

Arcserve Cyber Resilient Storage

バージョン 2

インストールおよびセットアップガイド

arcserve®

法律上の通知

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。

Arcserveの事前の書面による承諾を受けずに本書の全部または一部を複製、譲渡、変更、開示、修正、複製することはできません。本書はArcserveが知的財産権を有する機密情報であり、ユーザは(i)本書に関連するArcserveソフトウェアの使用について、Arcserveとユーザとの間で別途締結される契約により許可された以外の目的、または(ii)ユーザとArcserveとの間で別途締結された守秘義務により許可された以外の目的で本書を開示したり、本書を使用することはできません。

上記にかかわらず、本書で取り上げているソフトウェア製品(複数の場合あり)のライセンスを受けたユーザは、そのソフトウェアに関して社内で使用する場合に限り本書の合理的な範囲内の部数のコピーを作成できます。ただしArcserveのすべての著作権表示およびその説明を各コピー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 Sections 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。

© 2026 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 へのお問い合わせ

Arcserve サポート チームは、技術的な問題の解決に役立つ豊富なリソースを提供します。重要な製品情報に簡単にアクセスできます。

[Arcserve へのお問い合わせ](#)

Arcserve のサポート：

- 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。
- 弊社のライブ チャット リンクを使用して、Arcserve サポート チームとすぐ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。

目次

第1章: はじめに	1
第2章: 概要	2
第3章: バージョンの互換性とライセンス	3
第4章: Arcserve Cyber Resilient Storageをインストールする方法	4
インストール前のチェックリスト	5
ハードウェア要件	6
TCP/ネットワーク要件	11
ISO ファイルのダウンロード	16
ブート可能メディアの作成	17
Arcserve Cyber Resilient Storage のインストール	18
初期設定	19
トラブルシューティング オプション	22
復旧と再インストール	23
復旧	23
再インストール	23
相違点	23
第4章: セキュア ブート	25
不変性との統合	25
プラットフォームおよび展開のサポート	26
キーおよび信頼管理	26
更新およびアップグレード動作	26
利点	26
セキュアブートの有効化	27
VM でのセキュアブートの有効化	28
Arcserve Cyber Resilient Storageでのセキュアブートの有効化	30
MOK の登録	31
第5章: 非接続環境での展開	33
第6章: システムの健全性およびステータスのログイン バナー	36
問題解決の手引き	38
第7章: のアップグレード Arcserve Cyber Resilient Storage	40
更新のダウンロードとインストール	41
リムーバブルメディアを使用したオフライン更新	43
第7章: 更新後の設定アクション	45
システム設定とセキュリティポリシーの確認	47

設定変更の適用	49
第8章: インストール環境の復旧	51
既存のストレージ プールのインポート	52
第9章: ストレージの設定	53
命名規則	54
ストレージ プールの作成	55
ファイルシステムの作成	57
データ アクセストークンの作成	59
プールへのディスクの追加	60
プール内のディスクの交換	61
スペア ディスクの管理	62
スペア ディスクの使用方法	63
第10章: ジャンボ フレームのサポート	65
第11章: ネットワーク管理	66
ネットワーク プロファイルの管理	67
ネットワーク プロファイルの作成	68
ネットワーク プロファイルの一覧表示	70
ネットワーク プロファイルの変更	72
ネットワーク プロファイルの削除	74
ネットワーク プロファイルの切り替え	75
ネットワーク ボンディング	76
ネットワーク ボンディングの作成	77
ネットワーク ボンディングの変更	80
ネットワーク ボンディングの削除	81
第12章: アラート管理	82
ストレージ アラート	83
SMART ディスク アラート	85
アラートの電子メールの設定	87
アラートの設定	89
第13章: ユーザ管理	90
ユーザの作成	91
ユーザの更新	93
第14章: サポートとの連携	94
サポート バンドルの生成	95
サポート バンドルのアップロード	96
サポートのリモート アクセスを有効にする	97

USBドライブへのサポート バンドルの書き込み	99
第15章: OneXafe からのデータストアの移行	101
第16章: 一般的なエラーと問題	102
「利用可能なディスクが見つかりません」というエラーでストレージの作成に失敗する	103
制約のないシェルにアクセスできません	104
単一のディスクで作成されたプールにディスクを追加できない	105
再起動時のデバイス名の変更	106
データストアサイズの違い	107
シェルとUDP コンソールでの表記の違い	108
ファイルシステム空き容量が正しくない	109
間違ったキーを入力しても検証メッセージが表示されない	110
Admin/Superuser アカウントのパスワードをリセットできない	111
Arcserve Cyber Resilient Storage のリビルド	112
UDP のリビルド	113
logs コマンドが実行されている限り、ターミナルはタイムアウトしません	114
第17章: 付録	115
コマンド リファレンス	116

第1章: はじめに

Arcserve Cyber Resilient Storage は、既存の UDP 10.x インストールを補完し、データをサイバー攻撃から保護し、サイバーセキュリティコンプライアンスの整合性を維持するために役立ちます。Arcserve Cyber Resilient Storage を使用すると、オンプレミスストレージエンドポイント上のデータストア全体のイミュータブルスナップショットを取得して、ランサムウェアやその他の脅威に対する保護を強化できます。

Arcserve Cyber Resilient Storage は、イミュータブルスナップショットを利用してデータを保護し、データが変更されることなく回復可能な状態を維持し、以下を提供します。

- UDP の安全で占有量の少ないストレージ デスティネーション
- 不正な変更から保護されるイミュータブルスナップショットによるデータの整合性
- ストレージの整合性のためにハードウェア RAID または CRS SW RAID のどちらかを使用できるオプション

Arcserve Cyber Resilient Storage サーバは、シェルまたは CRS シェルとも呼ばれるコマンドラインインターフェース(CLI) を通じて管理されます。詳細については、「[コマンド リファレンス ガイド](#)」を参照してください。

注: このドキュメントには、以下の略語が含まれています。

- **CRS:** Arcserve Cyber Resilient Storage
- **CRS サーバ:** Arcserve Cyber Resilient Storage サーバ
- **CRS データストア:** Arcserve サイバーレジリエント データストア
- **CRS シェル:** Arcserve Cyber Resilient Storage サーバシェル

第2章: 概要

このマニュアルでは、Arcserve Cyber Resilient Storage (CRS サーバとも呼ばれる) のインストールとセットアップの包括的な手順を説明します。このマニュアルは Arcserve Cyber Resilient Storage のインストール、設定、および使用開始に役立ち、以下について説明します。

- ハードウェアおよびネットワークの前提条件
- インストールの種類
- 初期設定
- ストレージ管理
- ネットワークおよびストレージのセットアップ
- アラート管理
- ユーザ管理
- アップグレードの種類と手順
- サポートとの連携方法
- 問題とトラブルシューティング

第3章: バージョンの互換性とライセンス

Arcserve Cyber Resilient Storage と Unified Data Protection (UDP) バージョンは、一般的に相互運用可能です。古いバージョンの UDP は、新しいバージョンの Arcserve Cyber Resilient Storage と連携して動作し、逆も同様です。ただし、Arcserve Cyber Resilient Storage アクティベーションはバージョン固有であり、UDP バージョンおよび対応するライセンスによって異なります。

以下の点に注意してください。

- Arcserve Cyber Resilient Storage を注文する場合は、使用する UDP バージョンを指定する必要があります。
- 複数の UDP バージョンが展開されている場合は、各バージョンに適切な Arcserve Cyber Resilient Storage ライセンスを割り当てる必要があります。
- UDP をアップグレードする場合は、既存の Arcserve Cyber Resilient Storage ライセンスの有効性を維持し、アップグレードした UDP コンソールで引き続き使用できるようにするため、無償 (FOC) の注文を行う必要があります。

第4章: Arcserve Cyber Resilient Storageをインストールする方法

このセクションでは、Arcserve Cyber Resilient Storage をインストールして設定する方法について説明します。

重要: ローカルの NTS (Network Time Security) タイム サーバを設定しない場合は、システムが外部インターネットにアクセスできることを確認してください。Arcserve Cyber Resilient Storage が公開されている NTS タイム サーバにアクセスし、システムクロックの正確な同期を維持するには、外部接続が必要です。

具体的には、このセクションでは以下のトピックについて説明します。

インストール前のチェックリスト	5
ISO ファイルのダウンロード	16
ブート可能メディアの作成	17
Arcserve Cyber Resilient Storage のインストール	18
復旧と再インストール	23

インストール前のチェックリスト

このセクションでは、Arcserve Cyber Resilient Storage をインストールして設定するための前提条件について説明します。以下の内容が含まれます。

ハードウェア要件

このセクションでは、Arcserve Cyber Resilient Storage のインストールと管理に関する推奨ハードウェア仕様について説明します。これには、CPU、メモリ、ストレージメディア、およびネットワークインターフェースに関する考慮事項が含まれます。

Arcserve Cyber Resilient Storage のセットアップを検討する際は、以下の点に注意してください。

- データストレージは、ドライブの障害でもデータが失われないように冗長である必要があります。データストレージの冗長性を確保するには、ハードウェア RAID または CRS RAID を使用して、3 つ以上のディスクからソフトウェア RAID を作成します。

注：ハードウェア RAID とソフトウェア RAID の比較については、「[ソフトウェア RAID とハードウェア RAID](#)」を参照してください。

- Arcserve Cyber Resilient Storage の現在のバージョンは、RedHat バージョン 9 64 ビット (x86_64) で認定されたハードウェアコンポーネントをサポートしています([リンク](#)を参照) 。
- ドライブで障害が発生した場合の OS の冗長性を確保するために、ハードウェア RAID の使用を検討してください。

注：ハードウェア RAID はユーザ側で管理できます。

Arcserve Cyber Resilient Storage は以下に展開できます。

- ストレージドライブの使用方法を管理する IPMI または同様のシステムを使用するプラットフォーム。
- 複数のドライブを個別のストレージドライブとして使用できる非管理ストレージプラットフォーム。

IPMI または同様のシステムを使用する場合、管理者は必要に応じてハードウェア RAID ソリューションを利用できます。

注：OS とデータストレージ用にそれぞれ 1 つ以上の RAID が必要です。構成した RAID は、Arcserve Cyber Resilient Storage がデータストアの格納に使用する単一のドライブとして OS に示されます。

最小ハードウェア要件

このセクションでは、Arcserve Cyber Resilient Storage のインストールと管理に関する最小推奨ハードウェア仕様について説明します。

Arcserve Cyber Resilient Storage には、オペレーティングシステムが検出できる以下の仕様のディスクまたはボリュームが 2 つ必要です。

- インストール用に少なくとも 25 GB のストレージがあるドライブ/ボリュームを 1 つ
- データストア用にドライブ/ボリュームを 1 つ

ハードウェア RAID の展開に関する推奨事項

このセクションでは、Arcserve Cyber Resilient Storage の推奨されるハードウェア RAID 構成、それに応じたストレージ容量、推奨される CPU およびメモリの要件について説明します。

注：環境にハードウェア RAID アダプタが含まれる場合、Arcserve では CRS RAID の代わりにハードウェア RAID を使用することをお勧めします。

RAID 5 ボリューム(3.2% パツファを含む)	RAID 5 使用可能容量(TB) (3.2% パツファなし)	物理 CPU (最小)	推奨 CPU コア(最小)	RAM (GB 単位、最小)
4	3.87	1	1	7
8	7.74	1	1	10
16	15.49	1	2	15
24	23.23	1	3	21
32	30.98	1	4	26
40	38.72	1	4	32
48	46.46	1	5	37
56	54.21	1	6	42
64	61.95	1	7	48
72	69.70	1	7	53
80	77.44	1	8	59
88	85.18	1	10	64
96	92.928	1	10	70
104	100.672	1	12	75
112	108.416	1	12	80
120	116.16	1	14	86
128	123.90	1	14	91
144	139.39	1	16	102
160	154.88	1	16	113
192	185.86	1	19	135
224	216.83	1	22	156
256	247.81	1	25	178
288	278.78	1	28	200
320	309.76	1	31	221

CRS RAID の展開に関する推奨事項

Arcserve Cyber Resilient Storage は、他の従来の RAID アレイよりも CRS RAID 構成を使用します。これは、CRS RAID によりデータの整合性が向上し、RAID 5 の書き込みホールが排除され、ストレージ管理の柔軟性が向上するためです。

以下の表に、CRS RAID 構成を使用する環境の要件を示します。

重要：以下の各 RAID 構成は、使用可能容量、RAW ディスク容量、およびディスク数の組み合わせで構成されています。異なる組み合わせを使用して、同じ構成を作成できます。

使用可能なストレージ容量 (TB) (3.2% パツファなし)	合計 RAW 容量	ディスクごとの RAW ディスク容量*	ディスク数*	推奨 CPU コア	推奨 RAM (GB 単位)	3.2% パツファ (GB 単位)	物理 CPU の最小数
1.936	3	1	3	1	6	0.064	1
3.872	6	2	3	1	8	0.128	1
7.744	12	4	3	1	12	0.256	1
11.616	18	6	3	2	13	0.384	1
15.488	24	8	3	2	16	0.512	1
19.36	30	10	3	2	19	0.64	1
23.232	36	12	3	3	22	0.768	1
30.976	48	16	3	4	32	1.024	1
34.848	54	18	3	4	32	1.152	1
38.72	60	20	3	4	36	1.28	1
46.464	72	24	3	5	48	1.536	1
54.208	84	28	3	6	48	1.792	1
61.952	96	32	3	7	64	2.048	1
69.696	108	36	3	7	64	2.304	1
77.44	100	20	5	8	64	2.56	1
92.928	120	24	5	10	74	3.072	1
108.416	140	28	5	12	98	3.584	1
123.904	160	32	5	13	98	4.096	1
139.392	180	36	5	14	109	4.608	1
162.624	196	28	7	17	126	5.376	1
185.856	224	32	7	19	144	6.144	1
209.088	252	36	7	21	161	6.912	2
216.832	252	28	9	22	167	7.168	2
247.808	288	32	9	25	190	8.192	2
278.784	324	36	9	28	214	9.216	2
309.76	352	32	11	31	237	10.24	2

注：

- ディスクを追加する前に、以前使用したファイルシステムが含まれていないことを確認してください。Arcserve では、新しいディスクまたは完全に消去されたディスクを使用することをお勧めします。
- プールの予約領域として、使用可能容量の少なくとも約 3.2% (最小 128 MB、最大 128 GB) が確保されていることを確認してください。これは、ファイルシステムが重要な処理のために確保する、ストレージプールの容量の一部です。

TCP/ネットワーク要件

Arcserve Cyber Resilient Storage が UDP および RPS と通信するためのネットワーク要件は以下のとおりです。

- 少なくとも 1 つのサポートされているネットワーク インターフェース カード (NIC)。ほとんどのインストールでは、これはイーサネット インターフェースで、DHCP (自動 IP 割り当て) 用に設定するか、静的 IP アドレス、ネットマスク、ゲートウェイ、DNS を使用して手動で設定できます。詳細については、「[サポートされているネットワークカード](#)」を参照してください。
- 標準のインストールの場合は、ネットワーク ケーブルがネットワーク カードに接続されていて、アクティブになっていることを確認してください。
- セキュリティのために Arcserve Cyber Resilient Storage がセグメント化されたネットワークに展開されている場合、追加のポートを開いて通信とデータ転送を有効にします。これらのポートにより、UDP と Arcserve Cyber Resilient Storage サーバの両方のセグメント化されたネットワーク間の通信が可能になります。

以下の表に、Arcserve Cyber Resilient Storage アクセスのファイアウォール ホワイトリスト 登録要件を示します。必要なポート、S3 URL、更新に使用される URL、およびトンネルアクセスをサポートする URL が含まれます。

ポート番号	サービス / プロセス	IP/デスティネーション IP/ノード	TCP/UDP	コメント
22	SSH イ 管 理 者 ク セ ン ド ス	イン バ ウ ン ド	TCP	内部 / LAN のみ。境界でブロック

				Arcserve
				ve
				サービ
				スエン
53	DHC- P	ア ウ ト バCRS DNS カスタマ サーバ ウ ン ド	TCP/UD- P	ドポイ ントの ホスト 名解 決に 必要
222- 4	サ ウ ポート トバCRS supportconnect-crs.arcserve.com	ア ウ ト バCRS supportconnect-crs.arcserve.com	TCP	
443	更 新 サー ビス ウ ン ド	ア ウ ト バCR- https://downloads.arcserve.com/a- S rcserve_family_products/crs	TCP	
443	サ ポー トバウ ンドト ルのバCRS arcserve.castle.supportbundles.s3- us-west-2.amazonaws.com	ア ウ ン ド	TCP	
500- 0- 509- 9	デー タのバ ノール 役ウ 割ン ド	イ ンRPS バノールCRS	TCP	内部 /LAN のみ。 境界 でブ ロック
446- 0	NTS-ア KE ウ キート CRS 交バ 換ウ	■ Time.cloudflare.com ■ Nts.netnod.se ■ Oregon.time.system76.com ■ Brazil.time.system76.com	TCP	

