはアクセスできません。

データソースの作成

1. Acronis Cyber Files Web インターフェースを開きます。
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. **[新しいフォルダを追加]** ボタンを押します。
6. フォルダの表示名を入力します。
7. リソース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]** フィールドで **[SharePoint]** オプションを選択します。以下のフィールドが表示されます。
 - **URL:** アクセス権を付与する OneDrive for Business サーバー、サイト、またはサブサイトの SharePoint の場所を入力します（たとえば、
<https://sharepoint.company.com/mysite/mysubsite/%USERNAME%>）。
 この URL では、サブサイトより上位のレベルを指定することはできません（default.aspx は含め
 ないでください）。
 パスの一部としてワイルドカード文字列 %USERNAME% を含めることが可能です。ワイルドカード
 は、ユーザーのメインの個人フォルダ名に置き換えられます。%USERNAME% は大文字で指定する必
 要があります。
 - （オプション）**ドキュメント ライブラリ名:** このフィールドでは、特定のドキュメント ライブラ
 リの名前を指定できます。
 - （オプション）**サブパス:** このフィールドには、特定のドキュメント ライブラリ内にあるフォル
 ダ名を含めることができます。スラッシュ (/) を区切り記号として使用します。たとえば、
 Sales/Documents のようになります。
9. **[保存]** ボタンを押します。

割り当て済みのソース

このページでは、ユーザーまたはグループを検索して、どのリソースが割り当てられているかを確認で
 きます。リソースは、2つの表（サーバーとフォルダ）に一覧表示されます。

- サーバーの表には、ゲートウェイ サーバーの表示名、DNS または IP アドレス、およびこのサーバー
 が割り当てられているポリシーが一覧表示されます。
- フォルダの表には、データ ソースの表示名、ゲートウェイ サーバー、同期タイプ、パス、およびこ
 のデータ ソースが割り当てられているポリシーが一覧表示されます。
- 管理者は**[Xに割り当てられたリソースの編集]** ボタンを押すことで、このポリシーに対する割り当て
 をすばやく編集することができます。

クライアントで表示されるゲートウェイ サーバー

ゲートウェイ サーバーをユーザー ポリシーまたはグループ ポリシーに割り当て、データ ソースとして使用できます。このページには、ユーザーの Acronis Cyber Files モバイルアプリ内に表示されるすべてのゲートウェイサーバーと、それらのゲートウェイサーバーが特定のユーザーポリシーまたはグループポリシーに割り当てられているかどうかが表示されます。これらの割り当てをここで編集することもできます。Acronis Cyber Files モバイルユーザーがゲートウェイサーバーを参照すると、**[ゲートウェイサーバーの参照時に表示]** オプションが有効になっているデータソースが表示されます。

サーバーの現在の割り当てを編集するには

- そのサーバーの **[編集]** ボタンをクリックします。
 - このサーバーの割り当てをユーザーから解除する場合は、そのユーザーの **[X]** をクリックします。
 - 新規のユーザーまたはグループをこのサーバーに割り当てる場合は、ユーザー/グループ名を見つけてクリックします。
- [保存]** ボタンをクリックします。

注意

Cyber Files サーバー管理コンソールからゲートウェイサーバーを削除する場合、このサーバー上のデータソースのすべてのユーザーのモバイルブックマークは完全に削除されます。同じサーバーとデータソースが再び追加されたとしても、それらの復元は不可能です。

設定

Acronis Cyber Files

Mobile Access

Enroll Users

Policies

Gateway Servers

Data Sources

Settings

Sync & Share

Audit Log

Enrollment Settings

Mobile Client Enrollment Address

☐ Allow mobile clients restored to new devices to auto-enroll without PIN

☒ Use user principal name (UPN) for authentication to Gateway Servers ⓘ

Device Enrollment Requires:

☒ A PIN number + Active Directory username and password

☐ Active Directory username and password only

Save

登録設定

- **モバイル クライアントの登録用アドレス:** モバイル クライアントをクライアント管理で登録する際に使用するアドレスを指定します。

注意

モバイル クライアント登録アドレスに DNS 名を使用することを強くお勧めします。クライアント管理への登録に成功すると、Acronis Cyber Files モバイルアプリによって Acronis Cyber Files サーバーのアドレスが保存されます。そのアドレスが IP アドレスで、そのアドレスが変更された場合、ユーザーはサーバーに接続できなくなり、アプリケーションを非管理にはできないため、アプリケーション全体を削除して管理に再登録する必要があります。

- **モバイルクライアントを新しいデバイスに復元した場合でも、PIN コードなしで自動登録されるようにする:** この設定を有効にすると、以前のバージョンの Acronis Cyber Files モバイルによって管理されていたユーザーが PIN コードを使用せずに新しいサーバーに登録できるようになります。
- **ユーザー プリンシパル名 (UPN) を使用したゲートウェイ サーバーの認証:** この設定を有効にすると、ユーザーは UPN (例: user@company.com) を使用してゲートウェイ サーバーに対する認証を行います。無効にした場合は、ユーザーはドメイン名とユーザー名の組み合わせ (例: domain/user) を使用して認証を行います。

デバイスの登録に必要なもの:

- **PIN コード + Active Directory のユーザー名とパスワード:** ユーザーは、自分の Acronis Cyber Files アプリをアクティブ化して Acronis Cyber Files サーバーにアクセスするために、有効期限が設定されたワンタイム PIN コードと有効な Active Directory ユーザー名およびパスワードの入力が求められます。このオプションを使用する場合、ユーザーは、IT 管理者によって発行された PIN コードを受け取った後に 1 台のデバイスのみ登録することができます。このオプションは、2 つの要素によるデバイス登録でセキュリティを強化する必要がある場合に推奨されます。
- **Active Directory のユーザー名とパスワードのみ:** ユーザーは Active Directory のユーザー名とパスワードのみを使用して Acronis Cyber Files アプリをアクティブ化することができます。このオプションを使用すると、ユーザーが今後いつでも 1 台以上のデバイスを登録することができます。ユーザーには、Acronis Cyber Files サーバーの名前、または Acronis Cyber Files サーバーをポイントする URL のみを提供する必要があります。この情報は、Web サイトに掲示したり電子メールで送信したりできるので、多数のユーザーへの Acronis Cyber Files のロールアウトを簡素化することができます。このオプションは、2 つの要素による登録が不要な環境および学生用の導入など多くのユーザーがいつでも Acronis Cyber Files にアクセスする必要がある環境に推奨されます。

Sync & Share

ウェブインターフェースのこのセクションは、同期と共有機能を有効にしている場合にのみ使用できます。有効にしていない場合は、[同期と共有サポートを有効にする] ボタンが表示されます。

一般制限事項

General Restrictions

These restrictions apply to the usage of Sync & Share storage for all internal and external users

☐ Maximum allowed file size

1

MB

Blocklisted file types

Specify file types not allowed, by file extension (e.g. mp3, exe).

+ Add

- Remove

Save

ファイルの種類によるブロックリストや、指定サイズを超えるファイルの制限などの、基本的な制限事項を設定できます。

許可されている最大ファイルサイズ: Sync & Shareのすべてのファイルに対して最大ファイルサイズを設定できます。

ブロックリストに含まれるファイルの種類: Sync & Share機能で特定のファイルの種類を使用することをブロックできます。

ファイルの種類のブロックリストを設定するには、次の手順を実行します。

1. ウェブコンソールで **[Sync & Share]** タブを展開し、**[一般制限事項]** を開きます。
2. **[ブロックリストに含まれるファイルの種類]** の **[フィールドの追加]** で、ブロックするファイルの種類をすべてカンマ区切りで入力します。
3. **[保存]** をクリックします。

注意

指定した種類のファイルが既に存在する場合、同期も移動もされなくなります。手動でのみ、ファイルのダウンロードおよび削除を実行できます。

ファイルの最大サイズを設定するには、次の手順を実行します。

1. ウェブコンソールで **[Sync & Share]** タブを展開し、**[一般制限事項]** を開きます。
2. **[許可されている最大ファイルサイズ]** チェックボックスをオンにして、テキストフィールドに最大のファイルサイズ（MB単位）を入力します。
3. **[保存]** をクリックします。

注意

指定したファイルサイズより大きいファイルが既に存在する場合、同期も移動もされなくなります。手動でのみ、ファイルのダウンロードおよび削除を実行できます。

共有の制限

Acronis Cyber Files

Mobile Access

Sync & Share

General Restrictions

Sharing Restrictions

LDAP Provisioning

Quotas

File Purging Policies

User Expiration Policies

File Repository

Desktop Client

Audit Log

Users & Devices

General Settings

Sharing Restrictions

☒ Allow Collaborators to Invite Other Users

Single File Sharing

☒ Enable Single File Sharing

☒ Allow Public Download Links

☒ Allow 'All Acronis Cyber Files Users' Download Links

☒ Allow 'Shared to Users Only' Download Links

☒ Require that Shared Files Links Expire

Maximum Expiration Time: 365 days

☐ Only Allow Sharing of Single-Use Download Links

Folder Sharing

☐ Require that Shared Folders Expire

Allowlist

When enabled, only users in the configured LDAP groups or with email domains specified in the allowlist can have files and folders shared to them. Users are also required to be included in the allowlist to log into this Acronis Cyber Files server. If the LDAP group or email domain for an existing Acronis Cyber Files Sync and Share user is removed from the allowlist, they will lose the ability to log in to their account.

☐ Enable Allowlist

Blocklist

グループ作業者が他のユーザーを招待できるようにする: この設定が無効な場合、ユーザーをフォルダに招待するとき、**[グループ作業者が他のグループ作業者を招待できるようにする]** チェックボックスは表示されません。これにより、招待されたユーザーが他のユーザーを招待できないようになります。

単一ファイル共有の有効期限

単一ファイル共有を有効にする: この設定が有効な場合、単一ファイルリンクを共有できるようになり、ユーザーのリンクへのアクセス方法およびアクセス可能な期間を制御できます。

- **ダウンロードの公開リンクを許可する:** この設定が有効な場合、共有ファイルへのリンクを持っているすべてのユーザーがファイルにアクセスできます。
- **[すべての Acronis Cyber Files ユーザー] のダウンロードリンクを許可:** この設定が有効な場合、Acronis Cyber Files の資格情報を持っているユーザーのみが共有ファイルにアクセスできます。
 - **内部の (AD) ユーザー限定でダウンロードを許可する:** この設定が有効な場合、Acronis Cyber Files 用の Active Directory 資格情報を持っているユーザーのみが共有ファイルにアクセスできます。
- **共有済みユーザー専用のダウンロードリンクを許可:** この設定が有効な場合、共有済みユーザーのみがリンクを使用できます。

- **共有ファイルリンクの有効期限を必須にする:** この設定が有効な場合、ファイルリンクに有効期限が適用されます。
 - **最長有効期間:** ファイルの有効期限が終了するまでの最長期間（日単位）を制御します。
- **1 回限りのダウンロードリンクでの共有のみ許可する:** 有効にした場合、ユーザーは1回だけ使用できるリンクのみを送信できます。これらのリンクは1回目のダウンロード後に無効になります。

フォルダの共有

共有フォルダの有効期限を必須にする: この設定が有効な場合、すべての共有フォルダに有効期限を設定する必要があります。

- **最長有効期間:** フォルダの有効期限が終了するまでの最長期間（日単位）を制御します。

許可リスト

許可リストを有効にした場合、設定済みの LDAP グループ内のユーザーまたはリストで指定された電子メールアドレス（例: example.com）を使用するユーザーのみがログインできます。ドメインにワイルドカードを使用できます（例: *.example.com）。LDAP グループは、CN=mygroup,CN=Users,DC=mycompany,DC=com のように識別名で指定する必要があります。

ブロックリスト

LDAP グループ内のユーザーまたはブロックリストで指定された電子メールアドレス（例: example.com）を使用するユーザーは、許可リストに記載されていても、システムにログインできません。ドメインにワイルドカードを使用できます（例: *.example.com）。LDAP グループは、CN=mygroup,CN=Users,DC=mycompany,DC=com のように識別名で指定する必要があります。

注意

ワイルドカードのエントリは、* を 1 つのみ使用でき、必ず文字列の先頭に配置される必要があります。ワイルドカードの後にはピリオドが続きます（例: *.example.com、*.com）

LDAP プロビジョニング

ここに表示されているグループのメンバーは、初回ログイン時にユーザーアカウントが自動的に作成されます。そのためアカウント作成プロセスは簡単になり、管理者は各ユーザーに招待を送信する必要がありません。

LDAP Provisioning

Members of groups listed here will have their user accounts automatically created at first login.

LDAP Group

CN=Domain Users,CN=Users,DC=test,DC=biz

Remove

Search for an LDAP group and click on the Common Name to add it to the Provisioned LDAP Groups list. Click save once you have added all desired groups.

Find group that

begins with

Search

LDAP グループ

現在選択されているグループのリストです。

- **共通名/表示名:** ユーザーやグループに設定している表示名。
- **識別名:** ユーザーやグループに設定している識別名。識別名は、ディレクトリ サービスのエントリ用の固有の名前です。

クォータ

管理者は、システム内のユーザーごとに空き容量を設定できます。外部（一時的）ユーザーおよび内部（Active Directory - LDAP）ユーザー用に異なるデフォルト設定があります。

また、管理者は、個々のユーザーまたは Active Directory グループメンバーシップに基づいて異なるクォータ値を割り当てることもできます。

Enable Quotas? ☒

Default quota notification interval

2

days

Ad-hoc User Quota

2

GB

LDAP User Quota

2

GB

Enable admin-specific quotas? ☒

Admin Quota

15

GB

- **クォータを有効にしますか？**: 有効にすると、一人のユーザーに割り当てられるクォータの最大領域が制限されます。
 - **デフォルトのクォータ通知間隔**: クォータ上限に近づいたユーザーに対する通知電子メールの受信頻度を設定する時間間隔（日単位）です。
 - **一時的なユーザー クォータ**: 一時的なユーザーのクォータを設定します。
 - **LDAP ユーザー クォータ**: LDAP ユーザーのクォータを設定します。
 - **管理者固有のクォータを有効にしますか？**: 有効にすると、管理者には他のクォータが割り当てられます。
 - **管理者クォータ**: 管理者用のクォータを設定します。

注意

一人のユーザーが複数のグループのメンバーである場合は、最大のクォータのみが適用されます。

注意

クォータは個別のユーザーに対して指定できます。個別のクォータの設定は、他のすべてのクォータの設定よりも優先されます。他のユーザーの個別のユーザー クォータを追加するには、ユーザーごとに **[ユーザー]** ページでユーザーを編集します。

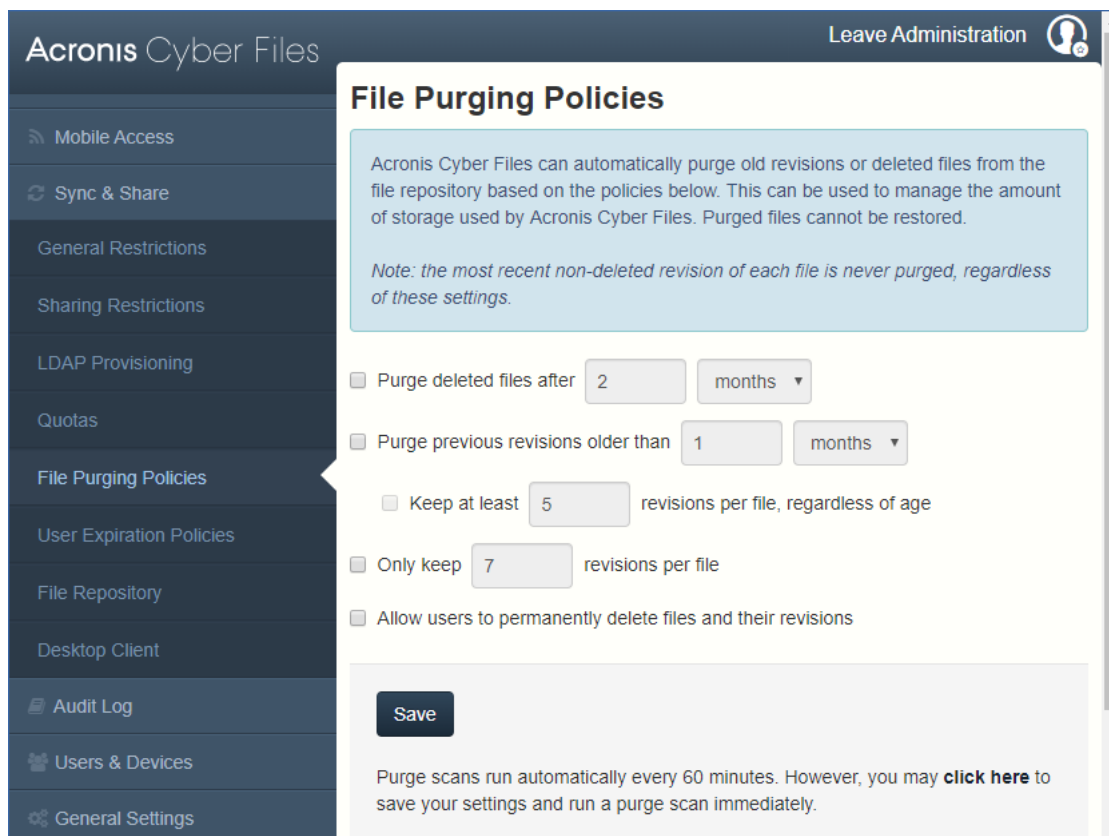
注意

クォータは 1 GB より小さいサイズで、メガバイト単位で設定することができます。例:**0.5**、**0.3**、**0.9**など。

ファイル消去ポリシー

Acronis Cyber Filesで、通常、ファイルは明示的に削除されない限りシステム内に保存されます。これにより、ユーザーは削除されたファイルをリカバリし、文書の以前のバージョンを維持することができます。Acronis Cyber Filesで管理者は、削除されたファイルを保存する期間、保存するリビジョンの最大数、古いリビジョンを削除するタイミングを決定するポリシーを定義できます。

Acronis Cyber Files では、下記のポリシーを基にして古いリビジョンや削除されたファイルをファイルリポジトリから自動的に完全削除することができます。この機能を利用して Acronis Cyber Files によって使用されるストレージの容量を管理することができます。消去されたファイルは復元できません。



注意

各ファイルの削除されていない最新のリビジョンは、以下の設定に関係なく消去されません。

- **削除済みファイルを消去する期限:** 有効にされている場合、この設定より古いファイルは削除されます。
- **過去のリビジョンを消去する期限:** 有効にされている場合、この設定より古いファイルのリビジョンは消去されます。
 - **ファイルごとにX以上のリビジョンを期間に関係なく保持する:** 有効にされている場合、ファイルの経過日数に関係なく、ファイルごとに最大のリビジョン数を保持します。
- **ファイルごとにXのリビジョンのみを保持する:** 有効にされている場合、ファイルごとに保持する最大のリビジョン数が制限されます。
- **ファイルおよびそのリビジョンの完全な削除をユーザーに許可する:** 有効にすると、ファイルとそのリビジョンが完全に消去されます。この操作を元に戻すことはできません。

注意

[保存] ボタンを使用して、設定を保持します。設定の保存に加えて完全削除を直ちに開始するには、**[ここをクリックしてください]** オプションを使用します。そうでない場合は、通常のスキャンが 60 分ごとに実行されます。

ユーザー期限切れポリシー

招待状とユーザーアカウントは、長時間操作されなくなると期限切れになるように設定できます。

User Expiration Policies

Users who expire will lose access to all their data. You can reassign the data from the Manage Deleted Users page.

☐ External user sharing invitations and password reset requests expire after days

☐ Expire pending invitations after days

Send email notification about expiration days before the invite is due to expire

☐ Delete external users who have not logged in for days

Send email notification about expiration days before the user is due to expire

☐ Remove sync and share access for LDAP users who have not logged in for days

Send email notification about expiration days before the user is due to expire

- **外部ユーザーの共有招待メールおよびパスワードリセットのリクエストは、X日後に期限切れになります:** 有効にした場合、外部ユーザー用の招待メールおよびパスワードリセットのリクエストは設定した日数の経過後に有効期限切れになります。
- **X 日後に保留中の招待メールが有効期限切れになります:** 有効にした場合、設定した日数の経過後に、すべての保留中の招待メールが有効期限切れになります。
 - **招待の有効期限の X 日前に期限切れに関する電子メール通知を送信する:** 有効にされている場合、招待が期限切れになる前に、日数についての通知が送信されます。
- **ログインしていない外部ユーザーはX日で削除されます:** 有効にした場合、設定した日数ログインしない外部ユーザーが削除されます。
 - **ユーザーの有効期限の X 日前に期限切れに関する電子メール通知を送信する:** 有効にされている場合、期限切れになる設定した日数の通知が一時ユーザーに送信されます。
- **ログインしていない LDAP ユーザーの同期および共有サポートを削除するまでの日数: X 日:** 有効にされている場合は、設定された日数ログインしなかった LDAP ユーザーの同期と共有アクセスを削除します。
 - **ユーザーの有効期限の X 日前に期限切れに関する電子メール通知を送信する:** 有効にされている場合、期限切れになる設定した日数の通知がユーザーに送信されます。

期限切れのユーザーアカウントのコンテンツはどうなりますか？

アカウントの有効期限が切れたユーザーは、すべてのコンテンツへのアクセスと所有権を失いますが、コンテンツはシステムに保持されます。

コンテンツを他のユーザーに再割り当てするか、完全に削除する必要があります。

重要

期限切れのユーザーアカウントのコンテンツを完全に削除するまで、そのコンテンツによって消費されるスペースは解放されません。ファイルのページでは、期限切れのユーザーが以前に削除したコンテンツのみが削除されます。

ファイル リポジトリ

この設定により、同期および共有するためにアップロードされるファイルの保存場所が決定されます。デフォルトの構成では、ファイルシステム リポジトリは、Acronis Cyber Files サーバーと同じサーバーにインストールされます。Acronis Cyber Files の Sync & Share ファイルおよび以前のリビジョンを保存するには、ファイルリポジトリを使用します。Acronis Cyber Files の構成ユーティリティは、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ロケーションを設定するために使用します。下に示す [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。これらの設定を表示または変更するには、AcronisAccessConfiguration.exe を実行します。通常は、それはエンドポイント サーバー上の C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility にあります。

File Repository

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Cyber Files Server. The Acronis Cyber Files Configuration utility is used to set the file repository address, port and file store location. The file store repository endpoint setting below must match the settings in the File Repository tab of the Configuration Utility. To view or modify these settings, run AcronisAccessConfiguration.exe, typically located in C:\Program Files (x86)\Acronis\Configuration Utility\ on the endpoint server. For more information, consult the [documentation](#).

File Store Type:

File Store Repository Endpoint:

Encryption Level:

File Store Low Disk Space Warning Threshold: GB

File Store Status: Free space for file store http://127.0.0.1:5787 = 77.7 GB (83441704960.0 bytes)

Please go to **Server Settings** to configure admin notifications.

- **ファイル ストア タイプ:** 仮想ファイルシステムのリポジトリで使用するストレージのロケーションを選択します。オプションは [ファイルシステム]、[Acronis Storage]、[Microsoft Azure Storage]、[Amazon S3]、[Swift S3]、[Ceph S3]、および [S3 と互換性のある他のストレージ] です。

注意

[S3 と互換性のある他のストレージ] オプションでこのリストに記載されていない S3 ストレージプロバイダを使用できます。しかし、すべての機能の正常な動作は保証されていません。

注意

MinIO S3 ストレージタイプがサポートされており、**[S3 と互換性のある他のストレージ]** オプションとして設定できますが、セキュリティで保護されていない HTTP 接続経由ではサポートされません。

注意

複数のユーザーが同じファイルをアップロードした場合は、消費されるストレージの合計がこれらのユーザーの数 x ファイルサイズと一致します。つまり、使用されるスペースはユーザーとアップロードの数に比例します。消費されるストレージは、すべての参加ユーザーによってアップロードされたすべてのファイルの合計ボリュームに相当します。ただし、占有されるストレージの量は、使用されるバックエンドストレージのタイプとそれらが同じファイルをアップロードするという事実に依存しません。

- **ファイルストアリポジトリエンドポイント:** ファイルシステム リポジトリのエンドポイントの URL アドレスを設定します。
- **暗号化レベル:** 仮想ファイルシステムのリポジトリに格納されるファイルを暗号化する際に使用する暗号化のタイプを指定します。オプションは、[なし]、[AES-128]、[AES-256] です。デフォルトは [AES-256] です。
- **ファイルストア空き容量警告しきい値:** 空き容量がこのしきい値を下回ると、管理者はディスク領域不足の通知を受信します。

Acronis Cyber Files クライアント

以下はデスクトップクライアントの設定です。

Force Legacy Polling Mode	☐
Minimum Client Update Interval	60
Client Notification Rate Limit	250
Show Client Download Link	☒
Minimum Client Version	7.0
Prevent Clients from Connecting	☐
Allow Client Auto-update to Version	Latest

- **レガシー ポーリング モードを強制:** サーバーによって非同期に通知されるのではなく、強制的にクライアントがサーバーをポーリングするようにします。このオプションは、アクロニス サポートによって指示された場合にのみ有効にしてください。
 - **クライアント ポーリング タイム:** クライアントがサーバーをポーリングする時間の間隔を設定します。このオプションは、[レガシー ポーリング モードを強制] が有効な場合のみ使用できます。
- **最小クライアント アップデート間隔:** アップデートされたコンテンツを使用できることをクライアントに再通知するまでにサーバーが待機する最小時間を設定します（秒単位）。
- **クライアント通知の頻度制限:** サーバーが 1 分ごとに送信するクライアント アップデート通知の最大数を設定します。
- **クライアント ダウンロード リンクを表示:** 有効にされている場合、ウェブ ユーザーにはデスクトップクライアントがダウンロードできるリンクが表示されます。
- **最小クライアント バージョン:** サーバーに接続できる最小クライアント バージョンを設定します。

注意

Acronis Cyber Files サーバー バージョン 7.5 以降では、バージョン 6.1 以降のデスクトップクライアントのみが接続できます。

- **クライアントが接続できないようにする:** 有効にされている場合、デスクトップクライアントはサーバーに接続できません。一般的に、これは管理を目的とする場合のみ有効にする必要があります。Web インターフェースへの接続は妨げられません。

- **クライアントの自動バージョン アップデートを許可:** 自動バージョンアップデートチェックを使用して、すべてのデスクトップクライアントに配置されるデスクトップクライアントバージョンを設定します。クライアントの自動アップデートを禁止するには、**[アップデートを許可しない]** を選択します。

ユーザーとデバイス

デバイスの管理

Acronis Cyber Files ユーザーが Acronis Cyber Files Web サーバーに接続すると、そのデバイスが **[デバイス]** リストに表示されます。

ここでは、使用されているすべてのデバイスに関する詳細なステータス情報を表示できます。Acronis Cyber Files アプリをワイプしたり、そのパスワードを変更したりすることもできます。

- **ユーザー名:** LDAP ユーザーの Active Directory (AD) 表示名または一時的なユーザーが選択した名前。
- **デバイス名:** ユーザーが設定したデバイス名。
- **モデル:** ユーザーのモバイルデバイスの製品名。
- **OS:** モバイルまたはデスクトップオペレーティングシステムのタイプとバージョン。
- **バージョン:** 使用されている Acronis Cyber Files アプリまたはデスクトップクライアントのバージョン。
- **ステータス:** Acronis Cyber Files アプリのステータス。以下の値を取ります。
 - 管理
 - 管理、リモートワイプの保留中
 - 非管理、リモートワイプが正常に実行されました
 - 非管理、保留中のリモートワイプ
 - ユーザーによって管理されていません
 - ユーザーが正しくないパスワードを入力した後にワイプされました

デスクトップクライアントの場合は、単一のステータスが Sync & Share です。

- **最後の接続:** 管理サーバーと Acronis Cyber Files アプリ/デスクトップクライアント間の最後の接続の日付と時刻。
- **ポリシー:** ユーザーに適用される管理ポリシーの名前とリンク。
- **操作**
 - **詳細情報:** デバイスや編集可能なデバイスの **[説明]** フィールドに関する追加の詳細情報が表示されます。
 - **アプリのパスワードのリセット** (モバイルデバイス専用) : 選択されたデバイス上の Acronis Cyber Files アプリロックパスワードをリセットします。これを行うには、ユーザーのデバイス画面に表示されるパスワード リセット コードを使用して確認コードを生成する必要があります。
 - **リモートワイプ** (モバイルデバイス専用) : 選択された場合は、デバイスが管理サーバーに接続されたときに、Acronis Cyber Files アプリ内のすべてのファイルとその個別の設定が削除されます。他のアプリや OS のデータには影響を与えません。
 - **リストから削除する:** **[デバイス]** リストからデスクトップクライアントを削除します。モバイルデバイスの場合は、リストから選択されたデバイスが削除され、ワイプせずに管理対象から外されます。これは、Acronis Cyber Files 管理サーバーに再度接続することはないと思われるデバイスを削除するために実行するのが一般的です。 **[モバイルクライアントを新しいデバイスに復元した場合**

でも、PIN コードなしで自動登録されるようにする] を有効にした場合は、このような新しいデバイスがサーバーに接続すると自動的に管理対象として表示されます。

デバイスに関するデータのエクスポート

このリスト内のデバイスに関するデータは txt、csv、または xml ファイルにエクスポートできます。

これを行うには、[エクスポート] ボタンをクリックして、必要なファイル形式を選択します。

エクスポートされるデータの構成要素:

1. ユーザー名
2. 使用されているモバイルデバイスまたはコンピューターの名前
3. モバイルデバイスのモデル
4. デバイスの OS のタイプとバージョン
5. Acronis Cyber Files アプリまたはデスクトップクライアントのバージョン
6. モバイルデバイスまたはデスクトップクライアントのステータス
7. Acronis Cyber Files Web サーバーへの Acronis Cyber Files アプリ登録の日付と時刻
8. Acronis Cyber Files Web サーバーと Acronis Cyber Files アプリまたはデスクトップクライアント間の最後の接続の日付と時刻
9. 適用されたユーザーポリシーの名前
10. メモ

リモート アプリケーション パスワード リセットの実行

アプリの起動時にロックパスワードの入力を要求することによって、Acronis Cyber Files アプリを保護することができます。このパスワードを忘れてしまった場合、Acronis Cyber Files は使用できなくなります。アプリパスワードは、ユーザーの Active Directory アカウントパスワードとは無関係です。

アプリロックパスワードを忘れた場合は、リモートパスワードリセットを実行するか、デバイスから Acronis Cyber Files アプリをアンインストールして、再度インストールするしかありません。アンインストールすると、既存のデータおよび設定はすべて削除されます。これによってセキュリティは確保されますが、ユーザーは新しい管理招待メールが送られるまで Acronis Cyber Files サーバーにアクセスできなくなります。

アプリケーション パスワードのリセット

Acronis デバイス上の Cyber Files ファイルは、Apple Data Protection (ADP) ファイル暗号化を使用して常に保護されています。iTunes および iCloud にバックアップされているデバイス上のファイルと、デバイス レベルのロック コードが有効になっていないデバイス上のファイルの保護を強化として、および一般的なセキュリティ強化機能として、Acronis Cyber Files アプリケーションによって直接適用されるフルタイムのカスタム暗号化の 2 つ目の階層が導入されました。

この暗号化の影響の 1 つとして、Acronis Cyber Files アプリのユーザーは、無線でアプリケーションロックパスワードをリセットすることができません。このことにより、Acronis Cyber Files による設定データベースの暗号化解除、およびユーザーによる新しいアプリパスワードの設定を可能にするため、

ユーザーと Acronis Cyber Files IT 管理者の間でパスワードリセットコードおよび確認コードを交換する必要があります。

iOS または Android 向けの Acronis Cyber Files アプリのパスワードをリセットするには:

1. エンドユーザーが管理者に Acronis Cyber Files アプリのパスワードリセットを依頼し、デバイス画面に表示されている**パスワードリセットコード**を伝えます。
2. **[ユーザーとデバイス]** タブを開きます。
3. **[デバイス]** タブを開きます。
4. アプリパスワードをリセットするデバイスを探して、**[操作]** ボタンをクリックします。
5. **[アプリのパスワードのリセット...]** を押します。
6. **パスワード リセット コード**を入力してから、**[確認の生成]** をクリックします。
7. 表示された**確認コード**を口頭または電子メールでユーザーに伝えます。
8. ユーザーがアプリのパスワード リセット ダイアログにこのコードを入力すると、新しいパスワードを設定するように指示されます。ユーザーが適切なアプリパスワードを設定せずにこの処理を中断した場合は、Acronis Cyber Files アプリへのアクセスを拒否され、アプリパスワードのリセット処理を繰り返す必要があります。

Reset App Password

Enter the password reset code displayed in this device's Acronis Cyber Files app, then click "Generate Confirmation". A confirmation code will be displayed that can be entered into the Acronis Cyber Files app to authorize a password reset.

Password Reset Code:

Generate Confirmation

Close

リモートワイプの実行

Acronis Cyber Files では、モバイルアプリに対してリモートワイプを実行することができます。これによって、ローカルに保存されている、または Acronis Cyber Files アプリ内にキャッシュされているすべてのファイルが削除されます。すべてのアプリ設定がリセットされて以前のデフォルトに戻り、アプリで設定されたすべてのサーバーが削除されます。

これを行うには、次のようにします。

1. Acronis Cyber Files Web インターフェースを開きます。
2. **[ユーザーとデバイス]** タブを開いて、**[デバイス]** に移動します。
3. リモートワイプを実行するデバイスを探して、**[操作]** ボタンを押します。
4. **[リモートワイプ...]** を押します。
5. **[ワイプ]** を押して、リモートワイプを確定します。

6. **[リモートワイプの保留中]** ステータスが、そのデバイスの **[ステータス]** 列に表示されます。

注意

アプリが管理サーバーに接続する前であれば、管理者が保留中のリモートワイプをキャンセルできます。このオプションは、リモートワイプが実行された後に **[操作]** メニューに表示されます。

7. リモートワイプは、デバイスがサーバーに再度接続したときに完了します。このステップは元に戻すことができません。

注意**接続要件**

Acronis Cyber Files クライアントが、プロファイルの更新、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 Cyber Files 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 Cyber Files 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 に接続する必要もあります。

ユーザーの管理

すべての Sync & Share ユーザーを **[ユーザー]** セクションで管理することができます。

[ユーザーの追加] ボタンから新規ユーザーを招待したり、**[操作]** ボタンから現在のユーザーを編集または削除することができます。

ユーザーの編集時に、管理者権限の付与（権限がある場合）、Eメールの変更、パスワードの変更、アカウントの有効/無効の切り替えなどを実行できます。

クォータを有効にしている場合、ユーザーに Sync & Share のアクセス権がある場合のみ、そのユーザーに対してカスタムクォータを設定できます。

ユーザーを削除する際には、ユーザーのコンテンツも管理する必要があります。ユーザーを削除すると、次のいずれかを実行することを求めるメッセージが表示されます。

- ユーザーのコンテンツを別の既存のユーザーに再割り当てして、データが引き続き利用できるようにする。
- コンテンツを完全に削除し、ユーザーアカウントと関連するすべてのファイルをシステムから削除する。

既に削除済みのユーザーの場合、**[ユーザーとデバイス]** セクションにある **[削除済みユーザーコンテンツを再割り当てする]** タブで、残っているコンテンツを管理できるので、後でコンテンツの再割り当てまたは完全削除ができます。詳細については、[ユーザーとそのコンテンツの削除](#)を参照してください。

Sync & Share ユーザーのタイプ

Sync & Share のユーザーアカウントは3つのタイプに分けられます。

外部（アドホック）ユーザーアカウント

このアカウントは、管理者により送信される E メールによる招待、または他のユーザーによる共有コンテンツ（ファイルまたはフォルダ）への招待により手動で作成する必要があります。

外部アカウントには次のようなサブタイプがあります: **無料** と **ライセンス取得済み**。

新規に作成された外部アカウントはデフォルトでは無料です。Acronis Cyber Files 管理者のみ、無料外部アカウントをライセンス取得済み外部アカウントに変換できます。

ライセンス取得済みアカウントを持つユーザーは、自身の Sync & Share 領域のファイルやフォルダを作成、アップロード、編集、削除できます。コンテンツを他のユーザーと共有することもできます。

無料アカウントを持つユーザーには Sync & Share 領域はありません。対応する権限がある場合、無料アカウントのユーザーは、共有されたフォルダ内でのみ、新規ファイルの作成、別の場所からのファイルのアップロード、既存ファイルの編集と削除を行えます。読み取り専用権限がある場合、ファイルの作成、アップロード、編集、削除は行えず、共有フォルダ内のファイルの参照、プレビュー、ダウンロードのみ行えます。

無料アカウントのユーザーは、新規ユーザーを共有リソースに招待することも、リソースを共有している他のユーザーを確認することもできません。ユーザーのアカウントが作成されたときにユーザーにそのような権限が割り当てられた場合でも同様です。

ファイルが無料アカウントのユーザーと共有されている場合、そのユーザーはファイルのプレビューとダウンロードのみ行えます。

無料アカウントのユーザーは、Acronis Cyber Files のデスクトップクライアントもモバイルアプリも使用できません。

注意

新規作成された外部アカウントはすべて手動で有効化する必要があります。ユーザーは、アカウントを有効化する手順を記載した E メールを受信します。

内部（LDAP）ユーザーアカウント

このアカウントは、Active Directory（AD）統合を利用しています。アカウントは外部アカウントとして手動で作成しますが、管理者が **LDAP グループのプロビジョニング** をセットアップして、AD ユーザーが初めて Acronis Cyber Files にログインしたときに自動作成されるようにすることもできます。

内部アカウントは作成時に自動的にライセンス取得済みになります。

内部アカウントを持つユーザーは、自身の Sync & Share 領域または共有フォルダ内のファイルやフォルダの作成、アップロード、編集、削除を行えます。コンテンツを他のユーザーと共有することもできます。

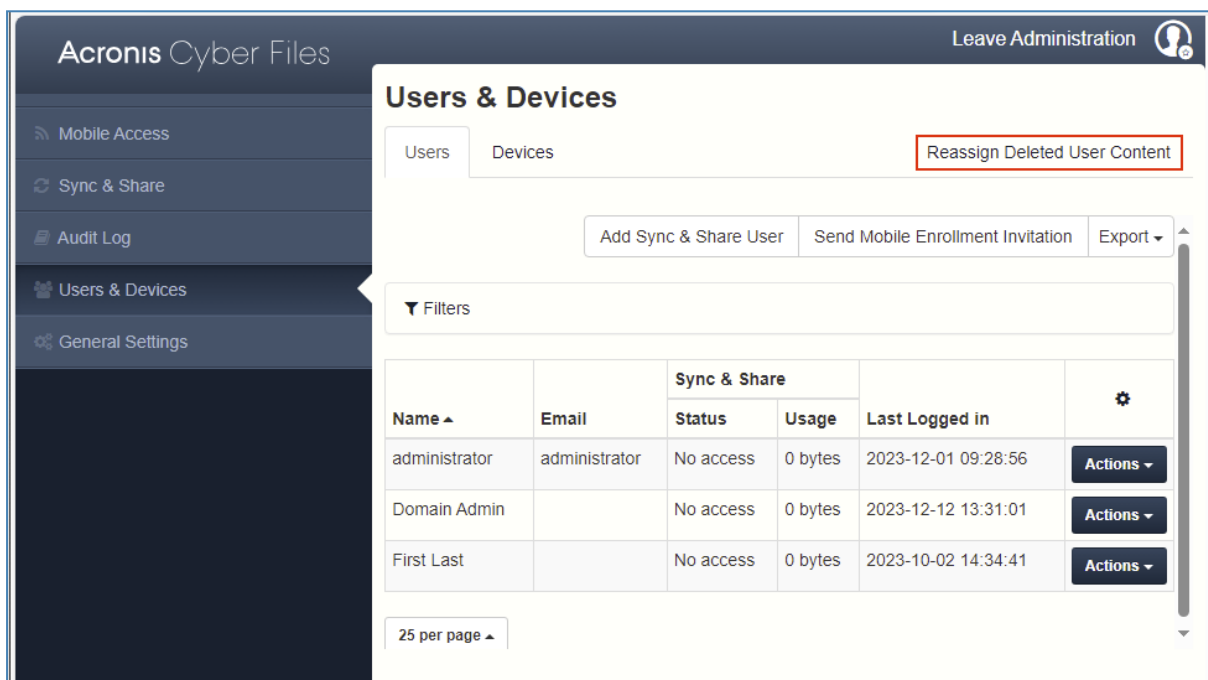
Acronis Cyber Files のデスクトップクライアントとモバイルアプリを使用できます。

アクセス権なしユーザーアカウント

これは Sync & Share へのアクセス権のない管理アカウントです。デフォルトではライセンス取得済みではありません。このアカウントを持つユーザーは、Acronis Cyber Files のデスクトップクライアントとモバイルアプリを使用できません。

注意

Sync & Share へのアクセス権のない管理者は、自身のアカウント用の E メールアドレスを設定する必要はありません。LDAP 資格情報のみでログインできます。このようなアカウントは、Acronis Cyber Files サーバーの SMTP をセットアップせずに作成できます。詳細については、「[管理者と権限](#)」を参照してください。



The screenshot shows the 'Users & Devices' section of the Acronis Cyber Files management console. The 'Users' tab is selected. A red box highlights the 'Reassign Deleted User Content' button. Below the buttons are 'Add Sync & Share User', 'Send Mobile Enrollment Invitation', and an 'Export' dropdown. A 'Filters' section is present above a table of users. The table has columns for Name, Email, Sync & Share Status, Usage, Last Logged in, and an Actions column. The table lists three users: administrator, Domain Admin, and First Last, all with 'No access' status and '0 bytes' usage. A '25 per page' selector is at the bottom left of the table.

Name ▲	Email	Sync & Share		Last Logged in	⚙️
		Status	Usage		
administrator	administrator	No access	0 bytes	2023-12-01 09:28:56	Actions ▼
Domain Admin		No access	0 bytes	2023-12-12 13:31:01	Actions ▼
First Last		No access	0 bytes	2023-10-02 14:34:41	Actions ▼

[ユーザー] タブで、以下の情報を表示できます。

- **名前:** ユーザー名 (LDAP ユーザーの Active Directory (AD) 表示名、またはアドホックユーザーが選択した名前) が表示されます。
- **ユーザー名 (オプション):** LDAP ユーザーのログオン名が表示されます。
- **UPN (オプション):** LDAP ユーザーのユニバーサルプリンシパル名が表示されます。
- **ドメイン (オプション):** LDAP ユーザーのドメインが表示されます。
- **E メール:** ユーザーの E メールアドレスが表示されます。
- **Sync & Share**
 - **ステータス:** 使用されているライセンスの種類を示します。
 - **使用量:** ユーザーのコンテンツの合計サイズが表示されます。
- **最後のログイン:** 最後のログインの時刻と日付が表示されます。
- **操作**

- **詳細情報:** ユーザーに関する詳細な情報が表示されます。
- **利用デバイスを表示:** このユーザーが使用しているデバイスに関する情報が表示されます。
- **Sync & Share のパスワードをリセット:** パスワードリセットの E メールを送信します。
- **ライセンス取得済みに変更:** 無料ユーザーをライセンス取得済みユーザーに変更します。
- **ユーザーの編集:** ユーザーに対する E メールの変更、アカウントの無効化/有効化、管理権限のすべてまたは一部の付与、アカウントのカスタムクォータの設定を行えます。外部ユーザーの場合、2FA に使用される携帯電話番号を変更することができます。
- **削除:** ユーザーを削除します。
- **削除済みユーザーコンテンツを再割り当てする:** システムから削除されたユーザーのコンテンツを管理者が管理できるようにします。この機能を使用すると、ユーザーのデータは直ちに削除されず、管理者は、コンテンツを別のユーザーに転送するか、後で完全に削除することができます。

ユーザーに関するデータのエクスポート

すべての登録ユーザーに関するデータを、txt、csv、または xml 形式のファイルにエクスポートできます。

これを行うには、[**エクスポート**] ボタンをクリックして、必要なファイル形式を選択します。

エクスポートされるデータの構成要素:

1. ユーザーの名前
2. ユーザーのログオン名 (LDAP ユーザーの場合)
3. ユニバーサルプリンシパル名 (LDAP ユーザーの場合)
4. LDAP ドメイン (LDAP ユーザーの場合)
5. 電子メール
6. ポリシー名
7. 保留ステータス
8. 管理者権限
9. ライセンス取得済みユーザーのステータス
10. 無効化ユーザーのステータス
11. LDAP 認証
12. ユーザーが所有するフォルダ数
13. ユーザーが所有するファイル数
14. ユーザーのコンテンツのサイズ (バイト単位)
15. ユーザーのクォータのサイズ (バイト単位)
16. 最後のログインの日付と時刻

外部 (アドホック) ユーザーの追加

外部 (アドホック) ユーザーを追加するには、次の操作を行います。

1. Acronis Cyber Files Web インターフェースを開きます。
2. 管理者アカウントでログインします。**ユーザー管理**権限があるアカウントのユーザーも同様の操作が実行できます。
3. **[ユーザーとデバイス]** タブを開きます。
4. **[ユーザー]** タブを開きます。
5. **[Sync & Share ユーザーの追加]** ボタンを押します。
6. ユーザーのEメールを入力します。
7. 招待メールの言語を選択します。
8. **[追加]** ボタンを押します。

ユーザーにリンクが記載された E メールが送信されます。リンクにアクセスすると、パスワードを設定するよう求められます。その後、ユーザーはアカウントの確認を行うための E メールを受信します。E メールに記載されたリンクを開くと、アカウントの登録が完了します。

内部 (LDAP) ユーザーの追加

内部 (LDAP) ユーザーを追加するには、次の操作を行います。

1. Acronis Cyber Files Web インターフェースを開きます。
2. 管理者アカウントでログインします。**ユーザー管理**権限があるアカウントのユーザーも同様の操作が実行できます。
3. **[ユーザーとデバイス]** タブを開きます。
4. **[ユーザー]** タブを開きます。
5. **[Sync & Share ユーザーの追加]** ボタンを押します。
6. ユーザーのEメールを入力します。
7. 招待メールの言語を選択します。
8. **[追加]** ボタンを押します。

ユーザーが LDAP 資格情報を使用してログインできるようになりました。ユーザーがログインすると、アカウントの登録が完了します。

注意

LDAP が有効にされており、LDAP 管理者グループがプロビジョニングされている場合は、その LDAP グループのユーザーは、LDAP 資格情報で直接ログインでき、完全な管理者権限が付与されます。

カスタムクォータを設定するには、次の手順を実行します。

Sync & Share アクセス権のあるユーザーにカスタムクォータを設定できます。

これを行うには、次の操作を行います。

1. ウェブインターフェイスで、**[ユーザーとデバイス]** タブを開きます。
2. 対象となるユーザーを見つけ、**[操作]** ボタンをクリックします。
3. **[ユーザーの編集]** を選択し、**[カスタムクォータを使用]** を有効にします。
4. 目的のクォータサイズを入力し、**[保存]** を押します。

注意

[カスタムクォータを使用] チェックボックスは、グローバルオプションの [クォータを有効にしますか?] が事前に有効になっている場合のみ使用できます。

ユーザーとそのコンテンツの削除

Acronis Cyber Files からユーザーを削除できますが、ユーザーのアカウントに関連付けられたコンテンツがあるかどうかによって、処理方法が異なります。

コンテンツを持たないユーザーを削除すると、アカウントが完全に削除されます。

コンテンツを含むユーザー（**期限切れのユーザー**を含む）を削除する場合、そのコンテンツをどうするかを選択する必要があります。

Delete User?

Are you sure you want to delete hristo <hristo@test.biz>?
[User owns 1 Folder / 10 Files / 4.90 MB]

This user's content can be reassigned to an existing user or deleted immediately. If you choose not to reassign or delete content now, you can reassign or delete it at a later time from the Reassign Deleted User Content page.

What would you like to do with this user's content?

☒ Save and reassign later

☐ Reassign to another user

☐ Permanently delete

Delete

Cancel

- **保存してから再割り当て** – ユーザーのコンテンツは一時的にシステムに残され、[削除済みユーザーコンテンツを再割り当てする] タブで管理できます。このようなコンテンツは、再割り当てしたり、完全に削除したりできます。

注意

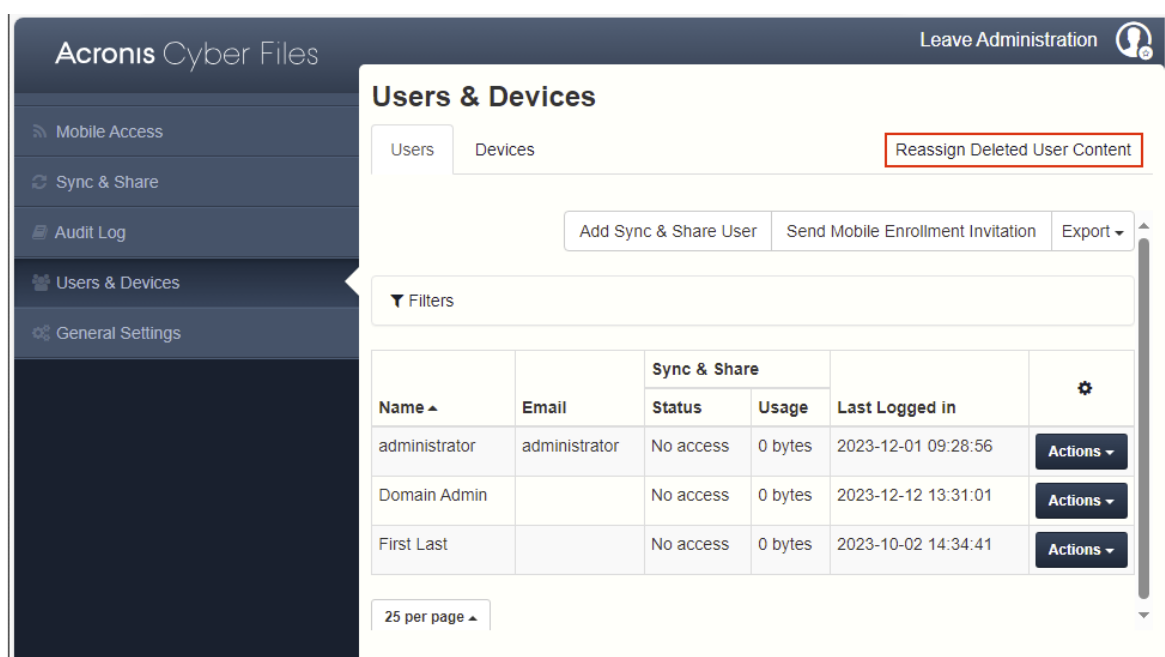
このコンテンツには引き続き、アクティブなユーザーのコンテンツと同じように消去ポリシーが適用されます。

- **別のユーザーに再割り当て** – コンテンツはすぐに選択したユーザーに再割り当てされ、「**Content inherited from DeletedUserName <deletedusersemail>**」という新しいフォルダが、そのユーザーの Sync & Shareスペースに作成されます。選択されたユーザーは、削除されたユーザーによって共有されていたフォルダを含む、継承されたコンテンツの所有者となります。
- **完全に削除** – ユーザーアカウントとコンテンツをすぐに削除します。

ユーザーとそのコンテンツの完全な削除

ユーザーとそのコンテンツを完全に削除するには

1. Acronis Cyber Files コンソールで、左側のメインメニューから **[ユーザーとデバイス]** セクションに移動します。



2. **[ユーザー]** タブで、削除するユーザーを見つけます。
検索バーまたはフィルタを使用して、ユーザーの一覧を絞り込むことができます。
3. ユーザー名の横にある **[操作]** ボタンをクリックします。
4. ドロップダウンメニューから**[ユーザーを削除]**を選択します。
確認ウィンドウが表示され、ユーザーの内容で実行する処理の決定を求めるメッセージが表示されます。

Delete User?

×

Are you sure you want to delete hristo <hristo@test.biz>?
[User owns 1 Folder / 10 Files / 4.90 MB]

This user's content can be reassigned to an existing user or deleted immediately. If you choose not to reassign or delete content now, you can reassign or delete it at a later time from the Reassign Deleted User Content page.

What would you like to do with this user's content?

☒ Save and reassign later

☐ Reassign to another user

☐ Permanently delete

Delete

Cancel

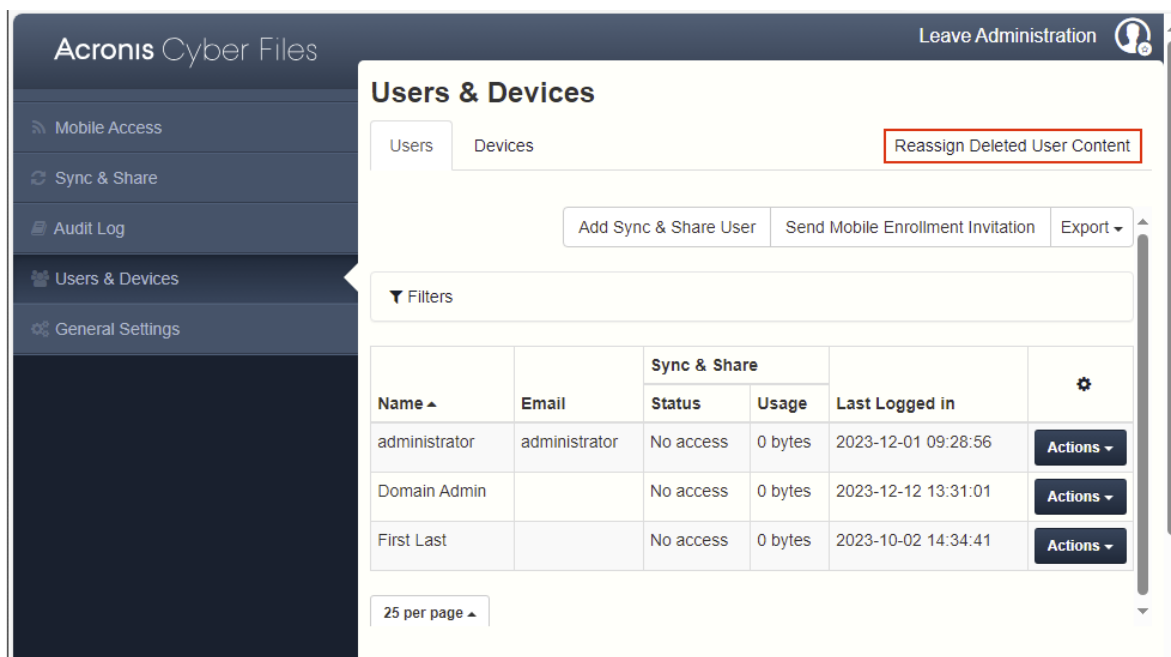
5. **完全に削除する**を選択します。

ユーザーのアカウントとコンテンツを直ちに削除します。

削除されたユーザーのコンテンツの他のユーザーへの再割り当て

削除したユーザーのコンテンツを他のユーザーに再割り当てするには

- Acronis Cyber Files コンソールで、左側のメインメニューから **ユーザーとデバイス** セクションに移動します。
- ページの上にある **削除済みユーザーコンテンツを再割り当てする** タブをクリックします。



再割り当て可能なユーザーの一覧が表示されます。

3. コンテンツを再割り当てするユーザーを選択します。

確認ウィンドウが表示され、削除したユーザーが所有していたすべてのコンテンツを再割り当てするように求められます。

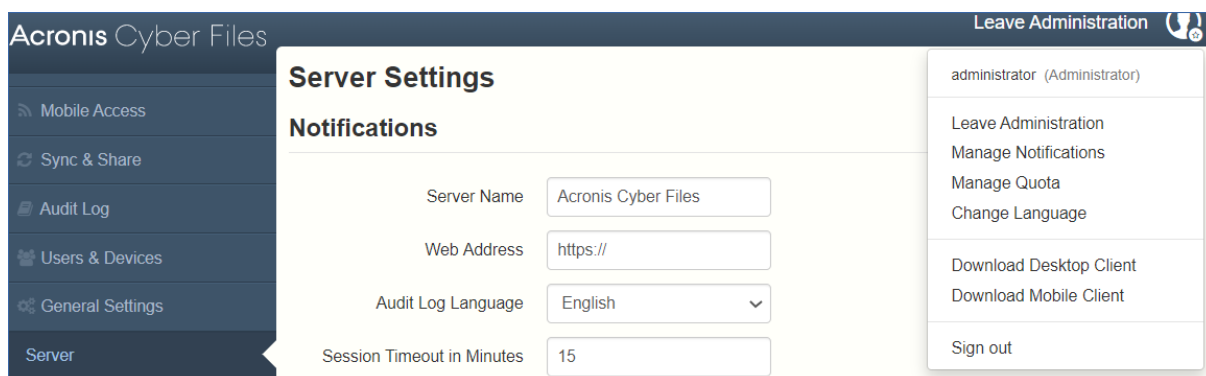
4. ドロップダウンメニューから、コンテンツを割り当てるユーザーを選択します。
5. **[再割り当て]** をクリックして再割り当てを確定します。
6. 再割り当てされたコンテンツを確認します。新しい所有者の領域に、Content inherited from DeletedUserName <deletedusersemail>

サーバーの管理

サーバーの管理

管理者の場合、Web インターフェースにログインすると、**管理モード**と**ユーザーモード**を切り替えることができます。

- **管理モード**に入るには、ユーザーアイコンをクリックして、**[管理コンソール]**を押します。
- **ユーザーモード**に入るには、右上にある**[管理画面を閉じる]** ボタンを押します。



注意

管理者は、API ドキュメントにアクセスできます。管理モードが有効になっている場合、Web インターフェースのフッターにそのリンクが表示されます。

管理者と権限

管理ページのアクセス制限

- **構成済みの IP アドレス範囲からの接続のみに管理ページへのアクセスを許可する:** 管理者が特定の IP アドレスのみに管理 Web インターフェースへのアクセスを許可できるようになります。
 - **管理ページへのアクセスを許可するIPアドレス:** 管理ページにアクセスできるIPアドレスを管理者が入力します。カンマ区切りの IP、サブネット、または IP 範囲を使用できます（例: 10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99）。

注意

localhost からの管理者アクセスを制限することはできません。

注意

この機能は、ゲートウェイサーバーを使用して Acronis Cyber Files サーバーへの要求をプロキシしているサーバーでは機能しません。

プロビジョニング済み LDAP 管理者グループ

Provisioned LDAP Administrator Groups						Add Provisioned Group
Members of groups listed here will have their user accounts automatically created at first login and will be given administrative access for as long as they are a member of a provisioned administrator group.						
LDAP Group	Full Rights	Manage Users	Manage Mobile Data Sources	Manage Mobile Policies	View Audit Log	
CN=Administrators,CN=Builtin,DC=gililabs,DC=com	✓	✓	✓	✓	✓	Actions ▾
CN=SecurityGroup,CN=Users,DC=gililabs,DC=com		✓		✓	✓	Actions ▾
25 per page ▾						Showing 1 to 2 of 2 groups
◀ ◁ 1 ▷ ▶ ▶▶						

このセクションでは、管理グループを管理することができます。これらのグループ内のユーザーは、グループの管理者権限を自動的に受け取ります。すべての権限は表に表示され、現在有効な権限には緑のマークが付けられます。

[操作] ボタンを使って、グループの削除または編集ができます。グループの権利権限を編集できます。

プロビジョニング済みの LDAP 管理者グループを追加するには

Add Provisioned LDAP Administrator Group

Selected group: CN=Administrators,CN=Builtin,DC=gililabs,DC=com

Administrative Rights

- ☒ Full administrative rights?
- ☒ Can manage users?
- ☒ Can manage mobile data sources?
- ☒ Can manage mobile policies?
- ☒ Can view audit log?

Search for an LDAP group and click on the Common Name to select it as a Provisioned Administrators LDAP Group.

