

アプライアンス ユーザ ガイド

Arcserve Unified Data Protection

バージョン 10.0

arcserve®

アプライアンス ユーザ ガイド

Arcserve Unified Data Protection

バージョン 10.0

目次が左側のペインに表示されます。すべてのトピックを表示するには、上部の  TOC アイコンをクリックします。

arcserve®

リーガル ノーティス

組み込みのヘルプシステムおよび電子的に配布される資料も含めたこのドキュメント(以下「本書」)はお客様への情報提供のみを目的としたもので、Arcserveにより随時、変更または撤回されることがあります。このドキュメントは、Arcserveの専有情報であり、Arcserveの事前の書面による承諾なしに、全部または一部をコピー、譲渡、複製、開示、変更、複写することを禁止します。

本ドキュメントで言及されているソフトウェア製品のライセンスを受けたユーザは、社内ユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを適切な部数だけ作成できます。ただし、Arcserveのすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本書を印刷するかまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、そのライセンスが終了した場合には、ユーザはArcserveに本書の全部または一部を複製したコピーをArcserveに返却したか、または破棄したことを文書で証明する責任を負います。

準拠法により認められる限り、ARCSERVEは本書を現状有姿のまま提供し、商品性、お客様の使用目的に対する適合性、他者の権利に対する不侵害についての黙示の保証を含むいかなる保証もしません。また、本システムの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の損失等、いかなる損害(直接損害か間接損害かを問いません)が発生しても、ARCSERVEはお客様または第三者に対し責任を負いません。ARCSERVEがかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本書に記載されたソフトウェア製品は、該当するライセンス契約書に従い使用されるものであり、当該ライセンス契約書はこの通知の条件によっていかなる変更も行われません。

本書の制作者はArcserveです。

「制限された権利」のもとでの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Section 12.212、52.227-14、52.227-19(c)(1) - (2)、DFARS Section 252.227-7014(b)(3)、またはこれらの後継の条項で規定されている該当する制限に従うものとします。

© 2024 Arcserve (その関連会社および子会社を含む) All rights reserved. サードパーティの商標または著作権は各所有者に帰属します。

Arcserve サポートへのお問い合わせ

Arcserve サポート

[テクニカルサポートへのお問い合わせ](#)

Arcserve サポートをご利用いただくと次のことができます。

- Arcserve サポートの専門家が社内で共有しているのと同じ情報ライブラリに直接アクセスできます。このサイトから、弊社のナレッジベース(KB)ドキュメントにアクセスできます。ここから、重要な問題やよくあるトラブルについて、製品関連 KB 技術情報を簡単に検索し、検証済みのソリューションを見つけることができます。
- ライブチャットリンクを使用して、Arcserve サポートチームと瞬時にリアルタイムで会話を始めることができます。ライブチャットでは、製品にアクセスしたまま、懸念事項や質問に対する回答を即座に得ることができます。
- Arcserve グローバルユーザコミュニティでは、質疑応答、ヒントの共有、ベストプラクティスに関する議論、他のユーザとの対話に参加できます。
- サポートチケットを開くことができます。オンラインでサポートチケットを開くと、質問の対象製品を専門とする担当者から直接、コールバックを受けられます。
- また、使用している Arcserve 製品に適したその他の有用なリソースにアクセスできます。

Arcserve アプライアンスの返品ポリシー

有効な RMA (返品認定) 番号は、製品を Arcserve に返却するために必要です。RMA 番号を取得するには、Arcserve テクニカルサポート部門にお問い合わせください。お客様の担当者の連絡先情報については、arcserve.com/support を参照してください。サポート チームから RMA データの送信先が通知される場合があります。

返品には、10% の返品手数料がかかります。以下は例外となります。1) 注文が間違っ て履行された場合、Arcserve は RMA を受け入れ、全額を返金します。2) 欠陥のあるアイテムが 30 日以内に返品された場合、Arcserve は RMA を受け入れ、全額を返金します。3) ハードウェアに技術的な問題がある場合、解決のための適切な期間を経過した後もサポートによって解決できなければ、Arcserve は RMA を受け入れ、同等の価値のあるハードウェアの交換を提供します。

RMA リクエストに必要な情報：

- 製品のシリアル番号(アプライアンスの背面に記載があります)
- Arcserve 注文番号
- パートナーの連絡先名
- パートナーの電話番号
- パートナーの電子メールアドレス
- お客様の連絡先名(可能な場合)
- 電話番号(可能な場合)
- 電子メールアドレス(可能な場合)
- 問題の説明とすでに実行されたトラブルシューティングの説明。
- 要求された配送サービスおよび出荷先住所。

RMA 番号は、パッケージの外側に明確に記されている必要があります。すべての RMA は、適切な梱包で出荷される必要があります。すべての RMA は、荷物のトラックングおよび保証を提供する信頼できる運送業者を使用して出荷する必要があります。出荷時の破損または RMA の損失はお客様の責任になります。

目次

第1章: Arcserve アプライアンス のドキュメントについて	1
言語サポート	2
製品ドキュメント	3
第2章: Arcserve アプライアンス の紹介	5
概要	6
Arcserve Unified Data Protection	7
Arcserve Unified Data Protection Agent for Linux	8
Arcserve Backup	9
Arcserve Continuous Availability	10
安全に関する注意事項	11
同梱されている内容	12
アプライアンス 10000 シリーズのボックスに同梱されている内容	12
アプライアンス 9000 シリーズのボックスに同梱されている内容	13
アプライアンス X シリーズのボックスに同梱されている内容	14
箱に含まれていない項目	16
利用可能なモデル	17
モデル 10024BU-10576DR	17
モデル 9012 - 9504DR	19
モデル X シリーズ	21
コントロールおよびインジケータ	24
前面パネル 10048DR-10576DR	24
ドライブ キャリアの LED	25
コントロールパネル	26
情報 LED	27
前面パネル 9012-9048	27
前面パネル 9072DR - 9504DR	28
前面パネル X シリーズ	29
背面パネル 10048DR-10576DR	29
電源 インジケータ	30
背面パネル 9012-9048	31
背面パネル 9072DR-9504DR	33
背面パネル X シリーズ	34
アプライアンスが使用するポート	35

Arcserve UDP	36
Microsoft Windows にインストールされるコンポーネント	37
Linux にインストールされているコンポーネント	43
リモートで UDP Linux により保護されているノード	44
Arcserve Backup	45
Linux 用 アプライアンスのサポート	46
第3章: アプライアンス上の Arcserve UDP のアップグレード	48
Arcserve ソフトウェアのアップグレード後にライセンスを適用する方法	49
Arcserve アプライアンスでのアップグレード シーケンス	50
Arcserve アプライアンスを Arcserve UDP コンソールおよび RPS として使用した場合のアップグレード	51
Arcserve アプライアンスを Arcserve UDP RPS として使用した場合のアップグレード	52
複数の Arcserve アプライアンスが環境で使用されている場合のアップグレード手順	53
Arcserve アプライアンス上の Arcserve UDP Linux エージェントのアップグレード	54
Arcserve アプライアンスに搭載された Arcserve Backup のアップグレード	55
UDP コンソール、RPS、エージェントのアップグレード シーケンス	56
第4章: Arcserve アプライアンスの設定	57
Arcserve アプライアンス向けのネットワーク設定を構成する方法	58
Arcserve アプライアンスを設定する方法	62
Arcserve アプライアンスをゲートウェイとして設定する方法	72
第5章: Arcserve アプライアンスでの操作	73
アプライアンス上の Arcserve 製品のアクティブ化	74
Arcserve アプライアンス ウィザードを使用したプランの作成	75
プランへのノードの追加	76
ホスト名/IP アドレスによるノードの追加	77
Active Directory によるノードの追加	79
vCenter/ESX ノードの追加	81
Hyper-V ノードの追加	83
Linux ノード用のバックアッププランの作成	85
テープ デバイスへのバックアッププランの作成	86
アプライアンス上仮想スタンバイプランの作成	87
Linux バックアップ サーバのバックアッププランの作成	88
ローカル アプライアンス Hyper-V に対して Linux インスタント VM ジョブを実行するための設定	92
ConsoleMigration.exe を使用した Arcserve UDP コンソールの移行	93
Arcserve アプライアンス間の移行	95
解決策	96

プレインストールされた Linux バックアップ サーバの入力ソースの変更	99
第6章: アプライアンス サーバのリモート モニタリング	102
iDRAC (Integrated Dell Remote Access Controller) での操作	103
iDRAC (Integrated Dell Remote Access Controller) のモニタと管理	104
iDRAC (Integrated Dell Remote Access Controller 9000 シリーズ) の IP アドレスの検出	106
iDRAC (Integrated Dell Remote Access Controller、X シリーズ) の IP アドレスの検出	107
iDRAC の DHCP または静的 IP アドレスの設定	109
ベースボード管理コントローラ(BMC) の操作	113
ベースボード管理コントローラ(BMC) のモニタおよび管理	113
BMC の IP アドレスを確認する方法	115
BIOS を使用した IP アドレスの確認	115
POST 画面での IP アドレスの確認	115
BMC の DHCP または静的 IP アドレスの設定	116
UEFI BIOS の設定	116
BMC の IP アドレスの設定	117
DHCP サーバを使用した DHCP IP アドレスの設定	117
BIOS を使用した静的 IP アドレスの設定	117
BIOS を使用した BMC への接続	120
第7章: Arcserve アプライアンス のリストアまたは修復	124
ファクトリリセットのデバッグ	125
Arcserve アプライアンス のインストール	127
Arcserve Backup 19.0 をインストールする方法	128
10024BU-10048BU シリーズ アプライアンスの設置方法	135
10048DR-10576DR シリーズ アプライアンスの設置方法	136
9012-9048 シリーズ アプライアンスの設置方法	136
9072-9504DR シリーズ アプライアンスの設置方法	136
X シリーズ アプライアンスの設置方法	136
10024BU-10576DR シリーズ アプライアンスでの Arcserve UDP ファクトリリセットの適用	136
BIOS からのファクトリリセット	137
Arcserve UDP コンソールからのファクトリリセット	139
9012 - 9504 DR シリーズ アプライアンスのブート オプションを使用した Arcserve UDP ファクトリリセットの適用	142
X シリーズ アプライアンスのブート オプションを使用した Arcserve UDP ファクトリリセットの適用	144
環境設定の消去およびアプライアンス ファクトリリセットの適用	147
ハードドライブの取り外しおよび交換	150

9012-9504DR シリーズ アプライアンスでのデータを保存しないベアメタル復旧 (BMR) の実行	152
9012-9504DR シリーズ アプライアンスでのベアメタル復旧 (BMR) およびデータ保存の実行	166
第9章: アプライアンスの容量拡張	173
Arcserve アプライアンス 10024BU-10576DR モデルの拡張キットでの操作	173
Arcserve アプライアンス 10024BU-10576DR モデルの SSD フラッシュ拡張キットでの操作	178
Arcserve アプライアンス拡張キットの操作 - X シリーズ モデル	181
Arcserve X シリーズ アプライアンスの SSD フラッシュ拡張キットの操作	183
Arcserve アプライアンス 9072-9504DR モデルの拡張キットでの操作	190
Arcserve アプライアンス 9072-9504 DR モデルの SSD フラッシュ拡張キットの操作	195
第10章: ネットワーク設定の操作	199
ネットワーク設定の詳細	200
DHCP サーバを無効化する方法	204
プリインストールされた Linux バックアップ サーバの IP アドレスを設定する方法	205
負荷分散のために DNS サーバ上でラウンド ロビンを有効にする方法	207
アプライアンスのネットワークステータスを確認する方法	208
第11章: 安全に関する注意事項についての理解	209
一般的な安全に関する注意事項	210
電気に関する安全のための注意事項	212
FCC コンプライアンス	213
静電気放電 (ESD) に関する注意事項	214
Arcserve アプライアンス 10000 シリーズのファームウェアのアップグレード	215
ファームウェアのバージョンの表示	215
ファームウェア アップグレード パッケージのダウンロード	217
ファームウェアのアップグレード	218
BMC ファームウェアのアップグレード方法	218
BIOS ファームウェアのアップグレード方法	221
更新されたファームウェアの確認	225
第11章: Arcserve アプライアンス 9000 シリーズのファームウェアのアップグレード	226
Arcserve アプライアンス 9000 シリーズの BIOS ファームウェアのアップグレード	226
ファームウェアのバージョンの表示	226
方法 1: iDRAC Web インターフェースから BIOS ファームウェアのバージョンを表示する	228
方法 2: BIOS Arcserve Appliance 9000 シリーズから BIOS ファームウェアバージョンを表示する	228
BIOS の更新されたパッケージのダウンロード	229

BIOS のアップグレード	229
更新されたファームウェアの確認	230
システム ログを使用して更新された BIOS を確認する	231
iDRAC Web インターフェースまたは BIOS から更新された BIOS を確認する	232
Arcserve アプライアンス 9000 シリーズの iDRAC ファームウェアのアップグレード	232
iDRAC ファームウェア バージョンの表示	232
iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示する	232
方法 2: BIOS Arcserve Appliance 9000 シリーズから iDRAC ファームウェアのバージョンを表示する	233
iDRAC パスワードの変更方法	234
iDRAC の更新されたパッケージのダウンロード	235
iDRAC のアップグレード	235
更新された iDRAC の確認	236
システム ログを使用して更新された iDRAC を確認する	236
iDRAC Web インターフェースまたは iDRAC から更新された BIOS を確認する	237
Arcserve アプライアンス X シリーズのファームウェアのアップグレード	238
Arcserve アプライアンス X シリーズの BIOS ファームウェアのアップグレード	238
BIOS ファームウェア バージョンの表示	238
方法 1: iDRAC Web インターフェースから BIOS ファームウェアのバージョンを表示する	238
方法 2: BIOS Arcserve アプライアンス X シリーズから BIOS ファームウェア バージョンを表示する	239
BIOS の更新されたパッケージのダウンロード	240
BIOS のアップグレード	240
更新された BIOS の確認	241
Arcserve アプライアンス X シリーズの iDRAC ファームウェアのアップグレード	241
iDRAC ファームウェア バージョンの表示	241
方法 1: iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示する	241
方法 2: BIOS Arcserve アプライアンス X シリーズから iDRAC ファームウェア バージョンを表示する	242
iDRAC の更新されたパッケージのダウンロード	243
iDRAC のアップグレード	243
更新された iDRAC の確認	244
第 12 章: トラブルシューティング	245
Linux バックアップ サーバにコンソールから接続できない	246
別のアプライアンスから Arcserve アプライアンス のバックアップを実行すると重複ノードがレポートされる	247
Linux バックアップ サーバがネット ワーク内のノードと通信できない	248
Linux バックアップ サーバがネット ワーク DNS サフィックスを取得できない	250
アプライアンスのデフォルトのタイムゾーン	251

ライセンスが利用可能な場合でもライセンスエラーが発生する	252
第13章: ベスト プラクティスの適用	253
ネットワーク構成に関する推奨事項	254
PowerShell コマンドレットによる Windows Defender のベストプラクティス	257
プリインストールされた Linux バックアップ サーバを外部ネットワークに設定する	257
ボリュームをまたぐデデュプリケーション データストアを作成するためのベスト プラクティス	258
第14章: 使用条件	261
PuTTY	262

第1章: Arcserve アプライアンス のドキュメントについて

Arcserve アプライアンス ユーザガイドは、Arcserve アプライアンスを使用する方法の理解に役立ちます。Arcserve アプライアンスの特長については、「概要」を参照してください。残りのセクションでは、Arcserve アプライアンスのインストールと使用方法について説明します。

このセクションには、以下のトピックが含まれます。

言語サポート	2
製品ドキュメント	3

言語サポート

翻訳済み製品(ローカライズ済み製品とも言います)とは、製品のユーザインターフェース、オンラインヘルプ、その他のドキュメントのローカル言語サポートに加えて、日付、時刻、通貨、数値に関してローカル言語でのデフォルトの書式設定をサポートする国際化製品です。

このリリースは英語版のみです。

製品ドキュメント

Arcserve UDP 関連のすべてのドキュメントを参照するには、このリンクをクリックして [Arcserve のドキュメント](#) にアクセスしてください。

Arcserve UDP ナレッジ センターは、以下のドキュメントで構成されています。

- **Arcserve UDP ソリューション ガイド**

一元管理されたコンソール環境で Arcserve UDP ソリューションを使用するための詳細情報が提供されています。このガイドには、ソリューションをインストールおよび設定する方法、データを保護およびリストアする方法、レポートを取得する方法、Arcserve High Availability を管理する方法などの情報が含まれています。手順には、コンソールの使用を中心に、さまざまな保護プランの使用方法が含まれています。

- **Arcserve UDP リリース ノート**

Arcserve Unified Data Protection の主な機能、システム要件、既知の問題、ドキュメントの問題、制限事項などの概要が説明されています。

- **Arcserve UDP Agent for Windows ユーザ ガイド**

Windows オペレーティングシステムで Arcserve UDP Agent を使用するための詳細情報が提供されています。このガイドには、エージェントをインストールおよび設定する方法、Windows ノードを保護およびリストアする方法などの情報が含まれています。

- **Arcserve UDP Agent for Linux ユーザ ガイド**

Linux オペレーティングシステムで Arcserve UDP Agent を使用するための詳細情報が提供されています。このガイドには、エージェントをインストールおよび設定する方法、Linux ノードを保護およびリストアする方法などの情報が含まれています。

第2章: Arcserve アプライアンス の紹介

このセクションには、以下のトピックが含まれます。

<u>概要</u>	6
<u>安全に関する注意事項</u>	11
<u>同梱されている内容</u>	12
<u>箱に含まれていない項目</u>	16
<u>利用可能なモデル</u>	17
<u>コントロールおよびインジケータ</u>	24
<u>アプライアンスが使用するポート</u>	35

概要

Arcserve アプライアンスは、アシュアード リカバリ™ を初めて搭載した、完成され最もコスト効率の良い保護アプライアンスです。各 Arcserve アプライアンスは、自己完結型の「set and forget (設定後は作業不要)」のバックアップ/復旧ソリューションです。クラウド ネイティブ機能によって構築されており、その極めて容易な導入とユーザビリティが、一連の幅広い機能(ソースベースのグローバル デデュプリケーション、マルチサイト レプリケーション、テープのサポート、自動化されたデータ復旧機能などの)と組み合わせられています。Arcserve アプライアンスは、運用において優れた敏捷性と効率性を実現し、障害復旧作業を大幅に簡略化します。

Arcserve アプライアンスは、最新のハードウェアにプリインストールされている主要な Arcserve Unified Data Protection ソフトウェアと完全に統合されています。アプライアンスは、すべてのユーザに対して、完全な統合データ保護ソリューションを提供し、現在の需要を満たすだけでなく、絶え間なく変化するバックアップ、アーカイブ、惨事復旧(DR)の今後の要件にも対応できます。

Arcserve アプライアンスにプリインストールされたソフトウェアは、以下のとおりです。

- Arcserve UDP
- Arcserve Unified Data Protection Agent for Linux
- Arcserve Backup

Arcserve アプライアンスにはハードウェア保証が規程されています。アプライアンスの保証の詳細については、[\[アプライアンスの保証\]](#)を参照してください。

Arcserve Unified Data Protection

Arcserve UDP ソフトウェアは、複雑な IT 環境を保護する包括的なソリューションです。このソリューションは、Windows、Linux、VMware ESX Server、Microsoft Hyper-V Server など、さまざまな種類のノードに存在するデータを保護します。ローカルマシンまたは復旧ポイント サーバのいずれかへデータをバックアップできます。復旧ポイント サーバは複数のソースからのバックアップが保存される中央サーバです。

サポートされているオペレーティングシステムの詳細については、「[動作要件](#)」を参照してください。

Arcserve UDP には、以下の機能が用意されています。

- 復旧ポイント サーバ上のデデュプリケーション/非 デデュプリケーション データストアにデータをバックアップ
- Arcserve Backup (アプライアンスに含まれています) との統合を使用して、復旧ポイントをテープにバックアップ
- バックアップ データから仮想スタンバイ マシンを作成
- バックアップ データを復旧ポイント サーバおよびリモート復旧ポイント サーバにレプリケート
- バックアップ データをリストアし、ベアメタル復旧 (BMR) を実行
- 選択したデータ バックアップ ファイルをセカンダリバックアップ先へコピー
- 環境内の重要なサーバに対して Arcserve Full System High Availability (HA) を設定および管理

Arcserve UDP は、あるサーバから別の復旧ポイント サーバに復旧ポイントとして保存されるバックアップ データをレプリケートします。バックアップ データから、ソースノードで不具合が発生したときにスタンバイ マシンとして機能できる仮想マシンを作成することもできます。スタンバイ仮想マシンを作成するには、復旧ポイントを VMware ESX または Microsoft Hyper-V 仮想マシン形式に変換します。

Arcserve UDP ソリューションは、Arcserve High Availability との統合を提供します。Arcserve High Availability でシナリオを作成した後、これらのシナリオを管理およびモニタし、デスティネーション マシンの追加や削除のような操作を実行できます。

詳細については、「[Arcserve UDP ソリューションガイド](#)」を参照してください。

Arcserve Unified Data Protection Agent for Linux

Arcserve Unified Data Protection Agent for Linux は、Linux オペレーティングシステム用に設計されたディスクベースのバックアップ製品です。重要なビジネス情報を保護および回復するための迅速でシンプル、信頼性の高い方法を提供します。

Arcserve Unified Data Protection Agent for Linux は、ノードの変更をブロックレベルで追跡し、増分プロセスで変更されたブロックのみをバックアップします。その結果、バックアップを頻繁に実行できるため、各増分バックアップのサイズ(およびバックアップ ウィンドウ) が小さくなり、より多くの最新のバックアップが提供されます。

Arcserve Unified Data Protection Agent for Linux には、単一のバックアップからファイルまたはフォルダをリストアし、ベアメタル復旧 (BMR) を実行する機能もあります。バックアップ情報は、バックアップソースノードで、NFS (Network File System) 共有または CIFS (Common Internet File System) 共有に保存できます。

Arcserve Unified Data Protection Agent for Linux の最新のバージョンは、アプライアンス内の仮想マシンにプリインストールされます。この仮想マシンが Linux バックアップサーバになります。Arcserve Unified Data Protection Agent for Linux は、Arcserve アプライアンスのデフォルトのインストールパスにインストールされます。

コンソールを開くと、Linux バックアップサーバはすでにコンソールに追加されています。Linux バックアップサーバのネイティブホスト名は *Linux-BackupSvr* です。ただし、コンソールでは、Linux バックアップサーバでは、ポート 8018 環境設定を使用してアプライアンスのホスト名を適用します。Linux バックアップサーバは、ポートの方向制御を通じて NAT の背後で動作します。Linux バックアップサーバでは、ポート 8018 を使用して通信を行い、Arcserve アプライアンス内のデータを転送します。

注: バックアッププランの作成および Linux マシンのリストアに関する詳細については、「[Arcserve UDP Agent for Linux ユーザガイド](#)」を参照してください。

Linux バックアップサーバでは、以下のデフォルトのログイン情報が使用されます。

- ユーザ名 - root
- パスワード - Arcserve

注: デフォルトのパスワードは変更することをお勧めします。

Arcserve Backup

Arcserve Backup は、多種多様な環境のビジネスニーズに対応する高性能なデータ保護ソリューションです。本製品は、柔軟なバックアップとリストア、容易な管理、幅広いデバイス互換性、そして信頼性を提供します。また、ストレージ要件に応じてデータ保護戦略をカスタマイズできるため、データストレージの機能を最大限に活用できます。さらに、柔軟なユーザインターフェースにより詳細な設定が可能で、あらゆるユーザがその技術的知識のレベルにかかわらず、さまざまなエージェント機能や各種オプションを展開して保守できます。

Arcserve Backup には分散環境向けの包括的なデータ保護機能があり、ウイルスフリーのバックアップおよびリストア操作を実現します。多種多様なオプションとエージェントにより、企業全体でのデータ保護機能が強化され、さまざまな拡張機能（オンラインホットバックアップや、アプリケーションおよびデータファイルのリストア、拡張デバイスおよびメディアの管理、惨事復旧など）が使用可能になります。

Arcserve アプライアンスに搭載されている Arcserve Backup との統合機能を使用すると、テープへのバックアップを実行できます。InstallASBU.iso ファイルを使用してマウントおよびインストールした後、Arcserve Backup はコンピュータの「C:\Program Files (x86)\Arcserve」の場所にインストールされます。Arcserve アプライアンスにインストールされているコンポーネントを使用して、Arcserve UDP のデスティネーションをテープにバックアップできます。サポートされているオペレーティングシステムの詳細については、「[動作要件](#)」を参照してください。

Arcserve Web サイトから Arcserve Backup のフルインストールパッケージをダウンロードして、他のコンポーネントをインストールできます。詳細については、Arcserve Backup の[ドキュメント](#)を参照してください。

Arcserve Backup サーバでは、以下のデフォルトのログイン情報が使用されます。

- ユーザ名 -- caroot
- パスワード -- Arcserve

Arcserve Continuous Availability

Arcserve Continuous Availability は、非同期リアルタイムレプリケーション、自動化されたスイッチオーバーおよびスイッチバックに基づくソリューションです。Windows サーバ上の仮想環境にコスト効率の高いビジネス継続性を提供します。サポートされているオペレーティングシステムの詳細については、「[動作要件](#)」を参照してください。

Arcserve Continuous Availability は、データをローカルサーバまたはリモートサーバにレプリケートできるため、サーバのクラッシュやサイトに惨事が発生した場合のデータの回復をサポートします。ハイアベイラビリティのライセンスを所有している場合、ユーザをレプリカサーバに手動または自動で切り替えることができます。

注： Arcserve Continuous Availability は、アプライアンスにプリインストールされていません。Arcserve Continuous Availability をインストールして設定する方法の詳細については、「[インストールガイド](#)」を参照してください

安全に関する注意事項

安全のため、Arcserve アプライアンスに対して開梱、接続、設置、電源投入などの操作を行う場合は、すべての手順を事前に確認し、指示に従ってください。安全に関する注意事項に従わないと、人身傷害、機器の破損、または誤動作などが発生する可能性があります。

安全に関する注意事項の詳細については、「[安全に関する注意事項\(付録\)](#)」を参照してください。

同梱されている内容

このセクションでは、以下のアプライアンスシリーズのボックスに同梱されている内容について説明します。

- [10000 シリーズ](#)
- [9000 シリーズ](#)
- [X シリーズ](#)

アプライアンス 10000 シリーズのボックスに同梱されている内容

10048DR-10576DR 付属品ボックスに同梱されている品目は、以下のとおりです。

- クイック スタート ガイド、Arcserve アプライアンス導入シート
- Arcserve QR リーフレット (ガイドへの QR コード付き)
- Arcserve 10K サーバハードウェア インストールガイド 1 冊
- 電源コード (c13 - nema 5-15p) 2 本。ボックスには、米国標準の電源コードに加えて、注文先の国の電源コードが一組追加されます。
- レールキット/ブラケット セット 一組
- 3.5 インチ HDD 用ネジ 1 袋
- 2.5 インチ HDD 用ネジ 1 袋
- ケーブル、Flexboot、CAT6、ネットワーク、3 フィート (約 0.9 m) 、青ケーブル、Flexboot、CAT6、ネットワーク、7 フィート (約 2.1 m) 、黒

アプライアンス 9000 シリーズのボックスに同梱されている内容

Arcserve アプライアンス 9000 シリーズのボックスは、9012、9024、9048 用と 9072DR-9504DR 用の 2 種類あります。下記リストには、両方のボックスの内容を記載します。

9012、9024、9048 付属品ボックスに同梱されている品目は、以下のとおりです。

- ベゼル、1U ボックス、CUS 14G ベゼルアセンブリ、LCD、AR、(380-7406)
- ARCSERVE クイック スタート ガイド、ARCSERVE アプライアンス導入シート
- ARCSERVE DELL R440 ハードウェア取り付けガイド
- ケーブル、FLEXBOOT、CAT6、ネットワーク、3 FT 赤
- ケーブル、FLEXBOOT、CAT6、ネットワーク、3 FT 青
- ケーブル、FLEXBOOT、CAT6、ネットワーク、7 FT 黒
- Dell 安全環境規制ブック
- US 電源コード (2x) a

注：アプライアンスに同梱されている内容をチェックして、足りない項目がないかどうか、および破損がないことを確認します。不足品や破損品がある場合は、すべてのパッケージ資材を保持して [Arcserve サポートにご連絡ください](#)。

ラックレールキットが付属する 9072DR-9504DR ボックスに同梱される品目は、以下のとおりです。

- ベゼル、2U ボックス、CUS 14G ベゼルアセンブリ、LCD、AR、(380-7405)
- ARCSERVE クイック スタート ガイド、ARCSERVE アプライアンス導入シート
- ハードウェア インストールガイド ARCSERVE DELL R740
- ケーブル、FLEXBOOT、CAT6、ネットワーク、3 FT 赤
- ケーブル、FLEXBOOT、CAT6、ネットワーク、3 FT 青
- ケーブル、FLEXBOOT、CAT6、ネットワーク、7 FT 黒
- ケーブルアセンブリ、ミニ SAS、外部、SFF-8644 から SFF-8088 1M
- Dell 安全環境規制ブック
- US 電源コード (2x)

アプライアンス X シリーズのボックスに同梱されている内容

Arcserve アプライアンス X シリーズには、以下の項目が含まれます。

▪ **アプライアンス X シリーズ コンピュート ノード:**

- ◆ MICROSOFT
- ◆ WIN SVR EMB STD 2019 16-CORE

コンピュート ノード アクセサリ ボックス:

- ◆ Windows 4-Core 拡張ライセンス(数量 10)
- ◆ ハードウェア セットアップ ガイド、ARCSERVE R740
- ◆ Arcserve クイック スタート ガイド、UDP アプライアンス導入シート
- ◆ Dell 安全に関する情報
- ◆ 電源コード(2本)、米国または国別仕様(注文した場合)
- ◆ ラック マウント スライド レール キット
- ◆ ケーブル管理アーム
- ◆ オプションのコンポーネント(注文した場合):
 - SFP
 - SAS ケーブル
 - DAC ケーブル

注: 以下は、アレイの前面に取り付けられます。Arcserve ME4084 ペイント ベゼルとバブル バッジ アセンブリ。

▪ **アプライアンス X シリーズ ストレージ ノード**

5U ストレージ システム ボックスには、以下のものが同梱されています。

- ◆ マニュアル
- ◆ 5U ストレージ アプライアンス エンクロージャ
- ◆ 電源 ケーブル 2 本
- ◆ 個別 パッケージ のディスク ドライブ(5U エンクロージャのみ)
- ◆ ファイバ チャネル または iSCSI SFP+ トランシーバ または ケーブル(ホストポートごとに1つ)
- ◆ ホスト ケーブル(コントローラ モジュール ホスト ポートごとに1本)
- ◆ 拡張 ケーブル(拡張 モジュールごとに1本)

- ◆ オプションのキー付きエンクロージャベゼルセット(5Uエンクロージャごとに1つ)
- ◆ 5Uストレージシステムエンクロージャ用の適切なラックマウントキット

ME4084 アクセサリボックス:

- ◆ ハードウェアセットアップガイド、ARCSERVE ME4084
- ◆ ラックマウントスライドレールセット
- ◆ C19からC20、PDU形式、2.5M電源コード(2本)
- ◆ シリアルケーブル
- ◆ 12Gb HD-Mini ~ HD-Mini SAS Cable、2M(4本)
- ◆ ストレージアレイ規制情報ドキュメント
- ◆ ストレージアレイのセットアップドキュメント
- ◆ 安全および環境情報ドキュメント
- ◆ ベゼル取り外しレンチ
- ◆ 未使用のドライブ番号ラベル

注: ハードドライブは、アレイの下の別のボックスに入っています。

注: アプライアンスに同梱されている内容をチェックして、足りない項目がないかどうか、および破損がないことを確認します。不足品や破損品がある場合は、すべてのパッケージ資材を保持して [Arcserve サポートにご連絡ください](#)。

箱に含まれていない項目

以下の項目は、箱に含まれておらず、アプライアンスの設置および設定に必要な場合があります。

- モニタ
- キーボード
- 外部ストレージ デバイス(必要な場合)

利用可能なモデル

Arcserve アプライアンス 9000 シリーズおよび X シリーズは、お客様のさまざまなニーズを満たすように設計された多種多様なモデルで提供されています。

- [モデル 10024BU - 10576DR](#)
- [モデル 9012-9504 DR](#)
- [モデル X シリーズ](#)

モデル 10024BU-10576DR

Arcserve アプライアンス モデル 10024BU - 10576DR

Arcserve アプライアンス 10K シリーズの仕様								
アプライアンス モデル	10048DR	10072DR	10144DR	10192DR	10288DR	10384DR	10576DR	
実効容量 (TB) 1	48	72	144	192	288	384	576	
使用可能な容量	16 TB	24 TB	48 TB	64 TB	96 TB	128 TB	192 TB	
拡張キット使用時の最大使用可能容量	40 TB	40 TB	80 TB	80 TB	160 TB	160 TB	N/A	
フォームファクタ	2U							
ベース RAM (DDR5 5600)	128 GB (4x32 GB)	256 GB (8x32 GB)					384 GB (12x32 GB)	
最大 RAM	512 GB							
SAS 12G HDD エンタープライズグレード 7.2k	6x4 TB	8x4 TB	8x8 TB	10x8 TB	8x16 TB	10x16 TB	14x16 TB	
NVMe M.2	OS および UDP 用に 2x480 GB (RAID 1)							
SSD	ハッシュ用に 2x 3.2 TB (RAID 1)							
CPU	デュアル Intel® Xeon® Silver 4510T 12C 2 G							
RAID コントローラ	Broadcom 3916 (CacheVault 書き込みキャッシュ保護付き)							
HDD RAID	RAID6							

設定							
ドライブ ベイ	14xHDD、2xSSD						
オプションの RAM 拡張 キット	✓	✓	✓	✓	✓	✓	✓
DIMM スロット	16						
NIC	合計 4 ポート。2x 10GbE オンボード。Broadcom BCM57416 を介した 2x 10 GbE Base-T						
利用可能な PCIe スロット	3 (ロープロファイル)						
リモート ハードウェア 管理	IPMI (拡張ライセンス)						
電源	2x 1600W 冗長チタンレベル(96%) ホットスワップ交換						
HDD キット (オプション)	8x4 TB (24 TB) RAM のアップグレードを推奨	6x4 TB (16 TB)	6x8 TB (32 TB)	4x8 TB (16 TB)	6x16 TB (64 TB)	4x16 TB (32 TB) RAM のアップグレードを推奨	X
RAM 拡張 キット (オプション)	128 GB (4x32) の各キットは複数個注文できます。最大 3 キット	128 GB (4x32) の各キットは複数個注文できます。最大 2 キット。					128 GB (4x32) 最大 1 キット。
Broadcom Aero HBA 9500-8e PCIe Gen4	オプション						
Broadcom BCM57416 デュアルポート 10Gbps Base-T アダプタ	オプション						
Intel X710 Std LP デュアルポート 10G SFP+	オプション						

Broadcom BCM57414 Std LP デュ アルポート 25G SFP28	オプション
QLogic 2692 デュ アルポート 16Gb ファイ バチャネル HBA	オプション
重さ	総重量：62 ポンド(28.12 kg) 正味重量：41.5 ポンド(18.82 kg)
パッケージ 寸法	658 x 274 x 998mm (25.9 インチ x 10.8 インチ x 39.3 インチ)
ラック内寸 法	437 x 89 x 705mm (17.2 インチ x 3.5 インチ x 27.75 インチ)

注：実効容量は、グローバルソース デデュプリケーションを考慮し、使用可能な容量の3 倍に等しくなります。実際のバックアップ容量は、データの種類、バックアップの種類、スケジュール、およびその他の要因によって異なる場合があります。

モデル 9012 - 9504DR

Arcserve アプライアンス モデル 9012 - 9504DR

Arcserve アプライアンス 9000 シリーズの仕様											
アプライ アンス モデル	901 2	902 4	904 8	9072D R	9096D R	9144D R	9192D R	9240D R	9288D R	9360D R	9504DR
使用可 能な容 量	4 TB	8 TB	16 TB	24 TB	32 TB	48 TB	64 TB	80 TB	96 TB	120 TB	168 TB
ソース バック アップ	12 TB	24 TB	48 TB	72 TB	96 TB	144 TB	192 TB	240 TB	288 TB	360 TB	504 TB
システム RAM	6 x 8 GB (48 GB)			12 x 16 GB (192 GB)							12 x 32 GB (384 GB)
最大 RAM / DIMM	176 GB / 10 DIMMS			576 GB / 24 DIMMS							768 GB / 24 DIMMS

SSD ドライブ	480 GB SSD	2 x 1.9 TB SSD (RAID1)									
プロセッサ	Intel Xeon Silver 4108, 8 - CORE, 1.8 GHz	Intel Xeon Silver 4114, 10 - CORE, 2.2 GHz									
プロセッサ数	1	2									
RAID カード	PERC H730P 低プロファイル、アダプタ、2 GB NV キャッシュ	PERC H730P、ミニカード、2 GB NV キャッシュ									
RAID 構成	RAID-5	RAID-6									
ドライブベイ	4	16									
拡張キット	N/A	11	10	8	6	4	6	4	N/A		
RAID 2	N/A	6									
ドライブ	3 x 2 TB 3 x 4 TB 3 x 8 TB	5 x 8 TB	6 x 8 TB	8 x 8 TB	10 x 8 TB	12 x 8 TB	10 x 12 TB	12 x 12 TB	16 x 12 TB		
基本 PCIe カード	オンボード Broadcom 5720 デュアルポート 1 Gb LOM	Broadcom 5720 QP 1 Gb ネットワークデータカード SAS 12Gbps HBA 外部コントローラ							Broadcom 5720 QP 1 Gb SAS 12Gbps HBA 外部デュアルポート 10 G Base-T 銅線		
PCIe カード (ファクトリオプション)	SAS 12Gbps HBA 外部コントローラ Broadcom 5719 クアッドポート 1 G NIC	デュアルポート 10 G 銅線 デュアルポート 10 G SFP + デュアルポート FC 16 G HBA							デュアルポート 10 G SFP + デュアルポート FC 16 G HBA		

	デュアルポート 10 G 銅線 デュアルポート 10 G SFP + デュアルポート FC 16 G HBA		
電源	デュアル、ホットプラグ、冗長電源(1+1)、550 W	デュアル、ホットプラグ、冗長電源(1+1)、750 W	
iDRAC Enterprise	1		

モデルXシリーズ

Arcserve アプライアンス モデルX シリーズ

Arcserve アプライアンス X シリーズの仕様					
アプライアンスモデル	X1000DR	X1500DR	X2000DR	X2500DR	X3000DR
実効容量 (TB) ¹	1,056	1,584	2,112	2,640	3,168
拡張キット使用時の最大実効容量 (TB) ¹	3,168				
注：実効容量は、グローバルソース デデュプリケーションを考慮したもので、HDDの使用可能容量の約3倍で、SSDは含まれません。実際のバックアップ容量は、データの種類、バックアップの種類、スケジュールなどの要因によって異なる場合があります。					
ディスクイメージングおよびディザスタリカバリソフトウェア	Arcserve UDP Premium Edition に含む				
テープ統合ソフトウェア	Arcserve Backup に含む				
Continuous Availability と自動フェールオーバー	Arcserve Continuous Availability のオプション				
コンピュータ ノード					
CPU	Dual Intel Xeon Gold 6258R 2.7G、28C/56T、10.4GT/s、38.5M キャッシュ、ターボ、HT (205W)				
デフォルト RAM	1,024 GB (16 x 64) DDR4-3200 RDIMM				
最大 RAM	2,048 GB				
DIMM スロット	24				

NVMe SSD	2 x 1.6TB (RAID-1) および 6 x 4TB (RAID-5)				
ドライブ ベイ	24x 2.5" Enterprise NVMe SSD				
SAS 12Gbps HBA 外部コントローラ	2x 付属				
Intel X550 Quad Port 10G Base-T アダプタ	同梱				
Broadcom 57414 デュアルポート 25Gb SFP28 アダプタ	オプション				
Intel X710 デュアルポート 10G SFP+ FC アダプタ	オプション				
QLogic 2692 デュアルポート 16Gb ファイバチャネル HBA	オプション				
リモート ハードウェア管理	iDRAC Enterprise に含む				
電源	デュアル、ホットプラグ、冗長電源 (1+1) 、1100W				
放熱	4100 BTU/時間				
重さ	75 ポンド (34 kg)				
フォームファクタ	2U				
ラック内寸法 (ベゼル、前面パネル、電源ハンドルを除く)	26.7" x 17.1" x 3.4" (67.9 cm x 43.4 cm x 8.7cm)				
外形寸法 (ベゼル、前面パネル、電源ハンドルを含む)	29.6 インチ x 19.0 インチ x 3.4 インチ (75.1 cm x 48.2 cm x 8.7cm)				
パッケージ寸法	38 インチ x 26 インチ x 12 インチ (97 cm x 66 cm x 30 cm)				
ストレージ ノード					
16TB SAS 12G ホットプラグ HDD	28	42	56	70	84
最小使用可能容量	352	528	704	880	1056
オプションキットによる線形拡張機能	✓	✓	✓	✓	
RAID レベル	RAID-ADAPT				
RAID コントローラ	デュアル 8-port SAS 12Gb コントローラ				
HDD のホットスペア容量	最大 64 TB				
電源	デュアル、冗長 (1+1) 、2200W				
放熱	7507 BTU				
重さ	141 ポンド (64kg) から 298 ポンド (135kg)				
フォームファクタ	5U				
外形寸法 (ベゼル、前面パネル、電源ハンドルを含む)	38.31 インチ x 19.01 インチ x 8.75 インチ (97.47 cm x 48.30 cm x 22.23 cm)				

む)	
----	--

コントロールおよびインジケータ

Arcserve アプライアンスには、前面および背面のパネルと各ドライブ キャリアにいくつかのコントロールとインジケータ(LED) が備わっています。これらのコントロールおよびインジケータによって、さまざまな機能を制御でき、アプライアンスとコンポーネントのステータスをすばやく参照する機能を提供します。

- [前面パネル 10024BU-10048BU](#)
- [前面パネル 10048DR-10576DR](#)
- [前面パネル 9012-9048](#)
- [前面パネル 9072DR-9504DR](#)
- [前面パネル X シリーズ](#)
- [背面パネル 10024BU-10048BU](#)
- [背面パネル 10048DR-10576DR](#)
- [背面パネル 9012-9048](#)
- [背面パネル 9072DR-9504DR](#)
- [背面パネル X シリーズ](#)
- [上面図 10024BU-10048BU](#)

前面パネル 10048DR-10576DR

Arcserve アプライアンスの前面パネルには、コントロールパネル ボタン、コントロールパネル LED、ドライブ キャリア LED が備わっています。以下の表で、これらのアイテムについて説明します。



Control Panel IPMI password and Arcserve Appliance model number

コントロール/インジケータ	説明
0 ~ 5	SAS 3.5 インチ HDD。詳細については、「 ドライブ キャリア LED 」を参照してください。
6 ~ 11	SAS 3.5 インチ HDD。詳細については、「 ドライブ キャリア LED 」を参照してください。
12 ~ 13	SAS 3.5 インチ HDD。詳細については、「 ドライブ キャリア 」

	LED を参照してください。
14 ~ 15	SAS 2.5 インチ SSD。詳細については、「 ドライブ キャリア LED 」を参照してください。
コントロールパネル	電源ボタン、リセット ボタン、および LED インジケータがあります。詳細については、「 コントロールパネル 」を参照してください。
IPMI パスワードおよび Arcserve アプライアンスのモデル番号	IPMI パスワードおよび Arcserve アプライアンスのモデル番号が記載されています。

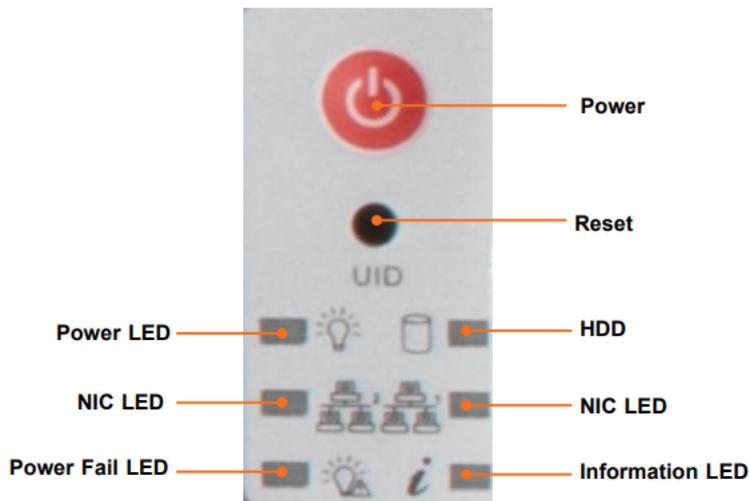
ドライブ キャリアの LED

各ドライブ キャリアには、アクティビティおよびステータス インジケータという2つの LED インジケータがあります。コントローラを使用した RAID 設定の場合、ステータス インジケータの意味は以下の表のとおりです。

	色	点滅パターン	デバイスの動作
アクティビティ LED	青	点灯	設置済みの SAS/NVMe ドライブがアイドル状態
	青	点滅	I/O アクティビティ
	オフ		設置済みの SATA ドライブがアイドル状態
ステータス LED	赤	点灯	RSTe をサポートするドライブの障害
	赤	1 Hz で点滅	RSTe をサポートするドライブの再構築
	赤	1 Hz で2回点滅し1回停止の繰り返し	RSTe をサポートするドライブのホットスペ

			ア
	赤	1 Hz で 2 回点滅し 1 回停止の繰り返し	RSTe をサポートするドライブの電源オン
	赤	4 Hz で点滅	RSTe をサポートするドライブの識別
	緑	点灯	NVMe ドライブを安全に取り外し可能
	黄	1 Hz で点滅	NVMe ドライブは取り外し不可

コントロールパネル



コントロール/インジケータ	説明
電源 ボタン	主電源スイッチは、サーバの主電源をオンまたはオフにしますが、スタンバイ電力は維持します。
リセット ボタン	システムを再起動します。
電源 LED	システムの電源ユニットに電力が供給されていることを示します。この LED は、システムが正常に動作しているときに点灯します。
HDD	点滅は、ストレージドライブのアクティビティを示します。
NIC LED	点滅は、LAN のネットワーク アクティビティを示します。

電源異常 LED	電源モジュールが失敗したことを示します。
情報 LED	オペレータに複数の状態を通知します。詳細については、「 情報 LED 」を参照してください。

情報 LED

以下の表で、情報 LED のステータスについて説明します。

色、ステータス	説明
赤、継続的	過熱状態が発生しました。
赤、1 Hz で点滅	ファン障害。動作していないファンがないか確認してください。
赤、0.25 Hz で点滅	電源障害。稼働中でない電源がないか確認してください。
青、点灯	ラック環境でサーバを見つけるために、UID がローカルでアクティブ化されています。
青、点滅	ラック環境でサーバを見つけるために、BMC を使用して UID がアクティブ化されています。

前面パネル 9012-9048

Arcserve アプライアンスの前面パネルには、コントロールパネルボタン、コントロールパネルLED、ドライブキャリアLEDが備わっています。以下の表で、これらのアイテムについて説明します。



番号	コントロール/インジケータ	アイコン	説明
1	左コントロールパネル	N/A	<p>システム健全性、システム ID、ステータス LED、および iDRAC クイック同期 2 (ワイヤレス) インジケータを搭載しています。</p> <p>注: DRAC クイック同期 2 インジケータは、特定の構成にのみ搭載されています。</p> <ul style="list-style-type: none"> ステータス LED: 障害の発生したハードウェアコンポーネントを識別することがで

			<p>きます。最大 5 つステータス LED およびシステム全体の健全性 LED (シャーシの健全性とシステム ID) バーを備えています。詳細については、リンクを参照してください。</p> <ul style="list-style-type: none"> • クイック同期 2 (ワイヤレス)：クイック同期が有効になっているシステムを示します。クイック同期機能はオプションです。この機能を使用すると、モバイルデバイスでシステムを管理できます。この機能により、ハードウェアやファームウェア インベントリ、および各種システムレベルの診断とエラー情報が集約され、システムのトラブルシューティングで使用することができます。詳細については、リンクを参照してください。
2	ドライブ スロット	N/A	システムでサポートされているドライブをインストールできます。ドライブに関する詳細については、 リンク を参照してください。
3	オプティカルドライブ(オプション)	N/A	オプションで 1 基のスリム SATA DVD-ROM ドライブまたは DVD + RW ドライブ
4	VGA ポート		表示デバイスをシステムに接続することができます。
5	USB ポート(オプション)		USB ポートは、USB 2.0 準拠です。
6	右コントロールパネル	N/A	電源ボタン、USB ポート、iDRAC ダイレクト マイクロポート、および iDRAC ダイレクト ステータス LED を搭載しています。
7	情報タグ	N/A	情報タグはスライド式のラベルパネルで、サービス タグ、NIC、MAC アドレスといったシステム情報が格納されています。iDRAC への安全なデフォルト アクセスを選択すると、情報タグには iDRAC の安全なデフォルト パスワードも格納されます。

前面パネル 9072DR - 9504DR

Arcserve アプライアンスの前面パネルには、コントロールパネル ボタン、コントロールパネル LED、ドライブ キャリア LED を搭載しています。以下の表で、これらのアイテムについて説明します。



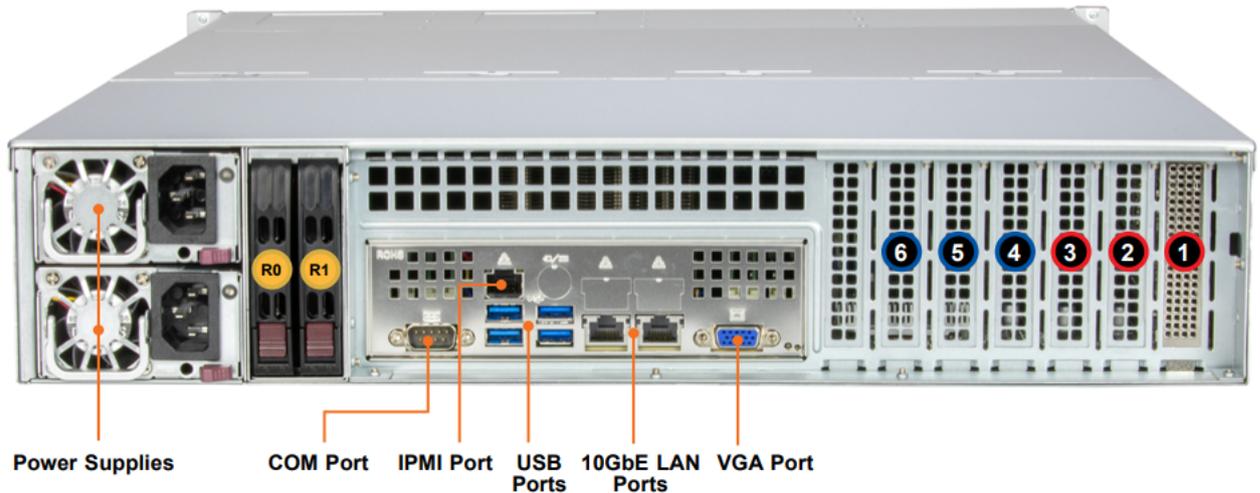
番号	コントロール/インジケータ	アイコン	説明
1	左コントロールパネル	N/A	システム健全性、システム ID、ステータス LED、オプションで iDRAC クイック同期 2 (ワイヤレス) インジケータを搭載しています。
2	ドライブ スロット	N/A	システムでサポートされているドライブをインストールできます。詳細については、 リンク を参照してください。
3	右コントロールパネル	N/A	電源ボタン、VGA ポート、iDRAC ダイレクト マイクロ USB ポート、および 2 つの USB 2.0 ポートを備えています。
4	情報タグ	N/A	情報タグはスライド式のラベルパネルで、サービスタグ、NIC、MAC アドレスといったシステム情報が格納されています。iDRAC への安全なデフォルト アクセスを選択すると、情報タグには iDRAC の安全なデフォルト パスワードも格納されます。

前面パネル X シリーズ

前面パネルの詳細については、「[X シリーズ アプライアンスの設置 - コンピュータ ノード](#)」および「[X シリーズ アプライアンスの設置 - ストレージ ノード](#)」を参照してください。

背面パネル 10048DR-10576DR

Arcserve アプライアンスの背面パネルには、拡張カード スロット、電源モジュール、ユニット 識別 LED、LAN ポート、USB ポート、VGA ポート、BMC LAN ポート、および COM ポートがあります。以下の表で、これらのアイテムについて説明します。



コントロール/インジケータ	説明
R0、R1	使用不可
1	ハードウェア RAID コントローラ
2	ハードウェア RAID コントローラのキャッシュポート
3	10 GbE Base-T
4	オプションカード用拡張スロット (ロープロファイル)
5	オプションカード用拡張スロット (ロープロファイル)
6	オプションカード用拡張スロット (ロープロファイル)
電源	デュアル冗長 1600 W 電源。詳細については、「 電源インジケータ 」を参照してください。
COM ポート	シリアルポート (RS-232)
IPMI ポート	専用 IPMI LAN ポート
USB ポート	4 つの USB 3.0 ポート
VGA ポート	1 つのビデオポート
LAN ポート	2 つの RJ45 10 GbE LAN ポート

注: シリーズ番号は、サーバの背面パネルの VGA ポートの近くと、IPMI インターフェイスで確認できます。

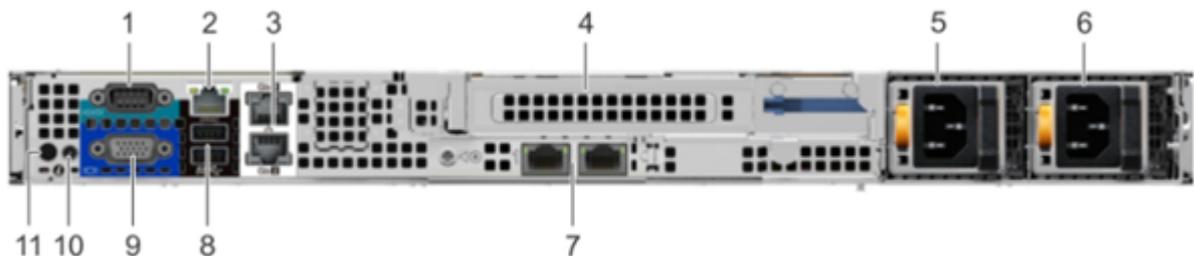
電源インジケータ

電源の状態	緑色の LED	黄色の
-------	---------	-----

		LED
AC 電源なし	消灯	消灯
電源の致命的なイベントによりシャットダウン/障害/OCP/OVP/ファン障害/OTP/UVP が発生	消灯	黄色の LED
高温、過電圧、低電圧などの電源警告イベント (電源は引き続き動作)	消灯	1 Hz で黄色に点滅
AC 電源があり、12 VSB のみがオン(PS オフ)	1 Hz で緑色に点滅	消灯
出力オン、正常	緑	消灯
AC コードが抜かれて冗長モード	消灯	黄

背面パネル 9012-9048

Arcserve アプライアンスの背面パネルには、アプライアンス用の電源、ケーブル接続、ポートが備わっています。以下の表で、これらのアイテムについて説明します。

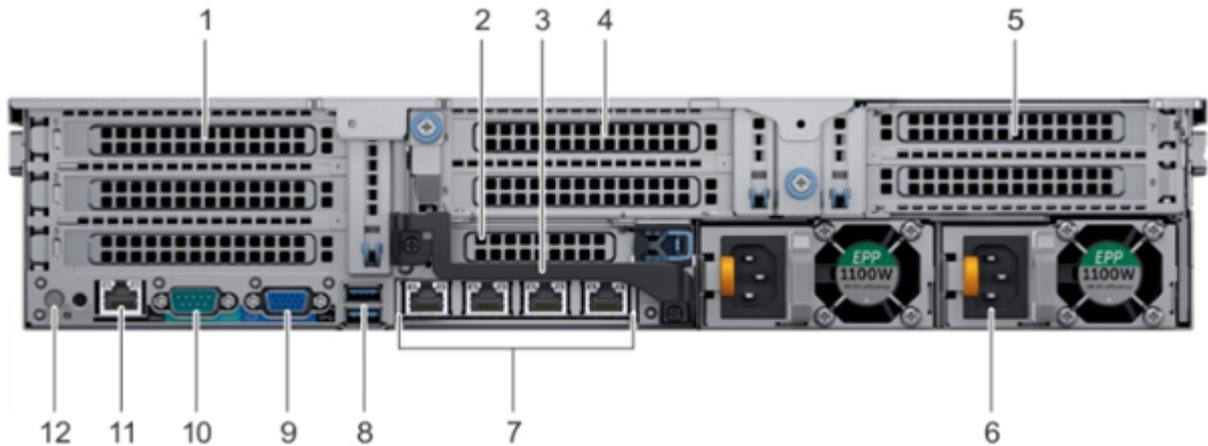


番号	コントロール/インジケータ	アイコン	説明
1	シリアルポート	IOIOI	システムにシリアルデバイスを接続する際にシリアルポートを使用します。詳細については、 リンク を参照してください。
2	iDRAC9 専用ネットワークポート		個別の管理ネットワーク上で埋め込み型 iDRAC に安全にアクセスするには、iDRAC9 専用のネットワークポートを使用します。詳細については、 リンク を参照してください。