123 NTP 時刻 同期	ンド	■	ntppool1.time.nl
	ア	■	Time.cloudflare.com
	ウ	■	Nts.netnod.se
	ト	■	Oregon.time.system76.com UDP
	バCRS	■	Brazil.time.system76.com
	ウ	■	ntppool1.time.nl
	ン		
	ド		

重要：一部の環境では、パフォーマンス、フェールオーバー、または信頼性の理由から、同じサブネットに複数のネットワークインターフェースが設定されている場合があります。この場合、現在サポートされていないネットワーク機能が必要になるため、Arcserve では、このような環境に Arcserve Cyber Resilient Storage をインストールしないことを強くお勧めします。

サポートされているネットワークカード

Arcserve Cyber Resilient Storage は、さまざまなパフォーマンス、セキュリティ、および展開の要件に対応するために、広範なネットワークインターフェースカード (NIC) をサポートしています。このセクションでは、互換性のある NIC とその仕様を概説します。

標準的なイーサネットカード

- **RedHat**: サポートされているネットワークカード。詳細については、[RedHat Catalog](#) を参照してください。
- **Intel イーサネット NIC**: 1GbE、10GbE、25GbE、40GbE、および 100GbE モデル (X520、X550、X710、E810 など) を含むほとんどのサーバグレードの Intel NIC が、カーネルドライバを利用してネイティブでサポートされます。
- **Broadcom**: NetXtreme シリーズの NIC (BCM5720、BCM57414 など) がサポートされていて、1GbE から 100GbE までの速度を提供します。RDMA 機能が含まれています。
- **Mellanox (NVIDIA)**: ConnectX シリーズの Infiniband およびイーサネットアダプタが、MLNX_OFED ドライバを使用してサポートされます。最新の MLNX_OFED リリースは、CentOS Stream 9 と互換性があります。

SFP および SFP+ モジュールのサポート

- **SFP モジュール (1Gbps)**: CentOS Stream 9 は、主要ベンダのシングルモードおよびマルチモード光ファイバを含む、最大 1Gbps の標準 SFP モジュールをサポートしています。
- **SFP+ モジュール (10Gbps)**: Intel、Mellanox、および Broadcom NIC で幅広くサポートされています。NIC とそのドライバ (Intel X520/X540/X550 用の ixgbe など) がモジュールを認識すれば、10GBASE-SR (850 nm、短距離) や 10GBASE-LR (1310 nm、長距離) などの一般的なモジュールは互換性があります。
- **サードパーティの SFP+ モジュール**: 一部の NIC ベンダ、特に Intel は、ファームウェアによるサードパーティの SFP+ モジュールのサポートを制限している場合があります。テストのために、カーネルパラメータを使用してこれらの制限を回避できます (例: `ixgbe.allow_unsupported_sfp=1`)。実稼働環境では、完全なサポートのためにベンダ認定の光ファイバを使用してください。

SFP28 モジュールのサポート

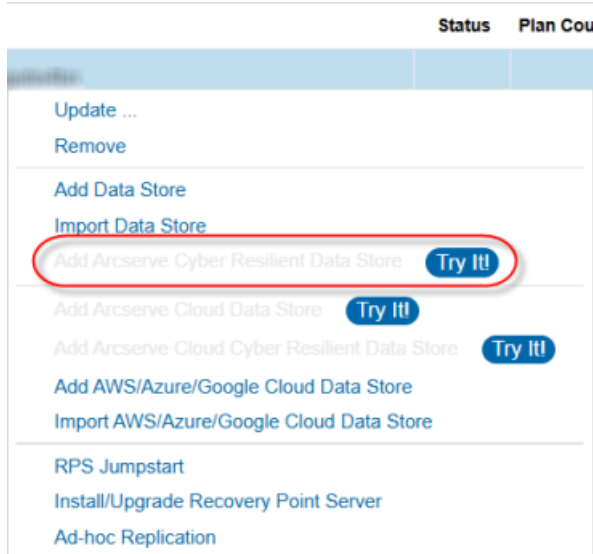
- **SFP28 モジュール (25Gbps)**: Mellanox ConnectX-4/5/6、Intel E810、または Broadcom 25Gb アダプタなどの互換性のある NIC と組み合わせる場合にサ

ポートされます。Linux カーネルバージョン 5.14 以降 (CentOS Stream 9 に含まれています) でネイティブ サポートを利用できます。

ISO ファイルのダウンロード

Arcserve Cyber Resilient Storage の ISO ファイルは、以下のいずれかの方法でダウンロードできます。

- Arcserve コンソールで、**復旧ポイント サーバ**ページの **アクション**メニューから **試す**をクリックします。[Arcserve Cyber Resilient Storage トライアル] ページが開きます。名前、会社情報、電子メールアドレスを入力し、**送信**をクリックします。Arcserve 営業チームからご連絡します。
- **サポート**ページを開きます。製品] から [Arcserve CRS] をクリックし、[Arcserve Cyber Resilient Storage のダウンロード リンク](#) をクリックします。
- UDP コンソールの **復旧ポイント サーバ**ページで、復旧ポイント サーバを右クリックし、メニューから **追加 Arcserve サイバーレジリエント データストア**の横にある **試す**をクリックします。[Arcserve Cyber Resilient Storage トライアル] ページが開きます。名前、会社情報、電子メールアドレスを入力し、**送信**をクリックします。Arcserve 営業チームからご連絡します。



ブート可能メディアの作成

一般的に利用可能なツールを使用して、Arcserve Cyber Resilient Storage の ISO ファイルからブート可能メディアを作成できます。

注：ブート可能 USB ドライブを作成するときに、ツールに DD モードまたは ISO モードのどちらかを選択するオプションが表示されている場合、DD モードを選択することをお勧めします。このモードでは、ISO ファイルの正確なコピーが作成されて、元の構造が保持されます。一方、ISO モードでは、特定の環境で互換性の問題を引き起こす可能性のあるブートローダが導入される場合があります。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage の ISO ファイルをダウンロードします。
2. 必要なツールを選択して、ブート可能メディアを作成します。
3. 目的のブート可能メディア(USB ドライブ、DVD、またはブルーレイ ディスク) を挿入します。

重要：この操作により、リムーバブルメディアからすべてのデータが消去されます。

4. ツールの指示に従って ISO ファイルとメディアを選択し、ブート可能メディアを作成します。

ブート可能メディアから起動するには、コンピュータを再起動し、ブートメニューからメディアを選択します。

Arcserve Cyber Resilient Storage のインストール

このセクションでは、Arcserve Cyber Resilient Storage をインストールして初期設定を完了する方法について説明します。

以下の手順に従います。

1. ブート可能メディアから ISO ファイルを起動します。
2. Arcserve Cyber Resilient Storage を選択します。

インストーラに、オペレーティングシステムのインストールに使用できるディスクのリストが表示され、1 つのディスクがあらかじめ選択されています。デフォルトで、最初に初期化されたディスクが選択されます。

3. 別のディスクを選択するには、目的のディスクを選択し、**Enter** キーを押して選択を確定します。

インストーラは OS のインストールを完了し、シャットダウンします。

4. Arcserve Cyber Resilient Storage をオンにし、以下のデフォルト認証情報を使用してログインし、初期設定を完了します。

- ユーザー名: *arcserve*
- パスワード: *arcserve*

Arcserve Cyber Resilient Storage にサインインすると、初期設定プロセスが開始されます。処理が完了すると、デフォルトのユーザーアカウント *arcserve* が削除され、セットアップ中に作成した新しいアカウントに置き換えられます。

詳細については、「[初期設定](#)」を参照してください。

重要: Arcserve Cyber Resilient Storage アプライアンスの場合、個別の [ファクトリリセット] オプションは必要ありません。クリーンリセットを実行するには、ISO からシステムを起動します。このプロセスにより、アプライアンスが自動的にフォーマットされ、オペレーティングシステムと必要な Arcserve コンポーネントの両方が再インストールされます。詳細については、「[復旧と再インストール](#)」を参照してください。

初期設定	19
トラブルシューティング オプション	22

初期設定

このセクションでは、インストール後の Arcserve Cyber Resilient Storage の初期設定について説明します。初期設定を完了するには、以下の手順が必要です。

- a. Super Admin アカウントの作成
- b. タイムゾーンの選択
- c. (オプション) ホスト名の変更
- d. (オプション) ネットワークプロファイルの変更
- e. (オプション) ストレージプールのセットアップ
- f. (オプション) タイムサーバのセットアップ

注：初期設定が中断された場合は、ユーザ「arcserve」としてシェルにログインすると、中断したところから再開できます。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage を再起動します。
2. インストール後に初めて Arcserve Cyber Resilient Storage にログインするには、ログインプロンプトで、ユーザ名とパスワードの両方に「arcserve」と入力し、Enter キーを押します。

注：これらの認証情報は、初期設定を完了すると削除されます。次のログイン時には、次の手順で作成する super admin の認証情報を使用します。

3. super-admin アカウントを作成してログインするには、ユーザ名とパスワードを入力し、プロンプトが表示されたらパスワードを確認して、Enter キーを押します。

注：

- パスワードは8文字以上で、大文字、小文字、数字が含まれている必要があります。
- パスワードのリセットオプションは、このアカウントでは使用できません。サポートが必要な場合は、Arcserve サポートにお問い合わせください。

4. Arcserve Cyber Resilient Storage システムのタイムゾーンを設定するには、矢印キーを使用して利用可能なタイムゾーンを移動し、Enter キーを押して必要なタイムゾーンを選択します。

注：目的のタイムゾーンがリストにない場合は、[UTC]を選択します。

5. ホスト名を変更するには、プロンプトで「Yes」と入力し、新しいホスト名を入力します。ホスト名を変更せずに続行するには、「No」と入力します。

注: ホスト名は、文字、数字、ハイフンを使用して1 ~ 64文字で指定します。ハイフンで開始または終了できません。

6. プロンプトで、ネットワークプロファイルを作成する場合は、プロンプトで「Yes」と入力します。ネットワークプロファイルを変更せずに続行するには、「No」と入力します。
7. プロファイルの名前を入力し、矢印キーを使用して移動し、Enter キーを押してデバイスを選択します。
8. 矢印キーを使用して移動し、Enter キーを押してネットワーク設定方法を選択します。

DHCP が使用可能で、希望するネットワーク設定方式である場合は、[pv4 Auto]または [pv6 Auto]を選択します。

Arcserve Cyber Resilient Storage を展開するネットワークセグメントがDHCPをサポートしていない場合は、[手動]を選択します。以下の情報があることを確認します。

- 使用するIPアドレス(CIDR表記のみを使用)
- デフォルトゲートウェイ

9. ネットワークプロファイルを自動接続する場合は、プロンプトで「Yes」と入力し、[autoconnect priority]を指定します。自動接続の優先度には、-999 ~ 999の整数を指定できます。

システムによって設定される自動接続優先度のデフォルト値は0です。

10. プロンプトで、MTU (最大転送単位) の値を指定します。MTU 値は60 ~ 9000の範囲で指定できます。

11. 以下のいずれかを実行します。

- 初期ストレージプールを設定するには、プロンプトで「Yes」と入力し、以下を実行します。
 - a. 初期ストレージプールの名前を入力します。
 - b. RAID/ディスク設定を選択します。ソフトウェアCRS RAIDのディスクを選択するには、矢印キーを使用して強調表示し、スペースバーを押します。追加するディスクごとに繰り返します。

注: 新しいCRS RAID ボリュームを作成するには、少なくとも3つのディスクまたは1つのハードウェアRAIDディスクを選択します。

サポートされている RAID 構成は、1 ディスクのハードウェア RAID 構成または 3 ディスクのソフトウェア CRS RAID 構成です。

ストレージプールを作成せずに続行するには、「No」と入力します。後でシェルからプールを作成できます。詳細については、「[ストレージプールの作成](#)」を参照してください。

- インストールプロセスの復旧中に既存の非アクティブなストレージプールをインポートするには、「[既存のストレージプールのインポート](#)」を参照してください。

12. システムで使用するタイムサーバを設定するには、以下のいずれかを実行します。

- 「Yes」と入力し、Enter キーを押します。次に、プロンプトで、1 つ以上の NTP タイムサーバの FQDN をカンマで区切って入力します。

注:

- ◆ Arcserve では、回復力の高い時刻管理を実現するために、少なくとも 3 台以上の独立した NTS サーバを設定することを推奨します。
- ◆ ローカル NTP サーバは、安全で信頼性のある同期された時間を維持するために、インターネットの公開されたタイムソースにアクセスできない、隔離されたネットワークやエアギャップ状態のネットワーク(非接続展開)で主に使用されます。
- 「No」と入力すると、デフォルトの Network Time Protocol (NTP) タイムサーバがシステムによって自動的に設定されます。

これで初期設定は完了になります。

トラブルシューティング オプション

インストーラの実行時にインストールのトラブルシューティングを行うには、以下の手順に従います。

- Ctrl + B + 1 キーを押す - メイン インストール ウィンドウに移動します。
- Ctrl + B + 2 キーを押す - シェルに移動します。
- Ctrl + B + 3 キーを押す - ログに移動します。
- Ctrl + B + 4 キーを押す - ストレージ ログに移動します。
- Ctrl + B + 5 キーを押す - プログラム ログに移動します。

注：ウィンドウを切り替えるには、Alt + Tab キーの組み合わせを使用します。

復旧と再インストール

このセクションでは、Arcserve Cyber Resilient Storage を使用した場合の復旧と再インストールの違いについて説明します。どちらのプロセスもデバイスを使用可能な状態にリストアしますが、目的は異なり、アプローチも異なります。この違いを理解しておく、問題が一時的な障害なのか、それともシステムの完全な再構築が必要なのかといった状況に応じて、管理者が適切な方法を選択するために役立ちます。

復旧

復旧は、状態のリストア操作です。復旧は、アプライアンスを再構築するのではなく、基盤となる CRS システムが変更されていないことを前提として、アプライアンスを以前の正常な状態に戻すことに重点が置かれます。これには、障害後の設定、サービス、またはシステム機能のリストアが含まれます。復旧では、システムの再フォーマットやオペレーティングシステムの再インストールは行いません。アプライアンスをワイプせずに問題を解決したり、変更をロールバックしたりするように設計されています。

詳細については、「[インストール環境の復旧](#)」を参照してください。

再インストール

再インストールプロセスは、インストールプロセスとほぼ同じですが、すでにインストールされているシステム上で実行される点が異なります。

再インストールは、アプライアンスが不安定であるか、設定に誤りがある場合、または完全に最初からやり直したい場合に使用します。Arcserve Cyber Resilient Storage システムのフルインストールを実行します。CRS ISO からアプライアンスを起動すると、システムディスクが完全にフォーマットされ、アプライアンスが最初から再構築されます。この処理により、CRS mini オペレーティングシステムと必要な Arcserve コンポーネントが再インストールされ、アプライアンスが工場出荷時に近い状態に戻ります。既存の設定、データ、および以前のシステム状態はすべて削除されます。

詳細については、「[Arcserve Cyber Resilient Storage サーバのインストール](#)」を参照してください。

相違点

以下の表で、この 2 つの違いについて詳細に説明します。

復旧	再インストール
障害または破損の後、CRS を既知	システム全体を新しい CRS イメージ

の信頼できる動作状態にリストアします。	で置き換えます。
システムの不安定性、ブートの失敗、ランタイム状態の破損。	メジャーバージョンの変更、重大な破損、またはデバイスの転用。
既存の不変のCRSイメージを使用します。	新しい不変のCRSイメージを書き込みます。
不変層の外部に保存されたユーザーデータおよび設定を保持します。	ユーザーデータと設定は、明示的にバックアップしない限り、通常は消去されます。
最小限のリセット。実行時状態と検証済みコンポーネントのみをリストアします。	完全なリセット。すべてを工場出荷時またはベースラインの状態に戻します。
高速	遅い
信頼できるイメージがデバイスにすでに存在するため、リスクは低い。	バックアップが不完全である場合や、イメージの選択を誤った場合は、リスクが高い。

第4章: セキュア ブート

Arcserve Cyber Resilient Storage のセキュア ブートでは、信頼された署名済みのソフトウェアコンポーネントのみがシステムにロードされます。Arcserve Cyber Resilient Storage は、暗号化によって検証されたブート チェーンを適用することで、ブート キットや不正なカーネル変更などの低レベルの改ざんから保護します。

物理および仮想の両方の展開用に設計されたセキュア ブートは、Arcserve Cyber Resilient Storage の CentOS 9 ベースのプラットフォームおよび OpenZFS ストレージ スタックとシームレスに動作し、ブート ロード、カーネル、およびストレージ モジュールを含むすべての重要なコンポーネントが初期化前に認証されるようにします。この機能はデフォルトで有効になっており、システムの更新後も引き続き適用されます。