Find group that begins with ▼ Administrators Search

Add Cancel

1. [プロビジョニング済みグループの追加] をクリックします。
2. グループにSync & Shareの機能を付与する場合はチェックします。
3. グループ ユーザーに付与するすべての管理者権限をチェックします。
4. グループを検索します。
5. グループ名をクリックします。
6. [保存] をクリックします。

管理ユーザー

このセクションでは、管理者権限を持つすべてのユーザー、認証タイプ（アドホックまたはLDAP）、Sync & Shareの権限の有無、およびその状態（無効または有効）を一覧表示します。

[管理者の追加] ボタンを使って、完全な権限または部分的な権限を持つ新しいユーザーを招待できます。[操作] ボタンを使って、ユーザーの削除または編集ができます。管理者権限、状態、またはパスワードを編集できます。

1 人の管理者を招待する

1. AcronisCyber Files Web インターフェースを開きます。
2. 管理者アカウントでログインします。
3. [全般設定] タブを展開して、[管理者] ページを開きます。
4. [管理ユーザー] で [管理者の追加] ボタンをクリックします。
5. どのタイプのユーザーを招待するのかと、招待するユーザーに何を管理させるのかに応じて、
[Active Directory/LDAP] タブまたは [Eメールによる招待] タブを選択します。
 - a. **Active Directory/LDAP を通じて招待する場合は、次のことを実行します。**
 1. Active Directory に追加するユーザーを検索し、ユーザーの [共通名] をクリックして選択します。

注意

[LDAP ユーザー] フィールドと [Eメール] フィールドは自動的に入力されます。

2. Sync & Share を有効/無効にする機能です。
3. ユーザーに持たせる管理者権限を選択します。
4. [追加] をクリックします。
- b. **Eメールを通じて招待する場合は、次のことを実行します。**
 1. 管理者として追加するユーザーのEメールアドレスを入力します。

注意

Eメールで招待されるアドホック ユーザーには、常に Sync & Share の機能が与えられます。

2. このユーザーにライセンスを供与するかどうかを選択します。
3. ユーザーに持たせる管理者権限を選択します。
4. 招待Eメールの言語を選択します。
5. [追加] をクリックします。

管理者権限

Administrative Rights

- ☐ Full administrative rights?
- ☐ Can manage users?
- ☐ Can manage mobile data sources?
- ☐ Can manage mobile policies?
- ☐ Can view audit log?

- **完全な管理者権限:** ユーザーに完全な管理権限を付与します。
- **ユーザーを管理する:** ユーザーを管理する権限をユーザーに付与します。これには、新しいユーザーの招待、LDAP グループのプロビジョニング、Acronis Cyber Files 登録招待の送信、および接続されているモバイルデバイスの管理が含まれます。
- **モバイル データ ソースを管理する:** モバイル データ ソースを管理する権限をユーザーに付与します。これには、新しいゲートウェイ サーバーとデータ ソースの追加、割り当て済みソース、クライアントで表示可能なゲートウェイ、およびレガシー データ ソースの管理が含まれます。
- **モバイル ポリシーを管理する:** モバイル ポリシーを管理する権限をユーザーに付与します。これには、ユーザーとグループのポリシー、許可されたアプリケーション、およびデフォルトのアクセス制限の管理が含まれます。
- **監査ログを表示する:** 監査ログを表示する権限をユーザーに付与します。

注意

プロビジョニング済み LDAP 管理者グループと、プロビジョニング済みの Sync & Share の LDAP グループの両方に属する新しいユーザーには、許可がまとめて付与されるようになりました。

ユーザーに管理者権限を付与するには:

1. [同期と共有] タブを開きます。
2. [ユーザー] タブを開きます。
3. 編集するユーザーの [操作] ボタンをクリックします。
4. [編集] をクリックします。
5. ユーザーに付与するすべての管理者権限をチェックします。
6. [保存] をクリックします。

管理者の固有の権限を付与するには:

1. 編集するユーザーの [操作] ボタンをクリックします。
2. [編集] をクリックします。
3. ユーザーに付与するすべての管理者権限をチェックします。
4. [保存] をクリックします。

監査ログ

ログ

ここでは、ログエントリを生成した最近のイベントの詳細を確認できます（消去ポリシーにより、時間制限が異なることがあります）。

注意

ゲートウェイ サーバーのログとログのレベルを設定する方法については、「[ゲートウェイサーバーのログ](#)」を参照してください。

ログリスト

Timestamp	Type	User	Message	Device Name	Device IP	Gateway Server	Gateway Server Path
2022-07-14 15:57:04	Info		File '...' xlsx' downloaded	iPhone7		Local	https://cyberfile.higland.com/contents/...
2022-07-14 15:56:25	Info		File '...' docx' was previewed in a Web browser.				
2022-07-14 15:56:17	Info		File '...' docx' was previewed in a Web browser.				
2022-07-14 15:56:00	Info		Downloaded file '...' docx'.				
2022-07-14 15:56:00	Info		File '...' docx' downloaded	iPhone7		Local	https://cyberfile.higland.com/contents/...
2022-07-14 15:55:54	Info		Updated file '...' docx'.				
2022-07-14 15:55:53	Info		logged in	iPhone7		Local	
2022-07-14 15:55:45	Info		Updated file '...' docx'.				
2022-07-14 15:54:28	Info		Updated file '...' docx'.				
2022-07-14 15:49:29	Warning		Free space for file store http://... is low: 9.6 GB (10334695424 bytes) remaining				
2022-07-14 15:44:02	Info		logged in	iPhone7		Local	

- **タイムスタンプ**: イベントの日時を示します。
- **タイプ**: イベントの重大度を示します。
- **ユーザー**: イベントの責任を負うユーザー アカウントを示します。
- **メッセージ**: 発生したことにに関する情報を示します。

ゲートウェイ サーバーで監査ログを有効にした場合、モバイル クライアントのアクティビティも表示されます。デスクトップクライアントやウェブ クライアントからモバイル データ ソースにアクセスできるようにした場合、これらの設定はログにも反映されます。

- **デバイス名** – 接続されているデバイスの名前。
- **デバイス IP** – 接続されているデバイスの IP アドレスを表示します。
- **ゲートウェイ サーバー** – デバイスが接続されているゲートウェイ サーバーの名前を表示します。
- **ゲートウェイ サーバーのパス** – ゲートウェイ サーバー上のデータ ソースへのパスを表示します。

ログリストのフィルタ

ログテーブルに表示されるログエントリをフィルタできます。ページの上にある  アイコンをクリックして、フィルタ設定パネルを開閉します。

▼ Filters

Filter by User:	All ▼	From:	📅
Filter by Shared Projects:	All ▼	To:	📅
Filter by Severity:	All ▼	Search for Text:	
Filter by Gateway Server:	All ▼	Filter by Device Name:	All ▼
Filter by Device IP:	All ▼		

- **ユーザーでフィルタを適用する** - [すべて] または [ユーザーなし] を選択するか、使用可能ないずれかのユーザーを選択できます。
- **共有プロジェクトでフィルタを適用する** - [すべて] または [共有なし] を選択するか、使用可能ないずれかの共有プロジェクトを選択できます。
- **重要度でフィルタを適用する** - [すべて]、[情報]、[警告]、[エラー]、[Fatal] というタイプがあります。
- **ゲートウェイサーバーでフィルタを適用する**: [すべて]、[サーバーなし] を選択するか、いずれかのゲートウェイサーバーを選択できます。
- **デバイス IP でフィルタを適用する**: [すべて]、[デバイス IP なし] を選択するか、ログエントリを生成したデバイス IP のいずれかを選択できます。
- **日時**: 日時でフィルタします。
- **テキストを検索**: ログ メッセージの内容でフィルタします。
- **デバイス名でフィルタを適用する**: [すべて]、[デバイス名なし] を選択するか、ログエントリを生成したデバイス名のいずれかを選択できます。

設定

Acronis Cyber Files Leave Administration

Mobile Access
Sync & Share
Audit Log
Log
Settings
Users & Devices
General Settings

Audit Log Settings

Acronis Cyber Files can automatically purge old logs and export them to files based on the policies below. It is recommended to export the log files to a folder outside the Acronis Cyber Files server directories so they will not be lost when the software is upgraded. The export file path must be a folder where the Acronis Cyber Files Tomcat Service user has read and write permissions.

☐ Automatically purge log entries more than old

☐ Export log entries to file as before purging

Export file path

Show timestamps in exported audit logs using:

Acronis Cyber Files では、特定のポリシーに基づき、古いログを自動的に完全削除したりファイルにエクスポートしたりすることができます。

- **XY 経過したログエントリを自動的に消去する**: 有効にした場合、指定した日数、週数、または月数を経過したログが自動的に完全削除されます。

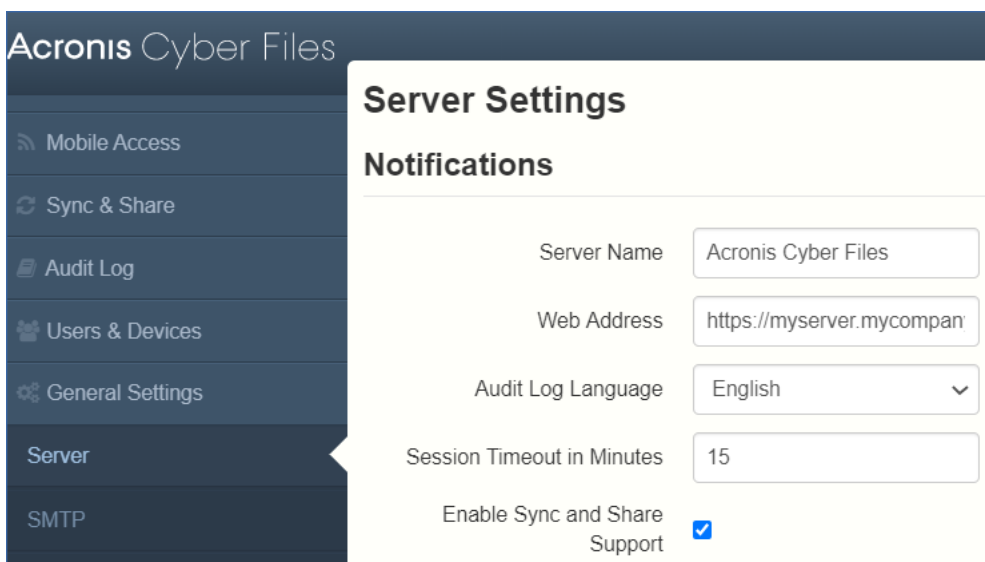
- **消去する前に X のファイル形式でログ エントリをエクスポートす**: 有効にした場合、ログが消去される前に CSV、TXT、または XML のいずれかの形式でコピーがエクスポートされます。エクスポートはサーバーのローカルタイムで 03:00 に自動的に設定されます。この設定は変更できません。
- **ファイル パスをエクスポートする**: ログのエクスポート先を設定します。

重要

アップグレード時にログが失われないように、Acronis Cyber Files のインストールフォルダ以外のフォルダにログをエクスポートすることをお勧めします。指定するフォルダには、Acronis Cyber Files Tomcat サービスを実行するユーザーアカウントの読み取り/書き込みのアクセス権が必要です。デフォルト設定を変更していない場合、アカウントはローカルシステムアカウントになります。

- **エクスポート済みの監査ログのタイムスタンプを表示する (Xを使用)**: 監査ログでサーバーのローカル時間形式を使用するか別の時間形式 (UTC) を使用するかを選択できます。

サーバー



サーバーの設定

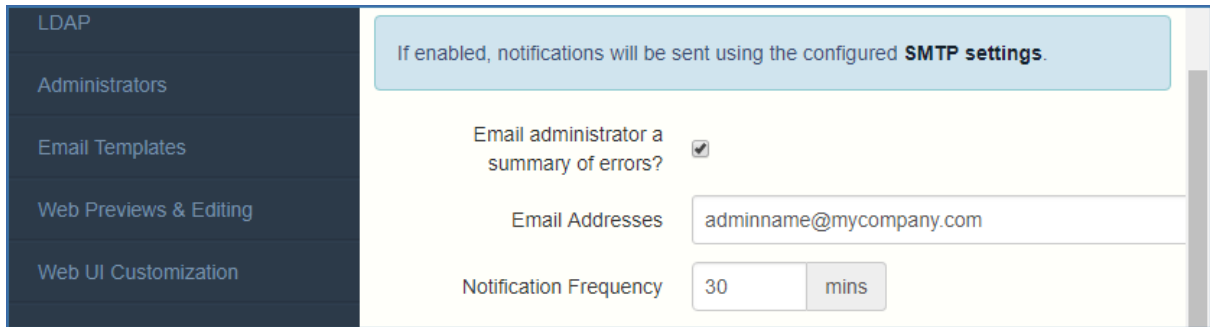
- **サーバー名**: ウェブサイトのタイトルとして使用され、管理者への通知メールでこのサーバーを識別するためにも使用される、表示用のサーバー名。
- **ウェブ アドレス**: ユーザーが (http:// または https:// で始まる) ウェブサイトにアクセスできる DNS 名または IP アドレスを指定します。ここでは「localhost」を使用しないでください。このアドレスは、電子メール招待リンクでも使用されます。
- **監査ログの言語**: 監査ログのデフォルト言語を選択します。現在のオプションは、[英語]、[ドイツ語]、[フランス語]、[日本語]、[イタリア語]、[スペイン語]、[チェコ語]、[ロシア語]、[ポーランド語]、[韓国語]、[中国語 (繁体字)]、[中国語 (簡体字)] です。デフォルト値は [英語] です。
- **セッションタイムアウト (分)**: 非アクティブユーザーがログアウトされるまでの時間の長さを設定します。選択された期間内にアクションが実行されなかった場合は、アクションを実行するかログア

ウトを行うよう促す時限ダイアログが表示されます。

注意

ユーザーがセッションタイムアウトより長い時間がかかるアップロードまたはダウンロードを開始した場合は、アップロードが終了するまでログイン状態が維持されます。

- **同期・共有のサポートを有効にする:** このチェックボックスで同期・共有の機能を有効または無効にします。



通知の設定

- **エラーの概要を管理者に電子メールで送信しますか?:** 有効にされている場合は、指定された電子メール アドレスにエラーの概要が送信されます。
 - **電子メールアドレス:** エラーの概要を受信する 1 つ以上の電子メール アドレス。
 - **通知頻度:** エラーの概要を送信する頻度。エラーがある場合にのみ電子メールが送信されます。

SMSの2要素認証

WebクライアントログインでSMSによる2要素認証のオプションが組み込まれました。AD携帯電話番号またはユーザー指定の電話番号を使用することができます。2要素認証を要求するのは、毎回のログイン時、指定した期間の経過後、または新しいブラウザからのログイン時のみにすることができます。

SMSコードの送信には、Twilio SMSメッセージングサービスでアカウントを確立しておく必要があります。詳細については、<https://www.twilio.com/sms>を参照してください。Twilioの試用版の実行方法については、[Twilio無料試用](#)を参照してください。

注意

Twilio では 1 つのアカウントしか必要ありません。そのアカウントが Acronis Cyber Files サーバーで使用されるため、すべてのユーザーのアカウントを用意する必要がありません。

SMS 2-factor authentication

☒ Require web client SMS 2-factor authentication For initial login to new browsers ▾

☒ Require for Internal / LDAP users

Source of mobile phone number Active Directory ▾

Fallback behavior if mobile phone number does not exist in Active Directory:

☐ Use Acronis Cyber Files account - Prompt user to enter a mobile phone number

☒ Allow login without 2-factor authentication

☐ Do not allow login

☒ Require for External users

Email mobile phone number recovery requests to

Twilio service settings for SMS messaging

In order to send 2-factor codes to users, you will need to establish a Twilio SMS messaging account and configure a messaging service that can be used by Acronis Cyber Files. [View more details](#)

Twilio Account SID

Twilio Auth Token

Twilio Messaging Service SID

注意

[内部ユーザー/LDAP ユーザーに要求] または [外部ユーザーに要求] の少なくとも一方のオプションを必ず選択してください。

ウェブクライアントにSMS 2要素認証を要求する:

- **新しいブラウザへの初期ログインの場合:** 新しいユーザーが Acronis Cyber Files サーバーのウェブページを初めて開くときに SMS 認証を要求します。確認コードを入力してブラウザを登録すると、別のブラウザまたはコンピューターを使用しない限り、再度 SMS コードの入力を要求されることはありません。
- **指定した間隔で:** ログイン試行の回数に関係なく、指定した時間間隔でSMS認証を要求します。
- **毎回のログインで:** ユーザーが接続を試行するたびに SMS 認証を要求します。

Twilioの設定:

- **Twilioアカウントの SID:** 会社の Twilio アカウントセキュリティ識別子 (SID)。
- **Twilio認証トークン:** 会社の Twilio 認証トークン。
これらの両方が<https://www.twilio.com/console>にあるTwilioコンソールで見つかります。
- **Twilio メッセージングサービスの SID:** 2要素認証メッセージングサービスのSIDです。このSIDは、<https://www.twilio.com/console/sms/dashboard>にあります。複数の Twilio メッセージングサービスを使用している場合は、2要素認証に使用するサービスの SID だけを使用します。Twilio

メッセージングサービスを作成するときに、[ユースケース] を空白のままにするか、2要素認証を選択します。

注意

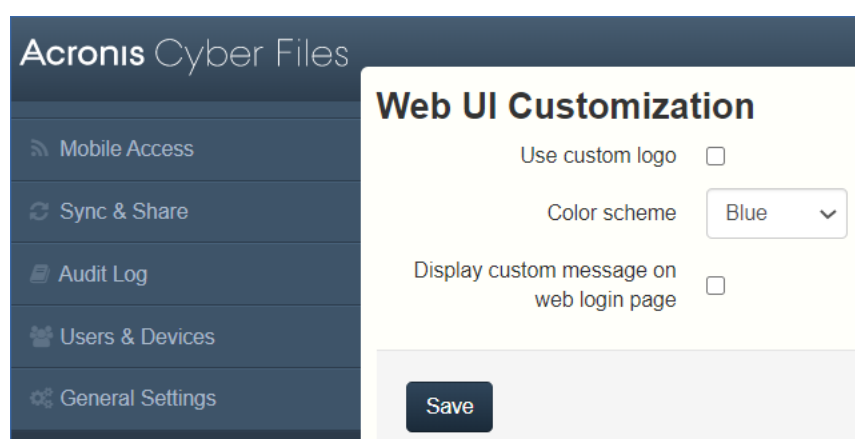
Twilio コンソールで、メッセージングサービスの使用を許可する国を選択する必要があります。希望する国のチェックボックスを選択してください。

ウェブUIのカスタマイズ

Acronis Cyber Files サーバーのロゴやカラスキームを簡単にカスタマイズできます。

注意

これらのカスタマイズを、Acronis Cyber Files API を介して実行することもできます。詳細については、「[Web UI API カスタマイズ](#)」を参照してください。



カスタム ロゴの使用

1. Acronis Cyber Files Web インターフェースを開き、管理者としてログインします。
2. [全般設定] → [ウェブ UI のカスタマイズ] に移動します。
3. [カスタム ロゴを使用] チェックボックスをオンにします。
4. 変更後のロゴファイルを選択し、ドロップダウン メニューで選択されていることを確認します。

注意

画像の最大サイズが括弧 () 内に示されます。

5. [保存] をクリックします。

カスタムのようこそメッセージを使用する

1. Acronis Cyber Files Web インターフェースを開き、管理者としてログインします。
2. [全般設定] → [ウェブ UI のカスタマイズ] に移動します。

3. [ウェブのログインページにカスタムメッセージを表示します] チェックボックスをオンにします。
4. テキストボックスに任意のメッセージを入力して、[保存] をクリックします。

カラー スキームの使用

1. Acronis Cyber Files Web インターフェースを開き、管理者としてログインします。
2. [全般設定] → [ウェブ UI のカスタマイズ] に移動します。
3. [カラー スキーム] ドロップダウンをクリックし、スキームを選択します。
4. [保存] をクリックします。

ウェブのプレビューと編集

Acronis Cyber Files では、一般的なタイプのドキュメントや画像が Web クライアントのインターフェース内でプレビューおよび編集できます。ファイルをダウンロードする必要はありません。

Web Previews & Editing

Acronis Cyber Files displays common types of documents and images within the web client interface, without requiring download of these files for viewing.

☒ Enable Office Online integration

Office Online URL

You will need to configure an on-premises Office Online server or you can use Microsoft's Office Online server if you are an Office Cloud Storage Partner. Members of the Cloud Storage Partner program can use their custom WOPI discovery URL to provide a more seamless user experience by not requesting users' Office 365 credentials.

Use Office Online for supported file types

☐ Enable Microsoft services for Bing spelling, proofing and Smart Lookup

☒ Allow connection to Office Online using self-signed / untrusted certificates

☐ Preview PDF files in Office Online

☒ Enable built-in document previewer in web client

☐ Only allow previews of files that do not require server-side rendering (PDF, images, text files)

Maximum cache size for recently rendered previews

Maximum concurrent generation calls

☒ Allow connections to web preview services using self-signed certificates

☐ Use custom URL for web preview service

☒ Enable media playback

☐ Play media after loading

☒ Loop media

☐ Mute media by default

☒ Enable media playback controls

- **Office Onlineとの統合を有効にする:** Office Online 統合機能を有効にします。
 - **Office Online URL:** Office Online の WOPI 検出 URL を入力します。オンプレミスの Acronis Cyber Files インストールの場合、この URL を利用できるようにするには、オンプレミスの Office Online セットアップを使用している必要があります。Microsoft の Office Online クラウドサービスは、サービスプロバイダーの使用に限定されており、特別な証明書と許可リストがなければ一般のアクセスはできません。

- **[Office Onlineの使用]: [編集]** を使用すると、Microsoft Office ファイル (**DOCX**、**PPTX**、**XSLX**) を編集することができ、**[表示および編集]** を使用すると、前述のファイルの編集と **DOC**、**XLS** および **PPT** ファイルのプレビューもできます。この設定を無効にすると、Office ファイルと PDF ファイルはすべて Acronis Cyber Files 内部プレビュー機能で開かれます。
- **Bingによるスペル、プルーフ、スマート検索用にMicrosoftサービスを有効にする**: スペルチェック機能に Microsoft の Bing サービスを使用します。
- **[自己署名証明書または信頼されていない証明書を使用した Office Online への接続を許可]**: 有効にすると、信頼されていない証明書を使用する Office Online サーバーにユーザーがアクセスできます。
- **Office Online で PDF ファイルをプレビュー有効にすると、[Office Online の使用] が [表示および編集] に設定されている場合に、ユーザーは Office Online で PDF ファイルをプレビューできます。** それ以外の場合はすべて、PDF ファイルは Acronis Cyber Files の内部プレビュー機能でプレビューされます。
- **ウェブクライアントで組み込みのドキュメントプレビューアーを有効にする**: Web プレビューが有効になります。

注意

パスワードで保護されたファイルにはサムネイルがないため、プレビューできません。

- **サーバー側での表示を必要としないファイル (PDF、画像、テキストファイル) のプレビューのみを許可**: 追加の表示を必要としないファイルのプレビューのみを許可することで、Web プレビューにより生じる負荷を軽減します。対象となるファイルは、PDF、画像、シンプルテキストファイルです。
- **最近表示されたプレビューの最大キャッシュサイズ**: ファイルをプレビューしたときに保存されるキャッシュの最大サイズを設定します。これにより、最近開いたファイルをプレビューしたときの速度が大幅に向上します。
- **最大同時生成呼び出し数**: 同時のプレビュー生成要求の最大数を設定します。
- **自己署名証明書を使用したウェブプレビューのサービスへの接続を許可**: 自己署名証明書を使用しているウェブプレビューサービスへの接続を許可します。これらは他の Acronis Cyber Files Tomcat サービスです。
- **ウェブプレビューのサービスにカスタムURLを使用**: 複数の Acronis Cyber Files サーバーを使用している場合に、Web プレビューを処理するサーバーを指定できます。
- **メディア再生を有効にする**: デフォルトのメディアプレイバック設定を制御できます。これにより、ファイル全体をダウンロードせずにブラウザでビデオがプレビューできます。
 - **読み込んだ後にメディアを再生する**: **[再生]** ボタンをクリックしなくてもビデオが自動的に開始します。
 - **メディアをループ再生する**: ビデオを自動的に繰り返し再生します。
 - **デフォルトでメディアをミュートにする**: ビデオと一緒にオーディオを再生するかどうかを指定します。オンにすると、音声なしでビデオが再生されます。
 - **メディア再生制御を有効にする**: **[再生/一時停止]**、**[ボリューム +/-]** など、ビデオ再生を制御するボタンの使用を許可します。

SMTP

Acronis Cyber Files サーバーは、構成された SMTP サーバーを使用して、共有リソースにユーザーを招待したりモバイルデバイスを登録したりするための電子メールを送信し、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。

The screenshot shows the 'SMTP' configuration page in the Acronis Cyber Files management console. On the left is a sidebar with navigation links: Licensing, General Settings, SMTP (selected), LDAP, Local Gateway Server, and File Repository. The main content area is titled 'SMTP' and contains a descriptive text box stating that the server uses the configured SMTP server for sending emails. Below this are several configuration fields: 'SMTP Server Address' (myemailserver.mycompany), 'SMTP Server Port' (25), 'Use secure connection?' (checked), 'From Name' (Acronis Cyber Files Admin), and 'From Email Address' (adminname@mycompany.c). There are also two unchecked checkboxes: 'Use only this address for all email notifications' and 'Use SMTP authentication?'. At the bottom are three buttons: 'Save', 'Send Test Email', and 'Skip SMTP Setup'.

- **SMTP サーバー アドレス:** 招待メールをユーザーに送信する際に使用される SMTP サーバーの DNS 名を入力します。
- **SMTP サーバー ポート:** SMTP サーバー ポートを入力します。この設定のデフォルト値はポート 587 です。
- **セキュリティで保護された接続を使用しますか?:** この設定は、SMTP サーバーへのセキュリティで保護された SSL 接続を可能にします。デフォルトで、有効になっています。セキュリティで保護された SMTP を無効にするには、ボックスをオフにします。
- **差出人名:** 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です。
- **差出人の電子メールアドレス:** サーバーによって送信される電子メールの「差出人」行に表示される電子メールアドレスです。
- **すべての電子メール通知にこのアドレスのみを使用する:** 有効にした場合、Acronis Cyber Files はすべての電子メール通知をこの電子メールアドレスだけから送信します。
- **SMTP 認証を使用しますか?:** SMTP ユーザー名とパスワードを使用して接続する場合はこのオプションを有効にし、それらを使用せずに接続する場合は無効にします。
 - **SMTP ユーザー名:** SMTP 認証用のユーザー名を入力します。
 - **SMTP パスワード:** SMTP 認証用のパスワードを入力します。
 - **SMTP パスワードの確認入力:** SMTP パスワードを再入力して確認します。

- **テスト用の電子メールの送信:** すべての設定が想定通りに機能していることを確認するために、電子メールを送信します。

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には、Microsoft Active Directory 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。その他の Active Directory 製品（Open Directory など）は現時点では使用できません。

Mobile Access

Sync & Share

Audit Log

Users & Devices

General Settings

Server

SMTP

LDAP

Administrators

Email Templates

Web Previews & Editing

Web UI Customization

Licensing

Debug Logging

Monitoring

LDAP

An LDAP connection to your Active Directory can be used to provide mobile access and sync and share access to users in your organization. LDAP is not required for unmanaged mobile access or sync and share support, but is required for managed mobile access. Only LDAP connections to Microsoft Active Directory are supported.

Enable LDAP?☒

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?☐

Disable LDAPS SSL certificate validation☐

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

e.g. mycompany.com. Users with email addresses whose domains are in this list must authenticate against LDAP. Users in other domains will authenticate against the Acronis Cyber Files database.

mycompany.com

+ Add

*company.com

mycompany.company.com

Remove

☒ Require exact match

LDAP information caching interval

Proactively Resolve LDAP Email Addresses☐

Use LDAP lookup for type-ahead suggestions for invites and download links.☒

Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials.☐

Save

LDAP users and groups are cached for performance. If recent updates to LDAP are not reflected, [click here](#) to clear the LDAP cache immediately.

- **LDAP を有効にしますか？**: 有効にすると、LDAP を構成できます。
 - **LDAPサーバーアドレス**: アクセスの規制に使用する Active Directory サーバーの FQDN または IP アドレスを入力します。
 - **LDAP サーバー ポート**: デフォルトの Active Directory ポートは 389 です。通常はこれを変更する必要はありません。

注意

複数のドメインをサポートしている場合、グローバルカタログポートを使用する必要がある場合があります。

- **セキュリティで保護された LDAP 接続を使用しますか？**: デフォルトで無効になっています。セキュリティで保護された LDAP (別名: LDAPS) を使用して Active Directory に接続するには、このボックスをオンにします。

注意

セキュリティで保護された LDAP 接続機能を有効にする場合、Acronis Cyber Files では、LDAP サーバーの完全修飾ドメイン名が、共通名 (CN) またはサブジェクト代替名 (SAN) として証明書に存在している必要があります。

- **LDAPS SSL 証明書の検証を無効にする**: LDAP サーバーに接続するときに LDAPS 証明書を確認しない場合は、このボックスをオンにします。これは、LDAP サーバー証明書が公的な認証局の証明がない場合に便利です。

バージョン 8.7.0 以降、このオプションは新規インストールではデフォルトで無効になっています (LDAPS 証明書は検証されます)。ただし、8.7.0 より前のバージョンからアップグレードした場合は、デフォルトで有効になります (LDAPS 証明書は検証されません)。既存の設定は、バージョン 8.7.0 以降からのアップグレード時に維持されます。

注意

使用している証明書の正確なタイプが分からない場合、または LDAPS 証明書が信頼される公的機関によって発行されていない場合は、このオプションを無効にしないでください。

- **LDAP ユーザー名/パスワード**: このログイン資格情報は、すべての LDAP クエリに使用されます。指定サービス アカウントがあってそれを使用する必要があるかどうかについては、AD 管理者に問い合わせてください。
- **LDAP 検索ベース**: ユーザーとグループの検索を始めるルート レベルを入力します。ドメイン全体を検索する場合は、「dc=domainname, dc=domainsuffix」と入力します。
- **LDAP 認証のドメイン**: このカンマ区切りリストに含まれるドメインの E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 Cyber Files データベースに対して認証します。

注意

ここでは、内部ドメインはサポートされません。パブリック名を持つ Eメール ドメインのみが許可されます。

- **完全に一致している必要があります:** 有効にしている場合、[LDAP 認証のためのドメイン] で入力されているドメインのユーザーのみが LDAP ユーザーとして処理されます。他のドメインやサブドメインのメンバーであるユーザーは、一時的なユーザーとして処理されます。
- **LDAP 情報をキャッシュする間隔:** Acronis Cyber Files で Active Directory 構造がキャッシュされる間隔を設定します。
- **LDAP 電子メール アドレスを事前に解決する:** この設定を有効にすると、Acronis Cyber Files は、ログイン イベント時と招待イベント時に、電子メール アドレスが一致するユーザーを Active Directory で検索します。これによりユーザーは自分の Eメールアドレスでログインした直後に招待メールでフィードバックを取得できますが、LDAP カタログが非常に大きい場合は実行に時間がかかることがあります。認証または招待でパフォーマンスの問題が発生するか応答が遅い場合は、この設定をオフにします。
- **招待およびダウンロードリンクで先行入力提案の LDAP 参照を使用する:** 先行入力の LDAP 参照は、Eメールアドレスが一致するユーザーを検索します。LDAP カタログが大きい場合、この検索に時間がかかることがあります。先行入力でパフォーマンスの問題が発生した場合は、この設定をオフにしてください。
- **既存の Windows/Mac ログイン資格情報を使用して、Web クライアントおよびデスクトップ同期クライアントからのログインを許可します。** それにより、資格情報を入力しなくても Web インターフェースおよびデスクトップクライアントにログインできるように、すべての LDAP ユーザーが有効になります。「[シングルサインオンの構成](#)」を参照してください。

LDAP キャッシュのクリア

最近の LDAP の変更はすべて LDAP サーバーに伝達されます。ただし、メモリに保持されている LDAP キャッシュの更新にはわずかな遅延があります。ページの下部にあるメッセージバーをクリックして LDAP キャッシュをクリアすると、LDAP の変更がすぐに利用できるようになります。

LDAP users and groups are cached for performance. If recent updates to LDAP are not reflected, [click here to clear the LDAP cache immediately.](#)

Eメール テンプレート

Acronis Cyber Files は Eメールメッセージを広範囲に使用し、ユーザーと管理者にダイナミックな情報を提供します。それぞれのイベントには、HTML 形式とテキスト形式のテンプレートがあります。[Eメール テンプレート] プル ダウン メニューをクリックすると、イベントを選択して両方のテンプレートを編集できます。

Cyber Files サーバーによって送信されるすべての Eメールは、ニーズに合わせてカスタマイズできます。各 Eメールについて、HTML とテキスト形式の E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、Liquid 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。

Acronis Cyber Files
Leave Administration

Mobile Access
Sync & Share
Audit Log
Users & Devices
General Settings
Server
SMTP
LDAP
Administrators
Email Templates
Web Previews & Editing
Web UI Customization
Licensing
Debug Logging
Monitoring

Email Templates

Save Templates

All emails sent by the Acronis Cyber Files server can be customized to meet your needs. For each email, you will need to provide both HTML and text-formatted email templates. Template bodies must be written in **Liquid**. Please review the default templates to determine how best to customize your templates.

Select Language: English
Select Email Template: Enroll user for mobile access

Available Parameters

invitation.email - User's email address
invitation.pin - User's PIN
invitation.display_name - User's display name
management_server_address - Acronis Cyber Files server address
expiration - PIN expiration date
url - Acronis Cyber Files URL
url_scheme - URL scheme to use for links (mobilecho://)
invitation.user - Username (User principal name)
app_name - App name ("Acronis Cyber Files" or "Acronis Cyber Files for BlackBerry Dynamics")
is_good - True if application is for BlackBerry Dynamics
send_ios_instructions - True if invitation should contain iOS instructions
send_android_instructions - True if invitation should contain Android instructions
send_windows_instructions - True if invitation should contain Windows instructions
has_web_access_to_shares - True if invited user has web access to network shares
email_templates_left_logo - URL to the image used for the left logo in the email templates
email_templates_right_logo - URL to the image used for the right logo in the email templates
locale - Locale code for this template
product_name - Product name (always displays as 'Acronis Cyber Files')
☐ Use configured Server Name 'Acronis Cyber Files' as product name

Email Subject
View Default
Preview

Welcome to {{ product_name }}

To use parameters in the subject, surround the parameter name with {{ }}, e.g. {{ parameter_name }}.

注意

Acronis Access Advanced のバージョン 7.3 以降では、Liquid がデフォルトのテンプレートマークアップです。ERBに書き込まれているカスタムテンプレートがある場合は、サーバーをアップグレードしていても、ERBがデフォルトのテンプレートマークアップになります。

注意

Eメールテンプレートにカスタム画像を使用している場合、これらの画像はインターネット上でホストされ、アクセス可能な状態にしておく必要があります。

- **言語の選択:** 招待メールのデフォルト言語を選択します。

注意

登録招待または共有招待を送信する場合、または単一のファイルを共有する場合は、招待ダイアログで別の言語を選択できます。

- **Eメール テンプレートの選択:** 表示または編集するテンプレートを選択します。各テンプレートは特定のイベントに使用します（ユーザーのモバイル アクセスの登録、ユーザーのパスワードの再設定など）。

注意

をアップデートしたときに、カスタムテンプレートが自動的にアップデートされることは**ありません**。Acronis によるアップデートを使用する場合は、アップデートをカスタムテンプレートに手動で実装する必要があります。この作業は、サポートおよび使用するすべての言語に対して実行する必要があります。

- **使用可能なパラメータ:** 使用可能パラメータはテンプレートごとに異なり、選択したテンプレートに基づいて変わります。
 - **Eメールの件名:** 招待メールの件名。
[デフォルトの表示] のリンクを押すと、その言語でのデフォルトの件名および電子メール テンプレートが表示されます。
 - **HTML Eメール テンプレート:** HTML コードの Eメール テンプレートが表示されます。有効な HTML コードを入力すると、それが表示されます。
[プレビュー] ボタンをクリックすると、現在のテンプレートのプレビューが表示されます。
 - **テキスト Eメール テンプレート:** テキストベースの Eメール テンプレートが表示されます。
[プレビュー] ボタンをクリックすると、現在のテンプレートのプレビューが表示されます。
-

注意

テンプレートの編集が終わったら、必ず [テンプレートの保存] ボタンをクリックしてください。

注意

英語のテンプレートを編集しても、他の言語を編集することにはなりません。言語ごとに個別のテンプレートを編集する必要があります。

テンプレートでは、パラメータを組み込んでダイナミックな情報を含めることができます。メッセージが配信されるとき、このパラメータは適切なデータで置き換えられます。

使用できるパラメータは、イベントごとに異なります。

注意

[デフォルトの表示] ボタンを押すと、デフォルトテンプレートが表示されます。

ライセンス

すべてのライセンスのリストが表示されます。

- **ライセンス:** ライセンスのタイプ（トライアル、サブスクリプションなど）。
- **Sync & Shareのライセンス取得済みクライアントの使用:** 現在使用されているSync & Share LDAP ユーザーライセンス。
- **Sync & Shareの無料クライアントの使用:** 現在使用されているSync & Shareの無料外部ユーザーライセンス。
- **モバイルアクセスクライアントの使用:** 現在使用されているモバイルクライアントのライセンス。

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]** をクリックします。

注意

ライセンスの固有 ID が同一である場合、許可されているユーザーの数は合計されます。

ゲートウェイサーバー用に新しいライセンスを追加する必要はありません

Acronis Access バージョン 6.0 から、Acronis Cyber Files サーバーとゲートウェイサーバーは同じライセンスを共有します。そのため、ゲートウェイサーバーに手動でライセンスを追加する必要はなくなります。

デバッグ ログ

このページの設定は拡張ログ情報を有効にするように設計されており、Acronis Cyber Files の構成時とトラブルシューティング時に役立つことがあります。これらの設定は、カスタマ 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。

注意

特定のゲートウェイサーバーにおけるデバッグログの有効化/無効化に関する情報については、「[ゲートウェイサーバーの編集](#)」の記事を参照してください。

It is recommended that the Debug Logging setting only be changed at the request of a customer support representative. Additional debug logging can be useful in troubleshooting problems on the server.

Please consult the [documentation](#) for more information on where log files are located.

General Debug Logging Level

Enabled debug modules always log at the debug level, regardless of the general debug logging level above.

Available Debug Modules

active_record
authentication
cluster
comet
database_connections
email
encryption
expiration

Add +

Remove

Remove All

Enabled Debug Modules

Acronis Cyber Files サーバーのバージョン 7.0 以降では、**exceptions** モジュールが使用可能なモジュールのリストから削除され、デフォルトで常に有効になります。以前のバージョンの Acronis Cyber Files からアップグレードしたユーザーの場合、これまでのように **exceptions** モジュールがリストに表示されていることがあります。ログオプションを変更し、[保存] を押すことで、このモジュールが表示されなくなります。

警告

これらの設定は通常の運用中および本稼働環境では使用しないでください。

- **全般的なデバッグ ログ レベル:** ログに記録する主要レベル（Info、警告、Fatal エラーなど）を設定します

注意

デバッグ モジュールを有効にすると、上記の全般的なデバッグ ログ レベルに関係なく常にデバッグ レベルでログに記録されます。

- **使用可能なデバッグ モジュール:** 使用可能なモジュールのリストを表示します。
- **有効になっているデバッグモジュール:** アクティブモジュールが表示されます。

注意

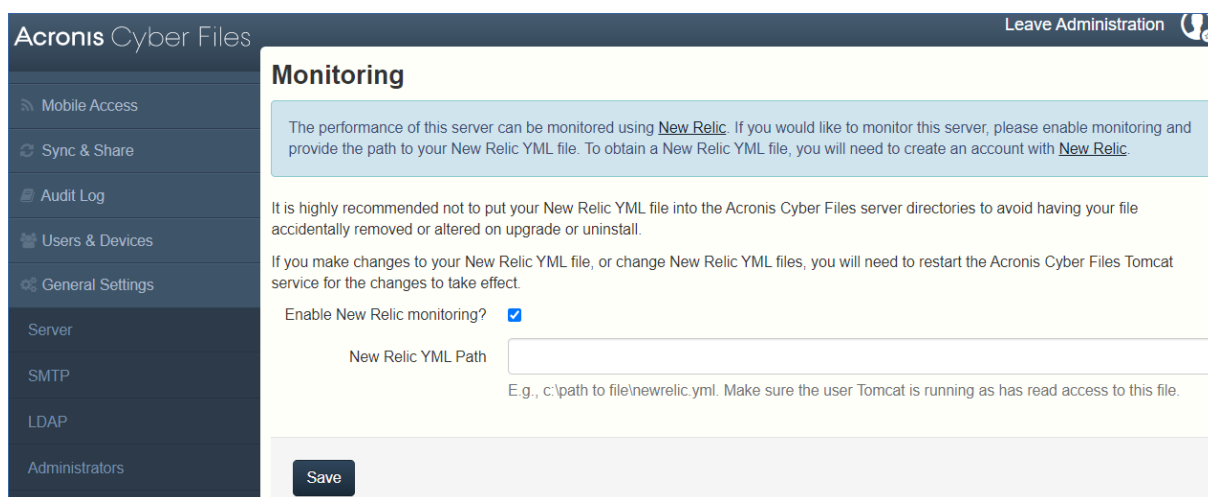
新規インストールではなく、製品をアップデートした場合、ログ ファイルは C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.42\logs に格納されます。

注意

Acronis Cyber Files をクリーンインストールした場合、ログファイルは C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.42\logs に格納されます。

監視

New Relicを使用してこのサーバーのパフォーマンスを監視できます。このサーバーを監視する場合は、監視を有効にし、New Relic YMLファイルのパスを指定してください。New Relic YMLファイルを取得するには、[New Relic](#)でアカウントを作成する必要があります。



注意

アップグレードまたはアンインストール時にファイルが誤って削除されたり変更されたりすることを防ぐために、Acronis Cyber Files サーバーがインストールされたディレクトリに New Relic YML ファイルを置かないことをお勧めします。

注意

New Relic YML ファイルに変更を加えたり、New Relic YML ファイルを置き換えたりした場合は、変更を有効にするために Acronis Cyber Files Tomcat サービスを再起動する必要があります。

New Relic の監視を有効にしますか?: 有効化した場合は、**New Relic** の構成ファイル (newrelic.yml) へのパスを指定する必要があります。

New Relic のインストール。New Relic による Acronis Cyber Files の監視

New Relic による Acronis Cyber Files の監視

この種類のインストールでは、Acronis Cyber Files サーバー アプリケーションがインストールされている実際のコンピューターではなく、このサーバー アプリケーションそのものを監視できます。

1. <http://newrelic.com/> を開き、New Relic アカウントを作成するか、既存のアカウントでログインします。上記の手順を完了すると、アプリケーションの設定画面に進みます。
2. アプリケーション タイプには **[APM]** を選択します。
3. プラットフォームには **[Ruby]** を選択します。
4. New Relic Starting Guide の手順 3 に示されている New Relic のスクリプト (newrelic.yml) をダウンロードします。
5. Acronis Cyber Files ウェブ コンソールを開きます。
6. **[設定]** → **[監視]** に移動します。
7. 拡張子も含めて、newrelic.yml へのパスを入力します (C:\software\newrelic.yml など)。Acronis Cyber Files フォルダ以外のフォルダにこのファイルを配置し、アップグレード時やアンインストール時に削除や変更されないようにすることをお勧めします。
8. **[保存]** をクリックし、New Relic サイトで **[Active application(s)]** ボタンが有効になるまで数分間待機します。
9. 10 分以上経過したら、Acronis Cyber Files Tomcat サービスを再起動して数分待機します。これでボタンがアクティブになります。
10. New Relic の Web サイトで Acronis Cyber Files サーバーを監視できます。

注意

New Relic への接続や監視の設定に関して Acronis Cyber Files サーバーがログに記録するすべての情報は、C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs にある **newrelic_agent.log** というファイルにあります。問題が発生した場合は、このログファイルで情報を検索できます。

注意

次のような内容で始まる警告やエラーが頻繁に発生することがあります。

「警告: IP アドレスをキャッシュ中に DNS エラーが発生しました: Errno::ENOENT: このようなファイルまたはディレクトリはありません - C:/etc/hosts」これは、New Relic の別のバグのパッチに使用されているコードの副次的な影響であり、問題はありません。

実際のコンピュータも監視する場合は、次の手順に従います

1. <http://newrelic.com/> を開き、自分のアカウントでログインします。
2. **[サーバー]** を押し、オペレーティング システムに合った New Relic インストーラをダウンロードします。
3. New Relic モニタをサーバーにインストールします。
4. New Relic サーバー モニタには Microsoft .NET Framework 4 が必要です。New Relic インストーラのリンクは Microsoft .NET Framework 4 Client Profile 専用です。New Relic Server Monitor インストーラを実行する前に、Microsoft Download Center に移動してインターネットから .NET 4 Framework 全体をダウンロードしてインストールする必要があります。
5. New Relic がサーバーを検出するまで待機します。

メンテナンス タスク

注意

Acronis Cyber Files のすべての構成要素をバックアップしたり、ベスト プラクティスの一環やバックアップ プロセスの一部としてバックアップしたりする場合、「[災害復旧ガイドライン](#)」の記事が有用な場合があります。

災害復旧ガイドライン

高可用性と迅速な復旧は、Acronis Cyber Files のようにミッションクリティカルなアプリケーションにおいて、非常に重要です。ローカルハードウェアのエラーからネットワーク中断やメンテナンスタスクまで、想定内または想定外の状況が原因で、非常に短い時間で、Acronis Cyber Files を稼働状態に復旧させる手段を準備しておく必要があります。

はじめに:

高可用性は、Acronis Cyber Files のようにミッションクリティカルなアプリケーションにおいては、非常に重要です。ローカルハードウェアのエラーからネットワーク中断やメンテナンスタスクまで、さまざまな状況が原因で、非常に短い時間で、Acronis Cyber Files を稼働状態に復旧させる手段を準備しておく必要があります。

災害復旧の実装には、バックアップの復元、イメージング、視覚化やクラスタリングなど、さまざまな方法があります。次のセクションで、バックアップの復元の手順を説明します。

Acronis Cyber Files の要素の説明:

Acronis Cyber Files は数々の個別の要素で構成されたソリューションですが、要素は相互に繋がりを持っています。

Acronis Cyber Files ゲートウェイ サーバー

注意

通常の場合: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server

Acronis Cyber Files サーバー

注意

通常の場合: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server

Acronis Cyber Files 構成ユーティリティ

注意

通常の場合: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Configuration Utility

ファイル ストア

ファイルストアのロケーションは、**構成ユーティリティ**を初めて使用したときのインストール中に設定されます。

注意

FileStore は、暗号化形式のユーザー ファイルで構成されています。FileStore 構成は、一般的なファイル コピー ツール（robocopy や xtree）のいずれを使用してもコピーやバックアップを取ることができます。通常、これらの構成は高い可用性のネットワーク ボリュームや NAS に配置され、デフォルトのロケーションとは異なる場合があります。

PostgreSQL データベース。これは Windows サービスとして実行される独立した要素です。Acronis Cyber Files によってインストールされ使用されます。Acronis Cyber Files データベースは、すべての構成、ユーザーとファイルの関連付け、ファイルのメタデータなどを保持しているため、最も重要な構成要素の 1 つです。

これらすべてのコンポーネントは、Acronis Cyber Files の動作するインスタンスを作成するために必要です。

迅速な復旧プロセスの実装に必要なリソース

災害復旧プロセスを実行するために必要なリソースは、次のとおりです。

- オペレーティングシステム、アプリケーション、そのデータをホストする適切なハードウェア。アプリケーションのシステムとソフトウェアの要件に対応したハードウェア。
- 切り替えが必要とされるときにすべてのソフトウェアとデータ要素が確実に、利用できるようにするバックアップと復元プロセスの配置。
- クライアント設定を変更しないか、最小限のクライアント設定の変更で、内部および外部のファイアウォールとユーザーに新しいノードへのアクセス許可するルーティングの規則を含む、ネットワーク接続。
- Active Directory ドメインコントローラーと SMTP サーバーにアクセスするための Acronis Cyber Files のネットワークアクセス。
- セカンダリ ノードへの受信リクエストをリダイレクトする、高速のまたは自動化された DNS 切り替え機能。

手順

バックアップ設定

安全で迅速な復旧シナリオを用意するのに推奨される手法は次のとおりです。

1. セカンダリ、リストア、ノードのすべての要素を Acronis Cyber Files のインストールに含めます。用意できない場合は、代わりに（元の）マシンの完全なバックアップやイメージを用意します。仮想環境では、定期的にスナップショットを取ることで効果的かつ安価に対応することができます。
2. Acronis Cyber Files サーバー ソフトウェア スイート（Apache Software ブランチすべてを含む、前述したすべての構成要素）を定期的にバックアップします。バックアップ タスクには、任意の一般的な、企業向けバックアップ ソリューションを使用します。

3. FileStore は可能な限り頻繁にバックアップしてください。標準的なバックアップ ソリューションを使用できますが、対象となるデータの量によっては、自動化された差分コピー ツールを使用した方が良い選択であったり、ときには望ましい代替の選択である場合もあります。差分コピーを取る方法は、元の FileStore と対象の FileStore 間で異なるデータをアップデートすることにより、作業にかかる時間を最小限に抑えることが可能です。
4. Acronis Cyber Files データベースは可能な限り頻繁にバックアップしてください。このタスクは、Windows のタスク スケジューラで実行されるデータベースの自動ダンプ スクリプトによって実行されます。次に、データベース ダンプを一般的なバックアップ ツールでバックアップします。

リカバリ

前述のセクションで示した要件を満たし、実装されている場合は、バックアップ リソースをオンラインに移行するプロセスは比較的シンプルです。

1. 復旧ノードをブートします。必要に応じて IP アドレスなどのネットワークの設定を調整します。Active Directory の接続と SMTP へのアクセスをテストします。
2. 必要に応じて、最新の Acronis Cyber Files ソフトウェアスイートバックアップを復元します。
3. Windows コントロール パネルやサービスを使用して、Tomcat が実行されていないことを確認します。
4. 必要に応じて、FileStore を復元します。FileStore の相対ロケーションが元のコンピューターと同一のロケーションにあることを確認してください。ロケーションが異なる場合は、構成ユーティリティを使用して、ロケーションを調整してください。
5. Windows コントロール パネルやサービスを使用して、PostgreSQL サービスが実行されていることを確認します。
6. Acronis Cyber Files データベースを復元します。
7. Acronis Cyber Files Tomcat サービスを起動します。
8. DNS を新しいノードのポイントに移行します。
9. Active Directory と SMTP が正常に動作していることを確認します。

運用例

1. データベースの定期的なバックアップ

データベースの継続的なバックアップは、Acronis Cyber Files の管理の最も重要な側面の 1 つです。
バックアップ処理はすべて自動化されているため、バックアップを常に最新の状態でできます。

Acronis Cyber Files サーバーの非常に大きなデータベースでのデプロイでは、提供されているものとは異なるバックアップおよび復元方法を使用する場合があります。

数ギガバイト以上のデータベースでのデプロイでは、**バックアップおよび復元処理の間にスピードを上げるため、または機能向上のための追加設定が必要となる場合があります。**特定の構成に関するヘルプや手順については、当社のテクニカルサポート (<http://www.acronis.com/ja-jp/mobilitysupport/>) にお問い合わせください。

2. 非常に大規模なデプロイでは、1 ヶ月ごとにデータベースに [バキューム] および [分析] 機能を適用することをおすすめします

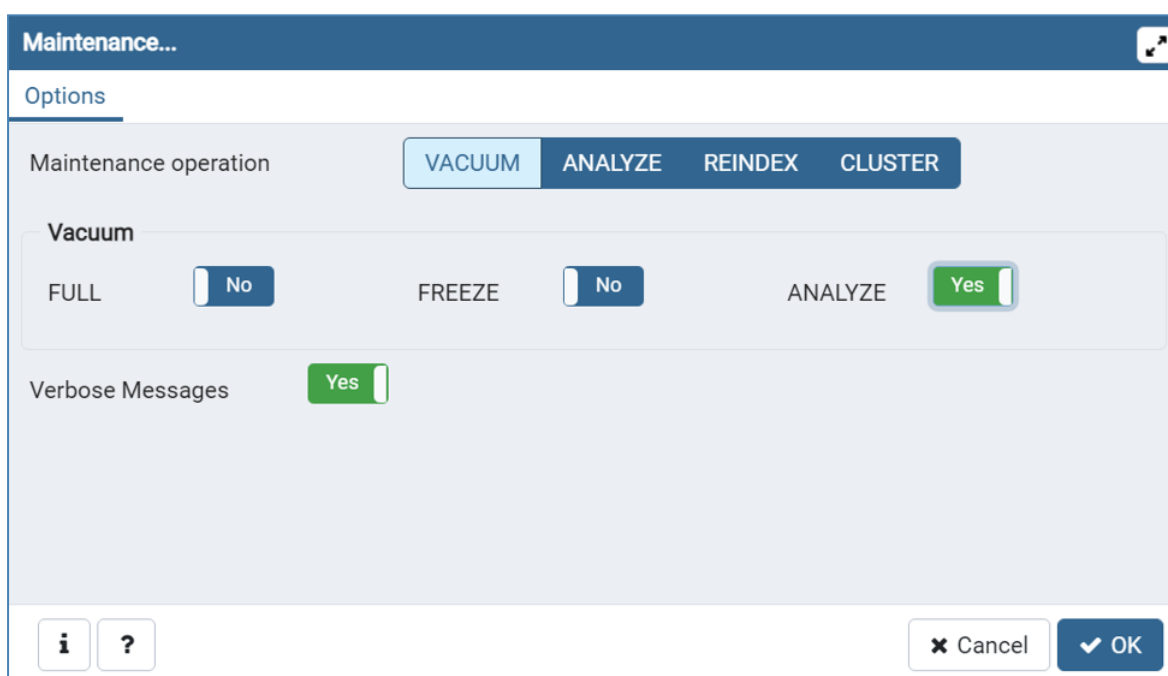
PostgreSQL データベースでは、vacuumingという定期メンテナンスが必要です。**バキューム**コマンドは各テーブルに定期的に実行する必要があります。

- 削除またはアップデートされた行で占められるディスク領域は復旧するか再利用してください。
- 非常に古いデータの損失を回避します。
- データ統計をアップデートしてインデックススキャンをスピードアップします。

分析コマンドでは、データベース内のテーブルのコンテンツに関する統計を収集し、結果を保存します。その後、クエリプランナがこれらの統計を使用してクエリの最適な実行プランを決定します。

データベースのバキューム処理や分析を手動で行うには、次の手順を実行します。

1. Acronis Cyber Files PostgreSQL 管理ツールを開きます。これは [スタート] メニューの Acronis Cyber Files フォルダにあります。[localhost] をダブルクリックして、サーバーに接続します。
2. acronisaccess_production データベースを右クリックして、[メンテナンス] を選択します。
3. [バキューム] を選択し、[分析] を [はい] に設定します。



警告

バキューム処理には長時間がかかる場合があります。サーバーの負荷が低いときにこのプロセスを実行してください。

4. [OK] をクリックします。
5. [バキューム] プロセスが終わると、[完了] を押します。
6. PostgreSQL 管理ツールを閉じます。

自動バキュームを設定するには、データベースの[自動バキューム](#)の記事を参照してください。

3. 大規模な配置では、[ロードバランス設定](#)や[ゲートウェイ サーバーのクラスター化](#)を検討する必要があります。

Acronis Cyber Files のバックアップと復元

アップグレードが必要な場合は、Acronis Cyber Files サーバーのアップデートまたはメンテナンスを行います。この記事では、データベースのバックアップと復元の基本について説明します。負荷分散構成では、このプロセスは通常のバックアップと復元とほぼ同じです。特定の仕様が関連するステップに追加されます。

注意

Acronis Cyber Files サーバーのデータベースが非常に大きく、数ギガバイトに達する場合には、別のバックアップおよび復元の方法が必要になることがあります。ヘルプや手順については、当社のテクニカルサポート (<https://support.acronis.com/mobility>) にお問い合わせください。

注意

Microsoft フェールオーバークラスターでは、一部のパスが異なる場合がありますが、バックアッププロセスは同じです。この処理はアクティブノードで実行する必要があります。また、役割がバックアップ中にフェールオーバーしたり開始しないことを確認する必要があります。

本番環境のバックアップ/復元に進む前に、テスト環境でテストバックアップ/復元を実行することを強くお勧めします。

Cyber Files データベースのバックアップ

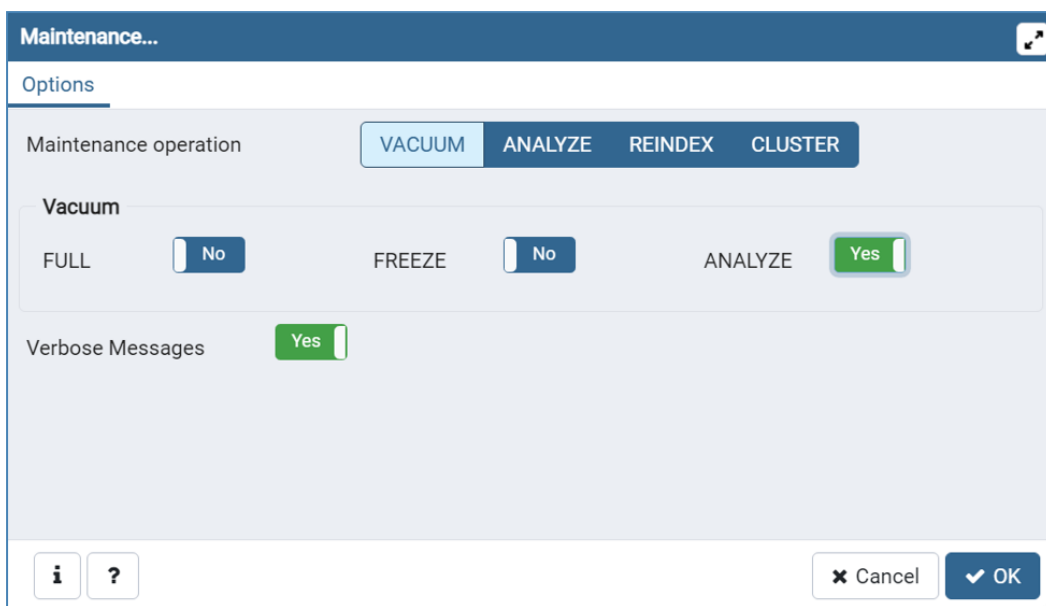
1. Acronis Cyber Files Tomcat サービスを停止します。

注意

複数の Acronis Cyber Files Tomcat サービスを負荷分散している場合は、それらをすべて停止します。

2. AcronisCyber Files PostgreSQL Administrator ツールを開きます。これは Windows の [スタート] メニューの [AcronisCyber Files] フォルダにあります。データベースサーバーに接続します。
postgres ユーザーのパスワード入力を求められる場合があります。
3. [データベース]を展開し、acronisaccess_productionデータベースを右クリックします。
4. [メンテナンス]を選択します。

5. **[バキューム]** を選択し、**[分析]** を **[はい]** に設定します。



6. **[OK]** を押します。
7. データベース、**[スキーマ]**、**[Public]**の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
8. PostgreSQL Administrator ツールを閉じ、管理者特権でのコマンドプロンプトを開きます。
9. コマンドプロンプトで、PostgreSQL bin ディレクトリに移動します。

例: `cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

注意

カスタムインストールまたは古いインストールを使用する場合には PostgreSQL bin フォルダを指すようにパスを編集する必要があります (例: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`) 。

10. コマンド `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql` を入力します。
- バックアップのファイル名は `alldbs.sql` になります。これは、PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を `--file D:\Backups\alldbs.sql` のように変更します。
 - デフォルト以外のポートを使用している場合は、`5432` を正しいポート番号に変更します。
 - デフォルトの PSQL 管理者アカウント `postgres` を使用していない場合は、上記コマンド内の `postgres` をご使用の管理者アカウント名に変更してください。
 - この手順では、`postgres` ユーザーのパスワードを何回か入力するように求められます。そのたびにパスワードを入力してEnterキーを押してください。

注意

パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

11. バックアップファイルを安全な場所にコピーします。
12. postgresql.conf ファイルには重要な設定が含まれているため、このファイルに移動して安全な場所にコピーします。このファイルは PostgreSQL のデータフォルダ内にあります（デフォルトでは C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data）。