3	Ethernet ポート (2)		Ethernet ポートを使用して、システムをローカルエリア ネットワーク(LAN) に接続します。詳細については、 リンク を参照してください。
4	フルハイット ライザー スロット		このカード スロットを使用して、フルハイット PCIe 拡張カードをフルハイット ライザーに取り付けます。
5	電源装置 (PSU)		PSU 設定の詳細については、 リンク を参照してください。
6	電源装置 (PSU)		PSU 設定の詳細については、 リンク を参照してください。
7	LOM ライザー ポート (2)		PSU 設定の詳細については、 リンク を参照してください。
8	USB 3.0 ポート (2)		USB 3.0 ポートを使用して、システムに USB デバイスを接続します。USB 3.0 ポートは、4 ピン USB 3.0 に準拠しています。
9	VGA ポート		VGA ポートを使用して、システムにディスプレイを接続します。
10	CMA 電源ポート		ケーブル管理 Arm (CMA) 電源ポートを使用して、CMA に接続することができます。
11	システム識別ボタン		<p>以下の場合に、システム ID ボタンを押します。</p> <ul style="list-style-type: none"> ラック内の特定のシステムを確認する場合 システム ID を有効または無効にする場合 <p>iDRAC をリセットするには、ボタンを 15 秒押し続けます。</p> <p>注：</p> <ul style="list-style-type: none"> システム ID を使用して iDRAC をリセットする場合、iDRAC のセットアップでシステム ID ボタンが有効になっていることを確認します。 実行後の処理中にシステムの応答が停止した場合、システム ID ボタンを押し続け(5 秒以上)、BIOS プログレスモードに切り替えます。

背面パネル 9072DR-9504DR

Arcserve アプライアンスの背面パネルには、アプライアンス用の電源、ケーブル接続、ポートが備わっています。以下の表で、これらのアイテムについて説明します。



番号	コントロール/インジケータ	アイコン	説明
1	フルハイト PCIe 拡張カード スロット (3)	N/A	PCIe 拡張カード スロット (ライザー 1) を使用して、最大 3 つのフルハイト PCIe 拡張カードをシステムに取り付けることができます。詳細については、 リンク を参照してください。
2	ハーフレングス PCIe 拡張カード スロット	N/A	PCIe 拡張カード スロット (ライザー 2) を使用して、1 つのハーフハイト PCIe 拡張カードをシステムに取り付けることができます。詳細については、 リンク を参照してください。
3	背面ハンドル	N/A	背面ハンドルを取り外すと、PCIe カードの外部ケーブルを PCIe 拡張カード スロット 6 に取り付けることができます。
4	フルハイト PCIe 拡張カード スロット (2)	N/A	PCIe 拡張カード スロット (ライザー 2) を使用して、最大 2 つのフルハイト PCIe 拡張カードをシステムに取り付けることができます。詳細については、 リンク を参照してください。
5	フルレングス PCIe 拡張カード スロット (2)	N/A	PCIe 拡張カード スロット (ライザー 3) を使用して、最大 2 つのフルハイト PCIe 拡張カードをシステムに取り付けることができます。詳細については、 リンク を参照してください。
6	電源装置 (2)	N/A	詳細については、 リンク を参照してください。
7	NIC ポート		ネットワークドーターカード (NDC) に統合されている NIC ポートを使用すると、ネットワークに接続することができます。サポートさ

			れている構成の詳細については、 リンク を参照してください。
8	USB ポート (2)		USB ポートは、9 ピンおよび 3.0 に準拠しています。USB ポートには、USB デバイスを接続できます。
9	VGA ポート		表示 デバイスをシステムに接続できます。詳細については、 リンク を参照してください。
10	シリアルポート		シリアル デバイスをシステムに接続できます。詳細については、 リンク を参照してください。
11	iDRAC9 専用ポート		iDRAC にリモート アクセスすることができます。詳細については、 リンク を参照してください。
12	システム識別ボタン		システム識別 (ID) ボタンは、システムの前面と背面にあります。ラック内のシステムを識別するには、システム ID ボタンを有効にしてから、このボタンを押します。また、iDRAC をリセットして、BIOS モードで手順に従う場合にも、システム ID ボタンを使用します。

背面パネル X シリーズ

背面パネルの詳細については、「[X シリーズ アプライアンスの設置 - コンピュータ ノード](#)」および「[X シリーズ アプライアンスの設置 - ストレージ ノード](#)」を参照してください。

アプライアンスが使用するポート

以下のトピックでは、Arcserve UDP、Arcserve Backup、Linux 用アプライアンスのサポートで使用されるポートに関する情報を紹介します。

- [Arcserve UDP](#)
- [Arcserve Backup](#)
- [Linux 用アプライアンスのサポート](#)

Arcserve UDP

このセクションには、以下のトピックが含まれます。

- [Microsoft Windows にインストールされるコンポーネント](#)
- [Linux にインストールされているコンポーネント](#)
- [リモートで UDP Linux により保護されている実稼働ノード](#)

Microsoft Windows にインストールされるコンポーネント

LAN 環境を使用している場合、バックアップなどのジョブを行うには以下のポートが必要です。

ポート #	ポートの種類	起動元	受信待機プロセス	説明
1433	TCP	リモート Java	sqlsrvr.exe	Arcserve UDP コンソールと Microsoft SQL Server データベースが異なるコンピュータに存在する場合、その間のデフォルトの通信ポートを指定します。 注：デフォルト通信ポートは、SQL Server をインストールするときに変更できます。
4090	TCP	Arcserve UDP エージェント	HATransServer.exe	プロキシモードで仮想スタンプイタスクのデータを転送します。
5000-5060	TCP	Arcserve UDP サーバ	GDDServer.exe	Arcserve UDP RPS グローバルデ

				<p>デュプリケーション データストア サービス (GDD) 用に予約されています。1 つの Arcserve UDP GDD データストアは、5000 以降の3つの空きポートを使用します。GDD データストアに対するバックアップが有効化されている場合、またはリストアタスクを使用している場合にはこれが必要です。</p>
6052	TCP	Arcserve Backup GDB	CA.ARCserve.CommunicationFoundation.WindowsService.exe	<p>Arcserve UDP コンソールと Arcserve Backup グローバルダッシュボードプライマリサーバでデータを同期するための通信。</p>
6054	TCP	Arcserve Backup	CA.ARCserve.CommunicationFoundation.WindowsService.exe	<p>Arcserve UDP コンソールと Arcserve Backup プラ</p>

				イマリサーバでデータを同期するための通信。
8006				Arcserve UDP コンソールによって使用される Tomcat をシャットダウンします。
8014	TCP	Arcserve UDP コンソール	Tomcat7.exe	<p>リモート管理コンソールと Arcserve UDP サーバの間のデフォルトの HTTP/HTTPS 通信ポートを指定します。</p> <p>リモート管理コンソールと Arcserve UDP エージェントの間のデフォルトの HTTP/HTTPS 通信ポートを指定します。</p> <p>注：デフォルトの通信ポートは、Arcserve UDP コンポーネントをインストールするときに変更</p>

				できます。
8014	TCP	Arcserve- e UDP サーバ	httpd.exe	<p>Arcserve UDP サーバ と Arcserve UDP コン ソールの間 のデフォル トの HTTP/HTTP- S 通信ポー トを指定し ます。</p> <p>*デフォル トの共有ポ ートであり、 Arcserve UDP サーバ をレプリケー ション デス ティネーショ ンとして使 用する場 合に開く必 要のある唯 一のポート を指定しま す。ポート 5000 ~ 5060 は、グ ローバルデ デュプリケー ションが有 効化されて いるときに データスト アによって 使用される ため開かな いください。</p> <p>注：デフォ ルトの通信 ポートは、 Arcserve UDP コン</p>

				ポーネットをインストールするときに変更できます。
8015	TCP	Arcserve UDP コンソール	Tomcat7.exe	<p>リモート管理コンソールと Arcserve UDP サーバの間のデフォルトの HTTP/HTTPS 通信ポートを指定します。</p> <p>リモート管理コンソールと Arcserve UDP エージェントの間のデフォルトの HTTP/HTTPS 通信ポートを指定します。</p> <p>注：デフォルトの通信ポートは、Arcserve UDP ポーネットをインストールするときに変更できます。</p>
8016	TCP	Arcserve UDP サーバ	Tomcat7.exe	同じサーバ上の Arcserve UDP RPS ポート共有サービスと通信する

				<p>Arcserve UDP サーバ Web サービス用に予約済みです。</p> <p>注：ポートはカスタマイズできません。ファイアウォール設定では無視できません。</p>
18005			<p>CA.ARCserve.CommunicationFoundation. WindowsService.exe</p>	<p>Arcserve UDP サーバ またはエージェントによって使用される Tomcat をシャットダウンします。</p>

Linux にインストールされているコンポーネント

LAN 環境を使用している場合、バックアップなどのジョブを行うには以下のポートが必要です。

ポート #	ポートの種類	起動元	受信待機プロセス	説明
22	TCP	SSH サービス		Arcserve UDP Linux サードパーティ依存性。SSH サービスのデフォルトを指定しますが、このポートは変更できます。このポートは受信および送信通信の両方に必要です。
67	UDP	Arcserve UDP Linux	bootpd	PXE ブート サーバで使用されます。PXE ブート機能の使用を必要としている場合のみ必須です。このポートは受信通信に必要です。 注：ポート番号はカスタマイズできません。
69	UDP	Arcserve UDP Linux	tffpd	PXE ブート サーバで使用されます。PXE ブート機能の使用を必要としている場合のみ必須です。このポートは受信通信に必要です。 注：ポート番号はカスタマイズできません。
8014	TCP	Arcserve UDP Linux	Java	リモート コンソールと Linux 用 Arcserve UDP エージェントの間のデフォルトの HTTP/HTTPS 通信ポートを指定します。このポートは受信および送信通信の両方に必要です。
18005	TCP	Arcserve UDP Linux	Java	Tomcat で使用され、ファイアウォールを不許可に設定できます。

リモートで UDP Linux により保護されているノード

LAN 環境を使用している場合、バックアップなどのジョブを行うには以下のポートが必要です。

ポート #	ポートの種類	起動元	受信待機プロセス	説明
22		SSH サービス		Arcserve UDP Linux サードパーティ依存性。SSH サービスのデフォルトを指定しますが、このポートは変更できます。このポートは受信および送信通信の両方に必要です。

* ポート共有はレプリケーションジョブのためにサポートされています。異なるポート上のデータはすべてポート 8014 (Arcserve UDP サーバ用のデフォルトポート。インストール時に変更可能) に転送できます。WAN 上にある 2 つの復旧サーバポイント間でレプリケーションジョブを実行する時には、ポート 8014 のみが開いている必要があります。

同様に、リモートレプリケーションの場合、リモート管理者はポート 8014 (データレプリケーション用) とポート 8015 (Arcserve UDP コンソール用のデフォルトポート。インストール時に変更可能) を開くか転送して、割り当てられたレプリケーションプランをローカル復旧ポイントサーバが取得できるようにする必要があります。

Arcserve Backup

LAN 環境を使用している場合、バックアップなどのジョブを行うには以下のポートが必要です。

ポート #	ポートの種類	起動元	受信待機プロセス	説明
135	TCP			Microsoft ポート マッパー
445	TCP		名前付きパイプ上の MSRPC	
6050	TCP/UDP	CASUniversalAgent	Univagent.exe	Arcserve Universal Agent
6502	TCP	Arcserve Communication Foundation	CA.ARCserve.CommunicationFoundation.WindowsService.exe	Arcserve Communication Foundation
6502	TCP	CASapeEngine	Tapeng.exe	Arcserve Tape Engine
6503	TCP	CASJobEngine	Jobengine.exe	Arcserve Job Engine
6504	TCP	CASDBEngine	DBEng.exe	Arcserve Database Engine
7854	TCP	CASportmapper	Catirpc.exe	Arcserve PortMapper
41523	TCP	CASDiscovery	casdscsvc.exe	Arcserve Discovery Service
41524	UDP	CASDiscovery	casdscsvc.exe	Arcserve Discovery Service
9000-9500	TCP		動的ポートを使用する他の Arcserve MS RPC サービス用	

Linux 用アプライアンスのサポート

LAN 環境を使用している場合、バックアップなどのジョブを行うには以下のポートが必要です。

ポート #	ポートの種類	起動元	受信機プロセス	説明
8017	TCP			NAT ポート リダイレクション。他の Linux ノードを Amazon S3 にバックアップするため、アプライアンス上の 8017 を Linux バックアップ サーバにリダイレクトします。
8018	TCP			NAT ポート リダイレクション。アプライアンス上の 8018 を Linux バックアップ サーバエージェントのポート 8014 にリダイレクトします。
8019	TCP			NAT ポート リダイレクション。アプライアンス上の 8019 を Linux バックアップ サーバの SSH ポート 22 にリダイレクトします。
8021	TCP			NAT ポート リダイレクション。8021 ポートを使用して他の Linux ノードをバックアップするため、アプライアンス上の 8021 を Linux バックアップ サーバにリダイレクトします。
8036	TCP			NAT ポート リダイレクション。アプライアンス上の 8036 を Linux バックアップ サーバのポート 8036 にリダイレクトします。
50000	TCP			NAT ポート リダイレクション。50000 ポートを使用して他の Linux ノードをクラウドにバックアップするため、アプライアンス上の 50000 を Linux バックアップ サーバにリダイレクトします。
50001	TCP			NAT ポート リダイレクション。50001 ポートを使用して他の Linux ノードをクラウドにバックアップするため、アプライアンス上の 50001 を Linux バックアップ サーバにリダイレクトします。
50002	TCP			NAT ポート リダイレクション。50002 ポートを使用して他の Linux ノードをクラウドにバックアップするため、アプライアンス上の 50002 を Linux バックアップ サーバにリダイレクトします。
50003	TCP			NAT ポート リダイレクション。50003 ポートを使用して他の Linux ノードをクラウドにバックアップするため、アプライアンス上の 50003 を Linux バックアップ サーバにリダイレクトします。
50004	TCP			NAT ポート リダイレクション。50004 ポートを使用して他の Linux ノードをクラウドにバックアップするため、アプライアンス上の 50004 を Linux バックアップ サーバにリダイレクトしま

				す。
--	--	--	--	----

第3章: アプライアンス上の Arcserve UDP のアップグレード

このセクションには、以下のトピックが含まれます。

Arcserve ソフトウェアのアップグレード後にライセンスを適用する方法	49
Arcserve アプライアンス でのアップグレード シーケンス	50
UDP コンソール、RPS、エージェントのアップグレード シーケンス	56

Arcserve ソフトウェアのアップグレード後にライセンスを適用する方法

Arcserve UDP を 10.0 にアップグレードした後、または Arcserve Backup を 19.0 にアップグレードした後は、Arcserve アプライアンス上の元のライセンスキーは機能しません。Arcserve UDP 10.0 および Arcserve Backup 19.0 用の新しいライセンスキーを取得するには、営業担当者までお問い合わせください。

Arcserve UDP にライセンスキーを追加する方法の詳細については、「[Arcserve 製品ライセンスオンラインヘルプ](#)」を参照してください

Arcserve アプライアンスでのアップグレード シーケンス

Arcserve アプライアンス v9.1 から Arcserve UDP 10.0 へのアップグレードでは、以下のいずれかのシーケンスを伴う場合があります。

- Arcserve UDP のアップグレード
 - ◆ [Arcserve アプライアンスを Arcserve コンソールおよび RPS として使用する場合のアップグレード](#)
 - ◆ [Arcserve アプライアンスを Arcserve UDP RPS として使用する場合のアップグレード](#)
 - ◆ [複数の Arcserve アプライアンスが環境で使用されている場合のアップグレード手順](#)
- [Arcserve アプライアンスでの Arcserve UDP Linux エージェントのアップグレード](#)
- [Arcserve アプライアンス上の Arcserve Backup のアップグレード](#)
- [UDP コンソール、RPS、エージェントのアップグレード シーケンス](#)

Arcserve アプライアンス を Arcserve UDP コンソールおよび RPS として使用した場合のアップグレード

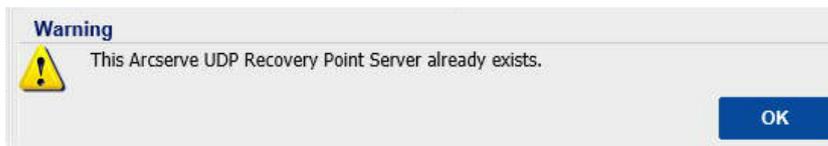
Arcserve アプライアンス をアップグレードした後、「[アップグレード シーケンス](#)」に説明されている手順に従って環境をアップグレードします。

Arcserve アプライアンス を Arcserve UDP RPS として使 用した場合のアップグレード

実稼働環境全体をアップグレードします。詳細については、「[アップグレード シーケンス](#)」を参照してください。

複数の Arcserve アプライアンス が環境で使用されている場合のアップグレード手順

- 実稼働環境全体をアップグレードします。詳細については、「[アップグレード シーケンス](#)」を参照してください。
- アップグレード後、Arcserve UDP コンソールからアプライアンスを RPS として追加するときに以下のような警告が表示される場合は、「[トラブルシューティング](#)」の「[別のアプライアンスから Arcserve アプライアンスをバックアップすると重複ノードが報告される](#)」トピックを参照してください。



Arcserve アプライアンス 上の Arcserve UDP Linux エージェントのアップグレード

以下の手順に従います。

1. Linux バックアップ サーバ環境を管理する Arcserve UDP コンソールをアップグレードします。
2. Arcserve アプライアンス 上の Linux バックアップ サーバをアップグレードします。

詳細については、「[Arcserve Unified Data Protection Agent: for Linux オンラインヘルプ](#)」を参照してください。

Arcserve アプライアンスに搭載された Arcserve Backup のアップグレード

Arcserve アプライアンスでアップグレードを実行するには、「[Arcserve Backup 実装ガイド](#)」を参照してください。

UDP コンソール、RPS、エージェントのアップグレード シーケンス

後方互換性サポート ポリシーに基づいて、以下の順序でアップグレードを計画し、アップグレードが円滑に行われるようにします。

1. Arcserve UDP コンソールをアップグレードします。
2. Arcserve UDP RPS (DR サイト) をアップグレードします。
3. Arcserve UDP RPS (データ センター) をアップグレードします。
4. Arcserve UDP エージェントレス プロキシ、データ センター内の一部エージェントをアップグレードします。
5. Arcserve UDP RPS (リモート サイト) をアップグレードします。
6. Arcserve UDP エージェントレス プロキシ、リモート サイトの一部エージェントをアップグレードします。

注: リモート サイトごとに、手順 5 と 6 を繰り返します。

7. Arcserve UDP 仮想スタンバイ モニタをアップグレードします。

注: レプリケーションの後方互換性サポート ポリシーに従って、常にソース RPS の前にターゲット RPS をアップグレードしてください。

第4章: Arcserve アプライアンス の設定

このセクションには、以下のトピックが含まれます。

Arcserve アプライアンス 向けのネットワーク設定を構成する方法	58
Arcserve アプライアンス を設定する方法	62
Arcserve アプライアンス をゲートウェイとして設定する方法	72

Arcserve アプライアンス 向けのネットワーク設定を構成する方法

Arcserve アプライアンスを管理するには、まずアプライアンスをネットワーク内に含めます。そのためには、ホスト名をアプライアンスに割り当て、ネットワークポートを設定する必要があります。

以下の手順に従います。

1. アプライアンスの電源をオンにした後、Microsoft ライセンス条項に対する設定画面が表示されます。条件を確認して、同意します。

UDP の [エンド ユーザ使用許諾契約] ダイアログ ボックスが表示されます。

2. 使用許諾契約の内容を確認して同意し、[次へ] をクリックします。

[Arcserve アプライアンス 環境設定 ツールへようこそ] 画面が表示されます。

3. 以下の詳細を入力します。

ホスト名

アプライアンスのホスト名を入力します。名前を割り当てると、ネットワーク上でアプライアンスを識別するのに役立ちます。

パスワード

管理者パスワードを指定します。

この Arcserve アプライアンス をドメインに追加します。

アプライアンスをネットワーク内のドメイン メンバにするには、チェック ボックスをオンにします。このオプションを選択すると表示される [ドメイン]、[ユーザ名]、および [パスワード] フィールドに値を指定します。

Arcserve® へようこそ。アプライアンス構成ツール

このツールを使用すると、Arcserve アプライアンスを LAN に接続し、Web ベースのコンソール UI で詳細な設定を実行できます。

アプライアンスにホスト名を割り当てます。これはローカル ネットワーク上のアプライアンスを識別するのに使用されます。必要に応じて、アプライアンスをドメインに追加できます。

❗ 新しいホスト名を有効にするには、再起動する必要があります。アプライアンスを再起動する前に、設定画面で他の設定を設定できます。

ホスト名

パスワード

この Arcserve アプライアンスをドメインに追加します。

保存

注: 新しいホスト名を適用するには、アプライアンスを再起動する必要があります。アプライアンスを今すぐ再起動するか、またはネットワーク設定後に再起動するかを選択できます。アプライアンスを再起動すると、他の任意のマシンから URL - `https://<hostname>:8015` を使用して、アプライアンスにアクセスすることができます。

4. [保存] をクリックします。

以下のダイアログボックスが表示されます。デフォルトでは、Arcserve UDP はネットワーク内のすべてのネットワーク接続を検出します。一部の接続が割り当てられていない場合は、手動で編集し、接続の詳細を指定します。

The screenshot shows the 'Arcserve アプライアンス構成' (Arcserve Appliance Configuration) interface. At the top, there is a warning message: 'ホスト名とドメイン設定を有効にするには、Arcserve アプライアンスを再起動する必要があります。' (To enable host name and domain settings, you must restart the Arcserve appliance.) Below this is a 'アプライアンスの再起動' (Restart Appliance) button. The configuration fields are: 'ホスト名/ドメイン' (Host Name/Domain) set to '(未割り当て)' (Not assigned) with an '編集' (Edit) button; 'UDP コンソール URL' (UDP Console URL) set to 'https://[redacted]:8015'; and '日付と時刻' (Date and Time) set to '2025/01/17 13:31:49' with an '編集' (Edit) button. The 'ネットワーク接続' (Network Connections) section contains a table with the following data:

接続名	IP アドレス	説明	
イーサネット 1 未接続	割り当てなし DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller	編集
イーサネット 2 未接続	割り当てなし DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller #2	編集
イーサネット 3 接続済み	10.147.16.184 DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller #3	編集
イーサネット 4 接続済み	10.147.16.191 DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller #4	編集
イーサネット 5 接続済み	169.254.3.1 DHCP を介した自動	Remote NDIS based Internet Sharing Device	編集

5. ネットワーク接続を編集するには、**ネットワーク接続**ボックスで **編集** をクリックします。

ネットワーク接続ダイアログボックスが表示されます。

ステータス 接続済み

説明 Intel(R) Ethernet 10G 2P X550-t Adapter

接続 DHCPを使用して IP アドレスを自動的に取得します。

IP アドレス 10 . 57 . 25 . 17

サブネット マスク 255 . 255 . 255 . 0

デフォルト ゲートウェイ 10 . 57 . 25 . 1

DNS サーバ アドレスを自動的に取得します。

優先 DNS サーバ 10 . 57 . 1 . 11

代替 DNS サーバ 10 . 64 . 1 . 11

保存 キャンセル

6. IP アドレス、サブネット マスク、デフォルト ゲートウェイの値を必要に応じて変更し、**保存** をクリックします。

注: 必要に応じて、ホスト名、ドメイン、日付と時刻を変更することもできます。

重要: コマンド プロンプトで *acrun.bat* などのスクリプトが実行されているかどうかを確認します。再起動を行う前に、このスクリプトが完了するまで必ず待機してください。

7. 変更を適用するには、**アプライアンスの再起動** をクリックしてアプライアンスを再起動します。

アプライアンスが新しいホスト名で再起動されます。再起動すると、**ログイン**画面が表示されます。

8. ユーザ名とパスワードを入力して、**Enter** キーを押します。

Arcserve アプライアンス 環境設定画面が表示されます。

9. アプライアンスの環境設定画面が再度開いたら、**ウィザードの起動** をクリックします。

Arcserve アプライアンス

arcserve® アプライアンス構成

[? アプライアンスについて](#)

i [ウィザードの起動] をクリックして、Arcserve UDP プラン環境設定ウィザードを使用してアプライアンスの環境設定を続行します。

[ウィザードの起動](#)

ホスト名/
ドメイン [REDACTED]
(未割り当て)

UDP コンソール URL [https://\[REDACTED\]:8015](https://[REDACTED]:8015)

日付と時刻 2025/01/17 13:46:46 [編集](#)

ネットワーク接続

接続名	IP アドレス	説明	
イーサネット ✖ 未接続	割り当てなし DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller	編集
イーサネット 2 ✖ 未接続	割り当てなし DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller #2	編集
イーサネット 3 ✔ 接続済み	10.147.16.184 DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller #3	編集
イーサネット 4 ✔ 接続済み	10.147.16.191 DHCP を介した自動	Supermicro 10GBASE-T Ethernet Controller #4	編集
イーサネット 5 ✔ 接続済み	169.254.3.1 DHCP を介した自動	Remote NDIS based Internet Sharing Device	編集

Arcserve アプライアンスを設定する方法

アプライアンスが新しいホスト名で再起動されると、Unified Data Protection ウィザードが表示されます。ウィザードを使用して、バックアップをスケジュールするための基本プランを作成できます。このプランでは、保護するノードを定義し、バックアップを実行するタイミングをスケジュールできます。バックアップ先は、アプライアンスサーバです。

注：アプライアンスがドメインで設定されている場合、ドメイン ユーザはアプライアンス ウィザードを設定できないため、管理者ログインを使用してアプライアンス ウィザードの設定を完了します。

Arcserve アプライアンス 設定 ウィザードのすべての手順はオプションです。[キャンセル] をクリックしてスキップし、直接 UDP コンソールを開いてプランを作成することもできます。

以下の手順に従います。

1. Arcserve UDP コンソールにログインします。

Unified Data Protection ウィザードが最初に関き、[Arcserve アプライアンス 管理] ダイアログボックスが表示されます。UDP コンソールは、スタンドアロンのインスタンスとして管理できます。または別の UDP コンソールからリモートで管理できます。リモート コンソール管理機能は、複数の UDP コンソールを管理している場合に便利です。

2. [Arcserve Appliance Management (Arcserve アプライアンス管理)] ダイアログボックスで、アプライアンスをローカルで管理するか(デフォルト)、別の UDP コンソールから管理するかを選択します。アプライアンスが別の UDP コンソールから管理されている場合、UDP コンソールの URL、ユーザ名、パスワードを指定します。



3. **次へ]**をクリックします。

データストアのダイアログボックスが表示されます。

データストアは、アプライアンス上の物理ストレージ領域で、バックアップ先として使用されます。

デフォルトでは、Arcserve UDP は <hostname>_data_store という名前でデータストアを作成します。このデータストアは、デデュプリケーションおよび暗号化に対応しています。

注:

- デフォルトのデデュプリケーションブロックサイズは 16 KB です。ただし、要件に基づいてデデュプリケーションブロックサイズを設定できます。

デデュプリケーションブロックサイズを設定するには、以下の手順に従います。

- a. 以下の場所に移動します。

*C:\Program Files\Arcserve\Unified Data
Protection\Management\Configuration*

- b. **ApplianceDefaultSetting.properties** ファイルを開き、*deduplicationBlockSize* を編集します。

- デデュプリケーションブロックサイズを設定した後に、データストアの暗号化パスワードを入力し、**次へ]** ボタンをクリックする必要があります。

デデュプリケーションおよび暗号化の詳細については、「Arcserve UDP ソリューションガイド」の「[データ デデュプリケーション](#)」を参照してください。

注: データストアは暗号化されるため、暗号化パスワードを指定する必要があります。

4. データストアのダイアログボックスで、データストアの暗号化パスワードを入力し、確認のために再度暗号化パスワードを入力して、**次へ]** をクリックします。

arcserve® アプライアンス 構成

データ ストア

データ ストア設定は以下のとおりです。Arcserve UDP コンソール からデータ ストアを追加できます。

usapp21_jpn_data_store

 <p>合計容量 145.52 TB</p>	圧縮	標準
	デデュPLICATION	有効
	暗号化	有効
	パスワード	<input type="password"/>
	パスワードの確認	<input type="password"/>

注: データ ストアは 16KB ブロック サイズで作成されます。
[カスタム ブロック サイズを設定する手順](#)

ステップ 2 / 9

電子メールとアラート]ダイアログ ボックスが表示されます。

アラートを送信するために使用される電子メール サーバと、アラートを受け取る受信者を定義できます。成功したジョブ、失敗したジョブ、またはその両方に基づいてアラートを取得するオプションを選択できます。

5. [email and Alert (電子メールとアラート)]ダイアログ ボックスで、以下の電子メールとアラートの詳細を指定します。

サービス

Google メール、Yahoo メール、Live メール、などの電子メール サービスを指定します。

電子メールサーバ

電子メール サーバのアドレスを指定します。たとえば、Google サーバ電子メールの場合は smtp.gmail.com を指定します。

ポート

電子メール サーバのポート 番号を指定します。

認証が必要

電子メール サーバに認証が必要かどうかを指定します。認証が必要な場合は、認証用のアカウント名とパスワードを指定します。

件名

受信者に送信される電子メールの件名を指定します。

送信者

送信者の電子メールIDを指定します。受信者はこの送信者からメールを受信します。

受信者

アラートを受信する受信者を指定します。複数の受信者がいる場合はセミコロン(;)で区切ることができます。

オプション

通信チャンネルに使用する暗号化方式を指定します。

プロキシサーバを使用して接続する

プロキシサーバ経由で電子メールサーバに接続している場合は、プロキシサーバのユーザ名とポート番号を指定します。また、プロキシサーバで認証が必要な場合は、ユーザ名とパスワードを指定します。

テスト電子メールを送信

テストメールを受信者に送信します。テストメールを送信することによって、詳細を確認できます。



arcserve[®] アプライアンス構成

電子メールとアラート

電子メール通知の設定と受信するアラート通知の種類の設定を行います。

電子メール通知を有効化します。

サービス

電子メールサーバ

ポート

電子メールサービスには認証が必要です。

件名

差出人

受信者

オプション(O)

SSL を使用

STARTTLS の送信

HTML 形式を使用

プロキシサーバを使用して接続する

ステップ 3 / 9

6. [次へ] をクリックします。

[リモート RPS にレプリケート] ダイアログ ボックスが表示されます。

7. アプライアンスで、リモートで管理された復旧ポイント サーバ (RPS) にレプリケートするには、[リモート RPS にレプリケート] ダイアログ ボックスで、以下の詳細を指定します。リモートで管理された RPS の詳細については、「Arcserve UDP ソリューション ガイド」を参照してください。

Arcserve UDP コンソールの URL

リモートの Arcserve UDP コンソールの URL を指定します。

ユーザ名 およびパスワード

リモート コンソールに接続するために使用されるユーザ名とパスワードを指定します。

プロキシ サーバを使用して接続する

リモート コンソールがプロキシ サーバの背後にある場合は、プロキシ サーバの詳細を指定します。

注：アプライアンスで、リモートで管理された RPS にレプリケートしないようにするには、**[このアプライアンスはリモートで管理された RPS にレプリケートしません]** オプションを選択します。

8. **[次へ]** をクリックします。

[プランの作成] ダイアログ ボックスが表示されます。基本プランを作成し、保護するノードおよびバックアップのスケジュールを指定できます。

注：ウィザードを使用して基本プランを作成しない場合は、以下の手順を実行します。

- a. **[プラン作成をスキップ]** をクリックします。
次の手順] ダイアログ ボックスが表示されます。
 - b. **[完了]** をクリックし、UDP コンソールを開いてプランを作成します。
9. **[プランの作成]** ダイアログ ボックスで、以下の詳細を指定してプランを作成します。

プラン名

プランの名前を指定します。プラン名を指定しない場合は、デフォルトの名前として「保護プラン <n>」が割り当てられます。

セッションパスワード

セッションパスワードを指定します。セッションパスワードは、データのリストア時に必要となるため重要です。

ノードをプランにどのように追加しますか?

ノードをプランに追加する方法を指定します。以下の方法から1つを選択します。

- ◆ [ホスト名/IP アドレス](#)

ノードのホスト名またはIPアドレスを使用してノードを手動で追加する方法を示します。必要な数だけノードを追加できます。

- ◆ [Active Directory からのノードのディスカバリ](#)

Active Directory 内にあるノードを追加する方法を示します。Active Directory の詳細情報を使用してノードを検出してから、ノードを追加できます。

- ◆ [vCenter/ESX Server からインポート](#)

ESX または vCenter Server から仮想マシンノードをインポートする方法を示します。このオプションでは、指定されたホスト名またはIPアドレス上で検出されたすべての仮想マシンがリスト表示されます。

- ◆ [Hyper-V Server からインポート](#)

Microsoft Hyper-V サーバから仮想マシンノードをインポートする方法を示します。

方法を選択したら、各ダイアログボックスで詳細を指定します。

The screenshot shows the 'arcserve アプライアンス構成' (Arcserve Appliance Configuration) wizard. The current step is 'プランの作成' (Plan Creation), which is step 5 of 9. The interface includes a 'プラン作成をスキップ' (Skip Plan Creation) button. The main form has the following fields:

- プラン名 (Plan Name): 保護プラン 1 (Protection Plan 1)
- セッションパスワード (Session Password): [Redacted]
- パスワードの確認 (Password Confirmation): [Redacted]
- ノードをプランにどのように追加しますか? (How to add nodes to the plan?): ホスト名/IP アドレス (Windows マシンのみ) (Host Name/IP Address (Windows VMs only))

At the bottom, there are three buttons: '前へ戻る' (Previous), '次へ' (Next), and 'キャンセル' (Cancel). The text 'ステップ 5 / 9' (Step 5 / 9) is visible in the bottom left corner.

10. ノードがプランに追加されたら、**[次へ]**をクリックします。
- {バックアップ スケジュール} ダイアログ ボックスが表示されます。
11. {バックアップ スケジュール} ダイアログ ボックスで、以下のスケジュールを入力します。
- Arcserve UDP エージェントのインストールまたはアップグレードのスケジュール: エージェントがインストールされていないソース ノードに、Arcserve UDP エージェントの最新バージョンがインストールされます。以前のエージェントのインストールは、最新のバージョンにアップグレードされます。
 - 増分バックアップ スケジュール: 初めての場合はフルバックアップが実行され、その後は増分バックアップが実行されます。
- 注: インストール/アップグレードの時刻より前にバックアップの時刻がスケジュールされている場合、バックアップは自動的に次の日にスケジュールされます。たとえば、エージェントのインストールを金曜日の午後 9 時にスケジュールし、バックアップを午後 8 時にスケジュールした場合、バックアップは土曜日の午後 8 時に実行されます。
- プランの作成をキャンセル: 作成したプランをキャンセルするには、**[プランの作成をキャンセル]**をクリックします。

arcserve[®] アプライアンス構成

バックアップ スケジュール

プランのバックアップ スケジュールの基準を入力します。

インストール/アップグレードおよび再起動のタイミング: 全曜日 21 : 00

日次増分バックアップの実行: 22 : 00

スケジュール サマリ (選択内容に基づく)

全曜日の 21:00 に、Arcserve UDP エージェントの最新バージョンがまだインストールされていないすべてのソース ノードに最新バージョンがインストールされます。
Hyper-v または vCenter/ESX からインポートされたノードには、エージェントはインストールされません。

全曜日の 22:00 に、最初のフル バックアップが実行されます。
インストール/アップグレードが完了した後は、毎日 22:00 に増分バックアップが実行されます。

プランの作成のキャンセル

ステップ 7 / 9

前に戻る 次へ キャンセル

12. **[次へ]**をクリックします。
- {プランの確認} ダイアログ ボックスが開きます。

13. [プランの確認]ダイアログボックスで、プランの詳細を確認します。必要に応じて、[ノードの編集]または[スケジュールの編集]をクリックしてノードまたはスケジュールを編集するか、プランを追加または削除できます。

ノードの編集

保護するソースノードを変更します。

スケジュールの編集

バックアップスケジュールを変更します。

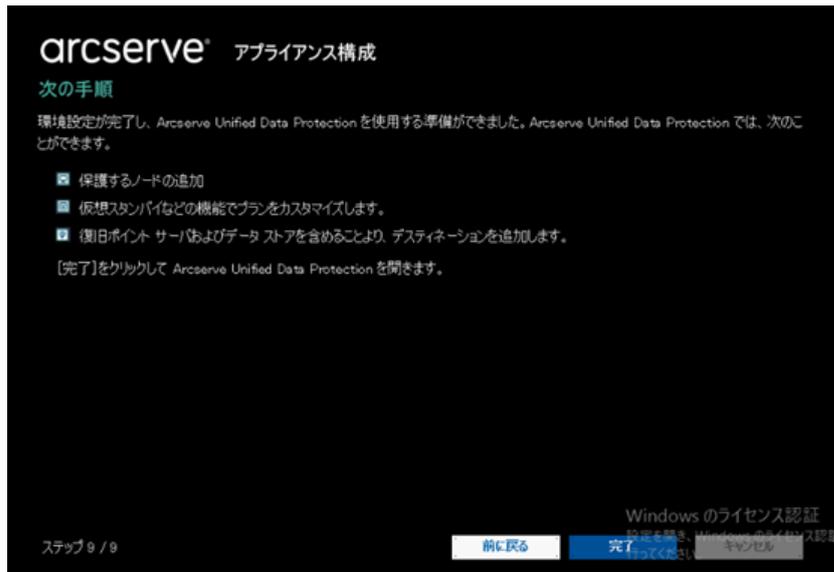


14. プランを検証したら、[次へ]をクリックします。

次の手順]ダイアログボックスが表示されます。

環境設定が正常に終了し、Arcserve UDP コンソールで作業する準備が整いました。保護するノードをさらに追加し、仮想スタンバイなどの機能でプランをカスタマイズし、復旧ポイント サーバおよびデータストアを含めることによってデスティネーションを追加することができます。

15. [完了]をクリックしてウィザードを終了し、Arcserve UDP コンソールを開きます。



注：ドメインの認証情報を使用して UDP コンソールにログインするには、「[ドメイン ユーザへの管理者権限および役割の割り当て](#)」を参照してください。

Arcserve アプライアンスをゲートウェイとして設定する方法

Arcserve アプライアンスをゲートウェイとして設定することができます。

以下の手順に従います。

1. Arcserve アプライアンスから Arcserve UDP コンソールをアンインストールします。
2. Arcserve UDPコンソールから **[ソース]** タブをクリックします。
3. Arcserve UDP コンソールの左 ペインで、 **[インフラストラクチャ]** に移動して、 **サイト** をクリックします。
4. **サイトの追加** をクリックします。
5. **サイトの追加** ウィザードの手順に従って、Arcserve UDP リモート管理ゲートウェイを Arcserve アプライアンスにインストールします。

注： Arcserve アプライアンスに Arcserve UDP リモート管理ゲートウェイをインストールした後に、Arcserve アプライアンス ウィザードで **ウィザードの起動** をクリックしても、Arcserve UDP コンソールは起動しません。Arcserve UDP コンソールにアクセスするには、コンソールの URL を直接入力します。Arcserve UDP

第5章: Arcserve アプライアンスでの操作

Arcserve アプライアンスを使用して、Windows、Linux、および仮想マシン用のバックアッププランを作成できます。テープデバイスにデータを書き込み、仮想スタンバイマシンを作成することもできます。

このセクションには、以下のトピックが含まれます。

アプライアンス上の Arcserve 製品のアクティブ化	74
Arcserve アプライアンス ウィザードを使用したプランの作成	75
プランへのノードの追加	76
Linux ノード用のバックアッププランの作成	85
テープデバイスへのバックアッププランの作成	86
アプライアンス上仮想スタンバイプランの作成	87
Linux バックアップサーバのバックアッププランの作成	88
ローカルアプライアンス Hyper-V に対して Linux インスタント VM ジョブを実行するための設定	92
ConsoleMigration.exe を使用した Arcserve UDP コンソールの移行	93
Arcserve アプライアンス間の移行	95
プレインストールされた Linux バックアップサーバの入力ソースの変更	99

アプライアンス上の Arcserve 製品 のアクティブ化

アプライアンス上で Arcserve 製品 をアクティブ化する場合は、「[Arcserve 製品 ライセンス オンライン ヘルプ](#)」を参照してください。

Arcserve アプライアンス ウィザードを使用したプランの作成

プランは、バックアップするノードおよびバックアップするタイミングを定義する手順の集合です。Arcserve アプライアンス では、基本プランを作成することができます。Arcserve ウィザードを使用したプランの作成には、以下の3つのステップがあります。

1. 保護するノードを追加します。

Windows ノードまたは仮想マシンを vCenter/ESX または Hyper-V サーバから選択できます。

2. バックアップ スケジュールを定義します。
3. プランをチェックして確認します。



基本的なプランに加えて、Arcserve UDP では、UDP コンソールから複雑なプランを作成して多くのパラメータを制御することができます。UDP コンソールから複雑なプランを作成するには、「Arcserve UDP ソリューションガイド」を参照してください。

プランへのノードの追加

さまざまなノードを保護するためのプランを作成することができます。ノードを保護するには、ノードをプランに追加する必要があります。Arcserve アプライアンス ウィザードからノードを追加できます。ウィザードでは、以下の方法を使用してノードを追加できます。

- ノードの IP アドレスまたはホスト名を手動で入力
([ホスト名/IP アドレスによるノードの追加](#))
- Active Directory からのノードのディスカバリ
([Active Directory によるノードの追加](#))
- VMware ESX/vCenter Server から仮想マシンノードをインポート
([vCenter/ESX ノードの追加](#))
- Microsoft Hyper-V サーバから仮想マシンノードをインポート
([Hyper-V ノードの追加](#))

ホスト名/IPアドレスによるノードの追加

ノードをプランに追加するためにIPアドレスまたはホスト名を手動で入力することができます。追加するノード数が少ない場合はこの方法を使用しますが、複数のノードを1つずつ追加できます。Arcserve Unified Data Protection Agent for Windows はこれらのノードにインストールされます。

以下の手順に従います。

1. [ホスト名/IPアドレスによるノードの追加] ダイアログボックスで、以下の詳細を入力します。

ホスト名/IPアドレス

ソースノードのホスト名またはIPアドレスを指定します。

ユーザ名

管理者権限を持つノードのユーザ名を指定します。

パスワード

ユーザパスワードを指定します。

説明

ノードを特定する説明を指定します。

プラン作成のキャンセル

作成したプランをキャンセルします。

2. [リストに追加] をクリックします。

ノードが右ペインに追加されます。さらにノードを追加するには、これらの手順を繰り返します。追加されたすべてのノードは、右ペインにリスト表示されます。

3. (オプション) 追加したノードを右ペインのリストから削除するには、目的のノードを選択して **削除**]をクリックします。
4. **次へ**]をクリックします。

ノードがプランに追加されます。

Active Directory によるノードの追加

Active Directory にノードを追加するには、Active Directory の詳細を指定し、ノードを検出して、プランにノードを追加します。

以下の手順に従います。

1. **Active Directory によるノードの追加** ダイアログボックスで、以下の詳細を入力します。

ユーザ名

<ドメイン>\<ユーザ名> の形式でドメインおよびユーザ名を指定します。

パスワード

ユーザパスワードを指定します。

コンピュータ名フィルタ

ノード名のディスカバリに使用するフィルタを指定します。

プラン作成のキャンセル

作成したプランをキャンセルします。

2. **参照** をクリックします。
検出されたノードが表示されます。



ノードを追加するには、ノードを選択して確認します。

3. 検証するには、ノードを選択し、ユーザ名およびパスワードを入力して **適用]**をクリックします。

認証情報が検証されました。検証済みノードには、緑色のチェックマークが付いています。ノードの検証が失敗した場合、認証情報を再入力して **適用]**を再度クリックします。

注: ノードをリストに追加する前に各ノードを検証する必要があります。

4. **[リストに追加]**をクリックします。
選択したノードが右ペインに追加されます。
5. (オプション) ノードを右ペインから削除するには、ノードを選択して **削除]**をクリックします。
6. **次へ]**をクリックします。
ノードがプランに追加されます。

vCenter/ESX ノードの追加

仮想マシンノードを VMware vCenter/ESX Server に追加できます。これらのノードを追加するには、vCenter/ESX Server からのノードを検出およびインポートする必要があります。

以下の手順に従います。

1. [vCenter/ESX によるノードの追加] ダイアログボックスで、以下の vCenter/ESX Server の詳細を指定します。

ホスト名/IP アドレス

vCenter/ESX Server のホスト名または IP アドレスを指定します。

ポート

使用するポート番号を指定します。

プロトコル

使用するプロトコルを指定します。

ユーザ名

サーバのユーザ名を指定します。

パスワード

ユーザパスワードを指定します。

プラン作成のキャンセル

作成したプランをキャンセルします。

The screenshot shows the 'arcserve アプライアンス構成' (Arcserve Appliance Configuration) window. The main title is 'vCenter/ESX によるノードの追加' (Add Node via vCenter/ESX). Below the title, it says 'vCenter/ESX の情報を入力して、プランにノードを追加します。' (Enter vCenter/ESX information to add nodes to the plan). The form contains several input fields: 'ホスト名/IP アドレス' (Host name/IP address), 'ポート' (Port) with the value '443', 'プロトコル' (Protocol) with a dropdown menu showing 'HTTPS', 'ユーザ名' (Username) with the value 'root', and 'パスワード' (Password). A '接続' (Connect) button is located below these fields. To the right, there is a separate window titled 'プランで保護されているノード' (Nodes protected in the plan), which contains a checkbox for 'ノード' (Node) and a note: '全フィールドが使用して、プランにノードを追加します。' (Use all fields to add nodes to the plan). A '閉じる' (Close) button is at the bottom of this window. At the bottom of the main window, there is a 'プランの作成のキャンセル' (Cancel plan creation) button, a progress indicator 'ステップ 6 / 9' (Step 6 / 9), and three navigation buttons: '前に戻る' (Back), '次へ' (Next), and 'キャンセル' (Cancel).

2. **接続**] をクリックします。

検出されたホスト名が表示されます。

3. ホスト名を展開してノードを参照します。



4. 追加するノードを選択してから、[リストに追加]をクリックします。
選択したノードが右ペインに追加されます。
5. (オプション) ノードを右ペインから削除するには、ノードを選択して [削除]をクリックします。
6. [次へ]をクリックします。
ノードがプランに追加されます。

Hyper-V ノードの追加

この方法を使用すると、Microsoft Hyper-V サーバから仮想マシンノードをインポートできます。

以下の手順に従います。

1. [Hyper-V ノードの追加] ダイアログボックスで以下の詳細を指定します。



ホスト名/IP アドレス

Hyper-V サーバの名前または IP アドレスを指定します。Hyper-V クラスタに含まれている仮想マシンをインポートするには、クラスタノード名または Hyper-V ホスト名のいずれかを指定します。

ユーザ名

管理者権限のある Hyper-V ユーザ名を指定します。

注：Hyper-V クラスタの場合は、クラスタの管理者権限を持つドメインアカウントを使用します。スタンドアロン Hyper-V ホストの場合は、ドメインアカウントを使用することをお勧めします。

パスワード

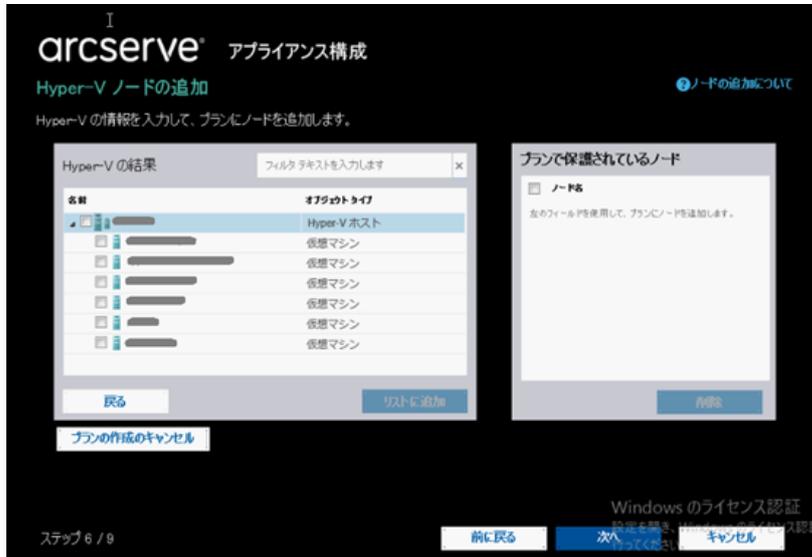
ユーザ名のパスワードを指定します。

プラン作成のキャンセル

作成したプランをキャンセルします。

2. **接続]**をクリックします。

検出されたホスト名が表示されます。ホスト名を展開してノードを参照します。



3. (オプション) [フィルタ]フィールドにノード名を入力して、ツリー内のノードを検索できます。
4. ノードを選択してから、**[リストに追加]**をクリックします。
選択したノードが右ペインに追加されます。
5. (オプション) ノードを右ペインから削除するには、ノードを選択して **削除]**をクリックします。
6. **次へ]**をクリックします。
ノードがプランに追加されます。

Linux ノード用のバックアッププランの作成

Arcserve アプライアンス コンソールから Linux ノードをバックアップできます。Linux バックアップ サーバはすでにコンソールに追加されています。

以下の手順に従います。

1. Arcserve アプライアンス コンソールを開きます。
2. [ソース]- [プラン]- [すべてのプラン]をクリックします。
3. Linux バックアップ プランを作成します。
4. [ソース]、[スチーゼーション]、[スケジュール]、[拡張]の設定を指定します。

注：各環境設定の詳細については、「ソリューション ガイド」の「[Linux バックアッププランを作成する方法](#)」を参照してください。

5. バックアップ プランを実行します。

テープ デバイスへのバックアップ プランの作成

Arcserve アプライアンスには、テープ デバイスにデータを書き込む機能があります。通常、ソース データは、UDP バックアップ プランを使用してデータストアに保存されている復旧ポイントで、デスティネーションはテープ デバイスです。Arcserve Backup マネージャを使用して、テープへのバックアップ ジョブを管理する必要があります。

以下のプロセスの概要は、Arcserve アプライアンスを使用してテープ デバイスにデータを書き込む方法を理解するのに役立ちます。

1. テープ デバイスを Arcserve アプライアンスに取り付けます

Arcserve アプライアンスには、テープ デバイスを接続するためのポートが背面パネルに備わっています。テープ デバイスを接続すると、Arcserve アプライアンスは自動的にテープ デバイスを識別します。

2. バックアップ マネージャを使用して、テープ デバイスを設定します。

バックアップ マネージャを開き、テープ デバイスをバックアップ マネージャに追加します。バックアップ マネージャは、Arcserve Backup を管理するためのインターフェースです。テープ デバイスをバックアップ マネージャに追加した後、テープ デバイスを設定します。

注：デバイスの設定および管理の詳細については、「Arcserve Backup 管理者ガイド」の「[デバイスおよびメディアの管理](#)」を参照してください。

3. UDP コンソールを使用して、1 つ以上のバックアップ ジョブを正常に完了します。

テープ デバイスに書き込み可能な正常なバックアップが少なくとも 1 つ存在している必要があります。データをバックアップするには、UDP コンソールを使用してプランを作成し、データストアにバックアップします。

注：別のノード用のバックアップ プランの作成に関する詳細については、「ソリューションガイド」の「[データを保護するプランの作成](#)」を参照してください。

4. バックアップ マネージャからのテープへのバックアップ ジョブの開始

バックアップ マネージャを開き、テープ デバイスにデータをバックアップするプランを作成します。ソース データは UDP バックアップ プランのデスティネーションで、デスティネーションはテープ デバイスです。

注：テープへのバックアップ プランの作成に関する詳細については、「Arcserve Backup 管理者ガイド」の「[D2D/UDP データのバックアップおよび回復](#)」を参照してください。

アプライアンス上 仮想スタンバイプランの作成

Arcserve アプライアンスには、仮想スタンバイマシンとして動作する機能があります。

以下の手順に従います。

1. 成功するバックアッププランであるかを検証します。
2. Arcserve アプライアンス コンソールを開きます。
3. プランに移動して、バックアッププランを変更します。
4. 仮想スタンバイタスクを追加します。
5. ソース、デスティネーション、仮想マシンの環境設定を更新します。

注: 環境設定の詳細については、「ソリューションガイド」の「[仮想スタンバイプランを作成する方法](#) Arcserve UDP」トピックを参照してください。

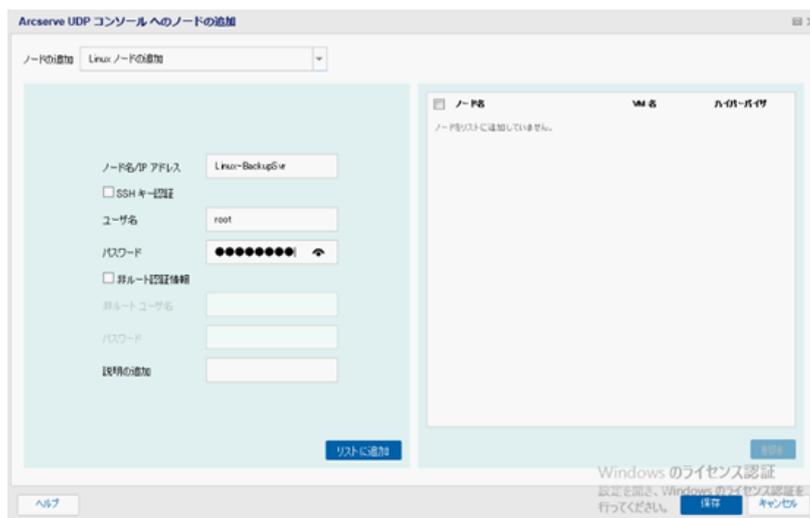
6. プランを保存して実行します。

Linux バックアップ サーバのバックアッププランの作成

Arcserve アプライアンスでは、Linux バックアップ サーバのバックアップを設定することができます。

以下の手順に従います。

1. Arcserve UDP コンソールから、[ソース] タブをクリックします。
2. 右側のペインの **すべてのノード**] をクリックします。
3. 中央のペインから、**ノードの追加**] をクリックします。
Arcserve UDP コンソールへのノードの追加] ダイアログボックスが表示されます。
4. **ノードの追加**] ドロップダウン リストから、**Linux ノードの追加**] を選択します。
5. ノードの認証情報を入力し、**リストに追加**] をクリックします。

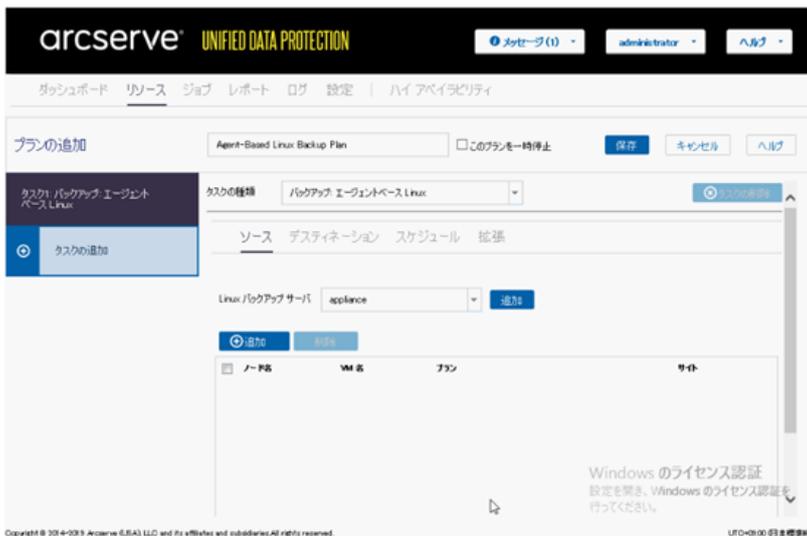


6. **保存**] をクリックします。
追加された Linux ノードは **すべてのノード**] リストに表示されます。

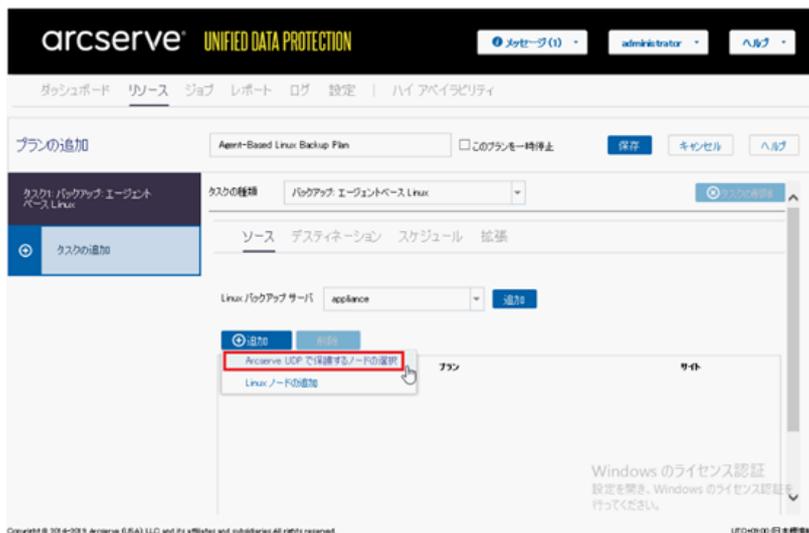


7. [すべてのプラン]に移動し、エージェント ベース Linux プランを作成します。

[ソース]タブが表示されます。

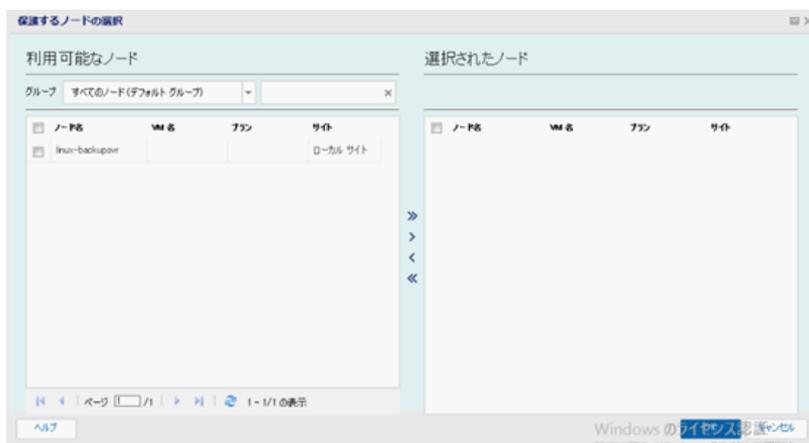


8. [追加]ドロップダウンリストから、Arcserve UDP で保護するノードの選択]を選択します。



保護するノードの選択] ダイアログ ボックスが表示されます。

- 追加された Linux ノードを保護して、**OK]** をクリックします。



デスティネーション] タブが表示されます。

- 表示されるデフォルトのデスティネーションは、アプライアンス ウィザードを使用して作成されたデータストアです。必要に応じて、ノードをバックアップするローカル ディスクまたは共有フォルダを選択します。

The screenshot shows the 'プランの追加' (Add Plan) configuration page in the Arcserve Unified Data Protection console. The page title is 'Agent-Based Linux Backup Plan'. There are buttons for '保存' (Save), 'キャンセル' (Cancel), and 'ヘルプ' (Help). The 'タスクの種類' (Task Type) is set to 'バックアップ: エージェントベース Linux'. Below this, there are tabs for 'ソース', 'デスティネーション', 'スケジュール', and '拡張'. The 'デスティネーションの種類' (Destination Type) is set to 'Arcserve UDP 復元ポイントサーバ'. The '復元ポイントサーバ' (Restore Point Server) is 'appliance', and the 'データストア' (Data Store) is 'appliance_data_store'. The 'パスワードによる保護' (Password Protection) checkbox is checked. There are fields for 'セッションパスワード' (Session Password) and 'セッションパスワードの確認' (Confirm Session Password). A note at the bottom right says 'Windows のライセンス認証' (Windows License Activation) and '設定を完了し、Windows のライセンス認証を行ってください。' (Complete the configuration and activate Windows license).