Arcserve Cyber Resilient Storage は、UEFI セキュア ブートの完全な信頼チェーンを実装します。ロードは、各ステージが次のステージに進む前に有効であることを確認します。ステージは以下のように進行します。

UEFI ファームウェア → 署名済み Shim → GRUB2 → 署名済みカーネル → 署名済み OpenZFS モジュール

- UEFI ファームウェアは、標準プラットフォームが信頼する署名済み shim ロードを検証します。
- shim は、GRUB2 をロードして検証します。
- GRUB2 は、Linux カーネルおよび initramfs を検証してロードします。
- カーネルは、ロードする前に、OpenZFS を含むすべての必要なモジュールが署名済みで信頼できる状態であることを確認します。

このエンドツーエンドの検証により、許可されたソフトウェアコンポーネントのみが起動時に実行されます。

不変性との統合

Arcserve Cyber Resilient Storage のイミュータブル アーキテクチャにより、セキュア ブートが強化されます。

- オペレーティングシステムは改ざんに対する耐性を備えています。
- 更新は、署名済みで検証済みのパッケージとして配信されます。

これらのメカニズムにより、不正な変更の永続化を防ぎ、システムの攻撃対象領域を削減します。

プラットフォームおよび展開のサポート

Arcserve Cyber Resilient Storage のセキュアブートは、以下のプラットフォームで動作するように設計されています。

- ベアメタル UEFI システム
- 以下を含む仮想環境：
 - ◆ VMware
 - ◆ Microsoft Hyper-V
 - ◆ Proxmox/KVM (OVMF/UEFI)

Arcserve Cyber Resilient Storage ISO は、これらの環境でセキュアブートを有効にして正常に起動するように事前設定されているため、手動で調整したり、プラットフォームのセキュリティ機能を無効にしたりする必要がありません。

キーおよび信頼管理

Arcserve Cyber Resilient Storage は、必要に応じて管理者が Arcserve Cyber Resilient Storage 固有の署名キーを信頼できるようにする、マシン所有者キー (MOK) の登録をサポートします。

ガイド付きのワークフローでは、セキュアブートを無効にすることなく、1 回限りのキー登録が可能です。登録後、OpenZFS を含むすべての必要なモジュールがエラーなしでロードされます。

更新およびアップグレード動作

すべてのカーネルおよびモジュールの更新は事前に署名および検証されているため、アップグレード後も手動での操作や再設定を必要とせずに、システムは引き続き安全に起動できます。

利点

セキュアブートは、起動時に不正なコンポーネントや改ざんされたコンポーネントが実行されるのを防ぐことで、Arcserve Cyber Resilient Storage のセキュリティを強化します。サポート対象のプラットフォームで設定変更を行うことなくシームレスに動作するため、導入を簡素化できます。また、信頼できるブートとシステムの整合性を前提とするコンプライアンス要件にも対応しています。

セキュアブートの有効化

このセクションでは、Arcserve Cyber Resilient Storage システムでセキュアブートを有効にする方法について説明します。セキュアブートを有効にするには、以下の3つの手順を実行します。

- ハイパーバイザでセキュアブートを有効にします。
- Arcserve Cyber Resilient Storage システムでセキュアブートを有効にします。
- MOK Manager (MOK マネージャ) に MOK を登録します。

詳細については、以下のセクションを参照してください。

VM でのセキュアブートの有効化	28
Arcserve Cyber Resilient Storageでのセキュアブートの有効化	30
MOK の登録	31

VM でのセキュアブートの有効化

このセクションでは、VMware vCenter でセキュアブートを有効にする方法について説明します。サポートされている他のハイパーバイザについては、対応するドキュメントを参照し、環境内で同等の手順を実行してください。

以下の手順に従います。

1. vCenter にログインします。
2. 左のナビゲーション ペインで、Arcserve Cyber Resilient Storage インスタンスを右クリックし、**設定の編集**]を選択します。
3. **VM オプション**]タブを選択し、**ブート オプション**]セクションを展開します。
4. **有効**]チェック ボックスをオンにして、セキュアブートを有効にします。

Edit Settings

Virtual Hardware
VM Options
Advanced Parameters

> General Options
VM Name:

> VMware Remote Console Options
Expand for VMware Remote Console settings

> Encryption
Expand for encryption settings

> VMware Tools
Expand for VMware Tools settings

Secure Boot
☐ Enabled

Boot Delay
When powering on or resetting, delay boot order by
0 milliseconds

Force EFI setup
☐ During the next boot, force entry into the EFI setup screen

Failed Boot Recovery
☐ If the VM fails to find boot device, automatically retry after

5. **OK** をクリックします。

Arcserve Cyber Resilient Storageでのセキュアブートの有効化

このセクションでは、Arcserve Cyber Resilient Storage システムでセキュアブートを有効に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 Cyber Resilient Storage にログインします。
2. 以下のコマンドを入力して DKMS キーを登録し、次に Enter キーを押します。

```
security enforce --category secureboot
```

セキュアブート登録パスワードを作成するように求められます。

3. プロンプトでパスワードを入力し、Enter キーを押します。

```
> security enforce --category secureboot
Create a new Secure Boot key enrollment password:
Confirm password:
Secure Boot enforcement has been initiated. To complete the process:
  1. Reboot the system.
  2. When prompted, enter the enrollment password and choose 'DKMS module s
  3. Ensure Secure Boot is enabled in UEFI.
After reboot, run 'security check' to confirm Secure Boot is fully enabled.
>
```

パスワードの確認を求められます。

4. パスワードを再度入力し、Enter キーを押します。

この時点で、セキュアブートの適用が開始されます。セキュアブートを完全に有効にするには、以下の手順に従います。

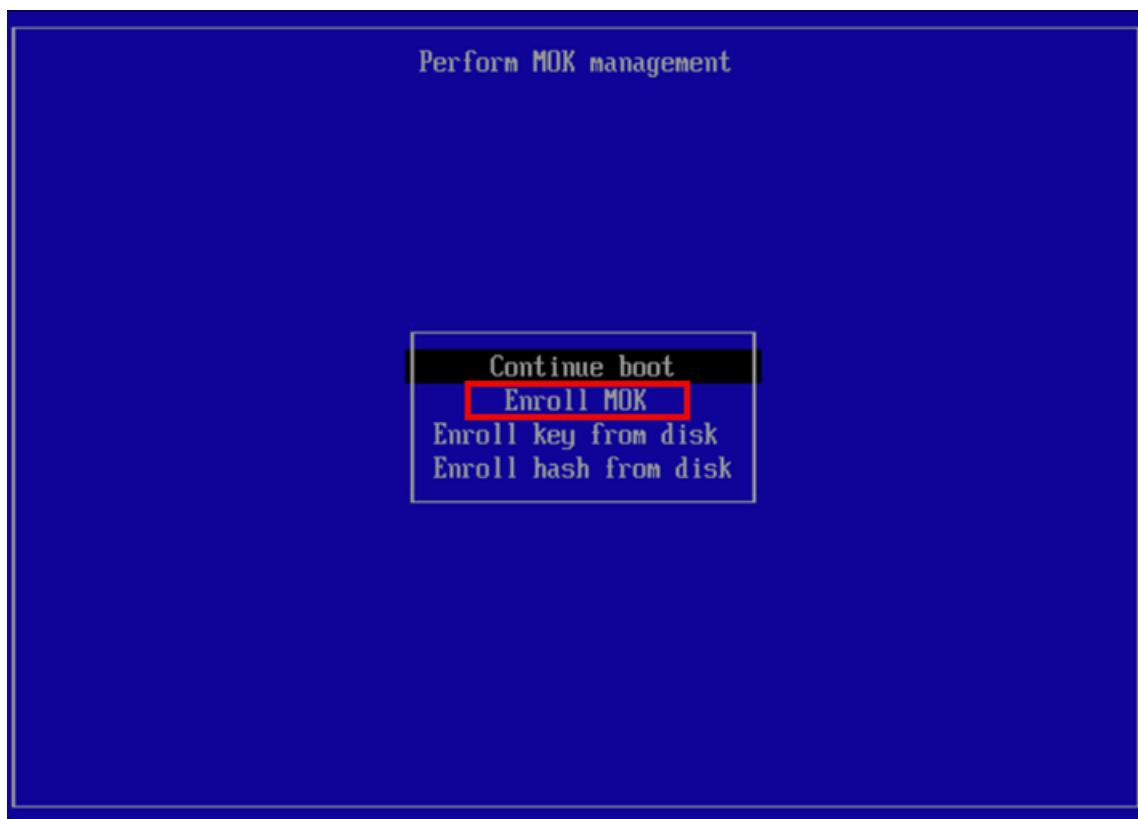
- a. システムを再起動します
- b. プロンプトが表示されたら、登録パスワードを入力し、DKMS モジュール署名キーを選択します。
- c. セキュアブート用のマシン所有者キーの管理に使用する UEFI ベースのインターフェースである MOK マネージャ画面から、セキュアブートを有効にします。詳細については、「[MOK の登録](#)」を参照してください。

MOK の登録

マシン所有者キー(MOK)の登録は、Arcserve Cyber Resilient Storage でセキュアブートを有効にするプロセスに必要な手順です。セキュアブート設定の一部として、MOK 登録は、システムファームウェアとデフォルトのプラットフォームキーによって署名されていない Arcserve Cyber Resilient Storage 固有のコンポーネントとの信頼関係を確立します。この手順を完了すると、Arcserve Cyber Resilient Storage がセキュアブート要件に準拠し、システムの整合性を維持しながら安全にブートできます。

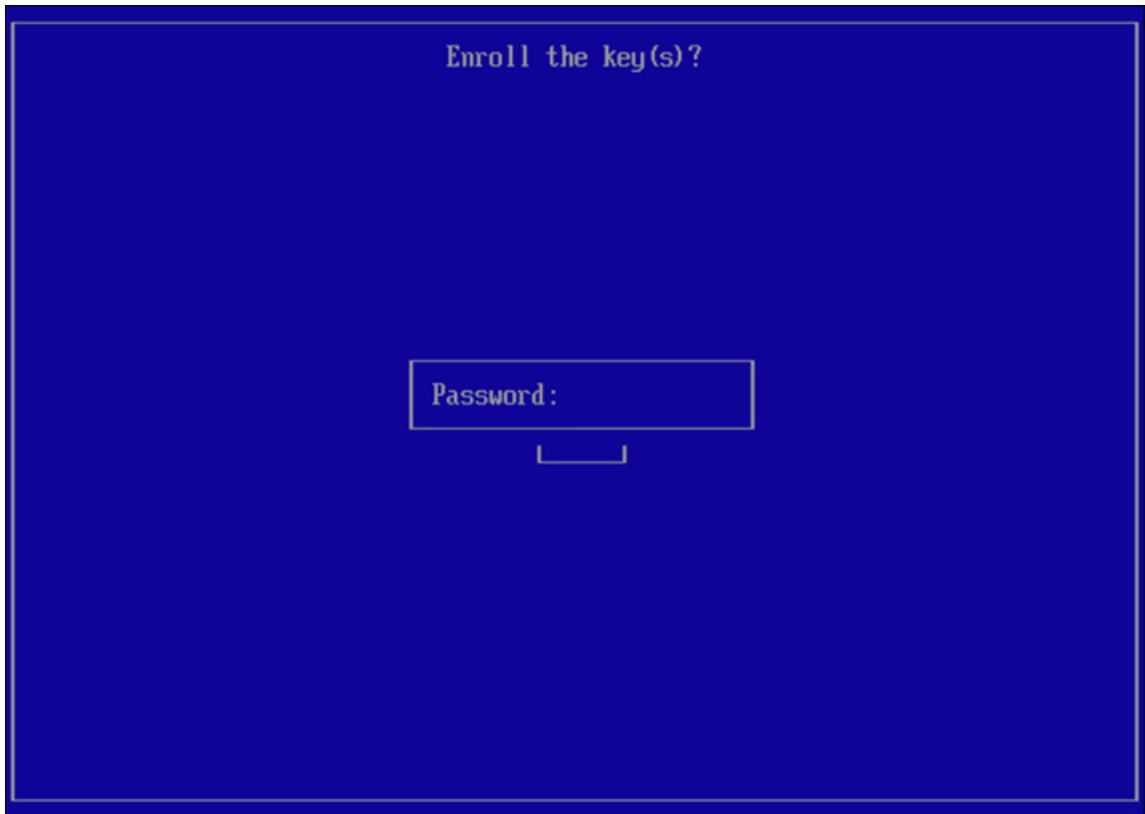
以下の手順に従います。

1. MOK Manager (MOK マネージャ) 画面で、任意のキーを押します。
2. 画面に表示されるオプションのリストから、[Enroll MOK (MOK の登録)]を選択し、[Continue (続行)]を選択します。



確認メッセージが表示されます。

3. [Yes (はい)]を選択し、[Password (パスワード)]テキスト ボックスに、作成したセキュアブート登録パスワードを入力します。



4. 次に、**Reboot (再起動)**]をクリックします。システムが再起動し、ログインプロンプトが表示されます。
5. ログイン ID とパスワードを入力します。

Arcserve Cyber Resilient Storage システムでセキュアブートが有効になりました。

第5章: 非接続環境での展開

Arcserve Cyber Resilient Storage は、セキュリティを重視する環境で運用している利用者をサポートするため、非接続環境(ダークサイト)での展開を可能にします。非接続展開のサポートにより、インターネットや外部ネットワークへの接続がない、完全なエアギャップ状態の環境で Arcserve Cyber Resilient Storage の運用が可能です。この機能は、政府、防衛、重要なインフラストラクチャ、規制対象の企業など、厳格なデータ処理ポリシーがある組織にとって不可欠です。

非接続展開では、Arcserve Cyber Resilient Storage は自己完結型のシステムとして機能しますが、外部サービスを利用せずに、データの不変性、保持ポリシー、および監査性の適用を継続します。そのため、非接続展開のサポートは、予測可能かつ検証可能なシステム動作を維持しながら、オンライン更新メカニズムおよびネットワークベースの時間の同期に依存しないように設計されています。

非接続環境に展開する場合、以下の機能により、安全で準拠したオフライン運用が可能になります。

- **オフラインのソフトウェア更新:** Arcserve Cyber Resilient Storage は、CD-ROM や USB メディアなどのリムーバブルメディアを使用したソフトウェアおよび設定の手動更新をサポートしていて、インターネット接続が不要になります (CentOS 9 および OpenZFS と互換性があります)。

以下のようなコンプライアンス関連の特性があります。

- ◆ 更新パッケージは、インポート前に、非接続環境外で準備、確認、および承認されます。
- ◆ 整合性と信頼性を確保するために、更新はローカルで検証されます。
- ◆ 許可されたユーザのみがオフライン更新処理を実行できます。
- ◆ ログ、設定、および関連するシステムメタデータを含む、完全な診断/サポートバンドルを USB メディアにエクスポートするコマンドが CLI で用意されています。
- ◆ どの段階でも、アウトバウンドまたはインバウンドのネットワーク接続は必要ありません。

この更新モデルは、規制の枠組みで一般的に必要とされる変更管理、職務の分離、および監査のトレーサビリティをサポートします。

詳細については、「[リムーバブルメディアを使用したオフライン更新](#)」を参照してください。

- **ローカルシステムタイムサーバ(NTS への依存なし):** 管理者は、一般に公開されているインターネットベースのタイムサーバを利用する代わりに、ローカ

ル NTS サーバをインストールおよび継続的な運用時の時間の同期に使用するように Arcserve Cyber Resilient Storage を設定できます。ローカル NTS サーバにアクセスできないか、サーバの検証に失敗した場合、インストール処理によって明確なエラーメッセージが表示され、管理者は再設定または再試行ができます。

以下のようなコンプライアンス関連の特性があります。

- ◆ 保持期間、不変性の適用、および監査ログは、すべてローカルシステム時間に基いています。
- ◆ 時間の設定は、制御された管理手順によって実行されます。
- ◆ 時間の同期は、インターネット接続を必要とせずに、ローカル NTS サーバを使用して機能し続けます。
- ◆ 外部の時間への依存をなくすことで、攻撃対象領域を減らし、ネットワークソースを通じた不正な時間操作を防止します。

この手法は、外部のタイムソースが利用できないか、許可されていない環境で、一貫したポリシーの適用をサポートします。

注：プライベート NTS タイムソースを展開する場合は、NTS サーバによって提供される証明書が、CentOS によって信頼されている認証局 (CA)、つまり一般に認められた CA によって署名されていることを確認してください。また、証明書の CN (共通名) は、サーバのホスト名と一致している必要があります。