ゲートウェイサーバーのデータベースのバックアップ

1. Acronis Cyber Files ゲートウェイサービスを停止します。
2. ゲートウェイサーバーのdatabaseフォルダに移動します。デフォルトでは次の場所にあります。
C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database
3. mobilEcho.sqlite3 ファイルを安全な場所にコピーします。
4. 複数のゲートウェイサーバーを使用している場合は、それぞれに対してこのプロセスを繰り返し、データベースファイルが取り違えられないようにします。

その他のバックアップ対象ファイル

以下のファイルで変更を加えたものがある場合は、Acronis Cyber Files 製品を復元または移行した際に設定を転送できるように、バックアップを作成しておくことをお勧めします。

postgresql.conf ファイル。このファイルには、データベース関連の重要な設定が含まれている場合があります。通常は、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン>\Data に配置されています。

- web.xml。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\ に配置されています。シングルサインオンの設定が含まれています。
- server.xml。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<バージョン>\conf に配置されています。Tomcatの設定が含まれています。
- krb5.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<バージョン>\conf に配置されています。シングルサインオンの設定が含まれています。
- login.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<バージョン>\conf に配置されています。
- Acronis Cyber Files に使用する証明書とキー。
- acronisaccess.cfg。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server に配置されています。
- カスタムカラースキーム。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\ に配置されています。
- pg_hba.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン>\Data に配置されています。
- newrelic.yml ファイル。Acronis Cyber Files サーバーの監視に **New Relic** を使用している場合。

Cyber Files データベースの復元

1. **[サービス]** コントロールパネルを開いて、AcronisCyber Files Tomcat サービスを停止します。

注意

負荷分散構成では、すべての AcronisCyber Files Tomcat サービスを停止します。

2. AcronisCyber Files PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して `acronisaccess_production` という名前のデータベースがあることを確認します。
3. データベースを右クリックして、**[更新]** を選択します。
4. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。
 - データベースにテーブルがある場合は、データベースを右クリックして、名前を `oldacronisaccess_production` に変更します。最後に、**[データベース]** に移動し、右クリックして `acronisaccess_production` という名前の新しいデータベースを作成します。
5. PostgreSQL Administratorを閉じ、管理者特権でのコマンドプロンプトを開きます。
6. このコマンドプロンプトで、PostgreSQLのbinディレクトリに移動します。
例: `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン>\bin"`
7. データベースのバックアップファイル `alldbs.sql` (またはユーザーが付けたファイル名) を **bin** ディレクトリにコピーします。
8. コマンドプロンプトで、次のコマンドを実行します: `psql -U postgres -f alldbs.sql`
9. `postgres` パスワードを求められたら入力します。

注意

データベースサイズによっては、復元にしばらく時間がかかることがあります。

10. 復元が完了したら、コマンドプロンプトのウィンドウを閉じます。
11. Acronis Cyber Files PostgreSQL Administrator アプリケーションをもう一度開き、ローカルデータベースサーバーに接続します。
12. **[データベース]** を選択します。
13. `acronisaccess_production` データベースを開き、**[スキーマ]**、**[Public]** の順に展開します。**[テーブル]** の数が、「Acronis Cyber Files のデータベースのバックアップ」セクションの手順 5 と同じであることを確認します。

注意

データベースを復元する Acronis Cyber Files Server のバージョンが、データベースバックアップでのバージョンよりも新しい場合、また Acronis Cyber Files Tomcat サービスが既に開始されている場合には、新しい Acronis Cyber Files Server データベースのテーブル数はバックアップ実行時のテーブル数よりも多くなる場合があります。

ゲートウェイサーバーのデータベースの復元

1. Acronis Cyber Files ゲートウェイサービスを停止します。
2. mobliEcho.sqlite3 ゲートウェイサーバーデータベースのバックアップを新しいゲートウェイサーバーの database フォルダ（デフォルトでは C:\Program Files (x86)\Acronis\Files Advanced\Gateway Server\database）にコピーし、既存のファイルと置き換えます。
3. すべてのゲートウェイサーバーに対してこのプロセスを繰り返します。

その他のファイルとカスタマイズの復元

Acronis Cyber Files の構成ファイル（web.xml、server.xml、krb5.conf、証明書、カスタムカラースキーム、電子メールテンプレート、pg_hba.conf、または newrelic.yml）へのすべてのカスタマイズをコピーして、新しいファイルに加えてください。

復元した Cyber Files サーバーのテスト

バックアップ/復元または別のコンピューターへの移行に成功したら、Acronis Cyber Files をオンラインに戻し、すべての設定が正しいことを確認します。

通常導入のオンライン化

1. Acronis Cyber Files 設定ユーティリティを起動して、すべての設定が正しいことを確認してください。
2. すべてのサービスを開始するには、[OK] を押します。
3. これにより、すべてのサービスが同時にオンラインになり、すべての Acronis Cyber Files 機能が復元されるはずです。
4. 一部のコンポーネントが別のコンピューター上に存在する場合は、そのコンピューターに移動してそれらを開始する必要があります。この場合は、PostgreSQL サービスが実行していないと、Acronis Cyber Files Tomcat サービスが正常に開始されません。

負荷分散導入のオンライン化

1. プライマリとして機能する Acronis Cyber Files サーバーの 1 つを選択します。このサーバーは、最初にオンライン化するという意味でのみプライマリになります。
2. PostgreSQL サービスが別のコンピューター上に存在する場合は、そのサービスを最初に開始して、Acronis Cyber Files サーバーに影響を与えないようにします。
3. プライマリ Acronis Cyber Files サーバー用のコンピューターに移動して、Acronis Cyber Files 設定ユーティリティを開始します。
4. そこにあるすべての設定が正しいことを確認します。問題がなければ、[OK] を押してすべてのサービスを開始します。
5. Acronis Cyber Files ウェブ コンソールを開き、管理者としてログインします。すべての設定が正しいことを確認します。

6. 設定を確認したら、Acronis Cyber Files コンポーネントが存在する各コンピューターの調査に進んで、設定ユーティリティ経由でそれらのコンポーネントを開始します。

Windows での Tomcat ログ管理

Tomcat は通常の動作の一部として情報を作成し、複数のログ ファイルに書き込みます。

定期的に消去されない限り、これらのファイルは蓄積していき、貴重な容量を消費します。一般的に近年の IT 業界では、これらのログが提供する情報の価値が低いと考えられるようになりました。特定のポリシーを伴う法規のような他の要素が関係していない限り、これらのログ ファイルはある程度の日数の間システムに保持しておきます。

はじめに

Tomcat は通常の動作の一部として情報を作成し、複数のログ ファイルに書き込みます。Windows では、これらのファイルは通常次のディレクトリに保存されています。

“C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs”
Acronis Cyber Files のログは、同一のディレクトリに別個のファイルとして保存されます。

注意

Acronis Cyber Files のログファイルは **acronisaccess_date** という名前です。

不要なログ ファイルの削除のタスクを自動化する機能を持つツールは多数用意されています。たとえば、Windows に組み込まれている ForFiles コマンドを使用することができます。

注意

ForFiles の構文の詳細と例については、[http://technet.microsoft.com/en-us/library/cc753551\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc753551(v=ws.10).aspx) を参照してください。

サンプルプロセス

このサンプル プロセスでは、特定の日数経過したログ ファイルを自動的に消去する手順を説明します。サンプルのバッチ ファイル内にはこの数値がパラメータとして定義されており、数々の適用されているポリシーに適合するように変更させることが可能です。

注意

サンプルスクリプト（バッチ）ファイルは Windows Server 2008 で動作するように設計されています。[スクリプトをダウンロードするにはこちらをクリックしてください](#)。
または、スクリプトコードをコピーして、空のテキストドキュメントに貼り付けることもできます。
「AASTomcatLogPurge.bat」と名前を付けて保存してください。

完全なバッチスクリプトコード:

ECHO OFF

REM スクリプト: aETomcatLogsPurge.bat

REM 2012-05-12: バージョン: 1.0: MEA: 作成済み

```

ECHO このスクリプトは、一定日数が経過したファイルをディレクトリから削除します
ECHO これをコマンドラインまたはスケジューラから実行します
ECHO プロセスに対象フォルダからファイルを削除する許可があることを確認します
REM ===== 設定 =====
REM 注意：空白を含むすべてのパスは二重引用符で囲む必要があります
REM このファイルを編集して、下記の LogPath と NumDays を設定します
REM Tomcat のすべてのログがあるフォルダへのパス
set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"
REM NumDays - NumDays より古いログファイルが処理されます
set NumDays=14
REM ===== 設定終了 =====
ECHO
ECHO ===== 開始 =====
REM ForFiles オプション:
REM "/p": ファイルを削除する場所のパス
REM "/s": バッチファイルパスで示されるフォルダにある他のサブフォルダ内を再帰的に確認します
REM "/d": 現在よりこの日数だけ古いファイルを削除します。たとえば、"/d -7" の場合、7 日前より古いファイルを削除します
REM "/c": ファイルを実際に削除するコマンド: "cmd /c del @file"。
forfiles /p %LogPath% /s /d -%NumDays% /c "cmd /c del @FILE"
:End
ECHO ===== バッチファイル終了 =====

```

警告

このサンプルはガイドラインとして提供するものです。ユーザーの実装環境の要件に基づいて必要なプロセスを計画し、導入してください。サンプル、すべての条件や環境ではテストされていません。また適合するものではありません。サンプルは基礎としてご利用いただき、ファイル削除の実作業はユーザーの責任に基づき行ってください。**サンプルは、オフラインであらかじめ完全にテストしていない限り、本稼動環境で使用しないでください。**

手順

1. Acronis Cyber Files (Tomcat) が動作しているコンピューターにスクリプトをコピーし、メモ帳か、適切なシンプルなテキストエディタを使用して開きます。

2. 下図に示されたセクションを探して、LogPath の値と NumDays の値をユーザー固有のパスとファイル保持の設定の値に編集します。

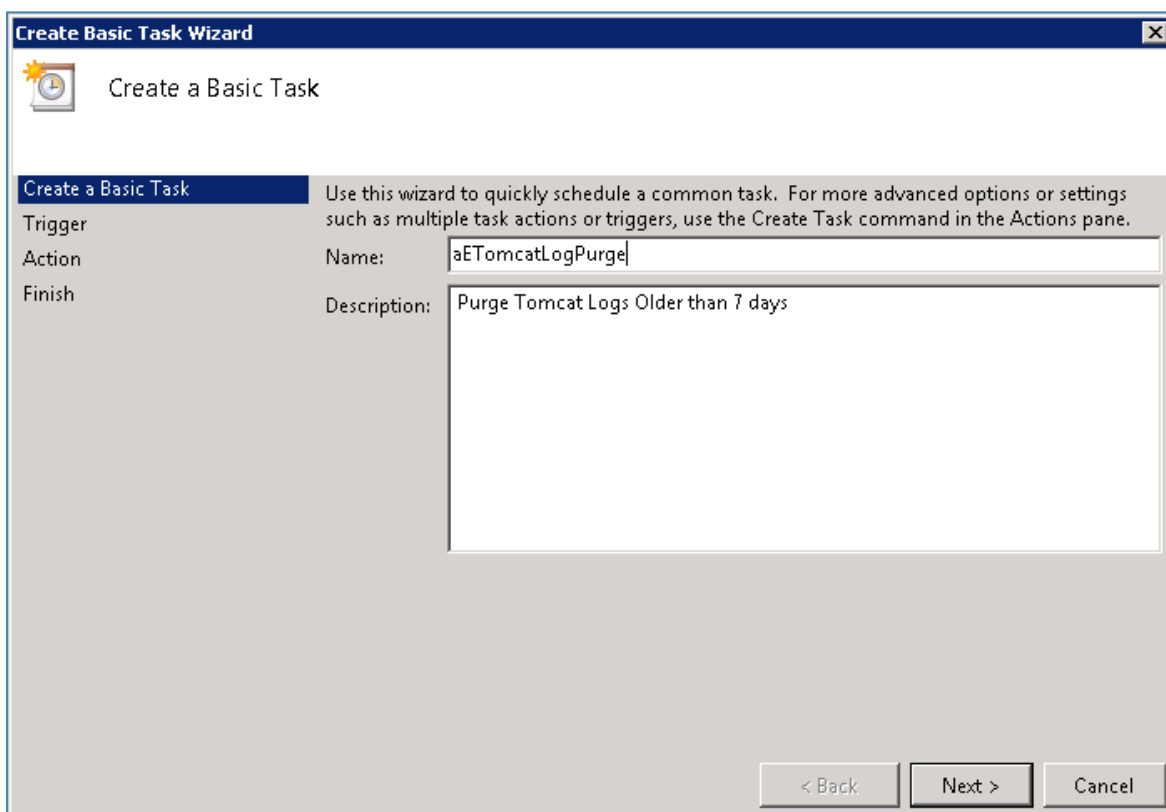
```
REM ===== CONFIGURATIONS =====
REM Note: all paths containing spaces must be enclosed in double quotes
REM Edit this file and set LogPath and NumDays below
REM Path to the folder where all Tomcat logs are
set LogPath="C:\Program Files (x86)\Group Logic\Common\apache-tomcat-7.0.34\logs"

REM NumDays - Log files older than NumDays will be processed
set NumDays=14
REM ===== END OF CONFIGURATIONS =====
ECHO
ECHO ===== START =====
```

注意

Acronis Cyber Files では、Tomcat と同一のフォルダにログファイルが保存されます（C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.34\logs）。

3. ファイルを保存します。
4. プロセスを自動化するには、[タスクスケジューラ]を開き、タスクを新しく作成してください。タスクの新しい名前と説明を定義します。



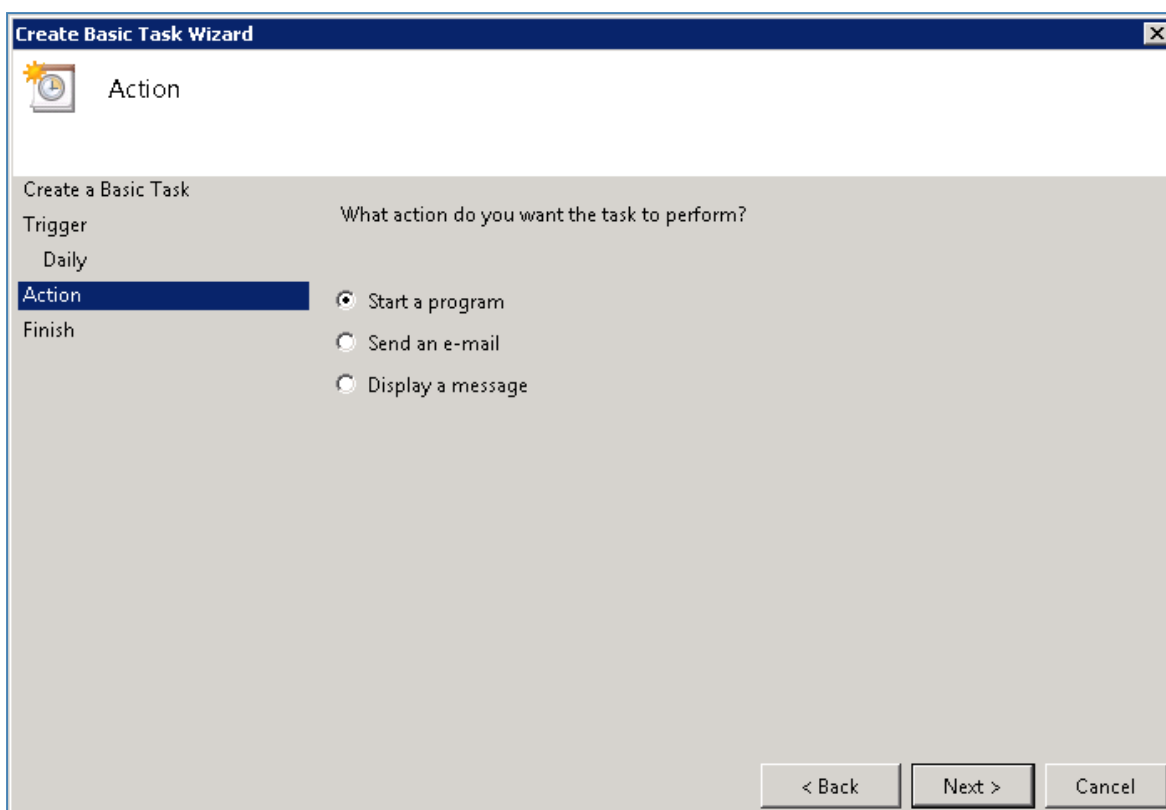
5. タスクが毎日実行されるように設定します。

The screenshot shows the 'Create Basic Task Wizard' dialog box with the title bar 'Create Basic Task Wizard' and a close button. The main area is titled 'Task Trigger' with a clock icon. On the left, a sidebar lists 'Create a Basic Task', 'Trigger', 'Action', and 'Finish'. The 'Trigger' step is selected. The main content area is titled 'When do you want the task to start?' and contains seven radio button options: 'Daily' (selected), 'Weekly', 'Monthly', 'One time', 'When the computer starts', 'When I log on', and 'When a specific event is logged'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

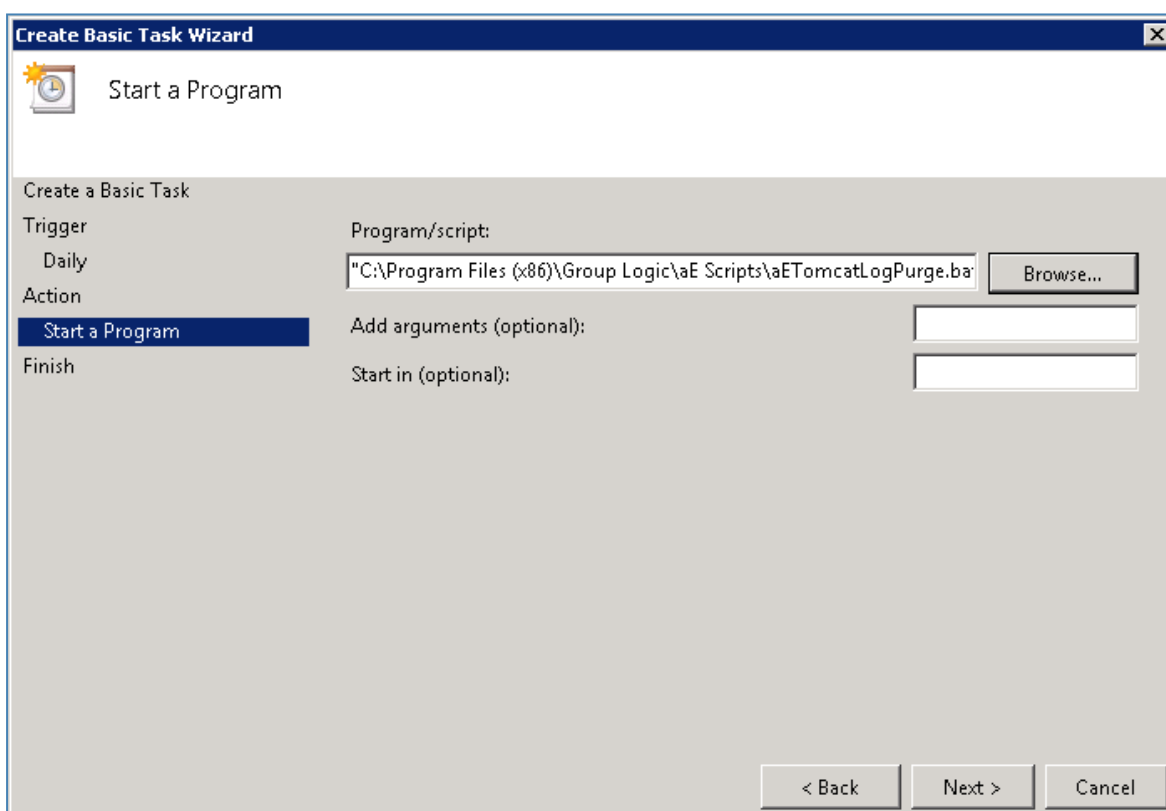
6. タスクが開始される時刻を定義します。このプロセスは、システムに極めて高い負荷がかかっている状態や、他のメンテナンス プロセスが実行中でないときに実行することをお勧めします。

The screenshot shows the 'Create Basic Task Wizard' dialog box with the title bar 'Create Basic Task Wizard' and a close button. The main area is titled 'Daily' with a clock icon. On the left, a sidebar lists 'Create a Basic Task', 'Trigger', 'Daily', 'Action', and 'Finish'. The 'Daily' step is selected. The main content area has a 'Start:' label followed by a date dropdown set to '5/17/2012', a time dropdown set to '2:00:00 AM', and a checkbox labeled 'Synchronize across time zones' which is unchecked. Below this, it says 'Recur every: 1 days'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

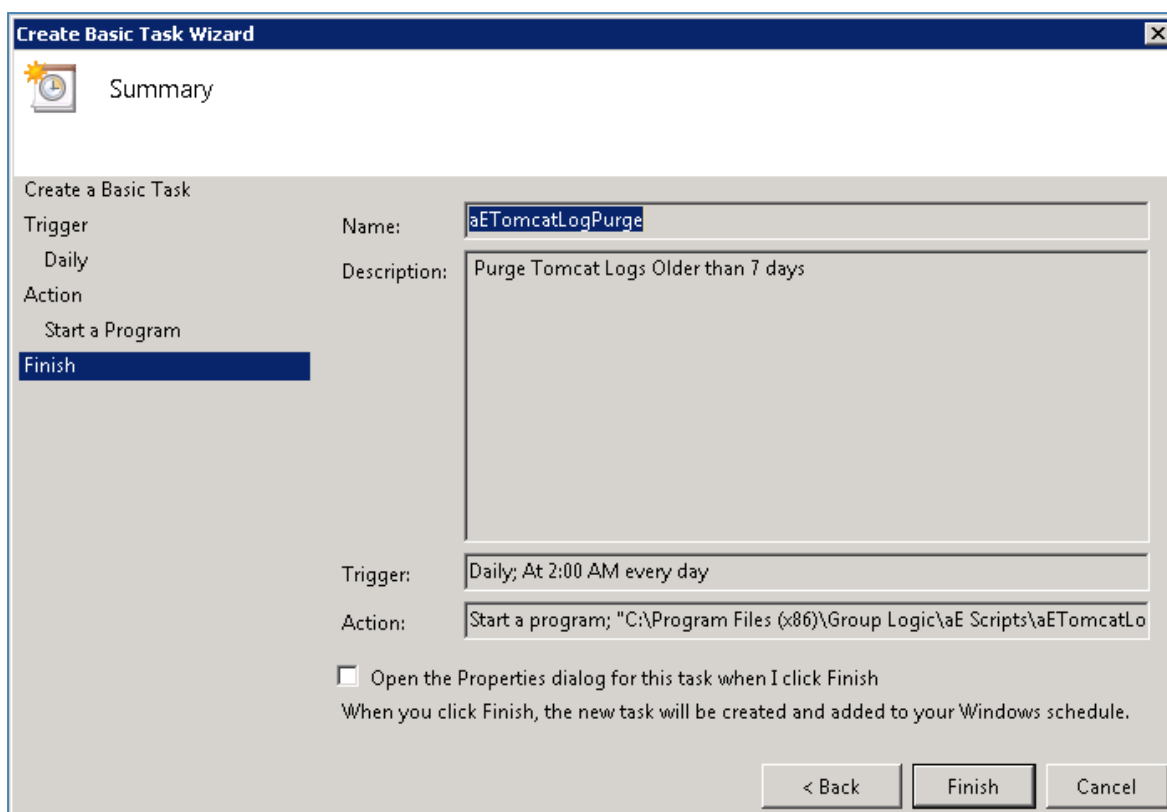
7. アクションタイプを「プログラムの開始」に設定します。



8. [参照] ボタンをクリックし、スクリプト（バッチ）ファイルを参照して選択します。



9. 終わったら **[完了]** をクリックします。



10. タスク リストでタスクを右クリックすると、プロパティを選択し、ユーザーのログイン状態に関わらず、たとえユーザーがログインしていなくても、タスクが実行されるか検証することができます。
11. タスクを選択して右クリックし、[実行] を選択することで、タスクが正常に構成され、適切に実行されるかを確認することができます。スケジューラのログには、開始や停止、すべてのエラーが報告されます。

データベースの自動バックアップ

Windows タスク スケジューラを活用して、Acronis Cyber Files データベースの自動バックアップスケジュールを簡単に設定できます。

データベース バックアップ スクリプトの作成

1. **メモ帳**（または他のテキスト エディタ）を開き、以下を入力します。

```
@echo off
```

```
for /f "tokens=1-4 delims=/ " %i in ("%date%") do (
```

```
set dow=%i
```

```
set month=%j
```

```
set day=%k
```

```
set year=%l
```

```
)
```

```
set datestr=%month%_%day%_%year%
```

```
echo datestr is %datestr%
```

```
set BACKUP_FILE=AAS_%datestr%_DB_Backup.sql
```

```
echo backup file name is %BACKUP_FILE%
```

```
SET PGPASSWORD=password
```

```
echo on
```

```
bin\pg_dumpall -U postgres -f %BACKUP_FILE%
```

```
move "%BACKUP_FILE%" "C:\destination folder"
```

2. のインストール時に入力した **postgres** ユーザーのパスワードで "**password**" を置き換えます。
3. バックアップを保存するフォルダへのパスで **C:¥destination folder** を置き換えます。
4. ファイル名を **DatabaseBackup.bat** にし、ファイルの種類で **[すべてのファイル]** を選択して保存します（拡張子が重要です）。
5. バージョン番号のディレクトリ（¥9.3¥ など）にある PostgreSQL のインストール フォルダにファイルを移動します。

スケジュール タスクの作成

1. **[コントロール パネル]** を開き、**[管理ツール]** を開きます。
2. **[タスク スケジューラ]** を開きます。
3. **[操作]** をクリックし、**[タスクの作成]** を選択します。

[全般] タブで次の操作を実行します。

1. タスクの名前と説明を入力します（例: AAS Database Backup）。
2. **[ユーザーがログオンしているかどうかにかかわらず実行する]** を選択します。

[トリガー] タブで次の操作を実行します。

1. **[新規]** をクリックします。
2. **[タスクの開始]** で **[スケジュールに従う]** を選択します。
3. **[毎日]** を選択し、スクリプトを実行する時間と、スクリプトの再実行頻度（データベースをバックアップする頻度）を選択します。
4. **[詳細設定]** で **[有効]** を選択し、**[OK]** を押します。

[操作] タブで次の操作を実行します。

1. **[新規]** をクリックします。
2. **[操作]** で **[プログラムの開始]** を選択します。
3. **[プログラム/スクリプト]** で **[参照]** を押し、**DatabaseBackup.bat** ファイルを選択します。
4. **[開始 (オプション)]** で、スクリプトがあるフォルダへのパスを入力します。たとえば、スクリプトへのパスが `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\PSQL.bat` の場合は、「`C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.3\`」と入力します。
5. **[OK]** をクリックします。
6. 他のタブで追加の設定を設定し、**[OK]** を押します。
7. 現在のアカウントの認証情報が要求されます。

データベースの自動バキューム

このガイドでは、PostgreSQLデータベースを実行し、バキュームするスケジュールタスクを作成する方法について説明します。特にデプロイに大きなデータベース（数ギガバイト）がある場合には、バキューム処理が重要となります。

注意

PostgreSQL は構成ファイルで自動バキュームを行うように設定されています。サーバーの負荷が高い場合には処理を行わないように設計されているため、高負荷のデプロイにおいては自動バキュームが行われない可能性があります。このような場合には、最低月に1回はバキューム処理を実行するようにスケジュールタスクを設定するのが最善策です。

PostgreSQLの構成とスクリプトの作成

タスクが実行可能なことの確認

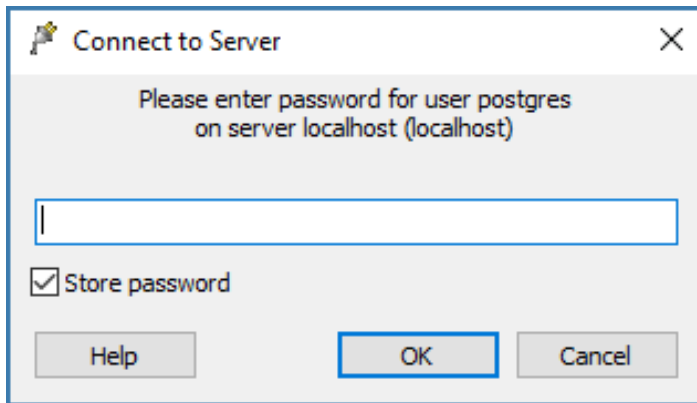
ご自身の PostgreSQL のパスワードが、pgpass ファイルに保存されていることを確認する必要があります。保存されていない場合には、スクリプトが動作しません。簡単に確認するには、Acronis Cyber Files PostgreSQL Administrator ツールを使用します。

1. Acronis Cyber Files PostgreSQL Administrator を開きます。これは Windows の **[スタート]** メニューの **[Acronis Cyber Files]** フォルダにあります。
2. データベースに接続し、ダイアログが開くとパスワードを入力します。**[パスワードを保存]** チェックボックスを有効にして、**[OK]** をクリックします。PostgreSQLのパスワードがpgpassファイルに保存されます。このファイルは、`C:\Users\<currentUser>\AppData\Roaming\postgresql` に作成され

ます。

注意

保存パスワードに関する情報を示したダイアログが表示されることがありますが、これは正常です。[OK] をクリックします。



- または、手動で **pgpass.conf** という名前のファイルを作成し、テキスト `localhost:5432:*:postgres:yourpassword` をファイルに入力して保存することもできます。
 - このとき、必ず**実際の** postgres ユーザーパスワードと正しいポートを入力してください。ファイルを保存します。
3. この例では、**pgpass.conf** ファイルをコピーして **D:¥Backup¥** フォルダに置きます。スケジュールタスクを実行するユーザーは、このファイルに対する読み取りアクセス権を持っている必要があります。

スクリプトの作成

下の例では、PostgreSQL bin ディレクトリパスが `C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\bin\` に設定されます。

注意

注意: カスタムインストールまたは古いインストールを使用する場合には PostgreSQL bin フォルダを指すようにパスを編集する必要があります (例: `C:¥Program Files (x86)¥Acronis¥Access¥Common¥PostgreSQL¥9.4¥bin¥`) 。

1. ログファイルを保存するフォルダを作成し、タスクを実行するユーザーにこのフォルダに対する読み取り、書き込み、および実行アクセス権を与えます。マシンの管理者として操作することをお勧めします。この例では、ログフォルダは `D:\Backup\` です。
2. 任意のテキストエディタ (例: メモ帳) を開き、以下のスクリプトを貼り付けます。

```
SET PGPASSFILE=D:\Backup\pgpass.conf

"C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\9.4\bin\psql.exe" --
host=localhost --port 5432 --username=postgres -d acronisaccess_production -c "VACUUM
VERBOSE ANALYZE" >"D:\Backup\vacuum_report_%date:/=.%log" 2>&1
```
3. このスクリプトをデプロイ環境に合うように編集します。

- psql.exe ファイルへのパスをそのファイルが存在するパスに変更します。
 - デフォルトを変更している場合は、--port の設定を正しいポート番号に変更します。
 - 別の PostgreSQL ユーザーを使用している場合は、postgres を対象のユーザーに置き換えることによって --username= を変更します。
 - ログ用のパスの D:\Backup\ の部分を必要なログフォルダに変更します。
 - pgpass.conf ファイル用のパスの D:\Backup\ の部分をそのファイルへのパスに変更します。
4. **vacuum.bat**という名前でファイルを保存します。保存する際には、**[ファイルの種類]**で**[すべてのファイル]**を選択していることを確認してください。

注意

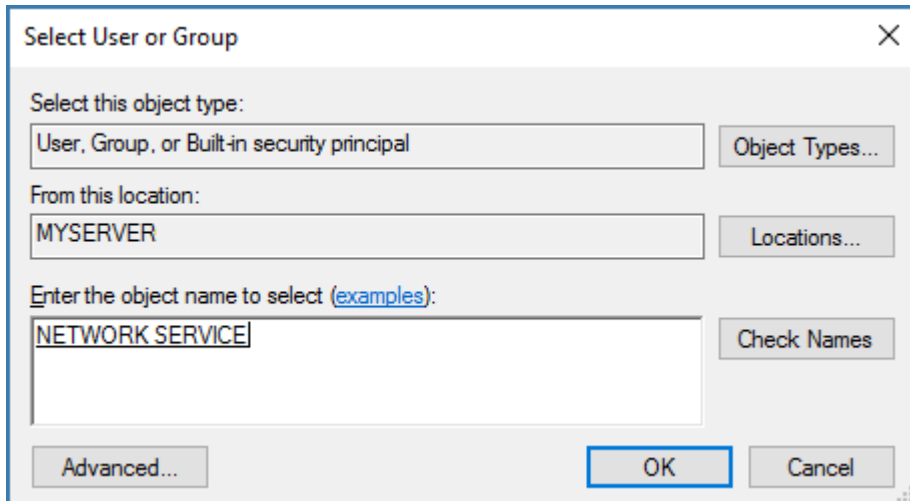
日付の形式により、この.logファイルの作成に失敗する場合があります。日付の形式を確認するには、コマンドプロンプトを開いて `echo %date%` を実行します。日付にフォワードスラッシュなどの不正な文字が含まれている場合には、他の文字に変更する必要があります。上の例では、余分な `:/=` が変換部分です。問題が発生した場合は、アクロニスサポートにお問い合わせください。

タスクスケジューラの設定

1. **[コントロールパネル]** → **[管理ツール]** → **[タスク スケジューラ]** の順にクリックして **[タスク スケジューラ]** を開きます。
2. **[タスク スケジューラ (ローカル)]** を右クリックし、**[タスクの作成]** を選択します。

3. **[全般]** タブの設定:

- [名前] と [説明] を入力します。
- [ユーザーがログオンしているかどうかにかかわらず実行する] を選択します。
- [タスクの実行時に使うユーザー アカウント] を、このタスクを実行するユーザーに設定します。
マシンの NETWORK SERVICE アカウントを使用することをお勧めします。



Select User or Group

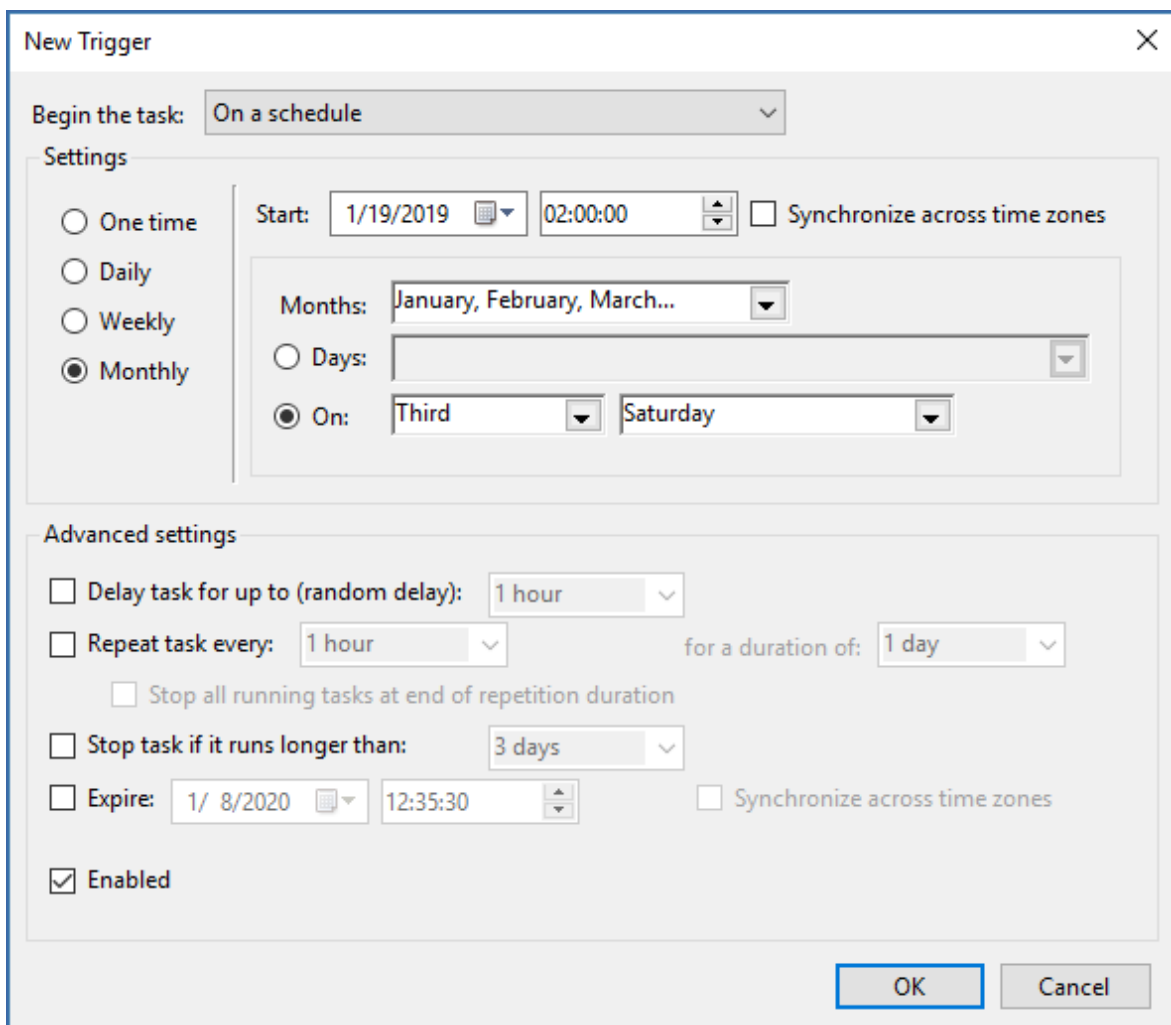
Select this object type:
User, Group, or Built-in security principal

From this location:
MYSERVER

Enter the object name to select (examples):
NETWORK SERVICE

Advanced... OK Cancel

4. [トリガー] タブの設定:



New Trigger

Begin the task: On a schedule

Settings

One time
Daily
Weekly
☒ Monthly

Start: 1/19/2019 02:00:00 ☐ Synchronize across time zones

Months: January, February, March...
Days:
On: Third Saturday

Advanced settings

☐ Delay task for up to (random delay): 1 hour

☐ Repeat task every: 1 hour for a duration of: 1 day
☐ Stop all running tasks at end of repetition duration

☐ Stop task if it runs longer than: 3 days

☐ Expire: 1/ 8/2020 12:35:30 ☐ Synchronize across time zones

☒ Enabled

OK Cancel

- **[新規]** をクリックして、バキュームを実行するスケジュールを設定します。サーバーへの負荷が低い時間帯に行うことをおすすめします。バキューム処理は、最低月に1回実行することをおすすめします。

5. **[操作]** タブの設定:

The screenshot shows the 'New Action' dialog box. At the top, it says 'You must specify what action this task will perform.' Below this, the 'Action:' dropdown menu is set to 'Start a program'. Under the 'Settings' section, the 'Program/script:' field contains 'cmd.exe' and there is a 'Browse...' button next to it. The 'Add arguments (optional):' field contains '/c "C:\Scripts\vacuum.b'. The 'Start in (optional):' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a blue border.

- **[新規]** をクリックし、**[操作]** で **[プログラムの開始]** を選択します。
- **[プログラム/スクリプト]** に、「cmd.exe」と入力します。
- **[引数の追加]** に、「/c "C:\Scripts\vacuum.bat"」と入力します。

注意

このコマンドに指定するパスを編集し、vacuum.bat ファイルの実際のパスを反映するようにしてください。

- **[条件]** タブおよび **[設定]** タブはデフォルト設定のままにします。
- **[OK]** を押して、新しいタスクを保存します。管理者パスワードの入力を求められます。

タスクの想定どおりの動作を確認

1. **[タスク スケジューラ]** からバキュームタスクを手動で実行してテストし、適切なフォルダにログファイルが作成されることを確認します。

2. スケジュールされたタスクが設定した時刻に実行されることを確認します。

Acronis Cyber Files の同一サーバーの移行

このガイドは、現在のマシンで Acronis Cyber Files セットアップを移行するのに役立ちます。

重要

本番サーバーを移行する前に、テスト環境でこれらの手順を実行することを強くお勧めします。本番環境との互換性を確保するために、テスト配置では、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、本番サーバーと同じアーキテクチャにする必要があります。

同一サーバーの移行を開始する前に

警告

本番環境外でのテストバックアップ/復元の実行を強くお勧めします。

現在の構成に関してメモする必要がある重要事項:

- Cyber Files Web サーバー、PostgreSQL、ゲートウェイとファイルリポジトリがすべて 1 台のコンピュータ上にありますか？
- Cyber Files Web サーバーの DNS、IP、ポートをメモします。
- ゲートウェイサーバーの DNS、IP、ポートをメモします。
- ファイルリポジトリのアドレスとポートをメモします。
- ファイルストアのロケーションをメモします。
- 現在のサーバーの PostgreSQL バージョン番号をメモします。

PostgreSQL のメインフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL）の中のフォルダ名（**9.2**、**9.3**、**9.4** など）が PostgreSQL のメジャーバージョン番号になっているので簡単に確認できます。

注意

これらの情報の大半は設定ユーティリティで確認できます。

同一サーバーの移行プロセスの基本概要

移行を開始する前に、これらの手順のすべてを実行する準備を整えておいてください。

1. PostgreSQL をバックアップします。
2. ゲートウェイサーバーのデータベースをバックアップします。
3. 一部の追加ファイルをバックアップします。
4. Acronis Cyber Files をアンインストールします。
5. PostgreSQL Data ディレクトリを削除します。
6. （オプション）Java を削除します。
7. アンインストール時と同じバージョンのインストーラを使用して Acronis Cyber Files をインストールします。

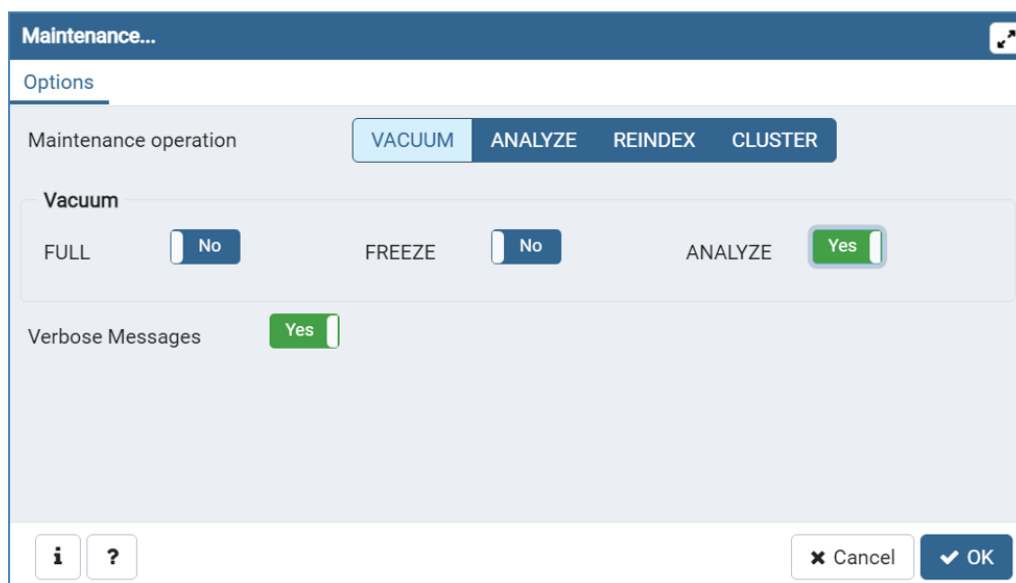
8. ゲートウェイサーバーデータベースの復元
9. サーバーを構成します。
10. Acronis Cyber Files の管理設定を確認します。
11. 新しい構成をテストします。

Acronis Cyber Files の移行

Acronis Cyber Files の移行は次の手順で実行します。

1. PostgreSQL のバックアップ

- a. **[サービス]** コントロールパネルを開いて、Acronis Cyber Files Tomcat サービスを停止します。
- b. Acronis Cyber Files PostgreSQL 管理ツールを開きます。これは Windows の **[スタート]** メニューの Acronis Cyber Files フォルダにあります。データベースサーバーに接続します。
postgres ユーザーのパスワード入力を求められる場合があります。
- c. **[データベース]**を展開し、acronisaccess_productionデータベースを右クリックします。
- d. **[メンテナンス]**を選択します。
- e. **[バキューム]**を選択し、**[分析]**を**[はい]**に設定します。



- f. **[OK]** をクリックします。
- g. データベース、**[スキーマ]**、**[Public]**の順に展開します。**[テーブル]**セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
- h. PostgreSQL Administrator ツールを閉じ、管理者特権でのコマンドプロンプトを開きます。
- i. このコマンドプロンプトで、PostgreSQLのbinディレクトリに移動します。

例:cd "C:\Program Files(x86)\Acronis\Acronis Cyber
Files\Common\PostgreSQL\<version>\bin"

注意

注意: カスタムインストールまたは古いインストールを使用する場合には PostgreSQL bin フォルダを指すようにパスを編集する必要があります (例: C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\)

- j. コマンド `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql` を入力します。
- バックアップのファイル名は `alldbs.sql` になります。これは、PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を `--file D:\Backups\alldbs.sql` のように変更します。
 - デフォルト以外のポートを使用している場合は、5432 を正しいポート番号に変更します。
 - デフォルトの PSQL 管理者アカウント `postgres` を使用していない場合は、上記コマンド内の `postgres` をご使用の管理者アカウント名に変更してください。
 - この手順では、`postgres` ユーザーのパスワードを何回か入力するように求められます。そのたびにパスワードを入力して **Enter** キーを押してください。

注意

パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

2. ゲートウェイサーバーのデータベースのバックアップ

- a. **Acronis Cyber Files ゲートウェイ** サービスを停止します。
- b. ゲートウェイサーバーの `database` フォルダに移動します。デフォルトでは次の場所にあります。
C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database
- c. `mobilecho.sqlite3` ファイルのバックアップコピーを作成します。

3. その他のバックアップ対象ファイル

以下のファイルで変更を加えたものがある場合は、Acronis Cyber Files 製品を復元または移行した際に設定を転送できるように、バックアップを作成しておくことをお勧めします。

- `postgresql.conf` ファイル。このファイルには、データベース関連の重要な設定が含まれている場合があります。通常は、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data に配置されています。
- `web.xml`。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\ に配置されています。シングルサインオンの設定が含まれています。
- `server.xml`。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf に配置されています。Tomcat の設定が含まれています。
- `krb5.conf`。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf に配置されています。シングルサインオンの設定が含まれています。

- login.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<version>\conf に配置されています。
- Acronis Cyber Files に使用する証明書とキー。
- acronisaccess.cfg。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server に配置されています。
- カスタムカラスキーム。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\ に配置されています。
- pg_hba.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data に配置されています。

4. Acronis Cyber Files のアンインストール

- Acronis Cyber Files インストーラを開きます。
- ライセンス契約に同意してから、**[アンインストール]** をクリックします。
- すべてのコンポーネントを選択し、**[アンインストール]** をクリックします。

5. PostgreSQL Data ディレクトリの削除

PostgreSQL サーバーの **データ** ディレクトリは自動的に削除されません。デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\ に配置される PostgreSQL ディレクトリ全体を手動で削除します。

注意

古いインストールまたはカスタムインストールを使用している場合は、このパスを編集する必要があります（例: C:\Program Files\Acronis\Access\Common\PostgreSQL\）。

6. (オプション) Java の削除

Acronis Cyber Files Web サーバー用にインストールされた Java を削除することもできます。Java もコントロールパネルから削除できます。

7. Acronis Cyber Files の再インストール

- 新しい Acronis Cyber Files インストーラを起動して、**[次へ]** をクリックします。
- ライセンス契約を読み、承諾します。
- [インストール]** を選択し、インストーラ画面の指示に従います。

注意

Acronis Cyber Files Web サーバー、PostgreSQL、およびゲートウェイを別々のマシンで実行している場合は、**[カスタム]** を選択して、目的のコンポーネントを選択します。

- [PostgreSQL の構成] 画面で、最初に使用していたのと同じ PostgreSQL スーパーユーザー用パスワードを入力します。
- [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を確認し、**[インストール]** をクリックします。
- インストーラが完了したら、**[終了]** をクリックします。次に設定ユーティリティを実行する旨のダイアログが表示されます。
- 設定ユーティリティが開いたら、**[OK]** も **[適用]** も押さずに開いたままにします。
- [サービス]** コントロールパネルを開いて、Acronis Cyber Files Tomcat サービスを停止します。

注意

負荷分散構成では、すべての Acronis Cyber Files Tomcat サービスを停止します。

- j. Acronis Cyber Files PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して `acronisaccess_production` という名前のデータベースがあることを確認します。
- k. データベースを右クリックして、**[更新]** を選択します。
- l. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。
 - データベースにテーブルがある場合は、データベースを右クリックして、名前を `oldacronisaccess_production` に変更します。
 - 次に、**[データベース]** に移動し、右クリックして `acronisaccess_production` という名前の新しいデータベースを作成します。
- m. PostgreSQL Administrator を閉じ、管理者特権でのコマンドプロンプトを開きます。
- n. このコマンドプロンプトで、PostgreSQL の `bin` ディレクトリに移動します。
例: `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
- o. データベースのバックアップファイル `alldbs.sql`（またはユーザーが付けたファイル名）を **bin** ディレクトリにコピーします。
- p. コマンドプロンプトで、次のコマンドを実行します: `psql -U postgres -f alldbs.sql`
- q. パスワードの入力を求められたら、`postgresql` パスワードを入力します。

注意

データベースサイズによっては、復元にしばらく時間がかかることがあります。

- r. 復元が完了したら、コマンドプロンプトのウィンドウを閉じます。
 - s. **Files Advanced PostgreSQL Administrator** を再び開き、ローカルデータベースサーバーに接続します。
 - t. **[データベース]** を選択します。
 - u. `acronisaccess_production` データベースを開き、**[スキーマ]**、**[Public]** の順に展開します。
テーブル の数が最初と同じであることを確認します。
8. **ゲートウェイサーバーデータベースの復元**
- 作成した `mobilEcho.sqlite3` ゲートウェイサーバーデータベースのバックアップファイルを新しいゲートウェイサーバーの `database` フォルダ（デフォルトでは `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`）にコピーし、既存のファイルと置き換えます。
9. **サーバーの構成**

注意

Acronis Cyber Files で使用される DNS 名は変更せず、ポイント先の IP アドレスのみを変更することをお勧めします。以下の手順では、Acronis Cyber Files の以前のインスタンスの DNS 名を再使用することを前提としています。

- a. 開いたままにしておいた Acronis Cyber Files 構成ユーティリティに戻り、ゲートウェイサーバー、Acronis Cyber Files サーバー、およびファイルリポジトリの設定を行います。
- b. **[適用]**、**[OK]** とクリックします。
- c. 次のダイアログで、**[OK]** をクリックします。Acronis Cyber Files Web インターフェースでブラウザが起動します。
- d. Accessサーバーにログインします。
- e. **[管理画面]** をクリックします。
- f. **[モバイルアクセス]** → **[ゲートウェイサーバー]** ページに移動します。
- g. ゲートウェイサーバーのリストに、使用しているゲートウェイサーバーが表示されます。
- h. ゲートウェイサーバーのアドレスが DNS エントリの場合は、この DNS エントリがサーバーマシンを指しているため、サーバーを変更する必要はありません。ゲートウェイのアドレスが IP アドレスの場合は、ゲートウェイサーバーの IP アドレスであることを確認します。

10. Acronis Cyber Files の管理設定の確認

データベースの復元が完了したら、続行する前に、Web インターフェースにサインインし、設定が正しく復元されていること、および設定が依然として適切なことを確認するよう強くお勧めします。確認する重要なアイテムの例を次に示します。

- 監査ログ: 新しい Acronis Cyber Files ログフォルダに、ログの書き込みに必要なすべてのアクセス権が設定されていることを確認します。
- 管理設定: すべての LDAP、SMTP、全般的な管理設定が正しいことを確認します。
- ゲートウェイサーバーとデータソース: 正しいアドレスでゲートウェイサーバーにアクセスできること、また、データソースのパスが有効であることを確認します。

新しい構成のテスト

移行が完了したら、いくつかの操作を実行して、すべて問題なく動作するか確認します。

- Web インターフェイスのナビゲーション操作を実行して、すべて問題なく動作するか確認します。設定が変更されていないことを確認します。
- Web インターフェースを介してファイルを Sync & Share セクションにアップロードします。セットアップしたその他のネットワークノードについても同じように実行します（もしあれば）。
- 移行前に存在した Sync & Share ファイルをダウンロードして、既存のファイルストアへの接続が動作することを確認します。
- デスクトップクライアントまたはモバイルクライアント（もしくはその両方）を使用して新しい構成に接続します。
- デスクトップクライアントまたはモバイルクライアント（もしくはその両方）からいくつかのファイルをアップロードおよびダウンロードします。

別のサーバーへの Acronis Cyber Files の移行

このガイドでは、既存の Acronis Cyber Files セットアップを新しいマシンに移行する方法について説明します。

重要

本番サーバーに移行する前に、テスト環境でこれらの手順を実行することを強くお勧めします。テスト環境は本番サーバーと同じアーキテクチャにするほか、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、本番環境との互換性を確保してください。

開始する前に

警告

本番環境外でのテストバックアップ/復元の実行を強くお勧めします。

現在の構成に関してメモする必要がある重要事項:

- Cyber Files Web サーバー、PostgreSQL、ゲートウェイとファイルリポジトリがすべて 1 台のコンピュータ上にありますか？
- Cyber Files Web サーバーの DNS、IP、ポートをメモします。
- ゲートウェイサーバーの DNS、IP、ポートをメモします。
- ファイルリポジトリのアドレスとポートをメモします。
- ファイルストアのロケーションをメモします。
- 現在のサーバーの PostgreSQL バージョン番号をメモします。

PostgreSQL のメインフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL）の中のフォルダ名（**9.2**、**9.3**、**9.4** など）が PostgreSQL のメジャーバージョン番号になっているので簡単に確認できます。

注意

これらの情報の大半は設定ユーティリティで確認できます。

移行プロセスの基本概要:

移行を開始する前に、これらの手順のすべてを実行する準備を整えておいてください。

1. 新しいサーバーマシンをポイントするように DNS エントリを変更します。
2. 現在のデータベースファイルと証明書をバックアップします。
3. データベースファイルと証明書を新しいマシンに移動します。
4. ファイルストアを移行します。
5. Acronis Cyber Files Web サーバーを新しいマシンにインストールします。
6. 証明書を新しいマシンに移動します。
7. データベースファイルを新しい Acronis Cyber Files Web サーバーのインストール環境に配置します。

8. 設定ユーティリティを使用して、新しい Acronis Cyber Files Web サーバーを起動します。
9. Acronis Cyber Files モバイルゲートウェイのアドレスが正しいことを確認します。
10. 新しい構成をテストします。

Acronis Cyber Files Web サーバーとゲートウェイデータベースの移行

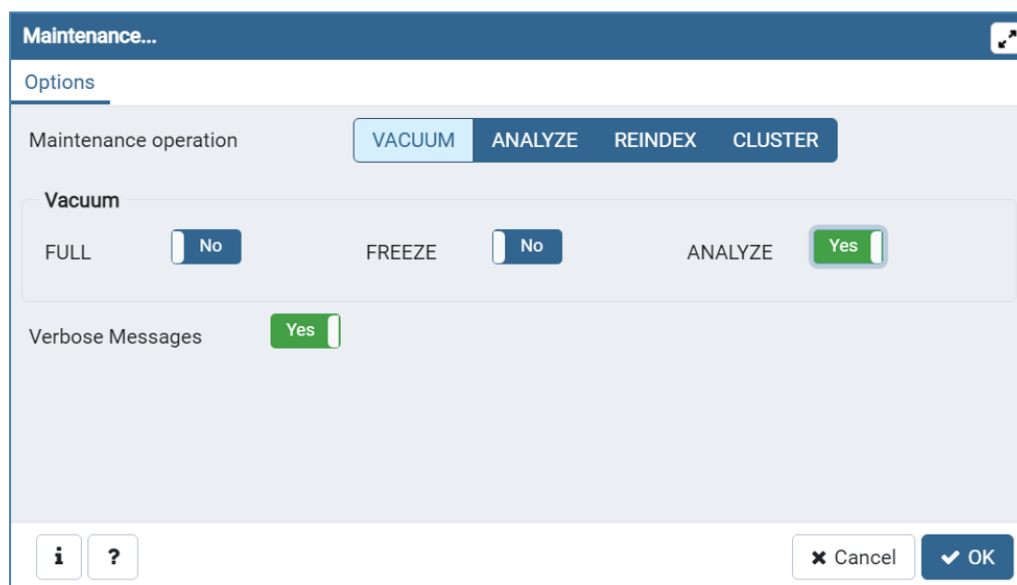
Tomcat/ゲートウェイ/PostgreSQL が現在稼働している元のサーバーで、次の手順を実行します。

注意

Acronis Cyber Files Web サーバーのデータベースが非常に大きい（数ギガバイト）場合には、別のバックアップおよび復元の方法が必要になることがあります。

ヘルプや手順については当社のテクニカルサポート（<https://support.acronis.com/mobility>）にお問い合わせください。

1. Acronis Cyber Files Tomcat サービスの停止
 - i. Acronis Cyber Files PostgreSQL 管理ツールを開きます。これは Windows の [スタート] メニューの [AcronisCyber Files] フォルダにあります。データベースサーバーに接続します。postgres ユーザーのパスワード入力を求められる場合があります。
 - ii. [データベース]を展開し、acronisaccess_productionデータベースを右クリックします。
 - iii. [メンテナンス]を選択します。
 - iv. [バキューム]を選択し、[分析]を[はい]に設定します。



- v. [OK] をクリックします。
- vi. データベース、[スキーマ]、[Public]の順に展開します。[テーブル]セクションの数字をメモします。これにより、復旧後にデータベースが正常に復元されたことを確認できます。
- vii. PostgreSQL Administrator ツールを閉じ、管理者特権でのコマンドプロンプトを開きます。

viii. このコマンドプロンプトで、PostgreSQLのbinディレクトリに移動します。

例: `cd "C:\Program Files(x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`

注意

注意: カスタムインストールまたは古いインストールを使用する場合には PostgreSQL bin フォルダを指すようにパスを編集する必要があります (例: `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\bin\`)。

ix. コマンド `pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql` を入力します。

- バックアップのファイル名は `alldbs.sql` になります。これは、PostgreSQL の bin ディレクトリに保存されます。別の場所に保存する必要がある場合は、上記のコマンド内でパスを使用できます。たとえば、コマンドの末尾を `--file D:\Backups\alldbs.sql` のように変更します。
- デフォルト以外のポートを使用している場合は、`5432` を正しいポート番号に変更します。
- デフォルトの PSQL 管理者アカウント `postgres` を使用していない場合は、上記コマンド内の `postgres` をご使用の管理者アカウント名に変更してください。
- この手順では、`postgres` ユーザーのパスワードを何回か入力するように求められます。そのたびにパスワードを入力してEnterキーを押してください。

注意

パスワードを入力しても、コマンドプロンプトウィンドウの視覚的な変化はまったくありません。

2. ゲートウェイサーバーのデータベースのバックアップ

- a. **AcronisCyber Files** ゲートウェイサービスを停止します。
- b. ゲートウェイサーバーのdatabaseフォルダに移動します。デフォルトでは次の場所にあります。

`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`

3. `mobilEcho.sqlite3` ファイルをゲートウェイサーバーのホストとなる新しいマシンにコピーします。

その他のバックアップ対象ファイル

以下のファイルで変更を加えたものがある場合は、Acronis Cyber Files 製品を復元または移行した際に設定を転送できるように、バックアップを作成しておくことをお勧めします。

`postgresql.conf` ファイル。このファイルには、データベース関連の重要な設定が含まれている場合があります。通常は、`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン>\Data` に配置されています。

- `web.xml`。デフォルトで `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\` に配置されています。シングルサインオンの設定が含まれています。
- `server.xml`。デフォルトで `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<バージョン>\conf` に配置されています。Tomcatの設定が含まれています。