11. プランに関連する設定を入力したら、**保存]**をクリックします。

The screenshot shows the 'プラン' (Plans) overview page in the Arcserve Unified Data Protection console. The page title is 'プラン: すべてのプラン'. There is a table with columns for 'プラン名' (Plan Name), '合計' (Total), and '保護ノード' (Protected Nodes). The table contains one entry: 'Agent-Based Linux Backup Plan' with a total of 1 and 1 protected node. There are buttons for 'アクション' (Action) and '詳細設定ウィザード' (Advanced Configuration Wizard). A note at the bottom right says 'Windows のライセンス認証' (Windows License Activation) and '設定を完了し、Windows のライセンス認証を行ってください。' (Complete the configuration and activate Windows license).

追加された Linux バックアップ サーバに対して正常にバックアップを実行することができます。

ローカル アプライアンス Hyper-V に対して Linux インスタント VM ジョブを実行するための設定

Arcserve アプライアンスを使用すると、ローカル アプライアンス Hyper-V 上で Linux インスタント VM ジョブを実行するようにネットワークを設定することができます。

以下の手順に従います。

1. Hyper-V マネージャを開きます。
2. 新しい外部仮想ネットワークスイッチを作成します。
3. Linux バックアップ サーバをオフにし、Linux バックアップ サーバに外部スイッチを追加します。
4. Linux バックアップ サーバをオンにして、新しいイーサネット接続下のネットワーク設定にプロファイルを追加し、IP アドレスを取得します。

注： IP アドレスが割り当てられていない場合、処理中に Linux バックアップ サーバが再起動されます。

5. Linux インスタント VM ジョブをローカル Hyper-V に対して実行するには、新しく追加された仮想ネットワークスイッチを選択します。

Linux インスタント VM ジョブをローカル アプライアンス Hyper-V に対して正常に実行できるようになりました。

ConsoleMigration.exe を使用した Arcserve UDP コンソールの移行

Arcserve アプライアンス アプライアンスでは、*ConsoleMigration.exe* を使用して Arcserve UDP コンソールを別のアプライアンスに移行できます。Arcserve UDP v6.5 Update 2 以降では、アプライアンスに属していない場合でも、任意の2つの Arcserve UDP コンソールの間で Arcserve UDP コンソールを移行できます。

BackupDB および RecoverDB 用の *ConsoleMigration.exe* を使用します。以下のスクリーンショットは、*ConsoleMigration.exe* の使用方法を示しています。

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe
Usage: ConsoleMigration.exe [-BackupDB|-RecoverDB [-Force]]
-BackupDB: Backup UDP Console database Arcserve_APP
-RecoverDB: Recover UDP Console database Arcserve_APP
-Force (optional): Force recover UDP Console database
Your input is not valid. Please follow the usage.
```

移行プロセスを完了するには、以下の手順を実行します。

1. 古い Arcserve UDP コンソールで、Arcserve UDP データベースのバックアップを実行します。

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe -BackupDB
Start Backup...
Backed up DB and version files completed.
DB and version files were created at: "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\DB_Migration".
```

[DB_Migration] フォルダが正常に作成します。

2. 新しい Arcserve UDP コンソールで、[DB_Migration] フォルダを次のパスにコピーします。

<UDP_Home> \Management\BIN\Appliance\

3. 新しい Arcserve UDP コンソールが Arcserve アプライアンスの場合、ホスト名を変更してシステムを再起動し、アプライアンス ウィザードを使用してアプライアンス設定を終了します。

注： Arcserve UDP コンソールが Arcserve アプライアンス ではない場合、この手順をスキップします。

4. 新しい Arcserve UDP コンソールで、以下の画面に示される手順を実行して、Arcserve UDP コンソール データベースを復旧させます。データベースのリカバリプロセスが完了したら、新しい Arcserve UDP コンソールのノードが更新されます。ノードの更新に失敗した場合は、*C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\logs*

パスの下にある *DisconnectedNodesInfo-<mm-dd-yyyy>.txt* ファイルに切断されたノードが記録されます。切断されているノードは新しい Arcserve UDP コンソールから手動で更新できます。

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance>ConsoleMigration.exe -RecoverDB
Are you sure you want to recover the backup DB file? (y/n): y
Stopping Arcserve UDP Management service, please wait...
Recovering backup DB file...
Updating nodes, please wait...
Please update nodes manually from UDP console if you still encounter disconnected nodes.
The disconnected nodes(if existing) will be saved at "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\Appliance\logs".
Console migration completed. Console uses DB "localhost\ARCSERVE_APP".
```

注： Arcserve UDP コンソールで、ローカル サイト 以外のサイトが存在する場合、*NewRegistrationText.txt* ファイルに記載されている手順に従い、サイトを再登録します。

新しい Arcserve UDP コンソールへの Arcserve アプライアンス コンソールの移行が正常に完了しました。

このツールを使用して、リモート SQL データベースと接続している Arcserve UDP コンソールについて、コンソール移行を実行することができます。移行が完了すると、移行された Arcserve UDP コンソールは同じリモート SQL データベースに接続されるように設定されます。

注： Arcserve UDP v6.5 Update 4 以降、*ConsoleMigration.exe* コマンドに *-force* オプションが導入されました。このオプションを使用すると、以下の条件で、復旧用バックアップ データベース ファイルのターゲット コンソールへの移行が強制されます。

1. ソース コンソールで SQL Server Enterprise エディションを使用しており、ターゲット コンソールで SQL Server Express エディションを使用している 2 つのコンソール間で、コンソールの移行を実行する必要がある場合。この場合、ソース UDP コンソールで必要なデータベースの最小サイズは 4000 MB です。
2. SQL Server データベースの新しいバージョンを使用するコンソールから SQL Server データベースの古いバージョンを使用するコンソールへコンソールの移行を実行する必要がある場合。たとえば、SQL Server 2016 を使用するコンソールから SQL Server 2014 を使用するコンソールへの移行です。

Arcserve アプライアンス間の移行

このトピックでは、既存の Arcserve アプライアンス から別の新しい Arcserve アプライアンス への移行を実行するユーザ用に解決策を提供します。

たとえば、Arcserve アプライアンス 1 を Arcserve アプライアンス 2 に移行するとします。前提条件は次のとおりです。

- アプライアンス 1 とアプライアンス 2 の両方に接続できることを確認します。
- アプライアンス 2 の容量には、アプライアンス 1 上のすべてのデータを保持するために十分なメモリが必要です。
- Arcserve アプライアンス 1 で、ジョブが実行されていないことを確認します。
コンソールの移行の詳細については、「[ConsoleMigration.exe を使用して Arcserve UDP コンソールを移行する方法](#)」のトピックを参照してください。

任意のアプライアンスから新しいアプライアンスに移行するには、以下の解決策に従います。

- [解決策](#)

解決策

Arcserve アプライアンスの移行に関するソリューション

重要: 既存のアプライアンスが Arcserve UDP コンソールと Arcserve UDP RPS の両方として動作している場合、この解決策を使用することができます。

前提条件:

- Arcserve アプライアンス 1 で、ジョブが実行されていないことを確認します。
- Arcserve UDP コンソールを Arcserve アプライアンス 1 から 2 に移行済みです。

注: Arcserve UDP コンソールをアプライアンス 1 から 2 に移行する方法の詳細については、「[ConsoleMigration.exe を使用した Arcserve UDP コンソールの移行方法](#)」を参照してください。

以下の手順に従います。

1. コマンドラインで以下のコマンドを使用し、Arcserve アプライアンス 1 上のすべての Arcserve UDP サービスを停止します。

```
C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>  
cmdutil.exe /stopall
```

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files\Arcserve\Unified Data Protection\Management\BIN>endut
il.exe /stopall
Start to kill process explorer.exe

Killing process explorer.exe
Process killed.

Start to kill process D2DUUDgc.exe

Stopping service 'Arcserve UDP Agent Service'...
Service Stopped.

Stopping service 'Arcserve UDP RPS Data Store Service'...
Service Stopped.

Stopping service 'Arcserve UDP RPS Port Sharing Service'...
Service Stopped.

Stopping service 'Arcserve UDP Identity Service'...
Service Stopped.

Stopping service 'Arcserve UDP Management Service'...
Service Stopped.

Stopping service 'Arcserve UDP Management Port Sharing Service'...
Service Stopped.

Stopping service 'Arcserve UDP Agent Explorer Extension Service'...
Service Stopped.

Stopping service 'Arcserve UDP Update Service'...
Service Stopped.

Stopping Arcserve UDP agent monitor...
Arcserve UDP agent monitor stopped.

Start to kill Arcserve UDP processes

Killing process sync_utl_d.exe
Process killed.

Killing process AFD2DMonitor.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process GDDServer.exe
Process killed.

Killing process AStartup.exe
Process killed.

Killing process explorer.exe
Process killed.

Stopping mounting driver...
Mounting driver stopped.

Start Windows Explorer.
```

2. ディスク X および Y 上のすべてのデータを、Arcserve アプライアンス 1 から 2 に手動でコピーします。
3. アプライアンス 2 で、すべての Arcserve UDP サービスを起動し、アプライアンス 1 からコピーしたデータストアをインポートします。

The screenshot shows the 'データストアのインポート' (Data Store Import) configuration page in the Arcserve management console. The page has a navigation bar at the top with links for 'ダッシュボード', 'リソース', 'ジョブ', 'レポート', 'ログ', '設定', and 'ハイパフォーマンス'. The main content area is titled 'データストアのインポート' and contains the following fields:

- 旧ホストサーバ**: appliance
- データストアフォルダ**: X:\Arcserve\data_store\common (with a '参照' button)
- 暗号化パスワード**: [masked] (with a '変更' button)

At the bottom of the form, there are three buttons: '保存' (Save), 'キャンセル' (Cancel), and 'ヘルプ' (Help).

注: Arcserve UDP ログ ファイルは新しいアプライアンスには移行されません。

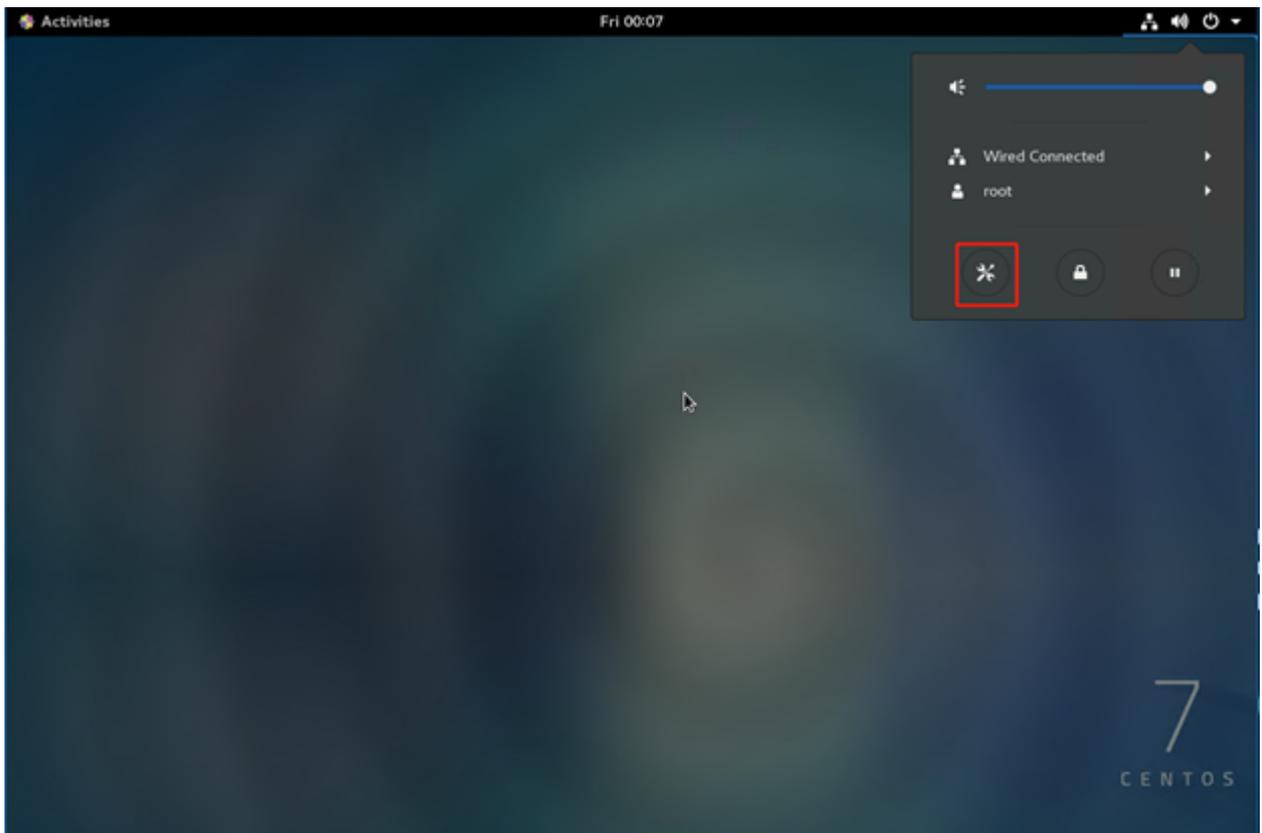
既存の Arcserve アプライアンス から別の新しい Arcserve アプライアンス への移行が完了します。

プレインストールされた Linux バックアップ サーバの入カソースの変更

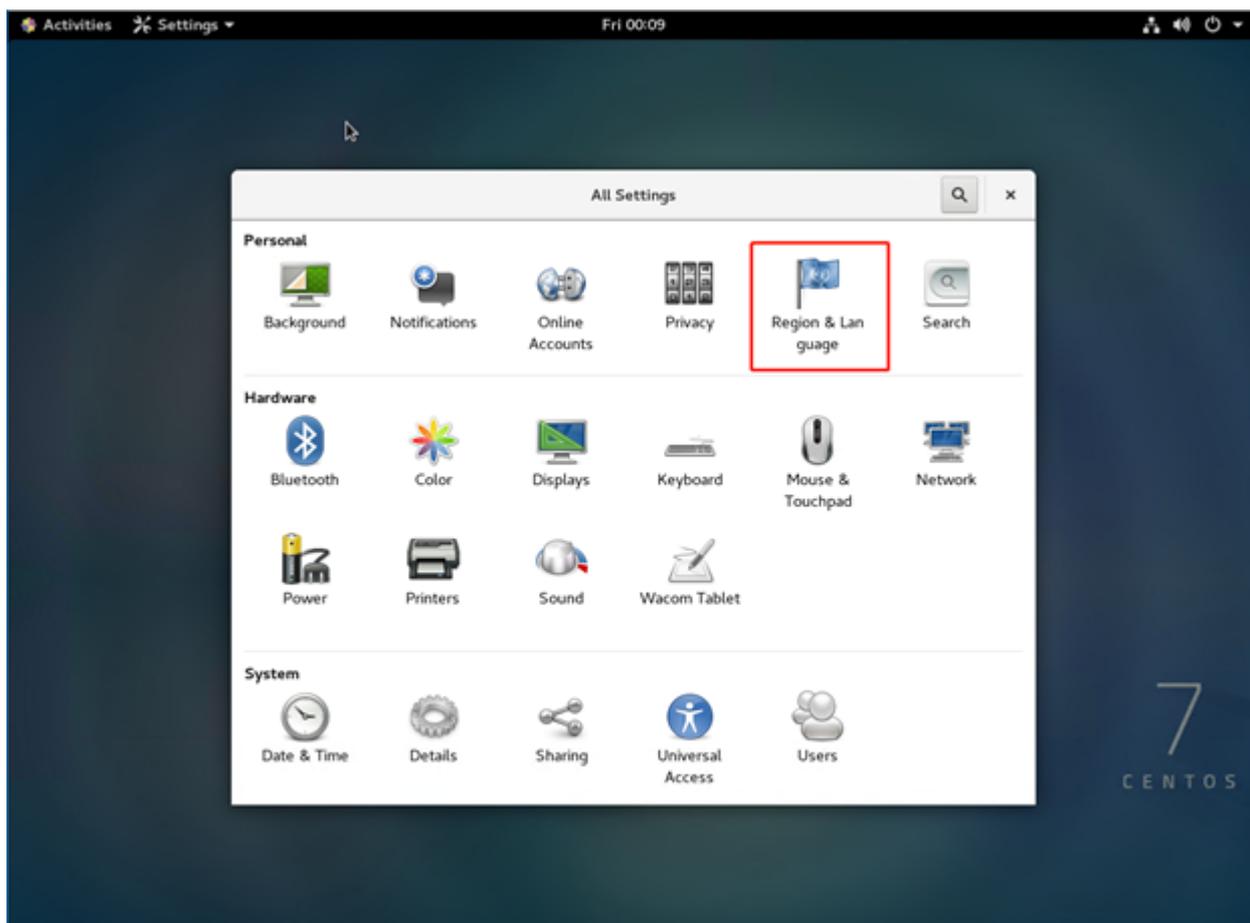
プレインストールされた Linux バックアップ サーバのキーボードを変更することができます。

以下の手順に従います。

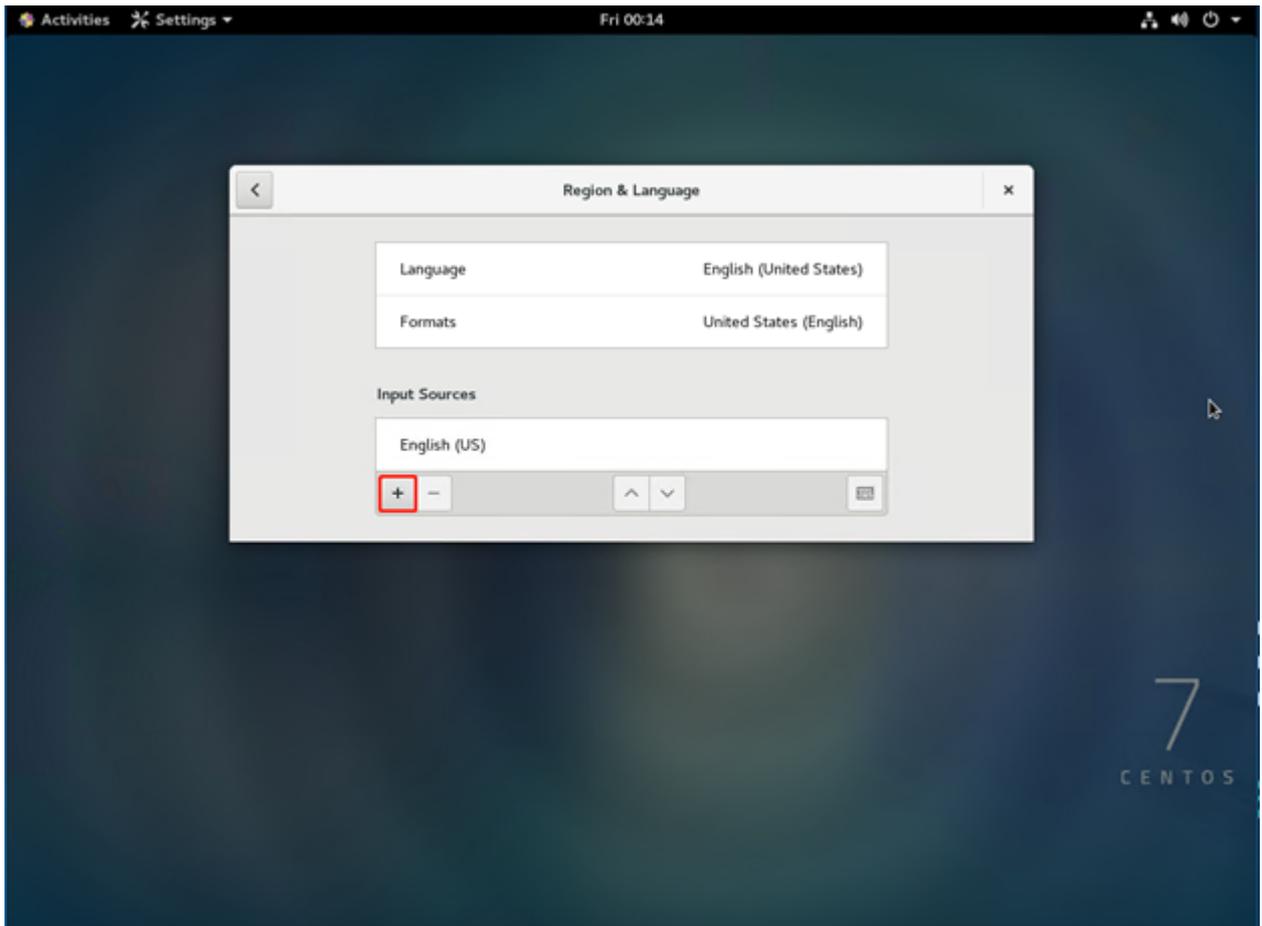
1. 管理者として Arcserve アプライアンス にログインします。
2. **設定**]をクリックします。



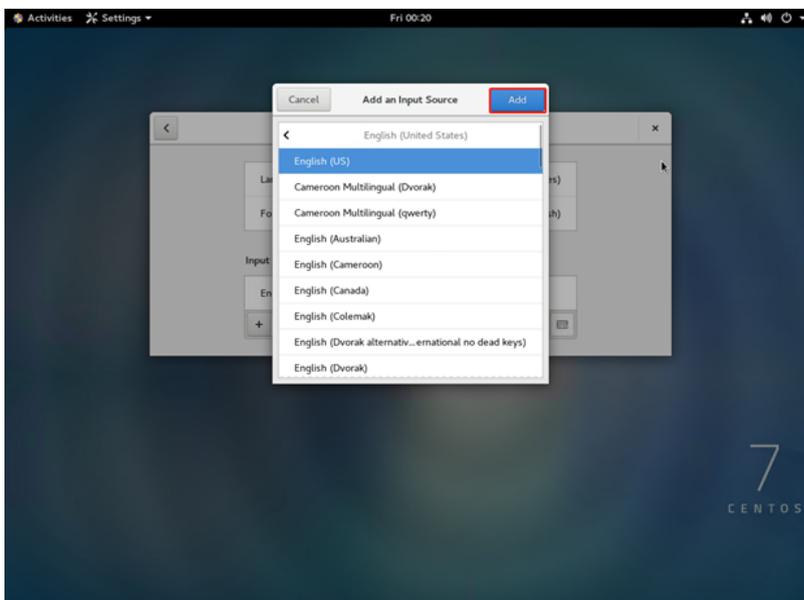
3. **地域と言語**]をクリックします。



4. [Region & Language] をクリックして、新しい入カソースを選択します。



5. 言語とキーボード レイアウトを選択します。



6. [追加]をクリックします。
入カソースが正しく追加されます。

第6章: アプライアンス サーバのリモート モニタリング

Arcserve アプライアンス をリモート でモニタリングすることができます。

このセクションには、以下のトピックが含まれます。

iDRAC (Integrated Dell Remote Access Controller) での操作

このセクションには、以下のトピックが含まれます。

iDRAC (Integrated Dell Remote Access Controller) の モニタと管理

Arcserve アプライアンス 9012-9504DR には、iDRAC9 (Integrated Dell Remote Access Controller 9) が搭載されています。iDRAC9 により、サーバ管理者は Arcserve アプライアンスの全体の可用性を向上させることができます。iDRAC によりサーバの問題に関するアラートが管理者に提供されるため、サーバのリモート管理を実行することができ、サーバへ物理的にアクセスする必要性が少なくなります。

システムステータスのモニタ、システム情報の管理、および仮想コンソールの起動を行うには、iDRAC にログインする必要があります。

以下の手順に従います。

iDRAC にログインします。

1. ブラウザを起動して、<https://<iDRAC-IP-address>> に移動します。
iDRAC のログイン ページが表示されます。
2. 以下の情報を入力します。
ユーザ名：root
パスワード：ARCAADMIN
3. [ログイン] をクリックします。

システムステータスのモニタとシステム情報の管理：

iDRAC システムステータスをモニタして、以下のシステム情報を管理できます。

- システムの健全性
- システムのプロパティ
- ハードウェアとファームウェアのインベントリ
- センサの健全性
- ストレージ デバイス
- ネットワーク デバイス
- ユーザ セッションの表示と終了

仮想コンソールを起動します。

1. <https://<iDRAC-IP-address>> にログインします。
2. [ダッシュボード] に移動して、[仮想コンソールの起動] をクリックします。

仮想コンソール] ページが表示されます。

仮想コンソールビューア] には、リモート システム デスクトップが表示されます。キーボードとマウスを使用してリモート システムを制御し、操作を実行することができます。

iDRAC (Integrated Dell Remote Access Controller 9000 シリーズ) の IP アドレスの検出

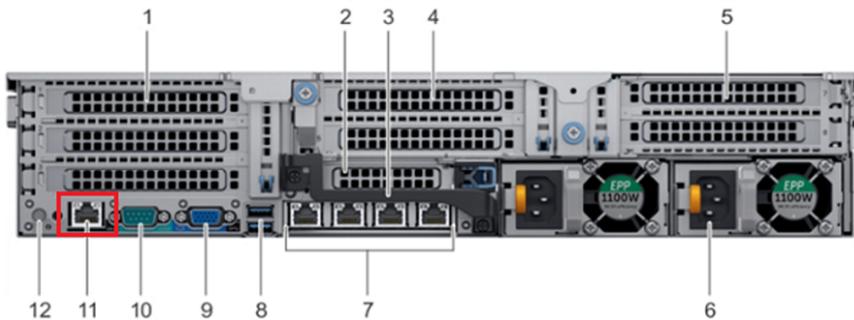
Arcserve アプライアンス 9012-9504DR シリーズ モデルは、デフォルトで iDRAC 対応の DHCP を使用するよう設定されています。iDRAC にアクセスするには、iDRAC9 専用ネットワークポートに Ethernet ケーブルを接続します。Arcserve アプライアンス 9012-9504DR シリーズ モデルの背面パネルおよび iDRAC9 専用ネットワークポートの詳細については、「[9012-9048 の背面パネル](#)」および「[9072DR-9504DR の背面パネル](#)」を参照してください。

iDRAC9 対応 9012-9048 の背面パネルの外観



iDRAC9 dedicated network port
on rear panel of Arcserve Appliance 9012-9048 series models

iDRAC9 対応 9072DR-9504DR の背面パネルの外観



iDRAC9 dedicated network port on
rear panel of Arcserve Appliance 9072DR-9504DR series models

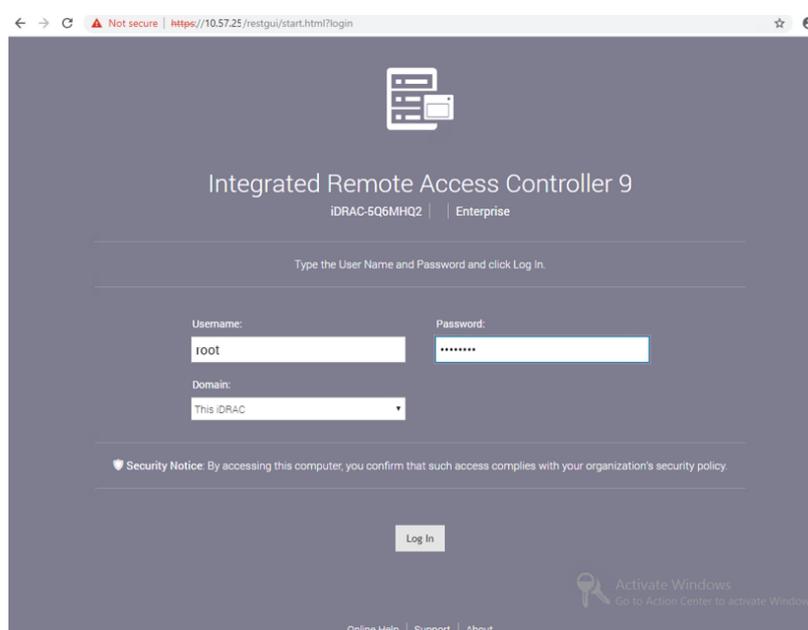
アプライアンスから iDRAC の IP アドレスを検出できます。

以下の手順に従います。

1. Arcserve アプライアンスの起動中に iDRAC IP をメモします。



2. ブラウザを起動して、`https://<iDRAC-IP-address>` に移動します。



iDRAC ログイン ページが表示されます。

iDRAC (Integrated Dell Remote Access Controller、X シリーズ) の IP アドレスの検出

Arcserve アプライアンス X シリーズ モデルは、デフォルトで iDRAC 対応の DHCP を使用するよう設定されています。iDRAC にアクセスするには、iDRAC9 専用ネットワークポートに Ethernet ケーブルを接続します。Arcserve アプライアンス X シリーズ モデルの背面パネルおよび iDRAC9 専用ネットワークポートの詳細については、「[X シリーズの背面パネル](#)」を参照してください。

X シリーズの背面パネルの表示

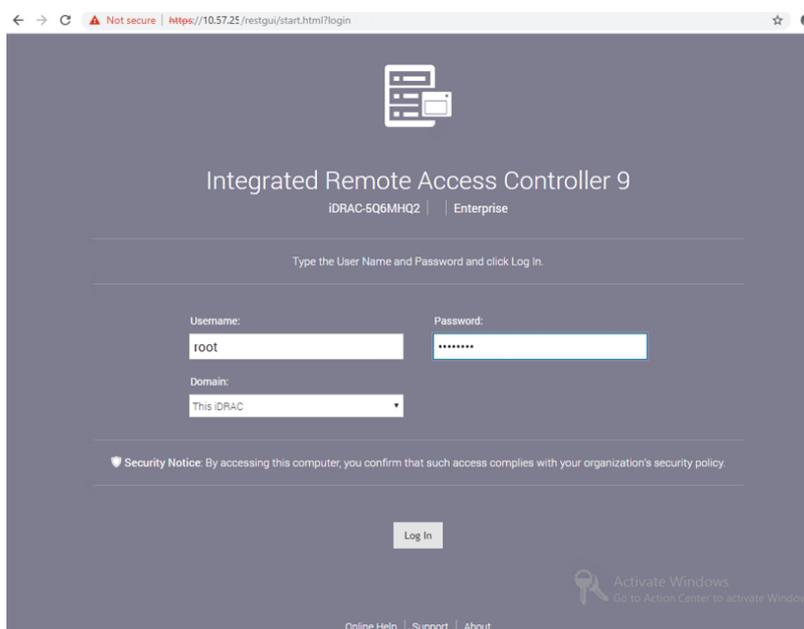
アプライアンスから iDRAC の IP アドレスを検出できます。

以下の手順に従います。

1. Arcserve アプライアンスの起動中に iDRAC IP をメモします。



2. ブラウザを起動して、`https://<iDRAC-IP-address>` に移動します。



iDRAC ログイン ページが表示されます。

iDRAC の DHCP または静的 IP アドレスの設定

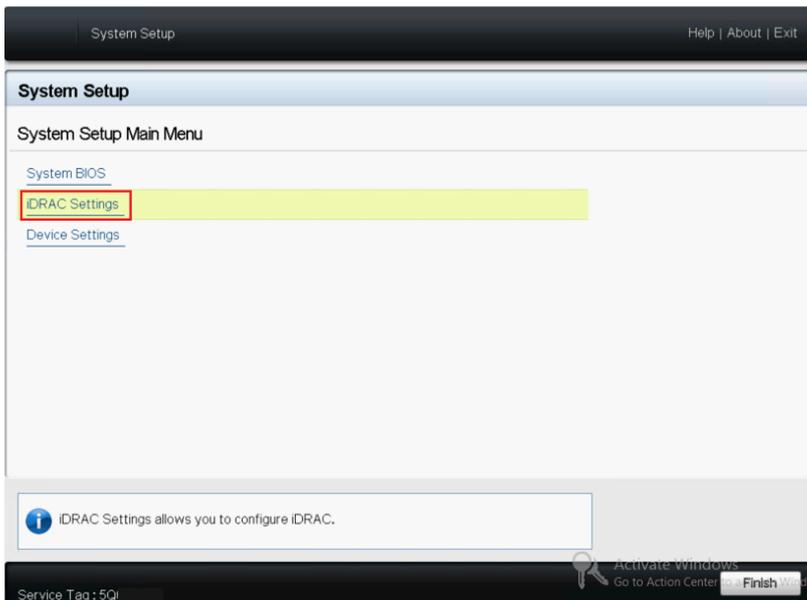
iDRAC に対して、DHCP ネットワークモードを設定することができます。

以下の手順に従います。

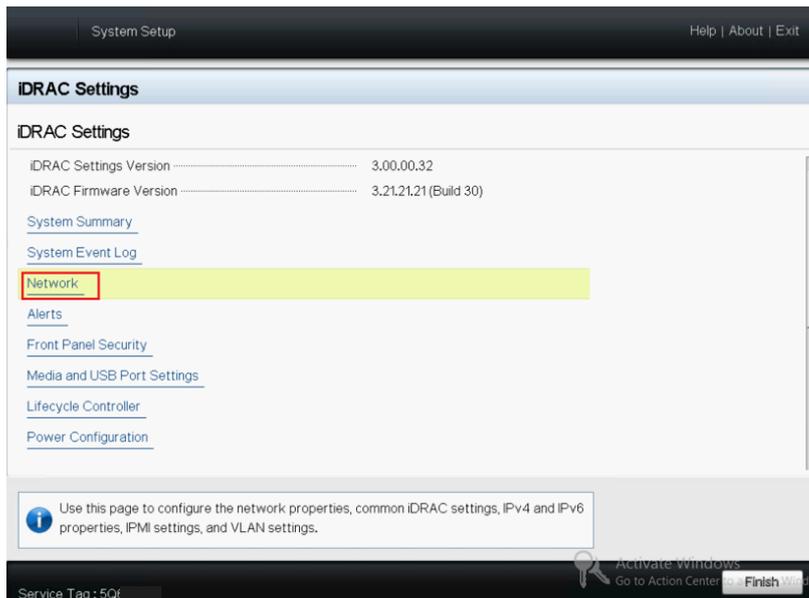
1. Arcserve アプライアンスの起動中に F2 キーを押して、システムのセットアップ画面に切り替えます。



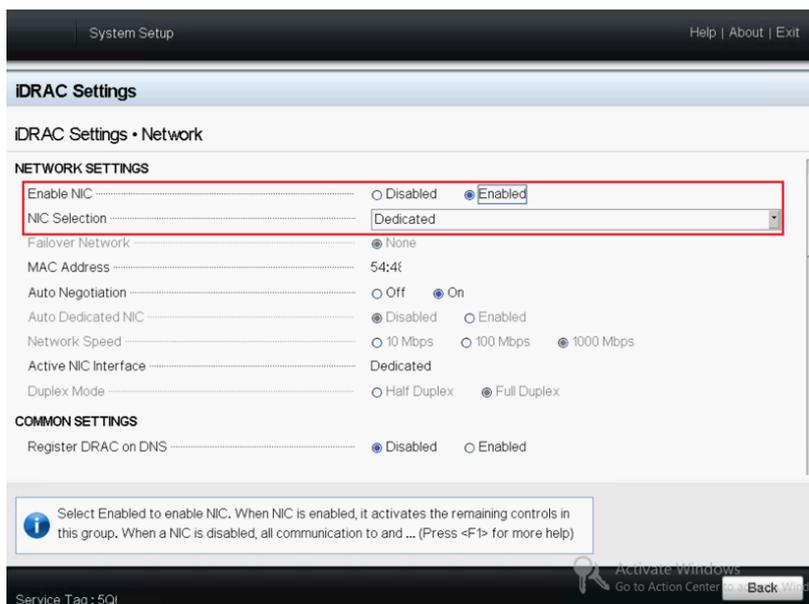
2. [システムセットアップメインメニュー]画面で、[iDRAC の設定]をクリックします。



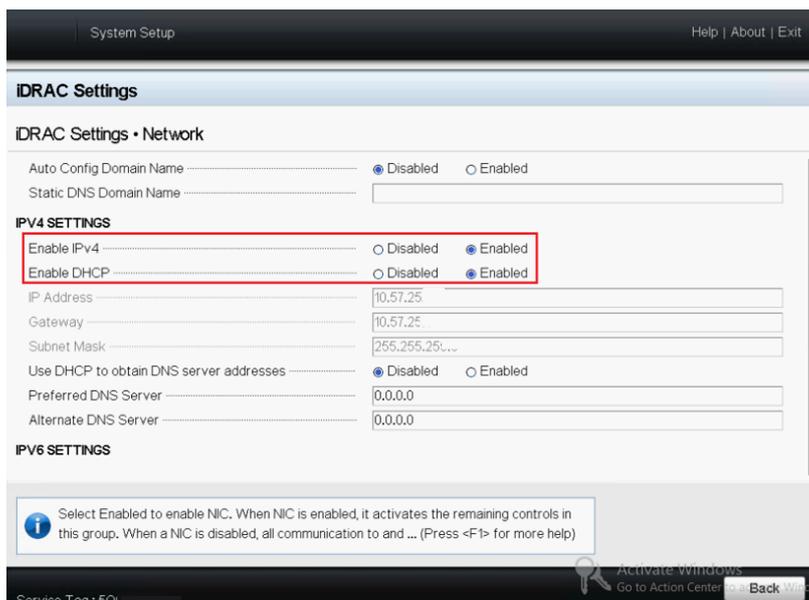
3. [iDRAC の設定]オプションで [ネットワーク]をクリックします。
[ネットワークの設定]フィールドが表示されます。



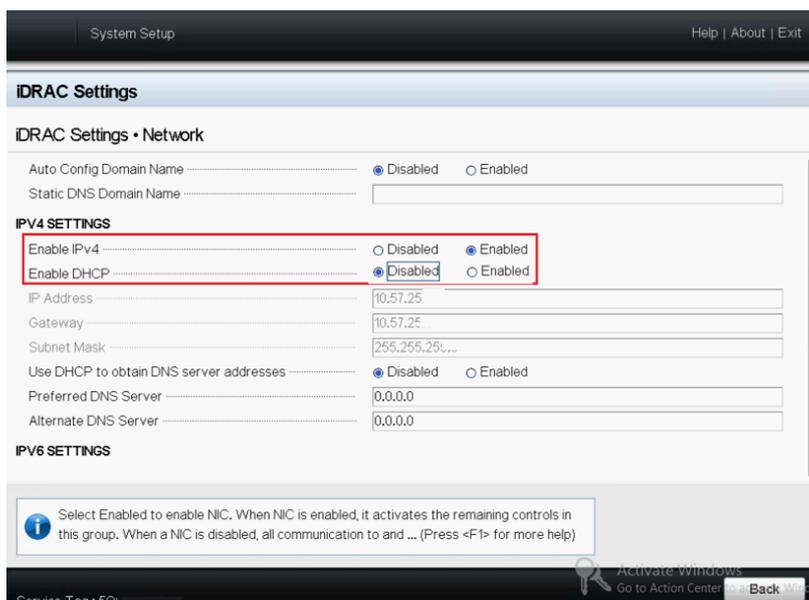
4. 専用ネットワーク インターフェースを使用するには、**[NIC 設定の有効化]** で **有効]** を選択し、**[NIC を選択]** で **専用]** を選択します。



5. DHCP モードを設定するには、IPV4 設定の **[Pv4 有効]** および **[DHCP 有効]** で、**有効]** オプションを選択します。

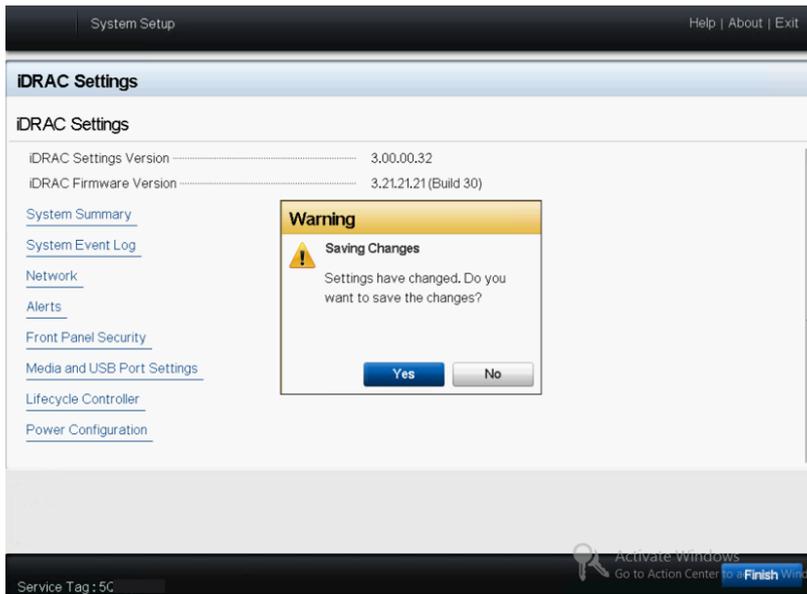


注: iDRAC 専用ネットワークに静的 IP を設定する場合は、[Pv4 有効] の設定を **有効**] にし、 [DHCP 有効] の設定を **無効**] にします。ネットワーク構成に従って、IP アドレス、ゲートウェイ、およびサブネット マスクを設定します。

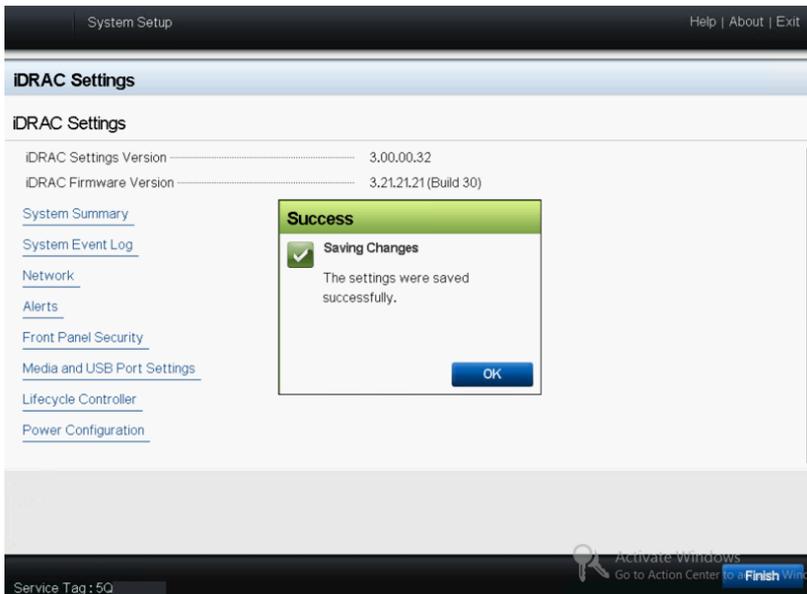


6. **警告**] ダイアログボックスで **戻る**] をクリックし、次に、 **完了**] - **[はい]** をクリックします。

ネットワーク情報が保存されます。

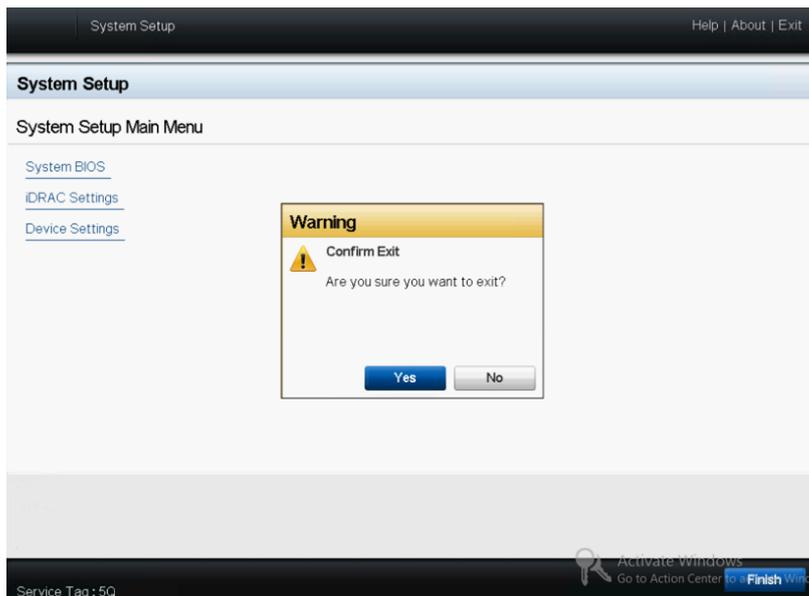


7. **成功**]ダイアログボックスで、**OK**]をクリックします。



iDRAC DHCP の設定が完了します。

8. **完了**] - **はい**]をクリックすると、セットアップが終了し、システムが起動します。



iDRAC に対して DHCP ネットワーク モードが設定されます。

ベースボード管理コントローラ(BMC) の操作

このセクションには、以下のトピックが含まれます。

ベースボード管理コントローラ(BMC) のモニタおよび管理

Arcserve アプライアンス 10024BU-10576DR シリーズ モデルには、ベースボード管理コントローラ(BMC) が搭載されています。BMC を使用すると、サーバ管理者は Arcserve アプライアンスの全体的な可用性を向上させることができます。

BMC によりサーバの問題に関するアラートが管理者に提供されるため、サーバのリモート管理を実行することができ、サーバへ物理的にアクセスする必要性が少なくなります。また、さまざまな場所の複数のユーザにリモート アクセスして、システムのメンテナンスおよび管理を行うこともできます。

システムのステータスをモニタし、システム情報を管理し、リモート コンソールを起動するには、IPMI (インテリジェント プラットフォーム管理 インターフェイス) にログインする必要があります。

以下の手順に従います。

1. Web ブラウザを開き、BMC の IP アドレスを以下の形式で入力します。
`https://BMC-IP-address.`
[ログイン] 画面が表示されます。
2. 以下のようにログイン認証情報を入力します。

- ユーザ名：ADMIN

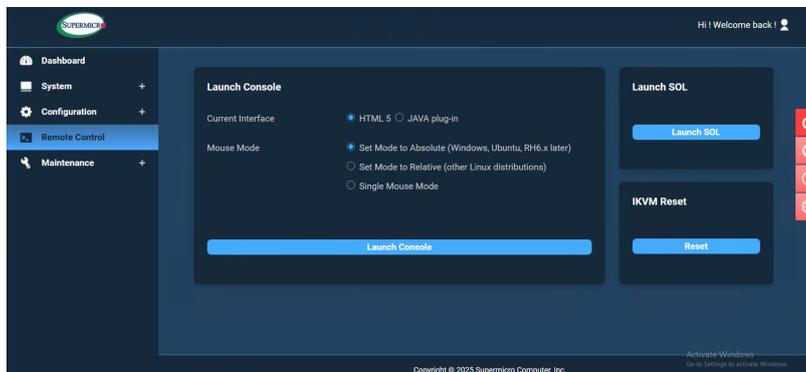
注：ユーザ名は大文字である必要があります。

- パスワード：BMC パスワードを入力します

注：BMC 固有のパスワードは、サーバの前面パネルにある引き出し式タグで確認できます。BMC パスワードは、BMC/IPMI MAC アドレスのすぐ下の行に記載されています。



3. **[ログイン]** をクリックします。
4. **[リモート コンソール]** に移動し、**[Launch Console (コンソールの起動)]** をクリックします。



[Remote Console Viewer (リモート コンソールビューア)]に、リモート システム デスクトップが表示されます。キーボードとマウスを使用してリモート システムを制御し、操作を実行することができます。

また、BMC システム ステータスをモニタして、以下のシステム情報を管理できます。

- システムの健全性
- システムのプロパティ
- ハードウェアとファームウェアのインベントリ
- センサの健全性

- ストレージ デバイス
- ネットワーク デバイス
- ユーザ セッションの表示と終了

BMC の IP アドレスを確認する方法

Arcserve アプライアンス 10024BU-10576DR シリーズ モデルは、デフォルトで BMC に DHCP を使用するように設定されています。BMC にアクセスするには、BMC 専用 ネットワーク ポートに Ethernet ケーブルを接続します。Arcserve アプライアンス 10024BU-10576DR シリーズ モデルの実際のパネルおよび BMC 専用 ネットワーク ポートの詳細については、「[背面パネル 10024BU-10048BU](#)」および「[背面パネル 10048DR-10576DR](#)」を参照してください。

BMC の IP アドレスは、以下の方法で確認できます。

BIOS を使用した IP アドレスの確認

このセクションでは、BIOS を使用して IP アドレスを確認する方法について説明します。

以下の手順に従います。

1. アプライアンス サーバの電源をオンにします。
2. システムの起動中に **Del** キーを押して、BIOS メニューを表示します。
3. **Server Management (サーバ管理)** タブに移動して、**BMC Network Configuration (BMC ネットワーク設定)** を選択します。

BMC Network Configuration (BMC ネットワーク設定) 画面が表示されます。

IPv4 Station IP address (IPv4 ステーション IP アドレス) パラメータで、IP アドレスを確認できます。DHCP で発行された IP アドレスを、希望する静的 IP アドレスに変更することもできます。詳細については、「[BIOS を使用した BMC IP アドレスの設定](#)」を参照してください。

POST 画面での IP アドレスの確認

このセクションでは、POST 画面で IP アドレスを確認する方法について説明します。

以下の手順に従います。

1. アプライアンス サーバの電源をオンにします。
2. システムの起動を開始します。

POST 画面が表示されます。

IP アドレスは、POST 画面の右下に表示されます。

BMC の DHCP または静的 IP アドレスの設定

このセクションでは、BMC の UEFI BIOS および IP アドレスの設定方法について説明します。

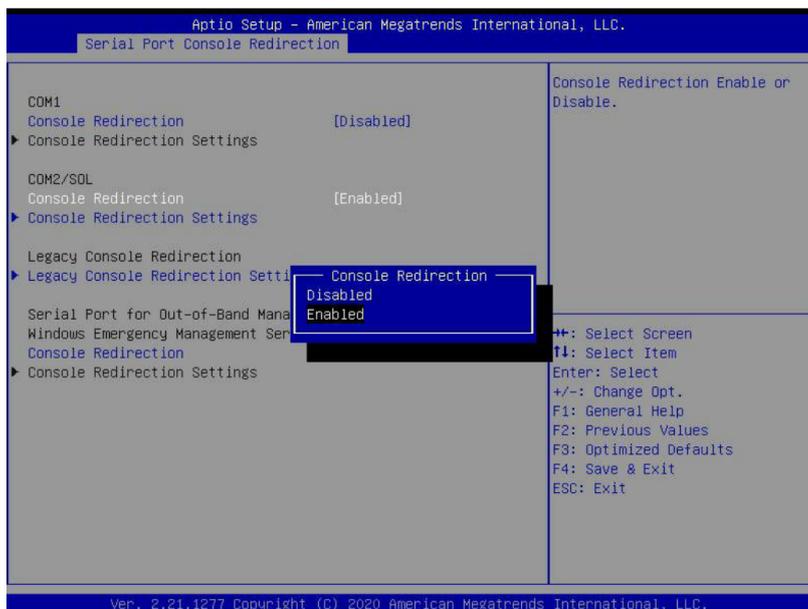
UEFI BIOS の設定

このセクションでは、UEFI BIOS の設定方法について説明します。

注： BMC を設定する前に、Arcserve アプライアンス サーバに直接接続されているモニタで BIOS を設定する必要があります。このプロセスは、BMC の BIOS 内でのみ実行できます。

以下の手順に従います。

1. Arcserve アプライアンス サーバの電源をオンにします。
2. システムの起動中に **Del** キーを押して BIOS 画面を表示します。
注： BIOS 内を移動するには、矢印キーを使用します。選択するには、**Enter** キーを押し、前の画面に戻るには、**Esc** キーを押しします。
3. BIOS セットアップメニューから **Advanced (詳細)** タブを選択します。
4. **Serial Port Console Redirection (シリアルポート コンソールリダイレクション)** を選択し、**Enter** キーを押します。
5. COM2/SOL の下の **Console Redirection (コンソールリダイレクション)** に移動し、**Enter** キーを押して、**Enabled (有効)** を選択します。



6. F4 キーを押し、保存して終了します。

BIOS が正常に設定されました。

BMC の IP アドレスの設定

このセクションには、以下のトピックが含まれます。

DHCP サーバを使用した DHCP IP アドレスの設定

このセクションでは、DHCP サーバを使用して DHCP IP アドレスを設定する方法について説明します

以下の手順に従います。

1. アプライアンス サーバで、MAC アドレス バーコード 付きの引き出し式 ID タグを見つけます。
2. MAC アドレス値を使用して、DHCP サーバに既知の登録済み DHCP IP アドレスを設定します。

POST 画面または BIOS から IP アドレスを確認できます。詳細については、「[BMC の IP アドレスを検索する方法](#)」を参照してください。

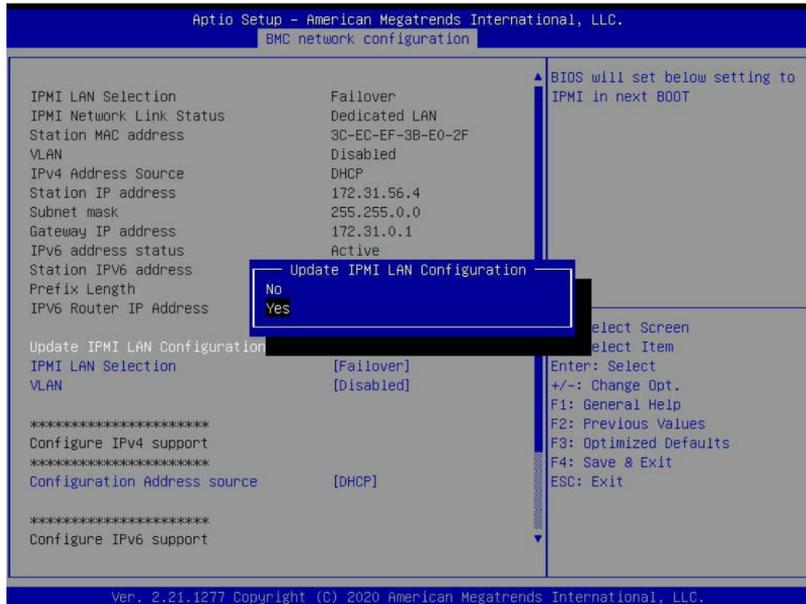
BIOS を使用した静的 IP アドレスの設定

このセクションでは、BIOS を使用して静的 IP アドレスを設定する方法について説明します。

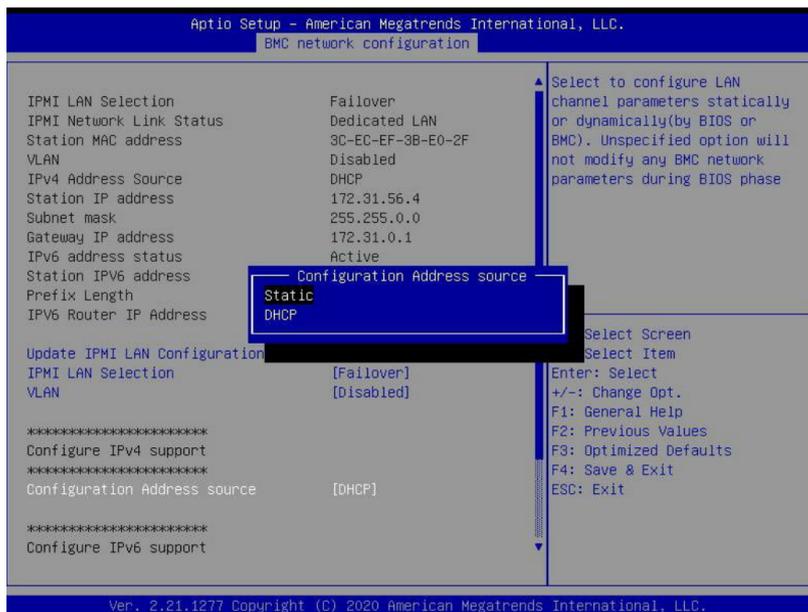
以下の手順に従います。

1. Arcserve アプライアンス サーバの電源をオンにします。
2. システムの起動中に Del キーを押して BIOS 画面を表示します。
3. **Server Management (サーバ管理)** タブの **BMC Network Configuration (BMC ネットワーク設定)** に移動し、Enter キーを押します。

BMC Network Configuration (BMC ネットワーク設定) 画面が表示されま

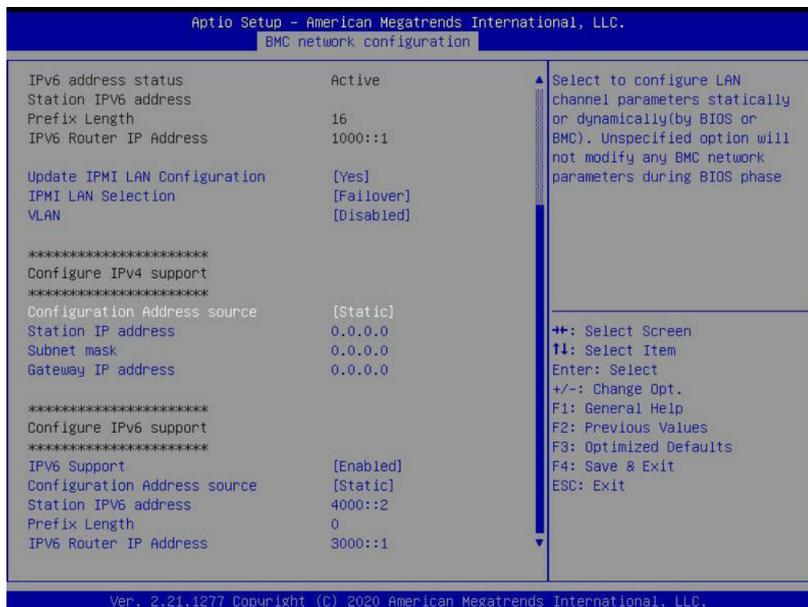


4. **Update IPMI LAN Configuration (IPMI LAN 設定の更新)** を選択し、Enter キーを押してから、**Yes (はい)** を選択します。
5. **Configuration Address source (設定アドレスソース)** を選択し、Enter キーを押してから、**Static (静的)** を選択します。