CentOS 9 でサポートされている IDP ソースのリストは、[こちら](#)で確認できます。

詳細については、「[初期設定](#)」の手順 8 を参照してください。

- **オフラインでの USB へのサポート バンドルの書き込み：** Arcserve Cyber Resilient Storage は厳格なセキュリティおよび不変性の要件を維持できる方法で診断をサポートしていて、ユーザはオフラインで USB ドライブにサポートバンドルを生成できます。これにより、ネットワークチャネルを通じてデータが環境から移動することがなくなり、機密性の高いログが公開されることを防止でき、システムの不変の状態が維持されます。

以下のようなコンプライアンス関連の特性があります。

- ◆ アウトバウンドの接続を必要とせず、非接続環境を定義する厳格なネットワーク分離を維持します。
- ◆ 機密性の高い設定やログデータは、承認および制御されたメディア (USB ドライブ) を利用しない限り、安全な境界を離れることはありません。

-
- ◆ システムの状態を変更したり、不変性の保証に違反したりせずに診断を生成することで、セキュリティおよび運用ポリシーに確実に準拠します。
 - ◆ 組織は、確立された物理メディアの手順を使用して、隔離された環境から安全にログを移動できます。
 - ◆ トラブルシューティングのワークフローで、クラウド接続、リモート エンドポイント、またはインターネットベースのサポート ユーティリティを利用しないようになります。
 - ◆ 環境をネットワークにまったく接続せずにトラブルシューティングを実行できます。

詳細については、「[USB ドライブへのサポート バンドルの書き込み](#)」を参照してください。

第6章: システムの健全性およびステータスのログイン バナー

Arcserve Cyber Resilient Storage にログインすると、システムの健全性およびステータス バナーが表示され、クリティカルなシステムの健全性およびステータスを即座に確認できます。サインインするとすぐに、バナーに関連するシステム テレメトリが集約されて表示されます。

```
      _  _  _
     [ ]--'--[ ]
     |'|""`""|'| | |
     | | / ^ \ | |
     |_|_|I|_|_|

Arcserve Cyber Resilient Storage Server version 26.05.343

Type help for a list of available commands.

----- Attention Required -----
FAILED Storage capacity threshold exceeded on pool 'pool1'.
FAILED Storage degradation has been detected on pool 'sdpool2'.

> |
```

ログイン時に主要なアラートとステータス インジケータを直接表示することで、個々の問題に対して複数の追加コマンドを実行しなくても、システムの現在の健全性とステータスをすばやく理解できます。これにより、ハードウェアの警告や設定上の問題をできるだけ早い段階で特定できます。

ログイン時に、以下のような簡潔で実用的な情報が表示されます。

- ストレージの劣化、エラー、しきい値アラート
- Network Time Security (NTS) ステータス
- S.M.A.R.T. ディスク チェック ステータス
- 電子メール アラート 設定 ステータス

この情報をログイン時に最初に表示することで、状況を迅速に把握でき、管理者は日常業務においてハードウェア障害やシステム異常を見落とすリスクを軽減できます。

問題解決の手引き

このセクションでは、ログインシステムの健全性バナーに表示されるシステム生成のアラートおよび警告を解釈して対応する方法について説明します。これらのアラートは、機能またはユーザエクスペリエンスに影響を与える可能性のある、システムの重大な状態またはパフォーマンスの低下を示します。以下の推奨事項では、問題を迅速に特定し、その影響を評価すると共に、通常の運用をリストアして影響を最小限に抑えるための適切な対処手順について説明します。

「ディスク SMART チェックがディスク '{disk_name}' で失敗しました。」

以下の disk list コマンドを実行し、報告された障害を確認して、ディスク障害の重大度を評価します。

```
disk list -v -d <ディスク名>
```

調査結果に基づいて、ディスクの交換が必要かどうかを判断します。交換が必要な場合は、次のメンテナンス期間中に交換を実施するようスケジュールします。

「プール '{pool}' でストレージ エラーが検出されました。」

以下の pool status コマンドを実行して、プールに関して報告されたエラーを確認します。

```
pool status -v -p <pool_name>
```

問題がディスク関連のエラーとして識別された場合は、次のメンテナンス期間中に影響を受けたディスクを交換します。

「プール '{pool}' でストレージ劣化が検出されました。」

以下の pool status コマンドを実行して、プールに表示されているエラーを確認します。

```
pool status -v -p <プール名>
```

ディスクエラーの場合は、次のメンテナンス ウィンドウでディスクを交換します。

「プール '{pool_name}' のストレージ容量しきい値を超えました。」

以下のコマンドを使用して、影響を受けたプールにディスクを追加します。

```
pool add-disk -p <プール名> -d <プールに追加するディスク>
```

「**[time show]** を実行して診断してください」

このメッセージは、ネットワークまたは NTS サーバに問題がある場合に表示されます。以下のコマンドを実行して問題を診断します。

```
time show
```

「**[email configure]** を実行して電子メール サーバをセットアップしてください。」

このメッセージは、電子メールサーバが設定されていない場合に表示されます。
以下のコマンドを実行して、電子メールサーバをセットアップします。

email configure

第7章: のアップグレード Arcserve Cyber Resilient Storage

このセクションでは、Arcserve Cyber Resilient Storage を古いバージョンから最新バージョンにアップグレードする方法について説明します。更新は、セキュリティアーキテクチャと展開モデルに合わせた、制御された明確な手順で実行されます。

- インターネットに接続された展開では、Arcserve Cyber Resilient Storage は承認されたソースから更新パッケージを直接安全にダウンロードできるため、整合性の検証と監査性を維持しながら、ソフトウェアとコンテンツの更新を適時に適用できます。
- ネットワーク接続が利用できないか許可されていない非接続展開では、更新は CD-ROM や USB ドライブなどのリムーバブルメディアを使用してオフラインでインストールされます。この方法を使用すると、安全で計画的かつ検証可能な方法で、更新をエアギャップ状態の環境に導入できます。

このセクションでは、Arcserve Cyber Resilient Storage の更新プロセスの概要を示し、両方の更新シナリオについて説明します。

注: 更新を続行する前に、すべてのプランおよびポリシーが一時停止または停止されていることを確認してください。

更新のダウンロードとインストール	41
リムーバブルメディアを使用したオフライン更新	43

更新のダウンロードとインストール

このセクションでは、更新をダウンロードしてインストールし、Arcserve Cyber Resilient Storage を古いバージョンから最新バージョンにアップグレ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。

1. Arcserve Cyber Resilient Storage にログインします。
2. コマンド プロンプトで以下のコマンドを入力して、**Enter** キーを押します。

update config show

ダウンロード チャンネルとタグが表示されます。

```
Arcserve Cyber Resilient Storage Server version 1.0.42

Type help for a list of available commands.

> update config show
CHANNEL                                     TAG
https://downloads.arcserve.com/arcserve_family_products/crs  latest
> _
```

3. 以下のコマンドを入力して、**Enter** キーを押します。

update check

利用可能な最新の更新がリストされます。

```
> update check
Updates available: version 0.9.1000 is available for installation.
> _
```

4. 次に、以下のコマンドを入力して、**Enter** キーを押します。

update install

更新後にシステムが再起動するというメッセージが表示されます。

5. 続行するかどうかを尋ねられたら、**y** キーを押し、次に **Enter** キーを押します。

```
> update install
The system will automatically reboot after updating.
Do you want to proceed? [y/n]: y
Rebooting node in 1 seconds _____ 80% 0:00:02
Broadcast message from root@10.10.10.10 (Fri 2025-06 16:30:00):

The system will reboot now!

Success
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
```

アップグレードが完了し、システムが再起動します。Arcserve では、メンテナンスの時間帯にシステムを再起動することをお勧めします。

リムーバブルメディアを使用したオフライン更新

Arcserve Cyber Resilient Storage が非接続環境として展開されている場合、またはポリシーによってネットワーク接続以外の方法で更新を配布する必要がある場合は、リムーバブルメディアを使用したオフライン更新が、承認されたシステムまたはアプリケーションの更新をシステムに転送する安全で監査可能な方法を提供します。この処理により、外部の脅威にさらされるリスクを軽減し、更新を制御された検証可能な方法で確実に導入できます。インターネットに接続された環境でも、機密性の高いコンポーネント、規制された展開、または継続運用においてオフライン更新手順が必要な場合があります。管理者は、リムーバブルメディア (CD-ROM や USB ドライブなど) を使用してオフライン更新をインストールすることで、不変性とセキュリティの保証を維持しながら、必要な更新を必要に応じて確実に適用できます。

重要:

オフライン更新を開始する前に

- 更新されたインストールメディアを含む CD-ROM または USB ドライブがシステムに接続されていることを確認してください。更新を開始する前に、リムーバブルメディアが正しく挿入され、システムに認識されていることを確認してください。*disk list* または *update check --offline* コマンドを使用して、正しい更新メディアが使用可能で、接続されているかどうかを確認します。
- 更新の実行に使用する USB ドライブに、16 GB 以上の空き容量があることを確認します。
- 正しい更新メディアを含むリムーバブルメディア デバイス (USB ドライブやその他の外部メディアなど) が 1 つだけシステムに接続されていることを確認してください。複数のリムーバブルメディア デバイスを接続すると、更新が失敗したり、間違った更新メディアが選択されたりする場合があります。

以下の手順に従います。

1. USB ドライブを接続したら、利用可能であることを確認するため、以下のコマンドを入力して Enter キーを押します。

disk list

```
> disk list
NAME      USE      SIZE      VENDOR
sda       OS       113.0G    ATA
sdb       USB      29.2G     SanDisk
```

これは、USBドライブが正しく装着され、利用可能であることを確認して、更新をコピーしてインストールできるようにするためです。

2. コマンド プロンプトで以下のコマンドを入力して、Enter キーを押します。

update check --offline

```
Arcserve Cyber Resilient Storage Server version 1.6.1386

Type help for a list of available commands.

> update check --offline
Update available: version 1.6.1398
>
```

このコマンドは、リムーバブルメディアで利用可能な更新があるかどうかを確認し、利用可能な更新とそのバージョン番号を一覧表示します。利用可能な更新がない場合は、以下のメッセージが表示されます。

「No updates found. (更新が見つかりませんでした。)」

3. 次に、以下のコマンドを入力して、Enter キーを押します。

update install --offline

```
Arcserve Cyber Resilient Storage Server version 1.6.1386

Type help for a list of available commands.

> update check --offline
Update available: version 1.6.1398
> update install --offline
The system may automatically reboot after updating. Please pause all plans using this storage server.
Local (offline) install: Updates will be applied from an attached CDROM or USB device.
Do you want to proceed? [y/n]:y
Updates have started...
Working...
```

確認メッセージが表示されます。

4. 「y」と入力して続行します。

注: 「n」と入力して更新を中止し、コマンドを終了します。

更新処理が開始され、進行状況バーが表示されます。更新のインストール後、システムが再起動します。

更新されたバージョンの Arcserve Cyber Resilient Storage にサインインするための認証情報を入力します。初期設定中または初期設定後に作成したユーザ名とパスワードを使用できます。

第7章: 更新後の設定アクション

アップグレード後、インストール中に確定できない設定変更があり、システムが更新されたソフトウェアを実行した後に適用する必要があります。更新後の設定アクション機能を使用すると、一貫性があり、予測可能で、検証可能な状態で設定変更を完了できます。

これを管理するために、Arcserve Cyber Resilient Storage は、現在のシステムおよびアプリケーションの設定を、新しいソフトウェアバージョンの予想される状態と比較して評価します。相違点がある場合は、ログイン時に保留中の設定アクションが通知されます。



これらの変更は、専用のファイナライズコマンドを使用して、運用上適切なときに確認および適用できます。このプロセスは、透明性と管理性を確保するように設計されています。

- ユーザは、設定の更新が保留中であるかどうかを確認できます
- 実行前に必要な更新の明確なリストが提供されます
- 各アクションは、繰り返し可能な(べき等)方法で適用されます
- 手順が失敗した場合のガイダンスを含む詳細な結果がレポートされます

システムが完全にアップグレードされて実行された後に設定の更新を適用することで、Arcserve Cyber Resilient Storage は不完全または不整合な設定を回避し、すべての変更を正しいランタイムコンテキストに適用します。この方法は、信頼性の

高いシステム操作をサポートすると同時に、管理者がアップグレード後のアクションを明確に把握して制御できるようにします。

重要：一度適用されると、これらの設定変更は永続的であり、元に戻すことはできません。

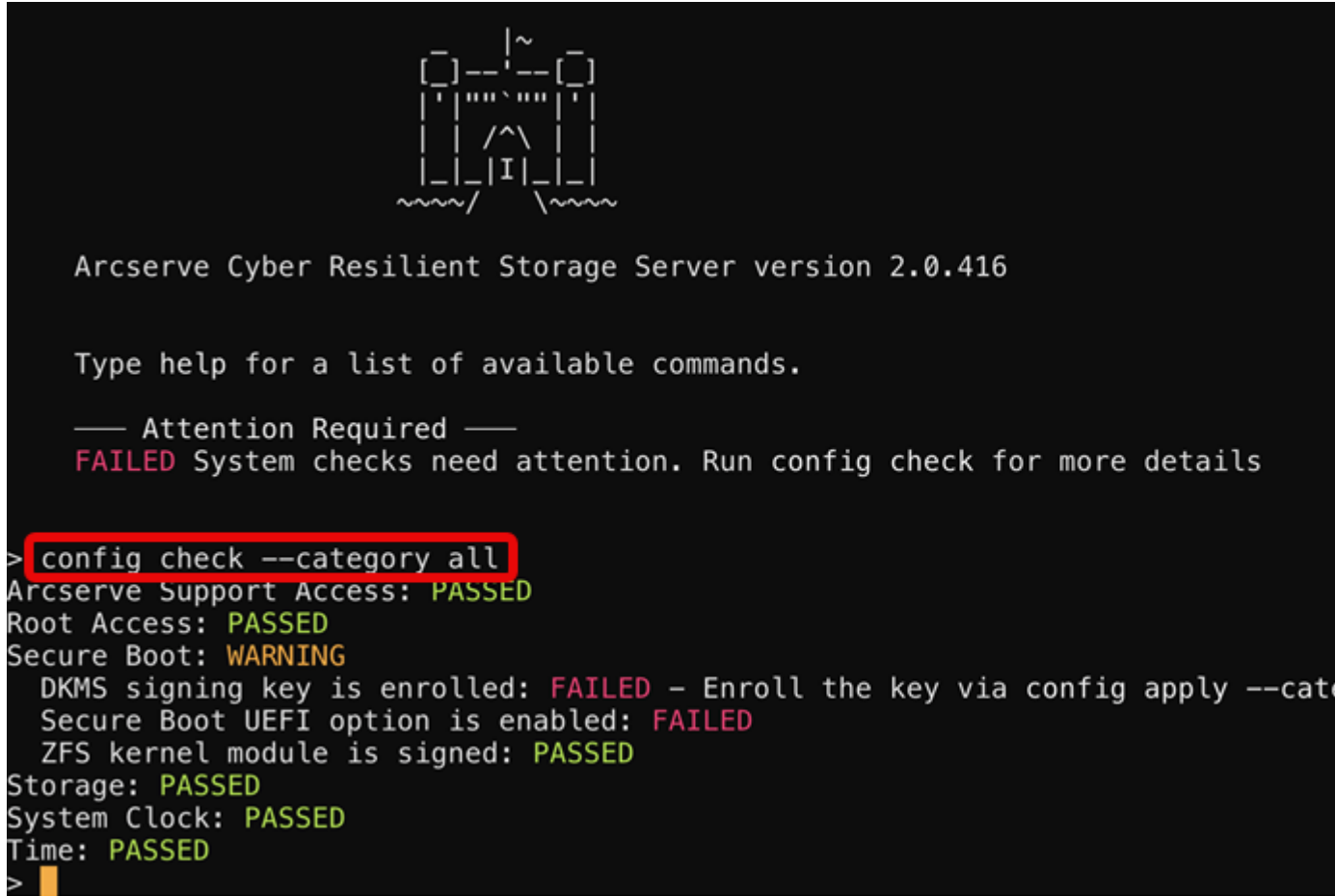
これらのコマンドを実行すると、システムは以下を実行します。

- 現在のシステムおよびアプリケーションの設定を、製品バージョンで定義されている目的の状態と比較します。
- ユーザが手動で追加の手順を実行しなくても、正しく動作させるために必要なすべての設定変更を適用します。
- 変更された内容、すでに準拠している内容、および失敗した内容を示す、人が読める形式のレポートを生成します。