- krb5.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<バージョン>\conf に配置されています。シングルサインオンの設定が含まれています。
- login.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-<バージョン>\conf に配置されています。
- Acronis Cyber Files に使用する証明書とキー。
- acronisaccess.cfg。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server に配置されています。
- カスタムカラススキーム。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\customizations\ に配置されています。
- pg_hba.conf。デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン>\Data に配置されています。
- newrelic.yml ファイル。Acronis Cyber Files サーバーの監視に **New Relic** を使用している場合。

Acronis Cyber Files サーバーのホストとなる新しいサーバー上で

Acronis Cyber Files のインストール

1. Acronis Cyber Files インストーラを起動して、**[次へ]** を押します。ライセンス契約を読み、承諾します。
2. **[インストール]** を選択し、インストーラ画面の指示に従います。

注意

Acronis Cyber Files Web サーバー、PostgreSQL、ゲートウェイを別々のマシンで実行している場合は、**[カスタム]** を選択して、目的のコンポーネントを選択します。

3. [PostgreSQL の構成] 画面で、元のサーバーで使用していたのと同じ PostgreSQL スーパーユーザー用パスワードを入力します。**[次へ]** を押します。
4. インストールされるコンポーネントを確認し、**[インストール]** を押します。
5. インストールが完了したら、**[終了]** を押します。次に設定ユーティリティを実行する旨のダイアログが表示されます。
6. 設定ユーティリティが表示されたら、**[OK]** も **[適用]** も押さずに開いたままにします。
7. **[サービス]** コントロールパネルを開いて、AcronisCyber Files Tomcat サービスを停止します。

注意

負荷分散構成では、すべての AcronisCyber Files Tomcat サービスを停止します。

8. AcronisCyber Files PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して acronisaccess_production という名前のデータベースがあることを確認します。
9. データベースを右クリックして、**[更新]** を選択します。
10. データベース、**[スキーマ]**、**[Public]** の順に展開して、**[テーブル]** に項目がないことを確認します。
 - データベースにテーブルがある場合は、データベースを右クリックして、名前を oldacronisaccess_production に変更します。最後に、**[データベース]** に移動し、右クリックし

て `acronisaccess_production` という名前の新しいデータベースを作成します。

11. PostgreSQL Administratorを閉じ、管理者特権でのコマンドプロンプトを開きます。
12. このコマンドプロンプトで、PostgreSQLのbinディレクトリに移動します。
例: `cd "C:\Program Files\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\bin"`
13. データベースのバックアップファイル `alldbs.sql`（またはユーザーが付けたファイル名）を **bin** ディレクトリにコピーします。
14. コマンドプロンプトで、次のコマンドを実行します: `psql -U postgres -f alldbs.sql`
15. `postgres` パスワードを求められたら入力します。

注意

データベースサイズによっては、復元にしばらく時間がかかることがあります。

16. 復元が完了したら、コマンドプロンプトのウィンドウを閉じます。
17. **Files Advanced PostgreSQL Administrator**を再び開き、ローカルデータベースサーバーに接続します。
18. **[データベース]** を選択します。
19. `acronisaccess_production` データベースを開き、**[スキーマ]**、**[Public]** の順に展開します。**テーブル**の数が元のサーバーと同じであることを確認します。

注意

データベースを復元する Acronis Cyber Files Web サーバーのバージョンが、データベースバックアップからの Acronis Cyber Files Web サーバーのバージョンより新しく、Acronis Cyber Files Tomcat サービスが既に開始されている場合、新しい Acronis Cyber Files Web サーバーデータベース内のテーブル数がバックアップ実行時のテーブル数より多くなる可能性があります。

ゲートウェイサーバーデータベースの復元

古いサーバーに付属していた `mobliEcho.sqlite3` ゲートウェイサーバーデータベースを新しいゲートウェイサーバーのデータベースフォルダ（デフォルトで `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Gateway Server\database`）にコピーして既存のファイルを置き換えます。

新しいサーバーの設定

注意

Acronis Cyber Files が使用する DNS 名は変更せずに、それらが指している IP アドレスのみを変更することを強くお勧めします。以下の手順では、Acronis Cyber Files の以前のインスタンスの DNS 名を再使用することを前提としています。

1. 開いたままにしておいた Acronis Cyber Files 構成ユーティリティに戻り、ゲートウェイサーバー、Acronis Cyber Files サーバー、およびファイルリポジトリの設定を行います。
2. **[適用]**、**[OK]** とクリックします。次のダイアログで **[OK]** をクリックすると、Acronis Cyber Files Web インターフェースを持つブラウザが起動します。
3. Accessサーバーにログインします。

4. **[管理画面]** をクリックします。**[モバイルアクセス]** → **[ゲートウェイサーバー]** ページに移動します。
5. ゲートウェイサーバーのリストに、使用しているゲートウェイサーバーが表示されます。
6. ゲートウェイサーバーのアドレスが DNS エントリの場合は、この DNS エントリが新しいサーバーマシンを指しているため、サーバーを変更する必要はありません。ゲートウェイのアドレスが IP アドレスの場合は、ゲートウェイサーバーを編集する必要があります。

Acronis Cyber Files の管理設定の確認

データベースの復元が成功したら、他の操作を行う前に Web インターフェースにログインし、設定が引き継がれたこと、および設定が依然として適切なことを確認するよう強くお勧めします。確認する重要なアイテムの例を次に示します。

- 監査ログ: 新しい Acronis Cyber Files ログフォルダに、ログの書き込みに必要なすべてのアクセス権が設定されていることを確認します。
- New Relic: New Relicを使用している場合は、`newrelic.yml` ファイルを古いマシンから新しいコンピュータへとコピーし、Acronis Cyber Files Web インターフェイスがこのファイルをポイントしていることを確認します。
- 管理設定: すべての LDAP、SMTP、全般的な管理設定が正しいことを確認します。
- ゲートウェイサーバーとデータソース: 正しいアドレスでゲートウェイサーバーにアクセスできること、また、データソースのパスが有効であることを確認します。

新しい構成のテスト

新しいサーバーの設定が完了したら、いくつかの簡単な操作を実行して、すべて順調に機能するか確認します。

- ウェブインターフェイスのナビゲーション操作を実行して、すべて問題なく動作するか確認します。設定が変更されていないか確認します。
- ウェブインターフェイスから **[同期・共有]** セクションにファイルをアップロードします。また、ネットワークノードを設定した場合には、そのすべてに対して同様の操作を実行します。
- デスクトップクライアントとモバイルクライアントアプリケーションを使用して新しいサーバーに接続します。
- デスクトップクライアントまたはモバイルクライアント（もしくはその両方）からいくつかのファイルをアップロードおよびダウンロードします。

元のサーバーのクリーンアップ

新しいサーバーが正常に稼働していることを確認した後、古いサーバーを再度使用する予定がない場合には、古いマシンから Acronis Cyber Files をアンインストールすることをお勧めします。

Acronis Cyber Files インストーラを開き、ライセンス契約に同意して **[アンインストール]** をクリックします。すべてのコンポーネントを選択し、**[アンインストール]** を押します。これで、すべての Acronis Cyber Files コンポーネントがマシンから削除されます。

注意

Acronis Cyber Files インストーラがない場合は、コントロールパネルを開き、Acronis Cyber Files PostgreSQL サーバー、Acronis Cyber Files ゲートウェイサーバー、Acronis Cyber Files File Repository サーバー、Acronis Cyber Files Web サーバー、Acronis Cyber Files 設定コレクションツール、Acronis Cyber Files 設定ユーティリティ、および LibreOffice をアンインストールします。

- PostgreSQLサーバーの**データ**ディレクトリは自動的に削除されません。デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\ に配置される PostgreSQL ディレクトリ全体を手動で削除します。

注意

古いインストールまたはカスタムインストールを使用している場合は、このパスを編集する必要があります（例: C:\Program Files\Acronis\Access\Common\PostgreSQL\）。

- Acronis Cyber Files Web サーバー用にインストールされた Java を削除することもできます。Java もコントロールパネルから削除できます。

PostgreSQL の新しいメジャーバージョンへのアップグレード

PostgreSQL のメジャーリリースでは、PostgreSQL の一部の内部動作を変える新機能が追加されることが多くあります。

単一サーバーのインストールでは、[同一サーバーの移行の手順](#)をすべて使用できます。

重要

Acronis Cyber Files では、Cyber Files インストーラを使用した PostgreSQL のアップグレードのみがサポートされています。公式の PostgreSQL の配布はサポートされていません。出荷されたバージョン以外はサポートされていません。

注意

PostgreSQL のアップグレードは、時間のかかるプロセスになる場合があります。

重要

本番環境外でのテストアップグレードの実行を**強く**おすすめします。

補足資料

ソフトウェアの競合

Acronis Cyber Files で問題となる可能性があるソフトウェア製品がいくつかあります。現在確認されている競合は次のとおりです。

- **VMware View™ Persona Management:** このアプリケーションは、Acronis Cyber Files デスクトップクライアントの同期プロセスおよびファイルの削除で問題となります。Acronis Cyber Files 同期フォルダを **Persona Management ユーザー プロファイル**の外に配置すると、この既知の競合を避けることができます。
- **ウイルス対策ソフトウェア**で同期フォルダをスキャンしないでください。同期プロセスと競合する場合があります。Acronis Cyber Files の Filestore フォルダをウイルス対策の無視または許可リストに追加することをお勧めします。暗号化をオフにしない限り、Filestore フォルダの項目がすべて暗号化されるため、ウイルス対策ソフトウェアは何も検出できませんが、一部の項目で問題が発生することがあります。

Acronis Cyber Files サーバーの場合

Acronis Cyber Files の負荷分散

Acronis Cyber Files を負荷分散する方法は 2 つあります。

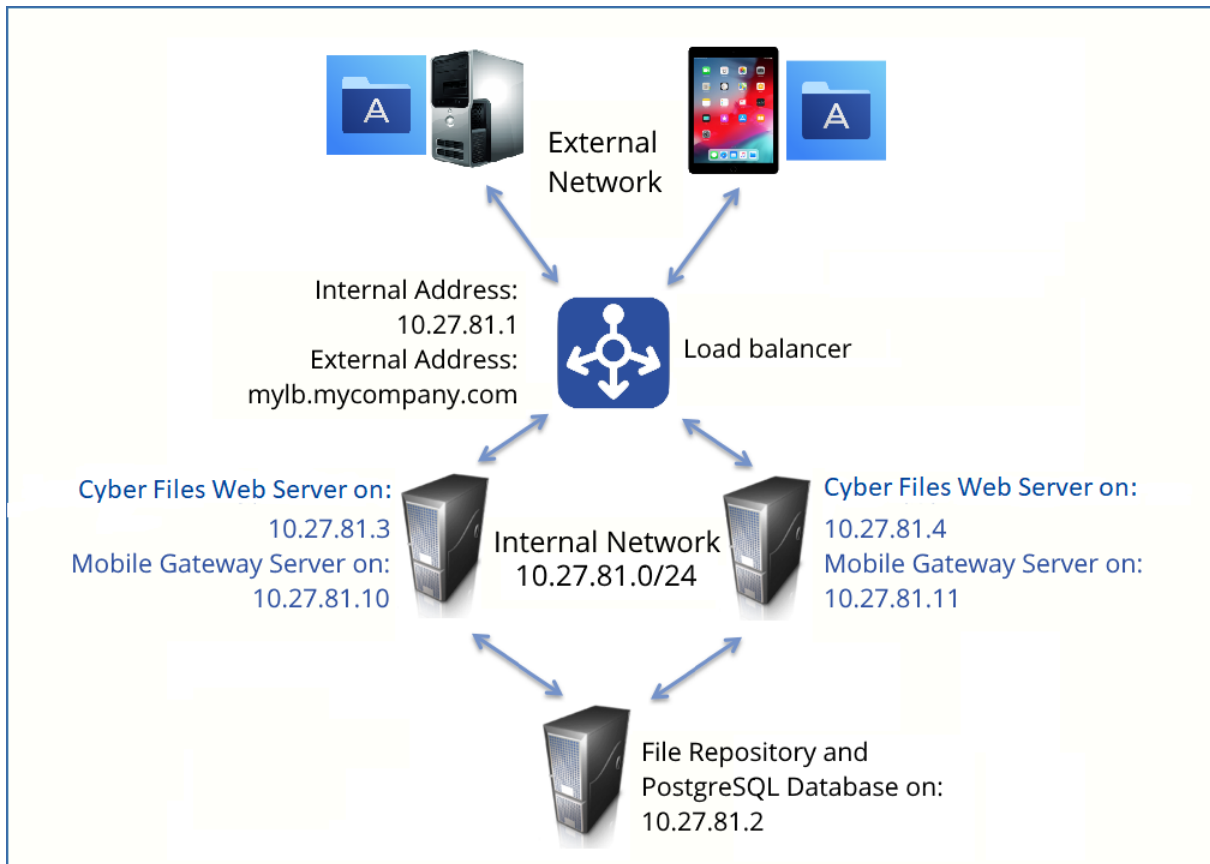
Acronis Cyber Files モバイルゲートウェイのみ負荷分散する

この設定によって、負荷が最も高くなる Acronis Cyber Files モバイルゲートウェイサーバーのコンポーネントが負荷分散され、モバイルクライアントは常時アクセス可能な状態になります。管理対象外のアクセスに対して Acronis Cyber Files モバイルゲートウェイに接続する必要がない場合は、Acronis Cyber Files サーバーは負荷分散装置の背後に配置されません。詳細については、「[クラスターグループ](#)」の記事を参照してください。

すべての Acronis Cyber Files の負荷分散

この設定によって、Acronis Cyber Files のコンポーネントのすべてが負荷分散され、すべてのユーザーに対して高可用性が確保されます。この設定をテストするには、2 つ以上のマシンが必要になります。負荷分散の設定時の設定項目の多くは、ソフトウェアやハードウェアにより異なるため、このガイドでは説明しません。

この設定例では、3 つのマシンを使用します。1 つはファイルリポジトリおよびデータベースとして機能し、他の 2 つは Acronis Cyber Files Web サーバーおよび Acronis Cyber Files モバイルゲートウェイとして機能します。この設定の構成方法について以下に示します。



このガイドでは、ご使用の環境で Acronis Cyber Files 製品を適切に負荷分散するために必要な詳細情報について説明します。

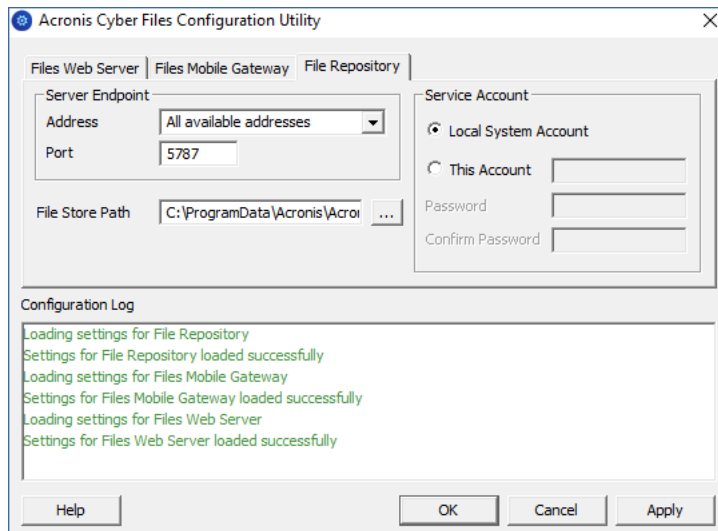
PostgreSQL データベースおよびファイル リポジトリをホストするサーバーの場合、次の手順を実行します。

1. Acronis Cyber Files インストーラを起動して、**[次へ]** を押します。ライセンス契約を読み、承諾します。
2. Acronis Cyber Files インストーラで **[カスタム]** を選択し、**[Acronis Cyber Files ファイル リポジトリ]** と **[PostgreSQL Database Server]** を選択して **[次へ]** を押します。
3. ファイル リポジトリと設定ユーティリティをインストールする場所を選択します。
4. PostgreSQL をインストールする場所を選択し、スーパーユーザー (**postgres**) のパスワードを入力します。
5. TCP ポート 5432 を開きます。このポートは、リモート マシンから PostgreSQL データベースにアクセスする際に使用されます。
6. インストール手順が完了したら、**設定ユーティリティ** で設定を続行します。
 - a. 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。
 - b. アクセスできるようにするファイル リポジトリのアドレスとポートを選択します。

注意

Acronis Cyber Files Web インターフェースで同じアドレスとポートを設定する必要があります。詳細については、「[設定ユーティリティの使用](#)」および「[ファイル リポジトリ](#)」の記事を参照してください。

- c. ファイルストアへのパスを選択します。このパスに実際のファイルが保存されます。



- d. [OK] をクリックして変更を適用し、**設定ユーティリティ**を閉じます。

7. PostgreSQL インストールディレクトリ（例: C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\data\）に移動し、テキストエディタで **pg_hba.conf** を編集します。

8. 内部アドレスを使用してそれぞれの Acronis Cyber Files サーバーにホストエントリを追加し、ファイルを保存します。**pg_hba.conf**（HBA はホストベース認証の略）ファイルではクライアント認証が制御されます。データベースクラスターのデータディレクトリにファイルが保存されます。このファイルで、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

データベースユーザーのアドレスメソッドを入力

最初の Acronis Cyber Files ゲートウェイサーバー

```
host all all 10.27.81.3/32 md5
```

2 番目の Acronis Cyber Files ゲートウェイサーバー

```
host all all 10.27.81.4/32 md5
```

これらの例では、最初の Acronis Cyber Files サーバー(10.27.81.3/32)と2番目の Acronis Cyber Files サーバー(10.27.81.4/32)から接続するすべてのユーザーが、md5暗号化接続を介してレプリケーション権限を除くすべての権限でデータベースにアクセスできます。

9. PostgreSQL インスタンスへのリモートアクセスを可能にするには、**postgresql.conf** ファイルを編集する必要があります。以下の手順を実行してください。

- a. 移動して、**postgresql.conf**を開きます。これは、デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<VERSION>\Data\postgresql.conf に配置されています。

- b. #listen_addresses = 'localhost' という行を探します。

- c. 行の先頭にある「#」記号を削除してコマンドを有効にします。
 - d. 利用可能なアドレスすべてをリッスンするために、「localhost」を「*」に置き換えます。
PostgreSQLで特定のアドレスのみをリッスンするには、「*」のかわりにIPアドレスを入力します。
 - 例listen_addresses = '*' - PostgreSQL が利用可能なすべてのアドレス上でリッスンすることを意味します。
 - 例listen_addresses = '192.168.1.1' - PostgreSQL がそのアドレス上でのみリッスンすることを意味します。
 - e. postgresql.confに加えた変更を保存します。
 - f. Acronis Cyber Files PostgreSQL サービスを再起動します。
10. **Acronis Cyber Files PostgreSQL Administrator ツール**を開きます。これは Windows の [スタート] メニューの [Acronis Cyber Files] フォルダにあります。ローカルサーバーに接続して、**[データベース]**を選択します。右クリックするか、**[編集]** → **[新規オブジェクト]** のメニューから **[新規データベース]** を選択して新しいデータベースを作成します。「acronisaccess_production」という名前を付けます。

注意

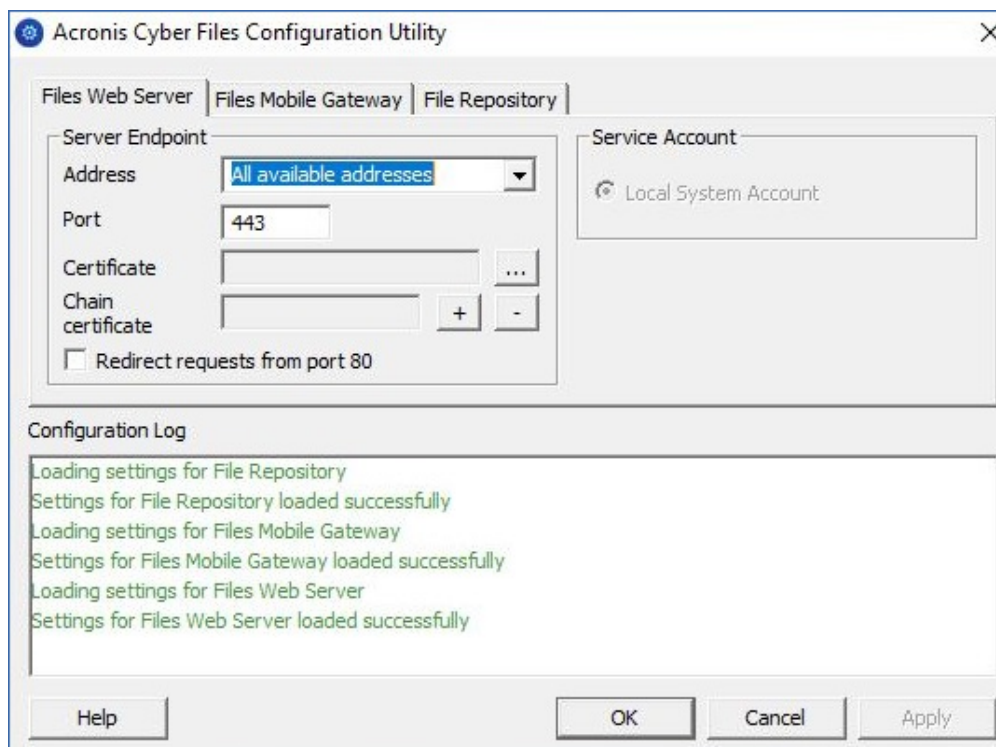
PostgreSQL は、デフォルトでポート 5432 を使用します。使用するすべてのファイアウォールまたはルーティングソフトウェアでこのポートが開放されていることを確認してください。

Acronis Cyber Files サーバーと Acronis Cyber Files ゲートウェイの両方として機能する 2 つのサーバーで、次の手順を実行します。

1. Acronis Cyber Files インストーラを起動して、**[次へ]** を押します。ライセンス契約を読み、承諾します。
2. Acronis Cyber Files インストーラで、**[カスタム]** を選択し、**[Acronis Cyber Files Web サーバー]** と **[Acronis Cyber Files モバイルゲートウェイ]** のみを選択して、インストール手順を続行します。
3. インストール手順が完了したら、**設定ユーティリティ**で設定を続行します。
 - a. 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。
 - b. **[AcronisCyber Files Web サーバー] タブ**で次の操作を実行します。
 - アクセスできるようにする Acronis Cyber Files 管理サーバーのアドレスとポートを入力します（例: 10.27.81.3 および 10.27.81.4）。
 - 証明書を選択します。負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものを選択する必要があります。
 - **[適用]** をクリックします。

注意

証明書がない場合は、Acronis Cyber Files によって自己署名証明書が作成されます。この証明書は実働環境では使用しないでください。

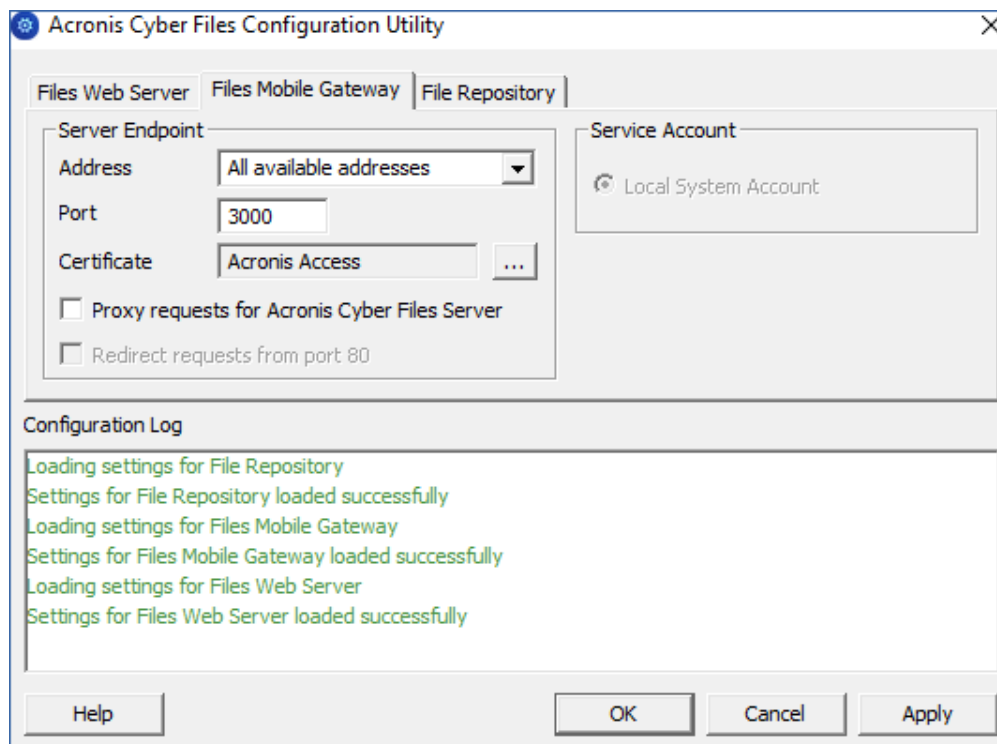


c. **[Acronis Cyber Files モバイルゲートウェイ] タブ**で次の操作を実行します。

- アクセスできるようにするゲートウェイ サーバーのアドレスとポートを入力します（例: 10.27.81.10 および 10.27.81.11）。
- 証明書を選択します。負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものを選択する必要があります。
- **[適用]** をクリックします。

注意

証明書がない場合は、Acronis Cyber Files によって自己署名証明書が作成されます。この証明書は実働環境では使用しないでください。



4. Acronis Cyber Files インストールディレクトリ（例: C:\Program Files (x86)\Acronis\Files Advanced\Access Server\）に移動し、テキストエディタで **acronisaccess.cfg** を編集します。
5. ユーザー名、パスワード、PostgreSQL データベースを実行するサーバーの内部アドレスを設定し、ファイルを保存します。これにより、Acronis Cyber Files サーバがリモートの PostgreSQL データベースに接続するよう設定されます。たとえば、次のように設定します。

```
DB_DATABASE =acronisaccess_production
DB_USERNAME =postgres
DB_PASSWORD =password123
DB_HOSTNAME =10.27.81.2
DB_PORT =5432
```

6. Services.msc を開き、Acronis Cyber Files サービスを再起動します。

Acronis Cyber Files Web サーバーまたは Acronis Cyber Files モバイルゲートウェイのいずれかで、次の手順を実行します。

これは最初に設定するサーバーです。このサーバーの設定は、他のすべてのサーバーにわたって複製されます。設定が複製されると、すべてのサーバーは同じ設定になります。どのサーバーを選択したかは問われません。

1. Services.msc を開き、**Acronis Cyber Files Tomcat** サービスを再起動します。作成したデータベースが使用されます。
2. ウェブブラウザで <https://myaccess>（例: <https://10.27.81.3>、<https://10.27.81.4> など）にアクセスして、[設定ウィザード](#)を完了します。
 - a. **[ライセンス] タブでの作業:**
 - 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、**[続行]** を押します。

b. **[全般設定] タブでの作業:**

- [サーバー名] にサーバー名を入力します。
- [ウェブ アドレス] には負荷分散装置の外部アドレスを指定してください（例: mylb.company.com）。ポート 443 を使用していない場合は、ポートも入力する必要があります。
- [クライアント登録アドレス] には負荷分散装置の外部アドレスを指定してください（例: mylb.company.com）。
- カラー スキームを選択します。
- 監査ログ メッセージの言語を選択します。

c. **[SMTP] タブでの作業:**

- SMTP サーバーの FQDN または IP アドレスを入力します。
- SMTP サーバーのポートを入力します。
- 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。
- サーバーから送信される E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。
- サーバーから送信される Eメールのアドレスを入力します。
- 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、**[SMTP 認証を使用しますか?]** をチェックし、認証情報を入力します。
- **[保存]** をクリックします。

d. **[LDAP] タブでの作業:**

- **[LDAPを有効にしますか?]** をチェックします。
- LDAP サーバーの FQDN または IP アドレスを入力します。
- サーバーの LDAP ポートを入力します。
- 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?]** をオンにします。
- LDAP の資格情報をドメインも含めて入力します（例: mycompany¥myname）。
- LDAP 検索ベースを入力します。
- LDAP 認証のドメインを入力します。（たとえば、「joe@glilabs.com」という EメールアカウントのLDAP認証を有効にするには、「glilabs.com」と入力します）。
- **[保存]** をクリックします。

e. **[ローカルゲートウェイ] タブでの作業:**

注意

同じマシンに Files Advanced モバイルゲートウェイと Acronis Cyber Files Web サーバーの両方をインストールする場合、ゲートウェイが自動的に検出され、Acronis Cyber Files Web サーバーに管理されます。

- 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。これは、負荷分散装置の背後の内部アドレスです（例: 10.27.81.10）。
- **[保存]** をクリックします。

f. **[ファイルリポジトリ] タブでの作業:**

- ファイル リポジトリのアドレスには、ファイル リポジトリの役割として作成したサーバーの内部アドレスを指定する必要があります（例: 10.27.81.2）。
3. 設定ウィザードの設定が完了したら、**[完了]** を押し、**[モバイルアクセス]** → **[ゲートウェイサーバー]** に移動します。
 4. 次に 2 つ目のゲートウェイ サーバーを登録します。
 - a. 2 つ目のゲートウェイの**表示名**を入力します。
 - b. **[管理のアドレス]** には、負荷分散装置の背後の内部アドレスを指定する必要があります（例: 10.27.81.11）。
 - c. **[管理キー]** を入力します。管理キーを取得するには、追加するゲートウェイがインストールされているマシンで <https://mygateway:443>（例: <https://10.27.81.10>、<https://10.27.81.11> など）にアクセスして、キーを表示します。詳細については、「新しいゲートウェイサーバーの登録」の記事を参照してください。
 - d. **[保存]** をクリックします。
 5. クラスターグループを作成し、すべてのゲートウェイ サーバーを追加します。プライマリ サーバーは、設定ウィザードが完了しているサーバーにする必要があります。詳細については、「クラスターグループ」の記事を参照してください。

注意

先に進む前に、各ゲートウェイ上で正しい管理用アドレスが構成済みであることを確認してください。これは、ゲートウェイ サーバーの DNS アドレスまたは IP アドレスです。

- a. **[モバイル アクセス]** タブを展開します。
- b. **[ゲートウェイ サーバー]** ページを開きます。
- c. **[クラスターグループの追加]** ボタンをクリックします。
- d. グループの表示名を入力します。
- e. 負荷分散装置の内部の FQDN または IP アドレスを入力します（例: 10.27.81.1）。
- f. グループに含めるそれぞれのゲートウェイのチェックボックスにマークを付けます。
- g. グループの設定を制御するゲートウェイを選択します。最初に設定したゲートウェイを選択してください。そのゲートウェイ上の既存の設定のすべて（割り当てられているデータ ソースは含まれますが、管理のアドレスは含まれません）が、グループ内の各ゲートウェイにコピーされます。

負荷分散装置での作業:

1. 負荷分散装置で時間ベースのセッション スティッキネス（またはご使用の負荷分散装置での同等の設定）を有効にし、期限切れにならないように設定します。
2. ヘルスチェック（HTTP ステータス 200 が返されることを確認する）が必要な場合は、<https://INTERNALSERVERNAME:MANAGEMENTPORT/signin> に ping を送信することで可能です（例: <https://myaccessserver1.company.com/signin> および <https://myaccessserver2.company.com/signin>）。

ブラウザで <https://mylb.company.com> を開き、設定が機能していることを確認します。

負荷分散型セットアップでの Acronis Cyber Files のインストール

このガイドは、負荷分散型セットアップの要件および負荷分散環境への Acronis Cyber Files 導入に伴うプロセスに関する一般的な概要として提供されています。実際のセットアップはここに記載する例と異なる場合がありますが、コンポーネントが相互作用する方法は同じです。

推奨される構成は、Acronis Cyber Files サーバーを個々のパーツに分けて、各パーツを負荷分散装置の背後にある個別のマシンに配置するという構成です。ファイルリポジトリとファイルストアは同じマシン上に配置できます。

これらの手順は、テスト環境で実行することを強くおすすめします。テスト環境は予定されている本番のセットアップと同じアーキテクチャにするほか、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、使用する環境との互換性を確保してください。

システム要件

ハードウェア要件

本番環境では、少なくとも 3 台の Acronis Cyber Files Tomcat サーバーと 3 台のゲートウェイサーバーを使用することをお勧めします。このようにすると、いずれかのサーバーで障害が発生したとしても、他の 2 台のアクティブサーバーで負荷を分散できます。

注意

このセットアップ案では、これらのサーバーが仮想マシンサーバー上でホストされることが前提となります。複数のサーバーを使用する場合、ゲスト仮想マシン間では低レイテンシの相互接続をおすすめします。

- Acronis Cyber Files Web サーバー用の 1 台の負荷分散装置。
- Acronis Cyber Files ゲートウェイサーバー用の 1 台の負荷分散装置。
- 3 Acronis Cyber Files Tomcat サーバー（それぞれ 32 GB の RAM と 16 コアの CPU を搭載したもの）。
- 3 Acronis Cyber Files ゲートウェイサーバー（それぞれ 8 GB の RAM と 4 コアの CPU を搭載したもの）。

注意

ゲートウェイサーバーでは、CPU またはメモリよりもディスクおよびネットワーク速度の方が重要になります。

- PostgreSQL サーバー用に1台（32GB の RAM と16コアの CPU を搭載したもの）。
- ファイルリポジトリサービスおよびファイルストア用に 1台。このサーバーのパラメータはそれほど重要ではありません。

ネットワーク接続

- Acronis Cyber Files Tomcat サーバー用の負荷分散装置が現在の Acronis Cyber Files サーバーの DNS アドレスを使用するように構成する必要があります。
- ゲートウェイサーバー用の負荷分散装置が現在のゲートウェイサーバーの DNS アドレスを使用するように構成する必要があります。
- Tomcat サーバーをゲートウェイ負荷分散装置に接続して、デスクトップネットワークノードを同期し、ウェブインターフェイス上のネットワークノードを参照できるようにします。このクラスターセットアップでは、Acronis Cyber Files Web UI の [管理] ページと [ゲートウェイサーバー] ページの [クライアント接続用アドレス] は、外部負荷分散装置のアドレスになります。ゲートウェイサーバーにも、[Acronis Cyber Files サーバー接続に代替アドレスを使用] 設定を使用し、[Acronis Cyber Files Web サーバー接続用アドレス] にゲートウェイ負荷分散装置の内部アドレスを設定しています。
- モバイルクライアント接続に対応するために、ゲートウェイサーバーを Tomcat 負荷分散装置に接続します。

注意

Sync&Share データソースについて、アドレスを Tomcat 負荷分散装置のアドレスに変更する必要があります。

PostgreSQL のインストールと構成

PostgreSQL サーバーコンポーネントのインストール

1. Acronis Cyber Files インストーラを起動して、**[次へ]** を押します。ライセンス契約を読み、承諾します。
2. **[カスタム]** をクリックし、PostgreSQL Database Server だけを選択します。**[次へ]** を押します。
3. PostgreSQL をインストールする場所を選択し、スーパーユーザー (postgres) のパスワードを入力して、**[次へ]** を押します。
4. **[ファイアウォールでポート 5432 を開く]** を選択します。このポートを、PostgreSQL データベースにリモートからアクセスするために使用します。
5. インストールを終了します。

Tomcat サーバーの接続許可

1. インストールが完了したら、PostgreSQL **data** フォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<version>\Data）に移動して、テキストエディタで pg_hba.conf を開きます。
2. Acronis Cyber Files Tomcat サーバーそれぞれのホストエントリを、内部アドレスを使用して組み込み、ファイルを保存します。

pg_hba.conf（HBA はホストベース認証を表す）ファイルは、クライアント認証を制御するもので、データベースクラスターのデータディレクトリに保存されます。このファイル内に、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

```
# TYPE DATABASE USER ADDRESS METHOD
# Loadbalancer1(最初のAcronis Cyber FilesおよびGatewayサーバー)
host acronisaccess_production postgres 10.144.70.247/32 md5
```

注意

この例では、postgres という名前のユーザーアカウントが md5 encrypted 接続を介して、10.144.70.247 にあるサーバーから接続し、完全な権限（レプリケーション権限を除く）で acronisaccess_production データベースにアクセスできます。

適切な接続数のセットアップ

1. max_connections を探して 510 に変更します。
2. 行 #listen_addresses = 'localhost'. から先頭の # を削除します。localhost を * に置き換えます。変更後は、listen_addresses = '*' となるはずです。
3. 行 #effective_cache_size = 128MB から先頭の # を削除し、**128MB** を **12GB** に置き換えます。変更後は、effective_cache_size = 12GB となるはずです。
4. 以下の注釈を追加します。-#NOTE: this tuning setting assumes that PostgreSQL is running by itself on a #VM with at least 16 GB RAM. More information at https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server
5. すべての変更を保存して、**postgresql.conf** ファイルを閉じます。
6. Acronis Cyber Files PostgreSQL サーバーサービスを再起動します。

Acronis Cyber Files サーバーのインストール

Acronis Cyber Files Web サーバーのみのインストール

1. Acronis Cyber Files インストーラを起動し、ライセンス契約に同意します。
2. **[カスタム]** を選択し、Acronis Cyber Files Tomcat サーバーのみを選択します。

注意

Tomcat サーバーをクリックすると自動的に PostgreSQL サーバーも選択されますが、クリックして選択を解除できます。

3. インストールを完了し、Acronis Cyber Files Tomcat サービスが停止していることを確認します。

サーバーの設定

Acronis Cyber Files Web サーバーで変更したすべての設定は、その他すべての Acronis Cyber Files Web サーバーでも同じ変更を行う必要があります。

注意

pg_hba.conf ファイルに各 Acronis Cyber Files Web サーバーのエントリを追加することを忘れないでください。

適切なデータベースに接続するようサーバーを構成する

1. Acronis Cyber Files Web サーバーフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Access Server）に移動して、acronisaccess.cfg ファイルを開きます。このファイルは、サーバーに PostgreSQL データベースサービスの場所を指示します。

2. 以下の値を設定します。

DB_HOSTNAME =10.144.70.248

DB_PORT =5432

DB_POOLSIZE =250

注意

DB_HOSTNAME は、PostgreSQL が現在実行されている IP アドレスです。この例では、10.144.70.248 となっています。

注意

DB_POOLSIZE を 250 以上に設定することをお勧めします。

3. ファイルを保存します。

最大スレッド数の構成

Tomcat の負荷分散型セットアップでは、すべての Tomcat インスタンスによって生成される可能性のあるスレッドの合計数が、PostgreSQL データベースで受け入れるように構成された最大接続数を超えないようにすることが重要です。

スレッドの合計数を決定する重要な 3 つの設定は、以下のとおりです。

- acronisaccess.cfg ファイルでは、DB_POOLSIZE = 200 です。250 以上の値に設定することをお勧めします。
- Tomcat server.xml ファイルでは、maxThreads = 150 です。この設定は、デフォルトの 150 のままにすることをお勧めします。
- postgresql.conf ファイルでは、max_connections です。この設定は、前の手順で構成済みになっているはずです。この設定の値は、すべての Acronis Cyber FilesWeb サーバーに設定されている Tomcat のすべての DB_POOLSIZE 値の合計に 10 を足した値以上でなければなりません。たとえば、Tomcat サーバーが 2 台の場合は 510、3 台の場合は 760 となります。

注意

これらのファイルに変更を加えた場合、対応するサービスを再起動する必要があります。

適切なロギングの構成

負荷分散構成では、Acronis Cyber Files Tomcat サービスによる IP アドレスのマッピングがログ内で適切に行われません。各接続が適切にログに記録されるよう、以下の変更を行う必要があります。

1. server.xml ファイルで、<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" prefix="localhost_access_log." suffix=".txt" pattern="%h %l %u %t

"%r" %s %b"/> という行を探します。

2. 行の末尾に requestAttributesEnabled="true" を追加します。
3. 同じ行の下に、以下を追加します。

```
<Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
```

4. ファイルを保存し、Acronis Cyber Files Tomcat サービスを再起動します。

ゲートウェイサーバーのインストール

新しいゲートウェイサーバーのインストール

1. 新しいマシン上で、Acronis Cyber Files インストーラを実行し、ライセンス契約に同意します。
2. **[カスタム]** を選択し、ゲートウェイサーバーコンポーネントのみをインストールします。インストールを終了します。
3. 設定ユーティリティで、ゲートウェイのアドレス、ポート、証明書を設定します。設定する証明書は、ゲートウェイ負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものでなければなりません。

ファイルストアとファイルリポジトリの設定

S3 ストレージを使用する予定の場合、選択する S3 ストレージ内でファイルストアがホストされることになるため、ファイルリポジトリサービスをインストールする必要はありません。

ファイルリポジトリサービスのインストール

1. Acronis Cyber Files インストーラを、ファイルリポジトリとファイルストアを配置するマシンにコピーします。
2. インストーラを起動し、ライセンス契約に同意してから、**[カスタム]** を選択します。
3. **[ファイルリポジトリ]** オプションのみを選択して、**[次へ]** を押します。
4. 目的のインストールパスを選択してから **[次へ]** を押します。
5. インストールが完了するまで、画面の指示に従います。
6. 設定ユーティリティが起動します。ファイルリポジトリサービスにアクセスするためのアドレスとポートを選択します。
7. ファイルストアのインストール先を選択します。デフォルトの場所は C:\ProgramData\Acronis\Acronis Cyber Files\FileStore です。

注意

ファイルストアがリモートネットワーク共有にある場合は、ファイルリポジトリサービスが実行されているコンピューターまたはユーザーアカウントに、ネットワーク共有のファイルストアフォルダに対する完全なアクセス権が必要です。

注意

このアカウントには、ログファイルを書き込むため、ローカルリポジトリフォルダ（たとえば、C:\Program Files (x86)\Acronis\Acronis Cyber Files\File Repository\Repository）への読み取り/書き込みアクセス権限も必要です。

8. Acronis Cyber Files ファイルリポジトリサービスを起動します。

Acronis Cyber Files の設定

1. Acronis Cyber Files Web インターフェースを開き、管理者としてログインします。
2. [共有・同期] -> [ファイルリポジトリ] に移動し、[ファイルストアリポジトリエンドポイント] に設定ユーティリティで選択したアドレスと同じアドレスが設定されていることを確認します。

負荷分散装置固有の設定

1. ブラウザで <https://mylb.company.com> を開き、設定が機能していることを確認します。
2. 負荷分散装置で時間ベースのセッションスティックネス（またはご使用の負荷分散装置での同等の設定）を有効にし、期限切れにならないように設定します。
3. ヘルスチェック（HTTP ステータス 200 が返されることを確認する）が必要な場合は、
https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version に ping します
（例: <https://myaccessserver.company.com/signin> および
https://myaccessserver.company.com/api/v1/server_version）。
4. 負荷分散型セットアップで IP アドレスと接続が適切にログに記録されるようにするには、負荷分散装置を構成して以下のヘッダーを設定する必要があります。
 - X-Forwarded-For: これにより、各接続で負荷分散装置の IP アドレスが表示される代わりに、接続しているクライアントの実際の IP アドレスが表示されるようになります。
 - X-Forwarded-Proto: これにより、実際に使用されているプロトコルが表示されます。

負荷分散構成への移行

このガイドは、負荷分散型セットアップおよび負荷分散環境への移行に伴うプロセスに関する一般的な概要として提供されています。実際のセットアップはここに記載する例と異なる場合がありますが、コンポーネントが相互作用する方法およびコンポーネントの設定は同じです。

推奨される構成は、Acronis Cyber Files サーバーを個々のパーツに分けて、各パーツを負荷分散装置の背後にある個別のマシンに配置するという構成です。ファイルリポジトリとファイルストアは同じマシン上に配置できます。

本番サーバーに移行する前に、テスト環境でこれらの手順を実行することを強くお勧めします。テスト環境は本番サーバーと同じアーキテクチャにするほか、テスト用のユーザーデスクトップとモバイルクライアントをいくつか用意して、使用する環境との互換性を確保してください。

このガイドでは例として、すべてのコンポーネントがマシン上にインストールされた、標準的な導入環境で動作する Acronis Cyber Files のセットアップを使用します。

注意

この例では、元の Acronis Cyber Files Tomcat サービスを引き続き実行し、このサービスを新しい構成に接続します。このステップは必須ではありません。

導入環境に変更を加える前に、「[バックアップと復旧](#)」の記事を参照してください。

システム要件

ハードウェア要件

本番環境では、少なくとも 3 台の Acronis Cyber Files Tomcat サーバーと 3 台のゲートウェイサーバーを使用することをお勧めします。このようにすると、いずれかのサーバーで障害が発生したとしても、他の 2 台のアクティブサーバーで負荷を分散できます。

注意

このセットアップ案では、これらのサーバーが仮想マシンサーバー上でホストされることが前提となります。複数のサーバーを使用する場合、ゲスト仮想マシン間では低レイテンシの相互接続をおすすめします。

- Acronis Cyber Files Web サーバー用の 1 台の負荷分散装置。
- Acronis Cyber Files ゲートウェイサーバー用の 1 台の負荷分散装置。
- 3 Acronis Cyber Files Tomcat サーバー（それぞれ 32 GB の RAM と 16 コアの CPU を搭載したもの）。
- 3 Acronis Cyber Files ゲートウェイサーバー（それぞれ 8 GB の RAM と 4 コアの CPU を搭載したもの）。

注意

ゲートウェイサーバーでは、CPU またはメモリよりもディスクおよびネットワーク速度の方が重要になります。

- PostgreSQL サーバー用に1台（32GB の RAM と16コアの CPU を搭載したもの）。
- ファイルリポジトリサービスおよびファイルストア用に 1台。このサーバーのパラメータはそれほど重要ではありません。

ネットワーク接続

- Acronis Cyber Files Tomcat サーバー用の負荷分散装置が現在の Acronis Cyber Files サーバーの DNS アドレスを使用するように構成する必要があります。
- ゲートウェイサーバー用の負荷分散装置が現在のゲートウェイサーバーの DNS アドレスを使用するように構成する必要があります。
- Tomcat サーバーをゲートウェイ負荷分散装置に接続して、デスクトップネットワークノードを同期し、ウェブインターフェイス上のネットワークノードを参照できるようにします。このクラスターセットアップでは、Acronis Cyber Files Web UI の [管理] ページと [ゲートウェイサーバー] ページの [クライアント接続用アドレス] は、外部負荷分散装置のアドレスになります。ゲートウェイサーバー

にも、[Acronis Cyber Files サーバー接続に代替アドレスを使用] 設定を使用し、[Acronis Cyber Files Web サーバー接続用アドレス] にゲートウェイ負荷分散装置の内部アドレスを設定しています。

- モバイルクライアント接続に対応するために、ゲートウェイサーバーを Tomcat 負荷分散装置に接続します。

注意

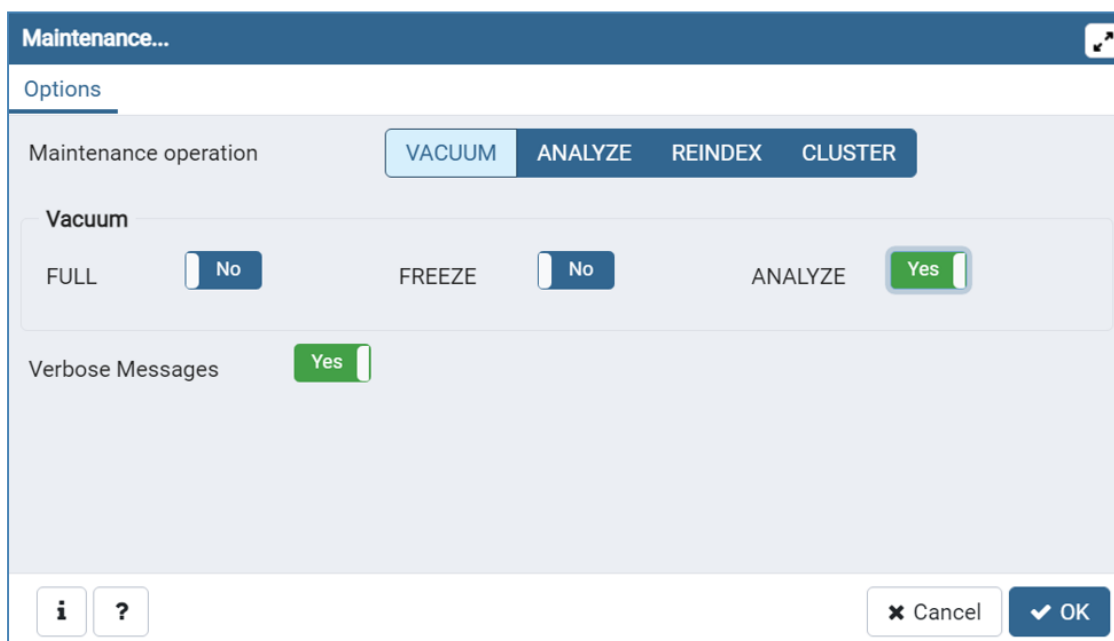
Sync&Share データソースについて、アドレスを Tomcat 負荷分散装置のアドレスに変更する必要があります。

PostgreSQL サーバーの移行

データベースは最も重要なコンポーネントであるため、最初に移行してください。

既存の PostgreSQL サーバー上での構成

1. [サービス] コントロールパネル (services.msc) を開いて、**Acronis Cyber Files Tomcat** サービスを停止します。
2. **Acronis Cyber Files PostgreSQL Administrator** アプリケーションを開き、データベースサーバーに接続します。[データベース] の横にある [+] をクリックします。
3. acronisaccess_production データベースを右クリックします。
4. [メンテナンス] を選択します。
5. [バキューム] を選択し、[分析] を [はい] に設定します。



6. [OK] をクリックします。
7. 管理者特権でコマンドプロンプトを開き、**cd** コマンドで Postgres の **bin** ディレクトリに移動します。（デフォルトで、C:\Program Files (x86)\Acronis\Files Advanced\Common\PostgreSQL\<バージョン>\bin）。

- 現在のコマンドプロンプトディレクトリが **bin** フォルダに変更されたら、以下のコマンドを入力します。

```
pg_dumpall --host localhost --port 5432 --username postgres --file alldbs.sql
```

注意

alldbs.sql というバックアップファイルが生成され、**bin** フォルダに保存されます。このファイルに含まれる完全なパスは、必要に応じて別の場所（たとえば、**D:¥Backups¥alldbs.sql**）に保存できます。

注意

別のポートや別のユーザーを使用している場合、それに応じてコマンドを変更してください。

- バックアップが完了したら、**Acronis Cyber Files PostgreSQL サーバー**サービスを停止して無効にします。
- バックアップファイルを、PostgreSQL をホストする新しいマシンにコピーして移動します。

新しい PostgreSQL サーバー上での構成

- Acronis Cyber Files インストーラを起動して、**[次へ]** を押します。ライセンス契約を読み、承諾します。
- [カスタム]** をクリックし、PostgreSQL Database Server だけを選択します。**[次へ]** を押します。
- PostgreSQL をインストールする場所を選択し、スーパーユーザー (postgres) のパスワードを入力します。

注意

この場所は、他のすべてのサーバーが到達可能な場所でなければなりません。パスワードは、元の PostgreSQL サーバーで前に使用していたパスワードと同じものにしてください。

- [ファイアウォールでポート 5432 を開く]** を選択して、インストールを続行します。このポートを、PostgreSQL データベースにリモートからアクセスするために使用します。

PostgreSQL データベースへのアクセスの構成

- インストールが完了したら、PostgreSQL **data** フォルダ（デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version>\Data）に移動して、テキストエディタで **pg_hba.conf** を開きます。
- Access Tomcat サーバーそれぞれのホストエントリを、内部アドレスを使用して組み込み、ファイルを保存します。すべてのサーバーのアドレスがわかっているわけではない場合、後でこのファイルに戻って編集できますが、それまでは、アドレスのわからないサーバーがデータベースに接続することはできません。

pg_hba.conf（HBA はホストベース認証を表す）ファイルは、クライアント認証を制御するもので、データベースクラスターのデータディレクトリに保存されます。このファイル内に、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。

```
# TYPE DATABASE USER ADDRESS METHOD
```

```
# Loadbalancer1(最初のAcronis Cyber FilesおよびGatewayサーバー)
```

host acronisaccess_production postgres 10.144.70.247/32 md5

注意

この例では、postgres という名前のユーザーアカウントが md5 encrypted 接続を介して、10.144.70.247 にあるサーバーから接続し、完全な権限（レプリケーション権限を除く）で acronisaccess_production データベースにアクセスできます。

postgresql.conf ファイルを開き、以下の変更を加えます。

1. 行 #listen_addresses = 'localhost'. から先頭の # を削除します。localhost を * に置き換えます。変更後は、listen_addresses = '*' となるはずです。
2. 行 #effective_cache_size = 128MB から先頭の # を削除し、**128MB** を **12GB** に置き換えます。変更後は、effective_cache_size = 12GB となるはずです。
3. 以下の注釈を追加します。- #NOTE: this tuning setting assumes that PostgreSQL is running by itself on a #VM with at least 16 GB RAM. More information at https://wiki.postgresql.org/wiki/Tuning_Your_PostgreSQL_Server
4. max_connections を探して正しい値に変更します。これは、すべての Access サーバーノードに構成されている Tomcat の DB_POOLSIZE 設定値の合計に 10 を足した値以上でなければなりません。DB_POOLSIZE は、250 に設定することをお勧めします。
この例では DB_POOLSIZE to 250 が設定されています。Access Tomcat サーバーは 2 台あることから、max_connections を 510 に設定する必要があります。Access Tomcat サーバーの場合は、760 に設定することになります。
5. すべての変更を保存して、**postgresql.conf** ファイルを閉じます。
6. Acronis Cyber Files PostgreSQL サーバーサービスを再起動します。

データベースのインポート

新しい PostgreSQL サーバー上

1. Acronis Cyber Files PostgreSQL Administrator アプリケーションを開き、ローカルデータベースサーバーに接続し、**[データベース]** を選択して acronisaccess_production という名前のデータベースがあることを確認します。
2. データベースのバックアップファイル **alldbs.sql** を、PostgreSQL インストールの **bin** ディレクトリにコピーします。（デフォルトで、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン>\bin）
3. 管理者特権でコマンドプロンプトウィンドウを開き、**cd** コマンドで PostgreSQL の **bin** ディレクトリに移動します。
4. コマンド **psql -U postgres -f alldbs.sql** を入力します。
5. パスワードの入力を求められたら、postgres ユーザーのパスワードを入力します。これにより、以前の PostgreSQL サーバーのデータベースが新しい PostgreSQL サーバーに復元されます。

Acronis Cyber Files サーバーの設定

その他の Acronis Cyber Files サーバーの接続

Acronis Cyber Files Web サーバーのみのインストール

1. Acronis Cyber Files インストーラを起動し、ライセンス契約に同意します。
2. **[カスタム]** を選択し、Acronis Cyber Files Web サーバーのみを選択します。

注意

Acronis Cyber Files Web サーバーをクリックすると、自動的に PostgreSQL サーバーも選択されますが、クリックして選択を解除できます。

3. インストールを完了し、Acronis Cyber Files Tomcat サービスが停止していることを確認します。

サーバーの設定

Acronis Cyber Files Web サーバーで変更したすべての設定は、その他すべての Acronis Cyber Files Web サーバーでも同じ変更を行う必要があります。

注意

pg_hba.conf ファイルに各 Acronis Cyber Files Web サーバーのエントリを追加することを忘れないでください。

適切なデータベースに接続するようサーバーを構成する

1. Acronis Cyber Files Web サーバーフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Access Server）に移動して、acronisaccess.cfg ファイルを開きます。このファイルは、サーバーに PostgreSQL データベースサービスの場所を指示します。
2. 以下の値を設定します。

DB_HOSTNAME =10.144.70.248

DB_PORT =5432

DB_POOLSIZE =250

注意

DB_HOSTNAME は、PostgreSQL が現在実行されている IP アドレスです。この例では、10.144.70.248 となっています。

注意

DB_POOLSIZE を 250 以上に設定することをお勧めします。

3. ファイルを保存します。

最大スレッド数の構成

Tomcat の負荷分散型セットアップでは、すべての Tomcat インスタンスによって生成される可能性のあるスレッドの合計数が、PostgreSQL データベースで受け入れるように構成された最大接続数を超えないようにすることが重要です。

スレッドの合計数を決定する重要な 3 つの設定は、以下のとおりです。

- `acronisaccess.cfg` ファイルでは、`DB_POOLSIZE = 200` です。250 以上の値に設定することをおすすめします。
- `Tomcat server.xml` ファイルでは、`maxThreads = 150` です。この設定は、デフォルトの 150 のままにすることをお勧めします。
- `postgresql.conf` ファイルでは、`max_connections` です。この設定は、前の手順で構成済みになっているはずです。この設定の値は、すべての Acronis Cyber FilesWeb サーバーに設定されている Tomcat のすべての `DB_POOLSIZE` 値の合計に 10 を足した値以上でなければなりません。たとえば、Tomcat サーバーが 2 台の場合は 510、3 台の場合は 760 となります。

注意

これらのファイルに変更を加えた場合、対応するサービスを再起動する必要があります。

適切なロギングの構成

負荷分散構成では、Acronis Cyber Files Tomcat サービスによる IP アドレスのマッピングがログ内で適切に行われません。各接続が適切にログに記録されるよう、以下の変更を行う必要があります。

1. `server.xml` ファイルで、`<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" prefix="localhost_access_log." suffix=".txt" pattern="%h %l %u %t "%r" %s %b"/>` という行を探します。
2. 行の末尾に `requestAttributesEnabled="true"` を追加します。
3. 同じ行の下に、以下を追加します。

```
<Valve className="org.apache.catalina.valves.RemoteIpValve" remoteIpHeader="X-Forwarded-For" protocolHeader="X-Forwarded-Proto"/>
```

警告

IP アドレスの制限機能も使用している場合には、この機能に関連するユーザーのセキュリティに影響が及ぶ可能性があるため、XFF ヘッダーは設定しないでください。代わりに、プロキシにより追加された XFF アドレスを信頼するようロードバランシングを設定することをお勧めします。この場合、リクエストからの XFF ヘッダーもまたコピーされます（そのようなヘッダーが既にある場合）。

4. ファイルを保存し、Acronis Cyber Files Tomcat サービスを再起動します。

古い Acronis Cyber Files サーバーの接続

必要に応じて、既存の Acronis Cyber Files サーバーを引き続き使用することもできますが、それにはそのサーバーを新しいデータベースに接続する必要があります。

リモートデータベースへの Acronis Cyber Files の接続

1. Acronis Cyber Files サーバーフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Access Server）に移動して、acronisaccess.cfg ファイルを開きます。このファイルは、サーバーに PostgreSQL データベースサービスの場所を指示します。
2. 以下の値に設定します。

DB_HOSTNAME =10.144.70.248

DB_PORT =5432

DB_POOLSIZE = 250

注意

DB_HOSTNAME は、PostgreSQL データベースが位置する IP アドレスを設定します。この例では、10.144.70.248 となっています。

3. ファイルを保存してから、[サービス] コントロールパネル (services.msc) で **Acronis Cyber Files Tomcat サービス** を起動します。
4. 未使用の Acronis Cyber Files コンポーネントはすべてアンインストールできます。

ファイルストアとファイルリポジトリの移行

「[ファイルストアとファイルリポジトリの移動](#)」ガイドを参照してください。確認しなければならない唯一の追加設定として、すべての Acronis Cyber Files コンポーネントがファイルリポジトリとファイルストアをホストする予定のマシンにアクセスできることを確認します。

S3 ストレージを使用する予定の場合、選択する S3 ストレージ内でファイルストアがホストされることになるため、ファイルリポジトリサービスをインストールする必要はありません。

ファイルリポジトリとファイルストアを現在の場所に維持することを予定している場合、必要な作業となるのは、新しい Acronis Cyber Files サーバーが適切にリポジトリエンドポイントを指し示していることを確認することだけです。

ゲートウェイサーバーの移行

新しいゲートウェイサーバーのインストール

1. 新しいマシン上で、Acronis Cyber Files インストーラを実行し、ライセンス契約に同意します。
2. **[カスタム]** を選択し、ゲートウェイサーバーコンポーネントのみをインストールします。インストールを終了します。
3. 設定ユーティリティで、ゲートウェイのアドレス、ポート、証明書を設定します。設定する証明書は、ゲートウェイ負荷分散装置の DNS アドレスに関連付けられている SSL 証明書と同じものでなければなりません。