設定アドレスソースが静的に設定された後、 [Static IP Address (静的 IP アドレス)]、 [Subnet Mask (サブネット マスク)]、および [Gateway IP Address (ゲートウェイ IP アドレス)] のフィールドの値 0.0.0.0 を更新できます。

6. [Static IP Address (静的 IP アドレス)]、 [Subnet Mask (サブネット マスク)]、および [Gateway IP Address (ゲートウェイ IP アドレス)] に必要な値を入力し、Enter キーを押します。



7. F4 キーを押し、保存して終了します。

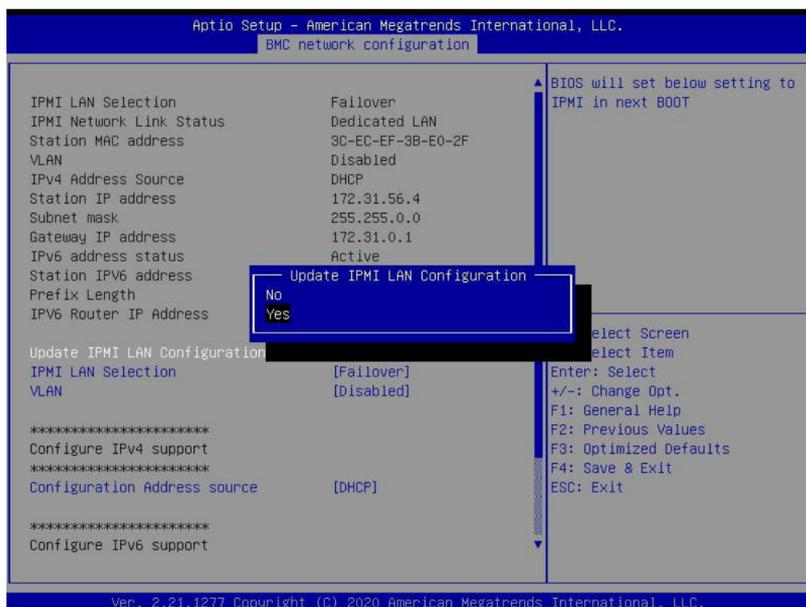
BMC 静的 IP アドレスが正常に設定されました。

BIOS を使用した BMC への接続

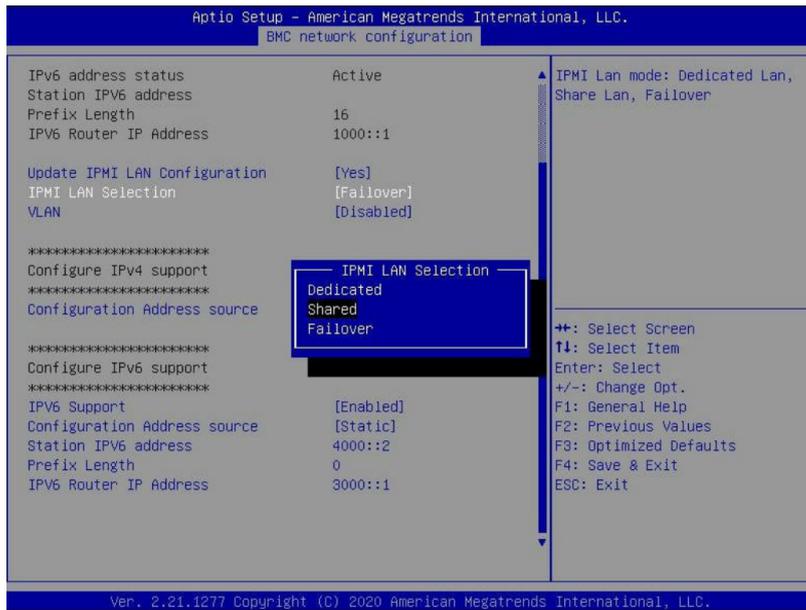
BMCに接続し、デバイスのBIOSメニューを起動するには、イーサネットケーブルの一端をラップトップまたはデバイスのイーサネットポートに接続します。次に、ケーブルのもう一方の端をサーバのIPMIまたはSHAREDポートに接続します。これで、BMCとデバイスは同じネットワークに接続されました。

以下の手順に従います。

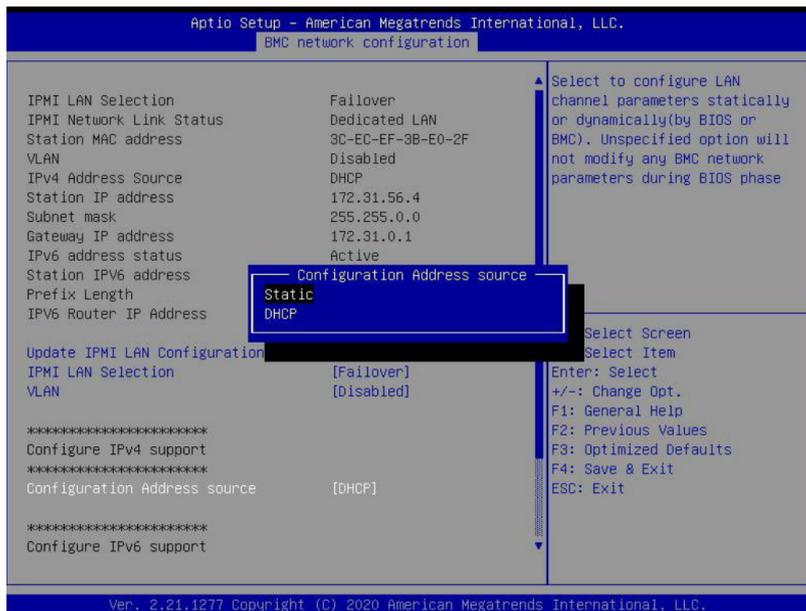
1. Arcserve アプライアンス サーバの電源をオンにします。
2. システムの起動中に **Del** キーを押して BIOS 画面を表示します。
3. **[Server Management (サーバ管理)]** タブの **[BMC Network Configuration (BMC ネットワーク設定)]** に移動し、**Enter** キーを押します。
[BMC Network Configuration (BMC ネットワーク設定)] 画面が表示されます。
4. **[Update IPMI LAN Configuration (IPMI LAN 設定の更新)]** を選択し、**Enter** キーを押してから、**[Yes (はい)]** を選択します。



5. **[IPMI LAN Selection (IPMI LAN の選択)]** を選択し、**Enter** キーを押してから、**[Shared (共有)]** を選択します。

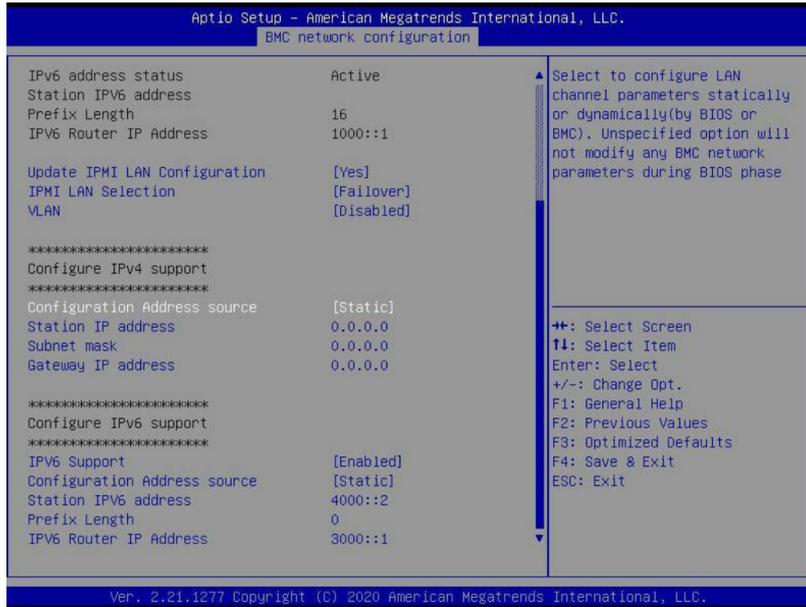


6. **Configuration Address source (設定アドレスソース)** を選択し、**Enter** キーを押してから、**Static (静的)** を選択します。



設定アドレスソースが静的に設定された後、**Static IP Address (静的 IP アドレス)**、**Subnet Mask (サブネット マスク)**、および **Gateway IP Address (ゲートウェイ IP アドレス)** のフィールドの値 0.0.0.0 を更新できます。

7. **Static IP Address (静的 IP アドレス)**、**Subnet Mask (サブネット マスク)**、および **Gateway IP Address (ゲートウェイ IP アドレス)** に必要な値を入力し、**Enter** キーを押します。



8. **F4** キーを押し、保存して終了します。

デバイスがBMCに正常に接続されました。

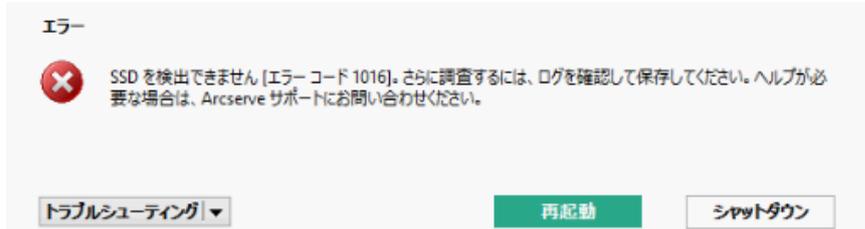
第7章: Arcserve アプライアンス のリストアまたは修復

このセクションには、以下のトピックが含まれます。

ファクトリリセットのデバッグ	125
--------------------------------------	-----

ファクトリリセットのデバッグ

このトピックでは、以下のエラーメッセージが表示された場合に、ファクトリリセットをデバッグする方法について説明します。



問題を解決するには、以下の手順を実行してください。

1. エラーメッセージで [トラブルシューティング] のドロップダウン オプションをクリックします。

以下のオプションが表示されます。

コマンド プロンプト

CMD (コマンド プロンプト) ダイアログ ボックスでは、いくつかの基本操作を行うことができます。たとえば、フォルダ内にファイルが存在するかどうかの確認、ファイルのコピーと削除、ディスクレイアウト情報の取得を実行できます。

ログの表示

[ログの表示] オプションでは、メモ帳にログを表示できます。ログを確認した後、 [ファイル]- 名前を付けて保存] をクリックしてログを保存し、後で利用することもできます。

ファクトリリセットの再起動

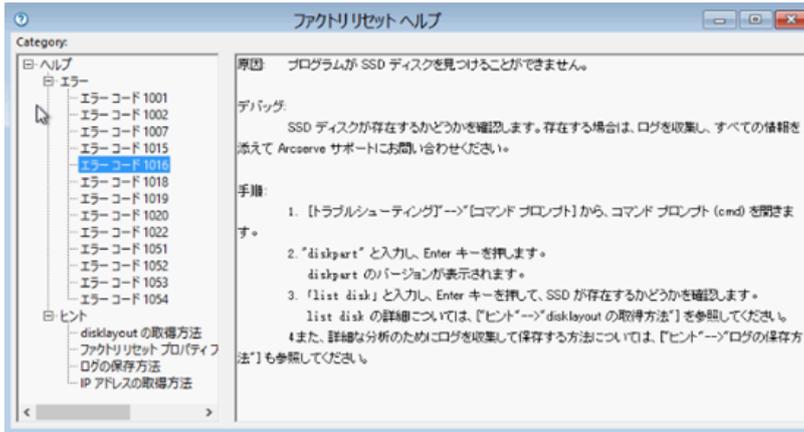
問題の解決後、このオプションを選択すると、ファクトリリセットを再起動できます。

ヘルプ

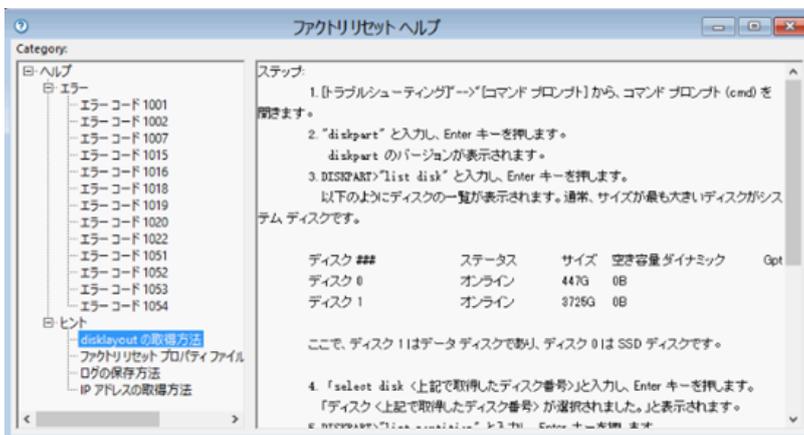
[ヘルプ辞書] ダイアログ ボックスには、エラーの原因、基本分析、および解決策に関する情報が表示されます。この問題を解決するには、以下の手順を実行してください。共通の操作についてのヒントも表示されます。たとえば、ディスクレイアウトの取得方法、ファクトリリセットのプロパティファイルコンテンツの取得方法、ログの保存方法などです。

2. 表示されるオプションの中から [ヘルプ] をクリックします。

画面には、複数のエラーコードとその詳細が表示されます。



3. エラーメッセージに表示されるエラーコードの [ヒント] に移動し、右側のパネルの下に表示されている指示に従います。



該当するエラーを選択し、ヒントに表示される指示に従うと、ファクトリリセットの問題を解決できます。

Arcserve アプライアンス のインストール

このセクションには、以下のトピックが含まれます。

Arcserve Backup 19.0 をインストールする方法

Arcserve Backup 19.0 は、アプライアンスに事前インストールされていません。Arcserve Backup 19.0 をインストールするには、デスクトップにある InstallASBU.iso ファイルをマウントします。

以下の手順に従います。

1. デスクトップで InstallASBU.iso ファイルを見つけてマウントし、アプリケーションのセットアップに移動して、管理者としてセットアップを実行します。

製品のインストール] ブラウザの右側の列で、Arcserve Backup for Windows のインストール] をクリックします。

前提条件コンポーネント] ダイアログボックスが表示されます。

2. [インストール] をクリックして、前提条件コンポーネントをインストールします。

前提条件コンポーネント] ダイアログボックスは、ターゲットコンピュータにインストールされている Arcserve Backup 前提条件コンポーネントが検出されなかった場合にのみ表示されます。

注: クラスタ対応環境内のアクティブノードに Arcserve Backup をインストールする場合は、アクティブノードが再起動する間に、アクティブノードからパッシブノードにクラスタリソースが移動されます。アクティブノードが再起動したら、元のアクティブノードにクラスタリソースを移動する必要があります。

3. [使用許諾契約] ダイアログボックスで、使用許諾契約の条件に同意して [次へ] をクリックします。
4. 表示されるプロンプトに従って、ダイアログボックスに必要なすべての情報を記入します。

以下のリストは、Arcserve Backup のインストールに関するダイアログボックス固有の情報について説明しています。

インストール/アップグレードの種類を選択ダイアログボックス

リモートインストールオプションを選択すると、Arcserve Backup を複数のシステムにインストールできます。

リモートインストールでは、ターゲットのリモートシステムを異なる Arcserve サーバタイプ、異なる Arcserve Backup エージェントとオプション、またはその両方で構成することができます。

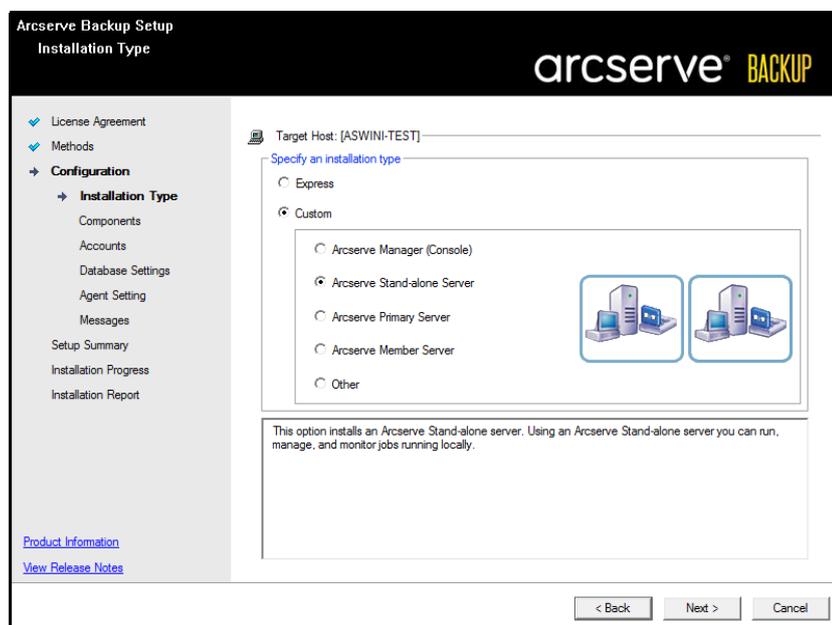
注: クラスタマシンのセットアッププログラムは Arcserve Backup ベース製品または Arcserve Backup エージェントのリモートインストールはサポートしていません。Arcserve Backup エージェント(たとえば Agent for Microsoft

SQL Server または Agent for Microsoft Exchange Server) に関するこのリモート インストールの制限は、仮想ホストを使用している場合のみ当てはまります。クラスタの物理ホストを使用した Arcserve Backup エージェントのリモート インストールはサポートされています。

[インストールの種類] ダイアログ ボックス

インストールの種類として [高速] または [カスタム] を選択することによって、インストールする Arcserve Backup コンポーネントの種類を指定できます。

注：以前のリリースからアップグレードする場合、インストールウィザードでは、現在の Arcserve 設定を検出し、新しいインストールに適切なインストール/アップグレードの種類を選択します。詳細については、「[Arcserve Backup サーバインストールのタイプ](#)」および「[Arcserve Backup サーバオプション](#)」を参照してください。



[コンポーネント] ダイアログ ボックス

ターゲット システムにインストールする Arcserve Backup コンポーネントを指定できます。

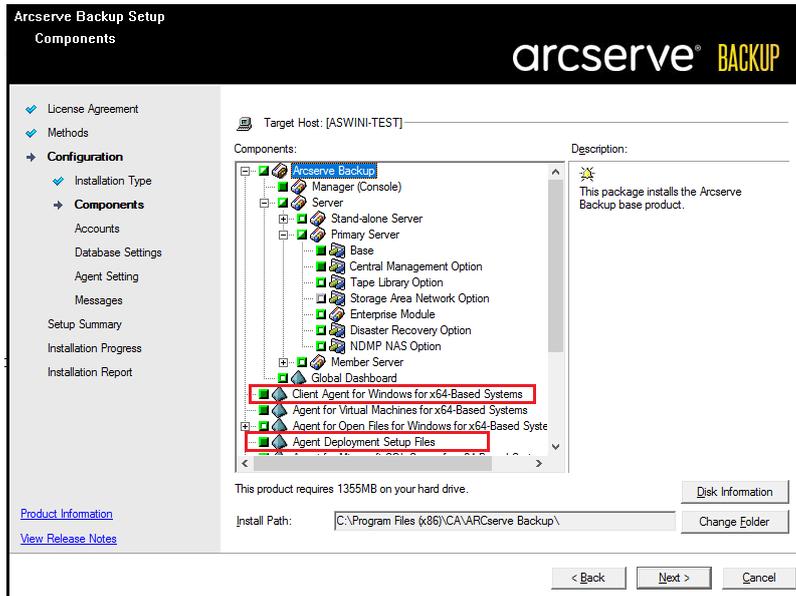
以下の点に注意してください。

- ◆ プライマリサーバをインストールするには、プライマリサーバに Arcserve Backup Central Management Option をインストールする必要があります。
- ◆ メンバサーバをインストールするには、インストールウィザードがネットワーク内の Arcserve Backup ドメイン名とプライマリサーバ名を検出できる必要があります。

あります。したがって、メンバサーバインストールを実行する前に、少なくとも1つのプライマリサーバインストールを完了しておく必要があります。

- ◆ Arcserve Backup オブジェクトまたはサーバオブジェクトを **製品の選択** ダイアログボックスでクリックすると、インストールウィザードでは、**[インストール/アップグレードの種類]**ダイアログボックスで指定したインストールの種類に関係なく、デフォルトのスタンドアロンサーバインストールコンポーネントが指定されます。正しいコンポーネントをインストールするには、サーバオブジェクトを展開し、インストールする Arcserve Backup サーバのタイプのオブジェクトを展開して、インストールするコンポーネントに対応するチェックボックスをオンにします。
- ◆ Agent Deployment は、Arcserve Backup をインストールした後で、Arcserve Backup エージェントを複数のリモートシステムにインストールしてアップグレードできるウィザード形式のアプリケーションです。この機能をサポートするには、セットアッププログラムで Setup ソースファイルを Arcserve Backup サーバにコピーする必要があります。インストールメディアのコンテンツを Arcserve Backup サーバにコピーするには、**[コンポーネント]**ダイアログボックスで Agent Deployment を選択する必要があります。Agent Deployment を選択すると、Arcserve Backup のインストールまたはアップグレードに要する時間がかなり長くなります。
- ◆ リモートインストールまたはサイレントインストールを実行する場合、Arcserve Backup Client Agent for Windows を Arcserve Backup ベース製品と同じディレクトリにインストールしないでください。
- ◆ Global Dashboard はプライマリサーバ、スタンドアロンサーバおよびメンバサーバにインストールできます。ただし、メンバサーバをセントラルプライマリサーバおよびブランチプライマリサーバとして機能するように設定することはできません。セントラルプライマリサーバおよびブランチプライマリサーバの詳細については、「[Dashboard ユーザガイド](#)」を参照してください。
- ◆ Windows Server Core を実行するコンピュータでは、以下の Arcserve Backup 製品のみをインストールできます。
 - メンバサーバおよびサポートされるオプション
 - Agent for Open Files
 - Agent for Virtual Machines
 - Client Agent for Windows
 - Disaster Recovery Option

以下の図では、Client Agent for Windows のデフォルトのインストールパスが表示されていて、Agent Deployment が指定されています。



【アカウント】ダイアログ ボックス

Arcserve Backup アカウントを設定し、**Arcserve Backup Web サービスのインストール**]を有効にするオプションを提供します。

セットアップ中に、クラスタ対応アプリケーションが環境内で実行されていることが検出された場合、Arcserve Backup をクラスタ対応環境にインストールするには、**クラスタ環境インストール**]オプションを選択して Arcserve Backup をインストールする共有ディスクのパスを指定します。

注： Arcserve Backup サーバ名と Arcserve Backup ドメイン名は、15 バイト以内である必要があります。合計 15 バイトの名前は、およそ 7 ~ 15 文字に相当します。

Arcserve Backup Web サービスは、UDP テープへのコピー タスクと Arcserve Backup の間のブリッジとして機能します。デフォルトでは、Arcserve Backup をインストールすると、**Arcserve Backup Web サービスのインストール**が有効になります。**Web サービス設定**のデフォルトのポート番号は8020です。このポート番号は変更できます。

Arcserve Backup Web サービスのインストール チェック ボックスをオフにして、Arcserve Backup Web サービスを無効にします。

Arcserve Backup のインストール後に **Arcserve Backup Web サービスのインストール**を有効化/変更できます。

注： Arcserve Backup Web サービスを Arcserve Backup ドメインのすべてのサーバにインストールする場合は、同じポート番号を指定します。Arcserve UDP は、同じポート番号を使用して、Arcserve Backup ドメインの Arcserve Backup プライマリサーバとメンバサーバの両方に接続します。

以下の手順に従います。

1. コマンドラインから Arcserve Backup ベース インストールパスに移動します。
2. コマンド プロンプトで、以下のコマンドを入力します。

Bconfig -c

{Arcserve Backup> アカウント}ダイアログ ボックスが表示されます。

3. Web サービスを設定または更新します。

データベースの設定ダイアログ ボックス

Arcserve Backup データベースを設定できます。

このダイアログ ボックスで、データベース アプリケーション(Arcserve Backup のデフォルト のデータベースまたは Microsoft SQL Server) を指定するか、必須フィールドの入力を完了した後、**[次へ]**をクリックします。

注：Unicode ベースの東アジア言語文字(JIS2004 など) を含むデータを保護する必要がある場合は、Arcserve Backup のデータ検索および並べ替えを可能にするために SQL 照合順序を有効にする必要があります。これを行うには、**[東アジア言語の照合順序]**をクリックしてドロップダウン リストから言語を選択します。

Arcserve Backup Setup
Database Settings
The database stores critical information about Arcserve Backup and its operations.

arcserve BACKUP

License Agreement
Methods
Configuration
Installation Type
Components
Accounts
Database Settings
Agent Setting
Messages
Setup Summary
Installation Progress
Installation Report

Product Information
View Release Notes

Target Host: [-TEST]
Choose a database type: Arcserve Default Database

Specify the installation path for Arcserve default database
 Default installation path: C:\Program Files (x86)\Microsoft SQL Server
 Select a custom path

Data file path for Arcserve default database
 Default installation path: C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.ARCSEVER\DB\MSSQL\DATA
 Select a custom path

SQL Language Collation Setting
 Default collation
 East Asian collation: Chinese_PRC

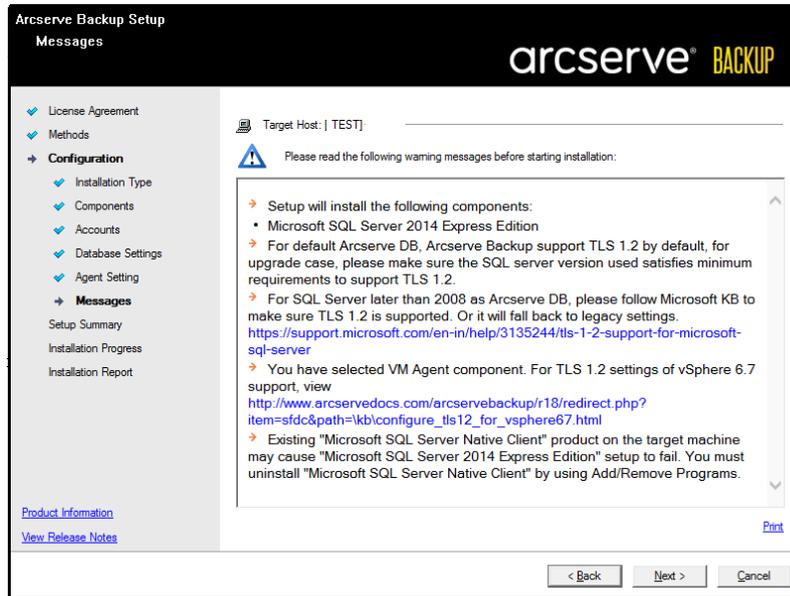
Installation Path for Catalog Files: C:\Program Files (x86)\CA\Arcserve Backup\CATALOG.DB\

< Back Next > Cancel

[メッセージ] ダイアログ ボックス

[メッセージ] ダイアログ ボックスでメッセージを確認し、この時点で問題の解決を試みる必要があります。

以下は、重要な警告メッセージ]ダイアログ ボックスを示しています。



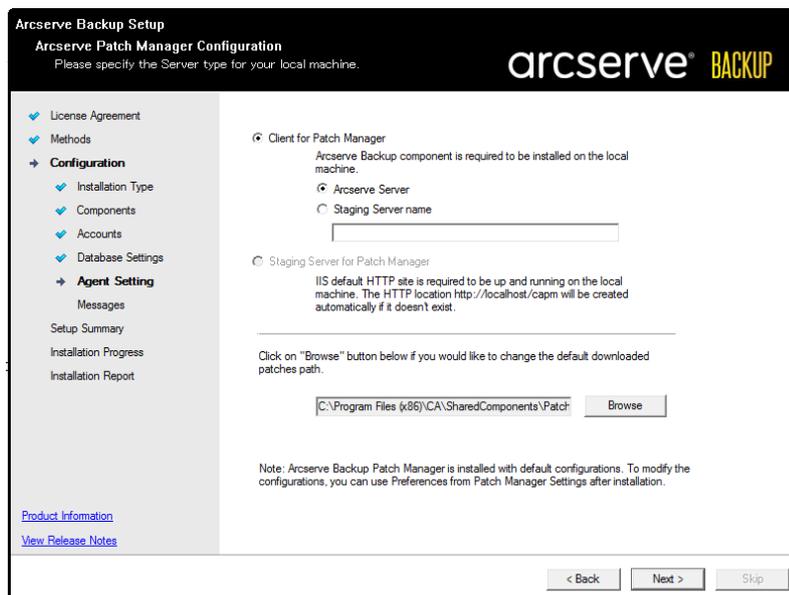
【セットアップ サマリ]ダイアログ ボックス

インストールするコンポーネントを変更するには、変更するインストールオプションが表示されているダイアログ ボックスに戻るまで **戻る]** ボタンをクリックしてください。

【インストールレポート]ダイアログ ボックス

選択したコンポーネントで設定が必要な場合は、インストールの最後に設定ダイアログ ボックスが表示されます。すぐにコンポーネントを設定することも、後から **【デバイス環境設定]** または **【Enterprise Module 環境設定]** を使用して設定することもできます。たとえば、単一ドライブのオートローダを使用している場合は、セットアップで **【インストール サマリ]ダイアログ ボックス** でメッセージをダブルクリックすることで、該当する **【デバイス環境設定]** を起動するように指定することができます。

以下に、[インストールレポート]ダイアログ ボックスを示します。
Agent for Microsoft SQL Server で環境設定が必要とされています。



注： Arcserve Backup のインストール時に、サーバの再起動が必要になる場合があります。これは、すべてのファイル、サービス、およびレジストリの設定がオペレーティングシステムレベルで更新されたかどうかによって決まります。

インストール サマリ]ダイアログ ボックス

選択したコンポーネントで設定が必要な場合は、インストールの最後に設定ダイアログ ボックスが表示されます。すぐにコンポーネントを設定することも、後から [デバイス環境設定] または [Enterprise Module 環境設定] を使用して設定することもできます。たとえば、単一ドライブのオートローダを使用している場合は、セットアップで [インストール サマリ] ダイアログ ボックスでメッセージをダブルクリックすることで、該当する [デバイス環境設定] を起動するように指定することができます。

5. [インストール サマリ]ダイアログ ボックスで [完了] をクリックしてインストールを完了します。

10024BU-10048BU シリーズ アプライアンスの設置方法

アプライアンスは、限られた領域のみに設置することを目的としています。初期設定およびメンテナンスは、専門の担当者が実行する必要があります。

完全な設置プロセスについては、「[10024BU-10048BU のアプライアンスの設置](#)」を参照してください。

10048DR-10576DR シリーズ アプライアンスの設置方法

アプライアンスは、限られた領域のみに設置することを目的としています。初期設定およびメンテナンスは、専門の担当者が実行する必要があります。

完全な設置プロセスについては、「[10048DR-10576DR のアプライアンスの設置](#)」を参照してください。

9012-9048 シリーズ アプライアンスの設置方法

アプライアンスは、限られた領域のみに設置することを目的としています。初期設定およびメンテナンスは、専門の担当者が実行する必要があります。

完全な設置プロセスについては、「[9012-9048 のアプライアンスの設置](#)」を参照してください。

9072-9504DR シリーズ アプライアンスの設置方法

アプライアンスは、限られた領域のみに設置することを目的としています。初期設定およびメンテナンスは、専門の担当者が実行する必要があります。

完全な設置プロセスについては、「[9072-9504DR のアプライアンスの設置](#)」を参照してください。

X シリーズ アプライアンスの設置方法

アプライアンスは、限られた領域のみに設置することを目的としています。初期設定およびメンテナンスは、専門の担当者が実行する必要があります。

完全な設置プロセスについては、「[X シリーズ アプライアンスの設置 - コンピュート ノード](#)」および「[X シリーズ アプライアンスの設置 - ストレージ ノード](#)」を参照してください。

10024BU-10576DR シリーズ アプライアンスでの Arcserve UDP ファクトリリセットの適用

このセクションでは、10000 シリーズ アプライアンスでファクトリリセットを実行する方法について説明します。

UDP ファクトリリセット オプションを使用すると、Arcserve アプライアンス 10000 シリーズをクリーンで設定されていないステータスに戻すことができます。

注：UDP ファクトリリセットの実行中に、**[preserve the backup data (バックアップデータの保持)]** チェックボックスを選択することもできます。

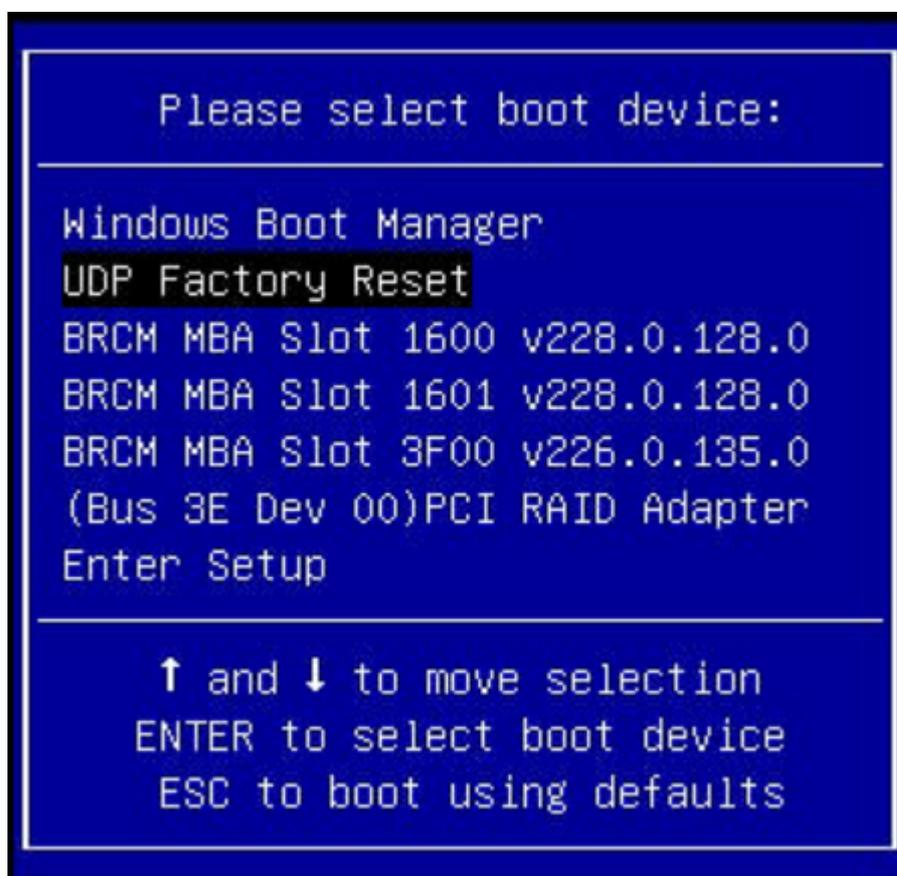
10000 シリーズ アプライアンスのファクトリリセットを実行するには、以下のいずれかの方法を使用します。

BIOS からのファクトリリセット

このセクションでは、BIOS から UDP ファクトリリセットを実行する方法について説明します。

以下の手順に従います。

1. Arcserve アプライアンスの電源をオンにします。
2. キーボードの F11 キーを押して、ブートメニューを起動します。
3. **[UDP Factory Reset (UDP ファクトリリセット)]** ブートオプションを選択します。



ファクトリリセット ウィザードが表示されます。

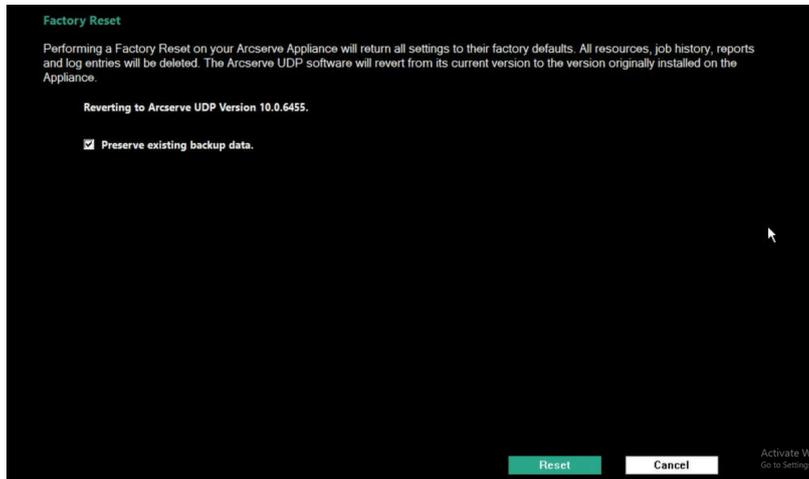
4. **[リセット]** をクリックします。

Notes:

- デフォルトで、**既存のバックアップデータを保持** チェックボックスがオンになっています。リセット中にすべてのバックアップデータが保持され

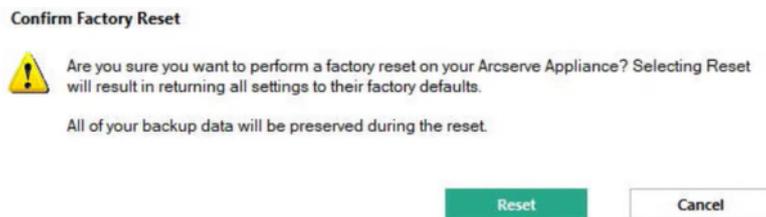
ます。元のオペレーティングシステムの C:\ ボリュームのみが再構築されます。

- **既存のバックアップデータを保持**] チェックボックスをオフにすると、リセット中にすべてのバックアップデータが削除されます。元のオペレーティングシステムの C:\、X:\、Y:\ の各ボリューム上のデータが再構築されます。

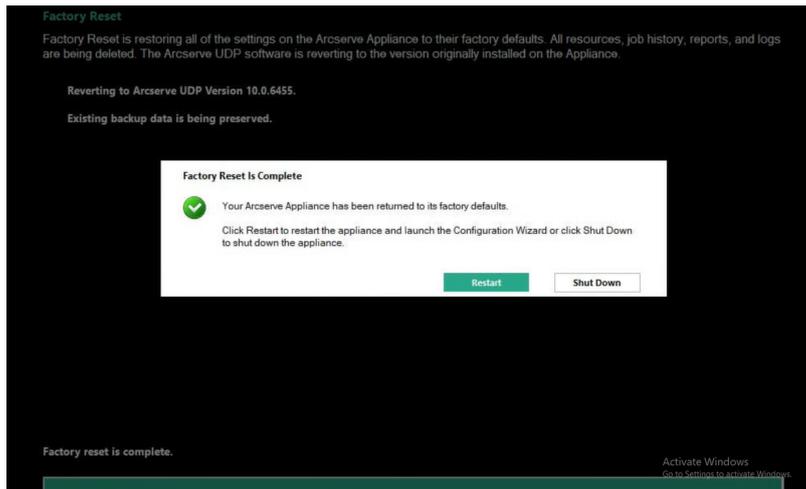


確認のダイアログボックスが表示されます。

5. ファクトリリセットを実行するには、**[リセット]** をクリックします。



6. ファクトリリセットが完了したら、以下のいずれかのアクションを実行できます。
 - アプライアンスを再起動するには、**再起動**] をクリックします。
 - アプライアンスを閉じるには、**シャットダウン**] をクリックします。



10000 シリーズ アプライアンスの BIOS からのファクトリリセットが正常に完了しました。

Arcserve UDP コンソールからのファクトリリセット

このセクションでは、Arcserve UDP コンソールからファクトリリセットを実行する方法について説明します。

以下の手順に従います。

1. Arcserve UDP コンソールにログインします。
2. **設定** > **ファクトリリセット** に移動します。



3. **ファクトリリセット** 画面で、**ファクトリリセットを実行** をクリックします。

Notes:

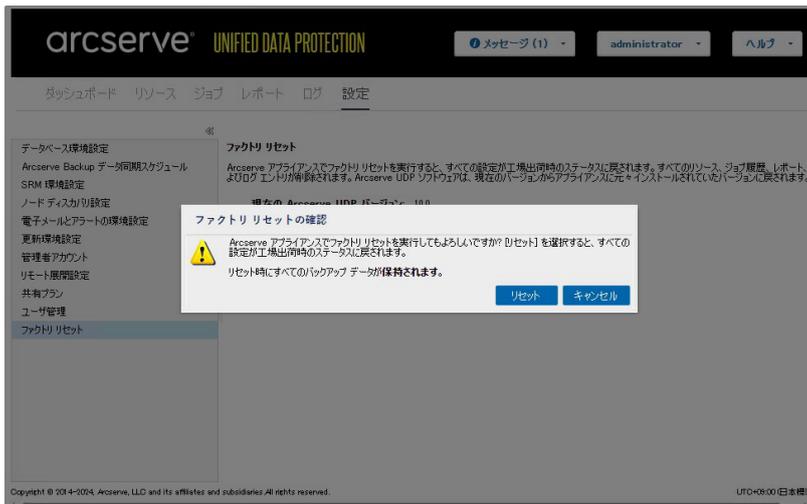
- デフォルトで、**既存のバックアップデータを保持** チェックボックスがオンになっています。リセット中にすべてのバックアップデータが保持されます。元のオペレーティングシステムの C:\ ボリュームのみが再構築さ

れます。

- **既存のバックアップ データを保持**] チェック ボックスをオフにすると、リセット中にすべてのバックアップ データが削除されます。元のオペレーティング システムの C:\、X:\、Y:\ の各 ボリューム上のすべてのデータが再構築されます。

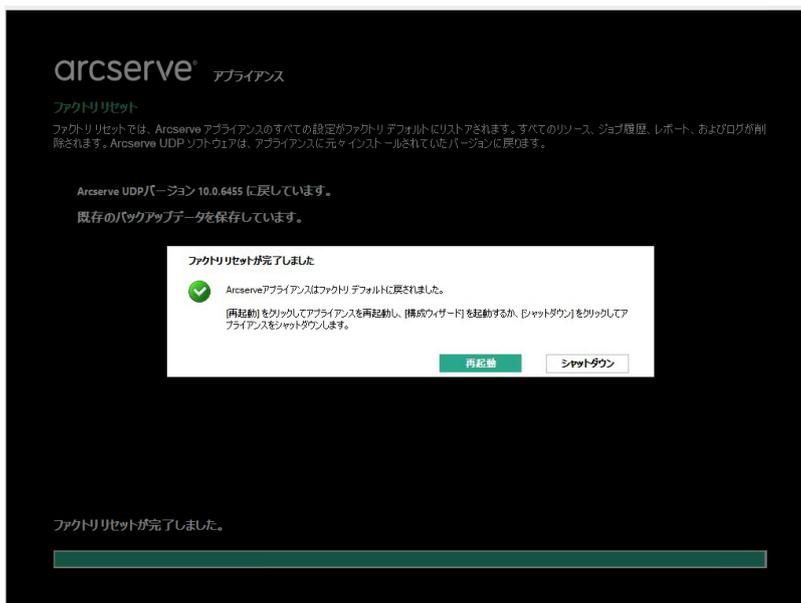
確認のダイアログ ボックスが表示されます。

4. ファクトリリセットを実行するには、**[リセット]** をクリックします。



5. ファクトリリセットが完了したら、以下のいずれかのアクションを実行できます。

- アプライアンスを再起動するには、**再起動**] をクリックします。
- アプライアンスを閉じるには、**シャットダウン**] をクリックします。



10000 アプライアンスの Arcserve UDP コンソールからのファクトリリセットが正常に完了しました。

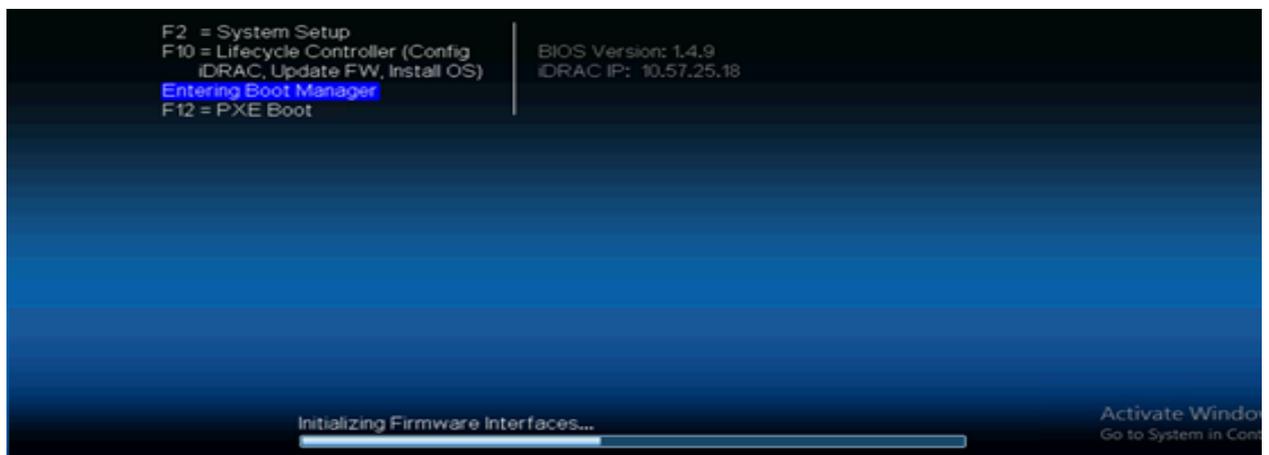
9012 - 9504 DR シリーズ アプライアンスのブート オプションを使用した Arcserve UDP ファクトリリセットの適用

UDP ファクトリリセットは、Arcserve アプライアンス 9012-9504DR シリーズのブートメニューから適用することができます。UDP ファクトリリセットを使用して、Arcserve アプライアンス 9012-9504DR シリーズをクリーンな未設定の状態に戻すことができます。

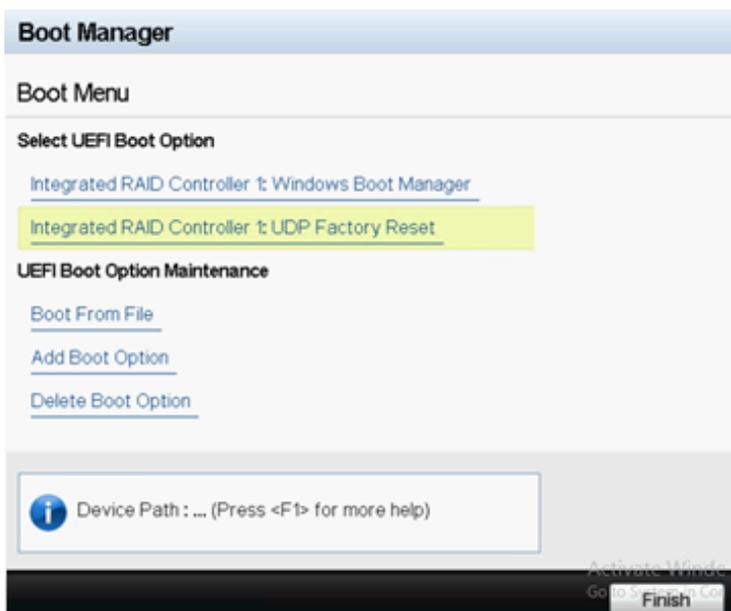
注：UDP ファクトリリセットの実行中に、バックアップデータを保持するオプションを選択することもできます。

以下の手順に従います。

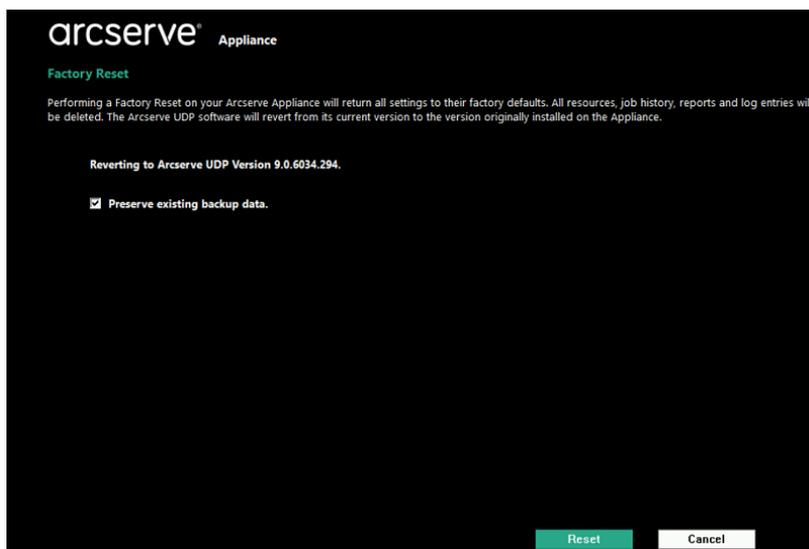
1. キーボードの F11 キーを押して、ブートメニューを起動します。



2. [Integrated RAID Controller 1: UDP Factory Reset (統合 RAID コントローラ 1: UDP ファクトリリセット)] ブート オプションを選択します。



ファクトリリセットに関するページが表示されます。

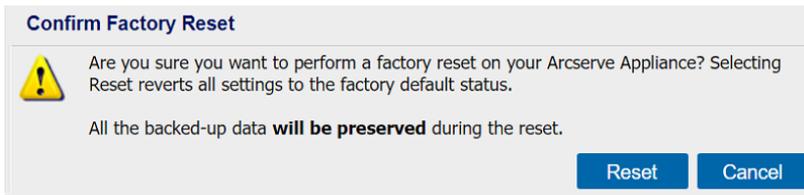


注：

- デフォルトで、**既存のバックアップデータを保持**]オプションが選択されています。元のオペレーティングシステムの C:\ ボリュームのみが再構築されます。X:\ volume および Y:\ volume のデータは変更されないままになります。
- **既存のバックアップデータを保持**]オプションの選択をオフにすると、元のオペレーティングシステムの C:\、X:\、Y:\ の各ボリューム上のすべてのデータが再構築されます。

3. **[リセット]** をクリックします。

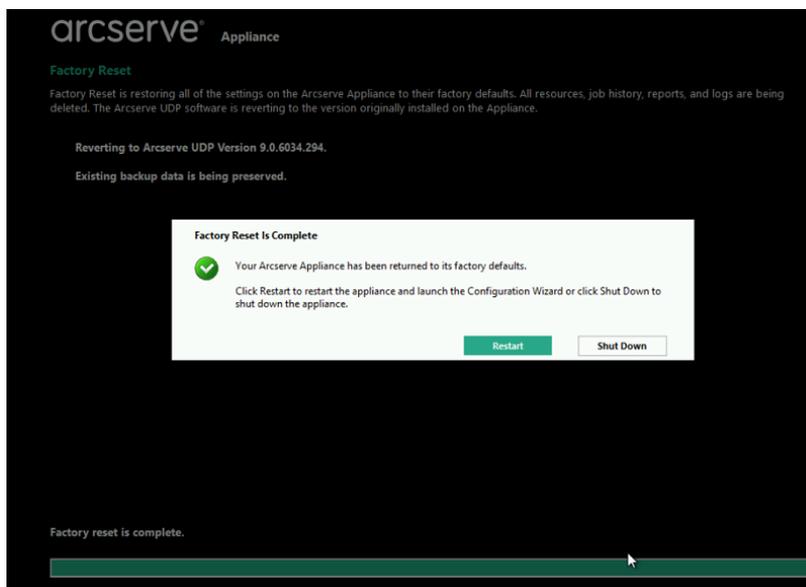
確認のダイアログボックスが表示されます。



[キャンセル]をクリックすると、Arcserve アプライアンス ユニット を再起動できません。

4. ファクトリリセットが完了した後、以下のいずれかの操作を実行できます。

- ◆ **再起動**]をクリックしてアプライアンスを再起動します。
- ◆ **シャット ダウン**]をクリックしてアプライアンスを閉じます。



X シリーズ アプライアンスのブート オプションを使用した Arcserve UDP ファクトリリセットの適用

UDP ファクトリリセットは、Arcserve アプライアンス X シリーズのブート メニューから適用することができます。UDP ファクトリリセットを使用して、Arcserve アプライアンス X シリーズをクリーンな未設定の状態に戻すことができます。

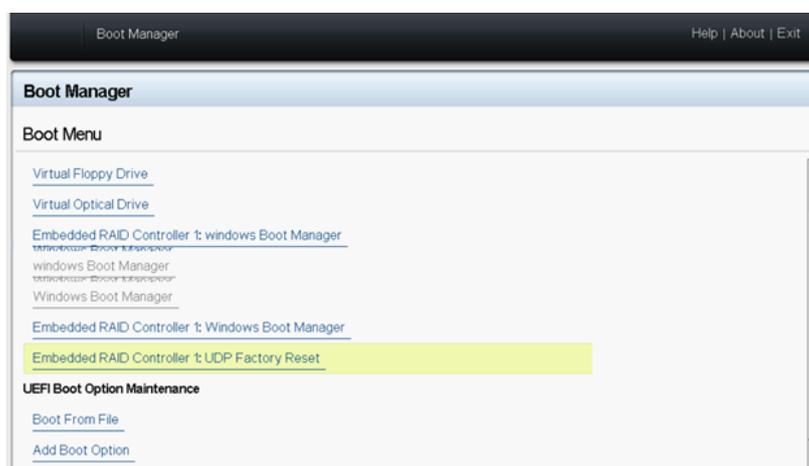
注：UDP ファクトリリセットの実行中に、バックアップ データを保持するオプションを選択することもできます。

以下の手順に従います。

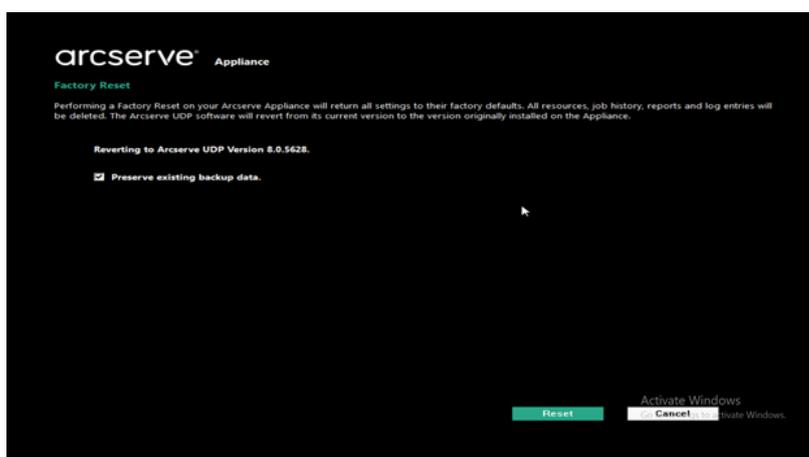
1. キーボードの F11 キーを押して、ブート メニューを起動します。



2. **組み込み RAID コントローラ 1: UDP ファクトリリセット**]ブート オプションを選択します。



ファクトリリセットに関するページが表示されます。



注:

- デフォルトで、**既存のバックアップデータを保持**]オプションが選択されています。元のオペレーティングシステムの C:\ ボリュームのみが再構築されます。X:\ volume および Y:\ volume のデータは変更されないままになります。
- **既存のバックアップデータを保持**]オプションの選択をオフにすると、元のオペレーティングシステムの C:\、X:\、Y:\ の各ボリューム上のすべてのデータが再構築されます。

3. **[リセット]**をクリックします。

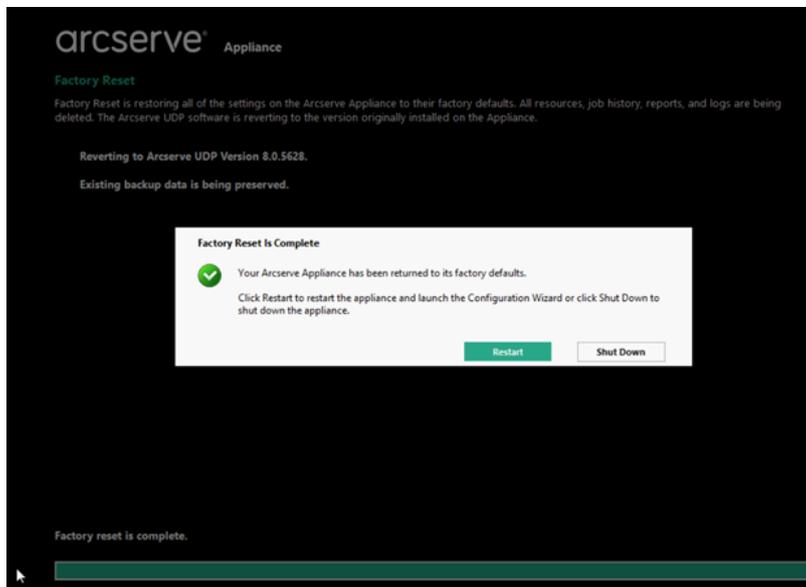
確認のダイアログボックスが表示されます。



[キャンセル]をクリックすると、Arcserve アプライアンス ユニットを再起動できません。

4. ファクトリリセットが完了した後、以下のいずれかの操作を実行できます。

- ◆ **再起動]**をクリックしてアプライアンスを再起動します。
- ◆ **シャット ダウン]**をクリックしてアプライアンスを閉じます。

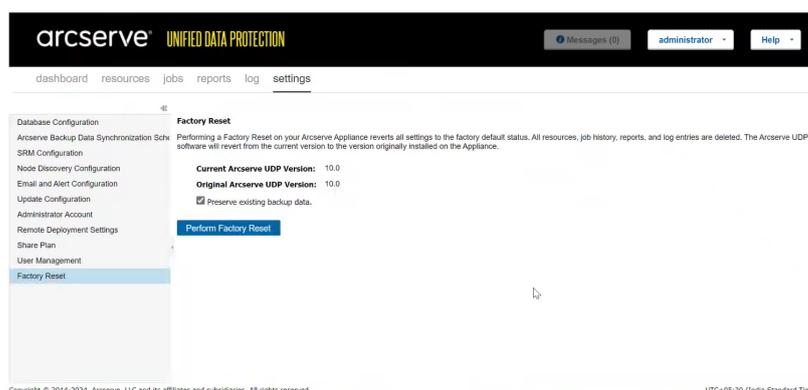


環境設定の消去およびアプライアンスファクトリリセットの適用

ファクトリリセットを使用して、Arcserve アプライアンス をクリーンな未設定の状態に戻すことができます。ファクトリリセットは Arcserve UDP コンソールから適用できます。