システム設定とセキュリティポリシーの確認	47
設定変更の適用	49

システム設定とセキュリティポリシーの確認

一部の設定およびポリシーは、アップグレード後にのみ適用できます。設定チェックコマンドは、保留中の更新後の設定変更を確認し、一覧表示します。



以下の構文でコマンドを使用します。

```
config check [-h] [-v] -c CATEGORY
```

各項目の説明

-v, --verbose

正常なカテゴリを含む、すべての情報を表示します。

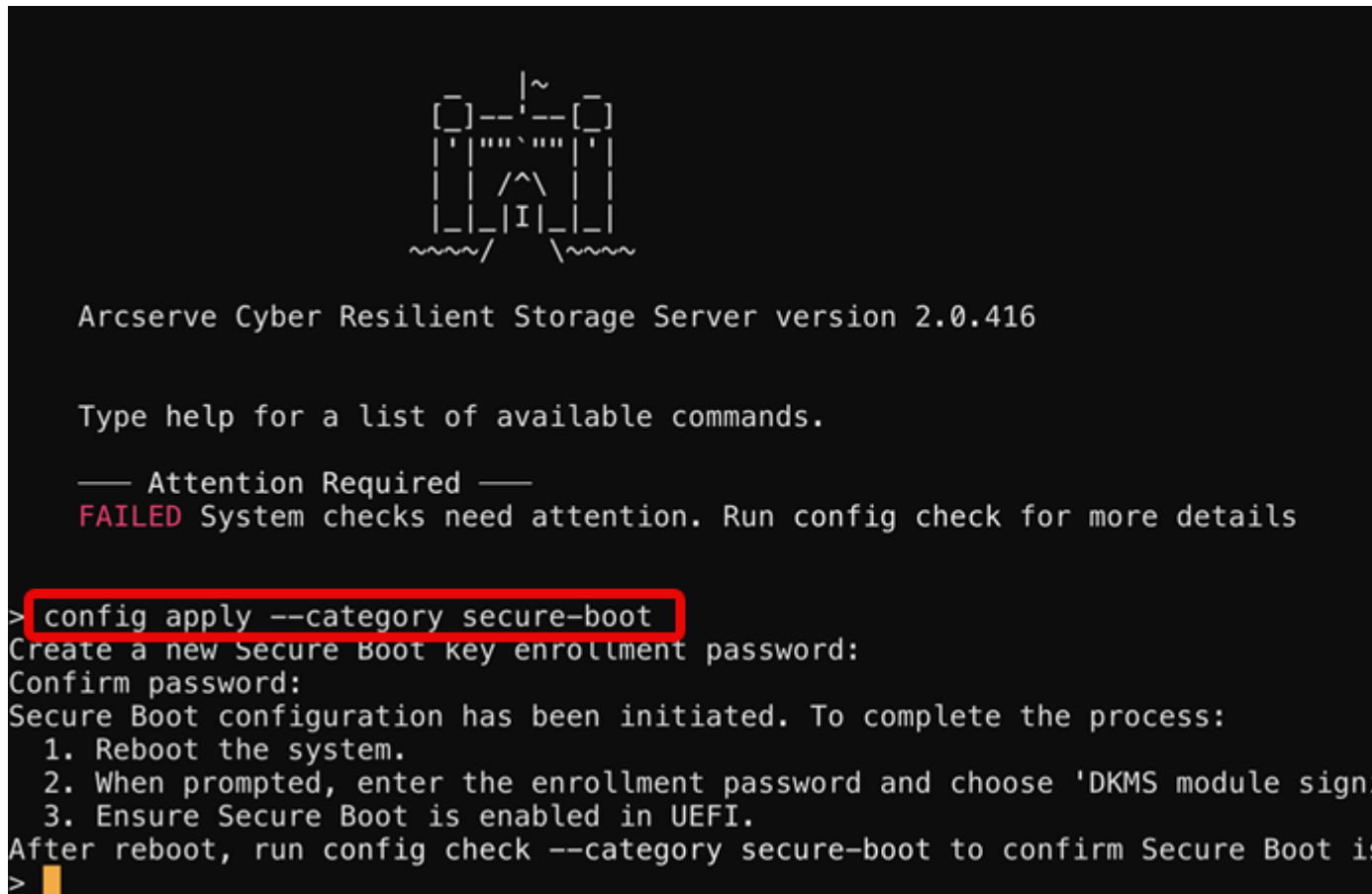
`-c`、`--category`

可能な選択: arcserve-support-access、root-access、secure-boot、system-clock、time、security、system、all

カテゴリの詳細については、「コマンド リファレンス ガイド」の「[check](#)」を参照してください。

設定変更の適用

このセクションでは、アップグレード後にシステムに設定変更を適用するコマンドの実行方法について説明します。



以下のコマンドを使用して、システム設定およびセキュリティポリシーを目的の状態に変更します。

```
config apply [-h] [-v] -c CATEGORY
```

各項目の説明

`-v`、`--verbose`

適用後のルールごとの結果を表示します。

デフォルト： False

-c, --category

可能な選択: arcserve-support-access、root-access、secure-boot、system-clock、time、security、system、all

カテゴリの詳細については、「コマンド リファレンス ガイド」の「[apply](#)」を参照してください。

第8章: インストール環境の復旧

このセクションでは、Arcserve Cyber Resilient Storage インストール環境の復旧を実行する方法について説明します。復旧は通常、システムクラッシュやOS環境の破損、更新やインストールの失敗が発生した場合に実行されます。

重要: Arcserve のサポート チームのガイダンスなしで、インストール環境を独力で復旧しようすると、システムが不安定になったり、データが失われたり、さらに複雑な事態になったりする場合があります。Arcserve Cyber Resilient Storage システムの整合性と適切な機能のために、**手順 4 と 5 はご自身で実行しないでください。**

プロセスを完了するには、以下の手順が必要です。

1. オペレーティングシステムを再インストールします。詳細については、「[Arcserve Cyber Resilient Storageのインストール](#)」を参照してください。
2. 初期設定を完了します。詳細については、「[初期設定](#)」を参照してください。
3. 既存のストレージプールをインポートします。詳細については、「[既存のストレージプールのインポート](#)」を参照してください。
4. ファイルシステムのマウント
5. 設定ファイルのリストア

重要: 手順 4 と 5 については、[Arcserve サポート](#)にお問い合わせください。

既存のストレージプールのインポート	52
---	----

既存のストレージ プールのインポート

このセクションでは、以前のインストールから既存の非アクティブなストレージ プールをインポートするために必要な手順について説明します。既存のプールのインポートは、復旧プロセスの重要な手順であり、ユーザが既存のストレージおよびデータにアクセスできるようにします。

復旧プロセスの詳細については、[\[インストール環境の復旧\]](#)を参照してください。

以下の手順に従います。

1. 非アクティブなプールのインポートするように求められたら、「Yes」と入力し、**Enter** キーを押します。
非アクティブなプールのリストが表示されます。
2. 矢印キーを使用して移動し、スペースバーを押して必要なプールを選択します。
選択したプールがインポートされます。
3. プールがインポートされたことを確認するには、以下のコマンドを入力し、**Enter** キーを押します。

pool list

第9章: ストレージの設定

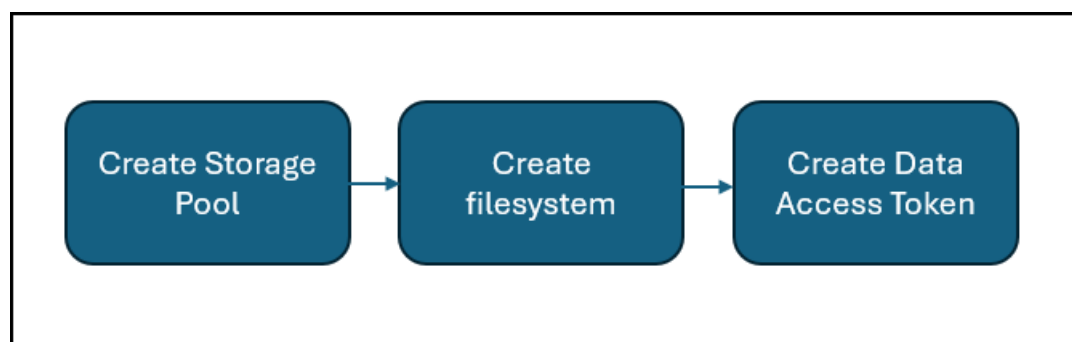
Arcserve Cyber Resilient Storage に追加のストレージを設定すると、不変性の保証を維持し、サービスの中断を回避し、既存のデータ構造およびアクセスポリシーとのシームレスな統合を実現できます。

このプロセスには、以下のための重要な手順とベストプラクティスが含まれます。

- システムの互換性を維持する
- データの整合性を保持する
- パフォーマンスへの影響を最小限に抑える

これらのガイドラインに従うことで、運用の信頼性とセキュリティを維持しながら、ストレージインフラストラクチャを効果的に拡張できます。

以下の図は、UDPでストレージを設定するための一般的なプロセスワークフローを示しています。



命名規則	54
ストレージプールの作成	55
ファイルシステムの作成	57
データアクセストークンの作成	59
プールへのディスクの追加	60
プール内のディスクの交換	61
スペアディスクの管理	62
スペアディスクの使用方法	63

命名規則

Arcserve Cyber Resilient Storage コンポーネント (データセット やプールを含む) に名前を付けるときには、以下のルールに従います。

- コンポーネント名に使用できるのは英数字のみです。
- コンポーネント名には以下の特殊文字を含めることができます。
 - ◆ アンダースコア(_)
 - ◆ ハイフン(-)
 - ◆ コロン(:)
 - ◆ ピリオド(.)
- プール名は文字で始まる必要があり、以下の制限があります。
 - ◆ 英数字、アンダースコア(_)、ハイフン(-)、ピリオド(.)を含めることができます。
 - ◆ 開始シーケンス c[0-9] は使用できません
 - ◆ log という名前は予約されています
 - ◆ mirror、raidz、raidz1、raidz2、raidz3、または spare で始まる名前は、予約されているため使用できません
 - ◆ パーセント記号(%) は使用できません
- データセット名は以下を満たす必要があります。
 - ◆ 英数字で始まる
 - ◆ パーセント記号(%) を含まない
 - ◆ 予約名を使用しない
- 空のコンポーネントは使用できません。

ストレージ プールの作成

このセクションでは、ディスクをプールに追加してストレージを作成する方法について説明します。

注：ソフトウェア RAID 設定では、少なくとも 3 つのディスクが必要です。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. コマンド プロンプトで以下のコマンドを入力して、**Enter** キーを押します。

```
disk list
```

既存のディスクのリストが表示されます。これにより、プールに追加できるディスクが表示されます。

3. 以下のコマンドを入力して、**Enter** キーを押します。

```
pool create [-h] -p POOL -d DISKS [DISKS ...] [-P {single,double,triple}] [-F | --force | --no-force]
```

各項目の説明

-p, --pool

プールの名前。

-d, --disks

プールに追加するディスクの名前。

注：ディスク名をスペースで区切ることで、複数のディスクを追加できます。

-P, --parity

プールのパリティ。

可能な選択：single、double、triple。

-F, --force, --no-force

警告を無視してプールの作成を強制します。既存のディスクデータを上書きする可能性があります。

デフォルト：False

注：ディスクを追加するときに、以下のエラーが発生する場合があります。

- 「ディスクには既存のデータがあります。」
- 「ディスクは使用中ですが、不明なファイルシステムが含まれています。」

- 「異なるサイズのディスクが指定されています。プール内のすべてのディスクの使用量は、最小のディスクのサイズに制限されます。」

これは、以前に使用したディスクを使用していて、ディスクに保存されているデータが消去されていない場合に発生します。続行する前に、一覧表示されているディスクがこのプールに使用するディスクであることを確認してください。

既存のデータを削除するには、以下のコマンドを使用します。

```
pool create --force
```

指定したディスク上にストレージ プールが作成されます。

プール関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[pool](#)」を参照してください

ファイルシステムの作成

このセクションでは、ファイルシステムの作成方法について説明します。

以下の手順に従います。

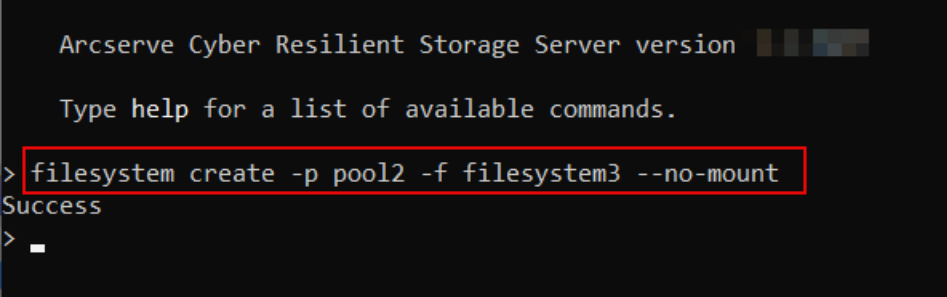
1. Arcserve Cyber Resilient Storage にログインします。
2. コマンド プロンプトで以下のコマンドを入力して、Enter キーを押します。

```
filesystem list
```

既存のファイルシステムのリストが表示されます。

3. 次に、以下のコマンドを入力して、Enter キーを押します。

```
filesystem create [-h] -p POOL -f FILESYSTEM [-m | --mount | --no-mount]
```



```
Arcserve Cyber Resilient Storage Server version 10.0.0.0
Type help for a list of available commands.
> filesystem create -p pool2 -f filesystem3 --no-mount
Success
>
```

各項目の説明

-p、--pool

プールの名前。

-f、--filesystem

ファイルシステムの名前。

-m、--mount、--no-mount

作成後にファイルシステムをマウントする。

デフォルト：True

ファイルシステムが作成されます。

4. ファイルシステムが作成されたかどうかを確認するには、以下のコマンドを入力し、Enter キーを押します。

```
filesystem list
```

注：ファイルシステムに関連付けられたポート番号は、UDP および Arcserve コンソールで Arcserve サイバーレジリエント データストアを追加またはインポートするときに使用されます。

ファイルシステム関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[filesystem](#)」を参照してください。

データ アクセストークンの作成

このセクションでは、データ アクセストークンの作成方法について説明します。データ アクセストークンは、UDP および Arcserve コンソールで Arcserve Cyber Resilient Storage アカウントを設定するときに使用されます。

詳細については、以下を参照してください。

- 「[UDP ソリューション ガイド](#)」の「[Cyber Resilient Storage アカウントの追加](#)」
- 「[Arcserve クラウド コンソール ユーザ ガイド](#)」の「[Arcserve Cyber Resilient Storage アカウントの追加](#)」

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. 以下のコマンドを入力して、**Enter** キーを押します。

```
key create [-h] -i ID [-c [COMMENT]]
```

各項目の説明

-i, --id

アクセス キーの識別子

-c, --comment

オプションのコメント

新しいキーが作成され、ID とシークレット アクセス キーが表示されます。キーをコピーして安全に保管します。

```
> key create -h
usage: key create [-h] -i ID [-c [COMMENT]]

options:
  -h, --help            show this help message and exit
  -i ID, --id ID        identifier for the access key
  -c [COMMENT], --comment [COMMENT]
                        optional comment

> key create -i wqgzzz -c "first account for the demo"

ID          SECRET
wqgzzz      L-xLgdzJ7ez4rUfCrThDHJSoCoJpxr5jA4_usEPrmEw

Make note of the secret above. This is the only time it will be shown.
>
```

キー関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[key](#)」を参照してください。

プールへのディスクの追加

このセクションでは、ディスクをプールに追加して追加のストレージを作成するために必要な手順について説明します。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. ディスクを追加するには、以下のコマンドを入力して、**Enter** キーを押します。

```
pool add-disk [-h] [-p POOL] [-t [DISK_TYPE]] -d DISK
```

各項目の説明

-p、--pool

プールの名前。

-t、--disk-type

プールに追加するディスクの種類。指定できる種類は *data* と *spare* です。

種類が指定されていない場合、ディスクは種類が *data* のディスクとして追加されます。

-d、--disk

プールに追加するディスクの名前。

ディスクがプールに追加されます。再同期化プロセスが完了するまで待機し、以下のコマンドを使用して、プールが使用可能かどうかを確認します。

```
disk status
```

新しいディスクがプールに追加されたかどうかを確認するには、以下のコマンドを使用します。

```
disk list
```

注：新しいディスクをストレージプールに追加しても、すぐには使用できません。システムは、「再同期化」と呼ばれるプロセスを実行する必要があります。このプロセスでは、プール内の冗長性と整合性を確保するために、新しいディスクまたは交換されたディスク間でデータをコピーして検証します。データのサイズとハードウェアの速度によっては、このプロセスに時間がかかる場合があります。ストレージプールは、再同期化プロセスが正常に完了して初めて完全に利用可能となり、安全に使用できる状態になります。

プール関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[pool](#)」を参照してください。

プール内のディスクの交換

このセクションでは、ストレージ プール内のディスクを交換する手順について説明します。RAID アレイのストレージ ディスクは、通常、障害が発生した場合、またはまもなく障害が発生すると予測されるときに交換されます。