以前のゲートウェイサーバーのすべての設定の移行

1. Tomcat とゲートウェイの両方を実行していた前のマシン上で、Acronis Cyber Files Web インターフェースを開き、[ゲートウェイサーバー] ページを開きます。以前のゲートウェイのエントリが表示されます。
2. 新しいゲートウェイを追加するために、[ゲートウェイサーバーの追加] をクリックし、該当するすべてのデータを入力します。
3. [クラスターグループの追加] をクリックします。
 - 表示名を入力します。
 - [クライアント接続のアドレス] に値を入力します。クラスターでは、[クライアント接続用アドレス] に外部負荷分散装置のアドレスを入力します。次に、[... サーバー接続に代替アドレスを使用] をクリックし、[Acronis Cyber Files サーバー接続用アドレス] にゲートウェイ負荷分散装置の内部アドレスを入力します。
4. [クラスター化に使用できるゲートウェイ サーバー] で、両方のゲートウェイサーバーの [追加] ボックスをオンにします。
5. [設定に使用するゲートウェイサーバー] で、旧ゲートウェイサーバーを選択します。
6. [追加] をクリックします。[ゲートウェイサーバー] ページに新しいクラスターが表示されます。[+] を使用してクラスターを展開します。
7. 新しいゲートウェイに、すべての設定が移行されているはずです。新しいゲートウェイをクラスターのマスターにするために、[操作] ドロップダウンメニューをクリックし、[グループマスターにする] を選択します。
8. 以前のゲートウェイはそのままにすることも、クラスターグループから除外することも、除外して削除することもできます。セットアップが正常に動作するようになるまで、クラスターの一部として残しておくことをおすすめします。

ログの管理と消去

追加の Acronis Cyber Files サーバーをインストールした後、Acronis Cyber Files Tomcat ログが維持されているフォルダに移動し、それらのフォルダに対する適切な権限を設定して、ログの書き込みおよび消去を行えるようにしてください。

負荷分散装置固有の設定

1. ブラウザで <https://mylb.company.com> を開き、設定が機能していることを確認します。
2. 負荷分散装置で時間ベースのセッションスティックネス（またはご使用の負荷分散装置での同等の設定）を有効にし、期限切れにならないように設定します。
3. ヘルスチェック（HTTP ステータス 200 が返されることを確認する）が必要な場合は、https://INTERNALSERVERNAME:MANAGEMENTPORT/api/v1/server_version に ping します（例: <https://myaccessserver.company.com/signin> および https://myaccessserver.company.com/api/v1/server_version）。
4. 負荷分散型セットアップで IP アドレスと接続が適切にログに記録されるようにするには、負荷分散装置を構成して以下のヘッダーを設定する必要があります。

- X-Forwarded-For: これにより、各接続で負荷分散装置の IP アドレスが表示される代わりに、接続しているクライアントの実際の IP アドレスが表示されるようになります。
- X-Forwarded-Proto: これにより、実際に使用されているプロトコルが表示されます。

元のサーバーのクリーンアップ

元の本番サーバー上の Acronis Cyber Files Tomcat を引き続き使用する場合は、そのサーバーで使用されなくなった Acronis Cyber Files 項目をアンインストールすることをお勧めします。

コントロールパネルから、Acronis Cyber Files PostgreSQL サーバー、Acronis Cyber Files ゲートウェイサーバー、および Acronis Cyber Files ファイルリポジトリサーバー（存在する場合）をアンインストールできます。

API で Web インターフェースをカスタマイズする

API による Web インターフェースのカラースキームのアップデートは、サービスの再起動が不要でダウンタイムを生じさせず、簡単に行うことができます。これらのカスタマイズには、[Acronis Cyber Files の Web インターフェース](#)から実行できるものもあります。

CURL のインストール

1. API コマンドを使用するには Curl をインストールする必要があります。

- a. 次の公式サイトから Curl をダウンロードしてください。

<https://curl.haxx.se/download.html>

注意

SSL をサポートするバージョンをダウンロードしてください！

- b. インストールが終了するまで、または単に Curl アーカイブが抽出されるまでは、Curl インストーラの表示に従ってください。

カスタムカラースキームの作成

1. 管理者特権でコマンドプロンプトを開き、次のコマンドを入力します。

```
curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@<path_to_file> -F customization_settings[color_scheme_client_scss_file]=@<path_to_file> -u <user>:<password> https://<your_site>/api/v1/settings/customization -v
```

注意

ファイル名には特定の命名構文を使用する必要があります。管理コンソールでは color_scheme_<name_of_scheme>.css を、ウェブクライアントコンソールでは web_client_<name_of_scheme>.scss を使用する必要があります。<name_of_scheme> は、Acronis Cyber Files インターフェースに表示される新しいスキームの名前で、両方のファイルで同じにする必要があります。

上記コマンドは次のように動作します。

- 管理コンソールでは **.css** ファイルを選択します。
- ウェブクライアントコンソールでは **.scss** ファイルを選択します。
- Web インターフェースの **[カラスキーム]** ドロップダウンから選択可能な新しいテーマを作成します。

注意

カラススキームの一部分だけを変更する場合は、上記コマンドを入力する際に、変更する部分には新しい .css スキームを使用し、変更しない部分には既存の .css スキームを使用する必要があります。

2. ここで、インターフェースの管理部分用の配置されているスキームとウェブクライアント用の配置されているスキームをアップロードするコマンドの例を示します。
3. この例では、両方のファイルが D:\WebUI に配置されており、Web インターフェースに表示されるカラススキーム名として **NewColor** を選択します。

```
curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@D:\WebUI\color_scheme_NewColor.css -F customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_client_NewColor.scss -u administrator:123456 https://myCompany.com/api/v1/settings/customization
```

4. `-F customization_settings[color_scheme]=<name_of_scheme>` コマンドを使用して、現在のテーマを、追加している新しいテーマに切り替えることもできます。後ろにこのコマンドを追加すると次のようになります。

```
curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@D:\WebUI\color_scheme_NewColor.css -F customization_settings[color_scheme_client_scss_file]=@D:\WebUI\web_client_NewColor.scss -F customization_settings[color_scheme]=NewColor -u administrator:123456 https://myCompany.com/api/v1/settings/customization -v
```

トラブルシューティング

- コマンドは実行されるが、インターフェースに新しいテーマが表示されない
ファイル名が **color_scheme_<name_of_scheme>.css** と **web_client_<name_of_scheme>.scss** の正しい構文に従っていることを確認します。
- 「**libcurl でプロトコル https がサポートされていないか、無効になっています**」というエラーが表示される
アドレスを囲んでいる単一引用符 (") を削除します。引用符を使用する必要がある場合は、代わりに、"https://myCompany.com/api/v1/settings/customization" のように二重引用符 (") を使用します。
- 証明書エラーが表示される
自己署名証明書を使用している場合または IP アドレスを使用してコマンドを実行している場合は、コマンドの最後に **-k** フラグを追加して証明書エラーを無視する必要があります。

デスクトップクライアントの無人設定

Microsoft のグループポリシー管理を使用することで、Acronis Cyber Files デスクトップクライアントを複数のコンピューターにリモートから簡単にインストールして設定することができます。エンドユーザーが行うのは、クライアントの起動とパスワードの入力だけです。また、グループポリシー管理では、エンドユーザーが正しい設定を誤って変更したり置き換えたりすることはできません。誤って変更してしまった場合、ユーザーはログオフするだけで、正しい設定が次のログイン時に再適用されます。

グループポリシー管理オブジェクトの作成および設定:

1. ドメイン コントローラで **[グループ ポリシー管理コンソール]** を開きます。
2. 目的のドメインを右クリックし、**[このドメインに GPO を作成し、このコンテナにリンクする...]** を選択します。
3. 名前を入力して **[OK]** をクリックします。
4. **[グループ ポリシー オブジェクト]** セクションを展開し、新しいポリシーを選択します。
5. **[スコープ]** タブで目的のサイト、ドメイン、OU、グループ、ユーザー、およびコンピュータを選択します。

クライアントの無人インストール

このセクションでは、ユーザーのログイン時に、目的のすべてのコンピューターに Acronis Cyber Files デスクトップクライアントをサイレントインストールする方法について説明します。

インストーラ配布ポイントの作成

クライアントをインストールするすべてのコンピューターに、インストーラへのアクセス権が必要です。このためには、フォルダを作成し、目的のユーザーグループと共有してから、そのフォルダにインストーラを置きます。

1. インストーラがあるフォルダを右クリックして **[プロパティ]** を選択します。
2. **[共有]** タブを開き、**[共有]** を押します。
3. Accessクライアントをインストールするドメイングループ、OU、またはユーザーを入力します。このグループ（またはOU、ユーザー）は **[グループポリシーオブジェクト]** で選択したものと同等である必要があります。
4. **[OK]/[完了]** を押して残りのダイアログをすべて閉じます。

注意

目的のコンピューターがネットワークアドレス (\\WIN2008\\Software\\AAClientInstaller.msi など) でインストーラにアクセスできることを確認します。

ユーザーのコンピューターへのインストーラの保存

1. ドメインコントローラで、**[グループポリシーオブジェクト]** セクションを展開し、新しいポリシーオブジェクトを右クリックします。

2. **[編集]** を選択し、**[ユーザーの構成]** → **[基本設定]** → **[Windowsの設定]** → **[ファイル]** の順に展開します。
3. **[ファイル]** を右クリックし、**[新規]** → **[ファイル]** の順に選択します。
4. **[操作]** で **[作成]** を選択します。
5. **[ソースファイル]** で、**[参照]** ボタンをクリックしてアクセスクライアントのインストーラに移動するか、インストーラの完全なパスを入力します（¥¥WIN2008¥Software¥AAClientInstalelr.msi など）。
6. **[宛先ファイル]** に、宛先フォルダと宛先ファイル名を入力します。これで、ネットワーク共有から Access クライアントのインストーラがコピーされ、ログオンしているユーザーのコンピュータの宛先フォルダに保存されます。

注意

たとえば、**C:¥Folder¥ThisFile.msi** と入力すると、クライアントのインストーラがユーザーの **C** ドライブ上の Folder フォルダに **ThisFile.msi** という名前で保存されます。

7. **[OK]** を押します。

クライアントのインストール

インストールスクリプトの作成

1. 空のテキストファイルを作成し、次のスクリプトを貼り付けます。

```
msiexec /i "C:\AAC.msi" /quiet  
sleep 180  
DEL /F /S /Q /A "C:\AAC.msi"
```

このスクリプトによってコマンドプロンプトが開きます。プロンプトに何も表示されずに Access クライアントがインストールされ、3分後に Access クライアントのインストーラが削除されます。

2. 両方の場所でパス C:\AAC.msi を、**[宛先ファイル]** フィールドに入力したパスに変更し、**[ファイル]** → **[名前を付けて保存...]** の順に押します。
3. スクリプトの名前を入力し、拡張子が **.bat** であることを確認します。**[ファイルの種類:]** フィールドで、**[すべてのファイル]** を選択します。ファイルがドメインコントローラ上にあるか、ドメインコントローラがファイルにアクセスできることを確認します。このファイルは重要です。変更したり削除したりせず、変更されない特定の場所に保存してください。

ユーザーログオン時のスクリプトの使用

1. **[グループポリシーマネージャ]** を開き、**[グループポリシーオブジェクト]** セクションを展開して、新しい **ポリシーオブジェクト** を右クリックします。
2. **[編集]** を選択し、**[ユーザーの構成]** → **[基本設定]** → **[Windowsの設定]** → **[スクリプト（ログオン/ログオフ）]** の順に展開します。
3. **[ログオン]** をダブルクリックして **[追加]** を押します。
4. **[スクリプトの追加]** ダイアログで、**[参照...]** を押し、スクリプトを保存したフォルダに移動します。
5. スクリプトを選択して **[開く]** を押します。
6. **[OK]** を押し、次のダイアログで **[OK]** をもう一度押します。

7. 操作は完了です。指定したグループまたは OU 内のすべてのユーザーに、ログオン時に Acronis Cyber Files クライアントがインストールされます。

フォルダおよびレジストリ エントリの作成:

次の例では、ユーザー名、同期フォルダ、サーバー URL、自動アップデートのチェックボックスのエントリ、およびクライアントによる自己署名証明書でのサーバーへの接続を必須にするエントリを作成します。

1. **[グループ ポリシー オブジェクト]** セクションを展開し、新しいポリシー オブジェクトを右クリックします。
2. **[編集]** を選択し、**[ユーザーの構成]** → **[基本設定]** → **[Windows の設定]** の順に展開します。

同期フォルダの作成:

1. **[フォルダ]** を右クリックし、**[新規]** → **[フォルダ]** の順に選択します。
2. **[操作]** を **[作成]** に設定します。
3. パスに次のトークンを入力します: %USERPROFILE%\Desktop\AAS Data Folder。

レジストリの作成:

1. **[レジストリ]** を右クリックし、**[新規]** → **[レジストリ項目]** の順に選択します。
2. **[操作]** を **[作成]** に設定します。
3. **[ハイブ]** で **[HKEY_CURRENT_USER]** を選択します。
4. パスに「Software\Group Logic, Inc.\activeEcho Client\」と入力します。
5. 目的のエントリで次の操作を実行します。
6. ユーザー名:
 - a. **[値の名前]** に「Username」と入力します。
 - b. **[値の種類]** で **[REG_SZ]** を選択します。
 - c. **[値データ]** に次のトークンを入力します: %USERNAME%%%USERDOMAIN%。

注意

シングルサインオンを使用する場合は、Username トークンを設定しないでください。代わりに、次の操作を実行します。

- **SSO:**
 - a. **[値の名前]** に「AuthenticateViaSSO」と入力します。
 - b. **[値の種類]** で **[REG_SZ]** を選択します。
 - c. **[値データ]** に「1」と入力します。
7. サーバー URL:
 - a. **[値の名前]** に「Server URL」と入力します。
 - b. **[値の種類]** で **[REG_SZ]** を選択します。
 - c. **[値データ]** に、**https://myaccess.com** などの Acronis Cyber Files サーバーのアドレスを入力します。
 8. 同期フォルダ:

- a. [値の名前] に「**activEcho Folder**」と入力します。
 - b. [値の種類] で [REG_SZ] を選択します。
 - c. [値データ] に次のトークンとパスを入力します: %USERPROFILE%\Desktop\AAS Data Folder。
9. 自動アップデート:
- a. [値の名前] に「**AutoCheckForUpdates**」と入力します。
 - b. [値の種類] で [DWORD] を選択します。
 - c. [値データ] に「**00000001**」と入力します。値「**1**」でこの設定が有効になり、クライアントは自動的にアップデートを確認します。値を「**0**」に設定すると、この設定は無効になります。
10. 証明書:
- a. [値の名前] に「**AllowInvalidCertificates**」と入力します。
 - b. [値の種類] で [DWORD] を選択します。
 - c. [値データ] に「**00000000**」と入力します。値「**0**」でこの設定が無効になり、クライアントは無効な証明書を使って Acronis Cyber Files サーバーに接続できなくなります。値を「**1**」に設定すると、この設定は有効になります。

シングルサインオンの設定

このガイドでは、Acronis Cyber Files でシングルサインオン機能を有効化するための詳細設定の方法について説明します。

注意

シングルサインオンは有効なドメインでのみ使用できます。

注意

Acronis Cyber Files を単一ポート設定で実行している場合（ゲートウェイサーバーが Acronis Cyber Files サーバーのリクエストをプロキシ処理している場合）、シングルサインオンは**機能しません**。

注意

Acronis Cyber Files がドメインコントローラーにインストールされている場合、シングルサインオンは**機能しません**。また、SSO の制限事項を無視する場合でも、パフォーマンス上の理由から、Acronis Cyber Files サーバーをドメインコントローラーにインストールしないことを強くお勧めします。

シングルサインオンの機能を使用すると、有効な LDAP ユーザーはすべて、資格情報を入力しなくても Web インターフェースおよびデスクトップクライアントにログインできます。ユーザーは Acronis Cyber Files アカウントが必要になります。または、LDAP プロビジョニングがサーバーで有効にされている必要があります。

- Acronis Cyber Files のログインページにリンクが表示されます。ユーザーは、このコンピューターへのログインに使用しているアカウントでログインします。

注意

SSO の正常な動作のために、FQDN (https://access.company.com など) を使用して Acronis Cyber Files インターフェースを開く必要があります。IP アドレスを使用してインターフェースを開く場合、シングルサインオンは**機能しません**。

ユーザーがモバイルアプリケーションから KCD を使用して Sync & Share フォルダにアクセスできるようにするために、UPN はメイン SSO のセットアップと同じドメインにある必要があります。

- デスクトップクライアントの場合、SSOを有効にできる新しいラジオボタンがあります。ユーザーは、Acronis Cyber Files サーバーの URL を入力するだけです。この機能により、コンピューターへのログインに使用しているアカウントで自動的にログインできます。

注意

この機能は Windows クライアントでのみ利用できます。Mac でのサポートは今後のリリースで追加されます。

注意

デスクトップクライアントからのシングルサインオンには、企業ネットワークへのアクセス権が必要です。これは、SSO ユーザーは自身のネットワークへのアクセスも必要であることを意味します。

Acronis 同一マシン上の Cyber Files Web サーバーとゲートウェイサーバー

この構成は、ほぼ共通で、同一マシン上にある 1 台の Acronis Cyber Files Web サーバーと 1 台の Acronis Cyber Files ゲートウェイサーバーで構成されます。これは、デフォルトのインストールです。

ドメイン上

Acronis Cyber Files Web サーバーと、ドメインの Kerberos サーバーを登録するために実行する必要がある手順を説明します。この手順を実行するのは 1 度だけです。SSO 認証チェックのクエリ送信先になる LDAP アカウントを指定するには、「setspn.exe」を使用します。

注意

証明書認証を使用してモバイルクライアントを使用する場合、Acronis Cyber Files Web サーバーの DNS エントリとコンピュータ名は**同じにしないでください**。Acronis Cyber Files Web サーバーの SPN がコンピュータ名と同じである場合、ゲートウェイサーバーでは Acronis Cyber Files Web サーバーを「同じコンピュータ上にあるもの」として扱うため、Kerberos 認証の実行は試行されません。たとえば、computerAccess.domain.com / computer.domain.com および computerAccess.domain.com / computerGW.domain.com は動作しますが、computer.domain.com / computerGW.domain.com は動作しません。

SSOを処理するLDAPアカウントの設定

注意

SMBまたはSharePointのデータソースを使用する場合、Active Directoryアカウントを設定して、SMBおよびSharePointデータソースごとにKerberos委任を許可してください。詳細については、「[詳細委任設定](#)」を参照してください。

1. コマンドプロンプトを開きます。

注意

setspn を使用する権限のあるドメインアカウントでログインする必要があります。

2. コマンド **setspn -s HTTP/computername.domain.com account name** を入力します。

たとえば、Acronis Cyber Files Web サーバーがahsoka.acme.comにインストールされており、認証済みのLDAPアカウントとしてjohn@acme.comを使用してKerberosチケットを付与する場合、コマンドは次のようになります。

```
setspn -s HTTP/ahsoka.acme.com john
```

注意

上記のコマンドに使用するLDAPアカウント名は、web.xmlのspnego.preauth.usernameプロパティで指定するアカウントと一致させる**必要があります**。

注意

通常、このアカウントは、Acronis Cyber Files Web インターフェース（**[全般設定]** → **[LDAP]** → **[LDAP ユーザー名/LDAP パスワード]**）の管理者によって指定されているLDAPアカウントと一致します。ただし、必ずしも一致させる必要はありません。

3. Acronis Cyber Files Web サーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNを登録する必要もあります。

例: サーバーがポート444で動作している場合、コマンドは次のようになります。

```
setspn -s HTTP/ahsoka.acme.com:444 john
```

注意

上記のコマンドの**HTTP**は、**HTTP**プロトコルではなく**HTTP**サービスクラスを指しています。**HTTP**サービスクラスでは、**HTTP**と**HTTPS**の両方のリクエストが処理されます。サービスクラスの名前に**HTTPS**を使用してSPNを作成する必要はありません。また、**作成しないでください**。

4. ドメインコントローラにアクセスし、**[Active Directoryユーザーとコンピュータ]**を開きます。
5. 上記のコマンドで使用されているユーザーを検索します（この場合、john）。
6. **[委任]** タブをクリックし、**[任意のサービスへの委任でこのユーザーを信頼する（Kerberosのみ）]**を選択します。
7. **[OK]**を押します。

ゲートウェイサーバーのSPNの設定

KDC（「キー配布センター」）Kerberosサーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspnを実行してゲートウェイサーバーをKDCサーバーに登録し、「ユーザー」として実行されているサーバーのホスト名をsetspnコマンドで指定する必要があります。

この設定が機能するためには、ゲートウェイサーバーに追加のDNSエントリを設定する必要があります。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、ゲートウェイサーバーに新しい**ホストエントリ**(A record)を作成します。
2. 名前を入力します。これは、ゲートウェイサーバーへのアクセスに使用されるDNSアドレスになります。

例: ahsoka-gw.acme.com

3. ゲートウェイサーバーのIPアドレスを入力します（ポートは入力しません）。同じ IP アドレスでゲートウェイサーバーと Acronis Cyber Files サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR）レコードを作成する]** を選択し、**[ホストの追加]** を押します。
5. Acronis Cyber Files がインストールされているマシンに戻ります。
6. コマンドプロンプトを開きます。

7. **setspn** コマンドとして **setspn -s HTTP/gatewaydns.domain.com computername** を入力します。

たとえば、ゲートウェイサーバーがドメインのホスト 'ahsoka' で実行されていて、DNSエントリが ahsoka-gw.acme.com の場合は、次のコマンドを実行します。

```
setspn -s HTTP/ahsoka-gw.acme.com ahsoka
```

8. ゲートウェイサーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNを登録する必要もあります。たとえば、ゲートウェイサーバーがポート444で実行されている場合、次のように登録します。

```
setspn -s HTTP/ahsoka-gw.acme.com:444 ahsoka
```

9. 目的のゲートウェイサーバーの **[管理のアドレス]** と **[クライアント接続のアドレス]** を、手順 4 で作成した新しいゲートウェイサーバーの DNS エントリに変更します。

注意

両方のアドレスを同じにする必要があります、また正しい DNS エントリに更新する必要があります。

Acronis Cyber Files サーバー上

シングルサインオン認証で使用するドメインアカウントの設定

1. C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\に移動します。

2. ファイル web.xml を探して開きます。このファイルに、SSOサービスが実行されるドメインのユーザー名およびパスワードを設定します。このアカウントは、「**ドメイン上**」のセクションで、KerberosにHTTPサービスを登録するときに使用したアカウントと一致している**必要があります**。
3. web.xml には、設定が必要になる 2 つのプロパティ（SSO サービスが使用するドメインのユーザー名およびパスワード）があります。以下に示す行を検索します。

```
<init-param>

  <param-name>spnego.preauth.username</param-name>
  <param-value>yourusername</param-value>

</init-param>

<init-param>

  <param-name>spnego.preauth.password</param-name>
  <param-value>yourpassword</param-value>

</init-param>
```

4. **yourusername**を目的のLDAPユーザー名に置き換えます。
5. **yourpassword**を、上記で指定したLDAPアカウントのLDAPパスワードに置き換えます。パスワードに 5 つの特殊文字、**&**、**>**、**"**、**'**、**<**のいずれかが含まれている場合は、それらを XML ドキュメント内で正しくエスケープする必要があります。これを行うには、次のように置き換える必要があります。

- **<**は**<**;
- **>**は**>**;
- **"**は**"**;
- **'**は**'**;
- **&**は**&**;

たとえば、パスワードが `<my&best'password"` の場合、web.xml ファイルには次のように書き込む必要があります。`<my&best'password"`;

Kerberosドメインルックアップの設定

1. C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf に移動します。
2. krb5.conf ファイルを検索して開きます。
3. krb5.conf には、管理者から受け取る必要があるプロパティが 2 つだけあります。
 - a. シングルサインオン用のドメイン（例: ACME.COM）。サーバーのDNS名**ではなく**、ご使用のドメインの名前であることに注意してください。

注意

krb5.conf のドメインには必ず**大文字**を使用してください。大文字を使用しない場合、Kerberos チケットの参照に失敗する場合があります。

- b. Kerberos キー配布センターのアドレス（通常、プライマリドメインコントローラーのアドレスと一致します。例: acmedc.ACME.COM）
4. インストールする krb5.conf ファイルの内容は次のようになります。

```
[libdefaults]
    default_realm = ACME.COM
    default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
    default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
    permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
[realms]
    ACME.COM = {
        kdc = acmedc.ACME.COM
        default_domain = ACME.COM
    }
[domain_realm]
    .ACME.COM = ACME.COM
```

5. ACME.COM のすべてのインスタンスをドメイン（**大文字**）に置き換えます。サーバーのDNS名ではなく、ご使用のドメインの名前であることに注意してください。
6. "kdc =" の値をドメインコントローラーの名前に置き換えます。ドメインは大文字にする必要があります（例: kdc = yourdc.YOURDOMAIN.COM）。
7. 上記の設定ファイルのアップデート後、変更内容を適用するために、Acronis Cyber Files サーバー（Acronis Cyber Files Tomcat サービス）を再起動する必要があります。

ウェブインターフェイスでのシングルサインオンの有効化:

1. Acronis Cyber Files Web インターフェイスを開き、管理者としてログインします。
2. **[全般設定]** タブを展開して、**[LDAP]** ページを開きます。
3. ページの最下部で、**[Windows/Macの既存のログイン資格情報を使用してウェブクライアントおよびデスクトップ同期クライアントからログインすることを許可します]** のチェックボックスをオンにします。
4. **[保存]** をクリックします。

ゲートウェイサーバーの追加

注意

ゲートウェイサーバーをホストするマシンが Acronis Cyber Files Web サーバーと同じドメイン内にあ
る場合にのみ、以下の手順が使えます。

KDC（「キー配布センター」）Kerberosサーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspnを実行してゲートウェイサーバーをKDCサーバーに登録し、「ユーザー」として実行されているサーバーのホスト名をsetspnコマンドで指定する必要があります。

ゲートウェイサーバーが Acronis Cyber Files Web サーバーとは異なるマシンに存在する場合

1. コマンドプロンプトを開きます。
2. **setspn** コマンドとして `setspn -s HTTP/computername.domain.com computername` を入力します。

たとえば、ゲートウェイサーバーがドメインのホスト「cody」で実行されている場合は、次のコマンドを実行します。

```
setspn -s HTTP/cody.acme.com cody
```

3. ゲートウェイサーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNを登録する必要もあります。たとえば、ゲートウェイサーバーがポート444で実行されている場合、次のように登録します。

```
setspn -s HTTP/cody.acme.com:444 cody
```

4. 追加のゲートウェイサーバーすべてにこのセクションの手順を繰り返します。

SSO（シングルサインオン）サポートのためのブラウザの構成

ブラウザのシングルサインオンサポートを有効にするには、1 回限りのマイナーな構成を行う必要があります。

重要

それぞれのマシンでユーザーごとに実行する必要があります。

注意

この構成手順では、例として `acme.com` を使用します。複数のドメインにサービスがある場合は、すべてのドメインに `acme.com` を指定する手順を繰り返します。（たとえば、`*.acme.com` と `*.another.com` と `*.yetanother.com` を追加します）。

Acronis 異なるマシン上の Cyber Files サーバーとゲートウェイサーバー

ドメイン上

Acronis Cyber Files サーバーと、ドメインの Kerberos サーバーを登録するために実行する必要がある手順を説明します。この手順を実行するのは 1 度だけです。SSO 認証チェックのクエリ送信先になる LDAP アカウントを指定するには、「`setspn.exe`」を使用します。

注意

証明書認証を使用してモバイルクライアントを使用する場合、Acronis Cyber Files Web サーバーの DNS エントリとコンピューター名は**同じにしないでください**。Acronis Cyber Files Web サーバーの SPN がコンピューター名と同じである場合、ゲートウェイサーバーでは、Acronis Cyber Files Web サーバーを「同じマシン上にあるもの」として処理されるため、Kerberos 認証は試行されません。たとえば、

computerAccess.domain.com / computer.domain.com および computerAccess.domain.com / computerGW.domain.com は正常に処理されますが、computer.domain.com / computerGW.domain.com は正常に処理されません。

SSOを処理するLDAPアカウントの設定

注意

SMBまたはSharePointのデータソースを使用する場合、Active Directoryアカウントを設定して、SMB およびSharePointデータソースごとにKerberos委任を許可してください。詳細については、「[詳細委任設定](#)」を参照してください。

1. コマンドプロンプトを開きます。

注意

setspn を使用する権限のあるドメインアカウントでログインする必要があります。

2. コマンド **setspn -s HTTP/computername.domain.com account name** を入力します。

たとえば、Acronis Cyber Files サーバーがahsoka.acme.comにインストールされており、認証済みの LDAP アカウントとして john@acme.comを使用して Kerberos チケットを付与する場合、コマンドは次のようになります。

```
setspn -s HTTP/ahsoka.acme.com john
```

注意

上記のコマンドに使用する LDAP アカウント名は、web.xml の spnego.preauth.username プロパティで指定するアカウントと一致させる**必要があります**。

注意

通常、このアカウントは、Acronis Cyber Files Web インターフェース（**[全般設定]** → **[LDAP]** → **[LDAP ユーザー名/LDAP パスワード]**）の管理者によって指定されている LDAP アカウントと一致します。ただし、必ずしも一致させる必要はありません。

3. Acronis Cyber Files サーバーがデフォルト以外のポート（443 以外のポート）で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。

例: サーバーがポート 444 で動作している場合、コマンドは次のようになります。

```
setspn -s HTTP/ahsoka.acme.com:444 john
```

注意

上記のコマンドの **HTTP** は、**HTTP** プロトコルではなく **HTTP** サービスクラスを指しています。**HTTP** サービスクラスでは、**HTTP** と **HTTPS** の両方のリクエストが処理されます。サービスクラスの名前に**HTTPS**を使用してSPNを作成する必要はありません。また、**作成しないでください**。

- ドメインコントローラにアクセスし、**[Active Directoryユーザーとコンピュータ]**を開きます。
- 上記のコマンドで使用されているユーザーを検索します（この場合、**john**）。
- [委任]** タブをクリックし、**[任意のサービスへの委任でこのユーザーを信頼する（Kerberosのみ）]**を選択します。
- [OK]** を押します。

ゲートウェイサーバーのSPNの設定

KDC（「キー配布センター」）Kerberosサーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、**setspn**を実行してゲートウェイサーバーをKDCサーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を**setspn**コマンドで指定する必要があります。

ゲートウェイサーバーが Acronis Cyber Files サーバーとは異なるマシンに存在する場合

- コマンドプロンプトを開きます。
- setspn** コマンドとして **setspn -s HTTP/computername.domain.com computername** を入力します。
たとえば、ゲートウェイサーバーがドメインのホスト '**cody**' で実行されている場合は、次のコマンドを実行します。

```
setspn -s HTTP/cody.acme.com cody
```
- ゲートウェイサーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNに登録する必要もあります。たとえば、ゲートウェイサーバーがポート444で実行されている場合、次のように登録します。

```
setspn -s HTTP/cody.acme.com:444 cody
```
- すべてのゲートウェイサーバーにこのセクションの手順を繰り返します。

ゲートウェイサーバーが Acronis Cyber Files サーバーと同じマシンに存在する場合

ゲートウェイサーバーが Acronis Cyber Files サーバーと同じマシンに存在する場合にのみ、この手順を実行する必要があります。その他の場合には、このセクションをスキップしてください。この設定が機能するためには、ゲートウェイサーバーに追加のDNSエントリを設定する必要があります。

- DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、ゲートウェイサーバーに新しい**ホスト**エントリ(A record)を作成します。
- 名前を入力します。これは、ゲートウェイサーバーへのアクセスに使用されるDNSアドレスになります。

例: codygw.acme.com

- ゲートウェイサーバーのIPアドレスを入力します（ポートは入力しません）。同じ IP アドレスでゲートウェイサーバーと Acronis Cyber Files サーバーを実行している場合は、その IP アドレスを入力します。
- [関連付けられたポインタ（PTR）レコードを作成する]** を選択し、**[ホストの追加]** を押します。
- Acronis Cyber Files がインストールされているマシンに戻ります。
- コマンドプロンプトを開きます。
- setspn** コマンドとして **setspn -s HTTP/gatewaydns.domain.com computername** を入力します。

たとえば、ゲートウェイサーバーがドメインのホスト 'cody' で実行されていて、DNS エントリが codygw.acme.com の場合は、次のコマンドを実行します。

```
setspn -s HTTP/codygw.acme.com cody
```

- ゲートウェイサーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNを登録する必要もあります。たとえば、ゲートウェイサーバーがポート444で実行されている場合、次のように登録します。

```
setspn -s HTTP/codygw.acme.com:444 cody
```

- まだ実行しない場合は、目的のゲートウェイサーバーの**管理のアドレス**を、手順4で作成したゲートウェイサーバーのDNSエントリに変更する必要があります。

Acronis Cyber Files サーバー上

web.xml ファイルの編集:

- C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access server\Web Application\WEB-INF\に移動します。
- ファイル web.xml を探して開きます。このファイルに、SSOサービスが実行されるドメインのユーザー名およびパスワードを設定します。このアカウントは、「**ドメイン上**」のセクションで、KerberosにHTTPサービスを登録するときに使用したアカウントと一致している**必要があります**。
- web.xml には、設定が必要になる 2 つのプロパティ（SSO サービスが使用するドメインのユーザー名およびパスワード）があります。以下に示す行を検索します。

```
<init-param>
  <param-name>spnego.preauth.username</param-name>
  <param-value>yourusername</param-value>
</init-param>
<init-param>
  <param-name>spnego.preauth.password</param-name>
  <param-value>yourpassword</param-value>
</init-param>
```

- yourusername** を目的のLDAPユーザー名に置き換えます。
- yourpassword** を、上記で指定したLDAPアカウントのLDAPパスワードに置き換えます。パスワードに 5 つの特殊文字、**&**、**>**、**"**、**'**、**<** のいずれかが含まれている場合は、それらを XML ドキュメント内で正しくエスケープする必要があります。これを行うには、次のように置き換える必要があります

す。

- <は<
- >は>
- "は"
- 'は'
- &は&

たとえば、パスワードが <my&best'password" の場合、web.xml ファイルには次のように書き込む必要があります。<my&best'password"

krb5.conf ファイルの編集:

1. C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf に移動します。
2. krb5.conf ファイルを検索して開きます。
3. krb5.conf には、管理者から受け取る必要があるプロパティが2つだけあります。
 - a. シングルサインオン用のドメイン (例: ACME.COM)

注意

krb5.conf のドメインには必ず**大文字**を使用してください。大文字を使用しない場合、Kerberos チケットの参照に失敗する場合があります。

- b. Kerberos キー配布センターのアドレス (通常、プライマリドメインコントローラーのアドレスと一致します。例: acmedc.ACME.COM)
4. インストールする krb5.conf ファイルの内容は次のようになります。

[libdefaults]

```
default_realm = ACME.COM
default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
```

[realms]

```
ACME.COM = {
    kdc = acmedc.ACME.COM
    default_domain = ACME.COM
    [domain_realm]
```

```
.ACME.COM = ACME.COM
```

5. ACME.COM のすべてのインスタンスをドメイン (**大文字**) に置き換えます。
6. "kdc =" の値をドメインコントローラーの名前に置き換えます。ドメインは大文字にする必要があります (例: kdc = yourdc.YOURDOMAIN.COM) 。
7. 上記の設定ファイルのアップデート後、変更内容を適用するために、Acronis Cyber Files サーバー (Acronis Cyber Files Tomcat サービス) を再起動する必要があります。

ウェブインターフェイスでのシングルサインオンの有効化:

1. Acronis Cyber Files Web インターフェースを開き、管理者としてログインします。
2. **[全般設定]** タブを展開して、**[LDAP]** ページを開きます。
3. ページの最下部で、**[Windows/Macの既存のログイン資格情報を使用してウェブクライアントおよびデスクトップ同期クライアントからログインすることを許可します]** のチェックボックスをオンにします。
4. **[保存]** をクリックします。

SSO (シングルサインオン) サポートのためのブラウザの構成

ブラウザのシングルサインオンサポートを有効にするには、1 回限りのマイナーな構成を行う必要があります。

重要

それぞれのマシンでユーザーごとに実行する必要があります。

注意

この構成手順では、例として acme.com を使用します。複数のドメインにサービスがある場合は、すべてのドメインに acme.com を指定する手順を繰り返します。（たとえば、*.acme.com と *.another.com と *.yetanother.com を追加します）。

Acronis ドメインフォレスト内の Cyber Files

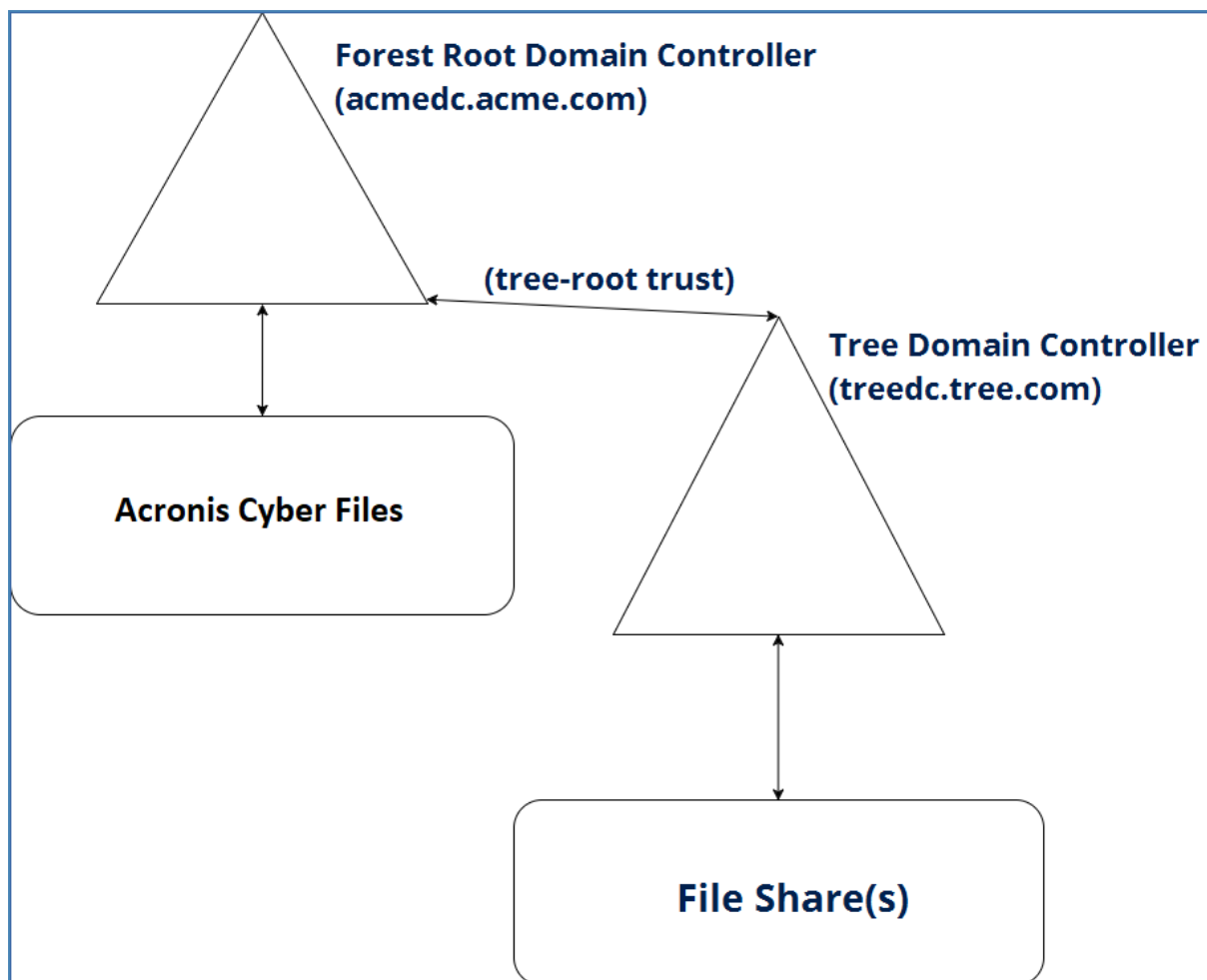
Windows Server 2012にはMicrosoftからリソーススペースの**Kerberos制約付き委任**が追加されており、これによりフォレスト間制約付き委任が可能になっています。そのため、導入環境で（同一フォレスト内の）複数のドメインにリソースがある場合でもシングルサインオンを使用することができ、リソースにゲートウェイサーバーをインストールする必要がありません。

注意

この機能を利用するには、フォレスト内のすべてのドメインが**ドメイン機能レベル 2012** 以上で稼働している必要があります。

この記事では、以下の作業を行う方法を説明します。

- Acronis Cyber Files サーバーを SSO 用にセットアップする。
- ゲートウェイサーバーをSSO用にセットアップする。
- フォレスト間制約付き委任を動作させるためのドメインでのすべての構成。
- SSOを使用するためにユーザーが行う必要のあるセットアップ。



要件

このガイドでは、単一のフォレスト内でマルチドメインを稼働させるための構成について説明します。現状で、LDAPが正しく構成されており、ユーザーが問題なくドメインにログインでき、フォレスト内のドメイン間の接続が正しく構成されていることを前提としています。

- このタイプの制約付き委任は、**ドメイン機能レベル2102**以上で稼働するドメインコントローラでのみ利用可能です。リソーススペースのKerberos制約付き委任は、Windows Server 2012で初めて可能になりました。
- **[グローバルカタログ]** が有効で動作している必要があります。

SSO（シングルサインオン）サポートのためのブラウザの構成

ブラウザのシングルサインオンサポートを有効にするには、1 回限りのマイナーな構成を行う必要があります。

重要

それぞれのマシンでユーザーごとに実行する必要があります。

注意

この構成手順では、例として acme.com を使用します。複数のドメインにサービスがある場合は、すべてのドメインに acme.com を指定する手順を繰り返します。（たとえば、*.acme.com と *.another.com と *.yetanother.com を追加します）。

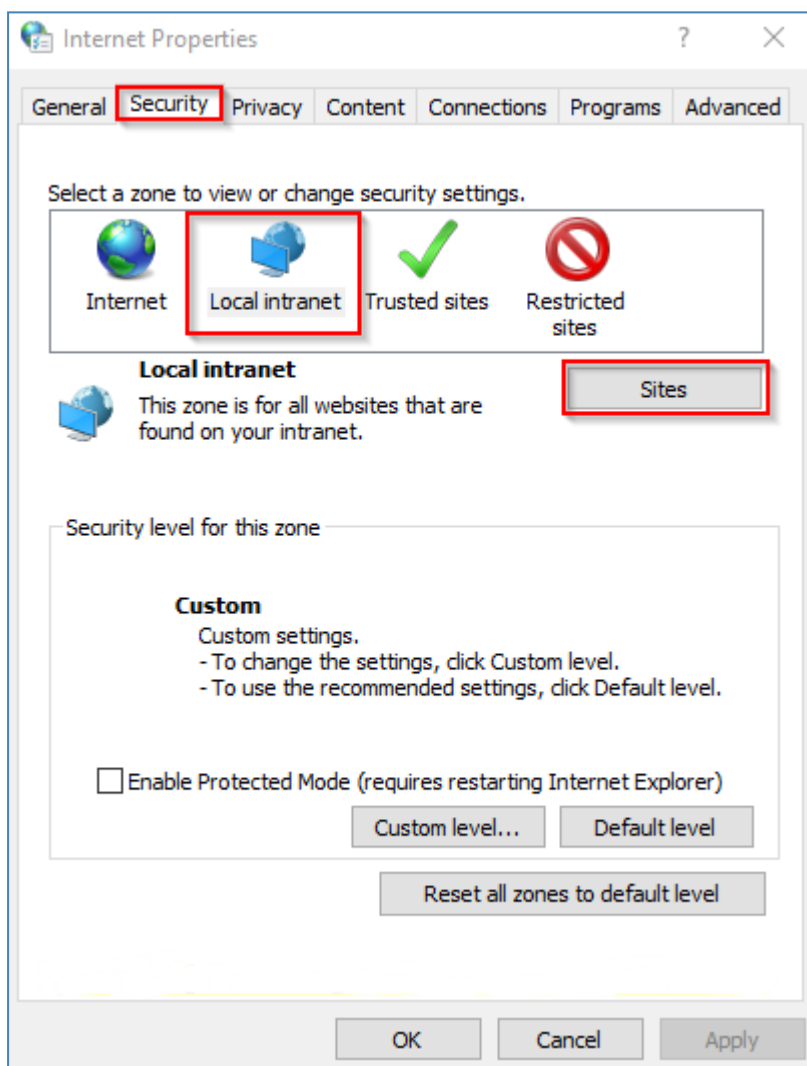
Windows 用の 1 回限りの構成

Microsoft Edge および Google Chrome の場合

Microsoft Edge と Google Chrome の両方の構成は、Microsoft Windows の [インターネットオプション] を使用して行われます。

Windows の [インターネットオプション] の構成

1. Windows の [コントロールパネル] を開きます。
2. [インターネットオプション] を選択します。
3. [セキュリティ] タブで、[ローカルイントラネット] をクリックします。



4. **[サイト]**、**[詳細]** の順にクリックします。
5. Acronis Cyber Files サーバーのアドレス（例、<https://ahsoka.acme.com> または単に *.acme.com）を追加します。
6. **[OK]** をクリックします。
7. ブラウザを再起動します。

Chrome で資格情報の委任を許可するには

重要

Web インターフェースからネットワークノードを参照するには、資格情報の委任が必要です。Microsoft Edge では、これはデフォルトで有効になっています。Chrome で資格情報の委任を有効にするには、許可するようにブラウザを構成する必要があります。

1. レジストリエディタ (**regedit32.exe**) を開きます。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome まで移動します。
3. まだ存在しない場合には Google\Chrome キーを作成します。
 - a. ポリシーフォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。
 - b. フォルダ名に「**Google**」と入力します。
 - c. **Google** フォルダを右クリックし、**[新規]** → **[キー]** の順に選択します。
 - d. フォルダ名に「**Chrome**」と入力します。
 - e. Chrome フォルダをクリックし、右側にあるホワイトパネルで右クリックして **[新規]** → **[キー]** の順に選択します。
 - f. キーの名前を入力します: AuthNegotiateDelegateWhitelist。
4. ドメイン名（たとえば、ahsoka.acme.com や *.acme.com）を AuthNegotiateDelegateWhitelist レジストリキーの値として設定します。
5. Chrome を再起動します。

Firefox の場合

1. アドレスバーに **about:config** と入力し、Enter キーを押します。
2. **network.negotiate-auth.trusted-uris** の設定を検索して編集し、<https://ahsoka.acme.com> または **just .acme.com**（カンマ区切りのリスト）を追加します。

注意

すべてのサブドメインを追加するには、「**.example.com**」という形式を使用します（***.example.com ではありません**）。

3. ネットワークの **[データソース]** サポートを有効にするには、**network.negotiate-auth.delegation-uris** を編集する必要もあります。具体的には、ahsoka.acme.com またはドメイン名 **acme.com** だけを追加します。
4. **Firefox** を再起動します。

Mac 用の 1 回限りの構成

注意

それぞれのマシンでユーザーごとに実行する必要があります。

Safari の場合

そのまま動作します。

Firefox の場合

1. アドレスバーに `about:config` と入力し、Enter キーを押します。
2. `network.negotiate-auth.trusted-uris` の設定を検索して編集し、`https://ahsoka.acme.com` または `just .acme.com` (カンマ区切りのリスト) を追加します。

注意

すべてのサブドメインを追加するには、「`.example.com`」という形式を使用します (`*.example.com` ではありません)。

3. ネットワークの [データソース] サポートを有効にするには、`network.negotiate-auth.delegation-uris` を編集する必要もあります。具体的には、`ahsoka.acme.com` またはドメイン名 `acme.com` だけを追加します。
4. **Firefox** を再起動します。

Chrome の場合

1. **Ticket Viewer** アプリケーション (`/System/Library/CoreServices/Ticket Viewer`) を使用して、Kerberos チケットがあるかどうかを確認し、自動的に作成されていなかった場合は作成することができます。

注意

`kinit` とパスワードを入力してから、**ターミナル** 経由でチケットを作成することもできます。

2. 使用するすべてのドメインに対する認証を許可するために Chrome の許可リストを設定するには、**ターミナル** を開いて次のコマンドを実行します。

```
$ defaults write com.google.Chrome AuthServerWhitelist "*.acme.com"
```

```
$ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist "*.acme.com"
```

3. Chrome ブラウザを再起動します。

Acronis Cyber Files サーバーの場合

シングルサインオン認証で使用するドメインアカウントの構成

1. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF\` に移動します。

2. ファイル `web.xml` を探して開きます。このファイルに、SSOサービスが実行されるドメインのユーザー名およびパスワードを設定します。

このアカウントは、以降のセクションでKerberosに**HTTP**サービスを登録するときに使用するアカウントと一致している**必要がある**ので、ここで書き留めておくことをお勧めします。

3. `web.xml` には、設定が必要になる 2 つのプロパティ（SSO サービスが使用するドメインのユーザー名およびパスワード）があります。以下に示す行を検索します。

```
<init-param>
  <param-name>spnego.preauth.username</param-name>
  <param-value>yourusername</param-value>
</init-param>
<init-param>
  <param-name>spnego.preauth.password</param-name>
  <param-value>yourpassword</param-value>
</init-param>
```

4. **yourusername** を目的のLDAPユーザー名に置き換えます。
5. **yourpassword** を、上記で指定したLDAPアカウントのLDAPパスワードに置き換えます。パスワードに 5 つの特殊文字、**&**、**>**、**"**、**'**、**<** のいずれかが含まれている場合は、それらを XML ドキュメント内で正しくエスケープする必要があります。これを行うには、次のように置き換える必要があります。

- **<** は **<**;
- **>** は **>**;
- **"** は **"**;
- **'** は **'**;
- **&** は **&**;

例: パスワードが `<my&best'password"` の場合は、`web.xml` ファイルに
「`<my&best'password"`」と書き込む必要があります。

Kerberos ドメインルックアップの設定

1. `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.59\conf` に移動します。
2. `krb5.conf` ファイルを検索して開きます。
3. `krb5.conf` には、管理者から受け取る必要があるプロパティが 2 つだけあります。
 - a. シングルサインオン用のドメイン（例: `ACME.COM`）。
 - これは、Acronis Cyber Files Web サーバーとゲートウェイサーバーがあるドメインである必要があります。
 - サーバーのDNS名**ではなく**、ご使用のドメインの名前であることに注意してください。

注意

`krb5.conf` のドメインには必ず**大文字**を使用してください。大文字を使用しない場合、Kerberos チケットの参照に失敗する場合があります。

- b. Kerberos キー配布センターのアドレス（通常、プライマリドメインコントローラーの **DNS** アドレスと一致します。例: `acmedc.ACME.COM`）。これは、Acronis Cyber Files とそのコンポーネントがあるドメイン内のドメインコントローラーのアドレスです。
4. インストールする `krb5.conf` ファイルの内容は次のようになります。

```
[libdefaults]
    default_realm = ACME.COM
    default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
    default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
    permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
    ACME.COM = {
        kdc = acmedc.ACME.COM
        default_domain = ACME.COM
    }

[domain_realm]
    .ACME.COM = ACME.COM
```

5. `ACME.COM` のすべてのインスタンスをドメイン（**大文字**）に置き換えます。サーバーのDNS名ではなく、ご使用のドメインの名前であることに注意してください。
6. "`kdc =`" の値をドメインコントローラーの DNS 名に置き換えます。ドメイン部分は大文字にする必要があります（例: `kdc = yourdc.YOURDOMAIN.COM`）。
7. 上記の設定ファイルのアップデート後、変更内容を適用するために、Acronis Cyber Files サーバー（Acronis Cyber Files Tomcat サービス）を再起動する必要があります。

Web インターフェースでのシングルサインオンの有効化

1. Acronis Cyber Files Web インターフェースを開き、管理者としてログインします。
2. **[全般設定]** タブを展開して、**[LDAP]** ページを開きます。
3. ページの最下部で、**[Windows/Macの既存のログイン資格情報を使用してウェブクライアントおよびデスクトップ同期クライアントからログインすることを許可します]** のチェックボックスをオンにします。
4. **[保存]** を押します。

SSOを処理するLDAPアカウントの設定

Acronis Cyber Files Web サーバー用の追加の DNS エントリの設定

同じマシンにゲートウェイサーバーがある場合は、Acronis Cyber Files Web サーバー用に別の DNS エントリが必要です。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]** を開いて右クリックし、Web サーバーに新しい **ホストエントリ** (A record) を作成します。

2. 名前を入力します。これは、Acronis Cyber Files Web サーバーへのアクセスに使用される DNS アドレスになります。
例:ahsokaccess.acme.com
3. Acronis Cyber Files Web サーバーの IP アドレスを入力します（ポートは入力しません）。同じ IP アドレスでゲートウェイサーバーと Acronis Cyber Files Web サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR）レコードを作成する]** を選択し、**[ホストの追加]** を押します。

Acronis Cyber Files Web サーバーの SPN の設定

1. Acronis Cyber Files が実行されているマシンで、コマンドプロンプトを開きます。

注意

setspn を使用する権限のあるドメインアカウントでログインする必要があります。

2. コマンド **setspn -s HTTP/access_DNS_name.domain.com account name** を入力します。

注意

このコマンドに使用される LDAP アカウント名は、web.xml ファイルで指定したアカウントと一致する必要があります。

- たとえば、Acronis Cyber Files Web サーバーが **ahsoka.acme.com** にインストールされており、認証済みの LDAP アカウントとして **john@acme.com** を使用して Kerberos チケットを付与する場合、コマンドは
setspn -s HTTP/ahsokaaccess.acme.com john のようになります。
- たとえば、Acronis Cyber Files Web サーバーが **ahsoka.acme.com** にインストールされており、認証済みの LDAP アカウントとして **jane@tree.com** を使用して Kerberos チケットを付与する場合、コマンドは
setspn -s HTTP/ahsokaaccess.acme.com tree\jane のようになります。

注意

通常、このアカウントは、Acronis Cyber Files の Web インターフェースの管理者によって **[LDAP の設定]** で指定された LDAP アカウントと一致します。ただし、必ずしも一致させる必要はありません。

3. Acronis Cyber Files Web サーバーがデフォルト以外のポート（443 以外のポート）で実行されている場合、ポート番号を使用して SPN を登録する必要もあります。

例:サーバーがポート 444 で実行されている場合、コマンドは

setspn -s HTTP/ahsokaaccess.acme.com:444 john または

setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane になります。

注意

上記のコマンドの **HTTP** は、**HTTP** プロトコルではなく **HTTP** サービスクラスを指しています。**HTTP** サービスクラスでは、**HTTP** と **HTTPS** の両方のリクエストが処理されます。サービスクラスの名前に**HTTPS**を使用してSPNを作成する必要はありません。また、**作成しないでください**。

4. ユーザーが利用しているドメインコントローラーにアクセスし、**[Active Directory ユーザーとコンピューター]**を開きます。ユーザーが利用するドメインが複数ある場合は、前のステップでを使用したユーザーが含まれるドメインを開きます。
5. 上記のコマンドで使用されているユーザーを検索します（この場合、**john**または**jane**）。
6. **[委任]** タブをクリックし、**[任意のサービスへの委任でこのユーザーを信頼する（Kerberosのみ）]**を選択します。この設定を有効にすると、LDAPオブジェクトが認証を任意のサービスに委任できるようになります。ここでは、ゲートウェイサーバーサービスに委任します。
7. **[OK]** をクリックします。

AcronisCyber Files にログインできることを確認する

1. ドメインコントローラーまたは Acronis Cyber Files Web サーバー以外のマシンに移動します。
2. Acronis Cyber Files ウェブ コンソールを開き、ログインページのパスワードフィールドの下にあるリンクを使用します。

注意

Acronis Cyber Files に招待されたドメインユーザー、既にログインしているドメインユーザー、またはプロビジョニング済み LDAP グループのメンバーであるドメインユーザーとして、そのマシンにログインする必要があります。

注意

ブラウザが SSO リクエストを受け入れるために、「[ユーザーマシン上](#)」セクションの手順をすべて行う必要があります。

ゲートウェイサーバー上

ゲートウェイサーバーのSPNの設定

KDC（「キー配布センター」）Kerberosサーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、**setspn**を実行してゲートウェイサービスをKDCサーバーに登録し、「ユーザー」として実行されているサーバーのホスト名を**setspn**コマンドで指定する必要があります。

ゲートウェイサーバーの追加DNSエントリの構成

この構成が機能するためには、ゲートウェイサーバーのDNSエントリも別個に設定する必要があります。

1. DNS サーバーで、ドメインの **[前方参照ゾーン]**を開いて右クリックし、ゲートウェイサーバーに新しい**ホスト**エントリ(A record)を作成します。

2. 名前を入力します。これは、ゲートウェイサーバーへのアクセスに使用されるDNSアドレスになります。
例: codygw.acme.com
3. ゲートウェイサーバーのIPアドレスを入力します（ポートは入力しません）。同じ IP アドレスでゲートウェイサーバーと Acronis Cyber Files サーバーを実行している場合は、その IP アドレスを入力します。
4. **[関連付けられたポインタ（PTR）レコードを作成する]** を選択し、**[ホストの追加]** を押します。

ローカルゲートウェイサーバーのSPNの構成

1. Acronis Cyber Files がインストールされているマシンに戻ります。
2. コマンドプロンプトを開きます。
3. ゲートウェイサーバーのSPNの設定:
 - a. ゲートウェイサーバーがローカルシステムアカウントとして実行している場合のコマンドは次のようになります。
b. setspn -s HTTP/gatewaydns.domain.com computername
たとえば、ゲートウェイサーバーがドメインのホスト 'cody' で実行されていて、DNSエントリが codygw.acme.com の場合は、次のコマンドを実行します。
setspn -s HTTP/codygw.acme.com cody
 - c. ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート）で実行されている場合は、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合は、
setspn -s HTTP/codygw.acme.com:444 cody とします。
4. まだ実行していない場合は、希望するゲートウェイサーバーの**管理のアドレス**を、作成したゲートウェイサーバー DNS エントリ（codygw.acme.com）に変更する必要があります。

SPNがゲートウェイ用に正しく設定されたことを確認する

1. ローカルゲートウェイ用のローカルボリュームがある場合、SSOを使用してログインすることにより、SPNと委任が機能していることを確認できます。この確認作業は、Acronis Cyber Files サーバーとドメインコントローラー以外のマシンで行います。そうしないと、SSO は機能しません。
2. ローカルゲートウェイのボリュームを参照します。参照できるなら、次に進みます。参照できない場合は、適切なオブジェクトに適切なSPNが正しく構成されているかを確認してください。

注意

リモートファイルサーバー上のボリュームを参照しようとする、アクセス拒否エラーになります。

リソースベース制約付き委任の設定

注意

このタイプの制約付き委任は、ドメイン機能レベル 2012R2 以上で稼働するドメインコントローラーでのみ利用可能です。ドメイン間のKerberos制約付き委任は、Windows Server 2012で初めて可能になりました。