以下の手順に従います。

1. Arcserve UDP コンソールの **設定** タブで **ファクトリリセット** をクリックします。



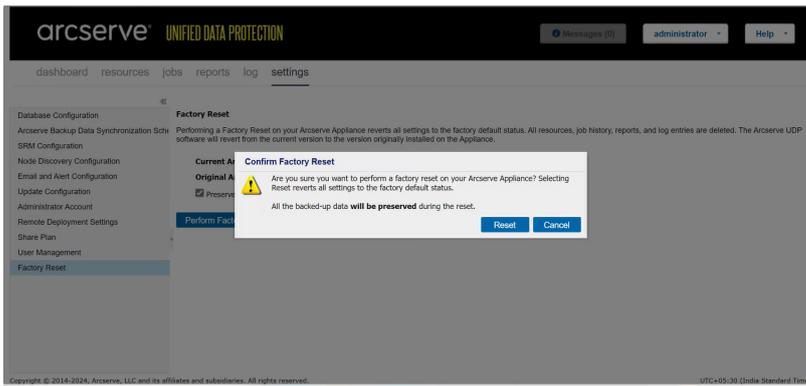
デフォルトではすべてのバックアップ データが保存されます。

注：Arcserve UDP には、**既存のバックアップ データを保持** オプションが用意されており、既存のデータストアを保存することができます。

- ◆ **既存のバックアップ データを保持** オプションを選択した場合、C:\ volume のみが再構築されます。X:\ volume および Y:\ volume のデータは変更されないままになります。
- ◆ **既存のバックアップ データを保持** オプションを選択しない場合、C:\, X:\ および Y:\ が再構築されます。

2. **ファクトリリセットを実行** をクリックします。

確認のダイアログ ボックスが表示されます。



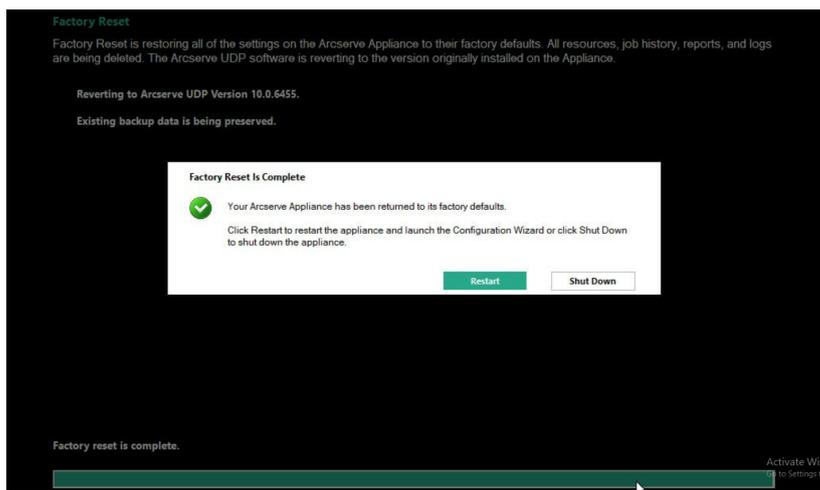
3. 確認のダイアログボックスで、**[リセット]**をクリックすると、ファクトリリセットが開始されます。

アプライアンスマシンが再起動され、ファクトリリセットが以下のように実行されます。



ファクトリリセットの完了により、確認のダイアログボックスが表示されます。

4. 確認ダイアログボックスで、以下のいずれかのオプションを実行します。
 - ◆ **[再起動]**をクリックしてアプライアンスを再起動します。
 - ◆ **[シャットダウン]**をクリックしてアプライアンスを閉じます。



ハードドライブの取り外しおよび交換

Arcserve アプライアンスを使用すると、ハードドライブの1つに障害が発生した場合、残りのドライブがすぐに起動し、データは失われずにアプライアンスが引き続き正常に動作します。そのため、複数のハードドライブの障害に関連する問題に対して防御するには、データが失われる可能性を最小限に抑えるためにできる限り早くハードドライブを置き換える必要があります。

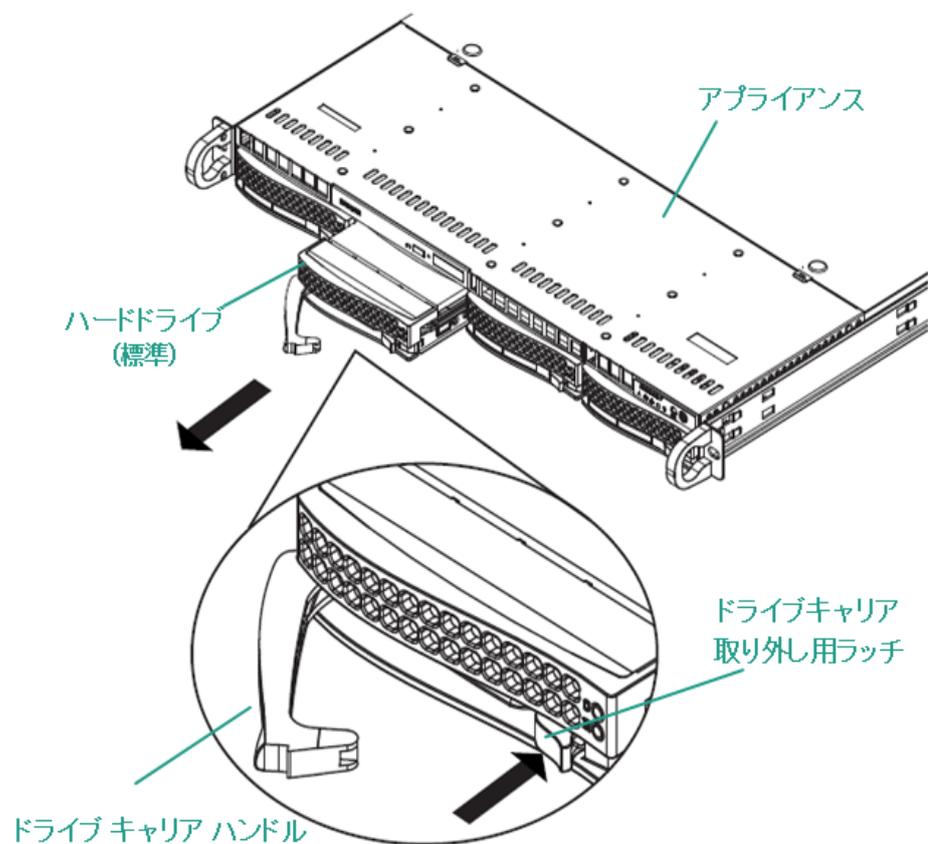
Arcserve アプライアンスには、4つのハードドライブ キャリアが含まれており、左から右に0、1、2、3とラベルが付けられています。一度に複数のハードドライブを交換する場合、各ドライブ キャリアでどのドライブが交換されたかがわかるように、交換したハードドライブにラベルを付ける必要があります。アプライアンスから取り外したハードドライブにもラベルを付け、どのドライブ キャリアによって占有されていたかがわかるようにします。

重要: ハードドライブは静電気に敏感なデバイスであり、損傷しやすいため、ハードドライブを扱う場合は適切な保護対策を講じてください。

- 静電気の放電を防ぐためにリストトラップを着用してください。
- 交換用ハードディスクを帯電防止のパッケージ袋から取り出す前に、接地された物体に触れるようにします。
- ハードドライブを扱う際は常に端のみを持つようにし、底面の露出している部品には一切触れないでください。

以下の手順に従います。

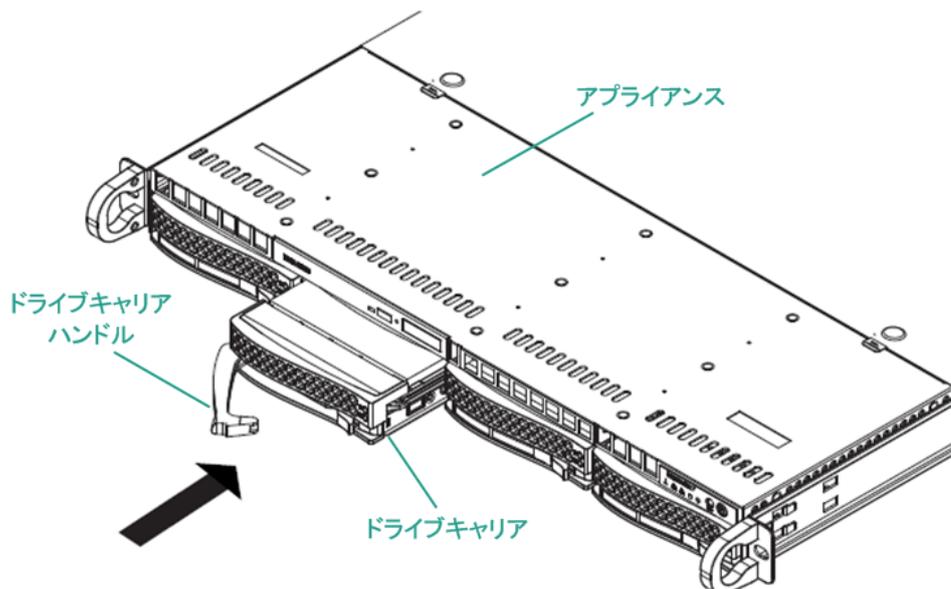
1. ドライブホルダーにアクセスするには、まずフェイスプレートを取り外す必要があります。
 - a. フェイスプレートのロックを解除します。
 - b. 取り外し用つまみを押してフェイスプレートピンを格納します。
 - c. フェイスプレートを慎重に取り外します(両手を使用)。
2. ドライブキャリアの取り外し用ラッチを押します。これにより、ドライブキャリアハンドルが展開されます。



3. ハンドルを使用して、アプライアンスの前面からドライブ キャリアを引き出します。ハードドライブは、アプライアンスに対する取り付け/取り外しを簡単に行うことができるよう、ドライブ キャリアにマウントされています。これらのキャリアは、ドライブ ベイに適切な換気が行われるようにするのにも役立ちます。

重要: 短時間の場合を除き(ハードドライブの交換など)、ドライブ キャリアが完全に設置されていない状態でアプライアンスを稼働させることはしないでください。

4. 古いハードドライブをドライブ キャリアから取り外し、新しいハードドライブを設置します。その際、交換用ハードドライブが正しい向きであるかに注意し、ラベルが上部、部品が下部にきていることを確認します。
5. ドライブトレイがアプライアンスに完全に設置されるまでスライドし、ドライブ キャリアハンドルを閉じて固定します。



6. ドライブを返却する場合は、返却に関する指示を Arcserve サポート から取得します。

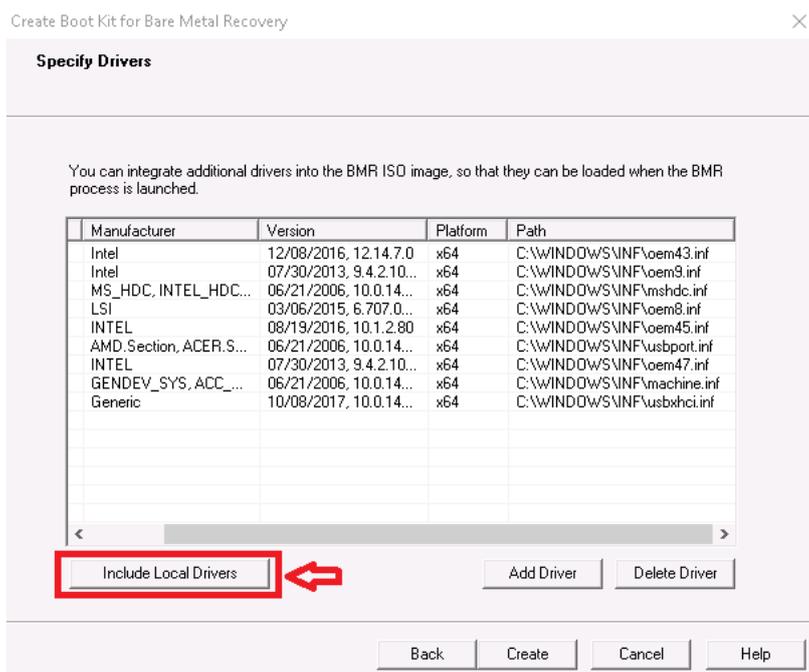
9012-9504DR シリーズ アプライアンスでのデータを保存しないベアメタル復旧(BMR)の実行

Arcserve アプライアンスでは、Arcserve UDP ブート キット を使用して、ベアメタル復旧を実行できます。

以下の手順に従います。

1. アプライアンスで Arcserve UDP ブートキット ウィザード を実行し、x64 プラットフォームでブート可能な BMR ISO イメージまたは USB スティックを生成します。

注：ISO イメージにはローカルドライバを含める必要があります。ローカルドライバを含めるには、**[ベアメタル復旧用のブートキットの作成]** ウィンドウで **[ローカルドライバを含む]** オプションを選択します。ブートキットの作成方法の詳細については、この[リンク](#)を参照してください。



2. BMR ISO イメージまたは USB スティックを使用して、Arcserve アプライアンスを起動します。

Arcserve ベアメタル復旧 のセットアップ画面が表示されます。

3. 必要な言語を選択して、**次へ]**をクリックします。



4. **Arcserve Unified Data Protection のバックアップからのリストア]** オプションを選択し、**次へ]**をクリックします。

arcserve® bare metal recovery

Bare Metal Recovery(BMR)
- Select the type of backup for BMR

Select type of restore source:

Restore from a Arcserve Unified Data Protection backup
Use this option to perform a restore from either a backup destination folder or a data store.

Recover from a virtual machine
Use this option to perform a virtual-to-physical (V2P) restore from a virtual machine created by Virtual Standby or Instant VM

Source is on a VMware machine

Source is on a Hyper-v machine

復旧ポイントの選択]ウィザードのウィンドウが表示されます。

5. **参照]**をクリックして、**復旧ポイント サーバから参照]**を選択します。

Bare Metal Recovery(BMR)
- Select a Recovery Point

The top pane displays all backed up machines and their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery point to continue.

Note: By default, only the backed up machines that are detected from local volumes are listed here. After a new removable disk is attached or detached, you can click "Refresh" the mypane list. You can also click "Browse" to add any backed up machines from the remote shared folder or the data store.

If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or the IP address is incorrect. If necessary, you can perform the following:
Click [here](#) to launch the load driver utility
Click [here](#) to launch the network configuration utility

The following backed up machines are detected:

Backed up Information

Host Name:

Operating System:

DNS Suffix:

Source:

Browse from network/local path

The following recovery points are detected for the specified machine. Select a recovery point as:

6 Network Adapter(s) Detected

Intel(R) 1350 Gigabit Network Connection
- IP Address: 10.10.255.255
- Status: Connected

Intel(R) 1350 Gigabit Network Connection #2
- IP Address: 0.0.0.0
- Status: Disconnected

[ノードの選択] ウィンドウが表示されます。

6. 復旧ポイント サーバのホスト名、ユーザ名、パスワード、ポート、およびプロトコルを入力します。
7. **接続]** をクリックします。
8. 接続が確立されたら、 **OK]** をクリックします。

Select Node

Enter the Recovery Point Server credentials and click "Connect" to connect to the server and retrieve the data store and node list.

Host Name: appliance7501 Port: 8014

User Name: administrator Protocol: HTTP HTTPS

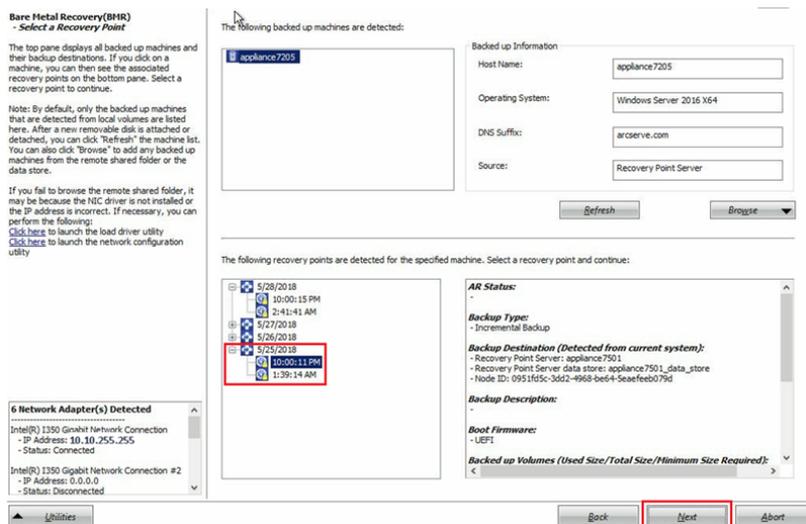
Password: [masked]

Data stores and nodes protected on this server:

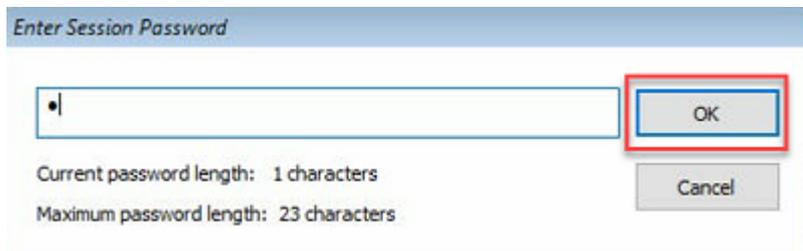
Property	Description
Node	appliance7205
DNS Suffix	arcserve.com
Node ID	0951fd5c-3dd2-4968-be64-5eaef...

[ベアメタル復旧 (BMR) - 復旧ポイントの選択] ダイアログ ボックスが表示されます。

9. リストアする復旧ポイントを選択して、 **次へ]** をクリックします。

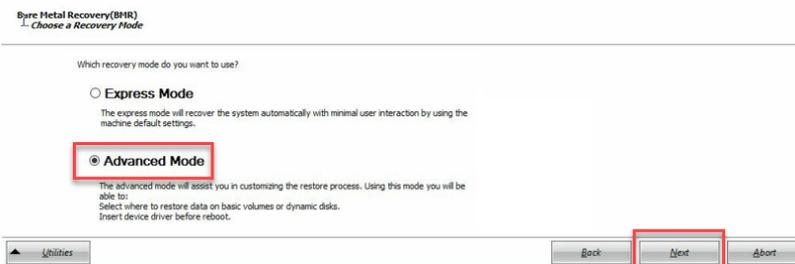


10. (オプション) 要求された場合はセッションパスワードを入力し、[OK]をクリックします。



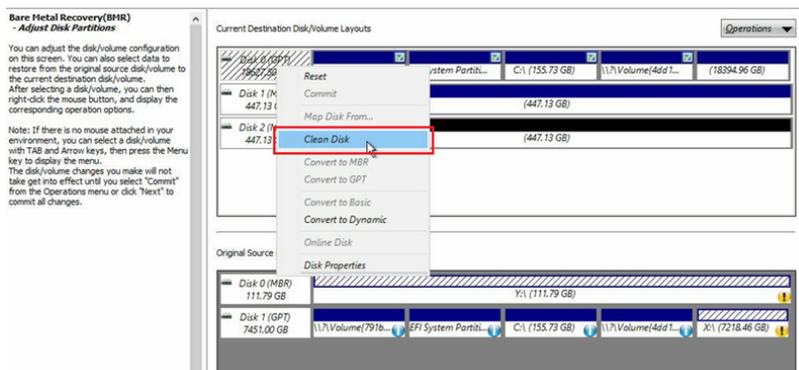
[ペアメタル復旧 (BMR) - 復旧モードの選択] ダイアログボックスが表示されます。

11. [拡張モード] を選択し、[次へ] をクリックします。

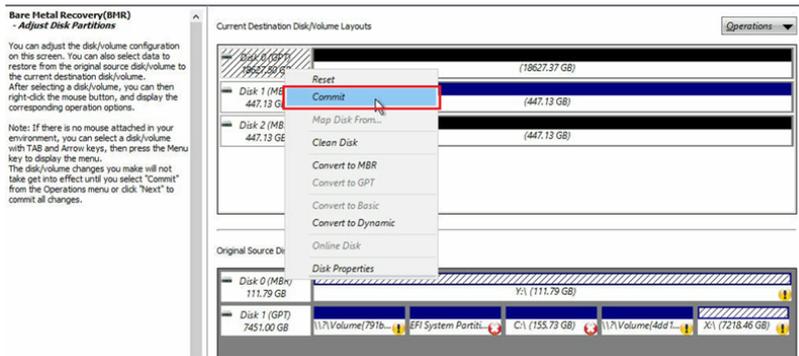


ベアメタル復旧 (BMR) - ディスクパーティションの調整] ダイアログボックスが表示されます。

12. 使用可能な最大の GUID パーティション テーブル (GPT) ディスクを右クリックし、**ディスクの消去**] をクリックします。

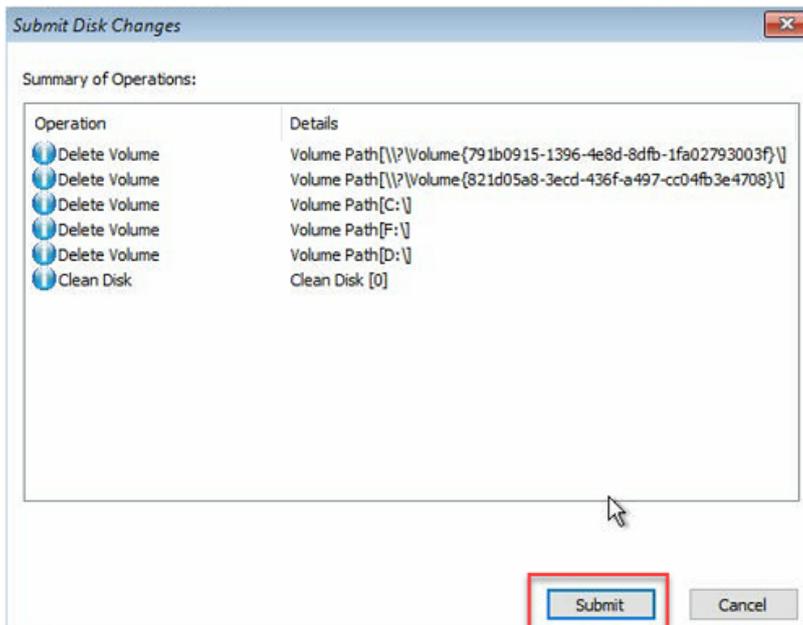


13. ディスクを消去した後、同じディスクを右クリックして **コミット**] をクリックします。

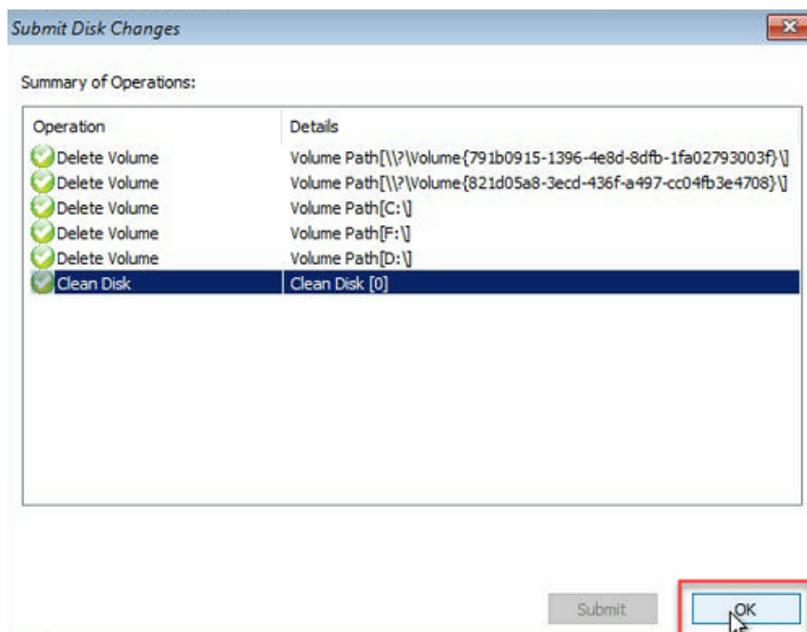


ディスク変更のサブミット] ウィンドウが表示されます。

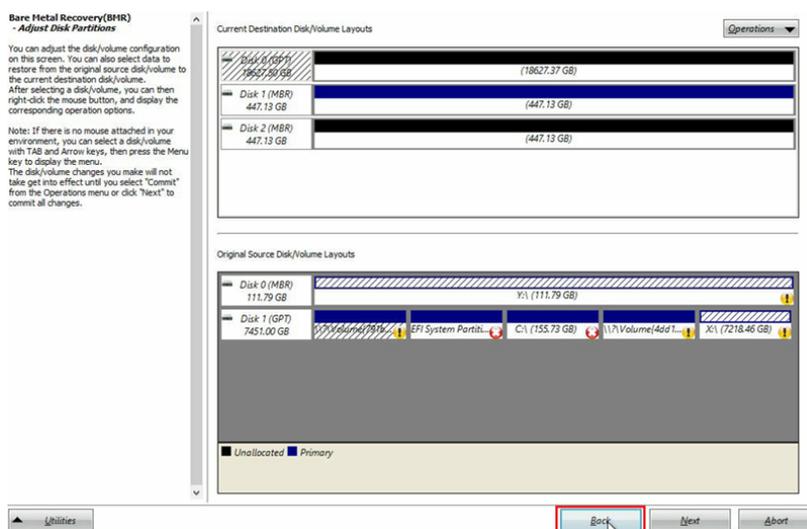
14. サブミット] をクリックします。



15. ディスクの消去が完了したら、OK] をクリックします。

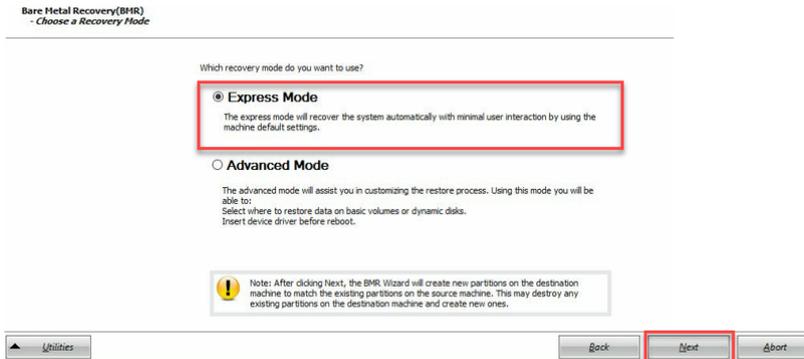


16. [ベアメタル復旧 (BMR) - ディスクパーティションの調整] ダイアログボックスで **戻る** をクリックします。



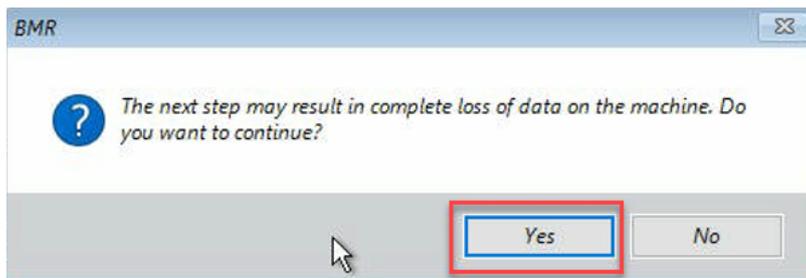
[ベアメタル復旧 (BMR) - 復旧モードの選択] ダイアログボックスが表示されます。

17. **高速モード**] を選択し、**次へ**] をクリックします。



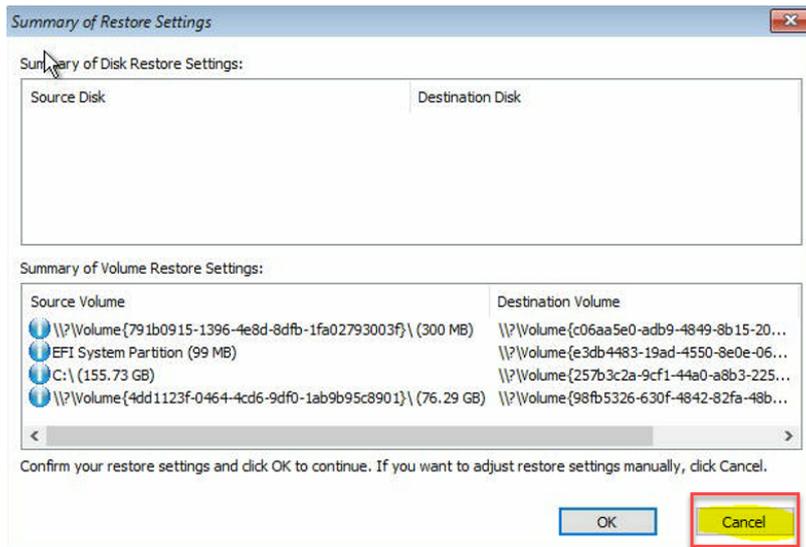
[BMR] ダイアログ ボックスが表示されます。

18. [はい] をクリックします。



[リストア設定のサマリ] ダイアログ ボックスが表示されます。

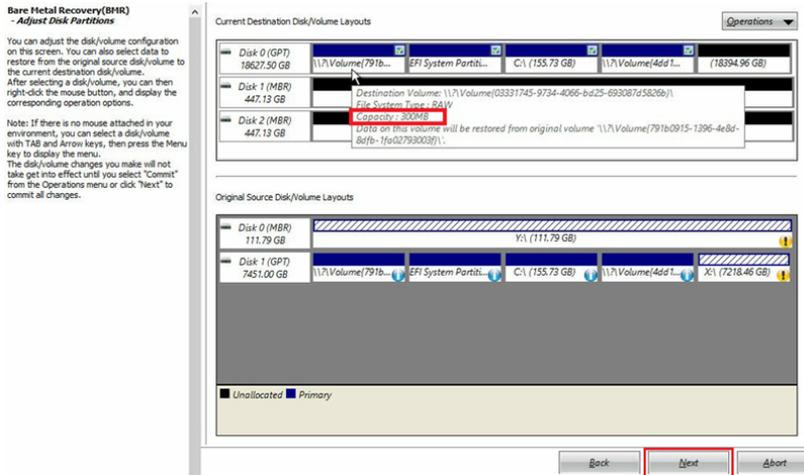
19. [キャンセル] をクリックします。



ベアメタル復旧 (BMR) - ディスクパーティションの調整 ダイアログボックスが表示されます。

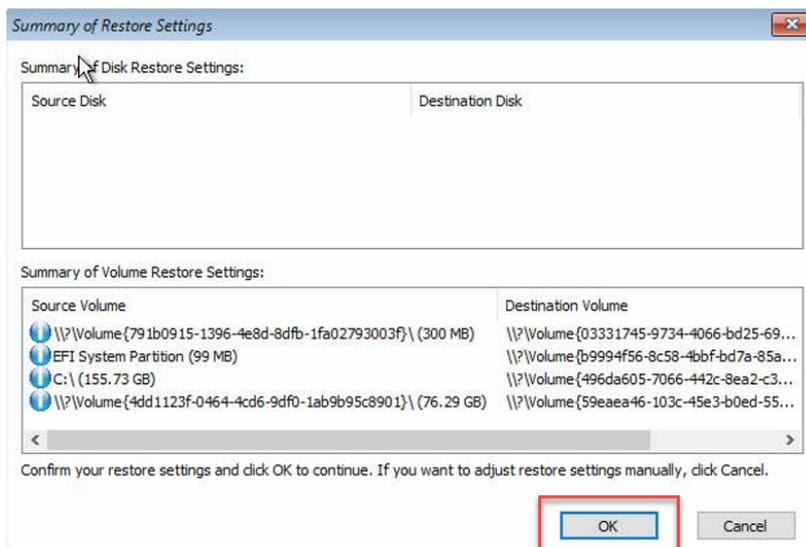
20. **現在のデスティネーション ディスク/ボリュームのレイアウト** タブで使用可能な最初の 4 つのパーティションの容量が、**元のソース ディスク/ボリュームのレイアウト** タブで使用可能な最大の GPT ディスクと一致するかどうかを比較して確認し、**次へ** をクリックします。

注：パーティションのサイズを表示するには、ディスクの上にマウスカーソルを移動させて、ディスクプロパティを表示します。



[リストア設定のサマリ] ダイアログ ボックスが表示されます。

21. [OK] をクリックします。



Bare Metal Recovery(BMR)- Start Recovery Process (ベアメタル復旧 (BMR) - 復旧プロセスの開始)]ダイアログボックスが表示されます。

- 再起動後にエージェント サービスを自動的に開始しない]オプションをオフにして、リストアの完了を待ちます。

Bare Metal Recovery(BMR)
- Start Restore Process

This page displays a summary of the disk/volume restore settings that you have made.

Note: After the BMR process is complete and server has been rebooted, you may not want to perform backup jobs from this server. If you are just testing the BMR functionality, we recommend that you select the "Do not start Agent service automatically after reboot" option. When you select this option, you can manually start the Agent service (and the Recovery Point Server service, if installed) after reboot if you want to perform backup jobs.

Enable Windows F8 boot option helps user perform further recovery or troubleshooting after BMR. For example, press F8 and boot into Active Directory Service Restore mode to perform Active Directory authoritative restore.

Summary of Restore Settings

Restore Item	Status	Progress	Throughput
Restore source volume "\[Volume{791b0915-1396-4e8d-8dfb-1fa02793003f}\] ...	Completed	100.0%	367.44 MB/Minute
Restore source volume "EFI System Partition" to current destination disk 0	Completed	100.0%	967.90 MB/Minute
Restore source volume "C:\\" to current destination disk 0	Restoring	0.8%	2705.50 MB/Minute
Restore source volume "\[Volume{4dd1123f-0464-4c06-9df0-1ab9b95c8901}\] ...	Not Started		

Automatically reboot your system after recovery.

Do not start Agent service automatically after reboot.

Boot the system to Advanced Boot Options (F8) Menu on the next boot for Windows 8 / Windows Server 2012 and later OS.

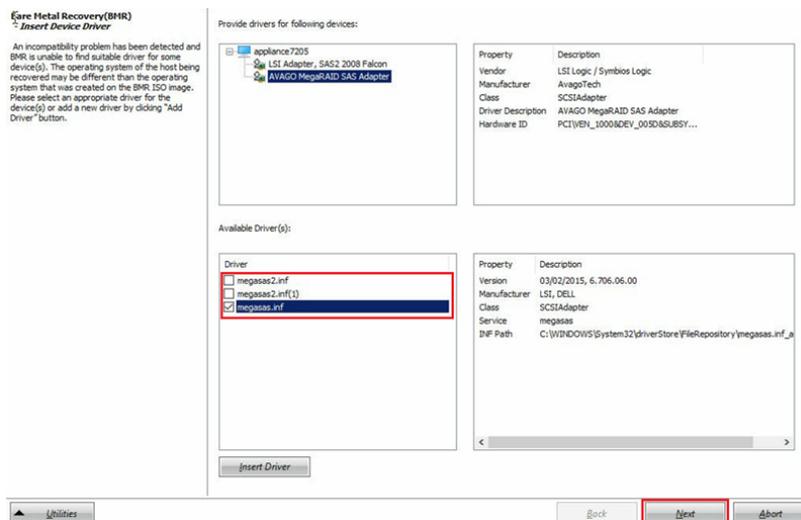
Elapsed Time: 00 : 00 : 24
Estimated Time Remaining: 01 : 30 : 50

[0.8%] [5769MB/76631MB] Restoring basic source volume "C:\\" to current destination disk 0

Utilities Back Next Abort

【ペアメタル復旧 (BMR) - デバイスドライバのインストール】ダイアログボックスが表示されます。

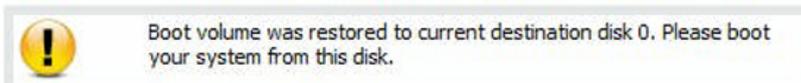
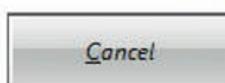
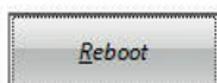
23. RAID コントローラで必要なドライバを選択し、**次へ**をクリックします。



再起動]ポップアップ ウィンドウが表示され、Arcserve アプライアンスが自動的に再起動します。

Click ReBoot to automatically reboot your system at this time. If you want to collect all BMR log files you can use the Activity log utility.
[Click here](#) to launch the Activity Log utility.

Your system will reboot in **11 second(s)**.



BMR の処理が正常に完了しました。

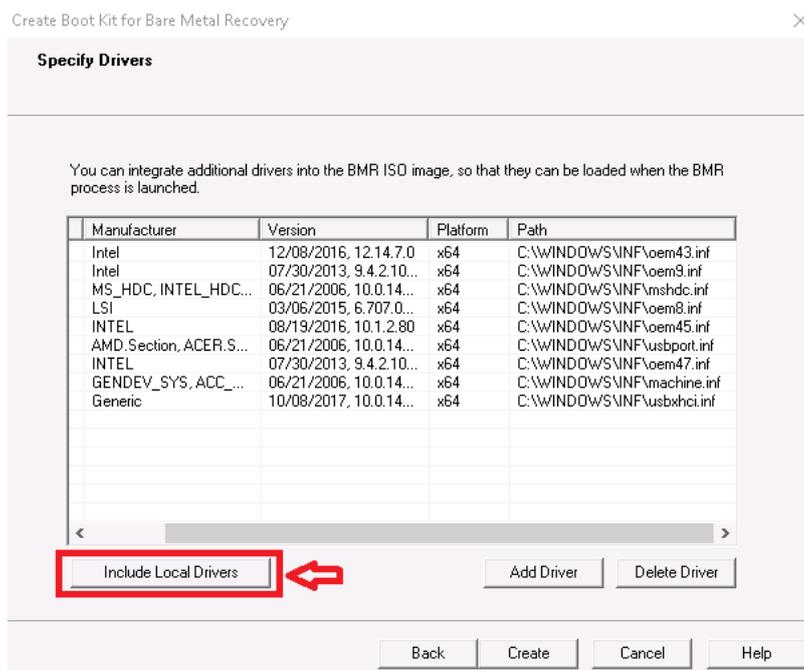
9012-9504DR シリーズ アプライアンスでのベアメタル復旧 (BMR) およびデータ保存の実行

Arcserve アプライアンスでは、Arcserve UDP ブート キットを使用して、ベアメタル復旧を実行できます。

以下の手順に従います。

1. アプライアンスで Arcserve UDP ブートキット ウィザードを実行し、x64 プラットフォームでブート可能な BMR ISO イメージまたは USB スティックを生成します。

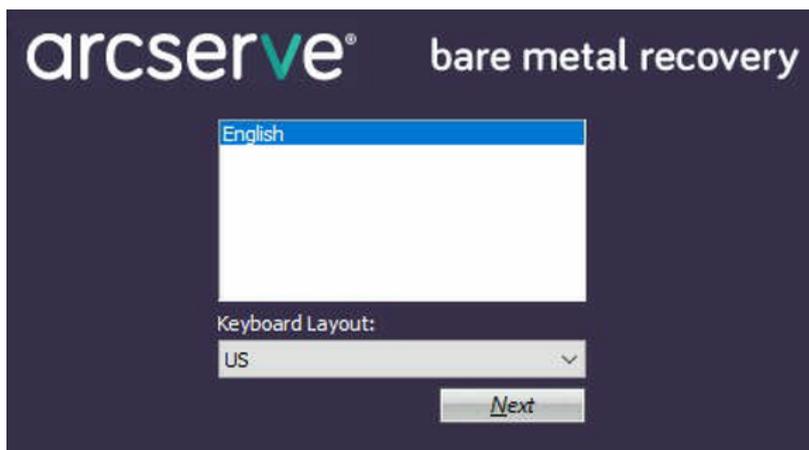
注：ISO イメージにはローカルドライバを含める必要があります。ローカルドライバを含めるには、**[ベアメタル復旧用のブートキットの作成]** ウィンドウで **[ローカルドライバを含む]** オプションを選択します。ブートキットの作成方法の詳細については、この[リンク](#)を参照してください。



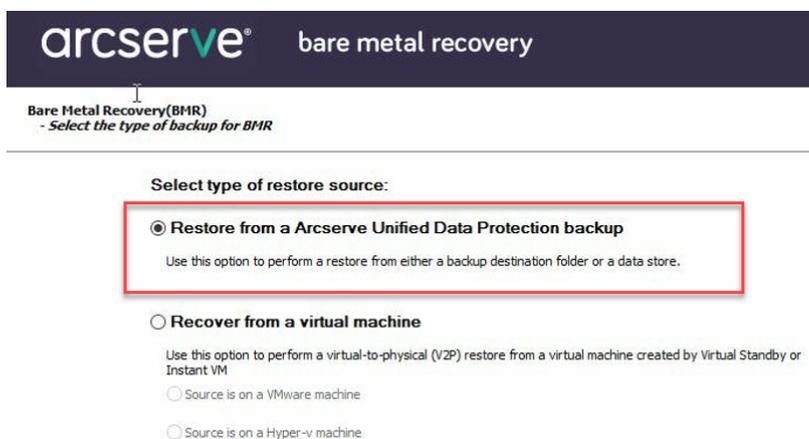
2. BMR ISO イメージまたは USB スティックを使用して、Arcserve アプライアンスを起動します。

Arcserve ベアメタル復旧 のセットアップ画面が表示されます。

3. 必要な言語を選択して、**[次へ]**をクリックします。

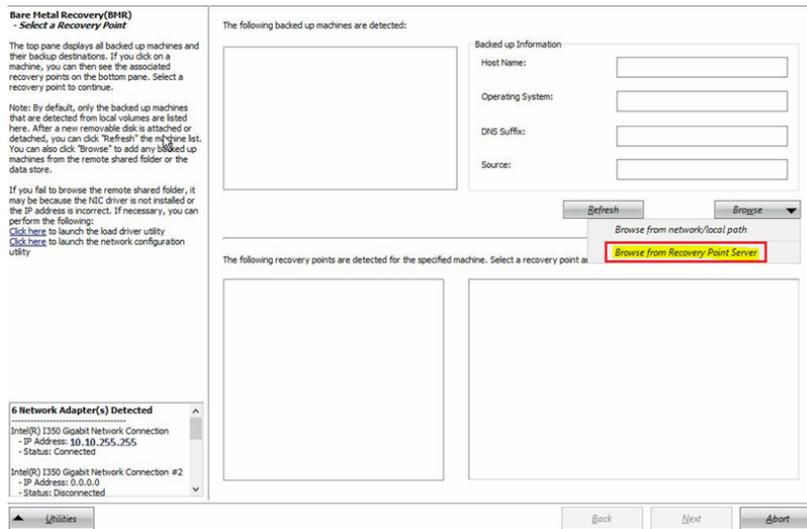


4. [Arcserve Unified Data Protection のバックアップからのリストア] オプションを選択し、[次へ]をクリックします。



復旧ポイントの選択] ウィザードのウィンドウが表示されます。

5. [参照]をクリックして、[復旧ポイント サーバから参照]を選択します。



[ホストの選択] ウィンドウが表示されます。

6. 復旧ポイント サーバのホスト名、ユーザ名、パスワード、ポート、およびプロトコルを入力します。
7. **接続**] をクリックします。
8. 接続が確立されたら、**OK**] をクリックします。

Select Node

Enter the Recovery Point Server credentials and click "Connect" to connect to the server and retrieve the data store and node list.

Host Name: Port:

User Name: Protocol: HTTP HTTPS

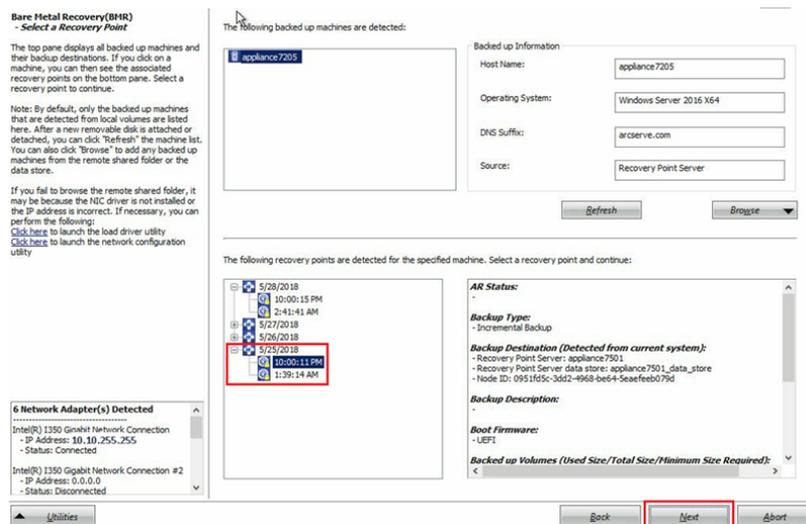
Password:

Data stores and nodes protected on this server:

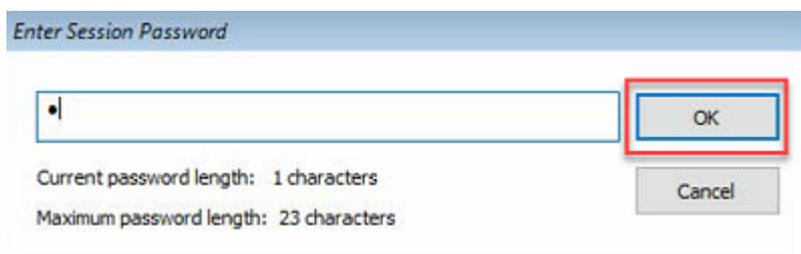
appliance7501_data_store	Property	Description
appliance7205	Node	appliance7205
	DNS Suffix	arcserve.com
	Node ID	0951fd5c-3dd2-4968-be64-5eaef...

【ペアメタル復旧(BMR) - 復旧ポイントの選択】ダイアログボックスが表示されます。

- リストアする復旧ポイントを選択して、**次へ**]をクリックします。

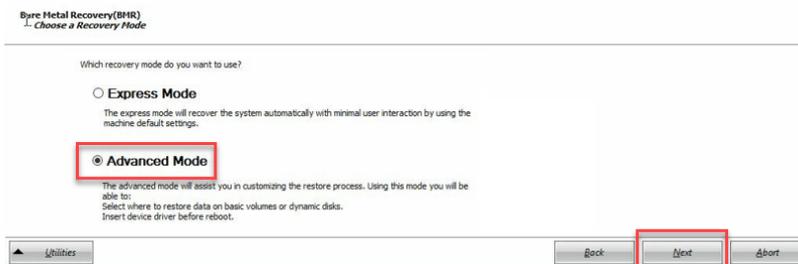


10. (オプション) 要求された場合はセッションパスワードを入力し、[OK]をクリックします。

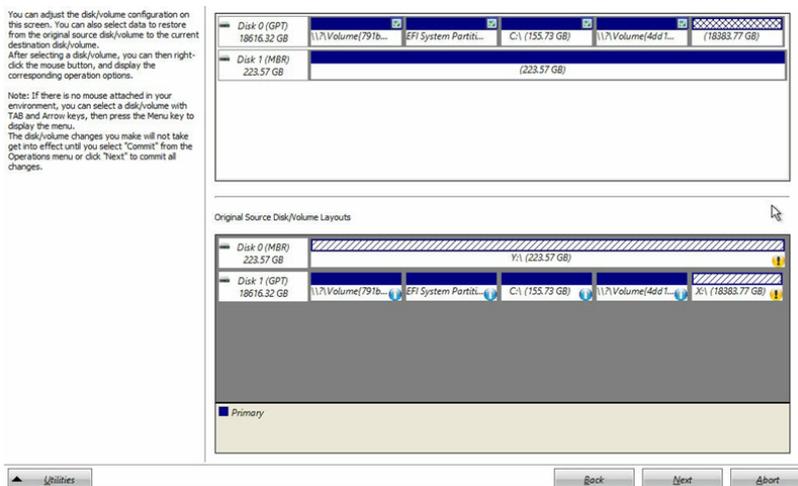


[ペアメタル復旧 (BMR) - 復旧モードの選択] ダイアログボックスが表示されます。

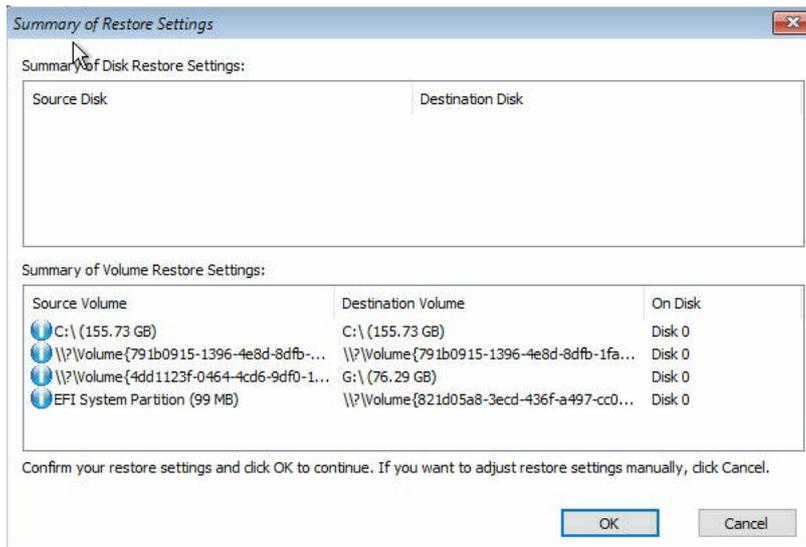
11. [拡張モード] を選択し、[次へ] をクリックします。



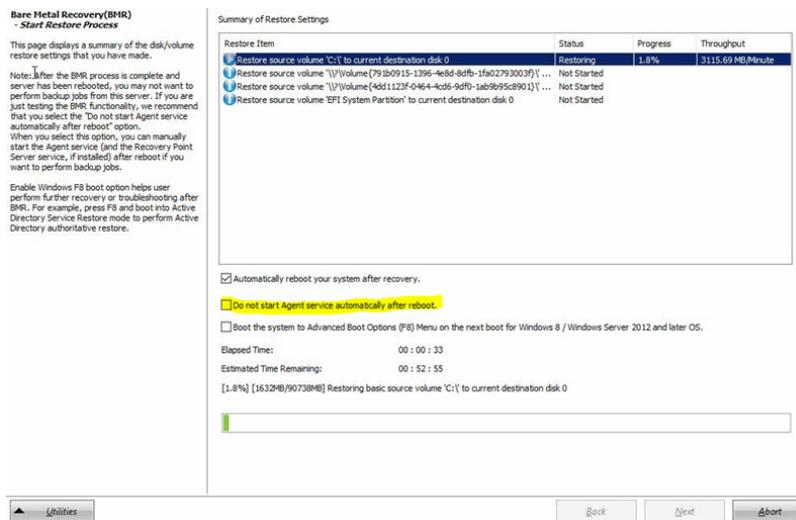
12. [ペアメタル復旧 (BMR) - ディスクパーティションの調整] ダイアログボックスで [次へ] をクリックします。



13. [ディスクリストア設定のサマリ] 画面で、[OK] をクリックします。



14. [Bare Metal Recovery(BMR)- Start Recovery Process (ペアメタル復旧 (BMR) - 復旧プロセスの開始)] ダイアログボックスで、再起動後にエージェントサービスを自動的に開始しない] オプションをオフにして、リストアの完了とマシンの再起動を待ちます。



BMR の処理が正常に完了しました。

第9章: アプライアンスの容量拡張

このセクションには、以下のトピックが含まれます。

Arcserve アプライアンス 10024BU-10576DR モデルの拡張キットでの操作	173
Arcserve アプライアンス 10024BU-10576DR モデルの SSD フラッシュ拡張キットでの操作	178
Arcserve アプライアンス拡張キットの操作 - X シリーズ モデル	181
Arcserve X シリーズ アプライアンスの SSD フラッシュ拡張キットの操作	183
Arcserve アプライアンス 9072-9504DR モデルの拡張キットでの操作	190
Arcserve アプライアンス 9072-9504 DR モデルの SSD フラッシュ拡張キットの操作	195

Arcserve アプライアンス 10024BU-10576DR モデルの拡張キットでの操作

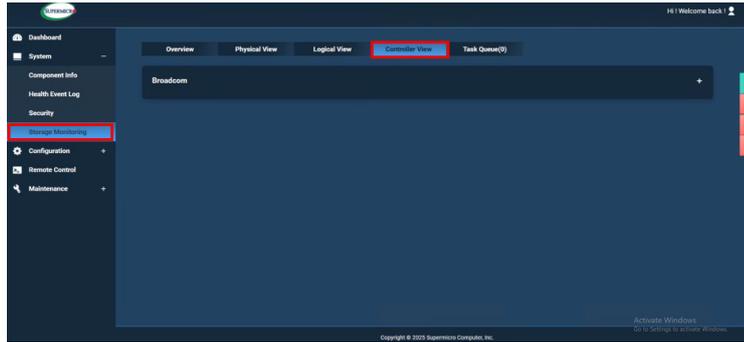
Arcserve 拡張キットを使用して、Arcserve アプライアンス 10024BU-10576DR モデルのデータ容量を拡張できます。

以下の手順に従います。

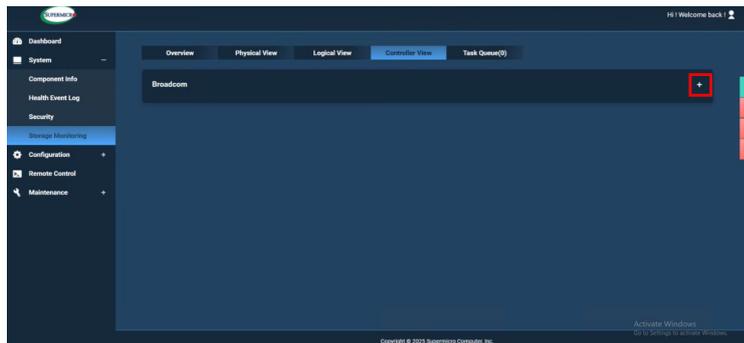
1. 空のディスクスロットにHDDを挿入するには、以下の手順に従います。
 - a. Arcserve UDP コンソールで、アプライアンス サーバ上に実行中のジョブがないことを確認します。実行中のジョブがある場合は、対応するプランを一時停止します。
 - b. HDD を空のディスクスロットに挿入します。



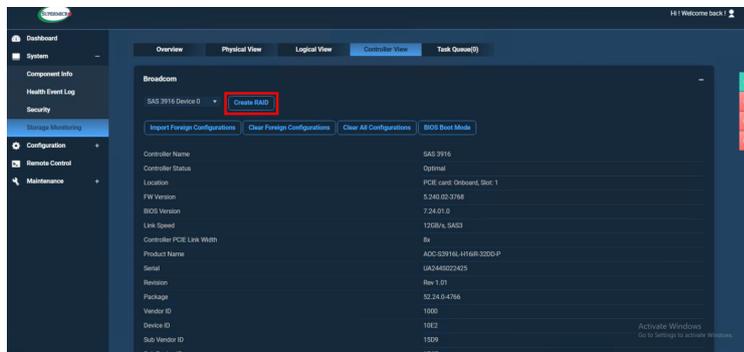
2. IPMI Web インターフェースから Raid-6 を作成して設定するには、以下の手順に従います。
 - a. IPMI コンソールにログインします。
 - b. **[システム] > [storage Monitoring (ストレージ モニタリング)] > [controller view (コントローラビュー)]** に移動します。



- c. [Controller view (コントローラビュー)] タブで、**プラス記号 (+)** をクリックし、**[Broadcom]** を展開します。



- d. [Broadcom] 画面で、**[create RAID (RAID の作成)]** をクリックします。



- e. [作成] ページで、すべての HDD スロットを選択し、以下を指定します。
- **RAID**: [RAID レベル] ドロップダウン リストから、**[RAID6]** を選択します
 - **PD per Span (スパンごとの PD)** : 1
 - **Enter % size be used (使用される % サイズの入力)** : 値を「100」のように入力します

- **New Logical Drive Count (新規論理ドライブ数)** : 値「1」を入力します
 - **Stripe size per DDF (DDF あたりのストライプ サイズ)** : **[256K]** オプションを選択します
 - **Virtual Drive name (仮想ドライブ名)** : 仮想ドライブの名前を入力します
 - **LD Read Policy (LD 読み取りポリシー)** : **[先読みなし]** オプションを選択します
 - **LD Write Policy (LD 書き込みポリシー)** : **[Write Back (書き戻し)]** オプションを選択します
 - **LD IO Policy (LD IO ポリシー)** : デフォルトでは、**[Direct IO]** オプションが選択されています。
 - **Access Policy (アクセスポリシー)** : **[Read Write (読み取りと書き込み)]** オプションを選択します。
 - **Disk Cache Policy (ディスク キャッシュ ポリシー)** : **[Unchanged (未変更)]** オプションを選択します
 - **Init State (初期化状態)** : **[Quick Init (クイック初期化)]** オプションを選択します
- f. **[サブミット]** をクリックします。

The screenshot shows a RAID6 configuration window. At the top, it says 'RAID6' and 'PD per Span: 1'. Below this is a table of drives:

Slot#	Product Name	Capacity	Interface Type	Media Type	Sector Size	
<input type="checkbox"/>	0	KPM7XVUG3T20	2980 GB	SAS	SSD	512
<input type="checkbox"/>	1	KPM7XVUG3T20	2980 GB	SAS	SSD	512
<input checked="" type="checkbox"/>	2	ST16000NM004J	14901 GB	SAS	HDD	512
<input checked="" type="checkbox"/>	3	ST16000NM004J	14901 GB	SAS	HDD	512
<input checked="" type="checkbox"/>	4	ST16000NM004J	14901 GB	SAS	HDD	512
<input checked="" type="checkbox"/>	5	ST16000NM004J	14901 GB	SAS	HDD	512
<input checked="" type="checkbox"/>	6	ST16000NM004J	14901 GB	SAS	HDD	512
<input checked="" type="checkbox"/>	7	ST16000NM004J	14901 GB	SAS	HDD	512
<input checked="" type="checkbox"/>	8	ST16000NM004J	14901 GB	SAS	HDD	512

Below the table, there are several configuration options:

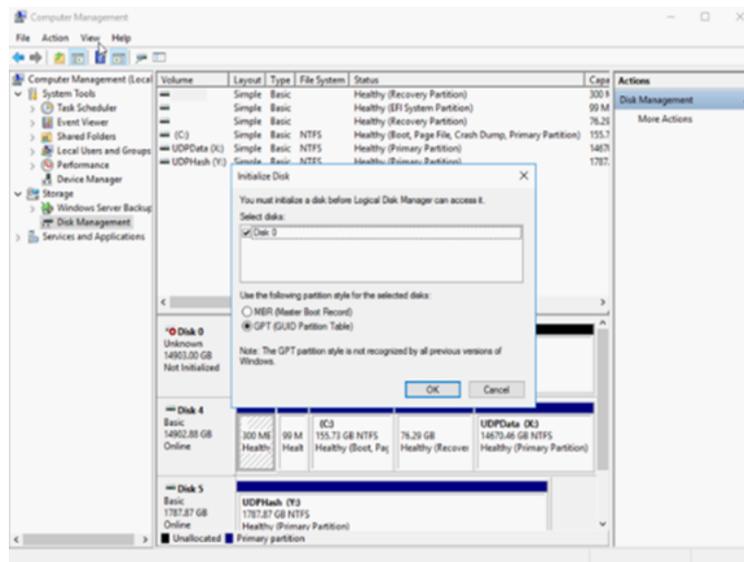
- Enter % size be used: 100
- New Logical Drive Count: 1
- Stripe size per DDF: 64K 128K 256K 512K 1024K
- Virtual Drive name: UDPDData
- LD Read Policy: No Read Ahead Always Read Ahead
- LD Write Policy: Write Through Write Back Always Write Back
- LD IO Policy: Direct IO Cached IO
- Access Policy: Read Write Read Only Blocked
- Disk Cache Policy: Unchanged Enable Disable
- Init State: No Init Quick Init Full Init

At the bottom, there are 'Cancel' and 'Submit' buttons.