重要: プール内のディスクを交換するときは、RAID アレイには同じサイズのディスクが使用されていることに注意してください。したがって、小さいディスクをより大きなストレージ容量のディスクと交換した場合でも、新しいディスクの容量はアレイ内の最小ディスクのサイズに制限されます。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. ディスクを交換するには、以下のコマンドを入力して、**Enter** キーを押します。

```
pool replace-disk [-h] -p POOL -d DISK -n NEW_DISK
```

各項目の説明

`-p`、`--pool`

交換するディスクを含むプールの名前。

`-d`、`--disk`

交換対象の古いディスクの名前。

`-n`、`--new-disk`

古いディスクを交換後の新しいディスクの名前。

新しいディスクがプールに追加されたかどうかを確認するには、以下のコマンドを使用します。

```
pool list
```

注: ストレージ プール内の既存のディスクを交換しても、すぐには使用できません。システムは、「再同期化」と呼ばれるプロセスを実行する必要があります。このプロセスでは、プール内の冗長性と整合性を確立するために、新しいディスクまたは交換されたディスク間でデータをコピーして検証します。データのサイズとハードウェアの速度によっては、このプロセスに時間がかかる場合があります。ストレージ プールは、再同期化プロセスが正常に完了して初めて完全に利用可能となり、安全に使用できる状態になります。

プール関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[pool](#)」を参照してください。

スペア ディスクの管理

最新のデータストレージシステムでは、データの整合性を維持し、ダウンタイムを最小限に抑えるために、信頼性と可用性が不可欠です。フォールトトレランスを向上させる効果的な方法の1つは、ストレージプールでスペアディスクを使用することです。

Arcserve CRS RAID は、ホットスペアとも呼ばれるスペアディスクの使用をサポートしています。スペアディスクは、アクティブディスクに障害が発生したときに自動的にアクティブになるスタンバイドライブです。このセットアップは、継続的なデータアクセスと稼働時間が重要な環境では特に重要です。

```
> pool status -v
```

NAME	STATE	CAPACITY	USED	FREE	STATUS
pool	ONLINE	0%	20.1M	1.5T	Healthy

DISK NAME	STATE	READ ERRORS	WRITE ERRORS	CRC ERRORS
sdb	ONLINE	0	0	0
sdc	ONLINE	0	0	0
sdd	ONLINE	0	0	0
sde	SPARE	-	-	-
sdf	SPARE	-	-	-

ストレージプールにスペアディスクを追加することは、信頼性、フォールトトレランス、復旧速度を向上させるプロアクティブな方法です。以下のような利点があります。

- **障害からの自動復旧**：ディスクに障害が発生すると、スペアディスクが自動的にそのディスクに取って代わります。システムはスペアディスクにデータを再構築するので、ダウンタイムとデータ損失のリスクが減ります。
- **冗長性の向上**：スペアディスクは、ハードウェア障害のバックアップとして機能します。これは、冗長性が不可欠な RAID または CRS 構成で特に重要です。
- **再構築中のリスクの最小化**：スペアディスクへのデータの再構築は、手動での交換を待つよりも迅速かつ安全です。これにより、プールの機能が低下した状態になっている時間が短縮されます。

スペア ディスクの使用 方法

スペア ディスクは、通常のディスクを追加する場合と同じ方法でストレージ プールに追加できます。ただし、アクティブ ディスクとは異なり、スペア ディスクはディスクの障害が発生するまでアイドル状態のままです。プールには、以下の 2 種類のディスクを追加できます。

- **データ:** このディスクは RAID 構成の一部として追加され、ユーザデータおよびパリティ(該当する場合)をアクティブに保存します。日常の読み取り/書き込み処理に参与します。
- **スペア:** これは、RAID アレイに追加される未使用のディスクで、通常の処理時にデータを保存せず、スタンバイとして機能します。常にオンラインですが使用されず、アクティブなディスクに障害が発生するまでアイドル状態のままです。ディスクの障害が発生すると、自動的にオンラインになり、障害が発生したディスクに取って代わります。システムは、パリティやミラーリングなどの冗長性方式を使用して、失われたデータをスペア ディスクに再構築します。

```
> pool status -v
NAME STATE CAPACITY USED FREE STATUS
pool ONLINE 0% 20.1M 1.5T Healthy
DISK NAME STATE REAS ERRORS CRC ERRORS
sdb ONLINE 0 0 0
sdc ONLINE 0 0 0
sdd ONLINE 0 0 0
sde SPARE - - -
sdf SPARE - - -
```

たとえば、4 つのデータ ディスクと 1 つのスペア ディスクがある RAID 5 構成では、データ ディスクにユーザデータが保存されます。1 つのディスクに障害が発生すると、スペア ディスクが自動的にオンラインになり、失われたデータを再構築します。

注:

- スペア ディスクのサイズは、プール内の最大ディスクのサイズ以上になっている必要があります。
- プールには最大 15 個のスペア ディスクを追加できます。

スペア ディスクを追加するには、以下のコマンドで、ディスクの種類パラメータ `[-t [DISK_TYPE]]` に「`spare`」と入力します。

```
pool add-disk [-h] [-p POOL] [-t [DISK_TYPE]] -d DISK
```

パラメータの詳細については、「[コマンド リファレンス ガイド](#)」の「[add-disk](#)」を参照してください。

スペア ディスクが障害の発生したディスクを引き継いだ後、`pool status` コマンドを使用して、プール内のディスクのステータスを確認します。プールのステータスには、スペア ディスクがオンラインで、障害が発生したディスクのステータスが「FAULTED」であることが示されます。

```
> pool status -v
```

NAME	STATE	CAPACITY	USED	FREE	STATUS				
pool	DEGRADED	0%	20.0M	1.5T	Unhealthy				
DISK NAME	STATE	REASON	ERRORS	CRC	ERRORS				
sdb	ONLINE		0	0					
sdc	ONLINE		0	0					
sdd	FAULTED	Disk is failed	0	0					
sde	ONLINE	Spare disk is online	0	0					
sdf	SPARE		-	-					

スペア ディスクがアクティブになると、以下のいずれかの方法でプールを管理できます。

- 障害が発生したディスクを交換する: 新しいディスクをプールに追加します。このオプションの場合、再同期化が必要になり、時間とリソースを費やすことになる可能性があります。再同期化が完了すると、スペア ディスクは解放されてプールに戻されます。
- スペア ディスクを使用して続行する: スペア ディスクはすでにオンラインで再同期化されているため、追加の作業は必要ありません。以下のコマンドを使用して、障害が発生したディスクをプールから削除します。

```
pool remove-disk
```

これにより、プールがオンライン状態に戻ります。その後、今後の障害に備えて、新しいディスクをスペアとしてプールに追加することを検討してください。

第10章: ジャンボ フレームのサポート

Arcserve Cyber Resilient Storage は、高速 ネットワーク全体でデータ転送の効率とパフォーマンスを向上させるジャンボフレームをサポートしています。標準の1,500 バイトを超えるイーサネット フレーム(通常は最大 9,000 バイト)を有効にすることで、システムによってプロトコルのオーバーヘッドが軽減され、大規模なデータ転送中に送信されるパケット数が最小限に抑えられます。これにより、CPU の使用率が低下し、ネットワークの輻輳が緩和され、レプリケーション、バックアップ、復旧などの主要な処理のスループットが増加します。

また、ジャンボフレームのサポートにより、同期の高速化が可能になり、データの検証および整合性のチェック時の遅延が減るため、サイバーレジリエンスが向上します。Arcserve Cyber Resilient Storage のインフラストラクチャは、ジャンボフレーム用に設定されたネットワークデバイスとシームレスに連携し、断片化やパケットの損失を防ぎます。これらの最適化により、全体的なパフォーマンスが向上し、データの可用性、整合性、サイバー脅威や中断発生時の迅速な復旧を維持するシステムの機能が強化されます。

ジャンボフレームを有効にするには、以下のコマンドの `--mtu MTU` パラメータで最大転送単位の値を指定します。

```
network profile modify [-h] -p PROFILE [-d DEVICE] [--ipv4 IPV4] [--ipv6 IPV6] [-a ADDRESS] [-g GATEWAY] [--dns [DNS ...]] [--mtu MTU] [--autoconnect | --no-autoconnect] [-r AUTOCONNECT_PRIORITY]
```

ジャンボフレームを適切に機能させるには、以下の点に注意してください。

- データパス内のすべてのデバイス(NIC、スイッチ、ルータ) がジャンボフレームをサポートしている必要があります。
- 一部のデバイスがジャンボフレームをサポートし、他のデバイスがサポートしていない混合環境では、MTU を慎重に設定する必要があります。
- IPv4 および IPv6 でサポートされる最小値と最大値は、ネットワークインターフェースがサポートできる値によって異なります。
- ジャンボフレームは、大規模なデータ転送には役立ちますが、小規模なトランザクションや遅延の影響を受けやすいアプリケーションのパフォーマンスは向上させません。

コマンドの構文とパラメータの詳細については、「[コマンド リファレンスガイド](#)」の「[modify](#)」を参照してください。

第11章: ネットワーク管理

「ネットワーク管理」では、インフラストラクチャ内で Arcserve Cyber Resilient Storage が確実かつ安全に動作するために必要なネットワーク設定の構成、維持、および最適化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。

ネットワークプロファイルの管理

Arcserve Cyber Resilient Storage のネットワークプロファイルは、事前に定義されたネットワークおよびセキュリティの一連の設定で、ネットワークへの接続方法とネットワークでの動作を制御します。これらは、環境全体で展開をシンプルにし、一貫性を適用し、セキュリティを強化するために使用されます。管理者は、展開および継続的な運用時にこれらのプロファイルを定義して Arcserve Cyber Resilient Storage に割り当て、接続性、アクセス制御、およびバックアップまたは管理システムとの統合がすべて標準化された監査可能な方法で処理されるようにします。

Arcserve Cyber Resilient Storage には、基盤となるシステムの状態を変更せずに、事前に定義されたネットワーク設定を定義、選択、および適用できる、ネットワークプロファイル管理コマンドがいくつか用意されています。ストレージはイミュータブルであるため、これらのコマンドは通常、ディスクのファイルを変更せずに、実行時に読み取り専用のネットワークプロファイルをロード、アクティブ化、または切り替えます。この手法では、接続の変更の制御を可能にしながら、再起動後も不正変更を防止できる一貫したネットワーク動作を実現できます。

これらのコマンドは、データの不変性の境界外で動作するので有用です。アクセスと通信を管理し、保存されたデータ自体は管理しません。この設計により、管理者はイミュータブルストレージの整合性を損なわずに、システムの維持、モニタ、および保護を行うことができます。

ネットワークプロファイルを管理するには、以下のコマンドを使用します。

```
network profile [-h] {create,list,delete} ...
```

Arcserve Cyber Resilient Storage には、以下のネットワークプロファイル管理コマンドが用意されています。

ネットワークプロファイルの作成

`network profile create` コマンドは、アクティブなネットワークにすぐには影響を与えずに、新しいネットワーク設定プロファイルを作成します。

ネットワークプロファイルを作成するには、以下のコマンドを使用します。

```
network profile create [-h] -p PROFILE -d DEVICE [--ipv4 IPV4] [--ipv6 IPV6] [-a ADDRESS] [-g GATEWAY] [--dns [DNS ...]] [--mtu MTU] [--autoconnect] [-r AUTOCONNECT_PRIORITY]
```

このコマンドでは:

- ライブ ネットワーク設定は変更されません。
- プロファイルメタデータを保護された設定ストアに書き込みます。
- 昇格した権限または管理者の役割が必要な場合があります。

シナリオ

デバイス `bar` で `foo` という IPv4 プロファイルを作成し、その IPv4 設定をネットワークから自動的に取得してすぐにアクティブになるように設定します。

```
::> network profile create -p foo -d bar --ipv4 auto --autoconnect true
```

結果

「foo」という新しいプロファイルがデバイス「bar」に対して作成され、作成後すぐにアクティブ化されます。これにより、デバイス「bar」で接続が設定され、ネットワーク内の DHCP から IPv4 設定の詳細が取得されます。

シナリオ

デバイス `bar` で `foo_2` という IPv4 プロファイルを作成し、そのアドレス情報を手動で指定して、すぐにアクティブになるようにします。

```
::> network profile create -p foo_2 -d bar --ipv4 manual -a 192.168.0.100/24 -g 192.168.0.1 --dns 1.1.1.1 --autoconnect true
```

結果

`foo_2` という新しいプロファイルがデバイス `bar` に対して作成されます。これにより、デバイス `bar` で、アドレスとして `192.168.0.100` とネットマスク `255.255.255.0` を使用し、ゲートウェイ `192.168.0.1` を経由してルーティングするように接続が設定されます。すべての FQDN クエリで DNS `1.1.1.1` を使用し、すぐにアクティブになります。「`autoconnect`」が「`true`」に設定されていて、優先度が指定されていないため、デバイス「`bar`」のプロファイル「`foo`」に取って代わり、アクティブなプロファイルになります。

コマンドの構文とパラメータの詳細については、「[コマンド リファレンス ガイド](#)」の「[create](#)」を参照してください。

ネットワークプロファイルの一覧表示

`network profile list` コマンドは、既存のネットワークプロファイルを表示します。
ネットワークプロファイルを一覧表示するには、以下のコマンドを使用します。

```
network profile list [-h] [-d DEVICE] [-v | --verbose | --no-verbose]
```

シナリオ

Arcserve Cyber Resilient Storage デバイスで設定されているすべてのプロファイルを表示します。

```
network profile list
```

結果

```
1 > network profile list
2 PROFILE NAME      DEVICE      ACTIVE      ADDRESSES      GATEWAY      DNS
3 ens192            ens192      True        10.10.10.1/22   10.10.10.1/32  10.10.10.1
4 lo                lo          True        127.0.0.1/8    -            -
5 ens224            -          False       -              -            -
```

シナリオ

特定のデバイスに対して設定されたプロファイルのみを表示します。

```
network profile list -d ens192
```

結果

```
1 > network profile list -d ens192
2 PROFILE NAME      DEVICE      ACTIVE      ADDRESSES      GATEWAY      DNS
3 ens192            ens192      True        10.10.10.1/22   10.10.10.1/32  10.10.10.1
```

シナリオ

特定のデバイスに対して設定されたプロファイルのすべての詳細を表示します。

```
network profile list -d ens192 -v
```

結果

1	> network profile list -d ens192 -v	
2		
3	PROFILE NAME	ens192
4	DEVICE	ens192
5	ACTIVE	True
6	TYPE	802-3-ethernet
7	MAC ADDRESS	00:50:56:A8:61:A4
8	AUTOCONNECT	True
9	AUTOCONNECT PRIORITY	-
10	METHOD	auto
11	IPV4 ADDRESSES	192.168.1.1/22
12	IPV4 DNS	192.168.1.1/32
13	IPV4 GATEWAY	192.168.1.1/32
14	IPV6 ADDRESSES	fe80::1/64
15	IPV6 DNS	-
16	IPV6 GATEWAY	-

コマンドの構文とパラメータの詳細については、「[コマンド リファレンス ガイド](#)」の「[list](#)」を参照してください。

ネットワークプロファイルの変更

`network profile modify` コマンドは、ネットワーク接続を変更します。

ネットワークプロファイルを変更するには、以下のコマンドを使用します。

```
network profile modify [-h] -p PROFILE -d [DEVICE] [--ipv4 IPV4] [--ipv6 IPV6] [-a ADDRESS] [-g GATEWAY] [--dns [DNS ...]] [--mtu MTU] [--autoconnect | --no-autoconnect] [-p AUTOCONNECT_PRIORITY] [--set-active]
```

シナリオ

デバイス *bar* の *foo_2* という IPv4 プロファイルを変更し、その IPv4 設定をネットワークから自動的に取得するように設定し、すぐにアクティブになるよう設定します。

```
::> network profile modify -d foo_2 --ipv4 auto --set-active
```

結果

この結果、デバイス *bar* に対して作成された *foo_2* というプロファイルが変更され、手動設定から切り替わり、DHCP 経由でネットワークから IPv4 ネットワーク設定が取得されます。以前にデバイス *bar* で *foo_2* がアクティブでなかった場合、それがアクティブプロファイルになります。

シナリオ

デバイス *bar* の *foo* というプロファイルを変更し、その IPv6 設定を指定します。

```
::>network profile modify -d foo --ipv6 manual -a 2001:db8::2/64 -g "2001:db8::1" --dns "2001:4860:4860::8888"
```

結果

デバイス *bar* に対して作成されたプロファイル *foo* を更新し、IPv6 ネットワークファミリの設定を手動で適用します。IPv6 については、アドレスに 2001:db8::2、アドレスの範囲として 2001:0db8:0000:0000:0000:0000:0000:0000 ~ 2001:0db8:0000:0000:ffff:ffff:ffff:ffff を使用し、2001:db8::1 のゲートウェイを経由してルーティングします。すべての FQDN クエリに DNS 2001:4860:4860::8888 を使用