リソースベース制約付き委任を使用して、ファイルサーバーまたは別のドメインにある他のネットワークリソースへのアクセス権をユーザーに付与することができます。

1. ファイルサーバーがあるドメインのドメインコントローラに移動して、**PowerShell**を開きます。
2. ゲートウェイサービスが**LocalSystem**アカウントとして実行している場合のコマンドは次のようになります。
 - a. **\$computer1 = Get-ADComputer -Identity <gateway_server_computer> -server <domain_controller_for_this_domain>**
例: `$computer1 = Get-ADComputer -Identity cody -server dc.acme.com`
このコマンドはゲートウェイサーバーのコンピューターオブジェクトを取得し、接続する AD ドメインサービスインスタンスを指定し、その情報を **\$computer1** 変数に保存します。
 - b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount \$computer1**
例: `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $computer1`
このコマンドは、ファイルサーバーコンピューターオブジェクトの **[Principals Allowed To Delegate To Account]** プロパティをゲートウェイサーバーのコンピューターオブジェクトに設定します。このように設定することにより、ゲートウェイサーバーコンピュータはファイルサーバーのコンピュータに委任することができます。
3. ゲートウェイサービスが**ユーザーアカウント**として実行している場合のコマンドは次のようになります。
 - a. **\$user1 = Get-ADUser -Identity <login_user_of_the_gateway_service> -server <domain_controller_for_this_domain>**
例: `$user1 = Get-ADUser -Identity jane -server dc.acme.com`
このコマンドは、ゲートウェイサーバーが実行するときのユーザーのオブジェクトを取得し、接続する AD ドメインサービスインスタンスを指定し、その情報を **\$user1** 変数に保存します。
 - b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount \$user1**
例: `Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount $user1`
このコマンドは、ファイルサーバーコンピューターオブジェクトの **[Principals Allowed To Delegate To Account]** プロパティを、ゲートウェイサーバーが実行するユーザーオブジェクトに設定します。このように設定することにより、選択したユーザーはファイルサーバーのコンピュータに委任することができます。
4. ゲートウェイユーザーアカウントが資格情報の委任先になり得るアカウントとして追加されたことを確認するには、次のコマンドを実行します。

Get-ADComputer <file_server_machine> -Properties

PrincipalsAllowedToDelegateToAccount

例: Get-ADComputer omega -Properties PrincipalsAllowedToDelegateToAccount

5. すべてのファイルサーバーにこれらのステップを繰り返します。

委任が伝播するにはいくらか時間がかかります。小規模なLDAP導入であれば10～15分、大規模な構造であればそれ以上の時間がかかります。

ゲートウェイサーバーの追加

注意

ゲートウェイサーバーをホストするマシンが Acronis Cyber Files Web サーバーと同じドメイン内にある場合にのみ、以下の手順が使えます。

KDC（「キー配布センター」）Kerberosサーバーによるゲートウェイサーバーへのユーザー認証を可能にするには、setspnを実行してゲートウェイサーバーをKDCサーバーに登録し、「ユーザー」として実行されているサーバーのホスト名をsetspnコマンドで指定する必要があります。

ゲートウェイサーバーが Acronis Cyber Files Web サーバーとは異なるマシンに存在する場合

1. コマンドプロンプトを開きます。
2. **setspn** コマンドとして **setspn -s HTTP/computername.domain.com computername** を入力します。

たとえば、ゲートウェイサーバーがドメインのホスト「cody」で実行されている場合は、次のコマンドを実行します。

```
setspn -s HTTP/cody.acme.com cody
```

3. ゲートウェイサーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNに登録する必要もあります。たとえば、ゲートウェイサーバーがポート444で実行されている場合、次のように登録します。

```
setspn -s HTTP/cody.acme.com:444 cody
```

4. 追加のゲートウェイサーバーすべてにこのセクションの手順を繰り返します。

別のドメインにあるゲートウェイサーバーの構成

リソーススペース Kerberos 制約付き委任へのアクセス権がない場合、リモート共有および別のドメインにあるリソースへのSSOを構成する別の方法は、そのドメイン内のマシンにゲートウェイサーバーをインストールする方法です。これにより、通常のKerberos制約付き委任を使用することができ、**機能レベル2008のドメインでも作業できます**。

対象のドメインのマシンにゲートウェイサーバーをインストールする

1. Acronis Cyber Files インストーラをダウンロードして、対象のマシンに移動します。
2. Acronis Cyber Files インストーラを起動し、ライセンス契約に同意してから、**[次へ]**を押します。
3. **[カスタム...]** インストールを選択して、ゲートウェイサーバーのチェックボックスのみを選択します。
4. **[インストール]**を押します。インストールが終了したら、インストーラを閉じます。
5. **設定ユーティリティ**で、ゲートウェイのIPアドレスとポートを設定します。

ゲートウェイサービスがユーザーアカウントとして実行するように設定する

1. **[コントロールパネル]** -> **[管理ツール]** -> **[サービス]**を開きます。
2. Acronis Cyber Files ゲートウェイサーバーサービスを探して、右クリックし、**[プロパティ]**を選択します。
3. **[ログオン]** タブを選択し、**[このアカウント]** ラジオボタンを選択します。
4. **[参照]**を押して検索するか、またはユーザーのユーザー名とパスワードを入力して、サービスを実行するときのユーザーを選択します。選択するユーザーは、Acronis Cyber Files がインストールされているのと同じドメインのユーザーでなければなりません。Acronis Cyber Files サーバーの SPN に使用するアカウントではなく、専用のアカウントを使用することをお勧めします。
5. **[OK]**を押して、**[サービス]** コントロールパネルを閉じます。選択したユーザーアカウントに必要な許可が設定されていない状態ではサービスが起動しないので、まだサービスは再起動しないでください。

選択したユーザーに必要な権限を付与する

1. サービスをユーザーとして実行するには、ユーザーに**オペレーティング システムの一部として機能**が付与され、ユーザーがローカル管理者グループに含まれている必要があります。
2. **[ローカルセキュリティポリシー]**を開いて、**[ローカルポリシー]** -> **[ユーザー権利の割り当て]**に移動します。この変更は、導入環境によっては**[グループポリシーマネージャー]**で行う必要があります。
3. **[オペレーティング システムの一部として機能]** オブジェクトを開き、**[ユーザーを追加]** または **[グループ]**を押します。
4. ゲートウェイサービスの専用ユーザーを選択します。
5. 開いているすべてのダイアログを閉じて、**[コントロールパネル]** -> **[ユーザーアカウント]** -> **[アカウントの管理]**を開きます。
6. **[追加]**を押して、専用アカウントのドメインとユーザー名を入力します。
7. これで、**[サービス]** コントロールパネルで Acronis Cyber Files ゲートウェイサービスを再起動できます。

リモートゲートウェイサーバーのSPNの構成

1. Acronis Cyber Files サーバーがあるドメインの任意のマシンに移動します。
2. コマンドプロンプトを開きます。
3. SPN を構成するために実行するコマンドは、次のとおりです。 **setspn -s**

HTTP/gatewaydns.domain.com useraccountfor_gw

例: ゲートウェイサーバーを **tree.com** ドメイン内のホスト 'magpie' で実行し、かつ **acme.com** ドメインの peter ユーザーアカウントとして実行する場合は、次のコマンドを実行します。

```
setspn -s HTTP/magpie.tree.com peter
```

ゲートウェイサーバーがデフォルト以外のポート（443 以外のポート）で実行されている場合は、ポート番号を使用して SPN を登録する必要もあります。たとえば、ゲートウェイサーバーがポート 444 で実行されている場合は、

```
setspn -s HTTP/magpie.tree.com:444 peter
```

 とします。

4. まだ実行していない場合は、希望するゲートウェイサーバーの**管理のアドレス**を、作成したゲートウェイサーバー DNS エントリ（magpie.tree.com）に変更する必要があります。
5. ゲートウェイサーバーの **[ユーザーモードでネゴシエート/Kerberos認証を実行します]** が有効になっていることを確認してください。この設定を有効にした後、Acronis Cyber Files ゲートウェイサービスを再起動する必要があります。
6. 2番目のドメインのリソース用に**データソース**を作成する際、同じドメインにあるゲートウェイサーバーを必ず使用してください。

例: ユーザーに repository.tree.com 上のファイルに対するアクセス権を付与する場合は、tree.com にあるゲートウェイサーバー（magpie.tree.com など）を指定する必要があります。

SPNがゲートウェイ用に正しく設定されたことを確認する

1. ローカルゲートウェイ用のローカルボリュームがある場合、SSOを使用してログインすることにより、SPNと委任が機能していることを確認できます。
2. ローカルゲートウェイのボリュームを参照します。参照できない場合は、適切なオブジェクトに適切なSPNが正しく設定されているかを確認してください。
3. 委任の変更が伝播するのに時間がかかる場合があります（小規模な LDAP 導入の場合は10～15分、大規模なLDAP導入の場合はそれ以上）。

SPN登録の確認

対象のSPNが適切に登録されたかどうかを確認するには、次の手順に従ってクエリを実行します。

1. [管理者特権でのコマンドプロンプト] を開きます。
2. **setspn -Q HTTP/computername.domain.com** コマンドを入力します。
例: `setspn -Q HTTP/ahsoka.acme.com`
3. 特定のドメインユーザーに登録されている SPN にクエリを実行するには、-l（小文字の l）スイッチを使用します。

例: `setspn -l john`

4. SPNの登録後、SSOを使用して認証できるようにするには、クライアントマシンを再起動するか、クライアントマシンで次のコマンドを実行する必要があります。

```
klist purge
```

SMBまたはSharePointデータソースの使用

SMBまたはSharePointのデータソースを使用する場合、Active Directoryアカウントを設定して、SMBおよびSharePointデータソースごとにKerberos委任を許可してください。

ネットワーク共有と SharePoint サーバーの場合の手順

次の手順を実行すると、ゲートウェイ サーバーからターゲット サーバーへの委任が可能になります。

1. **[Active Directory ユーザーとコンピューター]**を開きます。
2. ゲートウェイ サーバーに対応するコンピュータ オブジェクトを特定します。

注意

User アカウントを使用してゲートウェイサーバーを稼働させている場合は、代わりにその **User** オブジェクトを選択してください。

3. ユーザーを右クリックし、**[プロパティ]**を選択します。
4. **[委任]** タブを開きます。
5. **[指定されたサービスへの委任でのみこのコンピューターを信頼する]**をオンにします。
6. このセクションで、**[任意の認証プロトコルを使う]**を選択します。
7. **[追加]**をクリックします。
8. **[ユーザーまたはコンピューター]**をクリックします。
9. SMB 共有または SharePoint サーバーのサーバー オブジェクトを検索し、**[OK]**をクリックします。
 - SMB 共有の場合、**[cifs]** サービスを選択します。
 - SharePoint の場合、**[http]** サービスを選択します。
10. Acronis Cyber Files ゲートウェイサーバーがアクセスする必要があるサーバーごとに上記の手順を繰り返します。
11. ゲートウェイサーバーごとに上記のプロセスを繰り返します。

委任を変更する場合、ドメインフォレストのサイズによっては、反映が完了するまで数分かかることがあります。変更内容が有効になるまで、15分程度（場合によっては15分以上）待機する必要がある場合があります。15 分経過しても機能しない場合は、Acronis Cyber Files ゲートウェイサービスを再起動してください。

クライアント証明書認証でモバイルクライアントを使用する

これは、実行が必要な追加手順です。ゲートウェイサーバーと Acronis Cyber Files サーバーが同じマシン上にあるかどうかにかかわらず、ゲートウェイサーバーからこのサーバーへの委任を設定する必要があります。

Kerberos制約付き委任

この委任タイプは、Acronis Cyber Files サーバーとゲートウェイサーバーが同じドメイン内に存在する場合に機能します。

1. これを行うには、ドメインコントローラ上のActive Directoryを開きます。
2. ゲートウェイサーバーのコンピュータオブジェクトを検索して編集し、委任タブに移動します。
3. **[指定されたサービスへの委任でのみこのコンピューターを信頼する]** および **[任意の認証プロトコルを使う]** を選択します。
4. Acronis Cyber Files サーバーの SPN を選択するには、**[追加]** をクリックして、Acronis Cyber Files サーバーの **HTTP** SPN に関連付けられているアカウントのユーザー名を入力します。

注意

注意: Acronis Cyber Files サーバーが実行されているコンピューターを検索するのではなく、ユーザー名で検索してください。

注意

Acronis Cyber Files サーバーへの Kerberos 認証は、単一ポートモードとの互換性がありません。

5. ユーザーを検索すると **HTTP** サービスが表示されるため、これらのサービスを選択します（SPN をポート付きとポートなしで 2 回登録している場合は、サービスが 2 つ表示されることがあります）。
6. **[適用]** を押してすべてのダイアログを閉じます。

リソースベースのKerberos制約付き委任

この委任タイプは、Accessサーバーとゲートウェイサーバーがドメインフォレスト内の別々のドメインにある場合に機能します。

注意

この機能を利用するには、Acronis Cyber Files がアクセスするすべてのドメインを **ドメイン機能レベル 2012** 以上で稼働する必要があります。

1. Acronis Cyber Files サーバー専用で、SPN を設定した DNS エントリが実際に **[データソース]** ページで S&S ボリュームのアドレスとして設定されていることを再確認してください。
2. ゲートウェイサーバーと Acronis Cyber Files サーバーの間の委任を設定します。今回、委任はゲートウェイサーバーから Acronis Cyber Files サーバーへとなります。
3. 以下のユーザーに対して次のコマンドを実行します。

\$pc1 = Get-ADComputer -Identity <ゲートウェイマシンの名前>

Set-ADUser <Access_SSOユーザーアカウント> -PrincipalsAllowedToDelegateToAccount \$pc1

例: `$pc1 = Get-ADComputer -Identity ahsoka`

`Set-ADUser john -PrincipalsAllowedToDelegateToAccount $pc1`

4. ゲートウェイをユーザーアカウントとして実行している場合は、次のコマンドを使用して、2つのユーザーアカウントの間の委任として設定する必要があります。

\$user1 = Get-ADUser -Identity <ゲートウェイユーザーアカウント>

Set-ADUser <Access_SSOユーザーアカウント> -PrincipalsAllowedToDelegateToAccount \$user1

例: \$user1 = Get-ADUser -Identity gwuser

Set-ADUser john -PrincipalsAllowedToDelegateToAccount \$user1

委任が伝播するにはいくらか時間がかかります。小規模なLDAP導入であれば10～15分、大規模な構造であればそれ以上の時間がかかります。

負荷分散環境

ゲートウェイサーバーではオプションとして、ウェブサーバーによるKerberos/ネゴシエート認証を試行するのではなく、すべてのHTTP認証をユーザーモードで実行することを選択できます。このオプションは、単一または複数のゲートウェイのSSO処理を負荷分散装置の背後で実行する場合に必要になります。

この機能を有効にするには、Web インターフェースを開いて、**[モバイルアクセス]** → **[ゲートウェイサーバー]** の順に移動し、クラスターグループの **[編集]** オプションをクリックし、**[詳細設定]** に移動して、チェックボックス **[ユーザーモードでネゴシエート/Kerberos認証を実行します]** をオンにします。

ネットワークノードの有効化

SSOの使用中にウェブ内のネットワークノードにアクセスできるようにするためには、いくつかの変更が必要になります。ゲートウェイサーバーは負荷分散装置の背後で実行されているため、Kerberos への登録でコンピューター名ではなくユーザーアカウントを使用する必要があります。

このためには、ゲートウェイサービスをユーザーアカウントの下で実行する必要があります。Acronis Cyber Files サーバーが登録されている同じ LDAP ユーザーを使用するか、ゲートウェイサービス専用の新規の LDAP ユーザーを選択できます。

どちらの場合も、選択したユーザーに対して、ゲートウェイサーバーがインストールされているマシン上でオペレーティングシステムの一部として機能するための権限を与える必要があります。

オペレーティングシステムの一部として機能するユーザーの選択

1. ゲートウェイサーバーがインストールされているマシンで **[スタート]** → **[ファイル名を指定して実行]** の順にクリックします。
2. 「**gpedit.msc**」と入力し、**[OK]** を押します。
3. **[Windows の設定]** → **[セキュリティの設定]** の順に展開します。
4. **[ローカル ポリシー]** を展開し、**[ユーザー権利の割り当て]** をクリックします。
5. リストで **[オペレーティング システムの一部として機能]** を右クリックし、**[プロパティ]** を選択します。
6. このウィンドウで、ユーザーおよびグループの追加や削除ができます。目的のユーザー名を入力し、

[OK] を押します。

7. 残りのウィンドウをすべて閉じ、変更を有効にするためにサーバーを再起動します。

ゲートウェイサーバーのサービスを選択したユーザーアカウントとして実行する

サービスとして実行するユーザーを追加したら、ゲートウェイサービスをそれらのユーザーとして実行するように設定する必要があります。これを行うには、次の手順に従います。

1. ゲートウェイサーバーがインストールされているマシンで [スタート] → [ファイル名を指定して実行] の順にクリックします。
2. 「**services.msc**」と入力し、[OK] を押します。または、[コントロール パネル] を開き、[管理ツール] → [サービス] の順に移動します。
3. リストで [Acronis Cyber Files ゲートウェイ] を右クリックし、[プロパティ] を選択します。
4. [ログオン] タブをクリックします。
5. [このアカウント:] ラジオボタンを選択し、オペレーティングシステムの権限を与えたユーザーの資格情報を入力します。
6. [OK] をクリックしてすべてのウィンドウを閉じます。

ゲートウェイサーバーのSPNの設定

キー配布センターKerberosサーバーによるゲートウェイクラスターへのユーザーの認証を可能にするためには、それぞれのゲートウェイサーバーとゲートウェイの負荷分散装置をKDCサーバーに登録する必要があります。それには、**setspn**を実行してアカウント名を指定します（サービスはこのアカウントとして実行されます）。

1. コマンドプロンプトを開きます。
2. 次のコマンドを入力します。

```
setspn -s HTTP/computername.domain.com username
```

たとえば、ゲートウェイサービスがユーザー **john** として実行されている場合のコマンドは次のようになります。

```
setspn -s HTTP/gatewayserver1.acme.com john
```
3. ゲートウェイサーバーがデフォルト以外のポート（443以外のポート）で実行されている場合、ポート番号を使用してSPNを登録する必要もあります。たとえば、ゲートウェイサーバーがポート444で実行されている場合、次のように登録します。

```
setspn -s HTTP/gatewayserver1.acme.com:444 john
```
4. それぞれのゲートウェイサーバーと負荷分散装置について、上記の手順を繰り返します。負荷分散装置のSPNは次のようになります。

```
setspn -s HTTP/gwloadbalancerdns.acme.com john
```

注意

2 つのゲートウェイ間でトラフィックを分割する負荷分散装置（このケースでは `gwloadbalancerdns.acme.com`）がある場合は、これを登録しないでください。登録すると、要求の半分が正しいゲートウェイ（ローカル側）に到達しません。LB サーバーが要求を誤ったゲートウェイに転送すると、ログインが失敗します。DNS 名で起動後の他のサービスを指すことはできません。

これ以上のサポートについては、サポートチームにお問い合わせください。

シングルサインオンのトラブルシューティング

- デスクトップクライアントまたは Web クライアントのユーザーは、Acronis Cyber Files サーバーを実行しているコンピューターとは別の（ただし、同じドメイン内の）コンピューターを使用する必要があります。そうでなければ、SSO を使用できません。
- デスクトップクライアントからのシングルサインオンには、企業ネットワークへの接続が必要です。これは、SSO ユーザーは自身のネットワークへのアクセスも必要であることを意味します。
- サーバーへのアクセスには、SPN の場合と全く同じ FQDN を使用してください（`https://ahsoka.acme.com` など）。他の DNS 名や IP アドレスは使用できません（`https://localhost`、`https://10.20.56.33` など）。
- SSO を使用せずに、クライアントの Windows コンピューターと全く同じ LDAP 資格情報を入力して、Acronis Cyber Files サーバーにログインできることを確認します。これにより、SSO の設定にかかわらず、アカウントの資格情報が Acronis Cyber Files に対して有効であることが確認されます。
- SSO を使用せず、LDAP のログインアカウントと同じ資格情報を使用して、すべてのデータソースにアクセスできることを確認します。
- SSO を介してログインできない場合は、接続先の FQDN に対して SSO 用のウェブブラウザを設定していること、ドメインアカウントを使用してクライアントコンピューターにログインしていることを再確認してください。
- Acronis Cyber Files サーバーがドメインコントローラーで実行されている場合、シングルサインオンは機能しません。
- Acronis Cyber Files では、ドメインコントローラーのコンピューターからアクセスする場合、SSO は機能しません。

注意

Kerberos の仕様により、ドメインコントローラーまたは Acronis Cyber Files サーバー上で実行されているクライアントアプリケーションや Web ブラウザからは、SSO 認証を行うことができません。

注意

また、Acronis Cyber Files サーバーがドメインコントローラー上で実行されている場合、Acronis Cyber Files サーバーからドメインコントローラーへの認証を行うことはできません。

- SSO を使用してログインする際に **401エラー**が発生する場合には、**web.xml** ファイル内のユーザー名およびパスワードを確認し、特殊文字を適切にエスケープしてください。。特殊文字は **&**、**>**、**"**、

、またはくです。これらのエスケープ方法については、**web.xml ファイルの編集**セクションの**手順 5**を参照してください。

Acronis Cyber Files での信頼されたサーバー証明書の使用

このセクションでは、信頼できるサーバー証明書を使用して Acronis Cyber Files を設定する方法について説明します。

デフォルトで、Acronis Cyber Files はテスト目的の自己生成 SSL 証明書を提供します。信頼できる証明機関によって署名された証明書を使用することにより、サーバーの識別情報が確立され、エラーなしにクライアントが接続できるようになります。

注意

自己署名証明書を使用している場合、Web ブラウザで警告メッセージが表示されます。これらのメッセージを無視すると、テスト目的でシステムを使用できます。

本番環境での自己署名証明書の使用はサポートされていません。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。

証明書の要求の作成

注意

証明書の作成は、現在 Acronis Cyber Files の機能ではなく、今後もその予定はありません。証明書の要求は、証明書ベンダから求められるものであり、Acronis Cyber Files の操作には必要ありません。

注意

ベンダからサーバータイプを選択するよう求められた場合は、**IIS** を選択してください。証明書を Windows 証明書ストアにインストールして、Acronis Cyber Files が証明書を使用できるようにする必要があります。

IIS を介して証明書の要求を作成する

この手順に関する詳細については、Microsoft のナレッジベースの記事 ([http://technet.microsoft.com/ja-jp/library/cc732906\(v=ws.10\).aspx](http://technet.microsoft.com/ja-jp/library/cc732906(v=ws.10).aspx)) を参照してください。

OpenSSL を介して証明書の要求を作成する

注意

このガイドでは、OpenSSL がインストールされている必要があります。

注意

この手順に関する詳細やサポートについては、希望する証明書ベンダにお問い合わせください。

ウェブサーバー「AAServer」用の秘密キーおよび公開CSR（証明書署名要求）のペアを生成するには、次の手順を実行します。

1. 管理者特権でコマンドプロンプトを開き、次のコマンドを入力します。

```
openssl req -new -nodes -keyout myserver.key -out AAServer.csr -newkey rsa:2048
```

2. このコマンドにより2つのファイルが作成されます。**myserver.key**のファイルには秘密キーが含まれています。このファイルは公開しないでください。秘密キーを紛失した場合、秘密キーのバックアップ以外にリカバリできる方法はないため、必ずバックアップを実行するようにしてください。**CSR（証明書署名要求）**を生成するには、秘密キーをコマンドの入力として使用します。

注意

「警告: 構成ファイル: /usr/local/ssl/openssl.cnf を開くことができません」のようなエラーが表示された場合は、コマンド「**set OPENSSL_CONF=C:¥OpenSSL-Win64¥bin¥openssl.cfg**」を実行し、OpenSSL がインストールされている場所に依じて、パスを変更してください。この手順を完了した後に、最初の手順をもう一度実行してください。

3. CSRに登録される詳細情報を入力するように要求されます。ウェブサーバーの名前を**コモンネーム（CN）**として使用します。ドメイン名が**mydomain.com**である場合は、そのドメイン名にホスト名を追加します（完全修飾ドメイン名を使用してください）。
4. ウェブサーバー証明書の場合、Eメールアドレス、任意の会社名、およびチャレンジパスワードのフィールドは空白にすることができます。
5. CSRが作成されました。証明書ベンダから要求された場合は、**server.csr**をテキストエディタで開き、内容をコピーしてオンライン登録フォームに貼り付けます。

Windows 証明書ストアへの証明書のインストール

要件

使用する証明書には証明書の秘密キーが含まれている必要があります。証明書ファイルは、**.PFX** または **.P12** のいずれかのファイル形式である必要があります。

これらは互換であるため、どちらを使用しても問題ありません。

注意

証明書ベンダから証明書とキーが2つの別々のファイルとして提供された場合、次のコマンドを使用して、それらのファイルを1つの **.PFX** ファイルに結合することができます。

```
openssl pkcs12 -export -in <yourcertificate.extension> -inkey <yourkey.extension> -out <newfile.pfx>
```

例: `openssl pkcs12 -export -in acmecert.crt -inkey acmecertkey.key -out acmecombed.pfx`

このコマンドを実行するには、OpenSSLがインストールされている必要があります。

Windows 証明書ストアへの証明書のインストール

注意

使用している証明書が Acronis Cyber Files サーバーとゲートウェイサーバーで異なる場合は、両方の証明書に次の手順を行ってください。

1. サーバーで **[スタート]**、**[ファイル名を指定して実行]** の順にクリックします。
2. **[開く]** ボックスに「mmc」と入力し、**[OK]** をクリックします。
3. **[ファイル]** メニューの **[スナップインの追加と削除]** をクリックします。
4. **[スナップインの追加と削除]** ダイアログ ボックスで **[追加]** をクリックします。
5. **[スタンドアロンスナップインの追加]** ダイアログボックスで **[証明書]** をクリックしてから **[追加]** をクリックします。
6. **[証明書スナップイン]** ダイアログ ボックスで **[コンピューター アカウント]** をクリックしてから（デフォルトでは選択されていません）**[次へ]** をクリックします。
7. **[コンピューターの選択]** ダイアログボックスで **[ローカルコンピュータ]**（このコンソールを実行しているコンピューター）をクリックしてから **[完了]** をクリックします。
8. **[スタンドアロン スナップインの追加]** ダイアログ ボックスで **[閉じる]** をクリックします。
9. **[スナップインの追加と削除]** ダイアログ ボックスで **[OK]** をクリックします。
10. コンソールの左側のウィンドウで **[証明書（ローカルコンピュータ）]** をダブルクリックします。
11. **[個人]** を右クリックして **[すべてのタスク]** をポイントし、**[インポート]** をクリックします。
12. **[証明書のインポート ウィザードの開始]** ページで **[次へ]** をクリックします。
13. **[インポートするファイル]** ページで **[参照]** をクリックし、証明書ファイルを探して **[次へ]** をクリックします。

注意

PFX ファイルをインポートする場合は、ファイル フィルタを **“Personal Information Exchange (*.pfx, *.p12)”** に変更して、このファイルの種類を表示する必要があります。

14. 証明書にパスワードがある場合は、**[パスワード]** ページにパスワードを入力してから **[次へ]** をクリックします。
15. 以下のチェックボックスをオンにします。
 - a. **このキーをエクスポート可能にする**
 - b. **すべての拡張プロパティを含める**
16. **[証明書ストア]** ページで **[証明書をすべて次のストアに配置する]** をクリックし、**[次へ]** をクリックします。
17. **[完了]** をクリックしてから **[OK]** をクリックし、インポートが正常に実行されたことを確認します。

Acronis Cyber Files 構成ユーティリティを使用するとき、Windows 証明書ストアで正常にインストールされた証明書はすべて使用できます。

証明書を使用するように Cyber Files を設定する

Windows 証明書ストアに証明書を正常にインストールしたら、その証明書を使用するように Acronis Cyber Files を設定する必要があります。

1. Acronis Cyber Files 設定ユーティリティを起動します。Windowsの **[スタート]** メニューにショートカットがあるはずです。

注意

デフォルトでは、設定ユーティリティは C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility にあります。

2. [ウェブサーバー] タブで [...] ボタンを押して、リストから証明書を選択します。
3. [モバイルゲートウェイ] タブで [...] ボタンを押して、リストから証明書を選択します。
4. [適用] をクリックします。これにより、ウェブ サービスが再起動し、約1分後にはオンラインに戻って、選択した証明書が使用された状態になります。正しい証明書が使用されているかを確認できます。

中間証明書の使用

証明機関により証明書と共に中間証明書が発行されている場合、設定ユーティリティで Acronis Cyber Files サーバーに追加する必要があります。

注意

設定ユーティリティは**中間証明書**証明書ストア内のみを検索します。証明書が他のいずれかのストアにインストールされている場合は、**certmgr.msc**を開いて、中間証明書を今あるストアから**中間証明書認証局 -> 証明書**ストアに移動します。

1. Acronis Cyber Files 設定ユーティリティを起動します。Windowsの [スタート] メニューにショートカットがあるはずです。

注意

デフォルトでは、設定ユーティリティは C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility にあります。

2. [ウェブサーバー] タブで [...] ボタンを押して、リストから証明書を選択します。
3. [チェーン証明書] フィールドの横にあるプラス (+) ボタンを押して、使用する**中間証明書**をリストから選択します。希望する証明書がリストにない場合は、その証明書が正しくインストールされたか、およびどのストアにインストールされたかを確認してください。
4. [モバイルゲートウェイ] タブで [...] ボタンを押して、リストから証明書を選択します。中間証明書には、それ以上の追加の手順は必要ありません。
5. [適用] をクリックします。その後サービスが再起動するので、オンラインに戻ったら、選択した証明書が使用されているか確認できます。

複数のデスクトップクライアントバージョンのサポート

最新バージョンとは別のバージョンの Acronis Cyber Files デスクトップクライアントを使用する場合は、次の手順に従ってください。

1. 使用するバージョンのデスクトップクライアントをダウンロードします。次の4つのファイルがあることを確認します。

- ACFCClientMac.zip
 - ACFCClientInstaller.msi
 - AcronisCyberFilesInstaller.dmg
 - AcronisCyberFilesClientInstaller.exe
2. ファイルをコピーします。
 3. サーバーで、Acronis Cyber Files デスクトップクライアントフォルダ（C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\clients）を開きます。
 4. クライアントのこのバージョン用にサブフォルダを作成します。（8.5.0x664、8.6.2x632 のように）**クライアントのバージョン番号**で名前を付けてください。
 5. 作成したサブフォルダに 4 つのファイルを貼り付けます。
 6. 次に、Acronis Cyber Files サーバーの **Web ユーザーインターフェース**を開きます。
 7. **管理者**としてログインして **[Sync & Share]** タブに移動し、**[Acronis Cyber Files クライアント]** ページを開きます。
 8. **[クライアントの自動バージョン アップデートを許可]** 設定を探します。
 9. ドロップダウン メニューから、目的のバージョンを選択します。

注意

アカウントの**操作メニュー**のダウンロードリンクでは、利用可能な最新の Acronis Cyber Files デスクトップクライアントバージョンがダウンロードされます。ユーザーが最新バージョンをダウンロードしないようにするには、**¥Acronis¥Acronis Cyber Files¥Access Server¥Web Application¥clients** フォルダに移動し、最新のクライアントバージョン（8.6.2x632 など）のフォルダ名を「**（バージョン番号）は使わない**」（「**8.6.2x632 は使わない**」など）に変更します。

デフォルト以外のロケーションへの FileStore の移動

サービスがローカルシステムアカウントとして実行している

1. Cyber Files がインストールされているコンピュータに移動します。
2. **Cyber Files File Repository** サーバーと **Cyber Files Tomcat** サービスを停止します。
3. **構成ユーティリティ**で選択したフォルダに、現在の**FileStore**が見つかります。デフォルトの場所は C:\ProgramData\Acronis\Acronis Cyber Files\FileStore です。
4. **FileStore**フォルダ全体をそのすべての内容とともに、希望するロケーションにコピーするか移動します。
たとえば、D:\MyCustom Folder\FileStore のようにします。

注意

ファイルストアがリモートネットワーク共有にある場合は、**ファイルリポジトリ**サービスが実行中であるコンピューターに、ネットワーク共有の**ファイルストア**フォルダに対する完全なアクセス権が必要です。

5. **設定ユーティリティ**を開きます。
6. **[ファイルリポジトリ]** タブで、**FileStore** フォルダを移動した新しいパスに**FileStore**のパスを変更します。
7. **Acronis Cyber Files ファイルリポジトリサーバー**サービスを開始します。
8. **Acronis Cyber Files Tomcat** サービスを起動して、**[サービス]** コントロールパネルを閉じます。

サービスがユーザーアカウントとして実行している

1. Cyber Files がインストールされているコンピュータに移動します。
2. **Cyber Files File Repository サーバー**と **Cyber Files Tomcat** サービスを停止します。
3. **構成ユーティリティ**で選択したフォルダに、現在の**FileStore**が見つかります。デフォルトの場所は C:\ProgramData\Acronis\Acronis Cyber Files\FileStore です。
4. **FileStore**フォルダ全体をそのすべての内容とともに、希望するロケーションにコピーするか移動します。
たとえば、D:\MyCustom Folder\FileStore のようにします。
5. **設定ユーティリティ**を開きます。
6. **[ファイルリポジトリ]** タブで、**FileStore** フォルダを移動した新しいパスに**FileStore**のパスを変更します。
7. **ファイルストア**がリモートネットワーク共有にある場合は、**ファイルリポジトリ**サービスが実行中であるユーザーアカウントに、ネットワーク共有の**ファイルストア**フォルダに対する完全なアクセス権が必要です。
8. このアカウントには、ログファイルを書き込むため、ローカル**リポジトリ**フォルダ（たとえば、C:\Program Files (x86)\Acronis\Acronis Cyber Files\File Repository\Repository）への読み取り/書き込みアクセス権限も必要です。
9. **Acronis Cyber Files ファイルリポジトリサーバー**サービスを開始します。
10. **Acronis Cyber Files Tomcat** サービスを起動して、**[サービス]** コントロールパネルを閉じます。

New Relic による Acronis Cyber Files の監視

この種類のインストールでは、Acronis Cyber Files サーバー アプリケーションがインストールされている実際のコンピュータではなく、このサーバー アプリケーションそのものを監視できます。

1. <http://newrelic.com/> を開き、New Relic アカウントを作成するか、既存のアカウントでログインします。上記の手順を完了すると、アプリケーションの設定画面に進みます。
2. アプリケーション タイプには **[APM]** を選択します。
3. プラットフォームには **[Ruby]** を選択します。
4. New Relic Starting Guide の手順 3 に示されている New Relic のスクリプト（newrelic.yml）をダウンロードします。
5. Acronis Cyber Files ウェブ コンソールを開きます。
6. **[設定]** → **[監視]** に移動します。

7. 拡張子も含めて、newrelic.yml へのパスを入力します (C:\software\newrelic.yml など)。Acronis Cyber Files フォルダ以外のフォルダにこのファイルを配置し、アップグレード時やアンインストール時に削除や変更されないようにすることをお勧めします。
8. **[保存]** をクリックし、New Relic サイトで **[Active application(s)]** ボタンが有効になるまで数分間待機します。
9. 10 分以上経過したら、Acronis Cyber Files Tomcat サービスを再起動して数分待機します。これでボタンがアクティブになります。
10. New Relic の Web サイトで Acronis Cyber Files サーバーを監視できます。

注意

New Relic への接続や監視の設定に関して Acronis Cyber Files サーバーがログに記録するすべての情報は、C:\Program Files (x86)\Acronis\Common\apache-tomcat-7.0.34\logs にある **newrelic_agent.log** というファイルにあります。問題が発生した場合は、このログファイルで情報を検索できます。

注意

次のような内容で始まる警告やエラーが頻繁に発生することがあります。

「警告: IP アドレスをキャッシュ中に DNS エラーが発生しました: Errno::ENOENT: このようなファイルまたはディレクトリはありません - C:/etc/hosts」これは、New Relic の別のバグのパッチに使用されているコードの副次的な影響であり、問題はありません。

実際のコンピュータも監視する場合は、次の手順に従います

1. <http://newrelic.com/> を開き、自分のアカウントでログインします。
2. [サーバー] を押し、オペレーティング システムに合った New Relic インストーラをダウンロードします。
3. New Relic モニタをサーバーにインストールします。
4. New Relic サーバー モニタには Microsoft .NET Framework 4 が必要です。New Relic インストーラのリンクは Microsoft .NET Framework 4 Client Profile 専用です。New Relic Server Monitor インストーラを実行する前に、Microsoft Download Center に移動してインターネットから .NET 4 Framework 全体をダウンロードしてインストールする必要があります。
5. New Relic がサーバーを検出するまで待機します。

複数のポートでの Acronis Cyber Files Tomcat の実行

設定ユーティリティがサポートする Tomcat サービスの設定は1つのポートだけに限られますが、Tomcat 自体は複数のポートで実行するように構成できます。それは、Tomcat の server.xml ファイルに追加のコネクタと希望するポートを追加することにより行うことができます。アップグレードや設定ユーティリティによる Tomcat サービスの再起動を行っても、新しいコネクタへの影響はありません。

注意

この構成は、既に 1 回は設定ユーティリティを実行しており、Tomcat サービスが正常に開始した後に行うことをお勧めします。

追加のTomcatコネクタの構成

1. Acronis Cyber Files Tomcat サービスが実行中である場合は、このサービスを停止します。
2. server.xml ファイルを検索して開きます。これはデフォルトでは C:\Program Files (x86)\Acronis\Files Advanced\Common\apache-tomcat-7.0.59\conf にあります。

注意

パスに含まれている番号 (7.0.59) は、使用している Tomcat のバージョンによって異なります。

3. ファイルを参照して、次のような **Connector** セクションを探します。

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="$
{catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW
:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
address="0.0.0.0" port="443"/>
```

注意

使用するテキストエディタによっては、**server.xml** を開いたときに、上記のコードが 1 行で表示される場合があります。

注意

設定ユーティリティ で **443** 以外のポートを選択した場合は、上の例にある **Connector** セクションにそのポートがリストされます。

4. **Connector** セクション全体をコピーして、コピーを元のセクションの下に貼り付けてください。両方のセクションが同じレベルのインデントでなければなりません。
5. 次の例のように、**443** (または **設定ユーティリティ** で選択したポート) を、Tomcat を起動させるために指定する 2 番目のポートに置き換えます。

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="$
{catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW
:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
address="0.0.0.0" port="4430"/>
```

注意

新しい **Connector** のコードが既存のコードと同じように書かれていること、つまり古いコードが単一の行で書かれている場合は、新しい行も同じようになっていることを確認します。

6. Acronis Cyber Files Web インターフェースを開き、**[全般設定]** → **[サーバー設定]** に移動します。
7. **[ウェブアドレス]** フィールドに指定されているアドレスに、Connectorセクションに指定されているポートのいずれかが使用されていることを確認します。これは、ユーザーへの招待メールに表示されるアドレスで、それに選択できるポートは1つだけです。

Acronis Cyber Files のマルチホーム設定

Acronis Cyber Files ゲートウェイと Acronis Cyber Files サーバーのマルチホームは、設定ユーティリティを使用して簡単に設定できます。

必要となるのは、2つの別々のネットワークインターフェイスとIPアドレスのみです。

マルチホームの設定

1. Acronis Cyber Files 設定ユーティリティを開きます。
2. **[ウェブサーバー]** タブを開き、1つ目の IP アドレスと 443 ポートを入力します。
3. **[ゲートウェイサーバー]** タブを開き、2つ目のIPアドレスと443ポートを入力します。
4. **[OK]** をクリックします。

注意

Microsoft では、Windows Server 2008 で TCP/IP スタックの動作方法を完全に変更しました。単一の IP トランスポートで複数のレイヤがサポートされ、「プライマリ」IP アドレスはなくなりました。このため、単一インターフェイスに複数の IP アドレスを割り当てると、すべてのアドレスは均等に扱われて、すべて DNS に登録されます。言い換えると、この動作はバグではなくて設計によるものです。ただし、これについて何の対処も行わないと、使用するIPアドレスはラウンドロビン（DNS）になるため、この動作は問題の原因となります。

NIC でダイナミック DNS 登録を無効にしてホスト DNS エントリを手動で作成すると、これを回避できます。**KB975808**:<http://support.microsoft.com/?kbid=975808> に記載されている修正プログラムをインストールして、簡単に回避することもできます。ホットフィックスをインストールすると、`netsh skipassource` フラグを使用できるようになります。新しいアドレスを追加しているときにこのフラグを使用すると、新しいアドレスを発信パケットに使用しないようにスタックに指示することになります。このため、これらの IP アドレスは DNS サーバーで登録されません。次の例を参考にしてください。

```
netsh int ipv4 add address "Local Area Connection" 192.168.1.2 skipassource=true
```

複数のウェブプレビューサーバーレットのデプロイ

Acronis Cyber Files のウェブプレビュー機能を使用すれば、ファイル全体をダウンロードしなくてもファイルの内容を確認できます。ユーザーが多い場合には、パフォーマンスが低下することがあります。これに対処するために、ウェブプレビューサーバーレットを使用して追加の Tomcat サーバーをセッ

トアップできます。これにより、ウェブプレビューを処理し、メインの Acronis Cyber Files サーバーを支援できます。

負荷分散装置を一連の Tomcat サーバーの前方に配置して、ウェブプレビューサーブレットの負荷をさらに分散させることができます。プレビューリクエストにはどの状態も必要ないため、負荷分散装置の特別な構成は必要ありません。

注意

パスワードで保護されたファイルにはサムネイルがないため、プレビューできません。

サーブレットのインストールと構成

Tomcat のインストール

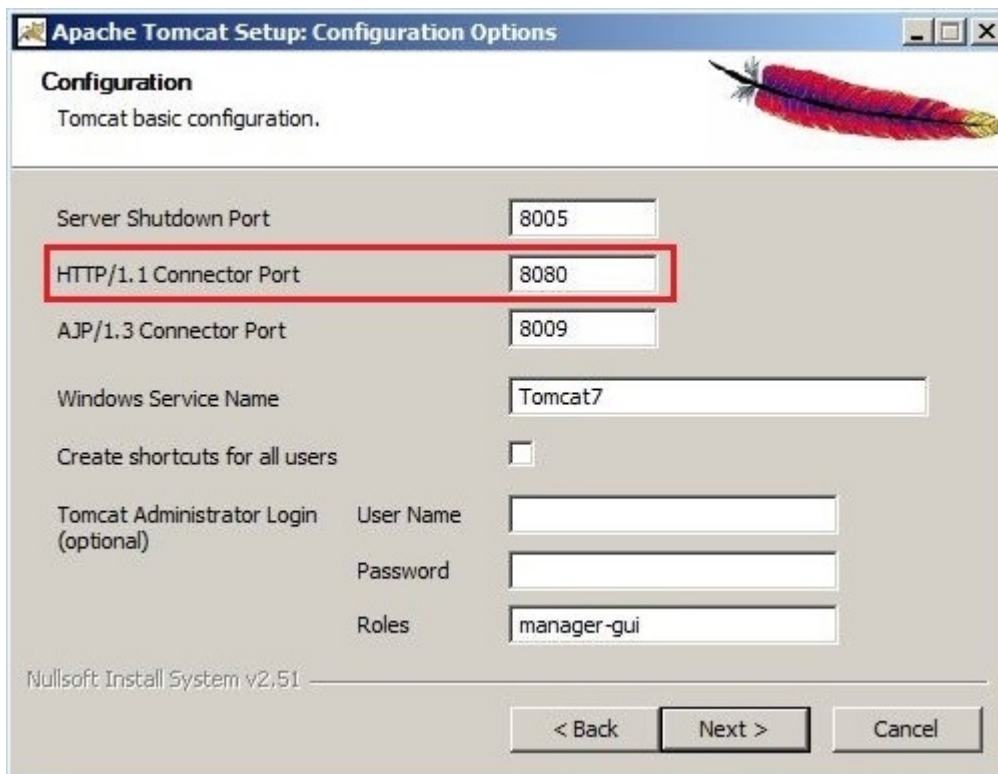
Apache Tomcat 9.0.88 サーバーは、.zip ファイルまたはインストール実行ファイルでインストールできます。インストーラの使用をお勧めしますが、.zip アーカイブも機能します。唯一の違いは、Apache Tomcat 9.0.88 サーバーを設定する方法です。

両方のシナリオの要件:

1. 64 ビットの Java Runtime Environment (JRE) がインストールされていることを確認します。64 ビットの Java Development Kit (JDK) でも問題ありません。Java はバージョン 8u412 以降を使用する必要があります。
2. 64 ビットの Apache Tomcat 9.0.88 をダウンロードします。使用するバージョンが、Acronis Cyber Files でサポートされているものよりも新しいバージョンは使用しないでください。Acronis Cyber Files で使用されるバージョンは、Acronis Cyber Files リリース履歴ドキュメントの冒頭に記載されています。

インストール実行可能ファイルの使用

1. Apache Tomcat 9.0.88 の 64 ビットバージョンの .zip インストールファイルをダウンロードします。バージョンの一覧は、[Apache Tomcat のサイト](#) で確認できます。目的のバージョンを見つけてクリックし、bin フォルダを開いて、.exe ファイル (**apache-tomcat-9.0.88.exe** など) をダウンロードします。
2. インストーラを開始して、インストールウィザードの手順に従います。デフォルト設定のすべてを使用できます。必要に応じてリスンポートを変更できます。デフォルトは 8080 です。



The image shows the 'Apache Tomcat Setup: Configuration Options' dialog box. It has a title bar with standard window controls and a feather icon. The main area is titled 'Configuration' with the subtitle 'Tomcat basic configuration.' Below this, there are several configuration options: 'Server Shutdown Port' (8005), 'HTTP/1.1 Connector Port' (8080, highlighted with a red rectangle), 'AJP/1.3 Connector Port' (8009), 'Windows Service Name' (Tomcat7), 'Create shortcuts for all users' (unchecked checkbox), and 'Tomcat Administrator Login (optional)' with fields for 'User Name', 'Password', and 'Roles' (manager-gui). At the bottom, there is a 'Nullsoft Install System v2.51' label and three buttons: '< Back', 'Next >', and 'Cancel'.

Apache Tomcat Setup: Configuration Options

Configuration
Tomcat basic configuration.

Server Shutdown Port: 8005

HTTP/1.1 Connector Port: 8080

AJP/1.3 Connector Port: 8009

Windows Service Name: Tomcat7

Create shortcuts for all users: ☐

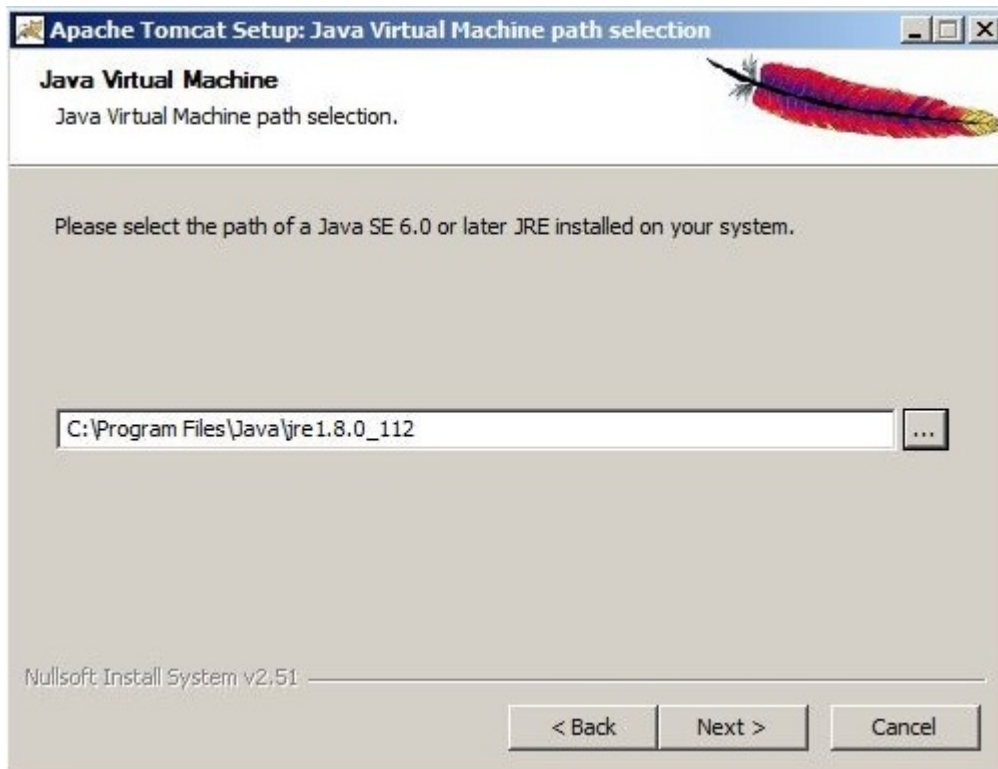
Tomcat Administrator Login (optional):
User Name:
Password:
Roles: manager-gui

Nullsoft Install System v2.51

< Back Next > Cancel

注意

インストーラが自動的に Java インストールフォルダを取得します。



The image shows the 'Apache Tomcat Setup: Java Virtual Machine path selection' dialog box. It has a title bar with standard window controls and a feather icon. The main area is titled 'Java Virtual Machine' with the subtitle 'Java Virtual Machine path selection.' Below this, there is a text prompt: 'Please select the path of a Java SE 6.0 or later JRE installed on your system.' A text field contains the path 'C:\Program Files\Java\jre1.8.0_112' and a browse button (...). At the bottom, there is a 'Nullsoft Install System v2.51' label and three buttons: '< Back', 'Next >', and 'Cancel'.

Apache Tomcat Setup: Java Virtual Machine path selection

Java Virtual Machine
Java Virtual Machine path selection.

Please select the path of a Java SE 6.0 or later JRE installed on your system.

C:\Program Files\Java\jre1.8.0_112

Nullsoft Install System v2.51

< Back Next > Cancel

3. インストールが完了したら、Acronis Cyber Files がインストールされているコンピューター上で、Acronis Cyber Files のインストールフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Access Server\）に移動します。
4. **AccessPreviewServlet** フォルダを Apache Tomcat がインストールされている新しいマシンにコピーし、Tomcat の **webapps** フォルダ（デフォルトでは C:\Program Files\Apache Software Foundation\Tomcat 9.0.88\webapps）に貼り付けます。
5. Apache Tomcatインストールの **conf**フォルダ（デフォルトでは C:\Program Files\Apache Software Foundation\Tomcat 9.0.8\conf）に移動し、**server.xml** ファイルをバックアップします。
6. このファイルを開いて、<Host name="localhost" appBase="webapps"unpackWARs="true" autoDeploy="true"> 行を探し、そのすぐ下に以下を追加します。

```
<!-- for Access Web preview -->
```

```
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Software Foundation\Tomcat 9.0.88\webapps\AccessPreviewServlet">
```

```
</Context>
```

注意

デフォルト以外の場所に Apache Tomcat をインストールした場合は、インストールの正しいパスを反映するように **docBase=""** パスを編集する必要があります。

7. ファイルを保存して終了します。
8. Tomcat Serviceを開始するには、[コントロール パネル] -> [管理ツール] -> [サービス] を開いて、Apache Tomcat Serviceを開始します。

アーカイブされたApache Tomcatインストールの使用

1. Apache Tomcat 9.0.88 の 64 ビットバージョンの **.zip** ファイルをダウンロードします。バージョンの一覧は、[Apache Tomcat のサイト](#) で確認できます。目的のバージョンを見つけてクリックし、binフォルダを開いて、コアの .zip ファイル（**apache-tomcat-9.0.88.zip** など）をダウンロードします。
2. アーカイブの内容を **C:\Program Files\Apache Tomcat** などの好きな場所に展開します。
3. **C:\Program Files\Apache Tomcat\apache-tomcat-<version>** に移動して、**bin** フォルダを開きます。

注意

展開先のフォルダ名にはバージョン番号が含まれているため、<version> を Tomcat のバージョンで置き換え、**C:\Program Files\Apache Tomcat\apache-tomcat-9.0.88** のようにします。

4. テキスト編集プログラムで **startup.bat** を開き、**setlocal** 行を探します。
5. その下に次の行を追加します。

```
set "CATALINA_HOME=Your Tomcat Folder"
```


e.g. set "CATALINA_HOME=C:\Program Files\Apache Tomcat\apache-tomcat-9.0.88"

注意

すべての設定に対するデフォルトの Tomcat フォルダが設定されます。Apache Tomcat フォルダの適切なパスを使用します。

```
set "JRE_HOME=Java main folder location"
```

e.g. set "JRE_HOME=C:\Program Files\Java\jre1.8u412"

注意

すべての設定に対するデフォルトの JRE フォルダが設定されます。Java フォルダの適切なパスを使用します。

注意

JDK を使用している場合は、コマンドが **JRE_HOME** ではなく **JAVA_HOME** になります。

6. ファイルに加えた変更を保存します。
7. インストールが完了したら、Acronis Cyber Files がインストールされているコンピューター上で、Acronis Cyber Files のインストールフォルダ（デフォルトで C:\Program Files (x86)\Acronis\Files Advanced\Access Server\）に移動します。
8. **AccessPreviewServlet** フォルダを Apache Tomcat がインストールされている新しいマシンにコピーし、Tomcat の **webapps** フォルダ（デフォルトでは C:\Program Files\Apache Tomcat\apache-tomcat-9.0.88\webapps）に貼り付けます。
9. Apache Tomcat のインストールの **conf** フォルダ（**C:\Program Files\Apache Tomcat\apache-tomcat-9.0.88\conf** など）に移動して、**server.xml** ファイルをバックアップします。
10. このファイルを開いて、<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true"> 行を探し、そのすぐ下に以下を追加します。

```
<!-- for Access Web preview -->
```

```
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Tomcat\apache-tomcat-9.0.88\webapps\AccessPreviewServlet">
```

```
</Context>
```

11. 正しいインストールのパスを反映するように docBase="" パスを編集します。ファイルを保存して終了します。

注意

サーバーがリスンしているデフォルトポートを変更しなかった場合は、サブレットは **8080** 上でリスンします。ポート変更するには、**server.xml** ファイルで次の行を探します。

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
```

8080を必要なポート番号に置き換えます。

12. Tomcatサービスを開始するには、binフォルダに移動して、**startup.bat** ファイルをダブルクリックします。Tomcatの実行中は、黒色のDOSウィンドウを開いたままにする必要があります。

Acronis Cyber Files サーバーの設定

1. Acronis Cyber Files Web インターフェースを開き、**[全般設定]** -> **[ウェブのプレビュー]** を開きます。
2. **[ウェブプレビューのサービスにカスタムURLを使用]** を有効にし、新しいウェブプレビューサブレットのアドレスを入力します(例: `http://accesswp.company.com:8080`)。指定した URL にポート番号が含まれている必要があります。負荷分散構成またはクラスター構成を使用している場合、このURLにロードバランサのアドレスを入力します。
3. ウェブプレビューサブレットを実行するようにセットアップしたサーバーの台数によっては、Acronis Cyber Files サーバーに設定する **[最大同時生成呼び出し回数]** の数を増やす必要があります。
4. **[最大同時生成呼び出し数]** 設定を探して、それに適切な値を設定します。
デフォルト値は2です。ドキュメントのレンダリングに1つのプロセッサコアの大部分が使用される可能性があります。レンダリングスレッドの数は、使用可能なプロセッサコアの50%以下に設定する必要があります。この推奨値を超えた場合は、サーバー上の他のサービスのパフォーマンスが低下する可能性があります。

ウェブのプレビューサブレットの負荷分散

[ウェブのプレビュー] サブレットはロードバランサの背後に配置する必要があります。

1. 負荷分散装置で時間ベースのセッション スティッキネス（またはご使用の負荷分散装置での同等の設定）を有効にし、期限切れにならないように設定します。
2. ヘルスチェック（HTTPステータス200が返されることを確認する）が必要な場合は、
`http://servername.yourdomain.com:port/AccessPreviewServlet/generate_preview/`にpingを送信することで可能になります。
例: `https://servlet1.acme.com/AccessPreviewServlet/generate_preview` と
`https://servlet2.acme.com/AccessPreviewServlet/generate_preview`。
3. ブラウザでロードバランサのアドレスを開き、構成が機能していることを確認します。
例: `https://loadbalancer.yourdomain.com`

PostgreSQLのストリーミングレプリケーション

このドキュメントの目的は、2台のPostgreSQLサーバー間でストリーミングレプリケーションを構成する手順を詳細に説明することです。ストリーミングレプリケーションは、PostgreSQLデータベースのオンライン状態を維持するために存在する多くの方法の1つです。その他の方法については、ここでは取り上げません。

注意

このドキュメントでは、PostgreSQL や Acronis Cyber Files のインストール処理については説明しません。ストリーミングレプリケーションの構成のみを説明します。

ストリーミングレプリケーション

ストリーミングレプリケーションは、ログ先行書き込み（WAL）セグメントに基づいています。WALは、データの整合性を確認する標準的な方法です。WALの基本的な概念とは、データファイル（テーブルおよびインデックスがおかれる場所）への変更は、必ずそれらの変更がログに記録された後（つまり、変更を記述したログレコードが永続的ストレージに書き込まれた後）に行われるということです。この手順に従えば、クラッシュが起きてもログを使用してデータベースを復元できるので、トランザクションのコミットのたびにデータページをディスクにフラッシュする必要はありません。データページに適用されなかったすべての変更は、ログレコードから再生できます。

WALを使用すれば、ディスクへの書き込みが大幅に低減されます。ディスクにログファイルをフラッシュするだけでトランザクションのコミットを保証できるため、トランザクションで変更されたデータファイルをすべてフラッシュする必要がなくなります。ログファイルはシーケンシャル書き込みのため、ログファイルの同期のコストはデータページのフラッシュのコストよりもかなり低くなります。

WALにより、オンラインバックアップ、特定時点の復元とレプリケーションのサポートも可能になります。ストリーミングレプリケーションとは、レプリケーション接続でwalsenderプロトコルを使用し、プライマリサーバーとスタンバイサーバーの間のTCP/IP接続を介してWALレコードを継続的に送信することです。ストリーミングレプリケーションは同期も可能ですが、同期処理に必要なリソースおよびパフォーマンスへの影響を考えた結果、効果的なシナリオとして非同期ストリーミングレプリケーションのみを考慮することにしました。

要件:

- 2台のPostgreSQLサーバー: この手順内では、アクティブサーバーを「プライマリサーバー」と呼び、パッシブサーバーを「スタンバイサーバー」と呼びます。

注意

Acronis Cyber Files の接続には、プライマリサーバーしか使用できません。 スタンバイサーバーを使用できるのは、フェイルオーバーが発生し、スタンバイサーバーがプライマリに昇格した場合のみです。

- PostgreSQL 11.6: 「レプリケーションスロット」など、PostgreSQL 11.21 を必要とする機能を実装します。このバージョンは Acronis Cyber Files 8.7 以降に組み込まれており、新規インストールの場合にのみ使用されます（アップグレードの際は使用されません）。
- 1 つの仮想 IP（任意）: この仮想 IP は、Acronis Cyber Files サーバーの役割を実行するすべてのフロントエンドで使用され、常にアクティブホスト（プライマリサーバー）によって所有される必要があります。
- 事前に Acronis Cyber Files をインストールし、プライマリサーバーのデータベースを初期化しておくことをお勧めします。

プライマリサーバー上

レプリケーションユーザーの作成

このユーザーは、レプリケーション処理で WAL をプライマリサーバーからスタンバイサーバーに送信する際に使用されます。セキュリティ上の理由から、デフォルトのスーパーユーザーアカウント（例: **postgres**）ではなく、レプリケーションのアクセス許可を持つ専用ユーザーを作成することをおすすめします。

1. プライマリサーバーで次のコマンドを実行します。

```
psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -U postgres
```

次のオプションを使用して、リモートからこのコマンドを実行することもできます。

```
psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -h <IP_OF_PRIMARY_SERVER> -U postgres
```

注意

PSQL は、PostgreSQL のインストールフォルダの **bin** サブフォルダ内にあります。PATH 環境変数によっては、コマンドの実行前に、コマンドへのパスの指定や、正しいディレクトリへの移動が必要になることがあります。この注意は、この手順で使用する以下のコマンドにも適用されます。

アクセス権の構成

プライマリサーバー上のアクセス制御を編集して、スタンバイサーバーからの接続を許可します。

1. そのためには、**pg_hba.conf** ファイル（**data** サブフォルダ内）を編集して、次の行を追加します。
2. データベースサーバー間でより高いセキュリティが求められる場合には、認証の際にクライアントに暗号化パスワード（md5）を要求することができます。この場合、オプションとして SSL 暗号化（**hostssl**）を使用するよう要求することもできます。例:

```
host replication replicator <スタンバイサーバーの IP>/32 trust
hostssl replication replicator <スタンバイサーバーの IP>/32 md5
```

ストリーミングレプリケーションの構成

1. PostgreSQL のインストールフォルダに移動します。デフォルトの場所は、

C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<バージョン> です。

2. [データ] フォルダで、`postgresql.conf` ファイルに移動して変更します。次の行に移動して編集します。

注意

これらの行の前に # 記号が付いていないことを確認してください。付いている場合、コマンドがコメントとして扱われ、有効になりません。