- g. タスクバーの検索ボックスに「コンピューターの管理」と入力し、Enter キーを押します。

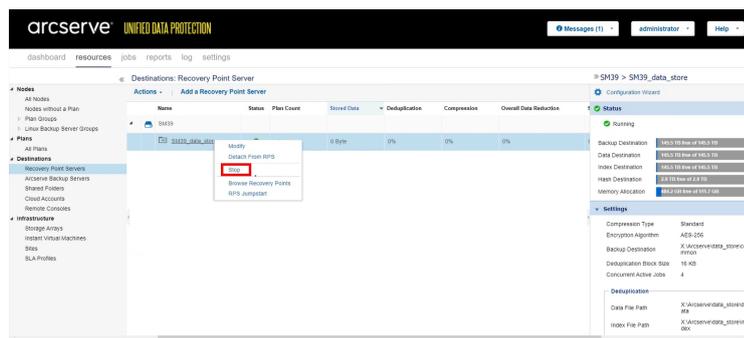
[コンピューターの管理] ウィンドウが表示されます。

- h. **記憶域**] > **ディスクの管理**] に移動します。
- i. 追加した新しい仮想ディスクをダブルクリックします。
ディスクの初期化] ウィンドウが表示されます。
- j. **GPT (GUID パーティション テーブル)**] オプションを選択して、**[OK]** をクリックします。



- k. **ディスクの管理**] ウィンドウで仮想ディスクを選択し、以下のプロパティを適用します。
 - ドライブ文字の割り当て
 - ファイルシステムとして NTFS を指定します。
 - ディスクのフォーマット
3. データストアを拡張するには、以下の手順に従います。
 - a. 追加したドライブに移動し、フォルダを作成します。
 - b. Arcserve アプライアンスのデスクトップから、**Arcserve アプライアンス**] ウィザードを起動します。
Arcserve Appliance Configuration (Arcserve アプライアンスの設定)] ページが開きます。
 - c. **[UDP コンソールの起動]** をクリックします。
Arcserve UDP コンソールのログイン ページが表示されます。
 - d. 管理者として UDP コンソールにログインします。
 - e. **[ソース]** > **デスティネーション**] > **復旧ポイント サーバ**] に移動します。

- f. データストアを右クリックし、**停止]** を選択します。



- g. コマンド ラインから C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN に移動し、以下のコマンドを実行します。

```
as_gddmgr.exe -DataPath Add <データストア名> -NewDataPath <新規データフォルダ>
```

以下の画面の例では、ボリューム容量、使用容量、プライマリデータパスの空き容量、拡張データパスの空き容量、合計値などの詳細が表示されています。合計値は、プライマリデータパスと拡張データパスの合計です。

以下のコマンドを実行して、データパスの詳細を表示することもできます。

```
as_gddmgr.exe -DataPath Display <データストア名>
```

```
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>as_gddmgr.exe -DataPath Add appliatest75_data_store -NewDataPath Y:\data
Successfully load data store configuration information.
Successfully added new expanded data path for the data store.
The data store has 1 expanded data path(s) now:

          Volume capacity      Used space      Free space
-----
Primary data path : X:\Arcserve\data_store\data\
                  18384 GB          1 GB          18383 GB
Expanded data path: Y:\data
                  224 GB           1 GB          223 GB
Total              18608 GB          2 GB          18606 GB

Success to add data path Y:\data.
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>
```

新しく展開されたデータパスがデータストアに正常に追加されました。

- h. UDP コンソールで、**[ソース] > [スケーリング] > 復旧ポイントサーバ]** に移動します。
- i. データストアを右クリックし、**開始]** を選択します。
- j. 一時停止していたプランを UDP コンソールから再開します。

Arcserve アプライアンスのデータ容量が正常に拡張されました。

Arcserve アプライアンス 10024BU-10576DR モデルの SSD フラッシュ拡張キットでの操作

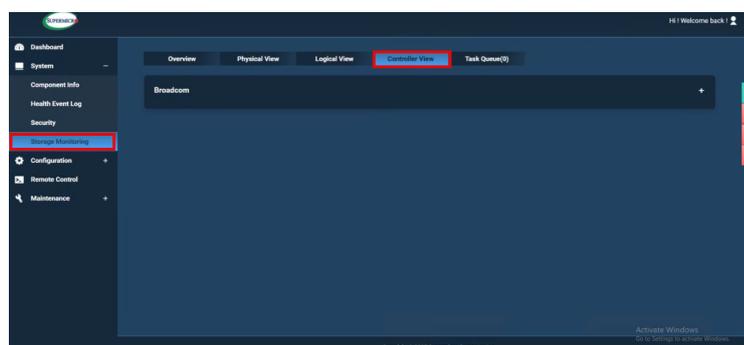
Arcserve SSD フラッシュ拡張キットを使用すると、Arcserve アプライアンス 10024BU-10576DR モデルでセカンダリデータストアを作成し、DR 関連操作 (IVM/VSB/Continuous Availability) を実行することで、データ容量を拡張できます。

以下の手順に従います。

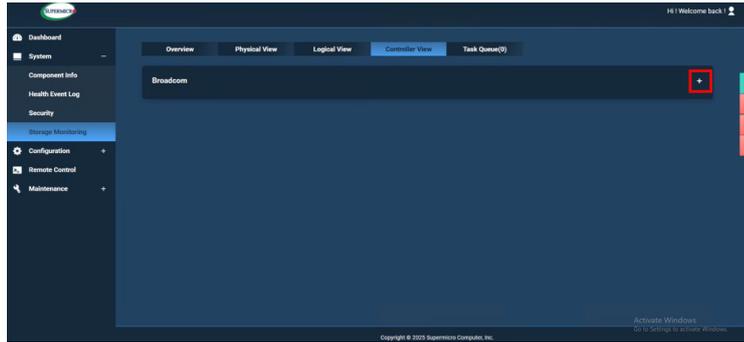
1. 空のディスクスロットにSSDを挿入するには、以下の手順に従います。
 - a. Arcserve UDP コンソールで、アプライアンスサーバ上に実行中のジョブがないことを確認します。実行中のジョブがある場合は、対応するプランを一時停止します。
 - b. SSD を空のディスクスロットに挿入します。



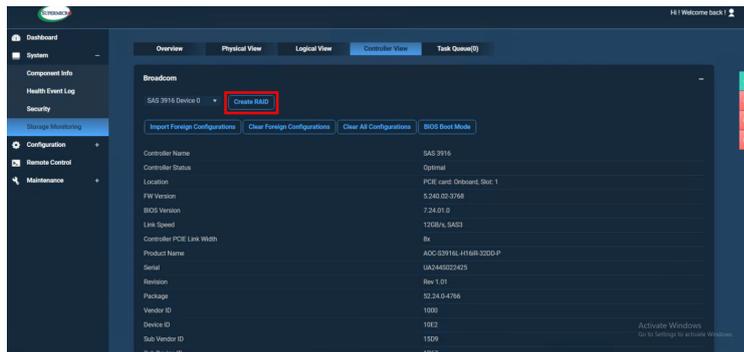
2. IPMI Web インターフェースから Raid-5 を作成して設定するには、以下の手順に従います。
 - a. IPMI コンソールにログインします。
 - b. [システム] > [storage Monitoring (ストレージ モニタリング)] > [controller view (コントローラビュー)] に移動します。



- c. [controller view (コントローラビュー)] タブで、プラス記号 (+) をクリックし、[broadcom] を展開します。



- d. [Broadcom] 画面で、[create RAID (RAID の作成)] をクリックします。



- e. [作成] ページで、すべての SSD スロットを選択し、以下の操作を実行します。
- RAID: [RAID レベル] ドロップダウン リストから、[RAID1] を選択します
 - PD per Span (スパンごとの PD) : 1
 - Enter % size be used (使用される % サイズの入力) : 値を「100」のように入力します
 - New Logical Drive Count (新規論理ドライブ数) : 値「1」を入力します
 - Stripe size per DDF (DDF あたりのストライプ サイズ) : [56K] オプションを選択します
 - Virtual Drive name (仮想ドライブ名) : 仮想ドライブの名前を入力します
 - LD Read Policy (LD 読み取りポリシー) : [先読みなし] オプションを選択します
 - LD Read Policy (LD 読み取りポリシー) : [Write Back (書き戻し)] オプションを選択します

- LD IO Policy (LD IO ポリシー) : デフォルトでは、 **[Direct IO]** オプションが選択されています。
- Access Policy (アクセスポリシー) : **[Read Write (読み取りと書き込み)]** オプションを選択します。
- Disk Cache Policy (ディスクキャッシュポリシー) : **[Unchanged (未変更)]** オプションを選択します
- Init State (初期化状態) : **[Quick Init (クイック初期化)]** オプションを選択します

f. **[サブミット]** をクリックします。

Slot#	Product Name	Capacity	Interface Type	Media Type	Sector Size
0	KPM7XVUG3T20	2980 GB	SAS	SSD	512
1	KPM7XVUG3T20	2980 GB	SAS	SSD	512

g. タスクバーの検索ボックスに「コンピューターの管理」と入力し、Enter キーを押します。

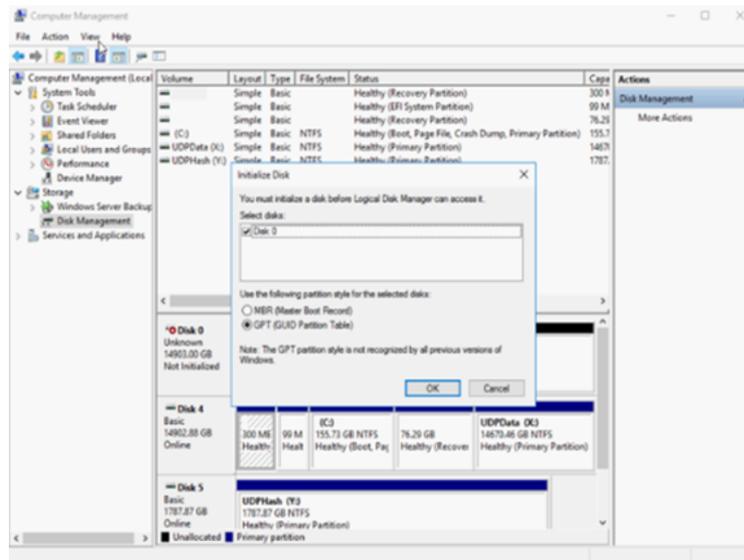
[コンピューターの管理] ウィンドウが表示されます。

h. **[記憶域] > ディスクの管理]** に移動します。

i. 追加した新しい仮想ディスクをダブルクリックします。

[ディスクの初期化] ウィンドウが表示されます。

j. **[GPT (GUID パーティション テーブル)]** オプションを選択して、 **[OK]** をクリックします。



- k. [ディスクの管理] ウィンドウで仮想ディスクを選択し、以下のプロパティを適用します。
- ドライブ文字の割り当て
 - ファイルシステムとして NTFS を指定します。
 - ディスクのフォーマット

仮想ディスクが正常に作成されました。

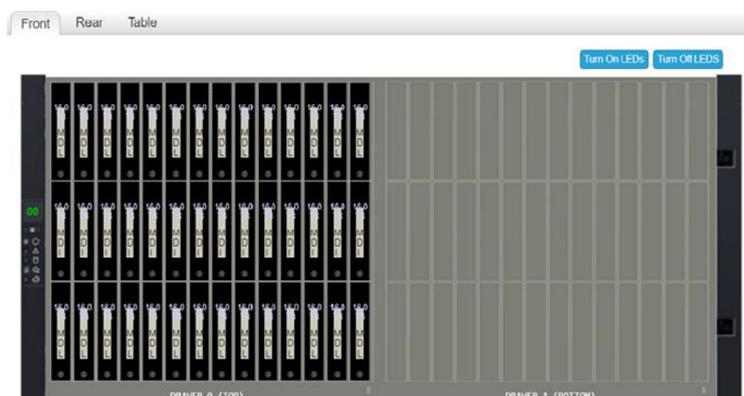
Arcserve アプライアンス拡張キットの操作 - X シリーズ モデル

Arcserve 拡張キットを使用して、Arcserve アプライアンス X シリーズ モデルのデータ容量を拡張できます。

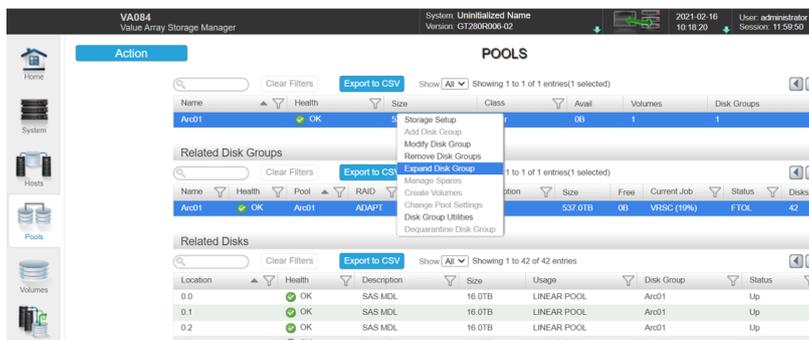
以下の手順に従います。

1. X シリーズ拡張キット - すべてのモデル(X3000DR を除く) の容量では、最大モデルの X3000DR に達するまで、オプションの拡張キットを使用して必要な回数だけ線形拡張を実行できます。
2. 以下の手順に従い、空のディスクスロットに HDD を挿入します。
 - a. Arcserve UDP コンソールで、アプライアンス サーバ上に実行中のジョブがないことを確認します。実行中のジョブがある場合は、対応するプランを一時停止します。
 - b. ストレージ ユニット - ME4084 Value Array の空のディスクスロットに HDD を挿入します。X シリーズ拡張キットの各キットは、14 x 16TB

ディスクで構成されています。

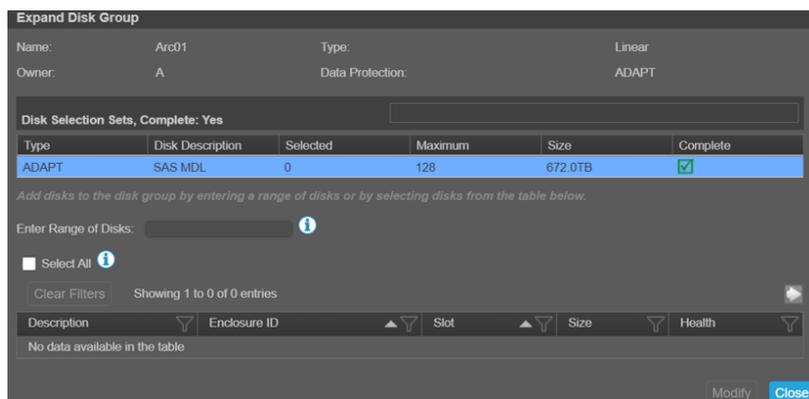


3. ME ユニット - Value Array ストレージ マネージャにログインし、**[プール]**に移動して拡張するディスクグループを選択します。



4. 選択したディスクグループを右クリックし、**[ディスクグループの拡張]**を選択します。

[ディスクグループの拡張]パネルが開き、ディスクグループの情報とディスクテーブルが表示されます。

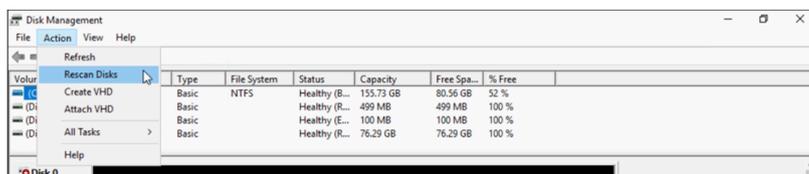


5. ディスクグループにディスクを追加するには、**[ディスクの範囲の入力]**フィールドにディスクの範囲を入力するか、テーブルからディスクを選択します。
6. **[変更]**をクリックします。

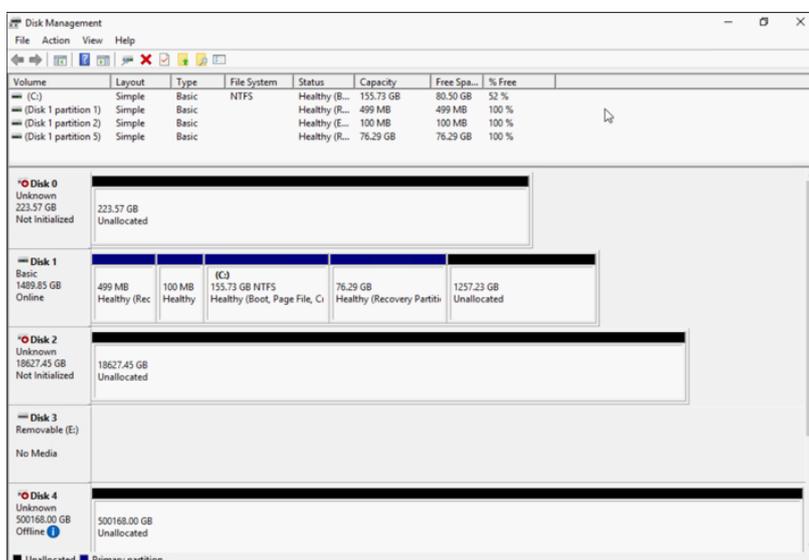
7. 確認パネルで [はい] をクリックしてグループの展開を開始し、[OK] をクリックしてパネルを閉じます。

注：拡張ジョブが完了すると、ディスクグループで再バランスジョブがトリガされます。

8. 拡張ジョブと再バランスジョブが完了したら、コンピュータ ユニットから [ディスクの管理] を開き、[アクション]- [ディスクの再スキャン] を選択します。



再スキャン後、ストレージユニットのディスクは拡張されたストレージと共に表示されます。



Arcserve X シリーズ アプライアンスの SSD フラッシュ拡張キットの操作

Arcserve SSD フラッシュ拡張キットを使用すると、セカンダリデータストアを作成してデータ容量を拡張し、Arcserve アプライアンス X シリーズで DR 関連操作 (IVM /VSB/Continuous Availability) を実行します。

以下の手順に従います。

1. 以下の手順に従い、空のディスクスロットに SSD を挿入します。
 - a. Arcserve UDP コンソールで、アプライアンスサーバ上に実行中のジョブがないことを確認します。実行中のジョブがある場合は、対応するプランを一時停止します。

- b. SSD を空のディスク スロットに挿入します。



2. 以下の手順に従い、BIOS ブート マネージャオプションから Raid-5 を設定します。

- a. 仮想コンソール ダッシュボードを起動するには、iDRAC にログインし、**仮想コンソールの開始**]をクリックします。
- b. 仮想コンソール ページで、**ブート**]をクリックし、**BIOS ブート マネージャ**]オプションを選択します。

確認 ウィンドウで **[はい]** をクリックして、BIOS ブート マネージャを再起動します。

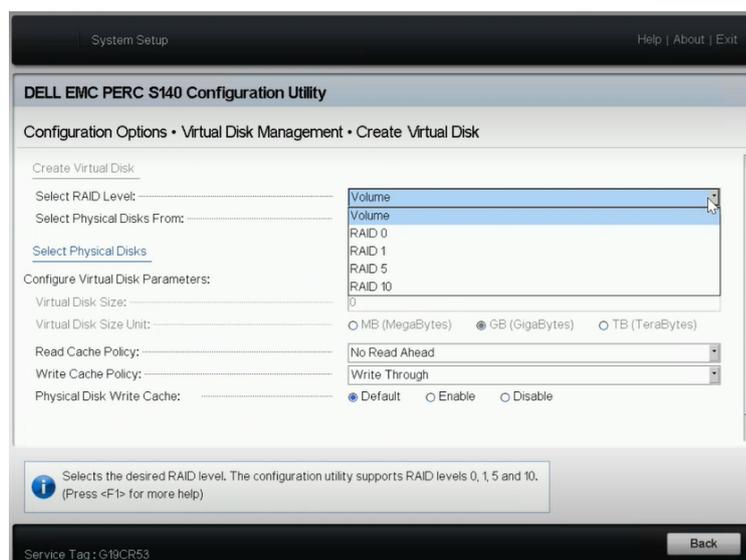
- c. **電源**]をクリックし、**システムのリセット (ウォーム ブート)**]を選択します。

アプライアンスが起動し、ブート マネージャ セットアップ ページが再起動します。

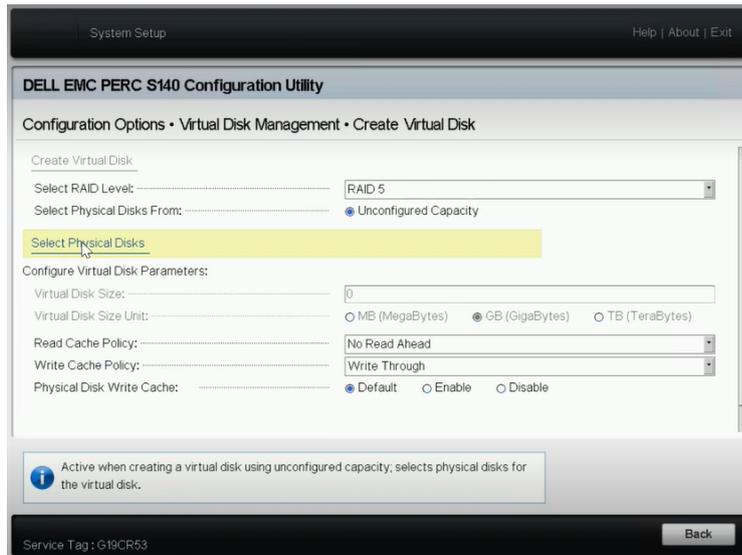
- d. ブート マネージャのメイン メニューで、**システム セットアップの起動**]をクリックしてから、**デバイス設定**] > **Dell EMC PERC S140 Controller**] > **仮想ディスク管理**] > **仮想ディスクの作成**]に移動します。

- e. **[RAID レベルの選択]** ドロップダウン リストから、**[RAID 5]** を選択します。

注: RAID 5 仮想ディスクは拡張キットに使用され、物理ディスクごとに新しく接続された 3.63 TB のディスクが含まれます。



- f. **物理ディスクの選択**]オプションを選択します。

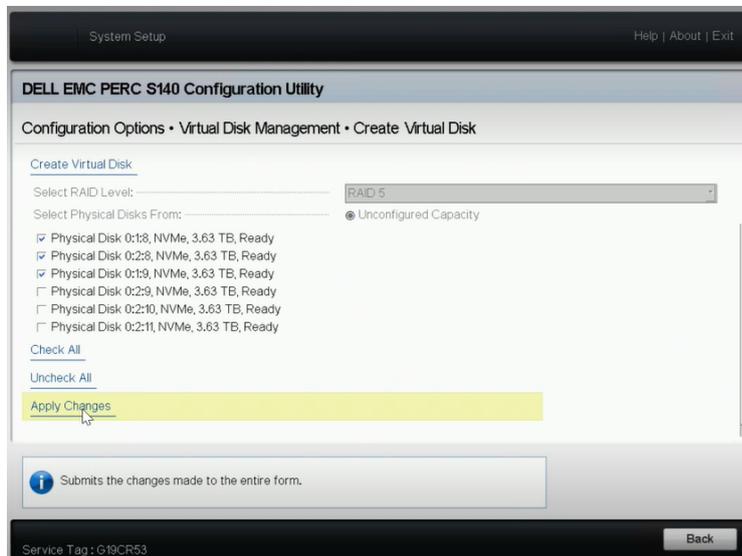


物理ディスク操作の選択]ウィンドウが開きます。

- g. **[インターフェースの種類を選択]**オプションで、**[NVMe]**をクリックします。

物理ディスクのリストが表示されます。

- h. 物理ディスクのリストから、必要に応じてディスクを選択し、**変更の適用**]をクリックします。



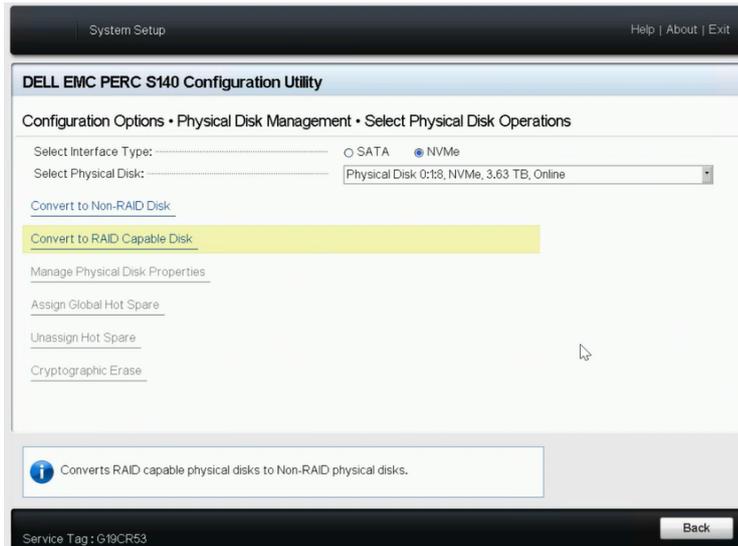
注: 最小 3 ディスク、最大 16 ディスクを選択します。

- i. 変更が適用されたら、**仮想ディスクの作成**]オプションを再度クリックして、仮想ディスクの作成プロセスを完了します。

3. **環境設定オプション] > 物理ディスク管理] > 物理ディスク操作の選択]**に移動します。

- a. インターフェースの種類を選択で、**[NVMe]**をクリックします。
- b. **物理ディスクの選択]**ドロップダウンリストから、必要に応じてオプションを選択し、**[RAID 対応ディスクに変換]**をクリックします。

注：RAID 対応ディスクに変換するオプションは、すべての物理ディスクに1 つずつ適用できます。

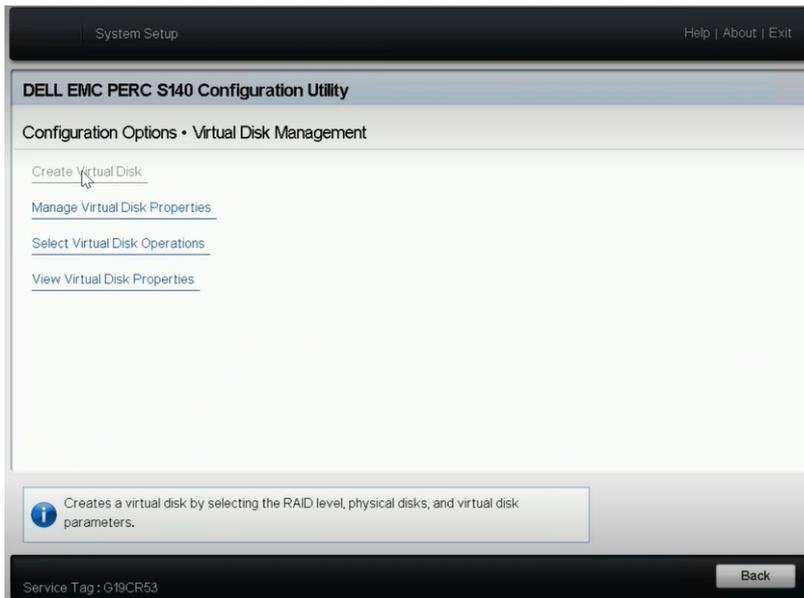


- c. 以下の警告メッセージが表示されたら、以下を実行します。

RAC0516: 物理ディスクドライブを RAID 互換に変換すると、OS で作成された RAID アレイは上書きされます。

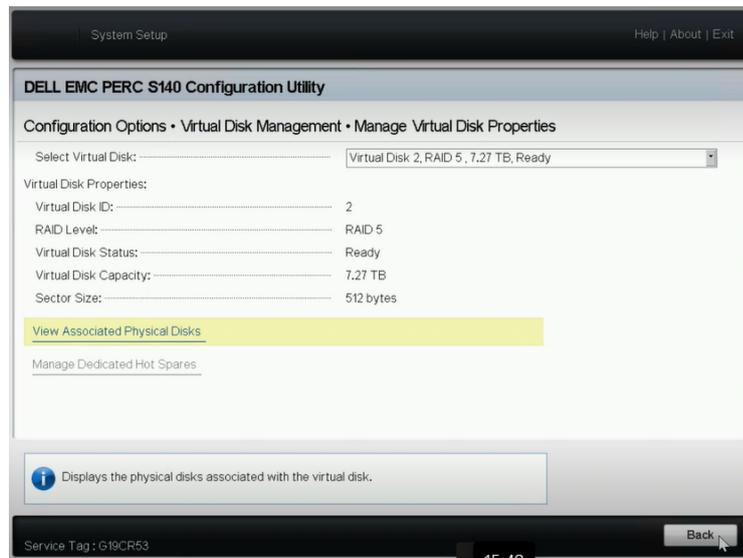
1. OS で構成された RAID アレイが存在しないことを確認し、**[OK]**をクリックします。
2. **[OK]**をクリックします。

4. **環境設定オプション] > 仮想ディスク管理]**に移動し、以下を実行します。

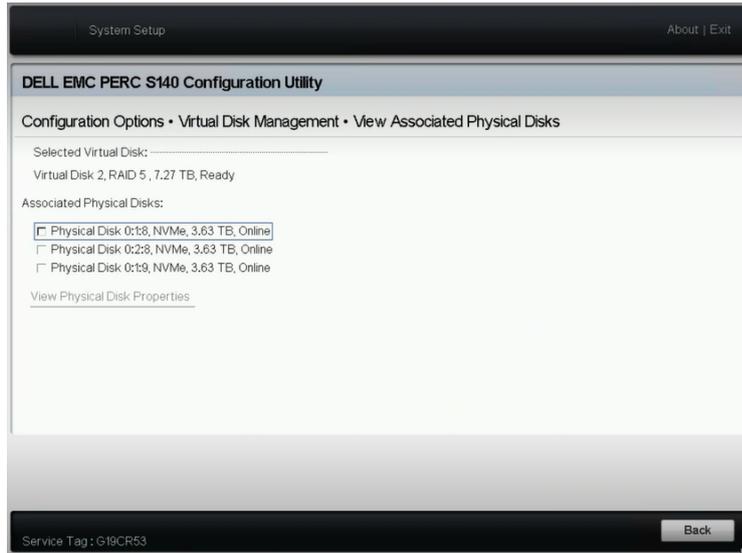


- a. 仮想ディスクを管理するには、**仮想ディスクプロパティの管理**]をクリックします。

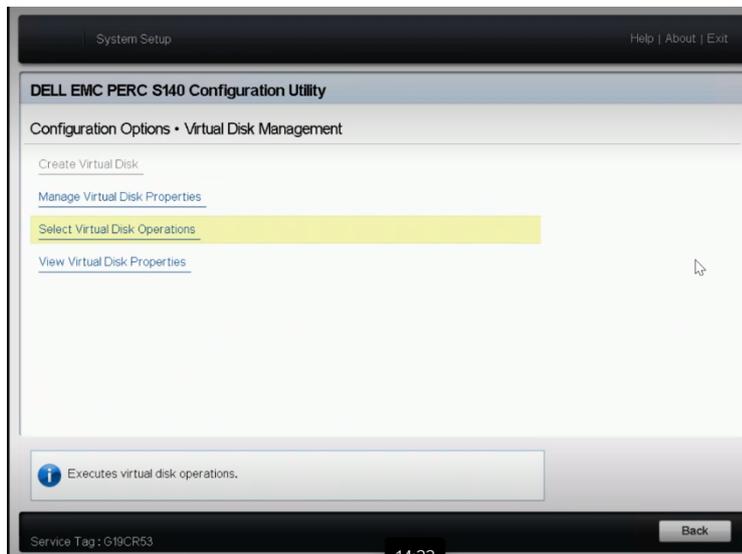
仮想ディスクの選択]ドロップダウンリストから、いずれかの RAID 5 ディスクを選択し、**関連する物理ディスクの表示**]をクリックします。



関連するディスクが表示されます。



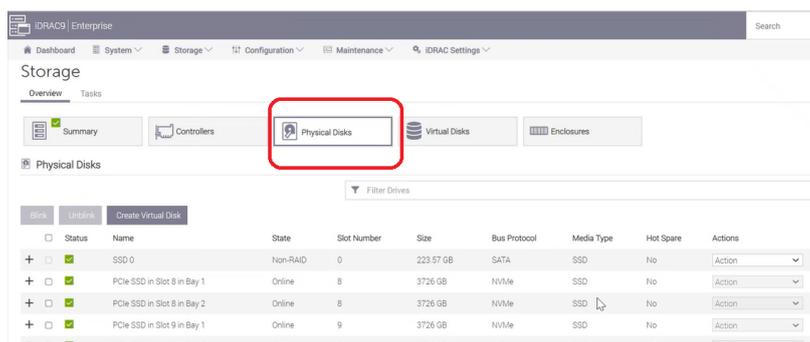
- b. 仮想ディスク操作を選択するには、**仮想ディスク操作の選択]**をクリックします。



- c. ブート マネージャで仮想ディスクのプロパティを表示するには、**仮想ディスクプロパティの表示]**をクリックします。
5. iDRAC でディスク情報を表示するには、iDRAC にログインしてから、**ストレージ] > 概要]**をクリックします。

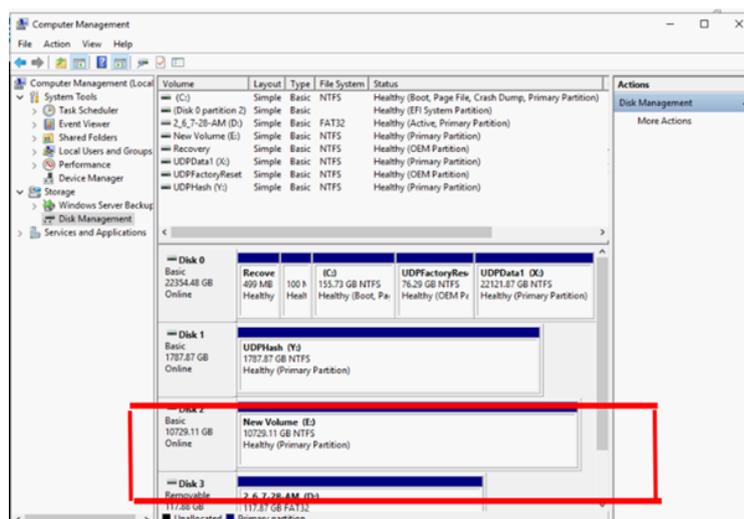


概要]セクションで、**物理ディスク]**をクリックして、作成した物理ディスクのリストを表示します。



6. 新しく追加した仮想ディスクを初期化してフォーマットするには、以下の手順に従います。

- コンピュータ管理]- **ディスク管理]**に移動します。
- 追加した新しい仮想ディスクをダブルクリックします。
ディスクの初期化]ウィンドウが表示されます。
- GPT (GUIDパーティションテーブル)]**オプションを選択して、**OK]**をクリックします。
- ディスクの管理]ウィンドウで仮想ディスクを選択し、以下のプロパティを適用します。
 - ◆ ドライブ文字の割り当て
 - ◆ ファイルシステムとしてNTFSを指定します。
 - ◆ ディスクのフォーマット



仮想ディスクが作成されます。

Arcserve アプライアンス 9072-9504DR モデルの拡張キットでの操作

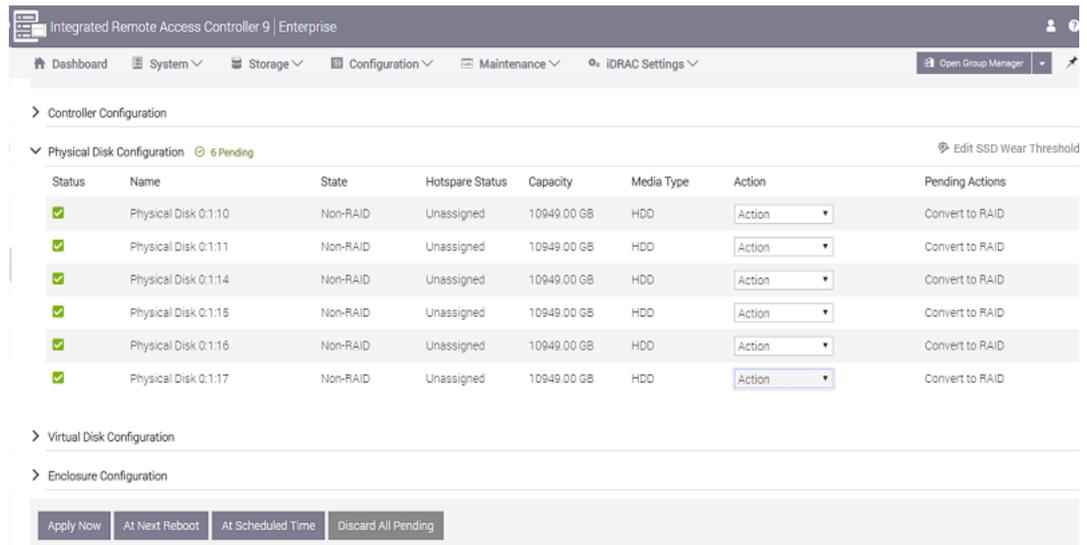
Arcserve 拡張キットを使用して、Arcserve アプライアンス 9072-9504DR モデルのデータ容量を拡張できます。

以下の手順に従います。

1. 以下の手順に従い、空のディスクスロットにHDDを挿入します。
 - a. Arcserve UDP コンソールで、アプライアンス サーバ上に実行中のジョブがないことを確認します。実行中のジョブがある場合は、対応するプランを一時停止します。
 - b. HDD を空のディスクスロットに挿入します。



2. 以下の手順に従い、iDRAC で RAID-6 を設定します。
 - a. iDRAC にログインし、**[環境設定]- [ストレージの環境設定]- 物理ディスクの環境設定]**に移動します。
 - b. 新しいディスクごとに、**物理ディスクの構成]**セクションの **[アクション]**ドロップダウンで、**[RAID への変換]**オプションを選択します。
ダイアログボックスに以下の警告メッセージが表示されます。
RAC0516: 物理ディスクドライブを RAID 互換に変換すると、OS で作成された RAID アレイは上書きされます。
OS で構成された RAID アレイが存在しないことを確認し、**[OK]**をクリックします。
 - c. **[OK]**をクリックします。
[保留中のアクション]の下に RAID ステータスが表示されます。



- d. 以下のオプションのいずれかをクリックして、保留中のアクションを完了します。

今すぐ適用

RAID 変換アクションがすぐに開始されます。

次回の再起動時

次の再起動時に RAID 変換アクションが開始されます。

スケジュールされた日時

スケジュールされた日時に RAID 変換アクションが開始されます。

すべての保留中を破棄

すべてのディスクの RAID 変換アクションが破棄されます。

- e. **[メンテナンス]- [ジョブ キュー]**に移動します。

RAID へのディスク変換を実行中のジョブリストが表示されます。RAID への変換ジョブが完了すると、ステータスが **完了 (100%)** に変更されます。

3. 以下の手順に従い、仮想ディスクを作成します。

- [環境設定]- [ストレージの環境設定]- [仮想ディスクの設定]**に移動します。
- [仮想ディスクの構成]**セクションで、**[仮想ディスクの作成]**をクリックします。
- [レイアウト]**で「**RAID-6**」を選択します。

- d. **物理ディスクの選択**] セクションで、RAID に変換するディスクを選択します。
- e. **保留中の操作に追加**] をクリックします。

Create Virtual Disk

Name	<input type="text" value="Enter or use auto-name"/>
Layout	RAID-6 ▼
Media Type	HDD ▼
Stripe Element Size	64 KB ▼
Capacity*	<input type="text" value="14.55"/> TB ▼
Read Policy	Read Ahead ▼
Write Policy	Write Back ▼
Disk Cache Policy	Default ▼
T10 PI Capability	Disabled ▼
Span Count	1 ▼

- f. **環境設定**] - **ストレージの環境設定**] に移動します。
- g. 以下のオプションのいずれかをクリックして、保留中の処理を完了します。

今すぐ適用

仮想ディスクの作成処理がすぐに開始されます。

次回の再起動時

次の再起動時に仮想ディスクの作成処理が開始されます。

スケジュールされた日時

スケジュールされた時刻に仮想ディスクの作成処理が開始されます。

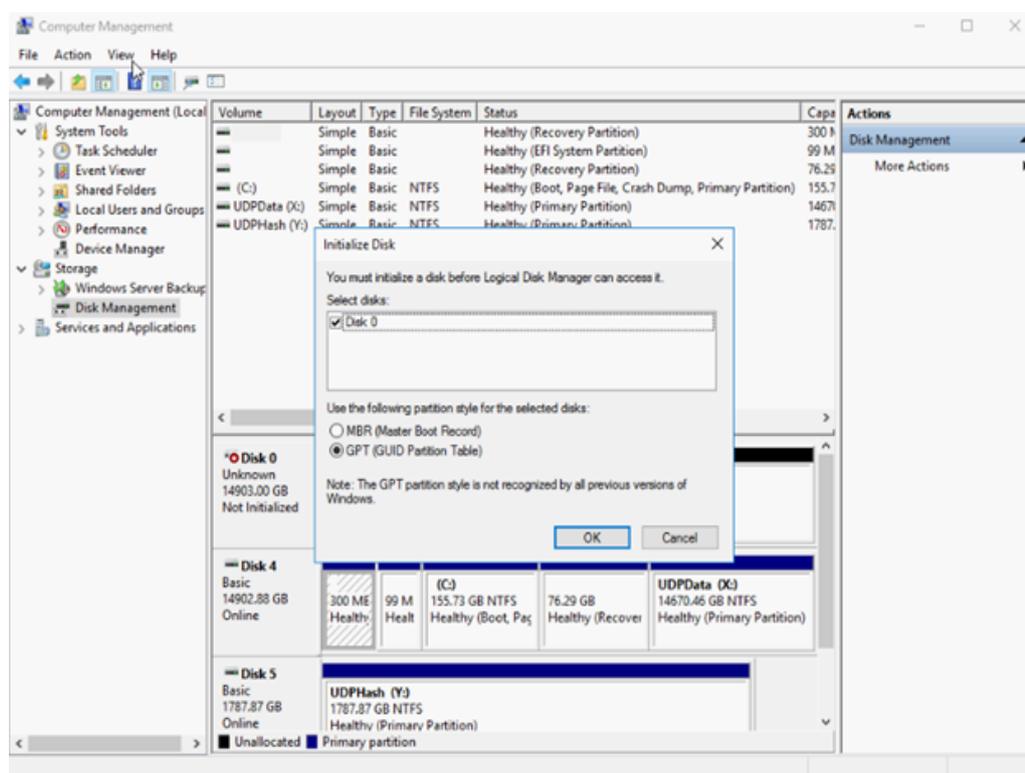
すべての保留中を破棄

すべてのディスクに対して、仮想ディスク作成処理が破棄されます。

- h. **メンテナンス**] - **ジョブ キュー**] に移動します。

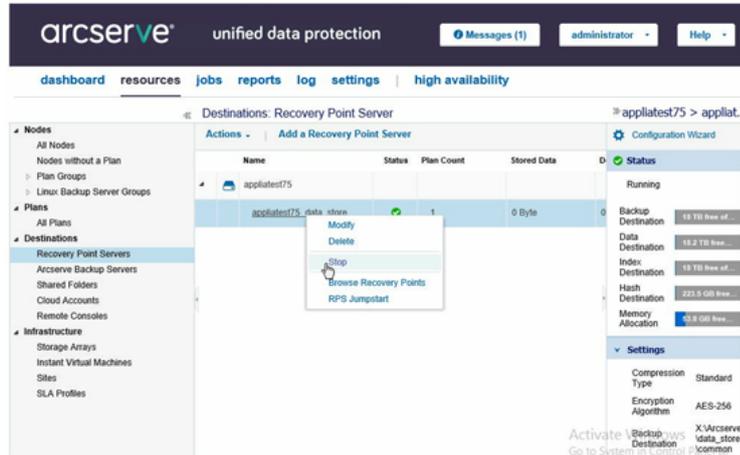
仮想ディスクの作成を実行中のジョブリストが表示されます。仮想ディスクの作成ジョブが完了すると、ステータスが **完了 (100%)** に変更されます。

- i. [コンピュータ管理]- [ディスク管理]に移動します。
- j. 追加した新しい仮想ディスクをダブルクリックします。
[ディスクの初期化]ウィンドウが表示されます。
- k. [GPT (GUIDパーティションテーブル)] オプションを選択して、[OK] をクリックします。
- l. [ディスクの管理] ウィンドウで仮想ディスクを選択し、以下のプロパティを適用します。
 - ドライブ文字の割り当て
 - ファイルシステムとして NTFS を指定します。
 - ディスクのフォーマット



4. 以下の手順に従い、データストアを拡張します。
 - a. 追加したドライブに移動し、フォルダを作成します。
 - b. Arcserve アプライアンス デスクトップで Arcserve アプライアンス ウィザードを起動します。
[Arcserve アプライアンス 環境設定] ページが表示されます。
 - c. [UDP コンソールの起動] をクリックします。
[Arcserve UDP コンソール ログイン] ページが表示されます。

- d. 管理者としての UDP コンソールにログインします。
- e. [ソース]- [デスティネーション]- 復旧ポイント サーバ]に移動します。
- f. データストアを右クリックし、 [停止] をクリックします。



- g. コマンド ラインから C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN に移動し、以下のコマンドを実行します。

```
as_gddmgr.exe -DataPath Add <データストア名> -NewDataPath <新規データフォルダ>
```

以下の画面の例では、ボリューム容量、使用容量、プライマリデータパスの空き容量、拡張データパスの空き容量、合計値などの詳細が表示されています。合計値は、プライマリデータパスと拡張データパスの合計です。

以下のコマンドを実行して、データパスの詳細を表示することもできます。

```
as_gddmgr.exe -DataPath Display <データストア名>
```

```
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>as_gddmgr.exe -DataPath Add appliatest75_data_store -NewDataPath Y:\data
Successfully load data store configuration information.
Successfully added new expanded data path for the data store.
The data store has 1 expanded data path(s) now:

          Volume capacity      Used space      Free space
Primary data path : X:\Arcserve\data_store\data\
                  18384 GB      1 GB          18383 GB
Expanded data path1: Y:\data
                  224 GB       1 GB          223 GB
Total              18608 GB      2 GB          18606 GB
Success to add data path Y:\data.
C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN>
```

データストアへの新しい拡張データパスの追加が完了します。

- h. UDP コンソールで、[ソース]- [デスティネーション]- 復旧ポイントサーバ]に移動します。
- i. データストアを右クリックし、**開始]** をクリックします。
- j. 一時停止していたプランを UDP コンソールから再開します。

Arcserve アプライアンス のデータ容量の拡張が完了します。

Arcserve アプライアンス 9072-9504 DR モデルの SSD フラッシュ拡張キットの操作

Arcserve SSD フラッシュ拡張キットを使用すると、セカンダリデータストアを作成してデータ容量を拡張し、Arcserve アプライアンス 9072-9504DR モデルで DR 関連操作 (IVM / VSB / Continuous Availability) を実行します。

以下の手順に従います。

1. 以下の手順に従い、空のディスクスロットに SSD を挿入します。
 - a. Arcserve UDP コンソールで、アプライアンス サーバ上に実行中のジョブがないことを確認します。実行中のジョブがある場合は、対応するプランを一時停止します。
 - b. SSD を空のディスクスロットに挿入します。



2. 以下の手順に従い、iDRAC で RAID-5 を設定します。
 - a. iDRAC にログインしてから、**環境設定]- [ストレージの環境設定]- 物理ディスクの環境設定]**に移動します。
 - b. **物理ディスクの環境設定]**セクションで、それぞれの新しい SSD ディスクの **アクション]**ドロップダウンリストから、**RAID 変換]**オプションを選択します。

ダイアログボックスに以下の警告メッセージが表示されます。

RAC0516: 物理ディスクドライブを RAID 互換に変換すると、OS で作成された RAID アレイは上書きされます。

OS で構成された RAID アレイが存在しないことを確認し、**[OK]** をクリックします。
 - c. **[OK]** をクリックします。

メディアの種類が SSD であるため、[保留アクション]列の下に [RAID 変換]ステータスが表示されます。

Status	Name	State	Hotspare Status	Capacity	Media Type	Action	Pending Actions
✓	Physical Disk 0:1.10	Non-RAID	Unassigned	10949.00 GB	HDD	Action	Convert to RAID
✓	Physical Disk 0:1.11	Non-RAID	Unassigned	10949.00 GB	HDD	Action	Convert to RAID
✓	Physical Disk 0:1.14	Non-RAID	Unassigned	10949.00 GB	HDD	Action	Convert to RAID
✓	Physical Disk 0:1.15	Non-RAID	Unassigned	10949.00 GB	HDD	Action	Convert to RAID
✓	Physical Disk 0:1.16	Non-RAID	Unassigned	10949.00 GB	HDD	Action	Convert to RAID
✓	Physical Disk 0:1.17	Non-RAID	Unassigned	10949.00 GB	HDD	Action	Convert to RAID

- d. 以下のオプションのいずれかをクリックして、保留中のアクションを完了します。

今すぐ適用

RAID 変換アクションがすぐに開始されます。

次の再起動時

次の再起動時に RAID 変換アクションが開始されます。

スケジュールされた日時

スケジュールされた日時に RAID 変換アクションが開始されます。

すべての保留中を破棄

すべてのディスクの RAID 変換アクションが破棄されます。

- e. [メンテナンス]- [ジョブ キュー]に移動します。

RAID へのディスク変換を実行中のジョブリストが表示されます。RAID 変換ジョブが完了すると、ステータスに 100% と表示されます。

Status	Name	State	Slot Number	Size	Security Status	Bus Protocol	Media Type	Hot Spare	Remaining Rated Write Endurance
+	Physical Disk 0:1.0	Online	0	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	Solid State Disk 0:1.1	Online	1	1676.38 GB	Not Capable	SAS	SSD	No	100%
+	Solid State Disk 0:1.2	Online	2	1676.38 GB	Not Capable	SAS	SSD	No	100%
+	Solid State Disk 0:1.3	Online	3	1676.38 GB	Not Capable	SAS	SSD	No	100%
+	Solid State Disk 0:1.4	Online	4	1676.38 GB	Not Capable	SAS	SSD	No	100%
+	Solid State Disk 0:1.12	Online	12	1787.88 GB	Not Capable	SATA	SSD	No	100%
+	Solid State Disk 0:1.13	Online	13	1787.88 GB	Not Capable	SATA	SSD	No	100%
+	Physical Disk 0:1.14	Online	14	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	Physical Disk 0:1.15	Online	15	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable
+	Physical Disk 0:1.16	Online	16	7451.5 GB	Not Capable	SAS	HDD	No	Not Applicable

3. 以下の手順に従い、仮想ディスクを作成します。

- a. **環境設定]- [ストレージの環境設定]- 仮想ディスクの設定]**に移動します。
- b. **仮想ディスクの構成]**セクションで、**仮想ディスクの作成]**をクリックします。
- c. **仮想ディスクの作成]**ウィンドウで以下を実行し、それ以外はデフォルトのままにします。
 - **レイアウト** - ドロップダウンリストから、**[RAID-5]**を選択します。
 - **メディアの種類** - ドロップダウンリストから、**[SSD]**を選択します。
- d. **物理ディスクの選択]**セクションで、下にスクロールして RAID に変換するすべての SSD ディスクを選択します。
- e. **保留中の操作に追加]**をクリックします。

Create Virtual Disk

Name: UDPFlash

Layout: RAID-5

Media Type: SSD

Stripe Element Size: 64 KB

Capacity*: 10.48 TB

Read Policy: Read Ahead

Write Policy: Write Back

Disk Cache Policy: Default

T10 PI Capability: Disabled

Span Count: 1

Cancel Add to Pending Operations

- f. **環境設定]- [ストレージの環境設定]**に移動します。
- g. 仮想ディスクの作成処理をすぐに行うには、**今すぐ適用]**をクリックします。

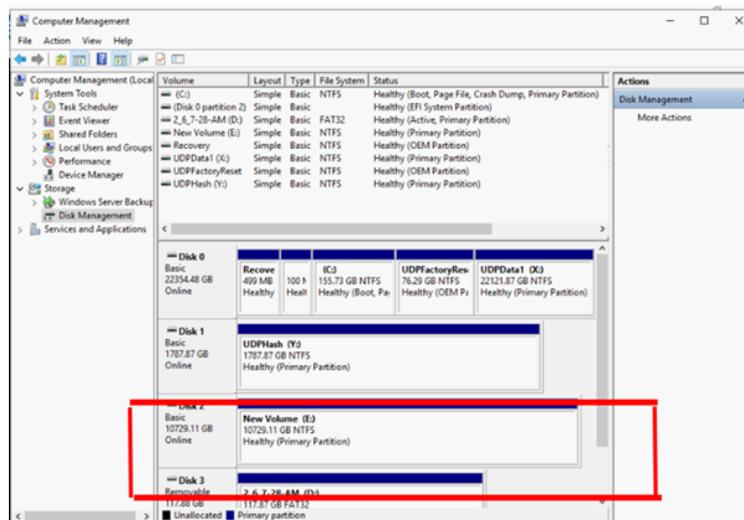
Status	Name	RAID Level	Dedicated Hotspans	Virtual Disk Actions	Pending Actions
<input checked="" type="checkbox"/>	UDFdata	RAID-5	None	Action	
<input checked="" type="checkbox"/>	UDFspan	RAID-1	None	Action	
<input checked="" type="checkbox"/>	UDFflash	RAID-5	None	Action	

- h. **[メンテナンス]- [ジョブ キュー]**に移動します。

仮想ディスクの作成を実行中のジョブリストが表示されます。仮想ディスクのジョブを作成すると、ステータスが **[100%]**に変更されます。

- i. **[コンピュータ管理]- [ディスク管理]**に移動します。

- j. 追加した新しい仮想ディスクをダブルクリックします。
ディスクの初期化] ウィンドウが表示されます。
- k. [GPT (GUID パーティション テーブル)] オプションを選択して、[OK] をクリックします。
- l. [ディスクの管理] ウィンドウで仮想ディスクを選択し、以下のプロパティを適用します。
 - ◆ ドライブ文字の割り当て
 - ◆ ファイルシステムとして NTFS を指定します。
 - ◆ ディスクのフォーマット



仮想ディスクが作成されます。

第10章: ネットワーク設定の操作

このセクションには、以下のトピックが含まれます。

ネットワーク設定の詳細	200
DHCP サーバを無効化する方法	204
プリインストールされた Linux バックアップ サーバの IP アドレスを設定する方法	205
負荷分散のために DNS サーバ上でラウンド ロビンを有効にする方法	207
アプライアンスのネットワークステータスを確認する方法	208

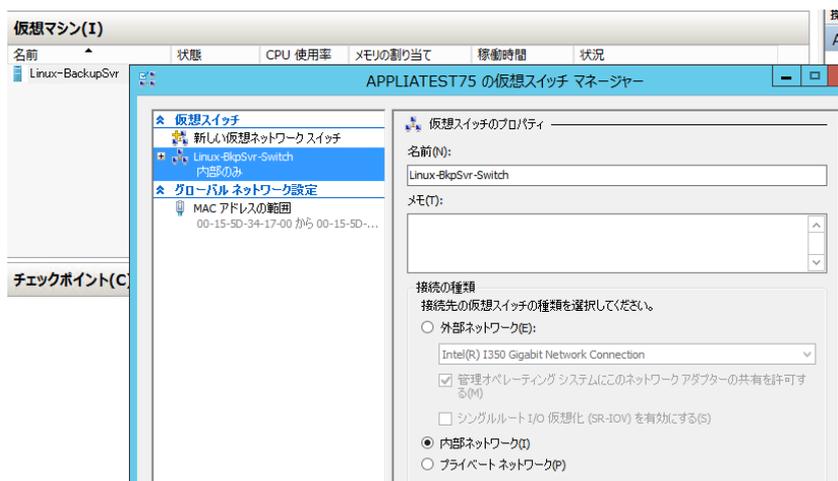
ネットワーク設定の詳細

アプライアンスのネットワーク設定により、組み込み Linux バックアップ サーバ (HYPER-V マネージャでの仮想名: Linux BackupSvr) を NAT の背後で稼働させることができます。これにより以下の利点があります。