します。--set-active パラメータが指定されていないため、デバイス *bar* でアクティブにならず、設定 *foo_2* が引き続きアクティブな設定となります。

コマンドの構文とパラメータの詳細については、「[コマンド リファレンス ガイド](#)」の「[modify](#)」を参照してください。

ネットワークプロファイルの削除

`network profile delete` コマンドは、既存のネットワーク接続プロファイルを削除します。

ネットワークプロファイルを削除するには、以下のコマンドを使用します。

```
network profile delete [-h] profile_name
```

コマンドの構文とパラメータの詳細については、「[コマンド リファレンス ガイド](#)」の「[delete](#)」を参照してください。

ネットワークプロファイルの切り替え

Arcserve Cyber Resilient Storage を使用すると、ユーザは、承認された設定を変更せずに、さまざまな環境でシームレスに運用できます。管理者は、企業の LAN プロファイル、リモート ワークプロファイル、VPN が適用されるパブリック ネットワークプロファイルなど、事前に設定されたネットワークプロファイルを定義およびロックダウンできます。ユーザは必要に応じてこれらのプロファイルを切り替えることができますが、基となる設定を変更することはできません。この手法により、セキュリティポリシーの一貫性を確保し、設定のドリフトを防止し、コンプライアンスを維持しながら、必要な柔軟性も確保できます。

必要に応じて、以下のコマンドを使用して、設定されたネットワークプロファイルをアクティブ化または非アクティブ化できます。

ネットワークプロファイルがアクティブ化されると、以前にアクティブであったネットワークプロファイルがあれば、それが非アクティブ化されます。非アクティブなネットワークプロファイルをアクティブにするには、以下のコマンドを使用します。

```
network profile up [-h] -p PROFILE
```

アクティブなネットワークプロファイルを非アクティブにするには、以下のコマンドを使用します。

```
network profile down [-h] -p PROFILE
```

重要：複数のネットワークプロファイルが自動接続するように設定されている場合（つまり、自動接続設定が *True* に設定されている場合）、デバイスは以下のルールに基づいてプロファイルを選択します。

- 低い値ほど高い優先度を示しているため、自動接続の優先度の値が低いプロファイルが最初に選択されます。
- 複数のプロファイルが同じ優先度の場合、デバイスは最後にアクティブ化されたプロファイルに接続します。

コマンドの構文とパラメータの詳細については、「[コマンド リファレンス ガイド](#)」の「[up](#)」と「[down](#)」を参照してください。

ネットワークボンディング

ネットワークボンディングは、2 つ以上の物理ネットワークインターフェースを 1 つの論理インターフェースに統合するネットワーク機能です。ネットワークボンディングにより、管理者は複数の物理ネットワークインターフェース(NIC) を単一の論理インターフェースに統合できるため、ネットワークの信頼性と可用性が向上します。ネットワークボンディングは Web ベースの管理インターフェースに完全に統合されているため、コマンドラインツールを使用せずに、ボンディングインターフェースを作成、設定、監視、および管理できます。

Arcserve Cyber Resilient Storage は、アクティブ/バックアップ(アクティブ/パッシブ) モードを使用します。このモードでは、1 つの NIC がすべてのトラフィックをアクティブに処理し、障害発生時にはスタンバイ NIC が自動的に引き継ぐため、複雑なスイッチ側の設定を必要とせずに途切れない接続を確保します。

管理者は、メンバ NIC の割り当て、リアルタイムステータスの表示、および実行時と永続的な設定の両方の管理を簡単に行うことができます。ビルトインの役割ベースのアクセス制御(RBAC) により、許可されたユーザのみがネットワークを変更できるようになり、包括的な監査ログによってすべての設定アクティビティを可視化できます。

セットアップと管理を簡素化することで、ネットワークボンディングは運用効率を高め、設定エラーを減らし、システムレジリエンスを強化すると共に、Arcserve Cyber Resilient Storage システム全体で一貫性のある最新の管理エクスペリエンスを提供します。

ネットワーク ボンディングの作成

このセクションでは、ネットワーク ボンディングを作成するための前提条件と、ボンディングの作成に必要な手順について説明します。ボンディング デバイスを作成する前に、プロファイルがどのように管理されるか、および正常に作成するために満たす必要がある条件を理解することが重要です。

前提条件

- ボンディング デバイスが動作するにはプロファイルが必要ですが、個々のメンバ デバイスには、ボンディングの作成時にアクティブ プロファイルが割り当てられていない必要があります。デバイスにすでにアクティブなプロファイルがある場合、システムはボンディング デバイスの作成を禁止し、エラーを表示します。この問題を回避するには、開始する前に、デバイスの既存のプロファイルがすべて削除または停止されていることを確認します。アクティブなプロファイルがなくなったデバイスは、ボンディング メンバとして追加できるようになります。
- ボンディング デバイスには、少なくとも 2 つのメンバ デバイスが含まれている必要があります。これらのデバイスは、ボンディング設定の一部として連動し、ボンディングが正しく機能するために必要です。

以下の手順に従います。

1. コマンド プロンプトで以下のコマンドを入力して、**Enter** キーを押します。

```
network bond create [-h] -b BOND -m MEMBERS [MEMBERS ...]
```

各項目の説明

-b、--bond

ボンディングの名前。

-m、--members

ボンディング内のメンバ デバイス。メンバ名をスペースで区切って入力します。ネットワーク ボンディングには少なくとも 2 つのメンバが必要です。

```
> network bond create -b foo -m ens36 ens37
Success
```

システムは、ボンディング デバイスと、そのボンディングに属するメンバの接続プロファイルを自動的に作成します。

2. ボンディングが作成されたことを確認します。これを行うには、コマンド プロンプトで以下のコマンドを入力し、Enter キーを押します。

```
network profile list
```

このコマンドは、すべてのプロファイルを一覧表示します。ネットワーク ボンディングにメンバ デバイスがある場合、それらはネットワーク ボンディングの下に表示されます。メンバの横のアスタリスクは、そのメンバがすべてのトラフィックを処理するアクティブ デバイスであることを示します。アクティブ デバイ스에 障害が発生すると、スタンバイ デバイスが自動的に処理を引き継ぎます。

```
> network profile list
PROFILE NAME      DEVICE  ACTIVE  METHOD  ADDRESSES  GATEWAY
foo
├─ foo-member1 *  ens36   True    -        -          -
└─ foo-member2    ens37   True    -        -          -
ens33             ens33   True    auto    [redacted] [redacted]
ens34             ens34   True    auto    [redacted] [redacted]
```

3. ネットワーク ボンディングの作成後、ネットワーク内のデバイスのステータスを確認するには、コマンド プロンプトで以下のコマンドを入力し、Enter キーを押します。

```
network device list
```

デバイスのリストが表示されます。

```
> network device list
DEVICE  TYPE      BOND  STATE      PROFILE
ens33   ethernet -      connected  ens33
ens34   ethernet -      connected  ens34
ens36   ethernet foo     connected  foo-member1
ens37   ethernet foo     connected  foo-member2
ens38   ethernet -      disconnected
foo     bond     -      connected  foo
```

ネットワークボンディングの作成に使用された2つのデバイスが、作成したボンディングの下に表示され、ボンディングへの所属は `[PROFILE]` 列にリストされています。

ネットワークボンディングの変更

既存のネットワークボンディングのメンバを追加または削除できます。

ネットワークボンディングを変更するには、以下のコマンドを使用します。

```
network bond modify [-h] -b BOND_DEVICE [-a ADD_MEMBERS [ADD_MEMBERS ...]] ...]]  
[-r REMOVE_MEMBERS [REMOVE_MEMBERS ...]]
```

各項目の説明

-b, --bond

変更するボンディング デバイスの名前。

-a, --add_members

デバイスをボンディングメンバとして追加します。

-r, --remove_members

ネットワークボンディングから削除するメンバデバイス。

ネットワーク ボンディングの削除

ネットワーク ボンディングを削除するには、以下のコマンドを使用します。

```
network bond delete [-h] -b BOND
```

各項目の説明

-b、*--bond*

削除するボンディングの名前。

第12章: アラート管理

「アラート管理」では、Arcserve Cyber Resilient Storage がシステム イベントをモニタし、注意が必要な可能性がある重要な状況を管理者に通知する方法について説明します。適時の正確なアラートは、特にデータの整合性とコンプライアンスが重要な環境で、デバイスの健全性、セキュリティ、およびパフォーマンスを維持するために不可欠です。このセクションでは、システムで生成されるアラートの種類を説明し、アラートの解釈と適切な対応についてのガイダンスを提供します。

具体的には、このセクションでは以下のトピックについて説明します。

ストレージ アラート

このセクションでは、ストレージ アラートの概要について説明します。

ストレージ アラートを設定することは、Arcserve Cyber Resilient Storage のパフォーマンスを最適に保つために重要です。アラートを使用すると、容量の使用率を継続的に監視できるため、サービスを中断させる可能性のある予期しないストレージ容量の枯渇を防ぐことができます。

データの増加、アクセス率、エラー ログを追跡することで、アラートはランサムウェアのアクティビティやシステム障害などの潜在的な脅威を示している可能性がある異常なパターンを検出できます。Arcserve Cyber Resilient Storage では WORM (write-once-read-many) ポリシーを適用してデータの変更や削除を防止しているため、アラートはアクセシビリティを損なわずにこれらのポリシーを正しく適用するのにも役立ちます。

さらに、アラートは使用状況の傾向に関する情報をリアルタイムで提供することで、効果的な容量計画をサポートします。これにより、適切なタイミングで拡張やアーカイブを判断できます。最終的に、アラートはデータの整合性を保護し、一貫したパフォーマンスを確保し、規制への準拠をサポートする早期警告システムとして機能します。

アラートは、以下の問題が発生した場合にトリガされます。

- **storage-degraded:** これは、Arcserve Cyber Resilient Storage が最適な状態で機能しなくなったが、引き続き動作していることを示します。通常は、1 つ以上のコンポーネント (ディスクなど) に障害が発生したか、正常に機能していないことを意味し、冗長性が損なわれたり、パフォーマンスが低下したりします。
- **storage-error:** これは、Arcserve Cyber Resilient Storage システムで重大な障害または回復不可能なエラーが発生し、データの可用性または整合性に影響を与えた可能性があることを示します。
- **storage-state-changed:** ストレージシステムのステータスまたは設定が変更されたことを示します。この変更自体が問題となる場合もあれば、問題とならない場合もあります。
- **storage-threshold:** これは、使用済みストレージ容量が事前定義されたしきい値に達したか、超過したことを示します。これにより、プールに新しいデータを保存できる容量が減少しています。ストレージ使用量がプール容量の 80% を超えるとアラートがトリガされ、75% 未満になるとクリアされます。
- **system-clock:** これは、システムクロックまたは時間同期に問題または不一致があることを示します。この問題は、ストレージシステムや分散環境に影響を与える可能性があります。

- **disks-smart-status:** これは、Arcserve Cyber Resilient Storage システム内の 1 つ以上のディスクが、オンボード S.M.A.R.T. モニタリングを通じて問題を報告したことを示します。これらの警告は、ディスク障害の可能性を示しています。データへのリスクを回避するには、これらの問題をできるだけ早く調査して対処してください。

SMART ディスクアラート

Arcserve Cyber Resilient Storage では、SMART (Self-Monitoring, Analysis, and Reporting Technology) ディスクテレメトリを使用して、システムの物理ストレージメディアの健全性と信頼性を管理者が常に把握できるようにします。Arcserve Cyber Resilient Storage はイミュータブルストレージプラットフォームであるため、耐久性があり、検証可能で、変更されていない状態のデータを確実に維持するために、長期間のディスクの安定性に依存します。

```
> disk list
NAME          USE          SIZE          VENDOR          MODEL
sda           OS           60.0G         VMware          Virtual disk
sdb           Available    128.0G         VMware          Virtual disk
sdc           Available    128.0G         VMware          Virtual disk
sdd           Available    128.0G         VMware          Virtual disk
sde           Available    128.0G         VMware          Virtual disk
sdf           Available    128.0G         VMware          Virtual disk
sdg           Available    128.0G         VMware          Virtual disk
sdh           Available    128.0G         VMware          Virtual disk
sdi           Available    128.0G         VMware          Virtual disk
sr0           CRS          2.8G          NECVMWar        VMware Virtual SATA CDRW Drive
>
exit to quit session
```

SMART は、ディスクの種類とストレージの技術に応じて、以下のようなさまざまな重要な属性をモニタします。

- 読み取り/書き込みエラー率
- 再割り当てされたセクタまたは不安定なセクタ
- I/O の信頼性 インジケータ
- 機械的な消耗 (HDD)
- フラッシュの耐久性 (SSD)
- 温度または電力の異常

以下の表に、さまざまなディスクの種類で一般的にモニタされる SMART 属性の比較を示します。

SMART 属性	S(ATA)	NVME	SCSI
READ_ERROR_RATE	○	--	--
REALLOC_SECTOR_COUNT	○	--	--
TEMPERATURE	○	○	○
POWER_ON_HOURS	○	○	○
POWER_CYCLES	○	○	--
UNSAFE_SHUTDOWNS	○	--	--
SEEK_ERROR_RATE	--	--	--

COMMAND_TIMEOUT_COUNT	--	--	--
CRC_ERROR_COUNT	--	--	--
MEDIA_ERRORS	--	○	○
AVAILABLE_SPARE	--	○	--

これらの属性が定義されたしきい値を超えるか、異常な傾向を示した場合、Arcserve Cyber Resilient Storage はアラートを生成します。これらのアラートは、管理者がハードウェアの劣化の初期兆候を特定し、障害のリスクのあるディスクを検出し、可用性や耐久性に影響が及ぶ前にプロアクティブなメンテナンスをスケジュールするのに役立ちます。

アラートの電子メールの設定

このセクションでは、アラートを受信するための電子メールアドレスの設定方法について説明します。

以下の手順に従います。:

1. Arcserve Cyber Resilient Storage にログインします。
2. コマンド プロンプトで以下のコマンドを入力して、**Enter** キーを押します。

```
email configure [-h] -H HOST [-P PORT] [-u USERNAME] [-n SENDER_
ADDRESS] [-s] [-t] [-x SUBJECT_PREFIX]
```

各項目の説明

-H、--host

SMTP サーバホスト名

-P、--port

SMTP サーバポート(デフォルト: *-ssl* または *-starttls* に基づいて
25、465、または 587)

-u、--username

SMTP サーバユーザ名

-n、--sender-address

送信者の電子メールアドレス(デフォルト: username)

-s、--ssl

初期接続を暗号化する

デフォルト: False

-t、--starttls

STARTTLS で接続をアップグレードする(*-ssl* が設定されている場合
は無視される)

デフォルト: False

-x、--subject-prefix

電子メールの件名行に追加するプレフィックス

プロンプトが表示されたら、SMTP サーバのパスワードを入力し、**Enter**
キーを押します。

```
Arcserve Cyber Resilient Storage Server version 6.5.1007

Type help for a list of available commands.

> email configure -H smtp.office365.com -P 587 -u Administrator@arcserve.com -t
Enter SMTP server password:
Success
>
```

指定した電子メールアドレスは、電子メールアラートを受信するように設定されています。

電子メールの設定が機能するかどうかをテストするには、以下のコマンドを使用して受信者にテスト電子メールを送信します。

```
email test [-h] -r RECIPIENT_ADDRESS
```

各項目の説明

`-r, --recipient_address`

受信者の電子メールアドレス

電子メール関連のコマンドの詳細については、「[コマンド リファレンスガイド](#)」の「[Email](#)」を参照してください。

アラートの設定

このセクションでは、アラートを受信するための電子メールアドレスの設定方法について説明します。

以下の手順に従います。:

1. コマンド プロンプトで以下のコマンドを入力して、Enter キーを押します。

```
alert create [-h] -t TYPE -r RECIPIENTS [RECIPIENTS ...]
```

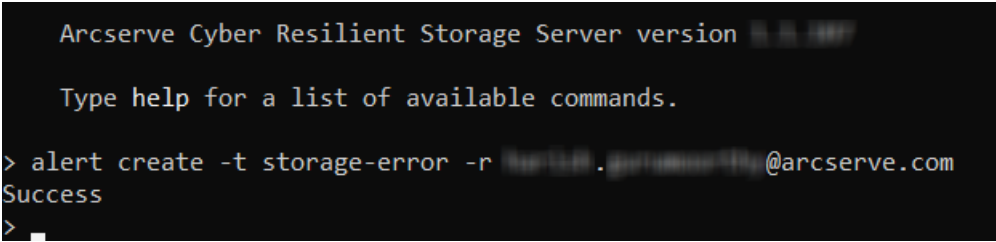
各項目の説明

-t、--type

アラートを作成する種類を指定します。詳細については、「[ストレージ アラート](#)」と「[SMART ディスク アラート](#)」を参照してください。

-r、--recipients

アラートの受信者のリスト。



```
Arcserve Cyber Resilient Storage Server version 9.5.1007

Type help for a list of available commands.

> alert create -t storage-error -r test.recipients@arcserve.com
Success
>
```