```
listen_addresses = 'IP_OF_PRIMARY_SERVER, 127.0.0.1'
```

3. 上記の変更を加えた後で、PostgreSQLサービスを再開します。

レプリケーションスロットの作成

1. プライマリサーバーで次のコマンドを実行します。

```
psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"
```

2. 次のコマンドを使用して、スロットが作成されていることを確認します。

```
psql -U postgres -c "SELECT * FROM pg_replication_slots;"
```

スタンバイサーバー上

必要なすべてのサーバーの相互アクセスの確認

フェールオーバーの際には、スタンバイサーバーがプライマリサーバーに昇格し、すべての Acronis Cyber Files サーバーのリクエストに応答します。

すべての Acronis Cyber Files サーバーのスタンバイサーバーに対するアクセスを今すぐ設定することをお勧めします。設定すると、フェールオーバーの際にスタンバイサーバー上の PostgreSQL サービスの再起動が不要になります。

注意

スタンバイサーバーがスタンバイモードのときは、そのデータベースは読み取り専用モード（ホットスタンバイ）です。誤ってスタンバイサーバーが本番データベースとして設定され、使用されることはありません。

1. スタンバイサーバー上のアクセス制御を編集して、すべての Acronis Cyber Files サーバーからの接続を許可します。
2. そのためには、PostgreSQL のインストールフォルダに移動し、**pg_hba.conf** ファイル（data サブフォルダ内）を編集して、各サーバーについて次の行を追加します。

```
host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
```

```
host all all <IP_OF_CYBER_FILES_SERVER_1>/32 md5
```

ストリーミングレプリケーションの構成

1. PostgreSQL のインストールフォルダに移動します。デフォルトの場所は、

C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\<version> です。

2. Data フォルダで、`postgresql.conf` ファイルに移動して、これを変更します。次の行を検索して編集します。

注意

これらの行の前に `#` 記号が付いていないことを確認してください。付いている場合、コマンドがコメントとして扱われ、有効になりません。

- `listen_addresses = 'IP_OF_STANDBY_SERVER, 127.0.0.1'`
- `hot_standby = on`

`hot_standby` 設定は、ストリーミングレプリケーション中に接続してクエリを実行できるかどうかを指定します。この設定を有効にすると、データベースは読み取り専用リクエストを受け入れるため、データベース参照が可能になります。そして、データベーステーブルの内容を参照してレプリケーション処理が動作していることを確認できます。

注意

`listen_addresses` パラメータについては、`postgresql.conf` ファイル内で行の重複が可能です。この場合、コメント化された最初の行はデフォルトのファイルテンプレートの一部として存在し、コメント化されていない 2 番目の行は製品のインストーラにより追加されます。このような場合は、最初の行のみを編集し、コメントになっている他の行はコメントのままにしてください。

注意

プライマリサーバーで `postgresql.conf` ファイルの `max_connections` 設定をデフォルト値以外の値に変更した場合、スタンバイサーバーでも同様に変更する必要があります。

注意

`pg_hba.conf` で指定された認証方法として `md5` または `password` を使用する場合は、その接続のためにパスワードが必要になります。このパスワードを「入力」するには、スタンバイサーバーの `recovery.conf` ファイルに次のコマンドを追加する必要があります：

```
primary_conninfo = 'host=<IP_ADDRESS_OF_PRIMARY_SERVER> port=<PORT_OF_PRIMARY_SERVER> user=<USERNAME> password=<PASSWORD_FOR_USERNAME>'
```

たとえば、IP 10.0.0.1 のポート 5432 で、ユーザー `replicator` とパスワード 1234 で実行されている Postgres を探す場合には、`primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'` となります。

3. データベースの初期シーディングを実行してストリーミングレプリケーション処理を開始するには、セカンダリサーバー上の PostgreSQL サービスを停止してください。

構成ファイルのバックアップ

`pg_hba.conf`、`postgresql.conf`、`pg_ident.conf` を含むすべての `.conf` 構成ファイルのバックアップを作成します。これらのファイルは初期シーディングの処理で上書きされるため、この手順の後に復元する必要はありません。

dataディレクトリのクリーンアップ

dataサブフォルダを削除（または単に名前を変更）します。フォルダの名前変更は、以前の構成のコピーを維持するには良い手段です。フォルダの名前変更により、初期シーディング中またはデータベースの起動時に問題が発生した場合に、スタンバイサーバーのデータベースを整合性のとれた状態に戻すことができます。

初期シーディング

初期シーディングは、プライマリデータベースのバックアップを使用して、スタンバイサーバー上のフォルダで行われます。

1. プライマリサーバーがアクティブで、使用中でないことを確認してください。Acronis Cyber Files Tomcat サービスをいったん停止し、シーディングが完了したら開始するのが最も簡単な方法です。
2. スタンバイサーバーレベルで初期シーディングを開始するには、次のコマンドを使用します。

```
pg_basebackup.exe -h <IP_OF_PRIMARY_SERVER> -D <PATH_TO_NEW_DATA_DIR> -U replicator -v -P --slot=access_slot
```

注意

<PATH_TO_NEW_DATA_DIR> は、新しい Data フォルダのパスである必要があります。たとえば、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\11.21\Data などです。

構成ファイルの復元

すべての **.conf** 構成ファイル（**pg_hba.conf**、**postgresql.conf**、**pg_ident.conf** など）を、バックアップフォルダから新しい Data フォルダにコピーして、既存のすべてのファイルを上書きします。

レプリケーションスロットの作成

1. セカンダリサーバーで次のコマンドを実行します。

```
psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"
```

2. 次のコマンドを使用して、スロットが作成されていることを確認します。

```
psql -U postgres -c "SELECT * FROM pg_replication_slots;"
```

ストリーミングレプリケーションの制御

1. Data フォルダを開き、**recovery.conf** ファイルを作成（または修正）します。
2. まだ存在しない場合には次の行を追加します。

- standby_mode = 'on'
- primary_conninfo = 'host=<IP_OF_PRIMARY_SERVER> port=5432 user=replicator password= <PASSWORD_USED_FOR_REPLICATOR_USER>'
- primary_slot_name = 'access_slot'
- trigger_file = '<PATH_TO_TRIGGER_FILE>' # As an example 'failover.trigger'
- recovery_min_apply_delay = 5min

3. 上記の変更を加えた後に、スタンバイサーバー上でPostgreSQLサービスを開始します。

注意

フェールオーバーの場合、`recovery.conf` ファイルの名前が `recovery.done` に変更されます。

追加情報

- `standby_mode` 設定で、PostgreSQL サーバーをスタンバイとして開始する指定ができます。この場合、アーカイブされた WAL の末尾に達してもサーバーは復元を停止しません。`primary_conninfo` 設定（スタンバイサーバーからプライマリサーバーへの接続文字列）で指定されたプライマリサーバーに接続し、新しい WAL セグメントを取得して復元を継続しようとします。
- `primary_slot_name` 設定を使用して、プライマリサーバー上で以前のステップで作成されたレプリケーションスロットを使用します。
- `trigger_file` 設定は、トリガファイル（存在するとスタンバイサーバーでの復元が終了してスタンバイサーバーがプライマリサーバーになる）を指定します。この設定はフェールオーバーの処理中に使用されます。
- 任意で、`recovery_min_apply_delay` 設定も使用できます。デフォルトでは、スタンバイサーバーはプライマリサーバーから可能な限り早く WAL レコードを復元します。データの遅延コピーを使用すると、データ損失エラーを修正する機会が得られ、有用な場合があります。このパラメータを使用して、指定した期間復元を遅延できます。単位を指定しない場合、ミリ秒とみなされます。

このパラメータに「5 min」を指定すると、プライマリサーバーからレポートされたコミット時刻がスタンバイサーバーのシステム時刻よりも5分以上過去のトランザクションである場合のみ、スタンバイサーバーによってトランザクションコミットが再発行されます。

サーバー間のレプリケーション遅延がこのパラメータ値を超えている可能性もあります。そのような場合、遅延は追加されません。遅延は、プライマリサーバーで書き込まれた WAL タイムスタンプと、スタンバイサーバーの現在時刻で計算されることに注意してください。ネットワークラグやカスケードレプリケーション構成を原因とする転送遅延によって、実際の待機時間が大きく短縮されることがあります。プライマリサーバーとスタンバイサーバーのシステム時刻が同期していない場合には、復元時に予期するより早くレコードが適用される可能性があります。ただし、サーバー間の一般的な時刻差よりも、このパラメータで実用的とされる設定のほうのはるかに大きいため、大きな問題にはなりません。

フェールオーバーのテスト

フェールオーバーを本番のセットアップで実装する場合は、事前に上記の設定でテストを行い、フェールオーバーが正常に機能することを確認することをおすすめします。

プライマリサーバーがダウンしていない場合は、先にプライマリサーバーを停止し、それから、プライマリサーバーの役割を引き継ぐようにスタンバイサーバーを設定する必要があります。これは、プライマリサーバーがクエリの処理を続けることで生じる問題の発生を回避するためです。

スタンバイサーバーをプライマリサーバーにするには、**`recovery.conf`** に記載されているトリガファイルを作成します。プライマリサーバーの役割がスタンバイサーバーに引き継がれたら、Acronis Cyber Files サーバーがスタンバイサーバーを使用するように設定されていることを確認します。

注意

フェールオーバーのプロセスが起動されて正常に完了すると、`recovery.conf` ファイルの名前が `recovery.done` に変更されます。トリガファイルは削除されます。

この操作を行うには、`C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server` に移動して `acronisaccess.cfg` を編集します。`DB_HOSTNAME` と `DB_PORT` が、現在プライマリサーバーになっている方の PostgreSQL サーバーのアドレスとポートを指していることを確認します。変更を加えた場合には、Acronis Cyber Files Tomcat サービスを再開する必要があります。

インスタンスの移行

1. このアップグレードを行うには、Acronis Cyber Files を停止してダウンタイムを確保する必要があります。
2. プライマリとスタンバイの両方の PostgreSQL サーバーも停止します。
3. "PostgreSQL の新しいメジャーバージョンへのアップグレード" (222ページ) からの手順に従って、プライマリサーバーをアップグレードします。
4. 同じ PostgreSQL のメジャーバージョンをスタンバイサーバーにインストールします。
5. [プライマリサーバー](#)と[スタンバイサーバー](#)の両方で使用可能なストリーミングレプリケーション手順に従います。

リモートアクセス用PostgreSQLの構成

重要

リモート管理は、PostgreSQL 9 サーバーでのみサポートされています。

PostgreSQLの複数のインスタンスを管理する場合、またはデータベースを単にリモートで管理したい場合には、リモートアクセスが役立ちます。

このPostgreSQLインスタンスへのリモートアクセスを有効にするには、次の手順を実行してください

1. PostgreSQL のインストールディレクトリ `C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\Data\` に移動します。
2. **pg_hba.conf**をテキストエディタで編集します。
3. リモートアクセスを有効にする各コンピューターのホストエントリを、内部アドレスを使用して組み込み、ファイルを保存します。**pg_hba.conf** (HBAはホストベース認証を表します) ファイルは、クライアント認証を制御するもので、データベースクラスターのデータディレクトリに保存されます。このファイルで、接続を許可するサーバーと権限を指定します。たとえば、次のように指定します。
データベースユーザーのアドレスメソッドを入力
最初の Acronis Cyber Files とゲートウェイサーバー
`host all all 10.27.81.3/32 md5`

2 番目の Acronis Cyber Files ゲートウェイサーバー

```
host all all 10.27.81.4/32 md5
```

In these examples all users connecting from the first computer (10.27.81.3/32) and the second computer (10.27.81.4/32) can access the database with full privileges (except the replication privilege) via a md5 encrypted connection.

4. 移動して、**postgresql.conf**を開きます。これは、デフォルトで C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\PostgreSQL\9.4\Data\ に配置されています。
 - a. #listen_addresses = 'localhost' という行を探します。
 - b. 行の先頭にある「#」記号を削除してコマンドを有効にします。
 - c. 利用可能なアドレスすべてをリッスンするために、「localhost」を「*」に置き換えます。
PostgreSQLで特定のアドレスのみをリッスンするには、「*」のかわりにIPアドレスを入力します。
 - 例listen_addresses = '*' - PostgreSQL が利用可能なすべてのアドレス上でリッスンすることを意味します。
 - 例listen_addresses = '192.168.1.1' - PostgreSQL がそのアドレス上でのみリッスンすることを意味します。
5. **postgresql.conf**に加えた変更を保存します。
6. Acronis Cyber Files PostgreSQL サービスを再起動します。

注意

PostgreSQL は、デフォルトでポート 5432 を使用します。使用するすべてのファイアウォールまたはルーティングソフトウェアでこのポートが開放されていることを確認してください。

PostgreSQL 11 インストール後の「postgres」アカウントのパスワード変更

以下の手順を実行してください

1. Acronis サービスを停止します。
 - a. Win+R キーを押して、services.msc と入力し、Enter キーを押して Windows Services アプレットを開きます。
 - b. 変更中にサーバーがデータベースをアクティブに使用しないように、**Acronis Cyber Files Tomcat** サービスを停止します。
2. 構成ファイルをバックアップします。手順については、[「Cyber Fileデータベースのバックアップ」](#)を参照してください。
3. pgAdmin 4 を使用してパスワードを変更します。
 - a. [スタート] メニューから、**Acronis Cyber Files PostgreSQL管理者**を開きます。
 - b. プロンプトが表示されたら、マスターパスワードを入力します。
 - c. 左側のパネルで、[サーバー] を展開し、[localhost] を選択します。
 - d. トップメニュー で、[オブジェクト] > [パスワードの変更] をクリックします。

- e. 現在のパスワードを入力し、新しいパスワードを設定し、**[OK]** をクリックして変更を保存します。
4. Acronis 設定をアップデートします。
 - a. C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server に移動し、`acronisaccess.cfg` ファイルを開きます。
 - b. `DB_PASSWORD` = 行を探し、新しく設定したパスワードでアップデートします。
 - c. ファイルを保存して、元のファイルを置き換えます（管理者権限が必要な場合があります）。
5. サービスを再起動します。
 - a. Windows Services アプレットに戻り（Win+R、`services.msc` と入力）、**Acronis Cyber Files Tomcat** サービスを再起動します。
6. 変更内容をテストします。
 - a. サービスを再起動したら、Acronis Cyber Files サーバーにログインして、データベース接続が新しいパスワードで動作することを確認してください。
 - b. 問題が発生した場合は、設定ファイルを復元してサービスを再起動し、変更を元に戻します。

HTTP モードでの Acronis Cyber Files の実行

Acronis Cyber Files と内部サービス（負荷分散ソリューションやプロキシソリューションなど）の間で暗号化されていない HTTP 通信を使用する必要がある場合に備えた設定が用意されています。セキュリティで保護されていないローカルネットワークやインターネットで通信を行う Acronis Cyber Files サーバーは、常に HTTPS モードで動作する必要があります。内部で HTTP モードで動作していると、内部ネットワークにアクセス可能であれば、誰でも Acronis Cyber Files ネットワークトラフィックを簡単に見られるようになってしまいます。

HTTPS から HTTP に切り替えるには、次のファイルで一部の設定を変更する必要があります。

- Tomcat の `server.xml` ファイル。これは C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-7.0.75\conf にあります。

注意

Tomcat のバージョン番号は、使用中の Acronis Cyber Files のバージョンによって異なる場合があります。

- `acronisaccess.cfg` ファイル。これは、C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server にあります。

server.xml ファイルの編集

このファイル内で、適切な HTTP コネクタを設定し、HTTPS コネクタを無効にする必要があります。

1. ファイルをテキストエディタで開き、既存の HTTPS コネクタを見つけます。以下のような内容になっているはずです。

```
<Connector maxHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1.2"
```

```
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW
:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" port="443" address="0.0.0.0"/>
```

2. HTTPS コネクタを無効にするために、<!-- と --> で囲みます。つまり、<Connector maxHttp. の前に <!-- を追加し、--> を address="0.0.0.0"/> の後ろに追加します。
3. 以下のような新しい HTTP コネクタを作成します。

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="http" secure="true"
connectionTimeout="-1" URIEncoding="UTF-8" port="80" address="0.0.0.0"/>
```

4. デフォルト以外のポートを選択することもできます。また、使用可能なすべてのアドレスがサービスに使用されないよう、接続用のアドレスを特定のアドレスに制限することもできます。
5. 使用するポートがファイアウォールで開かれていることを確認してください。
6. server.xml ファイルに、以下のリダイレクトコネクタが含まれているかどうかを確認します。

```
<!-- <Connector port="80" connectionTimeout="20000" protocol="HTTP/1.1"
redirectPort="443"/> -->
```

7. リダイレクトコネクタが含まれている場合、ポート 80 を使用するには、上述のように <!-- と --> を使用してコメント化することによって、リダイレクトコネクタを無効にします。
8. 必要な変更を行った後、ファイルを保存します。

acronisaccess.cfg の編集

このファイルで更新しなければならないのは、ファイルの末尾にある REQUIRE_SSL だけです。この設定を **true** から **false** に変更します。変更後は以下のようになります。

```
REQUIRE_SSL = false
```

1. 必要な変更を行った後、ファイルを保存します。
2. Acronis Cyber Files の Tomcat サービスを再起動して、すべての変更を適用します。

HTTP モードの制限事項

- ゲートウェイは **HTTPS** で動作する必要があるため、**HTTP** モードではゲートウェイサーバーとの通信がサポートされません。ウェブ UI またはモバイルクライアントを介してネットワークノードにアクセスすることはできません。
- シングルサインオンはサポートされません。
- デスクトップクライアントを使用している場合、サーバーアドレスフィールドに手動で **HTTP** を指定する必要があります。このようにしなければ、接続が失敗します。例: `http://myaccess.com:3000`

安全でない TLS バージョンを使用した Acronis Cyber Files Tomcat の実行

注意

このリリースで導入された変更により、古いバージョンの TLS を使用する配置が中断される場合があります。以下の回避策を確認してください。ただし、Acronis ではそのような構成をサポートしなくなりました。

Acronis Cyber Files 8.8.0 以降、すべての新規インストールおよびアップグレードでは TLSv1.2 のみを使用するように設定されます。

これらの手順はサポートされず、これらの安全でない TLS バージョンを使用する必要があるユーザーに対して TLSv1 および TLSv1.1 を有効にするために現状のまま提供されています。

Tomcat 9 のアップグレード時の TLS 構成の管理

注意

コネクタ構成の操作または更新方法は、「[HTTP モードでの Acronis Cyber Files の実行](#)」および「[複数のポートでの Acronis Cyber Files Tomcat の実行](#)」で説明されている方法と同様です。

注意

TLSv1 および TLSv1.1 を有効にする前に、それが実際に必要であるかどうかを確認してください。ほとんどの Web ブラウザでは TLSv1 と TLSv1.1 が既に廃止されており、デフォルトで TLSv1.2 が使用されます。Acronis Cyber Files と統合されている他の一部のサービスは、TLSv1.2 で動作するように更新することだけが必要です。たとえば、Office Online ではパッチ [KB5001973](#) が必要です。

1. Acronis Cyber Files Tomcat サービスを停止します。
2. server.xml ファイルに移動します。デフォルトのロケーションは、
C:\Program Files (x86)\Acronis\Cyber Files\Common\apache-tomcat-9.0.88\conf です。

注意

Acronis Cyber Files の新しいバージョンにアップグレードしている場合や、カスタム インストールを実行した場合には、パスが異なる可能性があります。Windows サービスの Acronis Cyber Files Tomcat エントリを使用して Apache Tomcat フォルダへのパスを確認することができます。これには conf フォルダが含まれます。

3. サポートされているバージョンに戻る場合に備えて、編集されていない元の server.xml ファイルを、別の名前を付けてコピーします。
4. 同じファイルの Connector セクションで、次のコンテンツを見つけます:

```
<Connector maxHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1.2"
SSLCertificateFile="{catalina.base}/conf/AACert.cer"
```

```
SSLCertificateKeyFile="${catalina.base}/conf/AACert.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL
:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" relaxedQueryChars="[,]" port="443" address="0.0.0.0"/>
```

5. 次のようにテキストを変更します。

変更前

```
SSLProtocol="TLSv1.2"
```

変更後

```
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
```

6. 最後に、ファイルを保存します。
7. Acronis Cyber Files Tomcat サービスを起動します。

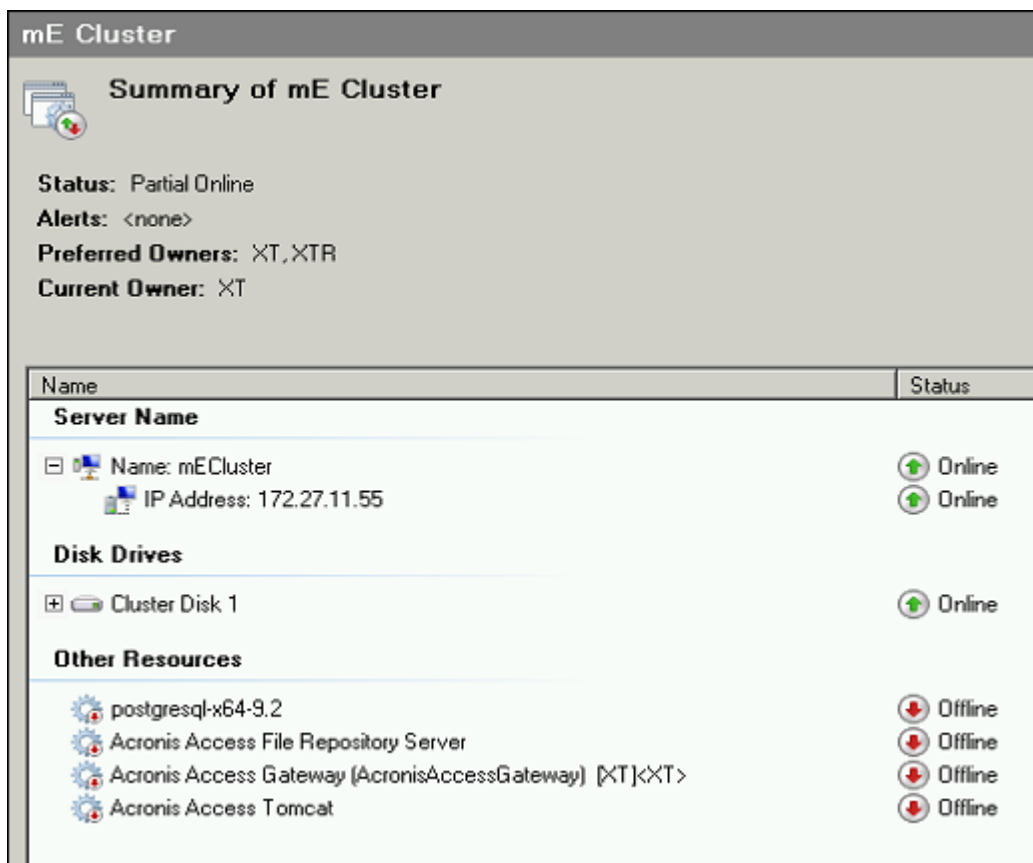
Microsoft フェールオーバークラスター上での Acronis Cyber Files のアップグレード

Acronis Cyber Files Server クラスターを Acronis Cyber Files 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。

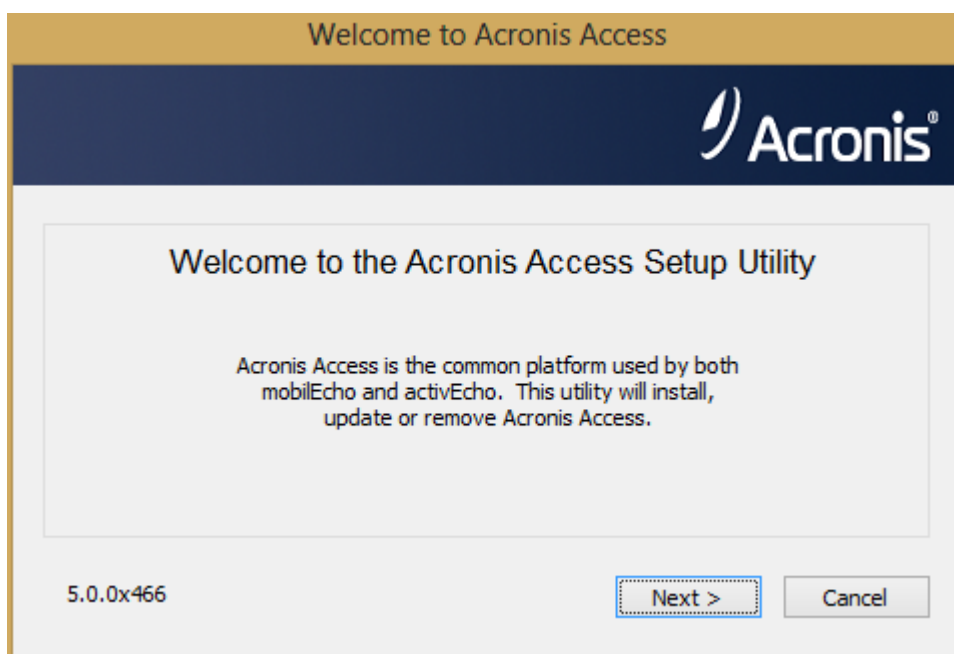
注意

アップグレードを実行する前に、「[バックアップ](#)」の記事を確認してから構成をバックアップしてください。

1. アクティブ ノードに移動します。
2. **[Cluster Administrator]/[フェールオーバー クラスタ管理]** を開きます。
3. Acronis Cyber Files のサービスをすべて (**postgres-some-version** も含む) 停止します。共有ディスクがオンラインでなければなりません。

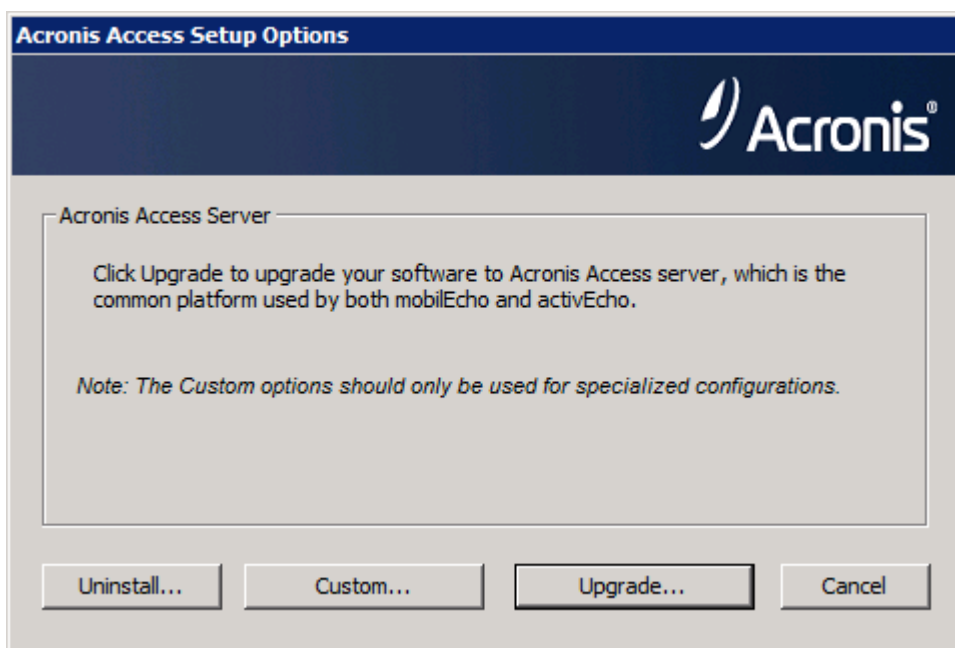


4. インストールされているウイルス対策ソフトウェアをすべて無効にしてください。無効にしない場合は、インストール手順が中断され、インストールが失敗する可能性があります。
5. 実行可能なインストーラをダブルクリックします。

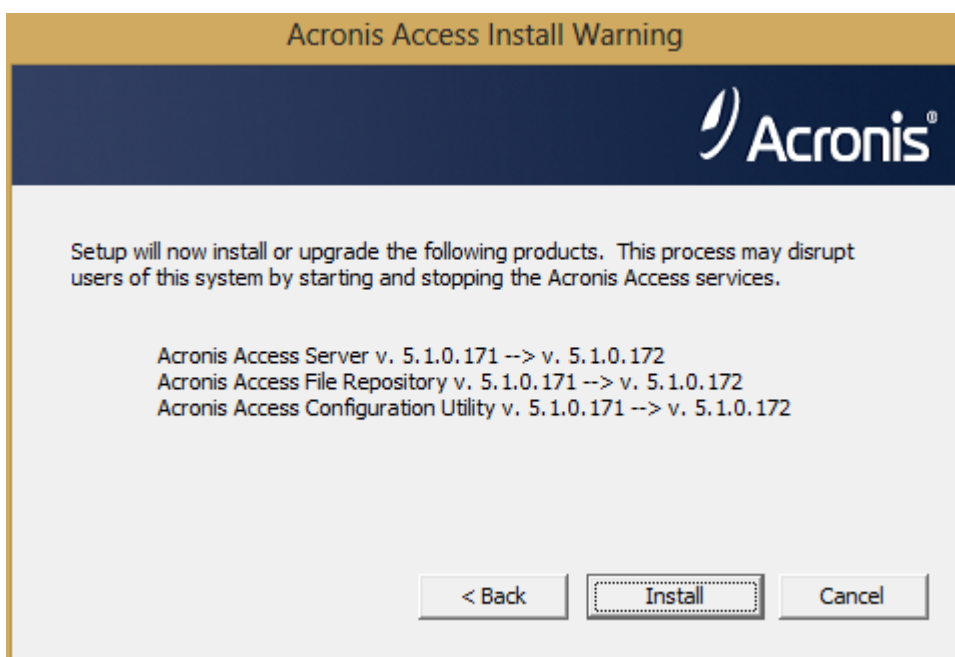


6. [次へ] をクリックして開始します。
7. ライセンス契約を読み、承諾します。

8. [アップグレード] をクリックします。



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

クラスター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 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 Cyber Files のサービスをすべてオンラインにします。

Microsoft フェールオーバークラスター上での Acronis Cyber Files のインストール

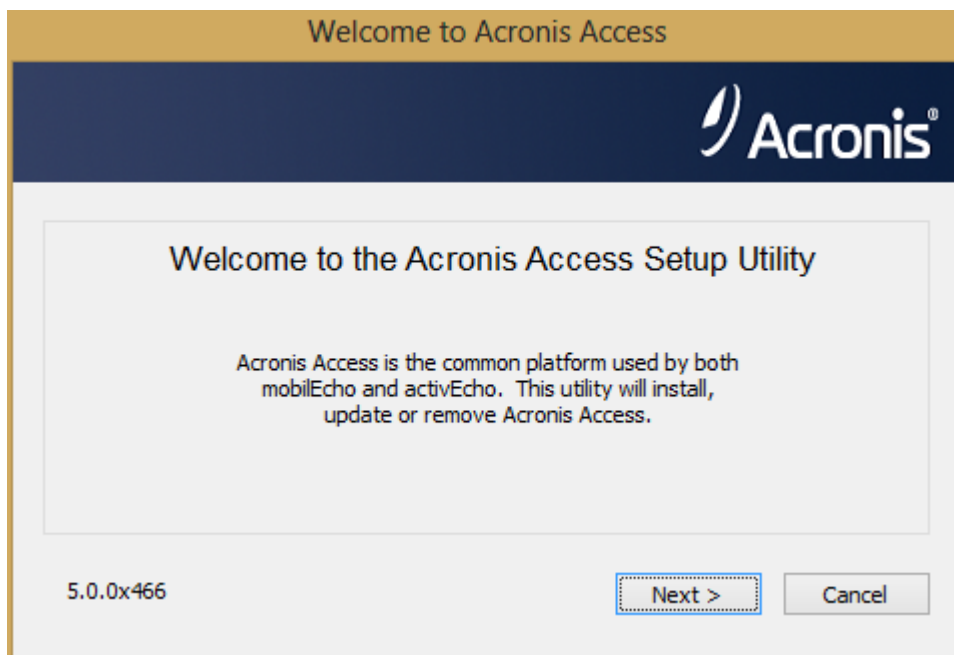
Acronis Cyber Files をクラスター上にインストールするには、以下のガイドが役立ちます。

Windows 2012 (R2) Microsoft フェールオーバークラスター上での Acronis Cyber Files のインストール

AcronisCyber Files のインストール

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

1. AcronisCyber Files 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。

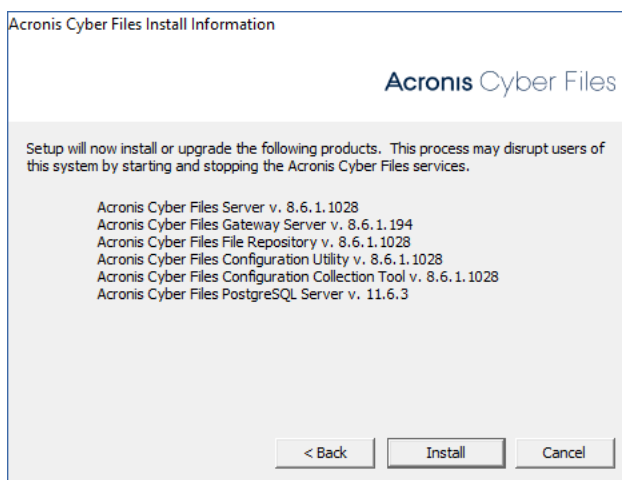


4. **[次へ]** をクリックして開始します。
ライセンス契約を読み、承諾します。
5. **[インストール]** をクリックします。

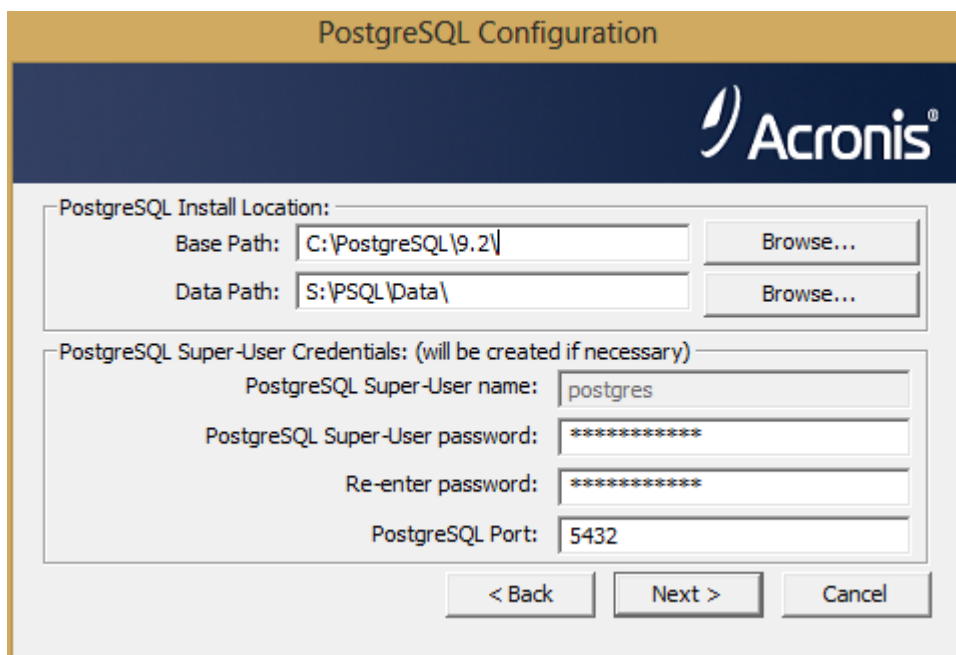
注意

複数の Acronis Cyber Files 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。

6. Acronis Cyber Files 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て、[OK] をクリックします。



7. ユーザー Postgres 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復旧に必要となります。
8. 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。

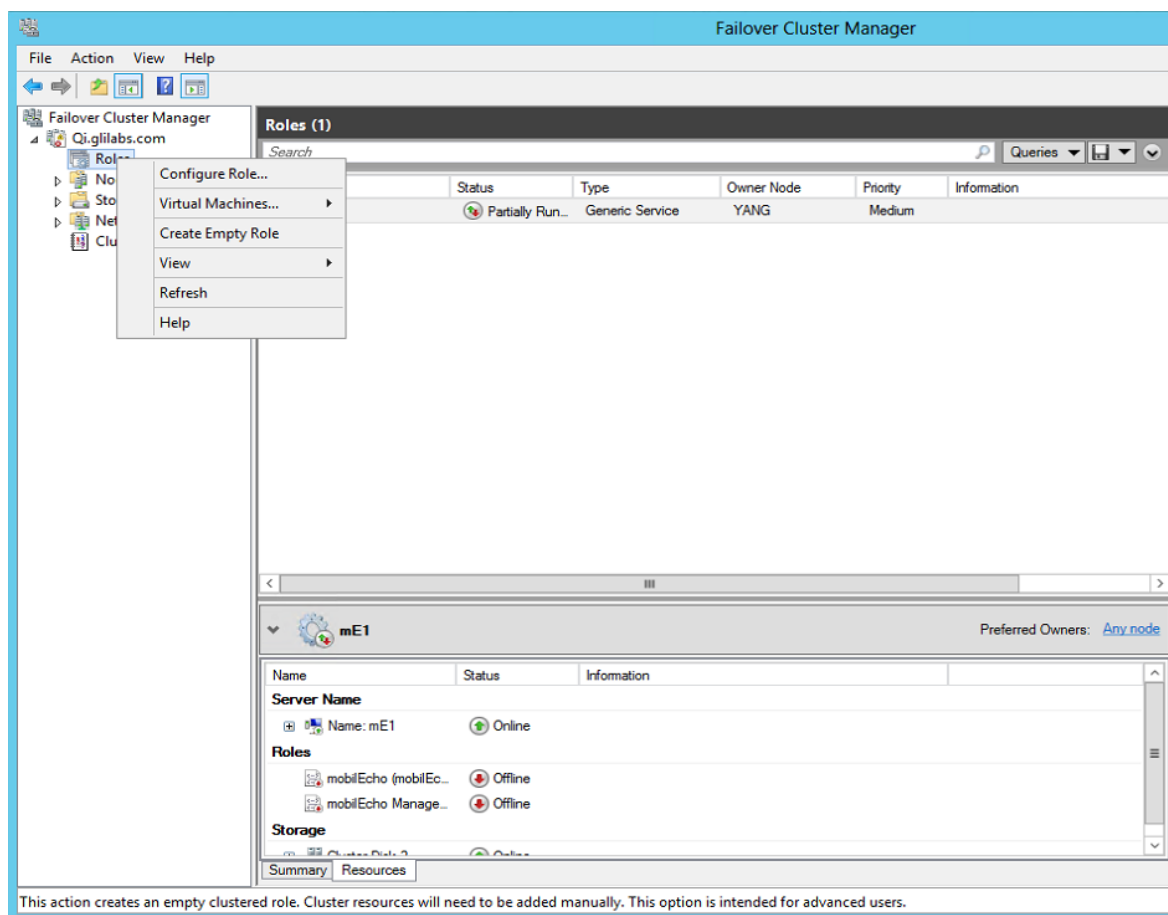


9. インストールされるコンポーネントがすべてリストされたウィンドウが表示されます。続行するには、[OK] をクリックしてください。
10. Acronis Cyber Files のインストーラが完了したら、[終了] をクリックします。

役割の作成

1. [フェールオーバー クラスター マネージャ] を開き、[役割] を右クリックします。
2. [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 Cyber Files、AAS クラス

ターなど）。



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\Acronis Cyber Files\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 (database_path: 'S:/access_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

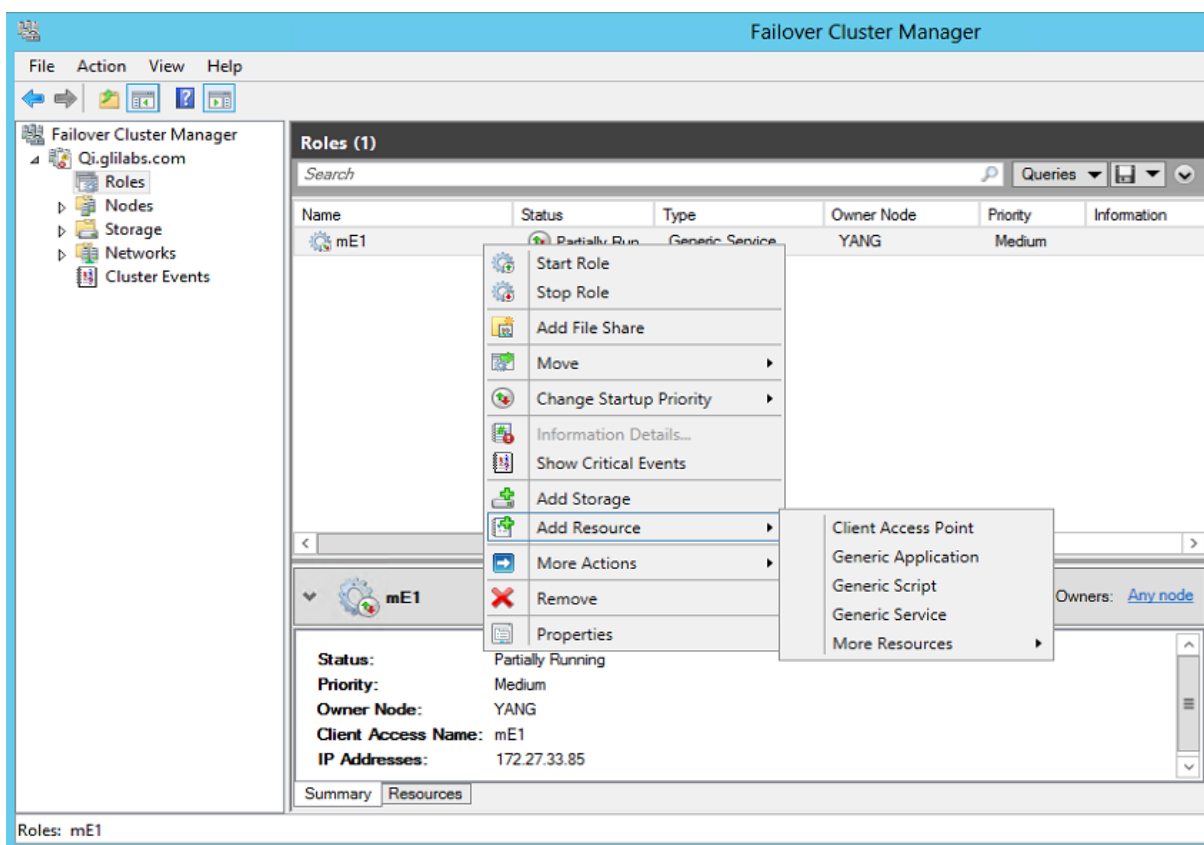
第 1 ノードで設定した database.yml をコピーして、第 2 ノードに貼り付けることができます。

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

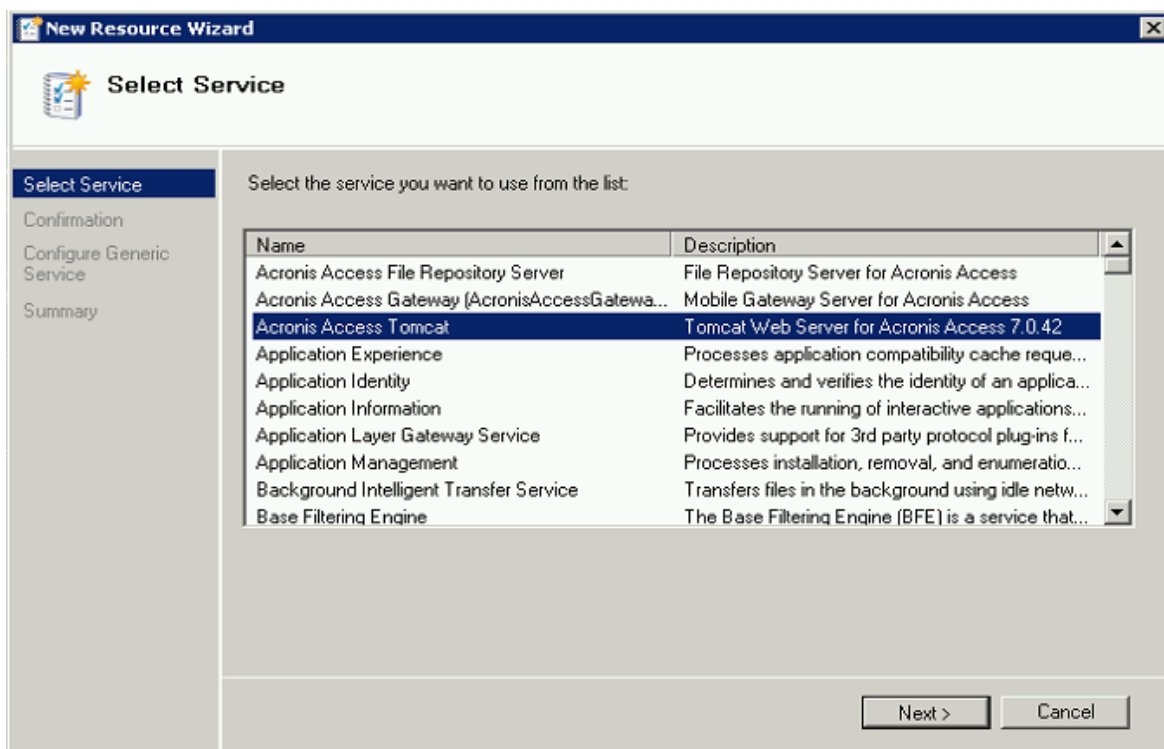
Acronis Cyber Files Gateway、Acronis Cyber Files PostgreSQL (Acronis Cyber Files のバージョンに応じて異なる) Acronis Cyber Files Repository および Acronis Cyber Files Tomcat の各サービスについて、以下の手順を実行します。

1. Acronis Cyber Files の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。



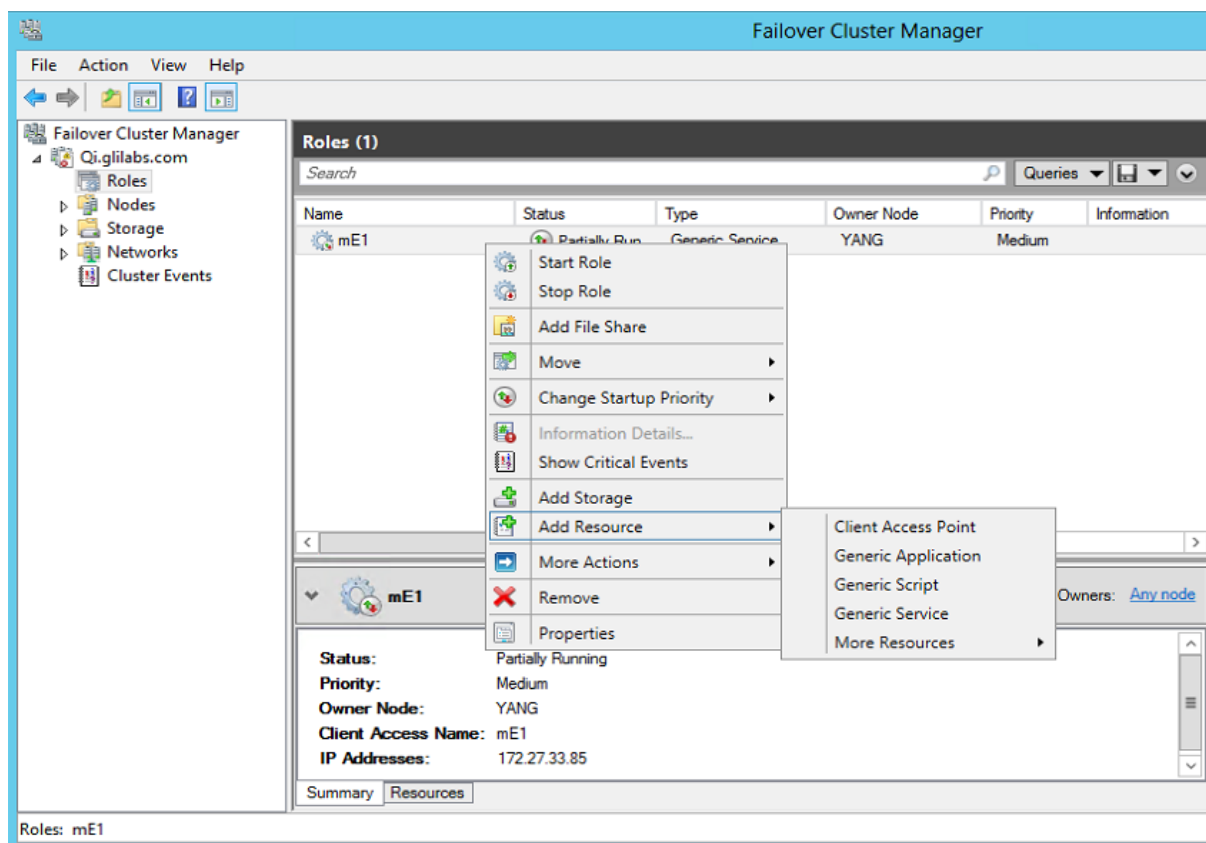
3. 適切なサービスを選択して [次へ] をクリックします。



4. 確認ウィンドウで **[次へ]** をクリックします。
5. サマリウィンドウで **[完了]** をクリックします。

アクセス ポイントの設定

1. Acronis Cyber Files の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。

New Resource Wizard

Client Access Point

Client Access Point
Confirmation
Configure Client Access Point
Summary

Enter Network Name and IP Address:

Name:

One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

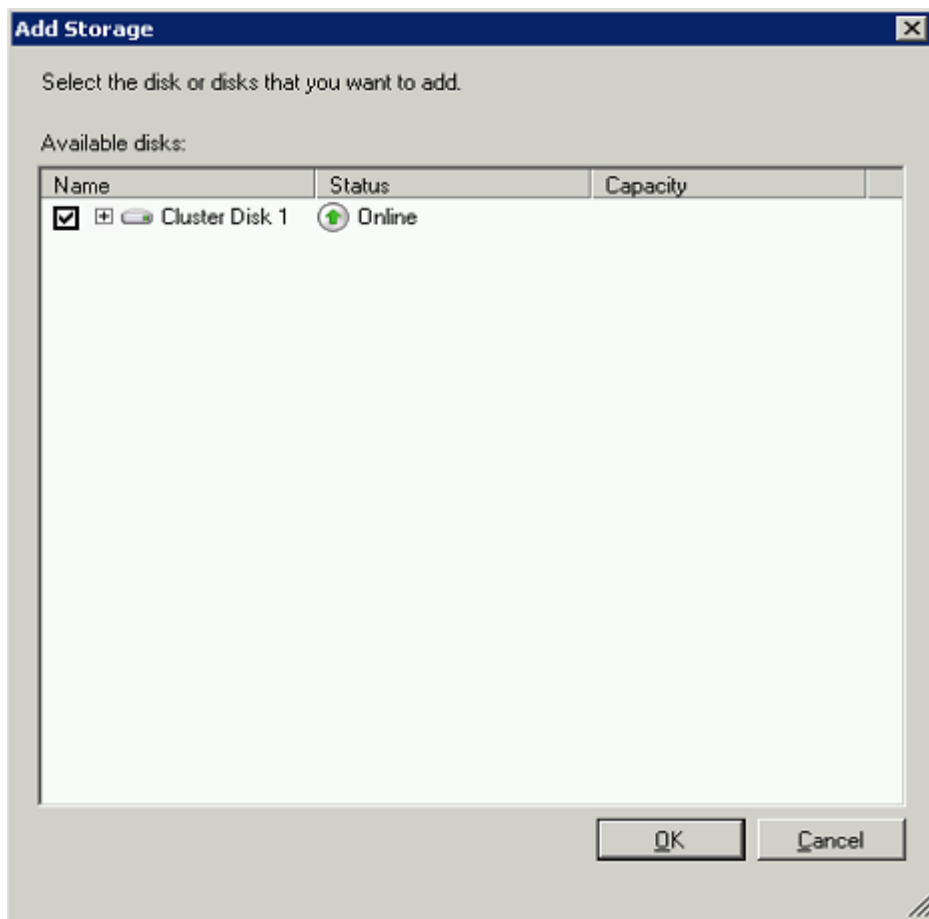
	Networks	Address
☒	172.27.0.0/16	172.27.25.25

Next > Cancel

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. サマリウィンドウで **[完了]** をクリックします。

共有ディスクの追加

1. Acronis Cyber Files 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. 目的の共有ドライブを選択します。



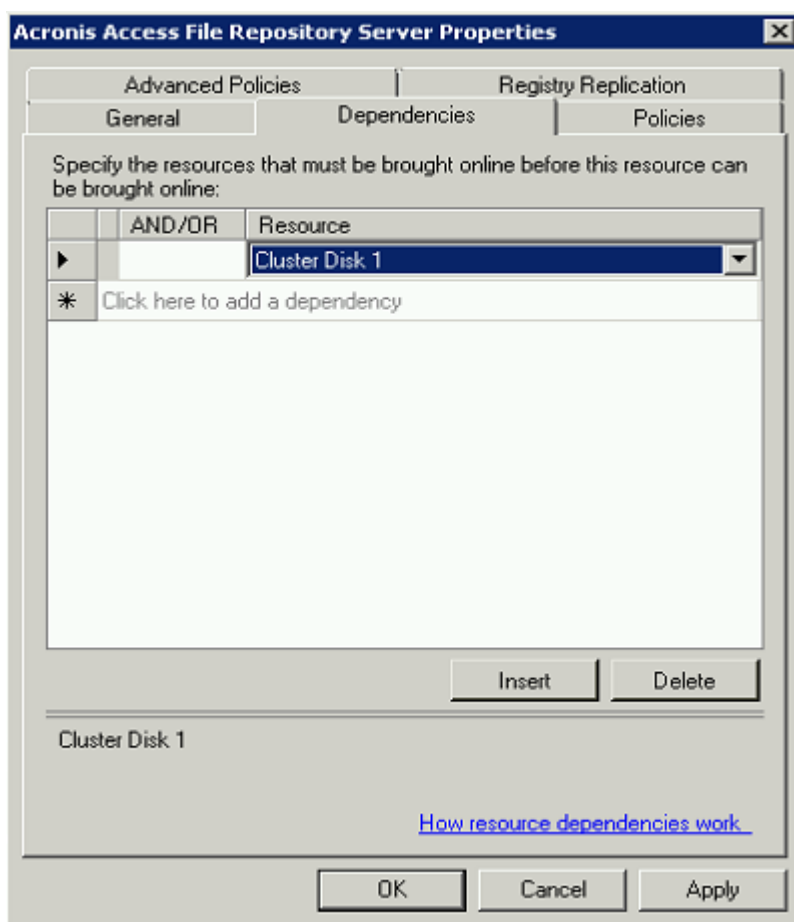
依存関係の設定

1. Acronis Cyber Files 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 Cyber Files 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。

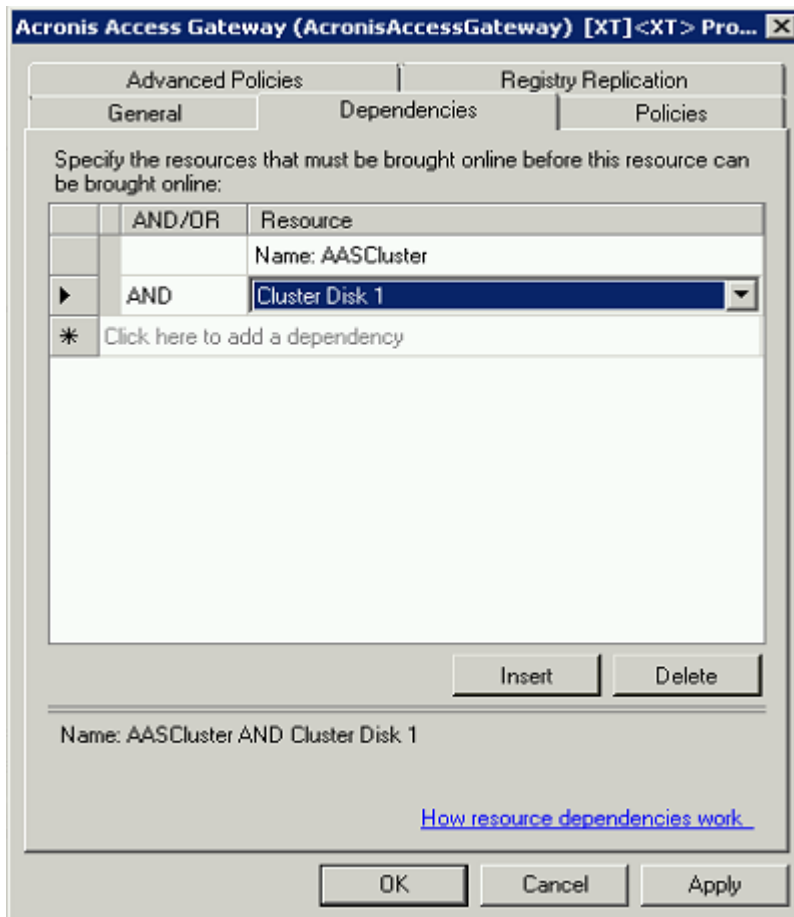
3. **[リソース]** をクリックし、追加した共有ディスクを選択します。



4. **[適用]** をクリックしてウィンドウを閉じます。

Acronis Cyber Files 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。



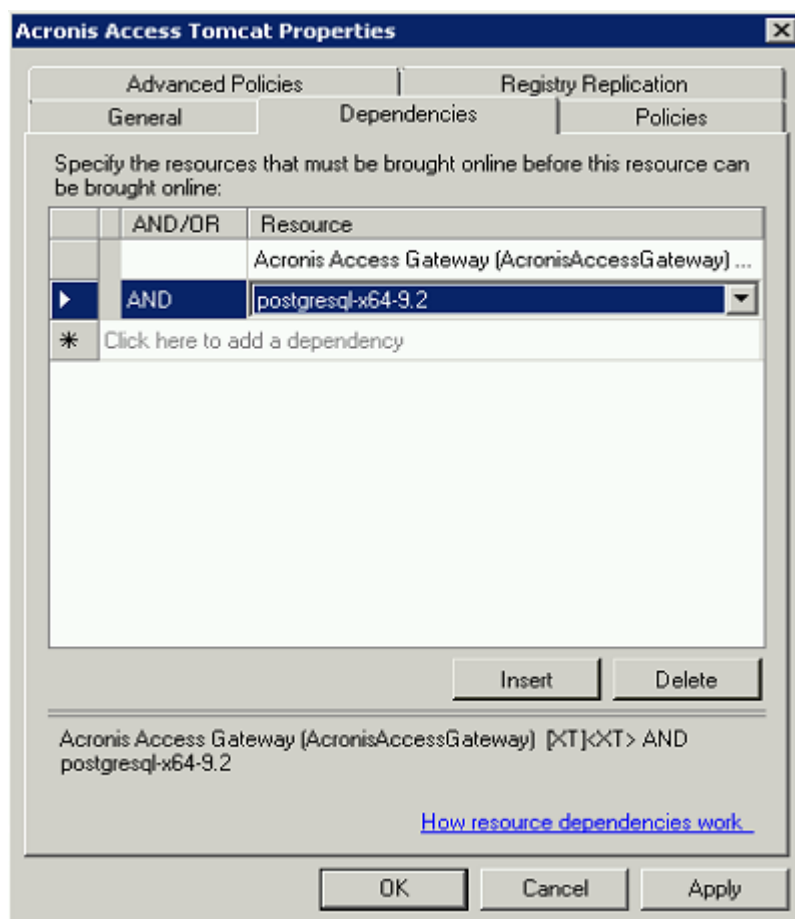
4. [適用] をクリックしてウィンドウを閉じます。

Acronis Cyber Files 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 Cyber Files 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。