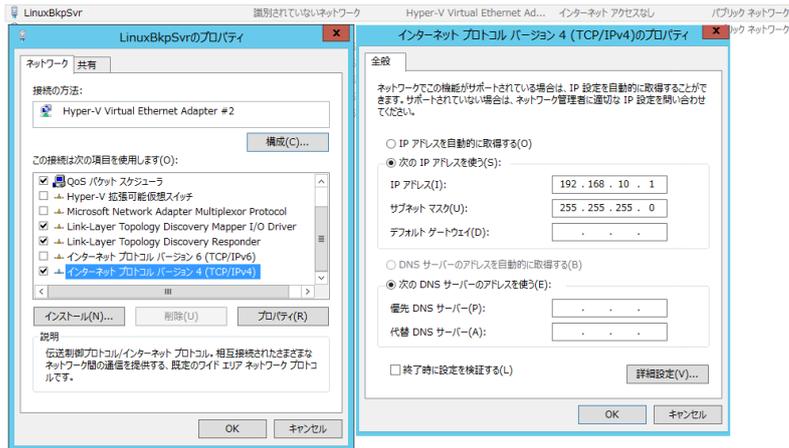
- ユーザは、組み込み Linux のホスト名を変更する必要がありません。
- ユーザは、Linux バックアップ サーバのネットワーク上の IP を保存します。
- Linux バックアップ サーバは、パブリック ネットワーク上のマシンに接続できます。
- アプライアンス サーバ専用の特別なポートを介して、パブリック ネットワーク上の任意のマシンを Linux バックアップ サーバに接続できます。

ネットワーク設定の詳細:

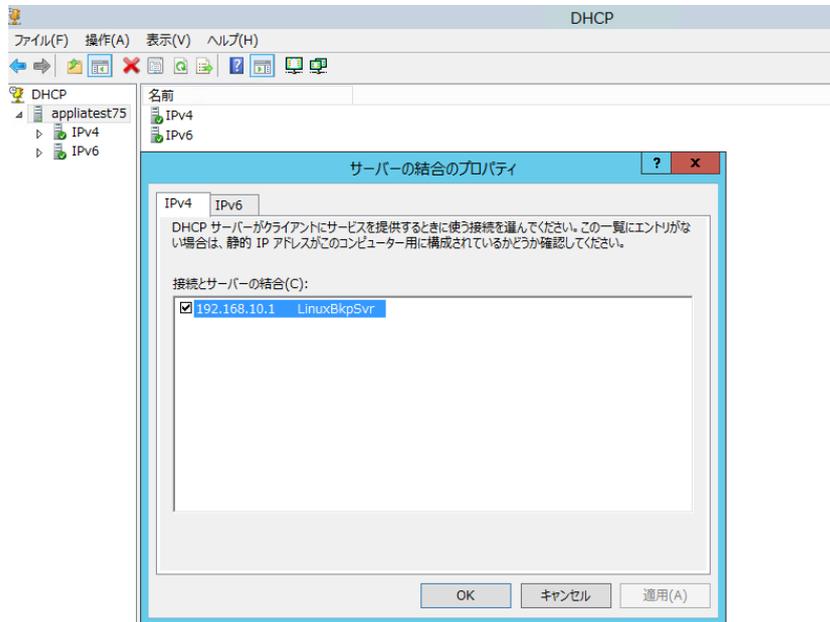
- Hyper-V マネージャで、Linux-BackupSvr によってのみ使用される内部のみの仮想スイッチ - *Linux-BkpSvr-Switch* が利用可能です。



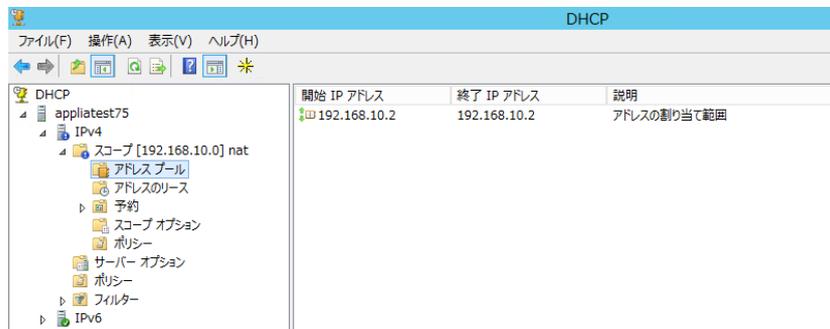
- コントロールパネル\ネットワークとインターネット\ネットワーク接続に、「LinuxBkpSvr」という名前の「Hyper-V Virtual Ethernet Adapter」が表示されます。デフォルトでは、以下のように、このスイッチの IPv4 を 192.168.10.1 として設定しています。



- デフォルトで、アプライアンスマシンには DHCP サーバが設定されています。DHCP サーバは、HYPER-V 仮想アダプタ上でのみ稼働します。



- デフォルトでは、アドレスプールには 192.168.10.2 のみがあり、これによって、組み込み Linux バックアップ サーバが IP 192.168.10.2 を確実に取得できます。



- アプライアンスマシン上で NAT が設定されました。

名前	状態	デバイス名	接続	ネットワークのカテゴリ
LinuxBkpSvr	識別されていないネットワーク	Hyper-V Virtual Ethernet Ad...	インターネット アクセスなし	パブリック ネットワーク
イーサネット	無効	Intel(R) I350 Gigabit Netwo...		
イーサネット 2	無効	Intel(R) I350 Gigabit Netwo...		
イーサネット 5	ARCserve.COM	Intel(R) I350 Gigabit Netwo...	インターネット アクセス	パブリック ネットワーク
イーサネット 6	無効	Intel(R) I350 Gigabit Netwo...		

```
C:\Windows\System32>netsh routing ip nat dump

# -----
# NAT 構成
# -----
pushd routing ip nat
uninstall
install
set global tcptimeoutmins=1440 udptimeoutmins=1 loglevel=ERROR

#
# インターフェイス イーサネット 2 の NAT 構成
#
add interface name="イーサネット 2 " mode=FULL

#
# インターフェイス イーサネット 5 の NAT 構成
#
add interface name="イーサネット 5 " mode=FULL

#
# インターフェイス LinuxBkpSvr の NAT 構成
#
add interface name="LinuxBkpSvr" mode=PRIVATE

popd
```

- Linux バックアップ サーバ用に、アプライアンス上でポート リダイレクションを設定しています。

```
C:\Windows\System32>netsh interface portproxy show all

ipv4 をリッスンする:          ipv4 に接続する:
Address      Port      Address      Port
-----
*            8018     192.168.10.2  8014
*            8019     192.168.10.2   22
*            8035     192.168.10.2  8035
```

- Linux バックアップ サーバは、DHCP サーバから IP アドレス 192.168.10.2 を取得します。IP アドレスを取得した後、バックエンド スクリプト (C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1) は Linux と通信し、Linux のシステム ロケールを変更して、アプライアンス Windows OS のシステム ロケールと一致させます。

```
[root@Linux-BackupSvr network-scripts]# cat ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=dhcp
DEFROUTE=yes
NAME="eth0"
[root@Linux-BackupSvr network-scripts]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:15:5D:0A:04:00
          inet6 addr: fe80::215:5dff:fe0a:400/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:481943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100859 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36784482 (35.0 MiB)  TX bytes:21795976 (20.7 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

DHCP サーバを無効化する方法

DHCP サーバは、アプライアンス上ではデフォルトで有効になります。DHCP サーバが、アプライアンス上の Hyper-V 仮想 Ethernet アダプタ - *LinuxBkpSvr* でのみ動作し、プリインストールされた Linux バックアップ サーバが IP アドレスを取得でき、アプライアンスとの通信が可能で、実稼働ネットワーク環境に影響を与えないことを確認します。

DHCP サーバを無効にするには、次の手順を実行します。

1. ファイル *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties* を開きます。
2. ファイルを *DHCP_ENABLE=false* と変更します。*Appliance.properties*には以下のように表示されます。

```
DHCP_ENABLE=false  
AdapterName=LinuxBkpSvr  
Appliance_IPAddress=192.168.10.1  
Linux_IPAddress=192.168.10.2
```

3. ファイルを保存します。
4. ファイル *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag* を削除します。
5. *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\resetdhcp.ps1*を DOS コマンド ラインから以下のように実行し、DHCP サーバサービスを無効化します。

```
C:\Program Files\Arcserve\Unified Data  
Protection\Engine\BIN\Appliance>powershell .\resetdhcp.ps1
```

プリインストールされた Linux バックアップ サーバの IP アドレスを設定する方法

注: この方法は、Arcserve Appliance for 9000 シリーズ以降に適用できます。

プリインストールされた Linux バックアップ サーバは、デフォルトで IP 192.168.10.2 を使用して、アプライアンス サーバと通信します。プリインストールされた Linux バックアップ サーバがアプライアンス サーバと通信する方法については、プリインストールされた Linux バックアップ サーバのネットワーク設定の概要を参照してください。

プリインストールされた Linux バックアップ サーバの IP アドレスを指定するには、次の手順を実行します。

1. `C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\Configuration\Appliance.properties` ファイルを開きます。
2. `Appliance_IPAddress` および `Linux_IPAddress` の IP アドレスを変更します。たとえば、`Appliance_IPAddress` を 192.168.100.1 に、`Linux_IPAddress` を 192.168.100.2 に設定します。

注:

- ◆ `Appliance_IPAddress` の IP アドレスは、このプリインストールされた Linux バックアップ サーバとの通信に使用されるネットワーク インターフェイス `LinuxBkpSvr` (Hyper-V 仮想 Ethernet アダプタ) に設定されます。
- ◆ `Linux_IPAddress` の IP アドレスは、プリインストールされた Linux バックアップ サーバに設定されます。
- ◆ `Appliance_IPAddress` および `Linux_IPAddress` が同じサブ ネットワークの IP アドレスを使用していることを確認してください。

変更後、ファイルの内容は以下ようになります。

```
DHCP_ENABLE=true
AdapterName=LinuxBkpSvr
Appliance_IPAddress=192.168.100.1
Linux_IPAddress=192.168.100.2
```

3. ファイルを保存します。
4. `C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\dhcpdone.flag` ファイルを削除します。
5. `C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance\User_Uilities\UpdateIcsHostAdapter.ps1`

を実行し、ネットワーク インターフェイス LinuxBkpSvr とプリインストールされた Linux バックアップ サーバの IP アドレスをリセットします。

注:

- ユーザが *Linux_IPAddress* を変更する場合、処理中にプリインストールされた Linux バックアップ サーバはシャットダウンし、再起動します。
- 実稼働 NIC アダプタのインターネット 接続を LinuxBkpSvr アダプタと共有するには、*UpdateIcsHostAdapter.ps1* ファイルを実行します。特定の NIC アダプタのインターネット 接続を LinuxBkpSvr アダプタと共有する場合は、以下のレジストリを調整します。

インターネット 接続の共有に使用するネットワーク アダプタの名前を指定するには、以下のレジストリキーを作成します

パス: "*HKLM:\SOFTWARE\Arcserve\Unified Data Protection\Appliance*"

値の種類: "文字列"

値の名前: "*IcsHostAdapter*"

値のデータ: "<Adapter Name> "

6. 上記のレジストリを変更した後、以下のコマンドを実行します。

```
C:\Program Files\Arcserve\Unified Data  
Protection\Engine\BIN\Appliance\User_Utilities >powershell .\  
UpdateIcsHostAdapter.ps1
```

負荷分散のために DNS サーバ上でラウンド ロビンを有効にする方法

Microsoft DNS サーバでは、サーバ間の負荷分散に使用される技術であるラウンド ロビンをサポートしています。この機能によって、DNS では `myserver.mydomain.com` のクエリを受信する場合に両方の IP アドレスを送信できます。クライアント (またはリゾルバ) では、常に最初のものを使用します。次に DNS がこの名前前のクエリを受信するときに、IP アドレスのリストの順序はラウンド ロビン手法を使用して変更されます (以前のリストで 1 番目だったアドレスは、新しいリストの最後になります)。1 つのエイリアスに対して 1 つのカノニカル名しか許可されないため、名前レコードのラウンド ロビンはサポートされていません。

アプライアンスで、ドメイン ネーム サーバ (DNS) にすべての IPv4 アドレスのレコードを追加し、ネットワーク インターフェース全体で負荷分散することができます。

サーバ間の負荷分散の詳細については、[RFC 1794](#) を参照してください。

追加の IP アドレスのレコードをドメイン ネーム サービス サーバに追加する方法

サーバに 2 つ以上のネットワーク インターフェースカード (NIC) があるか、サーバの NIC に 2 つ以上の IP アドレスが指定されている場合は、各 IP アドレスの「A」レコードを作成することによって、追加の IP アドレスのレコードを DNS サーバに追加できます。

例:

サーバの DNS ホスト名が `<myserver>` で、DNS ドメイン名が `<mydomain.com>` であるとして、このサーバには、以下の 2 つの IP アドレスが割り当てられています。

- IPAddress1
- IPAddress2

これらの IP アドレスを DNS サーバに追加するには、以下のように 2 つの「A」レコードを `<mydomain.com>` ゾーンに作成します。

- Myserver A <IPAddress1>
- Myserver A <IPAddress2>

リゾルバが毎回同じ IP アドレスを取得できるようにするには、以下のように、各アドレスに一意的な名前を割り当てる「A」レコードをさらに 2 つ作成します。

- Altname1 A <IPAddress1>
- Altname2 A <IPAddress2>

この方法を使用すると、リゾルバは Altname1 に対するクエリを送信するときは常に IPAddress1 を取得し、Altname2 に対するクエリを送信するときは常に IPAddress2 を取得します。

アプライアンスのネットワークステータスを確認する方法

ApplianceNetworkStatusCheck.ps1 ツールは、Arcserve アプライアンス サーバの現在のネットワーク状態全体に関する情報を収集し、XML 形式でレポートを生成するために使用されます。このレポートには、ネットワークアダプタ、ネットワークスイッチ、Hyper-V 仮想スイッチ、DHCP (Dynamic Host Configuration Protocol、動的ホスト構成プロトコル)、DNS (Domain Name System、ドメインネームシステム)、RRAS (Route and Remote Access Service、ルーティングとリモートアクセスサービス)、およびサーバ上のその他の主要な設定に関する情報が含まれます。

ApplianceNetworkStatusCheck.ps1 ツールは、Arcserve アプライアンス サーバ UDP V7.0 Update1 で利用可能です。

このツールを使用してアプライアンス サーバのネットワークステータスレポートを生成するには、以下の手順に従います。

1. 管理者として Arcserve アプライアンス サーバにログインします。
2. コマンド プロンプトを開き、フォルダの場所を入力します。

C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance

3. ApplianceNetworkStatusCheck.ps1 を実行してレポートを生成します。

```
#Powershell .\ApplianceNetworkStatusCheck.ps1
```

```
c:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance>powershell .\ApplianceNetworkStatusCheck.ps1
1. Check network switch
2. Check HyperV virtual switch
3. Check DHCP service and properties
4. Check ipv4 to ipv4 tcp netsh interface portproxy
5. Check RRAS NAT interface
CHECK FINISH
Start create html report
```

ブラウザが開き、アプライアンス サーバのネットワークステータスレポート全体が表示されます。

第11章: 安全に関する注意事項についての理解

このセクションには、以下のトピックが含まれます。

一般的な安全に関する注意事項	210
電気に関する安全のための注意事項	212
FCC コンプライアンス	213
静電気放電 (ESD) に関する注意事項	214

一般的な安全に関する注意事項

以下の一般的な安全に関する注意事項に従い、安全に注意を払い、またアプライアンスを障害や誤動作から保護する必要があります。

- EMI クラス A 機器 (商用機器) の場合、本装置は家庭用ではなく、商用機器 (A) として EMC (Electromagnetic Compatibility) Registration に登録されています。販売者およびユーザは、この点において注意する必要があります。

A급 기기 (업무용 방송 통신기자재)

이 기기는 업무용 (A급) 으로 전자파 적합 기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다

注: この注意事項は韓国にのみ適用されます。詳細については、Arcserve サポート (<https://www.arcserve.com/support>) までお問い合わせいただくか、0079885215375 (韓国) までお電話ください。

- アプライアンスに同梱されている内容をチェックして破損がないことを確認します。破損の証拠がある場合は、すべてのパッケージ資材を保持して Arcserve サポートにご連絡ください: <https://www.arcserve.com/support>。
- アプライアンスを格納するラックユニットの適切な場所を決定します。これは、よく換気され、ごみなどがなく清潔かつ無塵の領域に配置する必要があります。熱、電氣的ノイズ、電磁場が生じる場所は避けてください。
- また、接地された電源コンセントが少なくとも 1 つある場所の近くに配置する必要があります。モデルによっては、アプライアンスに 1 つの電源または冗長電源装置のいずれかが含まれており、2 つの接地されたコンセントが必要になります。
- アプライアンスは、限られた場所でのみ使用するものです。
 - 場所に適用される制限の理由および従うべき注意事項について指示されているユーザまたはサービス担当者からアクセスを得ることができます。
 - アクセスするには、ツールまたはロックおよびキー、セキュリティの別の手段によって与えられ、その場所に責任を持つ担当者によって制御されます。
- アプライアンスから取り外した上部のカバーやコンポーネントは、誤って踏むことがないようにテーブルの上に置きます。

- アプライアンスを使用して作業する際は、ネクタイや袖のボタンを留めていないシャツなどゆるやかな服装は避けてください。そのような服装は、電子回路に触れたり、冷却ファンに巻き込まれたりする可能性があります。
- 宝飾品や金属のものは、金属導体であり、プリント基板(PCB)または電流が流れている場所に接触すると、ショートしたり損傷を生じさせたりする可能性があるため、身に付けしないでください。
- アプライアンスの内部にアクセスし、すべての接続が行われたことを確認したら、アプライアンスを閉じて、留めねじでラックユニットに固定します。

電気に関する安全のための注意事項

以下の電気安全に関する注意事項に従い、安全に注意を払い、またアプライアンスを障害や誤動作から保護する必要があります。

- アプライアンス上の電源オン/オフのスイッチの場所と、部屋の緊急電源遮断スイッチ、切断スイッチ、電源コンセントの場所を確認します。電氣的事故が発生した場合は、アプライアンスから電力を素早く切断することができます。
- 高電圧の部品を扱う場合は、1人で作業しないでください。
- システムの主要部品(サーバボード、メモリモジュール、DVD-ROM、フロッピードライブなど)を取り外したり配置したりする場合は、必ずアプライアンスから電力を切断する必要があります(ホットスワップ可能なドライブには必要ありません)。電力を切断する場合は、最初にオペレーティングシステムでアプライアンスの電源を切り、次にアプライアンスのすべての電源モジュールから電源コードのプラグを抜きます。
- 露出している電子回路の周りで作業する場合、電源切断の制御に慣れている別の担当者が待機し、必要に応じて電源スイッチをオフにする必要があります。
- 電源がオンになっている電子機器を扱う場合は、片手のみを使用します。これは、完全に閉じられた回路を防ぐためです。完全な回路は電気ショックを引き起こす可能性があります。金属のツールを使用する場合、電子部品や回路基板に接触すると簡単に損傷を与える可能性があるため、特に注意します。
- 感電からの保護として静電気を軽減するために設計されたマットは使用しないでください。代わりに、電気絶縁体として特別に設計されているゴムのマットを使用します。
- 電源装置の電源コードには、アース端子付きプラグが含まれている必要があります。アース接地用コンセントに接続する必要があります。
- サーバボード バッテリ: **注意** - オンボード バッテリの上下を逆に設置すると、極性が逆になり、爆発の危険があります。このバッテリーは、メーカーによって推奨されるのと同じ種類または同等の種類でのみ置き換える必要があります。メーカーの指示に従って使用済みバッテリーを破棄します。
- DVD-ROM レーザー: **注意** - このサーバには、DVD-ROMドライブが装備されている場合があります。レーザービームへの直接の露出および有害な放射線被ばくを回避するため、筐体を開いたり、通常とは異なる方法でユニットを使用したりしないでください。

FCC コンプライアンス

このアプライアンスは、FCC 規則の Part 15 に準拠しています。以下の条件に従って運用される必要があります。

- このアプライアンスは、有害な干渉を引き起こしません
- このアプライアンスは、受け取った干渉を受け入れる必要があります(意図しない操作を発生させる可能性がある干渉を含む)

注：この機器はテストされ、クラス A のデジタル機器の制限に従っており、FCC 規則の Part 15 に準拠していることが検証されています。これらの制限は、機器が商用目的で運用された場合に有害な干渉に対して適切な保護を提供するように設計されています。この機器は、電磁波を発生および利用し、外部に放射することがあり、正式な手順に従って設置および使用されない場合は、無線通信に有害な干渉を引き起こす可能性があります。住宅地域でこの機器を稼働させると、有害な干渉が発生する可能性があります。ユーザは自らの費用負担で干渉を是正する必要があります。

静電気放電(ESD)に関する注意事項

静電気放電(ESD)は、異なる電荷の2つの物体が互いに接触することによって生じます。静電気は、この電荷の違いを中和しようとして発生し、電子部品やプリント回路基板に損傷を与える可能性があります。ESDに敏感なデバイスには、サーバボード、マザーボード、PCIeカード、ドライブ、プロセッサ、メモ리카ードなどがあり、特殊な扱いが必要となります。接触する物体の電荷の違いを中和するための努力として、接触前に以下の注意事項に従い、機器をESDから保護します。

- 電気絶縁体として特別に設計されているゴムのマットを使用します。感電からの保護として静電気を軽減するために設計されたマットは使用しないでください。
- 静電気の放電を防ぐように設計されている接地されたリストストラップを使用します。
- 帯電または放電(ESD)を予防する洋服または手袋を使用します。
- すべての部品およびプリント回路基板(PCB)は、使用するまで静電気防止バッグに入れておきます。
- 基盤を静電気防止バッグから取り出す前に、接地されたメタルオブジェクトに触れません。
- 部品またはPCBが洋服に触れないようにします。触れた場合は、リストストラップを装着していても静電気を帯びる可能性があります。
- ボードを扱う際は、その端のみに触れるようにします。その部品、周辺チップ、メモリモジュール、接点に触れないでください。
- チップまたはモジュールを扱う場合、そのピンに触れないようにします。
- サーバボードおよび周辺機器を使用しない場合は静電気防止バッグに戻します。
- 接地目的のため、アプライアンスが、電源、ケース、マウントファスナー、サーバボード間で優れた伝導性を提供することを確認します。

Arcserve アプライアンス 10000 シリーズのファームウェアのアップグレード

このセクションでは、以下の実行方法について説明しています。

ファームウェアのバージョンの表示

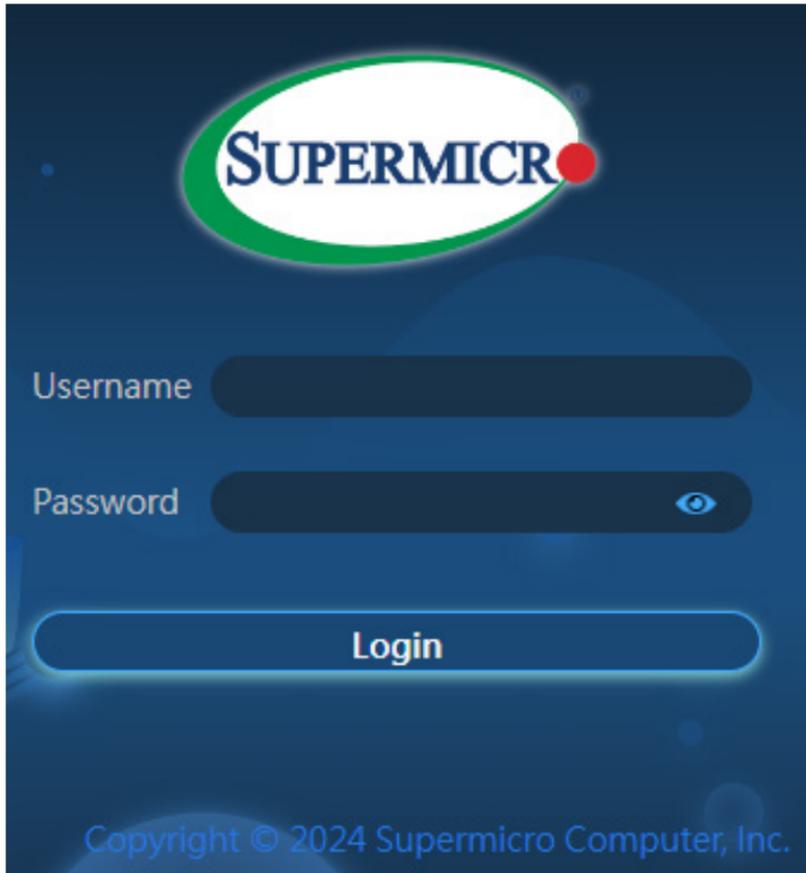
このセクションでは、最新のファームウェアのバージョンを表示する方法について説明します。

以下の手順に従います。

1. Web ブラウザを開き、IPMI (インテリジェントプラットフォーム管理インターフェース) の静的 IP を入力します。

[ログイン] 画面が表示されます。

2. 以下のようにログイン認証情報を入力します。
 - ユーザ名: ADMIN。
注: ユーザ名は大文字である必要があります。
 - パスワード: BMC パスワードを入力します。
3. [ログイン] をクリックします。

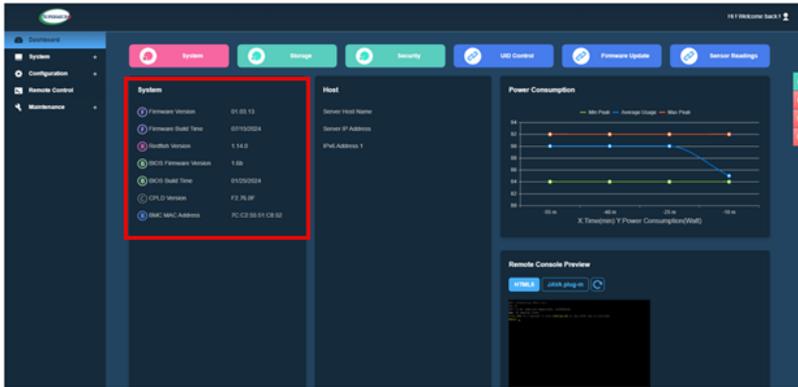


IPMI Web サーバ インターフェースが表示されます。

注：BMC/IPMI 固有のパスワードは、サーバの前面パネルにある引き出し式タグで確認できます。BMC パスワードは、BMC/IPMI MAC アドレスのすぐ下の行に記載されています。



[ダッシュボード] 画面の [システム] にファームウェアのバージョンが表示されます。



ファームウェア アップグレード パッケージのダウンロード

このセクションでは、最新のファームウェアバージョンをダウンロードする方法について説明します。

以下の手順に従います。

注：Supermicro Web サイトから最新のファームウェア更新パッケージをダウンロードするか、Supermicro サポートにお問い合わせください。

1. [Supermicro](#) Web サイトにアクセスします。
2. BMC リストで、サーバ 1U (X13SEW-F) または 2U (X13DEI-T) のマザーボード モデルを検索し、ファームウェア更新をダウンロードします。

BMC List

Model	Rev	Download ZIP 1	Release Notes	Description
X13SEDWF	X13SEDWF_2.5_AS01.03.31_SAA1.1.0-F_2.5_AS01.03.31_SAA1.1.0-p1	05.zip		Bundle
X14SBI-GAP	X14SBI-GAP_1.0_AS01.00.21.20_SAA1.1.0-1.00.21.20_5_SAA1.1.0-p5	05.zip		Bundle

3. 選択したマザーボード モデルに対応する **[Download Zip 1 (Zip 1 のダウンロード)]** をクリックします。
[End User License Agreement (使用許諾契約)] ページが表示されます。
4. **[Accept (同意する)]** をクリックして、ダウンロードを開始します。

ファームウェア更新ファイルがダウンロードされ、システムのローカルに保存されます。

注：ファームウェア更新ファイルの種類は、BMS や BIOS などのデバイスによって異なります。

ファームウェア更新ファイルが正常にダウンロードされました。

ファームウェアのアップグレード

このセクションには、以下のトピックが含まれます。

BMC ファームウェアのアップグレード方法

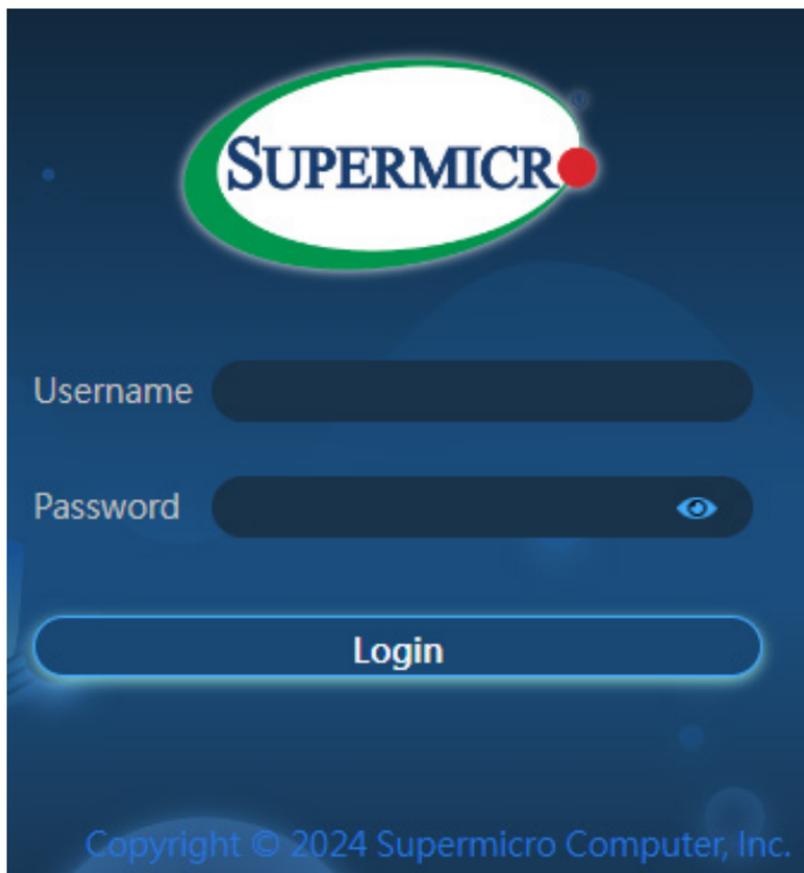
このセクションでは、BMC ファームウェアのアップグレードについて説明します。

以下の手順に従います。

1. Web ブラウザを開き、IPMI (インテリジェント プラットフォーム管理 インターフェイス) の静的 IP を入力します。

[ログイン] 画面が表示されます。

2. 以下のようにログイン認証情報を入力します。
 - ユーザー名: ADMIN。
注: ユーザー名は大文字である必要があります。
 - パスワード: BMC パスワードを入力します。
3. [ログイン] をクリックします。



IPMI Web サーバ インターフェイスが表示されます。

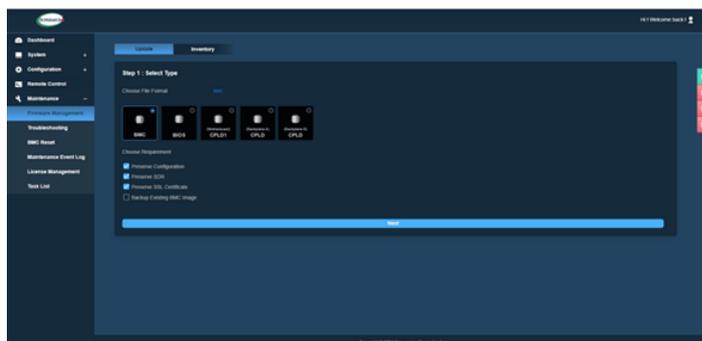
注：BMC の一意のパスワードは、サーバシャーシのサービスタグに記載されています。BMC パスワードは、IPMI (インテリジェント プラットフォーム管理インターフェース) の MAC アドレスのすぐ下の行に記載されています。



4. **メンテナンス**] > **firmware Management (ファームウェア管理)**] に移動します。
5. **更新**] 画面で、以下の操作を行います。
 - a. **step 1: Select Type (ステップ1: タイプの選択)**] で、ファイルフォーマットに **BMC**] を選択します。
 - b. (オプション) 必要に応じて、以下の設定の保存オプションを選択し、**次へ**] をクリックします。

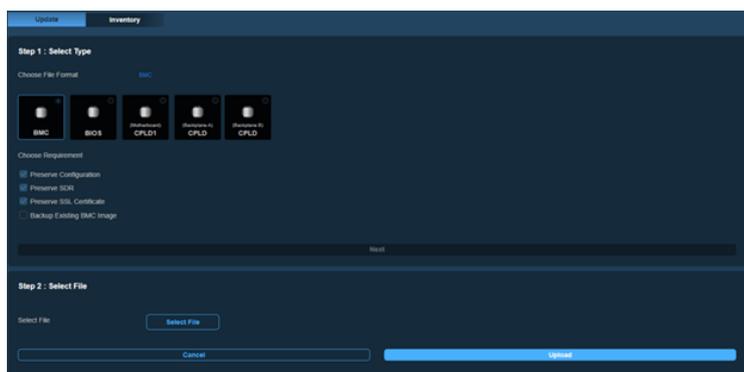
- Preserve Configuration (設定の保存) :
- Preserve SDR (SDR の保存) :
- Preserve SSL certificate (SSL 証明書の保存) :
- Backup existing BMC image (既存の BMC イメージをバックアップ) :

既存の BMC イメージをバックアップするには、**Backup Existing BMC Image (既存の BMC イメージをバックアップ)**] チェックボックスをオンにします。整合性が失われた場合はいつでも、バックアップイメージを使用して自動リカバリを実行できます。また、**インベントリ**] ページから BMC を手動で回復することもできます。

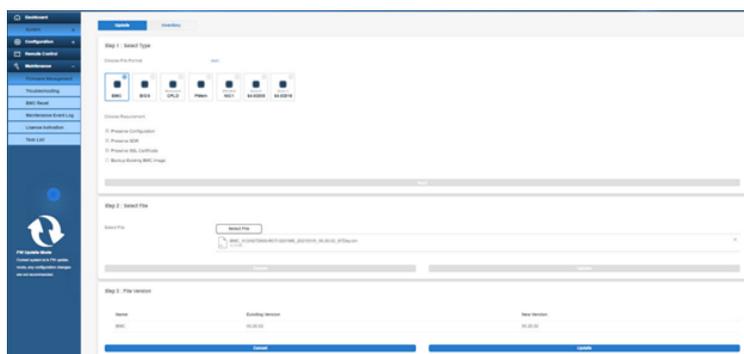


- c. *Step 2: Select File (ステップ2: ファイルの選択)* で、 **Select File (ファイルの選択)** をクリックし、ローカルに保存されたファームウェア更新ファイルを参照して、 **アップロード** をクリックします。

注: BMC イメージを含めずに **アップロード** をクリックすると、次のメッセージが表示されます: *Please select an image file. Click here to return (イメージファイルを選択してください。ここをクリックして戻ります)*。



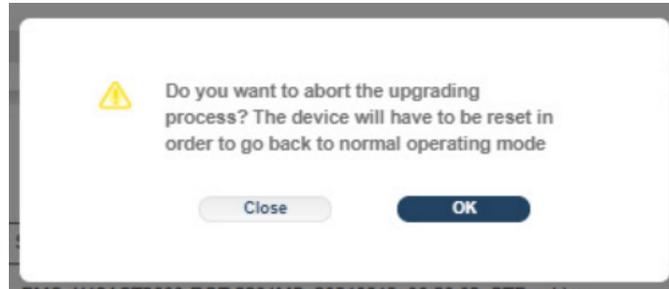
- d. *Step 3: File Version (ステップ3: ファイルのバージョン)* で、既存および新規のファームウェアバージョンを確認し、 **更新** をクリックします。



注:

- ほとんどのファームウェア更新では、システムのプロンプトに従ってマザーボードをシャットダウンする必要があります。マザーボードをシャットダウンした後、更新を続行できます。

- ファームウェア BMC の更新処理をキャンセルすると、アップグレードを中止するかどうかを確認するメッセージが表示されます。 [OK] をクリックすると BMC がリセットされ、「BMC is restarting (BMC を再起動しています) 」というメッセージが表示されます。データの損失を防ぐため、確認後、BMC がオンラインに戻るまで電源を切断しないでください。



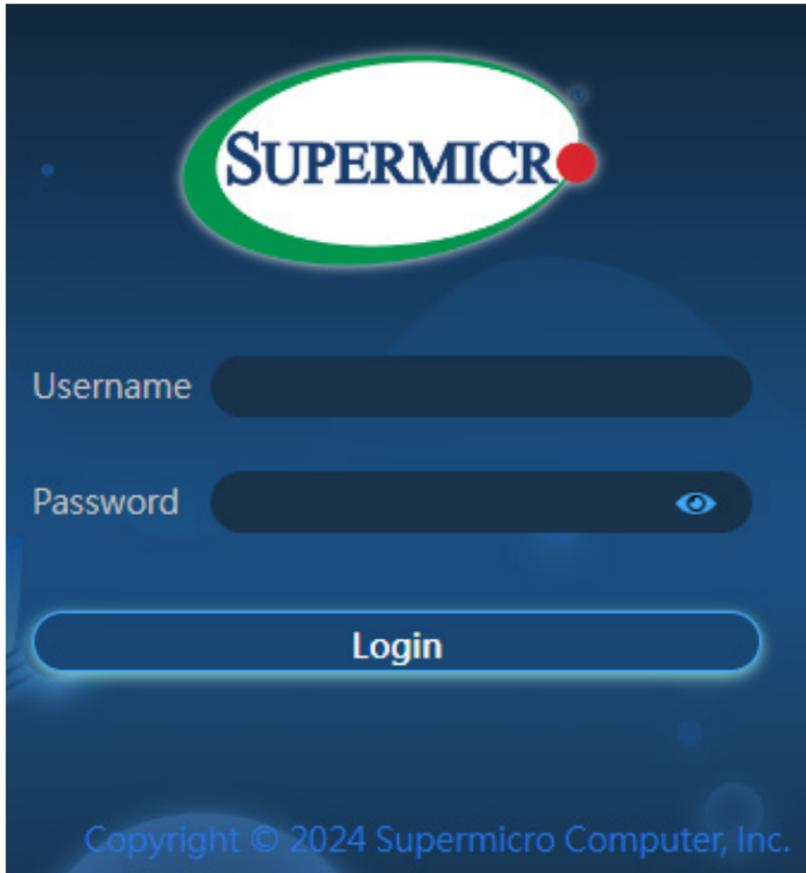
- ファームウェアの更新が完了した後、Web ブラウザの更新に時間がかかる場合があります。ログイン時に再起動メッセージが 1 ～ 2 分間表示される場合があります。

BMC のファームウェア アップグレードが正常に完了しました。

BIOS ファームウェアのアップグレード方法

BIOS ファームウェアをアップグレードするには、以下の手順に従います。

1. Web ブラウザを開き、IPMI (インテリジェント プラットフォーム管理 インターフェイス) の静的 IP を入力します。
[ログイン] 画面が表示されます。
2. 以下のようにログイン認証情報を入力します。
 - ユーザ名：ADMIN。
注：ユーザ名は大文字である必要があります。
 - パスワード：BMC パスワードを入力します。
5. [ログイン] をクリックします。



IPMI Web サーバ インターフェースが表示されます。

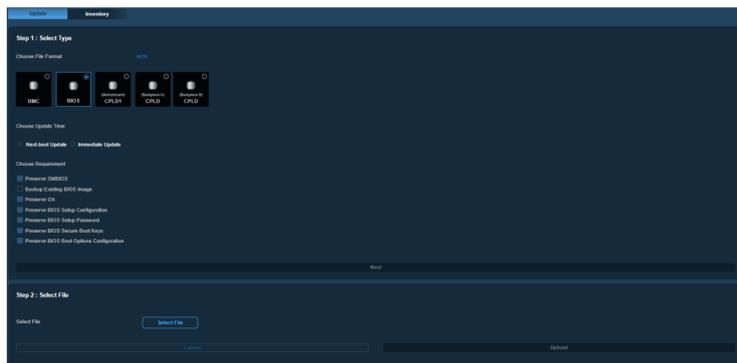
注：BMC の一意のパスワードは、サーバシャーシのサービス タグに記載されています。BMC パスワードは、IPMI (インテリジェント プラットフォーム管理 インターフェース) の MAC アドレスのすぐ下の行に記載されています。



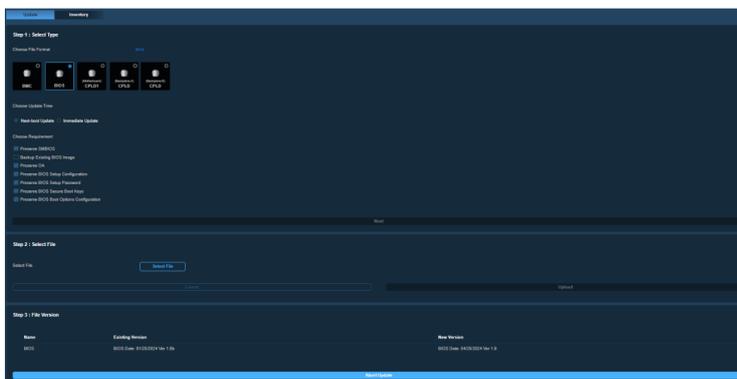
6. **メンテナンス**] > **firmware Management (ファームウェア管理)**] に移動します。
7. **更新**]画面で、以下の操作を行います。

- a. *\$step 1: Select Type (ステップ1: タイプの選択)*] で、ファイルフォーマットに **[BIOS]** を選択します。
- b. (オプション) 必要に応じて、以下の設定の保存オプションを選択し、**[次へ]** をクリックします。
 - Preserve SMBIOS (SMBIOS の保存)
 - Preserve OA (OA の保存)
 - Preserve SMBIOS (SMBIOS の保存)
 - Preserve BIOS Setup Configuration (BIOS セットアップ設定の保存)
 - Preserve BIOS Setup Password (BIOS セットアップパスワードの保存)
 - Preserve BIOS Setup Secure Boot Keys (BIOS セットアップセキュアブートキーの保存)
 - Preserve BIOS Setup Options Configuration (BIOS セットアップオプション設定の保存)
 - Backup Existing BIOS Image (既存の BIOS イメージをバックアップ) : 既存の BIOS イメージをバックアップするには、**[Backup Existing BIOS Image (既存の BIOS イメージをバックアップ)]** チェックボックスをオンにします。整合性が失われた場合はいつでも、バックアップイメージを使用して自動リカバリを実行できます。また、**[インベントリ]** ページから BIOS を手動で回復することもできます。
- c. 以下のいずれかを選択します。
 - **Next-boot Update (次回の起動時に更新)** : BIOS ファームウェアの更新は、システムの再起動後にスケジュールされます。
注: スケジュールされた次回の起動時の更新をキャンセルする場合は、**[Task List (タスクリスト)]** ページの削除オプションを使用します。
 - **Immediate Update (即時更新)** : BIOS ファームウェアの更新がすぐに開始されます。
- d. *\$step 2: Select File (ステップ2: ファイルの選択)*] で、**[select File (ファイルの選択)]** をクリックし、ローカルに保存されたファームウェア更新ファイルを参照して、**[アップロード]** をクリックします。
注: BIOS イメージを含めずに **[アップロード]** をクリックすると、次のメッセージが表示されます: *Please select an image file。Click here to*

return (イメージ ファイルを選択してください。ここをクリックして戻ります)。

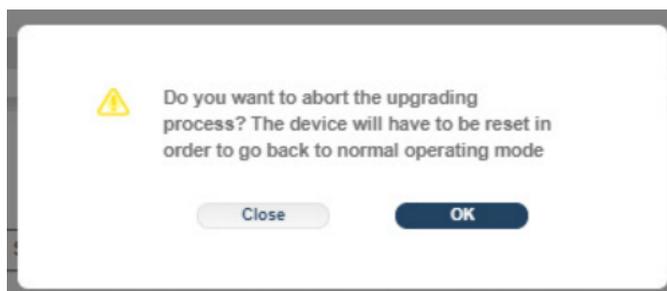


- e. [step 3: File Version (ステップ3: ファイルのバージョン)] で、既存のファームウェアバージョンと新しいファームウェアバージョンを確認し、**更新**] をクリックします。



注:

- ほとんどのファームウェア更新では、システムのプロンプトに従ってマザーボードをシャットダウンする必要があります。マザーボードをシャットダウンした後、更新を続行できます。
- ファームウェア BIOS の更新処理をキャンセルすると、アップグレードを中止するかどうかを確認するメッセージが表示されます。 **[OK]** をクリックすると BIOS がリセットされ、「BIOS is restarting (BIOS を再起動しています)」というメッセージが表示されます。データの損失を防ぐため、確認後、BIOS がオンラインに戻るまで電源を切断しないでください。



- ファームウェアの更新が完了した後、Web ブラウザの更新に時間がかかる場合があります。ログイン時に再起動メッセージが1 ～ 2 分間表示される場合があります。

BIOS のファームウェア アップグレードが正常に完了しました。

更新されたファームウェアの確認

このセクションでは、ファームウェア更新の進捗状況を確認する方法について説明します。

以下の手順に従います。

1. IPMI Web サイトにログインします。
2. **[メンテナンス]** > **[Task List (タスクリスト)]** に移動します。

[Task List (タスクリスト)] 画面に、システムで実行されているメンテナンス処理が表示されます。



3. ログを確認し、ファームウェア更新のステータスと進捗状況を確認します。

[Task List (タスクリスト)] 画面には、ファームウェア更新ジョブの以下の詳細が表示されます。

- **Health Status (健全性ステータス)**：現在のタスクの健全性ステータスが表示されます。
- **Task Name (タスク名)**：タスクの名前が表示されます。
- **状態**：現在の状態の値(実行中、完了、または失敗)が表示されます。
- **進捗状況**：現在実行中のタスクの進捗状況が表示されます。

注：管理者は、保留中の BMC および BIOS ファームウェアの更新をキャンセルできます。キャンセルするには、**[Task List (タスクリスト)]** の下の **[Abort pending Task (保留中のタスクを中止)]** オプションをクリックします。

第 11 章: Arcserve アプライアンス 9000 シリーズのファームウェアのアップグレード

このセクションには、以下のトピックが含まれます。

Arcserve アプライアンス 9000 シリーズの BIOS ファームウェアのアップグレード	226
Arcserve アプライアンス 9000 シリーズの iDRAC ファームウェアのアップグレード	232

Arcserve アプライアンス 9000 シリーズの BIOS ファームウェアのアップグレード

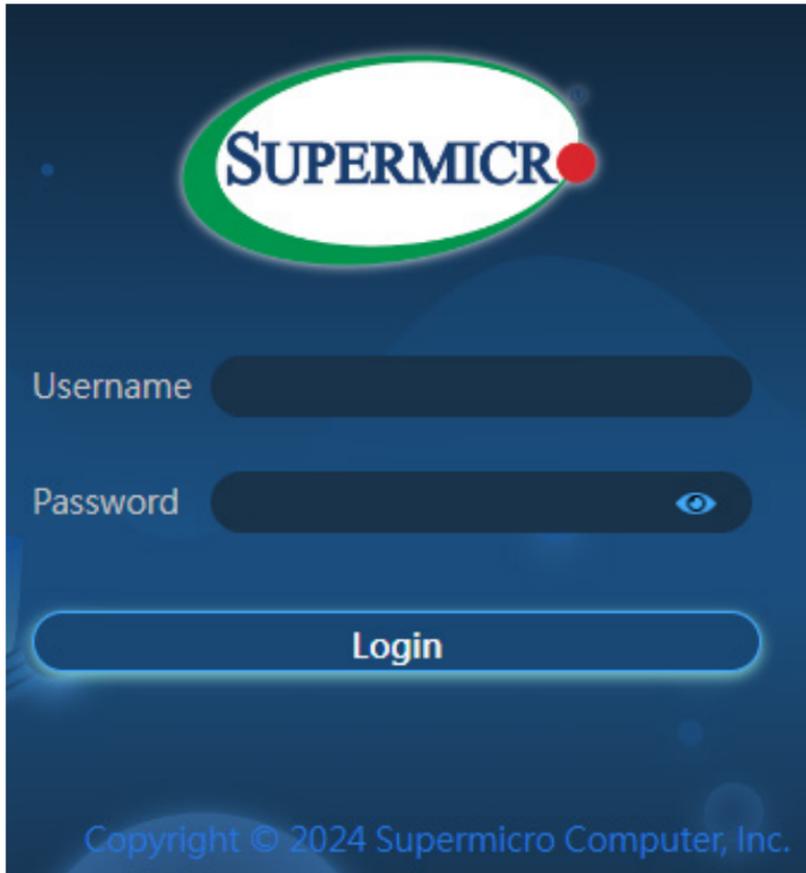
このセクションでは、以下について説明しています。

ファームウェアのバージョンの表示

このセクションでは、最新のファームウェアのバージョンを表示する方法について説明します。

以下の手順に従います。

1. Web ブラウザを開き、IPMI (インテリジェントプラットフォーム管理インターフェース) の静的 IP を入力します。
[ログイン] 画面が表示されます。
2. 以下のようにログイン認証情報を入力します。
 - ユーザ名: ADMIN。
注: ユーザ名は大文字である必要があります。
 - パスワード: BMC パスワードを入力します。
3. [ログイン] をクリックします。

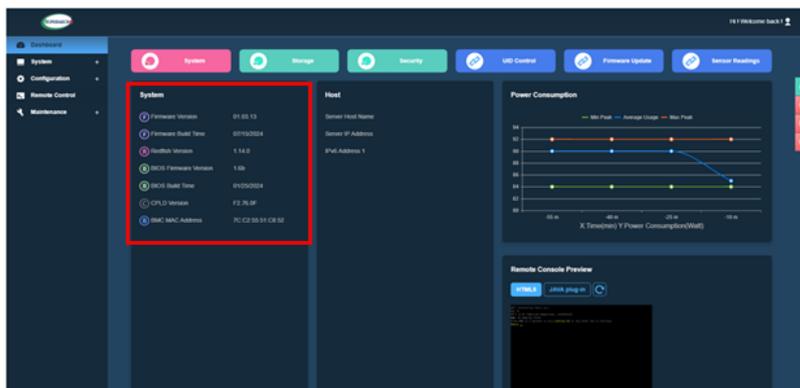


IPMI Web サーバ インターフェースが表示されます。

注：BMC/IPMI 固有のパスワードは、サーバの前面パネルにある引き出し式タグで確認できます。BMC パスワードは、BMC/IPMI MAC アドレスのすぐ下の行に記載されています。



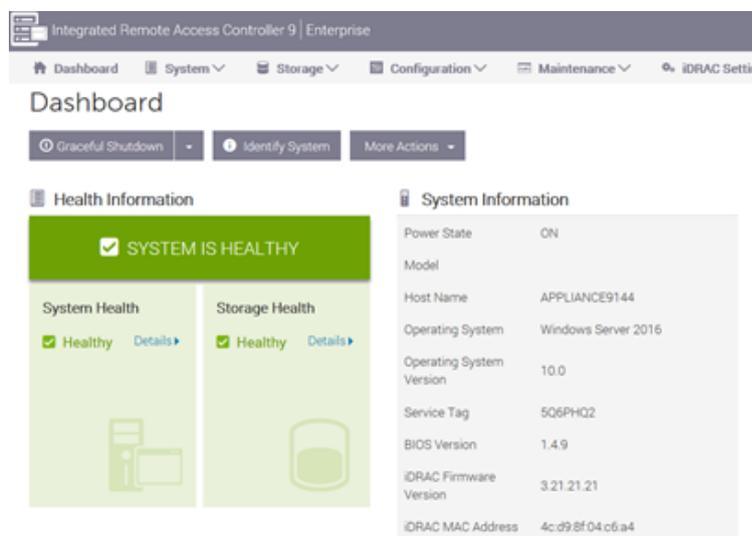
[ダッシュボード] 画面の [システム] にファームウェアのバージョンが表示されます。



方法 1: iDRAC Web インターフェースから BIOS ファームウェアのバージョンを表示する

以下の手順に従います。

1. iDRAC Web インターフェースに移動します。
2. ログインするには、以下のように入力します。
 - ユーザー名: root
 - パスワード: ARCADMIN

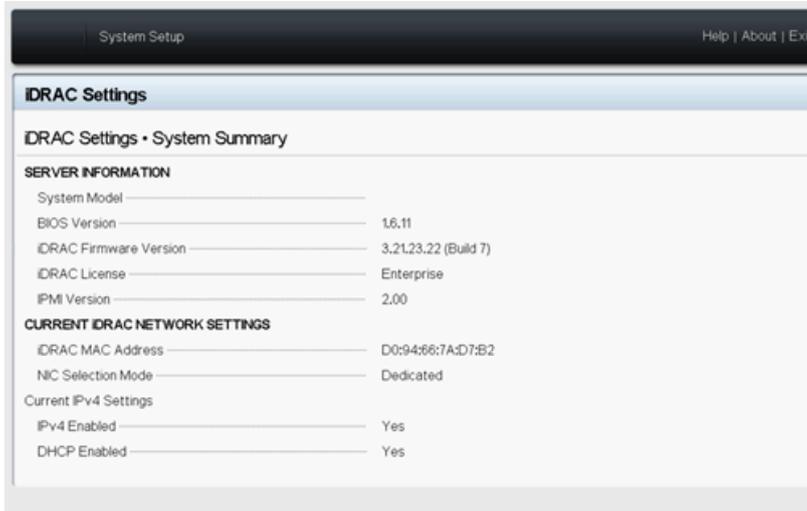


iDRAC ダッシュボード ページには、BIOS ファームウェア バージョンを含むシステム情報が表示されます。

方法 2: BIOS Arcserve Appliance 9000 シリーズから BIOS ファームウェア バージョンを表示する

以下の手順に従います。

1. システムが起動したら、**F11** キーを押してセットアップに入ります。
2. BIOS バージョンを表示するには **[System Setup] - [DRAC Settings]** または **[System BIOS]** に移動します。



このページにはファームウェアのバージョンが表示されます。



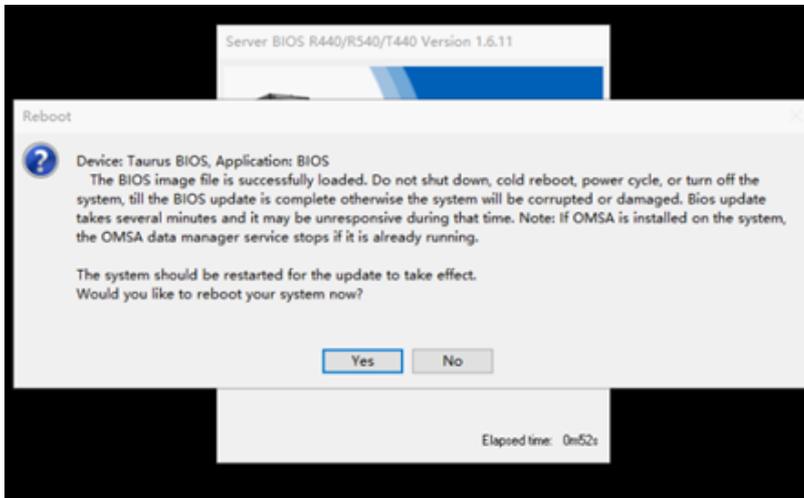
BIOS の更新されたパッケージのダウンロード

[Dell](#) の Web サイトから特定の Arcserve アプライアンス 9000 シリーズ モデルの最新の BIOS ファームウェア パッケージをダウンロードするか、Arcserve サポートにお問い合わせください。

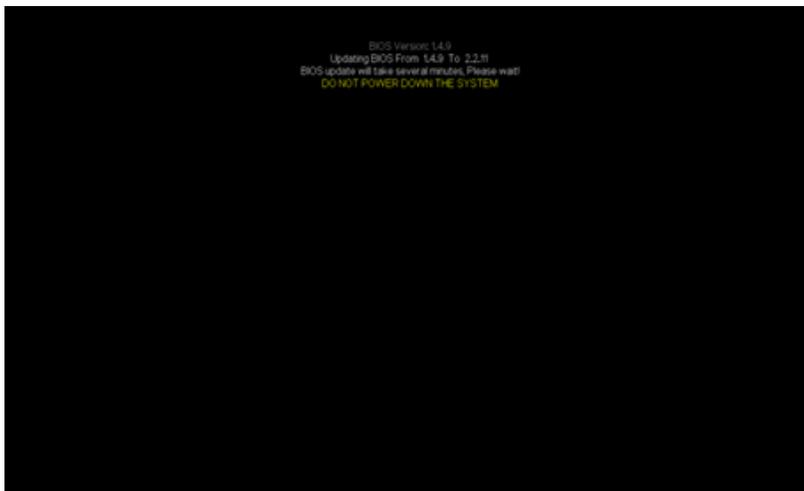
BIOS のアップグレード

以下の手順に従います。

1. アップグレード パッケージを Arcserve アプライアンス 9000 シリーズのローカル ディスクにコピーします。
2. アップグレード パッケージを起動し、画面の指示に従ってアップグレードを完了します。
3. 更新を完了するには、システムを再起動します。



注：アップグレード プロセスを開始する前に、すべてのアプリケーションが閉じられていることを確認してください。



更新されたファームウェアの確認

このセクションでは、ファームウェア更新の進捗状況を確認する方法について説明します。

以下の手順に従います。

1. IPMI Web サイトにログインします。
2. **[メンテナンス]** > **[task List (タスクリスト)]** に移動します。

Task List (タスクリスト) 画面に、システムで実行されているメンテナンス処理が表示されます。



3. ログを確認し、ファームウェア更新のステータスと進捗状況を確認します。

Task List (タスクリスト) 画面には、ファームウェア更新ジョブの以下の詳細が表示されます。

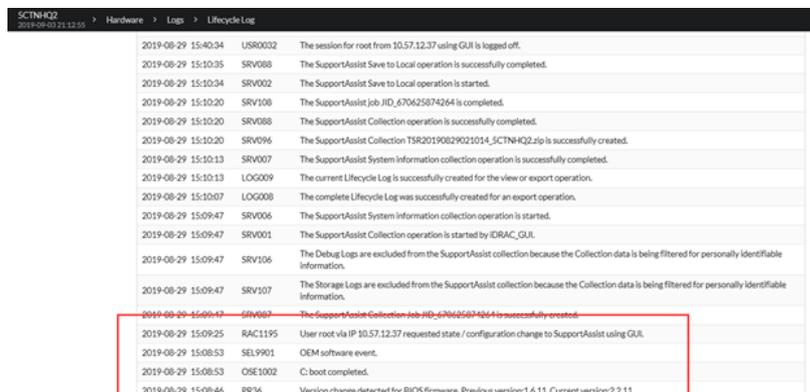
- **Health Status (健全性ステータス)**：現在のタスクの健全性ステータスが表示されます。
- **Task Name (タスク名)**：タスクの名前が表示されます。
- **状態**：現在の状態の値(実行中、完了、または失敗)が表示されます。
- **進捗状況**：現在実行中のタスクの進捗状況が表示されます。

注：管理者は、保留中の BMC および BIOS ファームウェアの更新をキャンセルできます。キャンセルするには、Task List (タスクリスト) の下の **Abort pending Task (保留中のタスクを中止)** オプションをクリックします。

システムログを使用して更新された BIOS を確認する

以下の手順に従います。

1. iDRAC にログインし、**[Maintenance]- [SupportAssist]- [start a Collection]** に移動します。
2. ログを確認し、更新プロセス中にエラーがないことを確認します。



iDRAC Web インターフェースまたは BIOS から更新された BIOS を確認する

iDRAC Web インターフェースにログインするか、システム BIOS に入って、更新された BIOS ファームウェアバージョンを確認します。

Arcserve アプライアンス 9000 シリーズの iDRAC ファームウェアのアップグレード

このセクションでは、以下について説明しています。

iDRAC ファームウェアバージョンの表示

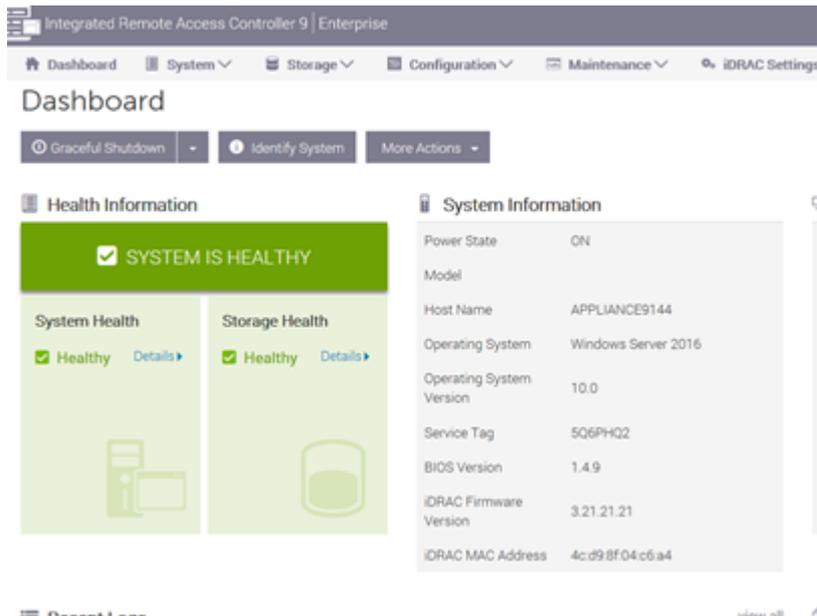
iDRAC ファームウェアバージョンを表示するには、以下の方法の方法のいずれかを使用します。

- [方法 1: iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示する](#)
- [方法 2: BIOS Arcserve Appliance 9000 シリーズから iDRAC ファームウェアのバージョンを表示する](#)

iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示する

iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示するには、iDRAC Web インターフェースにログインします。

注: デフォルトのパスワードをすぐに変更することを強くお勧めします。デフォルトのパスワードを変更する場合は、「[iDRAC パスワードを変更する方法](#)」を参照してください。

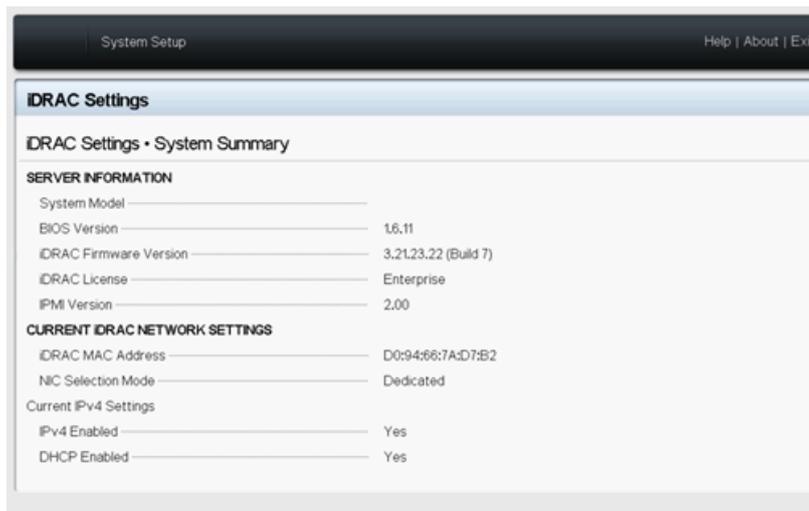


iDRAC ダッシュボードには、iDRAC ファームウェア バージョンを含むシステム情報が表示されます。

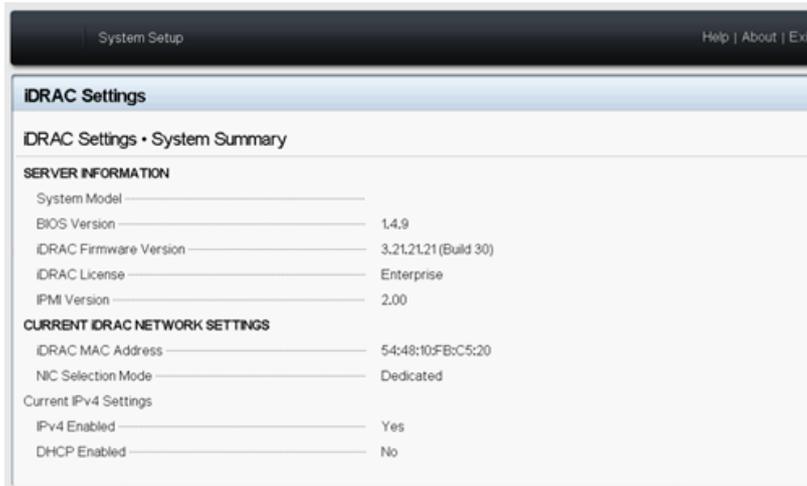
方法 2: BIOS Arcserve Appliance 9000 シリーズから iDRAC ファームウェアのバージョンを表示する

以下の手順に従います。

1. システムが起動したら、F11 キーを押してセットアップに入ります。
2. iDRAC バージョンを表示するには **\$system Setup]** - **[DRAC Settings]** または **\$system BIOS]** に移動します。



このページにはファームウェアのバージョンが表示されます。

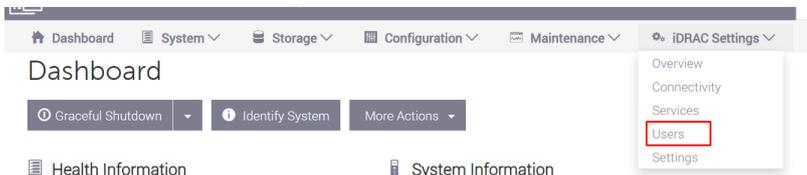


iDRAC パスワードの変更方法

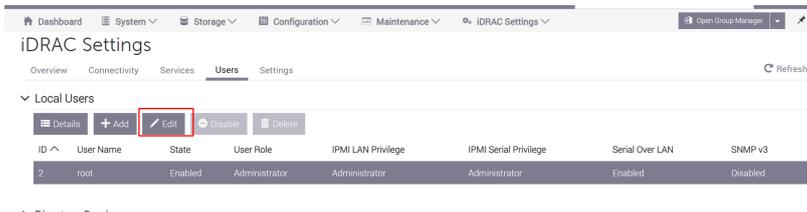
このセクションでは、iDRAC パスワードの変更方法について説明します。

以下の手順に従います。

1. 現在のパスワードで iDRAC にログインします。
2. **[DRAC の設定]** に移動し、**[ユーザ]** を選択します。



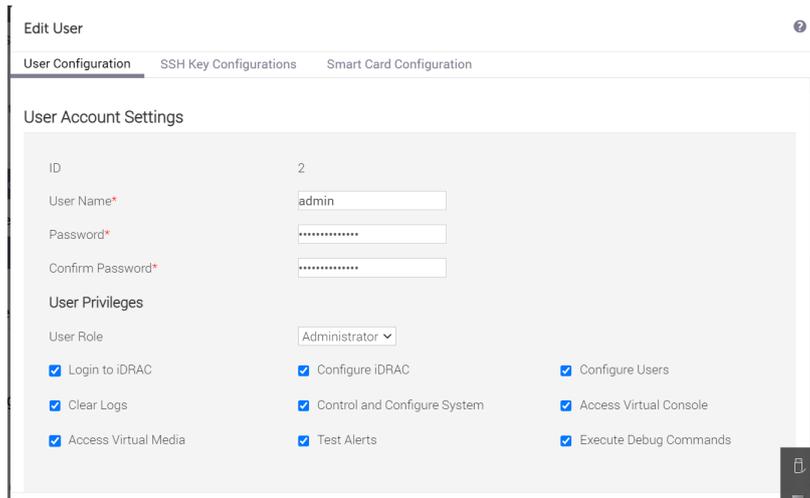
3. **[DRAC の設定]** ページで、**[local Users (ローカルユーザ)]** ドロップダウンボックスをクリックし、**[編集]** ボタンをクリックします。



[Edit User (ユーザの編集)] ダイアログボックスが表示されます。

4. **[ユーザ環境設定]** タブで、新しいパスワードを入力し、確認のためにもう一度入力して、**[保存]** をクリックします。

注: ユーザの役割は管理者のままにしておくことをお勧めします。



iDRAC パスワードが正常に変更されました。

iDRAC の更新されたパッケージのダウンロード

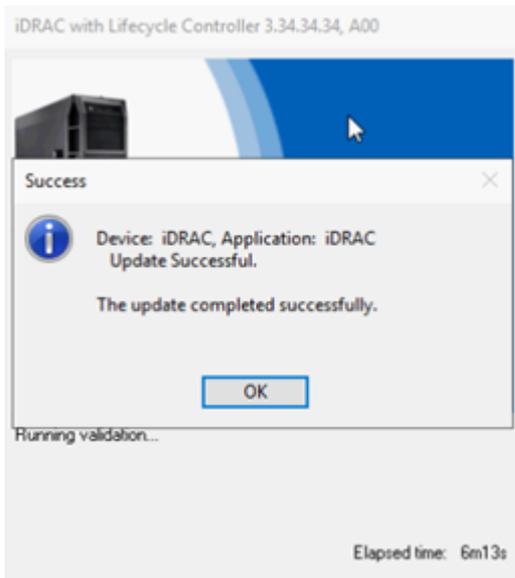
[Dell](#) の Web サイトから特定の Arcserve アプライアンス 9000 シリーズ モデルの最新の iDRAC ファームウェア パッケージをダウンロードするか、Arcserve サポートにお問い合わせください。

iDRAC のアップグレード

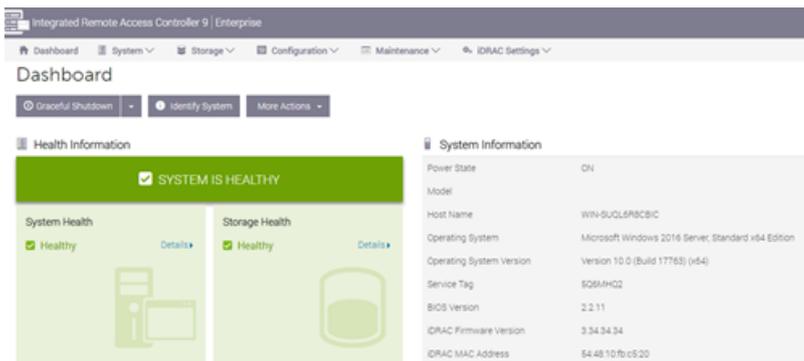
以下の手順に従います。

1. アップグレード パッケージを Arcserve アプライアンス 9000 シリーズのローカルディスクにコピーします。
2. アップグレード パッケージを起動し、画面の指示に従ってアップグレードを完了します。

注: アップグレード プロセスを開始する前に、すべてのアプリケーションが閉じられていることを確認してください。



- アップグレード プロセス中、iDRAC と仮想コンソールが数分間切断されます。iDRAC にログインし、仮想コンソールを再起動します。これでアップグレードが完了しました。



更新された iDRAC の確認

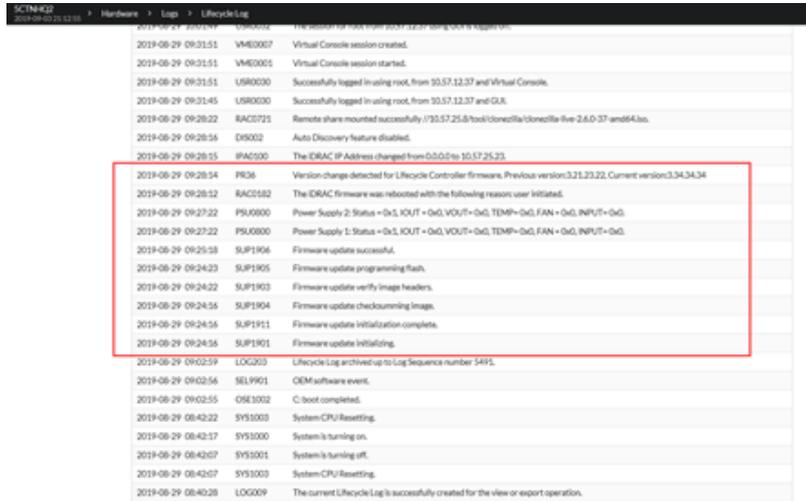
以下の方法のいずれかを使用します。

- システム ログを使用して更新された iDRAC を確認する
- iDRAC Web インターフェースまたは BIOS から更新された iDRAC を確認する

システム ログを使用して更新された iDRAC を確認する

以下の手順に従います。

1. iDRAC にログインし、[Maintenance] > [supportAssist] > [start a Collection] に移動します。
2. ログを確認し、更新プロセス中にエラーがないことを確認します。



Time	Code	Description
2019-08-29 09:31:51	VM0007	Virtual Console session created.
2019-08-29 09:31:51	VM0005	Virtual Console session started.
2019-08-29 09:31:51	USR0030	Successfully logged in using root, from 10.57.12.37 and Virtual Console.
2019-08-29 09:31:45	USR0030	Successfully logged in using root, from 10.57.12.37 and GUI.
2019-08-29 09:28:22	RAC0721	Remote share mounted successfully /10.57.25.8/total/consolla/consollefive-2.6.0-37-and64bit.
2019-08-29 09:28:16	DIS002	Auto Discovery feature disabled.
2019-08-29 09:28:05	IPAC000	The iDRAC IP Address changed from 00.0.0 to 10.57.25.23.
2019-08-29 09:28:04	FR36	Version change detected for Lifecycle Controller firmware. Previous version:3.21.23.22, Current version:3.34.34.34
2019-08-29 09:28:12	RAC0182	The iDRAC firmware was rebooted with the following reason user initiated.
2019-08-29 09:27:22	PSU0000	Power Supply 2: Status = Ok, IOUT = Ok, VOUT = Ok, TEMP = Ok, FAN = Ok, INPUT = Ok.
2019-08-29 09:27:22	PSU0000	Power Supply 1: Status = Ok, IOUT = Ok, VOUT = Ok, TEMP = Ok, FAN = Ok, INPUT = Ok.
2019-08-29 09:25:38	SLP1906	Firmware update successful.
2019-08-29 09:24:23	SLP1905	Firmware update programming flash.
2019-08-29 09:24:22	SLP1903	Firmware update verify image headers.
2019-08-29 09:24:16	SLP1904	Firmware update checksumming image.
2019-08-29 09:24:16	SLP1911	Firmware update initialization complete.
2019-08-29 09:24:16	SLP1901	Firmware update initializing.
2019-08-29 09:02:39	LOG003	Lifecycle Log archived up to Log Sequence number 5491.
2019-08-29 09:02:16	SEL9901	ODM software event.
2019-08-29 09:02:05	OS1002	C: boot completed.
2019-08-29 08:42:22	SYS1003	System CPU Resetting.
2019-08-29 08:42:17	SYS1000	System is turning on.
2019-08-29 08:42:07	SYS1001	System is turning off.
2019-08-29 08:42:07	SYS1003	System CPU Resetting.
2019-08-29 08:40:28	LOG009	The current Lifecycle Log is successfully created for the view or export operation.

iDRAC Web インターフェイスまたは iDRAC から更新された BIOS を確認する

iDRAC Web インターフェイスにログインするか、システム BIOS に入って、更新された BIOS ファームウェア バージョンを確認します。

Arcserve アプライアンス X シリーズのファームウェアのアップグレード

このセクションでは、以下について説明しています。

Arcserve アプライアンス X シリーズの BIOS ファームウェアのアップグレード

このセクションでは、以下について説明しています。

BIOS ファームウェア バージョンの表示

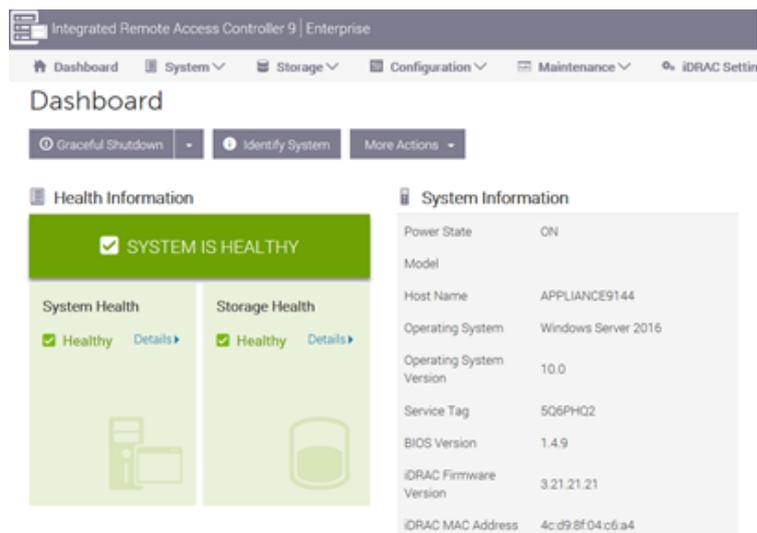
BIOS ファームウェア バージョンを表示するには、以下の方法の方法のいずれかを使用します。

- [方法 1: iDRAC Web インターフェースから BIOS ファームウェアのバージョンを表示する](#)
- [方法 2: BIOS Arcserve アプライアンス X シリーズから BIOS ファームウェア バージョンを表示する](#)

方法 1: iDRAC Web インターフェースから BIOS ファームウェアのバージョンを表示する

以下の手順に従います。

1. iDRAC Web インターフェースに移動します。
2. ログインするには、以下のように入力します。
 - ユーザー名: root
 - パスワード: ARCADMIN

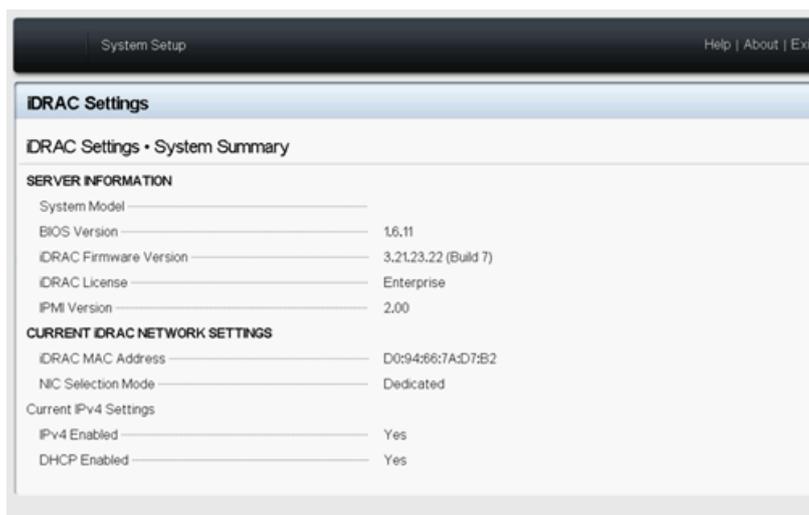


iDRAC ダッシュボード ページには、BIOS ファームウェア バージョンを含むシステム情報が表示されます。

方法 2: BIOS Arcserve アプライアンス X シリーズから BIOS ファームウェア バージョンを表示する

以下の手順に従います。

1. システムが起動したら、F11 キーを押してセットアップに入ります。
2. BIOS バージョンを表示するには **System Setup** - **DRAC Settings** または **System BIOS** に移動します。



このページにはファームウェアのバージョンが表示されます。



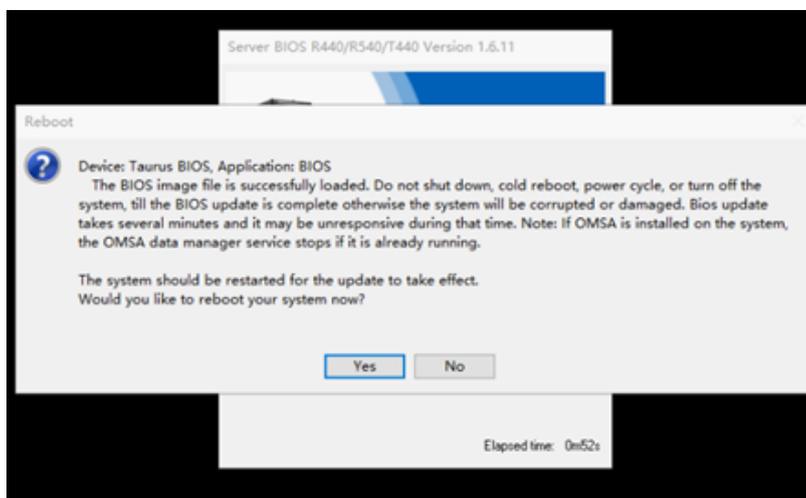
BIOS の更新されたパッケージのダウンロード

[Dell](#) の Web サイトから特定の Arcserve アプライアンス X シリーズ モデルの最新の BIOS ファームウェア パッケージをダウンロードするか、Arcserve サポートにお問い合わせください。

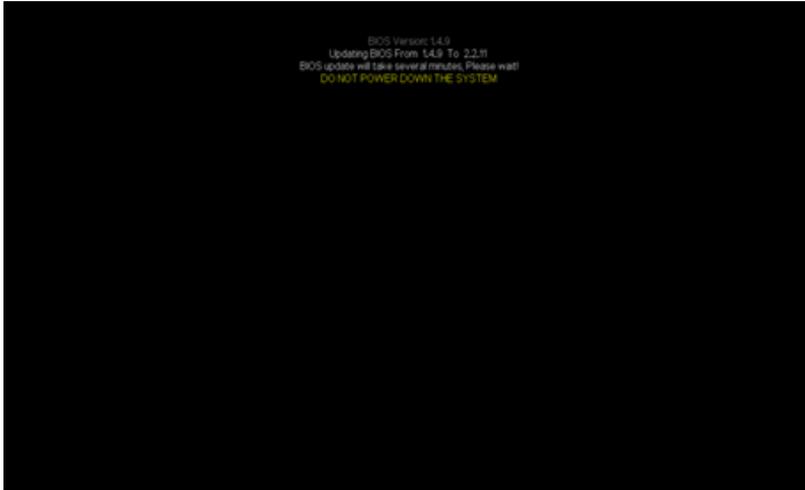
BIOS のアップグレード

以下の手順に従います。

1. アップグレード パッケージを Arcserve アプライアンス X シリーズのローカル ディスクにコピーします。
2. アップグレード パッケージを起動し、画面の指示に従ってアップグレードを完了します。
3. 更新を完了するには、システムを再起動します。



注: アップグレード プロセスを開始する前に、すべてのアプリケーションが閉じられていることを確認してください。



更新された BIOS の確認

以下の方法のいずれかを使用します。

- [システム ログを使用して更新された BIOS を確認する](#)
- [iDRAC Web インターフェースまたは BIOS から更新された BIOS を確認する](#)

Arcserve アプライアンス X シリーズの iDRAC ファームウェアのアップグレード

このセクションでは、以下について説明しています。

iDRAC ファームウェア バージョンの表示

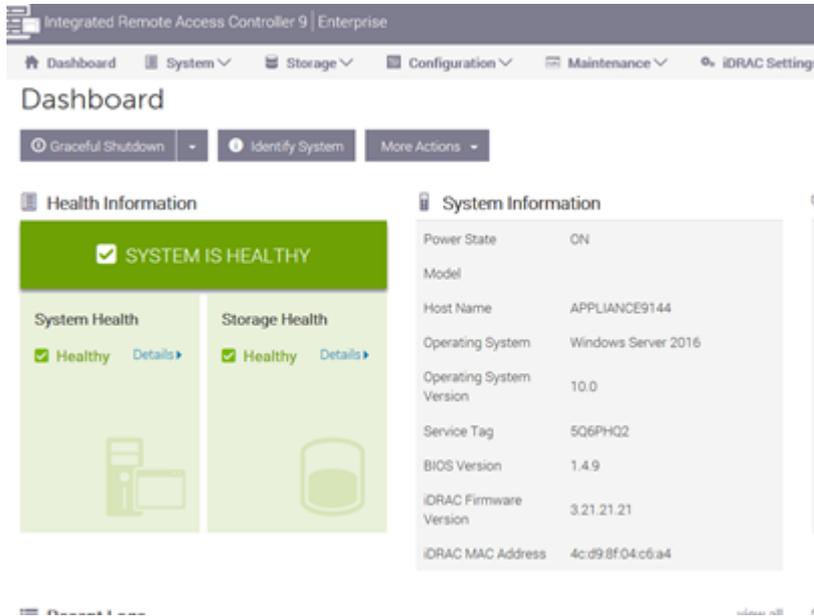
iDRAC ファームウェア バージョンを表示するには、以下の方法の方法のいずれかを使用します。

- [方法 1: iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示する](#)
- [方法 2: BIOS Arcserve アプライアンス X シリーズから iDRAC ファームウェアバージョンを表示する](#)

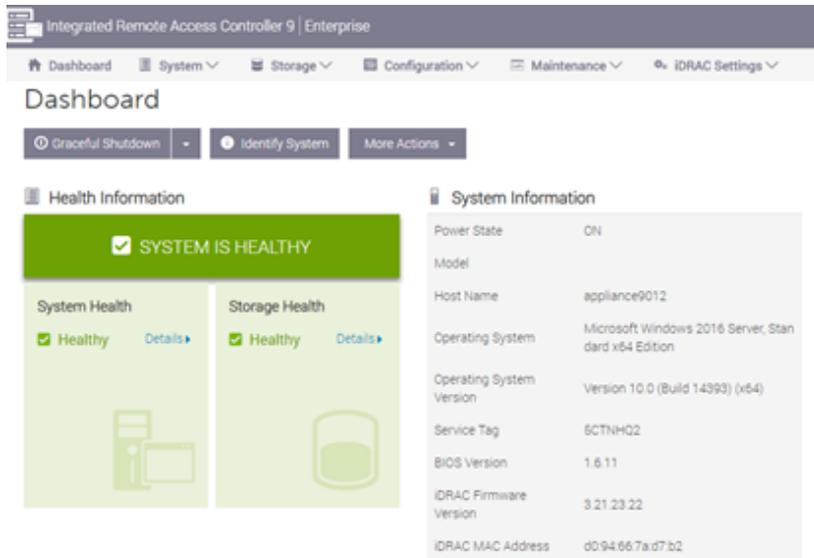
方法 1: iDRAC Web インターフェースから iDRAC ファームウェアのバージョンを表示する

以下の手順に従います。

1. iDRAC Web インターフェースに移動します。
2. ログインするには、以下のように入力します。
 - ユーザ名：root
 - パスワード：ARCAADMIN



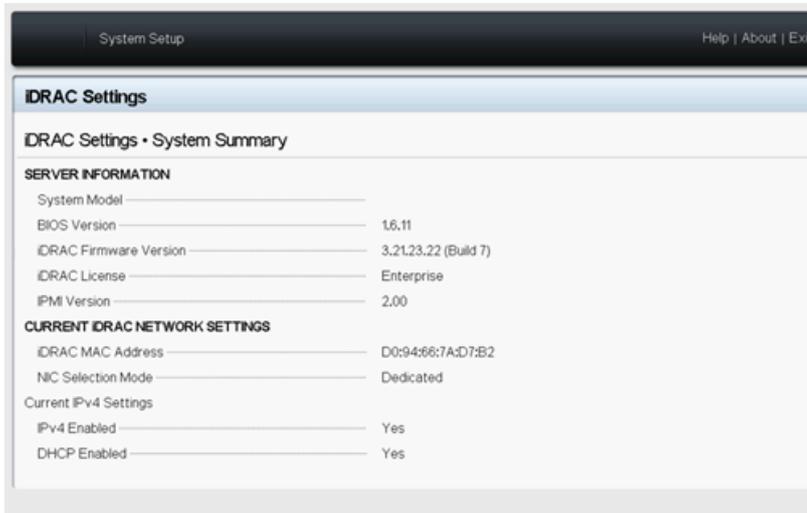
iDRAC ダッシュボードには、iDRAC ファームウェア バージョンを含むシステム情報が表示されます。



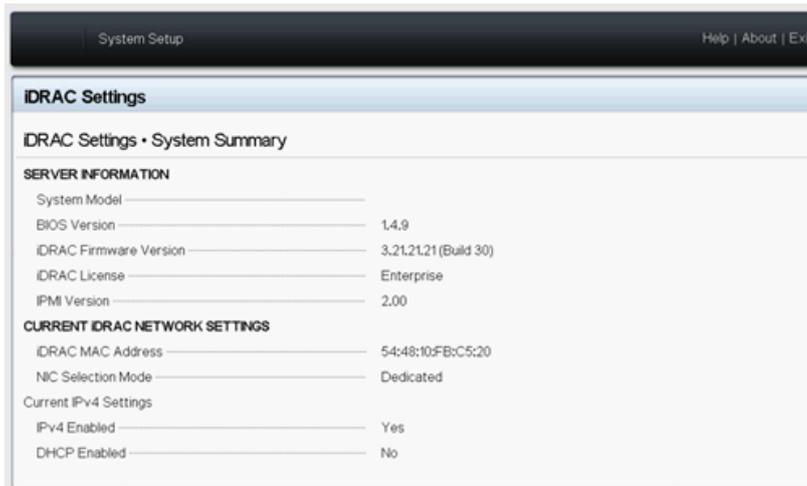
方法 2: BIOS Arcserve アプライアンス X シリーズから iDRAC ファームウェア バージョンを表示する

以下の手順に従います。

1. システムが起動したら、F11 キーを押してセットアップに入ります。
2. iDRAC バージョンを表示するには **System Setup] - [DRAC Settings]** または **System BIOS]** に移動します。



このページにはファームウェアのバージョンが表示されます。



iDRAC の更新されたパッケージのダウンロード

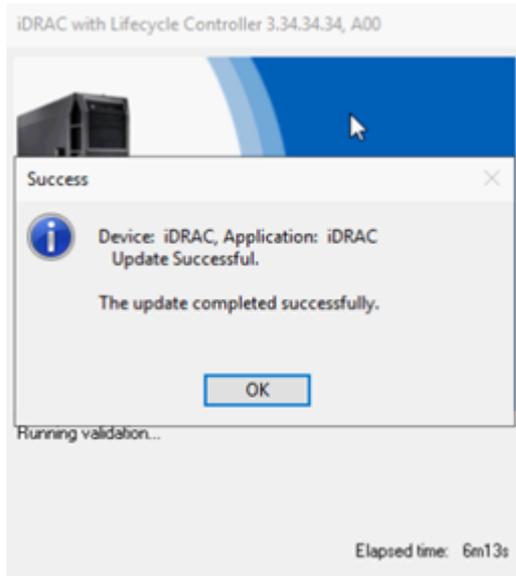
[Dell](#) の Web サイトから特定の Arcserve アプライアンス X シリーズ モデルの最新の iDRAC ファームウェア パッケージをダウンロードするか、Arcserve サポートにお問い合わせください。

iDRAC のアップグレード

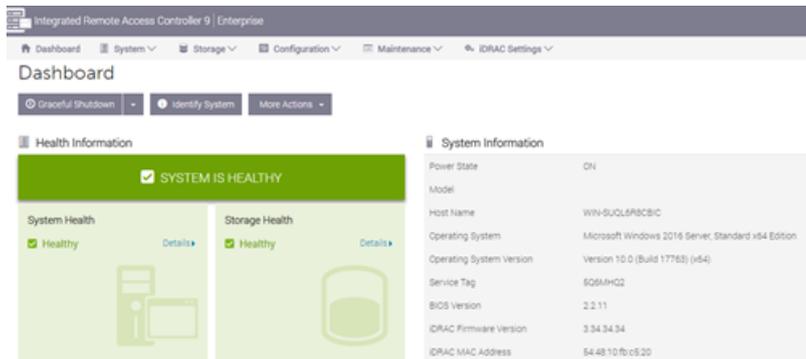
以下の手順に従います。

1. アップグレード パッケージを Arcserve アプライアンス X シリーズのローカル ディスクにコピーします。
2. アップグレード パッケージを起動し、画面の指示に従ってアップグレードを完了します。

注: アップグレード プロセスを開始する前に、すべてのアプリケーションが閉じられていることを確認してください。



3. アップグレード プロセス中、iDRAC と仮想コンソールが数分間切断されます。iDRAC にログインし、仮想コンソールを再起動します。これでアップグレードが完了しました。



更新された iDRAC の確認

以下の方法のいずれかを使用します。

- [システム ログを使用して更新された iDRAC を確認する](#)
- [iDRAC Web インターフェースまたは BIOS から更新された iDRAC を確認する](#)

第12章:トラブルシューティング

このセクションには、以下のトピックが含まれます。

Linux バックアップ サーバにコンソールから接続できない	246
別のアプライアンスから Arcserve アプライアンス のバックアップを実行すると重複ノードがレポートされる	247
Linux バックアップ サーバがネットワーク内のノードと通信できない	248
Linux バックアップ サーバがネットワーク DNS サフィックスを取得できない	250
アプライアンスのデフォルトのタイムゾーン	251
ライセンスが利用可能な場合でもライセンスエラーが発生する	252

Linux バックアップ サーバにコンソールから接続できない

現象

Arcserve UDP コンソールから Linux バックアップ サーバに接続しようとする、接続に失敗して赤色のマークが表示されます。

解決策

Linux バックアップ サーバにコンソールから接続できない場合、接続のトラブルシューティングを行って問題を特定することができます。

接続の問題のトラブルシューティングを行う方法

1. Hyper-V マネージャを起動し、Linux バックアップ サーバの仮想マシンに接続してログインします。
2. 以下のコマンドを実行します。