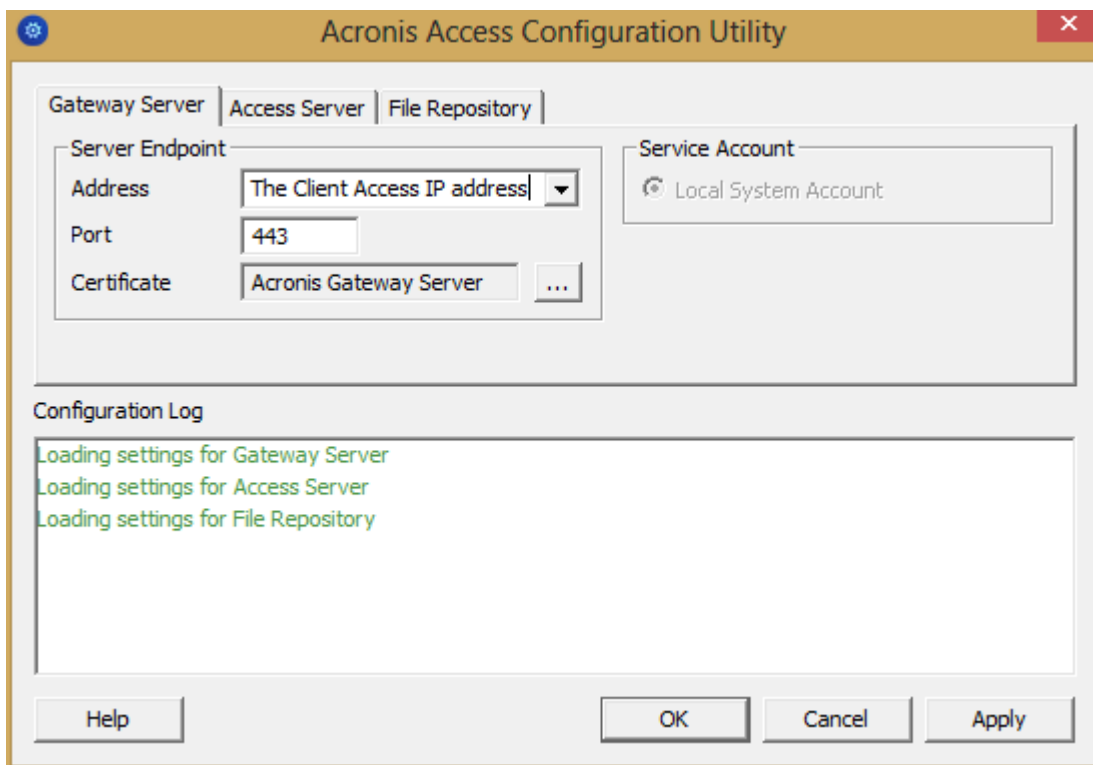
注意

ゲートウェイサーバーと Acronis Cyber Files ウェブサーバーを異なる 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 Cyber Files 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

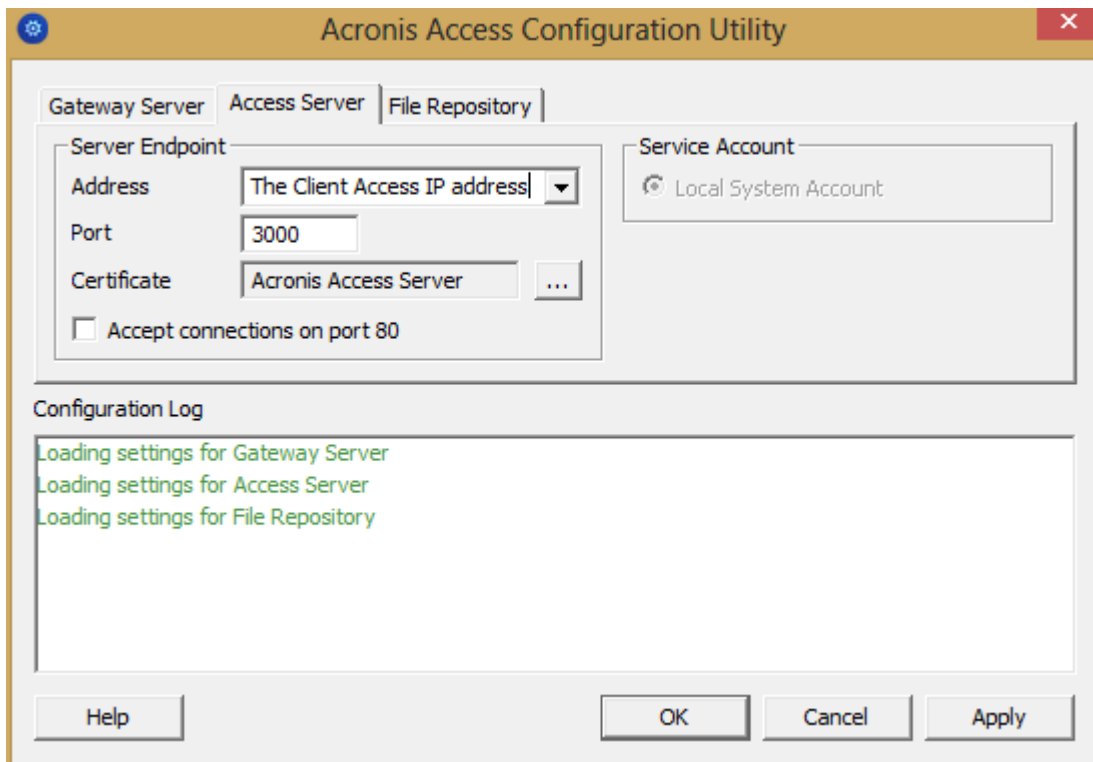
1. AcronisCyber Files の役割を右クリックして、**[役割の開始]** を押します。
2. 設定ユーティリティを起動します。クリーンインストールの場合、通常このユーティリティは C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility にあります。
3. Acronis Cyber Files ゲートウェイサーバーサービスが、IP アドレス上で Acronis Cyber Files サービスグループをリスンするように設定します。



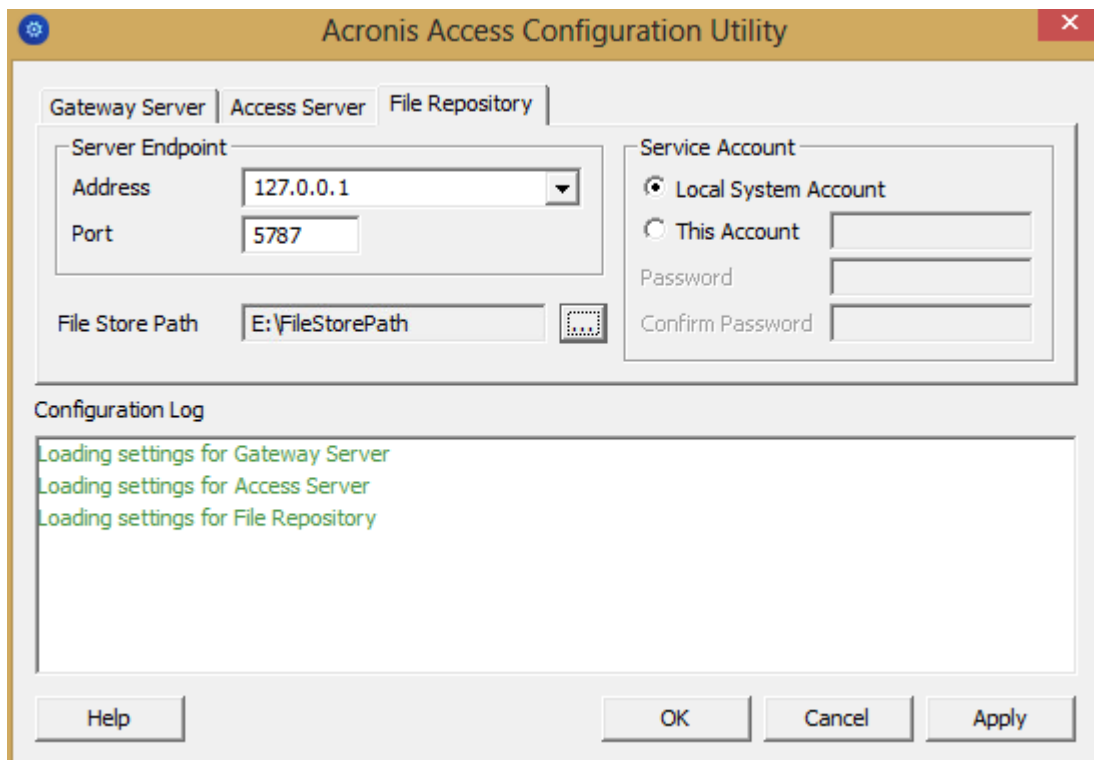
4. Acronis Cyber Files サーバーサービスが、IP アドレス上で Acronis Cyber Files サービスグループをリスンするように設定します。

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、



5. Acronis Cyber Files 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 Cyber Files 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\Acronis Cyber Files\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 (database_path: 'S:/access_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

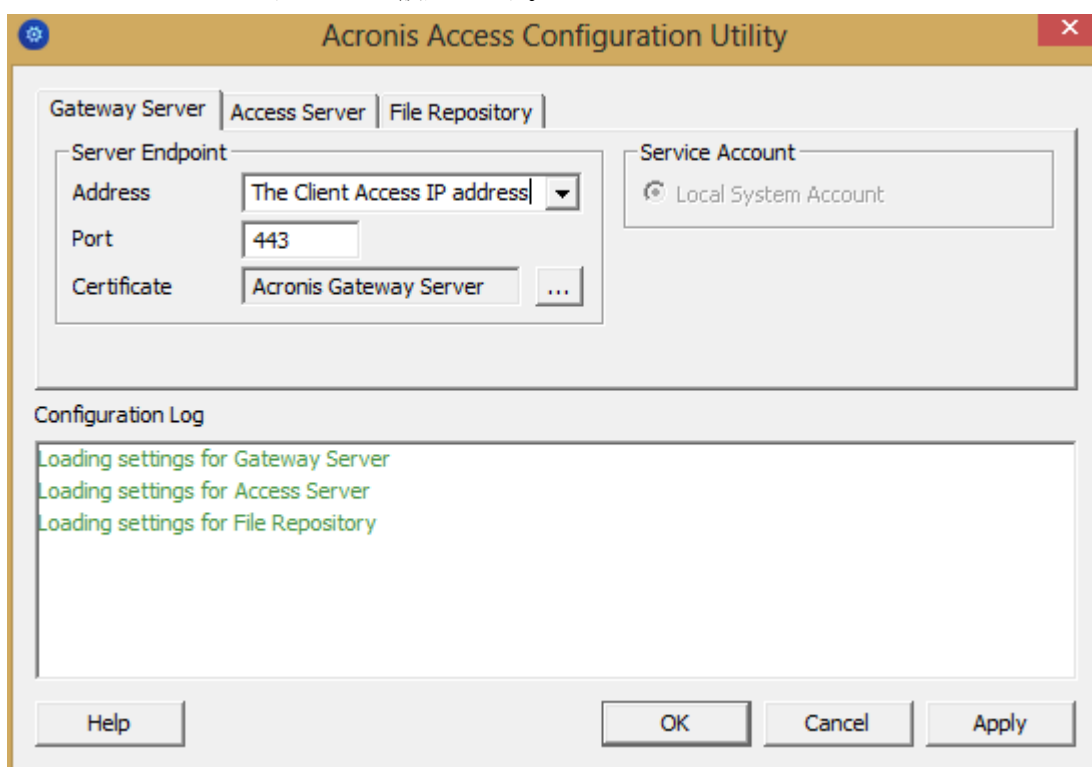
第1ノードで設定した database.yml をコピーして、第2ノードに貼り付けることができます。このパスは第1ノードで設定されているパスと同じでなければなりません。

PostgreSQL では、次の操作を実行します。

1. [ファイルオーバークラス管理] を開きます。
2. PostgreSQL 汎用サービスリソースを探して選択します。
3. アカウントを右クリックし、[プロパティ] を選択します。
4. [レジストリ レプリケーション] タブをクリックします。
5. [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 Cyber Files 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）。
6. Acronis Cyber Files 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

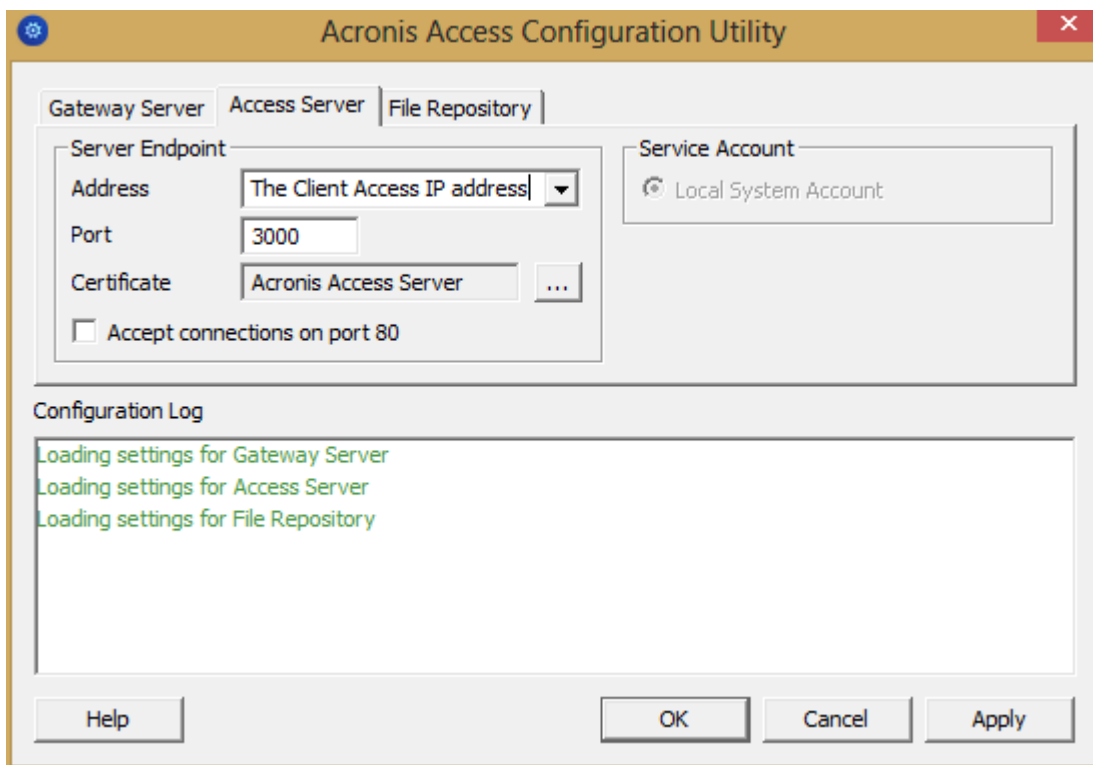
1. Acronis Cyber Files の役割を右クリックして、[役割の開始] を押します。
2. 設定ユーティリティを起動します。クリーンインストールの場合、通常このユーティリティは C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\Configuration Utility にあります。
3. Acronis Cyber Files ゲートウェイサーバーサービスが、IP アドレス上で Acronis Cyber Files サービスグループをリスンするように設定します。



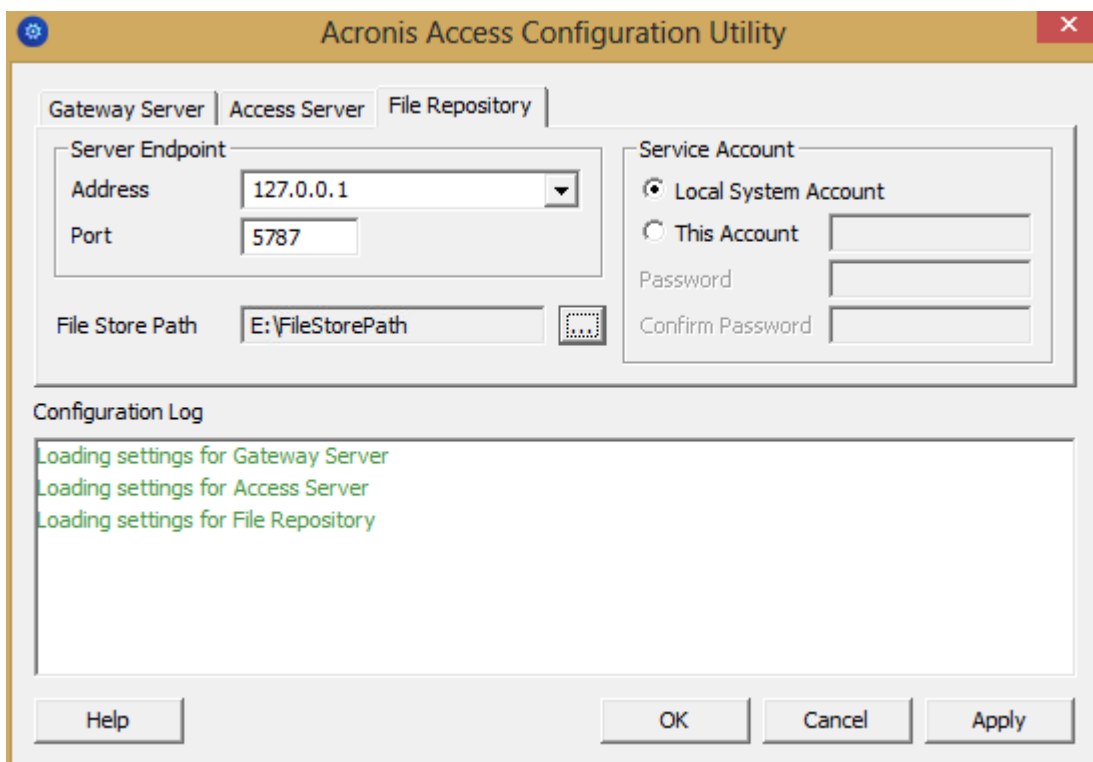
4. Acronis Cyber Files サーバーサービスが、IP アドレス上で Acronis Cyber Files サービスグループをリスンするように設定します。

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、



5. Acronis Cyber Files 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。

IPv6 のセットアップ

開始する前に – 既知の制限

現在、構成ユーティリティでは IPv6 は自動的にサポートされていません。server.xml ファイルと SSL バインディングに手動で変更を加えると、UI でサポートされていないすべての変更が削除されるため、構成ユーティリティを使用できなくなります。構成ユーティリティによって IPv6 がサポートされるまでは、すべてのサービスの再起動とサーバー構成の編集は手動で行う必要があります。

server.xml および web.xml ファイルに必要な手動の変更は、アップグレード時に保持されません。これらのファイルは、必ず Acronis Cyber Files サーバーのインストール以外の場所にバックアップしてください。アップグレード後、手動で編集したファイルを新しくインストールしたファイルと比較し、必要な変更を移植する必要があります。

IPv6 に解決されるすべてのアドレスは、webUI で DNS アドレスとして指定する必要があります。

注意

管理者ページ – 「管理ページアクセス制限」機能には、管理ページへのアクセスを許可する IP の範囲が必要です。現在の UI 形式では IPv4 のみがサポートされています。

IPv6 セットアップの実行

IPv6 サポートを有効にするには 3 つの手順が必要です。

IPv6 のセットアップ手順 1: ゲートウェイのセットアップ

ゲートウェイを IPv6 で動作させるには、SSL バインディングを作成してから、目的のアドレスを iplisten リストに追加する必要があります。

注意

この手順を完了するには、Acronis Access 証明書の拇印の thecerthash 値、特定の IPv6 IP アドレス、ゲートウェイがリッスンするポートが必要です。certhash 値を取得する方法については、[Acronis Access 証明書の拇印の取得](#)を参照してください。

SSL バインディングの作成

すべての IPv6 アドレスまたは特定の IPv6 アドレスに対してバインドできます。

すべての IPv6 アドレスへのバインディング

コマンドは、以下になるはずです。

```
netsh http add sslcert ipport=[:]:YourPortNumber certhash=Certhash値 appid={72876ec6-d443-48ef-add3-fa7a0cbc4762} certstorename=MY clientcertnegotiation=enable dsmapperusage=enable
```

重要

ゲートウェイがリッスンするポートを入力し、certhash 値を [自分の証明書](#) からの値に置き換える必要があります

注意

特定の IPv6 アドレスにバインドするには、 ":::" を希望するアドレスに置き換えます。

注意

SSL バインディングを削除する必要がある場合は、次のコマンドを使用し、アドレスとポートを削除するものに置き換えます。

```
netsh http delete sslcert ipport=[AddressToRemove]:PortToRemove
```

特定の IPv6 アドレスの `iplisten` リストへの追加

すべての IP アドレスまたは特定の IP アドレスを `iplisten` リストに追加できます。

すべての IPv6 IP アドレスの `iplisten` リストへの追加

1. 次のコマンドを使用します。 `netsh http add iplisten ipaddress=::`

注意

特定の IPv6 IP アドレスを `iplisten` リストに追加するには、 ":::" を希望する IPv6 IP アドレスに置き換えます。

E.g.: `netsh http add iplisten ipaddress=fd59:ffdf:9580::3`

2. Windows サービスからゲートウェイサービスを再開します。

注意

これで、ローカルホスト (:: 1) と任意の IP アドレスの両方を経由してゲートウェイにアクセスできるようになります。

特定の IPv6 IP アドレスを設定すると、ローカルホスト経由でゲートウェイにアクセスできなくなり、指定したアドレスでのみアクセスできます。

警告

ローカルホスト経由でゲートウェイにアクセスできるようにする場合は、特定の IP アドレスを設定した後、次のコマンドを使用して `iplisten` リストから特定のアドレスを削除し、Windows サービスからゲートウェイサービスを再開する必要があります。

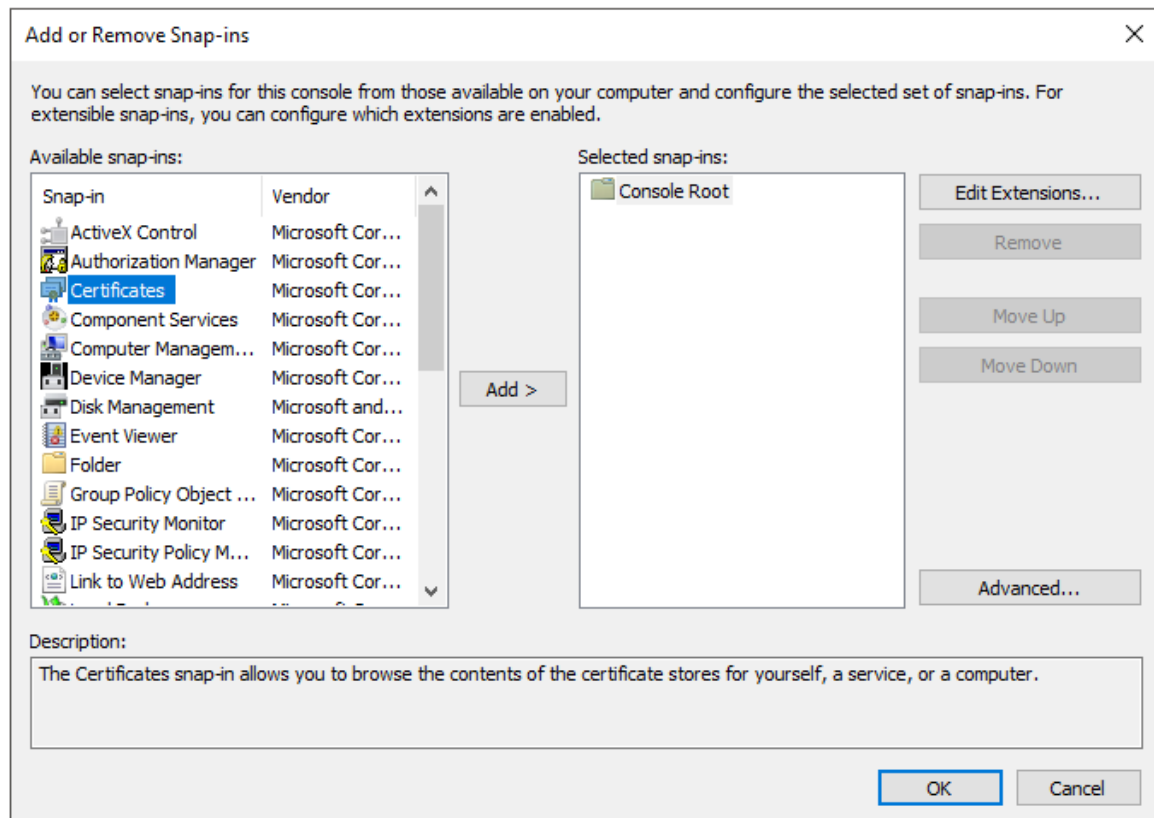
例: `netsh http delete iplisten ipaddress=fd59:ffdf:9580::3`

Acronis Access 証明書の拇印の取得

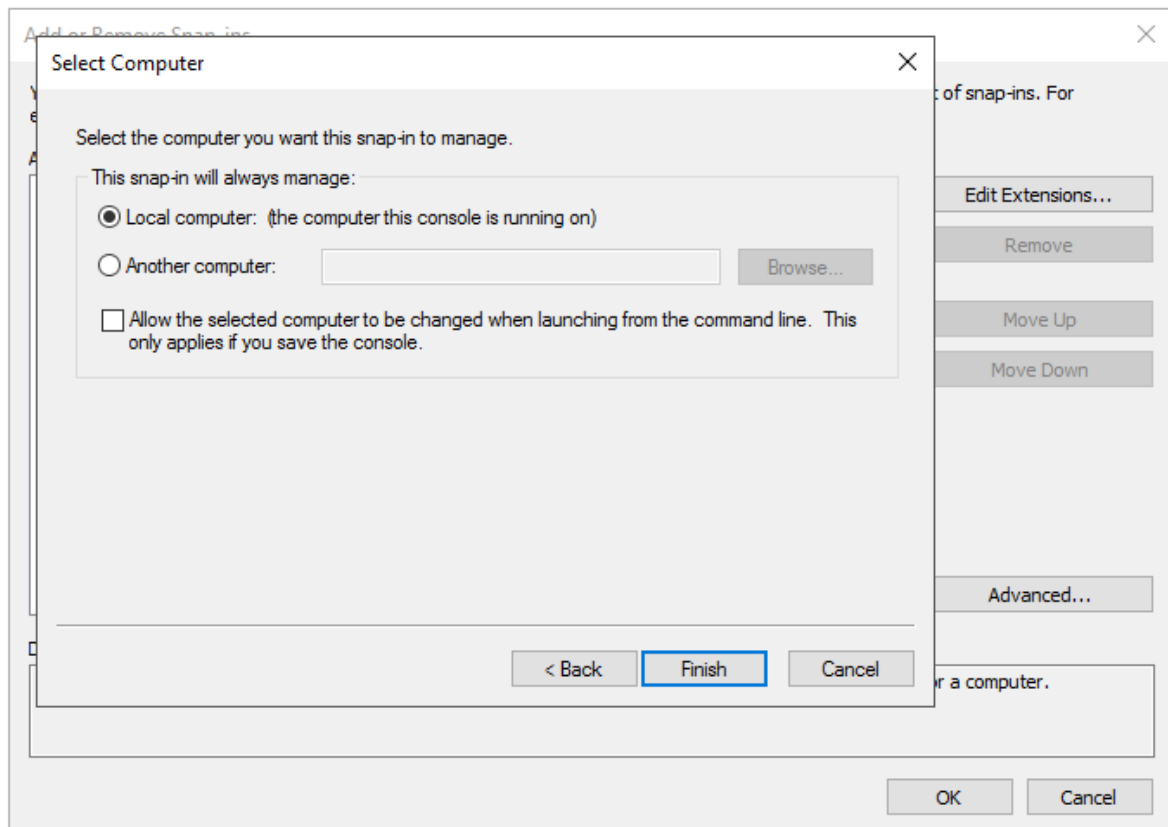
Acronis Access 証明書の拇印を取得する方法は 2 つあります。1 つは、[証明書スナップイン] の [証明書の詳細] タブから、もう 1 つは、コマンドプロンプトを使用して、すでに設定されている SSL バインディングから入手するという方法です。

証明書スナップインから証明書の拇印を取得するには

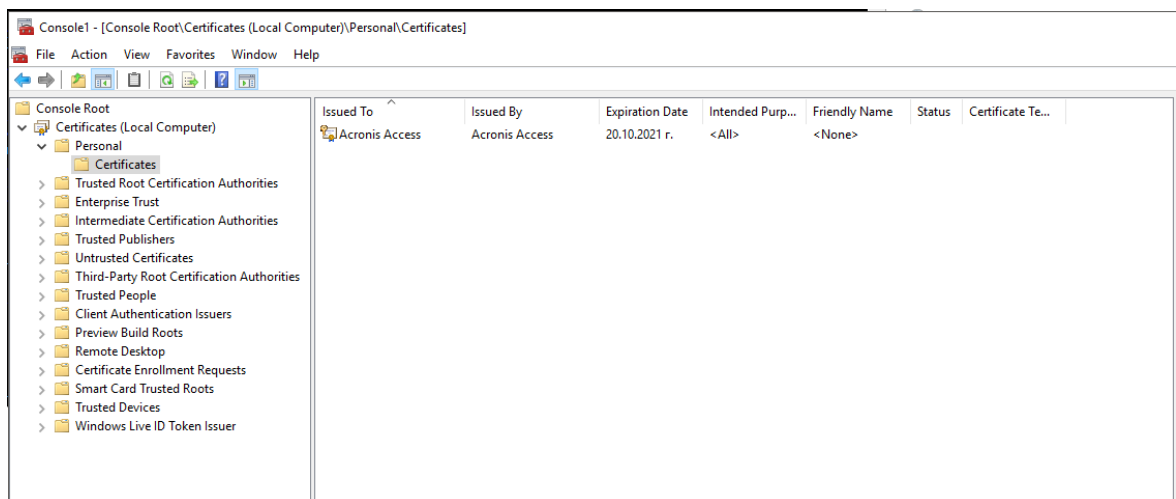
1. [ファイル名を指定して実行] ダイアログを開き、「mmc.exe」と入力して **Microsoft 管理コンソール** を開きます。
2. [ファイル] -> [スナップインの追加と削除...] をクリックします
3. [証明書] を選択します。



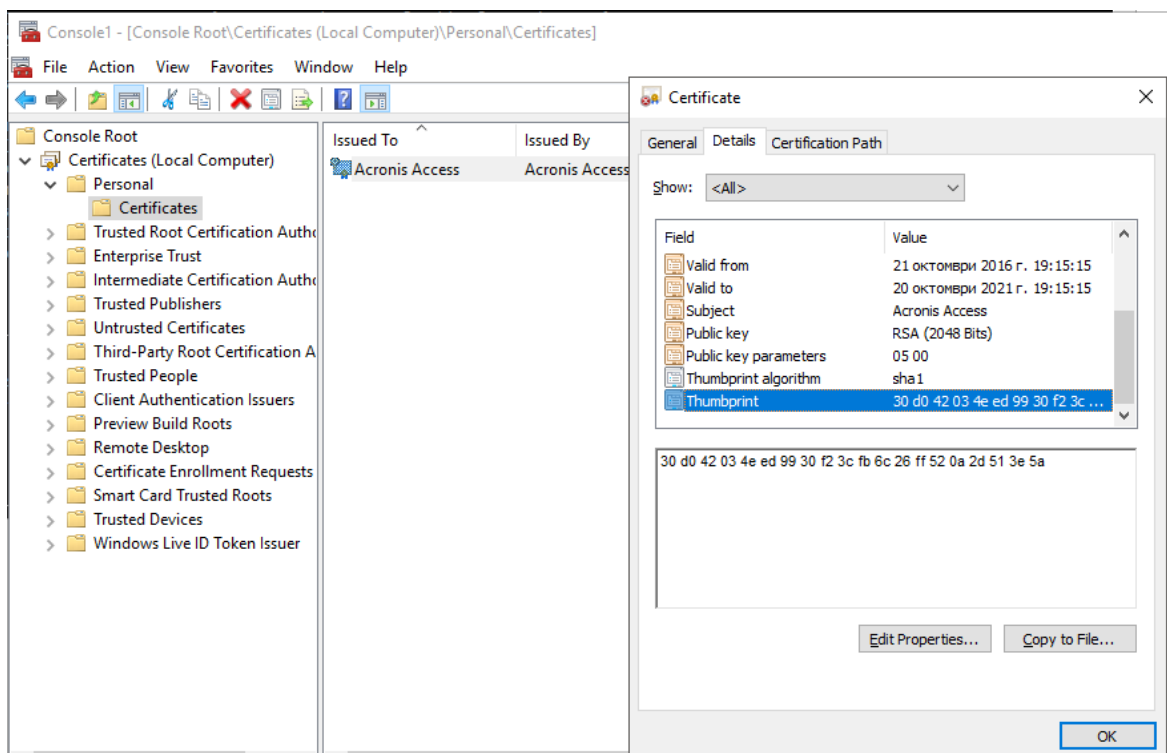
4. ダイアログで [追加] をクリックします。



5. [コンピューターアカウント] を選択し、[次へ] を押し、[ローカルコンピュータ] を選択して [完了] を押します。
6. [スナップインの追加と削除...] ダイアログで [OK] をクリックします。



7. 左側にある [証明書]、[個人用]、[証明書] の順に展開すると、Acronis Access 証明書が表示されます。



8. 証明書をダブルクリックして、[詳細] タブを選択し、拇印までスクロールします。
9. それを別の場所にコピーし、スペースを削除します。SSL バインディングを作成するコマンドでは、スペースなしにする必要があります。

既にセットアップされた SSL バインディングを使用して証明書の拇印を取得するには

1. コマンドプロンプトを開きます。
2. 次のように入力します。netsh http show sslcert
3. SSL バインディングが存在する場合は、それが表示されます。

```

Select Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netsh http show sslcert

SSL Certificate bindings:
-----
IP:port                : 192.168.2.34:4430
Certificate Hash       : 30d042034eed9930f23cfb6c26ff520a2d513e5a
Application ID        : {72876ec6-d443-48ef-add3-fa7a0cbc4762}
Certificate Store Name : (null)
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : (null)
Ctl Store Name       : (null)
DS Mapper Usage       : Enabled
Negotiate Client Certificate : Enabled
Reject Connections    : Disabled

C:\Users\Administrator>

```

注意

強調表示された文字列は、必要な証明書ハッシュです。

IPv6 のセットアップ手順 2: Acronis Cyber Files Server

サーバーがすべての IPv6 アドレスでローカルにリッスンできるようにします。

重要

特定の IPv6 アドレスにバインドするには、手順 4 の注を参照してください。

1. **server.xml** ファイルを見つけます。

注意

デフォルトでは、このファイルは **C:\Program Files (x86)\Acronis\Acronis Cyber Files\Common\apache-tomcat-9.0.88\conf** にあります。

パス内の番号 (7.0.70) は、Tomcat のバージョンによって異なる場合があります、アップグレードまたはカスタムインストールを実行した場合は、パスが異なる場合があります。。この場合、**Acronis Cyber Files Tomcat** エントリを **Windows サービス** で使用して、Tomcat プログラムフォルダのパスを特定できます。これには、**conf** フォルダが含まれます。

2. **server.xml** のバックアップコピーを作成します。
3. テキストエディターで、元の **server.xml** を開きます。
4. すべての IPv6 アドレスをサポートするには、`address="::"` を使用してコネクターをさらに追加します。
 - i. **server.xml** で、次のようなファイルの一部を見つけます

```
<Connector maxHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!
LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8"
bindOnInit="false" relaxedQueryChars="[,]" address="0.0.0.0" port="443"/>
```

- ii. 次に、新しい行の既存のコネクターの横に、この追加のコネクターを `address="::"` で追加します。

```
<Connector maxHeaderSize="65536" maxThreads="150" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key"
SSLHonorCipherOrder="true"
```

```
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" relaxedQueryChars="[,]" address="::" port="443"/>
```

注意

すべての IPv6 アドレスを追加する (::) 代わりに、コネクタブロックで "::" を希望するアドレスに置き換えることで特定の IPv6 アドレスを設定できます。

例:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="${catalina.base}/conf/AAServer_LocalHost.crt" SSLCertificateKeyFile="${catalina.base}/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true" SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS" connectionTimeout="-1" URIEncoding="UTF-8" bindOnInit="false" relaxedQueryChars="[,]" address="fd59:ffdf:9580::3" port="443"/>
```

5. 変更内容を保存し、Windows の [サービス] パネルから Acronis Cyber Files Tomcat サービスを再起動します。

重要

server.xml に対するすべての変更では、Acronis Cyber Files Tomcat サービスを再起動する必要があります。

警告

これらの手動による変更は、アップグレード時に保持されません。これらのファイルは、必ず Acronis Cyber Files サーバーのインストール以外の場所にバックアップしてください。アップグレード後、編集したファイルと新しくインストールしたファイルの違いを手動でマージし、必要な変更を新しい **server.xml** ファイルに転送する必要があります。

IPv6 のセットアップ手順 3: Strict Transport Security (HSTS)

1. **web.xml** ファイルを見つけます。

注意

デフォルトで、**web.xml** は次の場所に配置されています。**C:\Program Files (x86)\Acronis\Acronis Cyber Files\Access Server\Web Application\WEB-INF**

2. 既存の **web.xml** ファイルのバックアップコピーを作成します。
3. テキストエディタで元の **web.xml** を開き、次のブロックを追加します。

```
<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
    <init-param>
        <param-name>hstsMaxAgeSeconds</param-name>
        <param-value>31536000</param-value>
    </init-param>
    <init-param>
        <param-name>hstsIncludeSubDomains</param-name>
        <param-value>true</param-value>
    </init-param>
</filter>
<filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
    <dispatcher>FORWARD</dispatcher>
</filter-mapping>
```

4. 変更内容を保存します。
5. Windows の [サービス] パネルから Acronis Cyber Files Tomcat サービスを再起動します。

注意

ブラウザで開発ツールを使用すると、すべての要求の Strict-Transport-Security ヘッダーを確認できるはずです。

警告

これらの手動による変更は、アップグレード時に保持されません。このファイルは、必ず Acronis Cyber Files サーバーのインストール以外の場所にバックアップしてください。アップグレード後、手動で編集したファイルを新しくインストールしたファイルと比較し、必要な変更を新しい **web.xml** ファイルに移植する必要があります。

Mobile Device Management

Mobile Device Management (MDM) は、組織のモバイルデバイス、およびそれらのデバイスにインストールされているアプリの使用とセキュリティを管理します。

Acronis は、次の MDM プラットフォームで Cyber Files アプリをテストしました。

- **[Ivanti Neurons for MDM]** (旧 MobileIron Cloud) :
 - iOS 用 Cyber Files アプリ。
 - Android 用 Cyber Files アプリ (AppConnect 管理を使用しない)。
 - [Ivanti AppConnect対応バージョンの Android 用 Cyber Files アプリ](#)。

注意

Ivanti Neurons for MDM ドキュメントにアクセスするには、[こちら](#)をクリックしてください。

- **[Ivanti Endpoint Manager Mobile]** (旧 MobileIron Core) :
 - iOS 用 Cyber Files アプリ。
 - Android 用 Cyber Files アプリ (AppConnect 管理を使用しない)。
 - [Ivanti AppConnect対応バージョンの Android 用 Cyber Files アプリ](#)。

注意

Ivanti Endpoint Manager Mobile (EPMM) ドキュメントにアクセスするには、[こちら](#)をクリックしてください。

- **Microsoft Intune:**
 - iOS 用 Cyber Files アプリ。

管理対象アプリ構成 (AppConfig)

Acronis Cyber Files アプリは、管理対象アプリ構成 (AppConfig) をサポートしています。

リストされている前提条件が満たされている場合、特定のキーを Mobile Device Management (MDM) 構成に追加できます。これらのキーは Cyber Files アプリで有効になります。

前提条件

- デバイスは MDM サーバーで管理されている必要があります。
- アプリバイナリが MDM サーバーによってデバイス上にインストールされている必要があります。
- MDM サーバーで、**ApplicationConfiguration** 設定、および **ManagedApplicationFeedback** コマンドがサポートされている必要があります。

サポートされているキー

キー名	必須?	値	説明	コメント
enrollmentServer	Obligatory	DN アドレス	ユーザーが登録する Cyber Files サーバーの DNS アドレスに設	

			定する必要があります。	
enrollmentPIN	オプション	PIN コード	Cyber Files サーバーがクライアント登録に PIN コードを要求する場合は、登録フォームの [PIN コード] フィールドにこの値を自動入力できます。 AppConnect は、ワンタイム PIN コードではなく、ユーザーがアクセスを取得する前の認証の二次要因として機能できるので、多くの場合 Cyber Files サーバーの PIN 要求は無効になっています。 PIN 要件は、Webコンソールの [設定] ページ で設定します。	
userName	オプション	変数	Cyber Files 登録フォームの [ユーザー名] フィールドに入力します。 変数を使用すると、特定ユーザーのユーザー名でこの値を自動入力できます。 Ivanti の \$USERID\$ ワイルドカードを使用することができます。このワイルドカードを使用すると、Ivanti アプリをセットアップするときにユーザーが入力したユーザー名がフィールドに自動記入されます。	
enrollmentUserNameLock	オプション	Yes、No	Yes に設定すると、登録フォームの [ユーザー名] フィールドが変更できなくなります。	以下の場合、フィールドはロックされません。 - ロックキーが No に設定されている。 - ロックキーが設定されていない。

				ロックするフィールド値が空である。
enrollmentServerNameLock	オプション	Yes、No	Yes に設定すると、登録フォームの [サーバーアドレス] フィールドが変更できなくなります。	

plist ファイル

plist ファイルは、アプリケーションデータを保存するための XML ファイルです。シンプルなテキストエディタを使用して作成および編集できます。

plistファイルの作成

1. 任意のテキストエディタを起動します。
2. 次のとおり入力します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
```

```
<dict>
```

目的のキーをここに入力

```
</dict>
```

```
</plist>
```

例:

```
<dict>
<key>enrollmentServer</key>
<string>server.example.com</string>
<key>userName</key>
<string>username</string>
<key>enrollmentPIN</key>
<string>11Y9KL</string>
</dict>
```

3. **plist.xml** という名前でファイルを保存します。

Ivanti (旧 MobileIron)

Ivanti を使用した Android 用 Cyber Files アプリ

Ivanti AppConnect 対応 Android 用 Cyber Files アプリ

Ivanti AppConnect を使用して Acronis Android 用 Cyber Files アプリ のインスタンスを管理するには、Ivanti AppConnect 対応バージョンを使用する必要があります。

このバージョンの Android 用 Cyber Files アプリ は、Ivanti プラットフォーム内で 'in-house' アプリとして扱う必要があります。

注意

'in-house' アプリを追加または管理する際にヘルプが必要な場合は、「[Ivanti アプリドキュメントのページ](#)」を参照してください。

重要

このバージョンは、Google Play ストアでは配布されていません。

Ivanti AppConnect 対応 Android 用 Cyber Files アプリ の .apk ファイルは、「[Cyber Files ダウンロードページ](#)」から入手できます。

Android 用 Cyber Files アプリ の自動登録

利用可能な Ivanti 自動登録パラメータ:

- **Server name**
サーバーの URL。
- **Username**
ユーザー ID。
- **Client Certificate**
- **Password**
ユーザーのパスワード。
- **PIN**
ユーザーの PIN。
- **Enable auto submit**
このパラメータを Yes に設定すると、ユーザーは構成パラメータを確認する必要がなくなります。

Android Enterprise

[Android Enterprise](#) により、Acronis Android 用 Cyber Files アプリ アプリユーザーの安全な自動登録が可能になります。

Android Enterprise には、Endpoint Manager Mobile (EPMM) ソフトウェアが必要です。

重要

現在、Cyber Files は、Ivanti EPMM を使用したユーザーの自動登録のみをサポートしています。

そのため、Android Enterprise を使用するには、[AppConnect 対応版の Android アプリ](#)をインストールする必要があります。

Ivanti EPMM の詳細については、[Ivanti のドキュメント](#)を参照してください。

Ivanti を使用した iOS 用 Cyber Files アプリ

iOS 用 Cyber Files アプリ コンテナポリシー

以下のパラメータが使用可能です。

- **Allow Print** - ユーザーが Acronis iOS 用 Cyber Files アプリ からドキュメントを印刷できるようにするには、このオプションを選択します。
- **Allow Copy/Paste To** - ユーザーが iOS 用 Cyber Files アプリ に表示されるドキュメントのテキストをコピーして、AppConnect によって管理されていないデバイスのその他のアプリに貼り付けることを許可する場合は、このオプションを選択します。

警告

これが有効な場合、Cyber Files **開いているファイルからテキストをコピーする設定** よりも優先されます。

- **Allow Open In** - iOS 用 Cyber Files アプリ ユーザーがデバイスの別のアプリでファイルを開くことを許可する場合は、このオプションを選択します。

Ivanti による iOS 用 Cyber Files アプリ のアクティブ化

これは、Avanti VSP コンソールでアプリのリストに Acronis iOS 用 Cyber Files アプリ を追加しておらず、ユーザーがまだアプリを使用していない場合にのみ必要です。

アプリが Ivanti を使用して追加されている場合には、ユーザーはアプリを Ivanti ストアからダウンロードできます。設定によっては、デバイスに自動でインストールされる場合もあります。

アプリはインストールされており、Cyber Files サーバーに登録されていません

Mobile@Work と AppConnect VSP の構成が設定される前に、Acronis iOS 用 Cyber Files アプリ がデバイスにインストールされ、開始されている場合、アプリを起動しても AppConnect の設定処理は自動的に開始されない場合があります。

iOS 用 Cyber Files アプリ の Ivanti AppConnect 設定処理を手動で開始するには、次の操作を実行します。

1. アプリを開きます。
2. **[設定]** メニューを開きます。
3. リスト下部にある **[Ivanti AppConnect]** オプションをタップします。
4. **[有効]** ボタンをタップします。

注意

必要な Ivanti アプリがデバイスにインストールされていない場合、**[有効]** ボタンではなく警告が表示されます。

AppConnect の設定処理が開始されるまでに数分かかる場合があります。これが実行されると、処理は前のシナリオで示したように進みます。

アプリがインストールされ、Cyber Files サーバーに登録されました

このシナリオは前のシナリオに似ています。ただ 1 つの違いは、アプリを自動登録するために AppConnect Acronis Cyber Files の構成が使用されないという点です。アプリが既に Cyber Files サーバーに登録されている場合は、元の構成が維持されます。

iOS 用 Cyber Files アプリ を AppConnect で管理するには、次の操作を実行します。

注意

これにより、AppConnect のパスコードおよび許可コンテナポリシーの使用も開始されます。

1. iOS 用 Cyber Files アプリ を開きます。
2. **[設定]** -> **[Partner Features]** -> **[MobileIron]** を選択します。
3. **[AppConnect を有効にする]** をタップします。
4. プロセスが完了するまで待ちます。
5. アプリを再起動します。

注意

ユーザーに対して別の Cyber Files サーバーへの登録を求める場合は、AppConnect による構成が可能になるように、iOS 用 Cyber Files アプリ のアンインストールと再インストールが必要になります。

アプリがインストールされていない

このシナリオでは、Apple App Store または Ivanti ストアから Acronis iOS 用 Cyber Files アプリ をインストールする必要があります。

インストールしたら、ユーザーはアプリを起動する必要があります。構成済みの Ivanti アプリがデバイスに存在する場合、制御は一時的にそれに切り替えられ（これはチェックインと呼ばれます）、その後 iOS 用 Cyber Files アプリ に戻ります。

有効な Cyber Files AppConnect 構成が見つかり、iOS 用 Cyber Files アプリ は自動的に登録モードに入り、登録フォームをユーザーに提示します。

AppConnect 構成に含まれるフィールドは、自動的に入力されます。ユーザーは通常、フォームに AD パスワードを入力し、送信するだけですみます。これが完了すると、関連する Cyber Files クライアント管理ポリシーがアプリに適用され、アプリを使用できるようになります。

警告

iOS 用 Cyber Files アプリ の有効な構成が VSP に存在しない場合、または Ivanti アプリが構成されていない場合、ユーザーはエラーメッセージを受け取ります。

Ivanti アプリがデバイスにインストールされていない場合、iOS 用 Cyber Files アプリ は AppConnect を有効にせずに標準モードで起動します。

Ivanti チェックイン

Acronis Cyber Files アプリが Ivanti AppConnect によって管理される場合、そのアプリが Ivanti アプリにチェックインしたときに、適用可能なコンテナポリシーに対する変更がインストール済みアプリによって受信されます。

このチェックインにより、Cyber Files アプリが一時的に Ivanti アプリに切り替わります。

その結果、ユーザーがその時点でアクティブである場合、一時停止が発生する場合があります。

一方、Cyber Files アプリへのアクセスの取り消しなどもチェックイン時に適用されるため、組織のチェックイン回数は慎重に選ぶ必要があります。

注意

チェックイン頻度は Ivanti 製品で設定されます。

Microsoft Intune

Microsoft Intuneは、モバイルデバイス、モバイルアプリケーション、およびPCをクラウドから管理する機能を提供します。組織でIntuneを利用すると、社内情報をセキュリティで保護しながら、従業員がほぼすべてのデバイスで、事実上どこからでも、社内のアプリケーション、データ、およびリソースにアクセスできるようになります。モバイルデバイスを登録するためには、Intuneをモバイルデバイスの機関として設定し、管理を必要とするプラットフォームをサポートするようにインフラストラクチャを設定する必要があります。これには、デバイスとの信頼関係の確立が必要になります。

注意

この機能は、Acronis Cyber Files iOS クライアント、バージョン 7.0.5 以降でのみサポートされています。

注意

デバイスポリシーを適用するには、**Microsoft Intune Company Portal** を使用して Acronis Cyber Files をインストールし、**Acronis Cyber Files** の [デフォルトのアクセス制限] ([**モバイルアクセス**] > [**ポリシー**] > [**デフォルトのアクセス制限**]) または各ゲートウェイの [アクセス制限] で [**Intune が管理する iOS クライアントを許可**] と [**iOS 管理対象アプリ**] **iOS クライアントを許可** を有効にする必要があります。

注意

[**アプリケーションポリシー**] を適用し、Acronis Cyber Files を Intune で管理するには、Acronis Cyber Files サーバーから [**Intune Mobile Application Management の登録をトリガーする**] を有効にする必要があります ([**モバイルアクセス**] > [**ポリシー**] > [**サーバーポリシー**]) 。

Active Directory グループ

Active Directory グループを作成するには、次の操作を実行します。

1. Microsoft Azure ポータルを開きます。
2. [**すべてのサービス**] を選択します。
3. 検索ボックスに「**azure**」と入力して [**Azure Active Directory**] を選択します。
4. [**グループ**] を開きます。
5. [**新しいグループ**] を選択して、必要な情報を入力します。
6. グループの希望するメンバーを選択します。
7. [**作成**] を選択します。

Intune に追加された iOS 用 Cyber Files アプリ

Intune の **デバイスポリシー**を使用する場合、Intune 社内ポータルから iOS 用 Cyber Files アプリ をインストールする必要があります。

iOS 用 Cyber Files アプリ を Intune に追加するには、次の操作を実行します。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックします。
3. 検索ボックスに「Intune」と入力し、**[Microsoft Intune]** を選択します。
4. Intune ポータルで、**[モバイルアプリ]** を開きます。
5. **[アプリ]** を開きます。
6. **[追加]** を選択して、**[アプリの追加]** オプションを選択します。
 - **[アプリの種類]** で **[iOS]** を選択します。
 - **[App Store を検索]** をクリックして、**Acronis Cyber Files**を検索し、そのアプリを選択します。
 - **[アプリ情報]** をクリックして、希望する構成変更を行います。
7. **[会社のポータルでおすすめアプリとして表示します]** を有効にします。
8. **[OK]** を選択します。
9. リストのアプリをクリックし、**[割り当て]** を選択します。
10. このアプリに割り当てるユーザーまたはグループを選択します。

デバイスポリシー

iOS 用 Cyber Files アプリ のデバイスポリシーを追加するには、次の操作を実行します。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックします。
3. 検索ボックスに「Intune」と入力し、**[Microsoft Intune]** を選択します。
4. **[デバイス構成]** -> **[プロファイル]** を開きます。
5. **[プロファイルの作成]** を選択します。
6. 名前を入力し、**[プラットフォーム]** として **[iOS]** を選択して、デバイスに適用する制限を選択します。
7. iOS 用 Cyber Files アプリ では、次の制限のみをサポートします。
 - **App Store、ドキュメント表示、ゲーム -> 管理対象外のアプリでの社内ドキュメントの表示。**
管理対象アプリの **[他のアプリで開く]/[他のアプリに保存]** リストに管理対象外アプリを表示させたくない場合、このオプションの **[ブロック]** を選択します。
 - **App Store、ドキュメント表示、ゲーム -> 社内アプリでの社外ドキュメントの表示。**
管理対象外アプリの **[他のアプリで開く]/[他のアプリに保存]** リストに管理対象アプリを表示させたくない場合、このオプションの **[ブロック]** を選択します。
8. アプリがリストに追加されたら、それをタップし、**[割り当て]** を選択します。
9. 割り当て先となるユーザー/グループを選択します。

注意

デバイスポリシーをアプリに割り当てるには、社内ポータルからそのアプリをダウンロードする必要があります。

アプリ保護ポリシー

注意

このポリシーは、モバイルアプリ管理ポリシーとしても機能します。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]** をクリックします。
3. 検索ボックスに「Intune」と入力し、**[Microsoft Intune]** を選択します。
4. **[モバイルアプリ]** を開きます。
5. **[アプリ保護ポリシー]** を開きます。
6. **[ポリシーの追加]** を選択します。
7. ポリシーの名前を入力します。
8. **Acronis Cyber Files** を必要なアプリとして選択します。
9. **[設定]** をタップし、適用する保護ポリシーを選択します。
10. アプリがリストに追加されたら、それをタップします。
11. **[割り当て]** を選択します。
12. 割り当て先となるユーザー/グループを選択します。

注意

[元データを他のアプリに送信する]/[他のアプリからデータを受信する] を **[ポリシーで管理されているアプリ]** に設定した場合、**Acronis Cyber Files** ドキュメントプロバイダ拡張機能がその他の Microsoft Intune 管理対象アプリで動作するように、**IntuneMAMUPN** キーを使用して別々の **アプリ構成ポリシー** を Microsoft 管理対象アプリと Acronis Cyber Files アプリの両方に適用する必要があります。

注意

デバイスが IntuneMAMUPN キーにより管理される MDM であるとみなされる場合、**アプリ保護ポリシー** の **[元データを他のアプリに送信する]** と **[他のアプリからデータを受信する]** オプションの適用は停止され、**デバイス構成プロファイル** 内の MDM 設定の **[管理対象外のアプリでの社内ドキュメントの表示]** と **[社内アプリでの社外ドキュメントの表示]** が使用されます。

必ず Intune で管理されたアプリ間のみで社内ドキュメントが開かれるようにするには、特定のプロファイルの **[プロパティ]** -> **[設定]** -> **[App Store、ドキュメント表示、ゲーム]** に移動し、**[管理対象外のアプリでの社内ドキュメントの表示]** と **[社内アプリでの社外ドキュメントの表示]** の両方を **[ブロック]** に設定する必要があります。

注意

ドキュメントプロバイダ拡張機能がポリシー管理対象アプリと連携するためには、**[元データを他のアプリに送信する]** オプションを **[OS 共有を使用してポリシーで管理されているアプリ]** または **[すべてのアプリ]** に設定する必要があります。

注意

Acronis Cyber Files から Word（またはその他の Microsoft アプリ）でファイルを開くには、目的の Microsoft アプリケーション用に別の Intune **アプリ保護ポリシー**を用意する必要があります。また、**[すべての種類を対象とする]**を**[はい]**に設定する必要があります。

アプリ設定ポリシー

Intune の資格情報で自動的に登録するには、**[アプリ構成ポリシー]**を作成するか、独自のポリシーに追加する必要があります。

構成ポリシーに追加するには、次の操作を実行します。

1. Microsoft Azure ポータルを開きます。
2. **[すべてのサービス]**をクリックします。
3. 検索ボックスに「**Intune**」と入力し、**[Microsoft Intune]**を選択します。
4. **[モバイルアプリ]**を開きます。
5. **[アプリ構成ポリシー]**を開きます。
6. **[追加]**を選択して、ポリシーの名前を入力します。
7. **[デバイス登録の種類]**として**[マネージドデバイス]**を選択します。
8. **[プラットフォーム]**として**[iOS]**を選択します。
9. この構成を配置する対象となるアプリを選択します。
10. **[構成]**設定では、**[XML]**または**[構成デザイナー]**の2つのオプションから選択できます。
 - **[XML]**を選択する場合、次のように入力します。

```
<dict>
<key>IntuneMAMUPN</key>
<string>{{userprincipalname}}</string>
</dict>
```

- **[構成デザイナー]**を選択する場合、次のように入力します。
 - **[構成キー]**には、「**IntuneMAMUPN**」と入力します。
 - **[構成値]**には、「**{{userprincipalname}}**」と入力します。
 - **[値の型]**には**[文字列]**を選択します。

11. Cyber Files の資格情報で自動登録する場合、**[XML]**で次のキーを使用できます。

```
<dict>
<key>enrollmentServerName</key>
<string>192.168.1.10</string>
<key>enrollmentUserName</key>
<string>jprice</string>
<key>enrollmentAutoSubmit</key>
<string>Yes</string>
</dict>
```

12. アプリがリストに追加されたら、それを選択します。

13. **【割り当て】**を選択します。
14. 割り当て先となるユーザー/グループを選択します。

新機能

現在のリリースと過去のリリースに含まれる内容の詳細については、『Acronis Cyber Files [リリース履歴ドキュメント](#)』を参照してください。

既知の問題

- ファイルをデスクトップクライアントと同期する際に問題が発生する場合があります。回避策としては、デスクトップクライアントアプリを完全に削除してから再インストールし、サーバーへの接続を再確立します。
- 単一ポートのAccess Gateway Server構成を使用する場合、256文字を超えるパスのネットワークノード処理に問題が発生する可能性があります。 [Acronisサポートポータルの記事](#)を参照して、UrlSegmentMaxLengthを増やすことで、この問題を解決してください。
- SSOを使用している場合、ネットワークノードには Web UI からアクセスできず、アクセスを試みるとサインアウトされます。

古いバージョン用のドキュメント

古いバージョンの Acronis Cyber Files ドキュメントについては、以下のリンクから確認してください。

注意

古いバージョンのドキュメントはご希望の言語に対応していない場合があります。

- [8.9.x](#)
- [8.8.x](#)
- [8.7.x](#)
- [8.6.x](#)
- [8.9.x](#)
- [8.8.x](#)
- [8.5.x](#)
- [8.1.x](#)
- [8.0.x](#)
- [7.5.x](#)
- [7.4.x](#)
- [7.3.x](#)
- [7.2.x](#)
- [7.1.x](#)
- [7.0.x](#)
- [6.0.x](#)
- [5.0.x](#)

著作権情報

© Acronis International GmbH, 2003-2024. All rights reserved.

ユーザーズ ガイドに掲載されているすべての商標や著作権は、それぞれ各社に所有権があります。

著作権者の明示的許可なく本書を修正したものを配布することは禁じられています。

著作権者の事前の許可がない限り、商用目的で書籍の体裁をとる作品または派生的作品を販売させることは禁じられています。

本書は「現状のまま」使用されることを前提としており、商品性の黙示の保証および特定目的適合性または非違反性の保証など、すべての明示的もしくは黙示的条件、表示および保証を一切行いません。ただし、この免責条項が法的に無効とされる場合はこの限りではありません。

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。ソフトウェアまたはサービスで使用されているサードパーティコードおよび関連ライセンス条件の最新の一覧については <https://kb.acronis.com/content/7696>（英語）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 1 つ以上の米国特許によって保護されています。
7,047,380号、7,246,211号、7,275,139号、7,281,104号、7,318,135号、7,353,355号、7,366,859号、
7,383,327号、7,475,282号、7,603,533号、7,636,824号、7,650,473号、7,721,138号、7,779,221号、
7,831,789号、7,836,053号、7,886,120号、7,895,403号、7,934,064号、7,937,612号、7,941,510号、
7,949,635号、7,953,948号、7,979,690号、8,005,797号、8,051,044号、8,069,320号、8,073,815号、
8,074,035号、8,074,276号、8,145,607号、8,180,984号、8,225,133号、8,261,035号、8,296,264号、
8,312,259号、8,347,137号、8,484,427号、8,645,748号、8,732,121号、8,850,060号、8,856,927号、
8,996,830号、9,213,697号、9,400,886号、9,424,678号、9,436,558号、9,471,441号、9,501,234号、お
よび出願中特許。