```
service network restart
```

3. Linux バックアップ サーバに割り当てられている IP アドレスが 192.168.10.2 であることを確認します。確認するには、次のコマンドを実行します。

```
ifconfig
```

4. IP アドレスが 192.168.10.2 である場合は、Arcserve UDP コンソールに移動し、接続しようとしている Linux バックアップ サーバノードを更新します。
5. IP アドレスが 192.168.10.2 でない場合は、「DHCP Microsoft 管理コンソール (MMC) からのトラブルシューティング」の手順に従います。

DHCP Microsoft 管理コンソール (MMC) からのトラブルシューティング

重要: DHCP サーバサービスが、アプライアンス上で適切に実行されていることを確認します。

1. [サーバ マネージャ] - [ツール] - [DHCP] から DHCP MMC を起動します。
2. Linux サーバノード、IPv4、スコープを展開し、192.168.10.0 という名前のスコープがその下に存在することを確認します。
3. [アドレスのリース] を展開し、他のリースレコードの存在を削除します。
4. Linux バックアップ サーバにログインし、以下のコマンドを実行します。

```
service network restart
```

5. Arcserve UDP コンソールに移動し、接続しようとしている Linux バックアップ サーバノードを更新します。

Linux バックアップ サーバにコンソールから接続できるようになりました。

別のアプライアンスから Arcserve アプライアンス のバックアップを実行すると重複ノードがレポートされる

現象

アプライアンス A からアプライアンス B をバックアップすると、アクティビティ ログに以下の警告メッセージが表示されます。

"The following nodes are duplicated: Appliance_B, Appliance_A. As a result, they have the same agent identifier and may cause unexpected results. This duplicate node problem can be caused if the node was added using a different node name (such as the DNS name or IP address), or if some machines were set up by cloning from one to another." (次のノードが重複しています: Appliance_B、Appliance_A。その結果、これらのノードに同じエージェント識別子が指定され、予期しない結果が生じる可能性があります。異なるノード名 (DNS 名 や IP アドレスなど) を使用してノードが追加された場合や、別のマシンのクローンを作成してマシンがセットアップされた場合に、この重複ノードの問題が発生する可能性があります。)

ケース 1: アプライアンス B が RPS としてアプライアンス A の UDP コンソールに追加されます。

例: アプライアンス B から、UDP ウィザードを使用してアプライアンスを設定し、 [のアプライアンスは、別の Arcserve UDP コンソールによって管理される Arcserve UDP 復旧ポイント サーバのインスタンスとして機能します] を選択できます。

解決策

1. UDP コンソールの [RPS] ペインからアプライアンス B のノード内のデータストアを停止します。
2. アプライアンス B にログインし、[HKEY_LOCAL_MACHINE\SOFTWARE\CA\ARCserve Unified Data Protection\Engine] の下にあるノード ID のレジストリキーを削除します。
3. アプライアンス B のノードから Arcserve UDP エージェント Web サービスを再起動します。
4. アプライアンス B のノードから Arcserve UDP RPS データストア サービスを再起動します。
5. UDP コンソールから、 [ノード]- [すべてのノード] ペインに移動して、アプライアンス B のノードを更新します。
6. [復旧ポイント サーバ] ペインに移動して、アプライアンス B のノードを更新します。
7. アプライアンス B の RPS に元のバックアップ先を設定して、既存のデータストアをインポートします。

ケース 2: アプライアンス B がエージェント ノードとしてのみ、アプライアンス A の UDP コンソールに追加されます。

たとえば、あるプランでは、アプライアンス A の UDP コンソール上にあるエージェントベースのバックアップタスクを使用してアプライアンス B を保護します。

1. アプライアンス B にログインし、[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve Unified Data Protection\Engine] の下にあるノード ID のレジストリキーを削除します。
2. アプライアンス B から Arcserve UDP エージェント サービスを再起動します。
3. UDP コンソールから、[ノード]- [すべてのノード] ペインに移動して、アプライアンス B からのノードを更新します。

Linux バックアップ サーバがネットワーク内のノードと通信できない

現象

Linux バックアップ サーバが、ネットワーク内のどのノードとも通信できません。

解決策

アプライアンスの Windows Server がネットワーク内のどのノードとも通信できない場合、Linux バックアップ サーバもどのノードとも通信できません。

以下の手順に従います。

1. アプライアンスの Windows Server からノードにアクセスできるかを確認します。
2. 以下の場所へ移動して、ネットワークアダプタ LinuxBkpSvr が存在しているかを確認します。

[コントロール パネル]- [ネットワークとインターネット]- [ネットワーク接続]

3. LinuxBkpSvr が存在しない場合、以下の場所へ移動し、フラグファイル adapterNameChanged.flag が存在するかを確認します。

```
C:\Program Files\Arcserve\Unified Data  
Protection\Engine\BIN\Appliance
```

存在する場合は、adapterNameChanged.flag ファイルを削除します。

4. 以下に示すように、すべての利用可能なネットワークインタフェースと LinuxBkpSvr が、NAT に追加されていることを確認します。

すべてのネットワークインタフェースと LinuxBkpSvr がすでに一覧内にある場合は、別の物理ネットワークインターフェースが異なるサブネットワークに接続されているかどうかを確認します。このアクションにより、Linux バックアップ サーバの通信問題が解決します。

すべてのネットワーク インターフェースおよび *LinuxBkpSvr* が一覧に表示されたら、後続の手順に進みます。

5. 以下の場所で、ファイル *dhcpcd.flag* を削除します。

```
C:\Program Files\Arcserve\Unified Data  
Protection\Engine\BIN\Appliance
```

6. 以下に示すように、コマンドラインにフォルダ *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Appliance* を入力し、*resetdhcp.ps1* を実行します。

```
C:\Program Files\Arcserve\Unified Data  
Protection\Engine\BIN\Appliance>powershell .\resetdhcp.ps1
```

スクリプトが正常に実行されると、Linux バックアップ サーバの通信問題が解決されます。

Linux バックアップ サーバがネットワーク DNS サフィックス を取得できない

アプライアンス サーバに静的 IP アドレスを設定した場合、ネットワーク サービスを再起動した後に Linux バックアップ サーバがネットワーク DNS サフィックスを正しく取得できません。この問題によって、Linux バックアップ サーバと UDP コンソールの間の通信に問題が発生します。通信の問題により、この Linux バックアップ サーバを使用して Linux ノードを保護することができなくなります。

現象

Linux バックアップ サーバのステータスが、UDP コンソール上で切断状態のままになります。[ノードの更新]を実行しても Linux バックアップ サーバは正常に更新されず、黄色の警告アイコンは緑色に変化しません。この問題は、アプライアンス サーバに静的 IP アドレスを設定した場合に、Linux バックアップ サーバがネットワーク DNS サフィックスを正しく取得できないために発生します。

解決策

この問題を解決するには、Linux マシンの file/etc/resolv.conf を直接更新して正しい DNS サフィックスを追加します。

アプライアンスのデフォルトのタイムゾーン

現象

デフォルトのタイムゾーンは、最初にアプライアンスの電源をオンにしたときに選択した地域に関係なく、(UTC+05:30) チェンナイ、コルカタ、ムンバイ、ニューデリーになります。

解決策

タイムゾーンを変更するには、**Arcserve Backup アプライアンス ウィザード**]に移動し、**編集**]をクリックして、**日付と時刻**]を設定します。

ライセンスが利用可能な場合でもライセンスエラーが発生する

ライセンスがある場合でもアプライアンスで発生するライセンス関連のエラーの詳細については、[リンク](#)を参照してください。

第13章: ベスト プラクティスの適用

このセクションには以下のトピックが含まれます。

ネットワーク構成に関する推奨事項	254
PowerShell コマンドレットによる Windows Defender のベストプラクティス	257
プリインストールされた Linux バックアップ サーバを外部ネットワークに設定する	257
ボリュームをまたぐデデュプリケーション データストアを作成するためのベスト プラクティス	258

ネットワーク構成に関する推奨事項

- 複数のネットワーク インターフェースを実稼働環境で接続する場合は、各ネットワークアダプタが異なるサブ ネットワークに接続されていることを確認します。
- 保護する実稼働環境で Linux ノードが利用できない場合は、アプライアンス上の VM Linux-BackupSvr および DHCP サーバサービスを停止することをお勧めします。

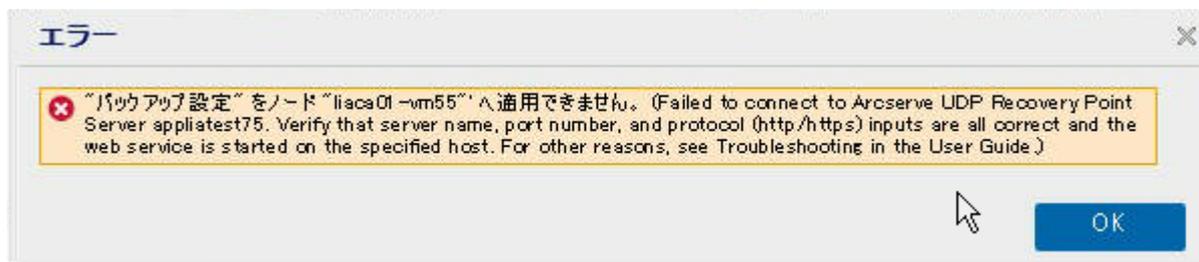
詳細については、「[DHCP サーバを無効にする方法](#)」を参照してください。

- アプライアンスとエージェント ノードが共に同一サブ ネットワーク上でオンラインの状態にあり、複数のネットワーク インターフェースがアプライアンス内の同一サブ ネットワークに接続されている場合、アプライアンスとエージェント ノード間で接続の問題が発生します。

現象

アプライアンスとエージェント ノードが共に同一サブ ネットワーク上でオンラインの状態にある場合、以下の事象が発生することがあります。

- ◆ Arcserve UDP コンソールで、エージェント ノードにプランを展開すると、以下のエラーメッセージが表示されます。



- ◆ 以下のようにエージェント ノードのバックアップジョブが失敗します。

12/25/...	Local Site	10.57.52.13	10.57.52.13	26	Backup	Failed to run backup job. Failed to connect to Arcserve UDP Recovery Point Server appliatest76. Verify that server name, port number, and protocol (http/https) inputs are all correct and the web service is started on the specified host. For other reasons, see Troubleshooting in the User Guide.
-----------	------------	-------------	-------------	----	--------	--

- ◆ アプライアンスからエージェント ノードに ping を送信し、次のようにエージェント ノードが接続されているかどうかを確認します。

```
C:\Users\Administrator> ping 10.57.52.13

10.57.52.13 に ping を送信しています 32 バイトのデータ:
10.57.52.13 からの応答: バイト数 =32 時間 <1ms TTL=128
```

- ◆ エージェント ノードから ping アプライアンス ホスト 名を実施し、アプライアンスは以下のように接続されていません。

```
C:\Users\Administrator>ping appliatest76

appliatest76 [10.57.52.47]に ping を送信しています 32 バイトのデータ:
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。
要求がタイムアウトしました。

10.57.52.47 の ping 統計:
    パケット数: 送信 = 4、受信 = 0、損失 = 4 (100% の損失)、
```

解決策

アプライアンスとエージェント ノードの間の接続の問題を解決するには、以下の手順のいずれかを実行します。

- ◆ 実稼働環境で Linux ノードが利用できない場合、アプライアンス上の DHCP サーバサービスを停止し、問題が解決されるかどうかを確認します。
詳細については、「[DHCP サーバを無効にする方法](#)」を参照してください。
- ◆ アプライアンスおよびエージェント ノードで、以下の手順を実行します。

アプライアンスで実行する手順

1. DOS コマンド プロンプトから `ipconfig/all` を実行し、アプライアンス上で利用可能な IPv4 アドレスを取得します。
2. DOS コマンド プロンプトから `Route Print` を実行し、IPv4 ルートテーブルを取得し、以下のように、アプライアンス上で利用可

能なすべての IPv4 アドレスの順番のリストを記録します。

```
IPv4 ルート テーブル
=====
アクティブ ルート:
ネットワーク宛先      ネットマスク      ゲートウェイ      インターフェイ
ス メトリック
-----
0.0.0.0                0.0.0.0            10.57.52.1        10.57.52.46      10
0.0.0.0                0.0.0.0            10.57.52.1        10.57.52.35     10
0.0.0.0                0.0.0.0            10.57.52.1        10.57.52.45     10
0.0.0.0                0.0.0.0            10.57.52.1        10.57.52.47     10
10.57.52.0            255.255.255.0     リンク上          10.57.52.46     266
10.57.52.0            255.255.255.0     リンク上          10.57.52.35     266
10.57.52.0            255.255.255.0     リンク上          10.57.52.45     266
```

エージェント ノードで実行する手順

1. DOS コマンド プロンプトから、次のように、エージェント ノードに接続しているアプライアンスの最初の IPv4 を取得するため、上記の順序に従って、アプライアンスの利用可能な各 IPv4 アドレスに ping を送信してみます。

```
C:¥Users¥Administrator>ping 10.57.52.46

10.57.52.46 に ping を送信しています 32 バイトのデータ:
10.57.52.46 からの応答: バイト数 =32 時間 <1ms TTL=128
```

2. ファイル C:\Windows\System32\drivers\etc\hosts を編集し、上記で取得した IPv4 アプライアンス ホスト名 ペアのレコードを追加して、ファイルを保存します。

PowerShell コマンドレットによる Windows Defender のベストプラクティス

Defender コマンドレットは、以下のコマンドを使用して取得することができます。

- `PS C:\> (Get-MpPreference).ExclusionPath`
Defender の除外パスを取得します。
- `PS C:\> (Get-MpPreference).ExclusionProcess`
Defender の除外プロセスを取得します。
- `PS C:\> Add-MpPreference -ExclusionPath "full_path_of_the_folder_or_file"`
除外リストにフォルダまたはファイルを除外します。
- `PS C:\> Add-MpPreference -ExclusionProcess "full_path_of_executable_programs"`
プロセスによって開かれているファイルを除外します。
- `PS C:\> Remove-MpPreference -ExclusionPath "full_path_of_the_folder"`
除外リストからフォルダを削除します。

プリインストールされた Linux バックアップ サーバを外部ネットワークに設定する

以下の手順に従います。

1. DHCP サーバを無効化します。詳細については、「[DHCP サーバを無効にする方法](#)」を参照してください。
2. Linux バックアップ サーバネットワークを外部ネットワークに設定するには、以下の手順に従います。
 - a. **Hyper-V** マネージャを開きます。
 - b. 新しい外部仮想ネットワークスイッチを作成します。
 - c. 新しく作成した外部仮想ネットワークスイッチを使用するように Linux バックアップ サーバ VM ネットワークアダプタの設定を変更します。
 - d. Linux バックアップ サーバのネットワーク設定を確認し、外部仮想ネットワークスイッチを介して IP アドレスと DNS が取得されていることを確認します。
 - e. 元の Linux バックアップ サーバを UDP コンソールから削除します。

- f. 以下の情報を使用して、Linux バックアップ サーバを UDP コンソールに再度追加します。

- ホスト名 : Linux-BackupSvr
- ポート : 8014

ボリュームをまたぐデデュプリケーション データストアを作成するためのベスト プラクティス

コマンド ライン ツールである `as_gddmgr.exe` を使用すると、ボリュームをまたぐデータパスをさらに追加して、既存のデデュプリケーション データストアのストレージ容量を拡張できます。

ボリュームをまたぐデデュプリケーション データストアを作成するには、以下の手順を実行します。

1. Arcserve UDP コンソール ユーザ インターフェイスにログインし、拡張データパスなしでデデュプリケーション データストアを作成します。詳細については、「[データストアの追加](#)」を参照してください。
2. データストアを停止します。詳細については、「[データストアの停止](#)」を参照してください。
3. コマンド プロンプトを開き、以下のコマンドを入力して、データストアの現在のパス構成を表示します。

```
as_gddmgr.exe -DataPath Display <データストア名>
```

以下のサンプル データストアには、X:\volume 上のプライマリデータパスが1つ含まれています。

```
C:\Users\Administrator> "C:\Program Files\Arcserve\Unified Data Protection\Engine\bin\as_gddmgr.exe" -DataPath Display appliancetest_data_store
Successfully load data store configuration information.

```

	Volume capacity	Used space	Free space
Primary data path :	X:\Arcserve\data_store\data	2 GB	59683 GB

4. デデュプリケーション データストアのストレージ容量を拡張するには、以下のコマンドを入力します。

```
as_gddmgr.exe -DataPath Add <データストア名> -NewDataPath <新規データフォルダ>
```

注: プライマリパスとすべての拡張パスが同じボリューム上にないことを確認してください。

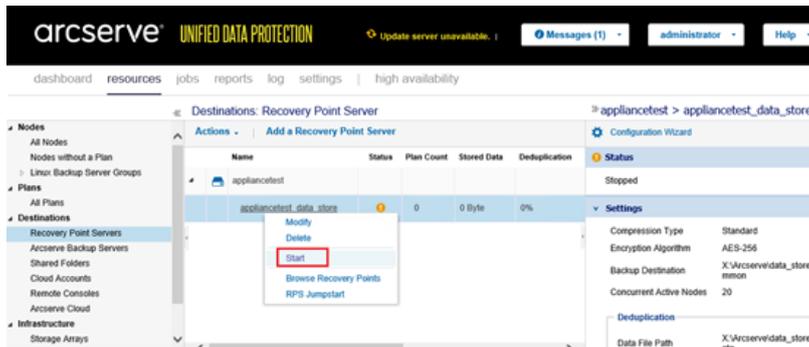
以下のサンプル データストアには、X:\volume 上の拡張データパスが1つ含まれています。

```

C:\Users\Administrator> "C:\Program Files\Arcserve\Unified Data Protection\engine\bin\as_gdopr.exe" -datapath Add appliancest_data_store -nobatspath W:\Arcserve\data_store\data1
Successfully load data store configuration information.
Successfully add new expanded data path for the data store.
The data store has 1 expanded data path(s) now.

Volume capacity    Used space    Free space
-----
Primary data path : X:\Arcserve\data_store\data1    59685 GB    2 GB
Expanded data paths: W:\Arcserve\data_store\data1    34678 GB    99 GB
Total              74363 GB    101 GB
    
```

5. 必要に応じて手順 4 を繰り返します。
6. Arcserve UDP コンソール ユーザ インターフェイスに戻り、データストアを起動します。詳細については、「[データストアの起動](#)」を参照してください。



注: 同様のディスクパーティションを持つ UDP アプライアンス上のバックアップ データストアをインポートすることをお勧めします。

第14章: 使用条件

この製品の一部には、サードパーティのソフトウェアプロバイダによって開発されたソフトウェアが含まれています。以下のセクションに、このサードパーティソフトウェアに関する情報を示します。

このセクションには、以下のトピックが含まれます。

[PuTTY](#)

PuTTY

この製品に含まれている「PuTTY」コンポーネントの詳細を以下に示します。

コンポーネント名	PuTTY
コンポーネントベンダ	Simon Tatham によって最初に開発されました。
コンポーネントバージョン	0.64
リーガルコメント	http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html
プロジェクト名	Appliance Rhodium
コンポーネントタイプ	オープンソース
ソースコードURL	http://the.earth.li/~sgtatham/putty/0.64/
必要なプラットフォーム	Windows 2012 R2、Windows 2016、Windows 2019
コンポーネントURL	http://the.earth.li/~sgtatham/putty/0.64/x86/
コンポーネントバージョンURL	http://the.earth.li/~sgtatham/putty/0.64/x86/

説明	<p>アプライアンスマシン上で、putty.exeを使用してLinuxバックアップサーバと通信し、システムロケールとUDP Linux ロケールを変更します。</p>
機能	<p>アプライアンス</p>
ライセンステキスト	<p>http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html</p> <p>PuTTYの著作権はSimon Tathamが有しています(1997-2019)。</p> <p>部分著作権 Robert de Bath、Joris van Rantwijk、Delian Delchev、Andreas Schultz、Jeroen Massar、Wez Furlong、Nicolas Barry、Justin Bradford、Ben Harris、Malcolm Smith、Ahmad Khalifa、Markus Kuhn、Colin Watson、Christopher Staite、Lorenz Diener、Christian Brabandt、Jeff Smith、Pavel Kryukov、Maxim Kuznetsov、Svyatoslav Kuzmich、Nico Williams、Viktor Dukhovni、およびCORE SDI S.A。</p> <p>このソフトウェアおよび関連する文書ファイル(以下「ソフトウェア」)を入手したすべての人は、このソフトウェアを制限なしに使用することが無償で許諾されています。これには、ソフトウェアの使用、複製、変更、結合、発行、配布、サブライセンスおよび販売についての制限なしの権利が含まれます。また、このソフトウェアを提供する相手に対してそのような行為を許可することも許諾されています。この許諾は次の条件を前提としています。</p> <p>上記の著作権に関する通知およびこの許諾通知は、ソフトウェアの複製物および実質的な部分のすべてに含めてください。</p> <p>本ソフトウェアは「現状のまま」で、明示であるか暗黙であるかを問わず、何らの保証もなく提供されます。ここでいう保証とは、商品性、特定の目的への適合性、および権利非侵害についての保証も含みますが、それに限定されるものではありません。著作権者は、契約行為、不法行為、またはそれ以外であろうと、ソフトウェアに起因または関連し、あるいはソフトウェアの使用またはその他の扱いによって生じる一切の請求、損害、その他の義務について何らの責任も負わないものとします。</p>
著作権テキスト	<p>http://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html</p> <p>PuTTYの著作権はSimon Tathamが有しています(1997-2019)。</p> <p>部分著作権 Robert de Bath、Joris van Rantwijk、Delian Delchev、Andreas Schultz、Jeroen Massar、Wez Furlong、Nicolas Barry、Justin Bradford、Ben Harris、Malcolm Smith、Ahmad Khalifa、Markus Kuhn、Colin Watson、Christopher Staite、Lorenz Diener、Christian Brabandt、Jeff Smith、Pavel Kryukov、Maxim Kuznetsov、Svyatoslav Kuzmich、Nico Williams、Viktor Dukhovni、およびCORE SDI S.A。</p> <p>このソフトウェアおよび関連する文書ファイル(以下「ソフトウェア」)を入手したすべての人は、このソフトウェアを制限なしに使用することが無償で許諾されています。これには、ソフトウェアの使用、複製、変更、結合、発行、配布、サブライセンスおよび販売についての制限なしの権利が含まれます。また、このソフトウェアを提供する相手に対してそのような行為を許可することも許諾されています。この許諾は次の条件を前提としています。</p> <p>上記の著作権に関する通知およびこの許諾通知は、ソフトウェアの複製物および実質的な部分のすべてに含めてください。</p> <p>本ソフトウェアは「現状のまま」で、明示であるか暗黙であるかを問わず、何らの保証もなく提供されます。ここでいう保証とは、商品性、特定の目的への適合性、および権利非侵害についての保証も含みますが、それに限定されるものではありません。</p>

	ん。著作権者は、契約行為、不法行為、またはそれ以外であろうと、ソフトウェアに起因または関連し、あるいはソフトウェアの使用またはその他の扱いによって生じる一切の請求、損害、その他の義務について何らの責任も負わないものとします。
使用目的	アプライアンスマシン上で、putty.exeを使用してLinuxバックアップサーバと通信し、システムロケールとUDP Linux ロケールを変更します。
必要な変更	x