指定したアラートの種類が作成され、トリガされるたびに受信者に電子メールで通知されます。

alert コマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[Alert](#)」を参照してください。

第13章: ユーザ管理

Arcserve Cyber Resilient Storage には、サーバ環境を管理するための2つのユーザー役割があります。これらの役割を以下に示します。

- **admin:** 設定の構成やデータ保護機能の管理など、操作タスクおよび管理タスクへのフルアクセス権があります。ただし、admin ユーザーはユーザーアカウントを作成または管理できません。
- **super admin:** すべての管理者権限を含む完全なシステム権限があります。さらに、super admin はユーザーアカウントを作成、変更、および削除できます。

このセクションには、以下のトピックが含まれます。

ユーザーの作成	91
ユーザーの更新	93

ユーザの作成

このセクションでは、新しいユーザを作成し、権限を割り当てる方法について説明します。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. コマンド プロンプトで、以下のコマンドを入力します。

```
user list
```

既存のユーザのリストが表示されます。

3. 次に、以下のコマンドを入力して、Enter キーを押します。

```
user create [-h] -u USERNAME [-r {admin,super_admin}]
```

各項目の説明

-u、--username

新しいアカウントのユーザ名。

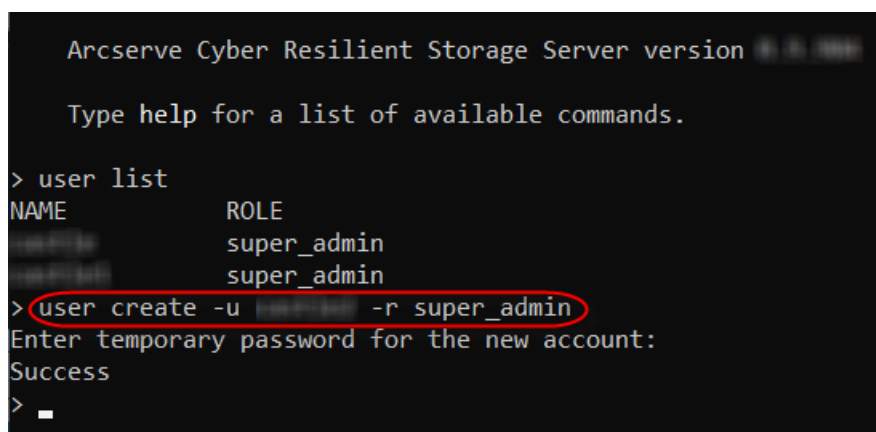
-r、--role

新しいアカウントの役割。可能な選択：admin、super_admin。

デフォルト：'admin'

ユーザの役割とその機能の詳細については、「[ユーザ管理](#)」を参照してください。

4. プロンプトが表示されたら、新しいユーザのパスワードを入力し、Enter キーを押します。



```
Arcserve Cyber Resilient Storage Server version 4.1.0.0
Type help for a list of available commands.

> user list
NAME                ROLE
super_admin         super_admin
super_admin         super_admin
> user create -u super_admin -r super_admin
Enter temporary password for the new account:
Success
>
```

新しいユーザが作成されます。

注：以下のコマンドは、ユーザを削除します。

```
user delete [-h] -u USERNAME
```

ユーザ関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[user](#)」を参照してください。

ユーザの更新

このセクションでは、ユーザを更新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 Cyber Resilient Storage にログインします。
2. コマンド プロンプトで、以下のコマンドを入力します。

```
user list
```

既存のユーザのリストが表示されます。

3. 以下のコマンドを入力して、**Enter** キーを押します。

```
user update [-h] -u USERNAME [-r {admin,super_admin}]
```

各項目の説明

-u、--username

変更するアカウントのユーザ名。

-r、--role

アカウントに設定する新しい役割。可能な選択：admin、super_admin

ユーザが更新されます。

```
Arcserve Cyber Resilient Storage Server version 6.6.0000
Type help for a list of available commands.

> user list
NAME          ROLE
-----
castle2       super_admin
> user update -u castle2 -r admin
Success
> user list
NAME          ROLE
-----
castle2       admin
>
```

ユーザ関連のコマンドの詳細については、「[コマンド リファレンス ガイド](#)」の「[user](#)」を参照してください。

第14章: サポートとの連携

このセクションでは、Arcserve サポートと連携してシステムのトラブルシューティングを行う方法について説明します。サポート チームと連携して問題を迅速に特定して解決することで、システムを復旧し、ダウンタイムを最小限に抑えることができます。

具体的に、このセクションには、以下のトピックが含まれます。

サポート バンドルの生成	95
------------------------------------	----

サポート バンドルの生成

問題のトラブルシューティング時に、サポート担当者がサポート バンドルを要求する場合があります。サポート バンドルには、問題を効率的に特定して解決するために役立つ診断データが含まれています。Arcserve Cyber Resilient Storage では、展開環境と接続オプションに応じて、このバンドルを生成する方法が2つあります。

- **バンドルを直接作成およびアップロードする:** Arcserve Cyber Resilient Storage がインターネット 接続を通じて外部ネットワークに接続されている環境では、サポート バンドルを生成し、サポート担当者がアクセスできる安全な場所に自動的にアップロードするコマンドを実行できます。
- **バンドルを USB ドライブに書き込む:** 外部接続が許可されていない非接続展開の場合、Arcserve Cyber Resilient Storage ではサポート バンドルをローカルで生成して USB ドライブに保存できます。その後、オフライン分析のためにサポート担当者にバンドルを安全に渡すことができます。

サポート バンドルのアップロード

このセクションでは、サポート バンドルを作成およびアップロードする方法について説明します。

サポート バンドルを生成すると、ログ、設定の詳細、その他の診断情報を安全に共有できるため、Arcserve サポート チームが問題を特定してすばやく解決するために役立ちます。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. コマンド プロンプトで以下のコマンドを入力して、**Enter** キーを押します。

```
support upload-bundle [-h] [-t TAG]
```

各項目の説明

-t、--tag

サポート バンドルを簡単に識別するためのオプションのタグ。このタグは1つの文字列である必要があります。

注：デフォルトでは、バンドル名の先頭にタグが付き、その後にマシン名とサポート バンドルが生成された時間が続きます。タグを使用すると、バンドルを簡単に識別できます。

```
> support -h
usage: support [-h] {enable,upload-bundle} ...

Support management commands.

positional arguments:
  {enable,upload-bundle}
                        Support sub-commands
  enable                Enable remote access to this server for Arcserve support
  upload-bundle         Upload a support bundle for diagnosis.

options:
  -h, --help            show this help message and exit
> support upload-bundle -t 07022025_0702140203UTC_rrs
Uploaded support bundle 07022025_0702140203UTC_rrs.zip
>
```

サポート バンドルが作成され、リレー サーバにアップロードされます。Arcserve サポートはそこからバンドルにアクセスして読み取り、問題を診断して解決策を提供します。

この例では、ポート番号は 45159 で、パスワードは *film-cause-decay-batch* です。

サポート ユーザが接続されると、シェルに以下のメッセージが表示されます。

「リモート サポート へのアクセスが開始されました。いつでも *Ctrl + C* キーを使用すると停止できます。」

注：サポート アクセスを無効にした後、以下のコマンドを使用して、アプライアンスがロックされ、外部ユーザへのアクセスが制限されていることを確認します。

```
support enable [-h] [-r RELAY] [-p PORT]
```

USB ドライブへのサポート バンドルの書き込み

非接続環境に展開する場合、Arcserve Cyber Resilient Storage は、セキュリティおよびコンプライアンスの要件を満たすために外部ネットワーク接続なしで動作します。アウトバウンド通信が完全に制限されているため、ユーザは標準の方法を使用して診断データやシステムログをサポート チームに送信できません。

この制限に対処するため、Arcserve Cyber Resilient Storage ではサポート バンドルを USB ドライブに直接書き込む機能が提供されています。これにより、ユーザは必要なシステム ログおよび診断情報を非接続環境から抽出できます。これにより、サポート 担当者はオフラインでデータにアクセスし、問題のトラブルシューティングや分析を実施し、非接続展開の整合性を損なうことなくシステム機能のリストアを支援できます。

このセクションでは、サポート バンドルを USB ドライブに書き込む方法について説明します。

重要:

- 開始する前に、USB ドライブが Arcserve Cyber Resilient Storage システムに接続され、利用可能であることを確認してください。
- 使用する USB ドライブに 16 GB 以上の空き容量があることを確認します。

以下の手順に従います。

1. Arcserve Cyber Resilient Storage にログインします。
2. USB ドライブを接続したら、利用可能であることを確認するため、以下のコマンドを入力して **Enter** キーを押します。

disk list

```
> disk list
NAME      USE      SIZE      VENDOR
sda       OS       113.0G    ATA
sdb       USB      29.2G     SanDisk
```

これは、USB ドライブが正しく装着され、利用可能であることを確認して、サポート バンドルをコピーできるようにするためです。

3. コマンド プロンプトで以下のコマンドを入力して、**Enter** キーを押します。

```
support upload-bundle --offline [-h] [-t TAG]
```

各項目の説明

-o、--offline

-t、--tag

注：デフォルトでは、タグを指定した場合、バンドル名の先頭にタグが付き、その後マシン名、ドメイン名、およびサポート バンドルが生成された日時が続きます。

```
Arcserve Cyber Resilient Storage Server
Version: 1.6.1504

localhost login: castle
Password:
Last login: Thu Feb 19 18:17:52 on tty1
```



```
Arcserve Cyber Resilient Storage Server version 1.6.1504

Type help for a list of available commands.
```

```
> support upload-bundle --offline -t [redacted]
WARNING: The USB drive will be formatted to save the support bundle, and ALL existing data on the drive will be permanently lo
y
Saved support bundle [redacted]_l[redacted].st.[redacted]n_2026_02_23_17_08_56_UTC_rrs.zip
> _
```

The USB drive will be formatted to save the support bundle, and ALL existing data on the drive will be permanently lost. (USBドライブはサポート バンドルを保存するためにフォーマットされ、ドライブにあるすべての既存データを回復することはできません。) Do you want to proceed? (続行しますか?)

- サポート バンドルが正 常にコピーされると、CLI にファイルが保 存されたことを示すメッセージが表 示されます。

第15章: OneXafe からのデータストアの移行

このセクションでは、OneXafe から Arcserve Cyber Resilient Storage にデータを移行するための基本的な手順と考慮事項について説明します。移行プロセスには、OneXafe ストレージから Arcserve Cyber Resilient Storage へのデータストアのレプリケーションが含まれます。

OneXafe からのデータ移行は、UDP コンソールから開始します。OneXafe システム (移行元) と Arcserve Cyber Resilient Storage (移行先) が異なるネットワークにある場合は、両方のシステムがインターネットに接続されていて、UDP コンソールからアクセスできることを確認してください。両方のシステムが同じネットワークにある場合は、インターネット接続は必要ありませんが、UDP コンソールからアクセスできる必要があります。

データの整合性、セキュリティ、正確性、およびシステムの継続性を維持するには、慎重な計画と検証を行って移行を実行することが不可欠です。移行を適切に実行することで、データの損失、破損、ダウンタイムを防ぐことができます。

移行の前後の注意点を以下に示します。

- 現在のデータのサイズ、構造、およびパフォーマンスを把握してください。移行に影響する可能性のある依存関係と制約を特定してください。
- 移行後に検証チェックを実行して、すべてのファイルが存在し、アクセス可能で、期待どおりに機能していることを確認してください。通常、これらのチェックには、レコード数/ファイル数のチェック、チェックサム/ハッシュの検証、データサンプリング/スポット チェックなど、一般的な検証方法が含まれます。
- 業務が中断しないように移行をスケジュールしてください。
- 大規模な転送の場合は、ネットワークへの影響を軽減するために、オフピーク時に移行することを検討してください。

移行プロセスの詳細については、「[同じ UDP コンソールで管理されているデータストア間でデータをレプリケートする方法](#)」を参照してください。

第16章: 一般的なエラーと問題

この章では、Arcserve Cyber Resilient Storage の展開または管理時に発生する一般的なエラーと問題について説明します。具体的には、以下のトピックについて説明します。

「利用可能なディスクが見つかりません」というエラーでストレージの作成に失敗する	103
制約のないシェルにアクセスできません	104
単一のディスクで作成されたプールにディスクを追加できない	105
再起動時のデバイス名の変更	106
データストアサイズの違い	107
シェルと UDP コンソールでの表記の違い	108
ファイルシステム空き容量が正しくない	109
間違ったキーを入力しても検証メッセージが表示されない	110
Admin/Superuser アカウントのパスワードをリセットできない	111
Arcserve Cyber Resilient Storage のリビルド	112
UDP のリビルド	113
logs コマンドが実行されている限り、ターミナルはタイムアウトしません	114

「利用可能なディスクが見つかりません」というエラーでストレージの作成に失敗する

現象

新規の Arcserve Cyber Resilient Storage 展開で、初期設定中にストレージプールの作成が「利用可能なディスクが見つかりません」というメッセージで失敗し、`disk list` コマンドを実行すると、「`libzfs` ライブラリの初期化に失敗しました。」と表示されます。「カーネルモジュールのロードに失敗しました。」エラーも表示されます。

解決策

この問題は、システムでセキュアブートが有効になっているが、セットアップ時にマシン所有者キー (MOK) の登録が完了していない場合に発生します。セキュアブートが有効になっている場合、Arcserve Cyber Resilient Storage によって使用される ZFS カーネルモジュールは信頼され、適切に署名されている必要があります。MOK 登録手順をスキップすると、必要なカーネルモジュールをロードできず、`libzfs` 初期化エラーが発生します。その結果、Arcserve Cyber Resilient Storage は利用可能なディスクを検出できず、ストレージプールも作成できません。このシナリオでは、システムに次のエラーメッセージも表示される場合があります:「カーネルモジュールのロードを開始できませんでした。」。

この問題を修正するには、[MOK キーを登録](#)します。

詳細については、「[セキュアブートの有効化](#)」を参照してください。

制約のないシェルにアクセスできません

現象

管理者またはスーパー管理者ユーザとしても、bash などの制約のないシェルにアクセスできません。これらの両方のアカウントには、システムの管理およびトラブルシューティングに使用できるコマンドが制限されています。

解決策

Arcserve Cyber Resilient Storage のシェルで使用可能なコマンドのみを使用できます。これらの制限は、システムの整合性とセキュリティを維持するために適用されます。シェルの対象外のコマンドについては、[Arcserve サポート](#)にお問い合わせください。

単一のディスクで作成されたプールにディスクを追加できない

現象

デフォルト プールを削除した後、新しいプールを作成し、ディスクを 1 つ追加しました。別のディスクを追加しようとすると、ユーザに以下のエラーが表示されます。

「ディスクの追加に失敗しました。エラー: 単一のディスクで作成されたプールにディスクを追加できません。」

解決策

Arcserve Cyber Resilient Storage は、単一ディスク(初期)プールへのディスクの追加はサポートしていません。

再起動時のデバイス名の変更

現象

デバイス名、特に OS ドライブのパーティション名は、再起動のたび変更されます。

解決策

デバイス番号はブート プロセス中に動的に割り当てられ、デバイスが検出される順序は異なる場合があります。Arcserve Cyber Resilient Storage はデバイス GUID に依存しています。

データストアサイズの違い

現象

同じデータストアがUDP コンソールと Arcserve Cyber Resilient Storage で異なるサイズが表示されます。

解決策

Arcserve Cyber Resilient Storage v1.0 の場合、すべてのストレージレポートはシェルからのみ行われます。

シェルとUDP コンソールでの表記の違い

現象

UDP コンソールとシェルでアクセス キーの表記が異なります。

解決策

UDP コンソールと Arcserve Cyber Resilient Storage シェルでは、アクセス キーの用語が異なります。

ファイルシステム空き容量が正しくない

現象

より大きな容量のディスクをプールに追加しても、空き容量コマンドでは、そのディスクの追加容量が反映されず、誤った情報が表示されます。

解決策

新しいディスクの容量が既存のディスクよりも小さい場合、システムはエラーをスローします。ディスク容量がプール内の他のディスクの容量よりも大きい場合は、既存のディスクのサイズのみが使用されます。これは、RAID アレイの正常な動作です。

間違ったキーを入力しても検証メッセージが表示されない

現象

UDP に Arcserve Cyber Resilient Storage アカウントを追加するときに、間違ったキーを入力しても検証メッセージが表示されません。システムは、キーの有効性に関係なく設定を受け入れて保存します。

解決策

これは既知の制限で、現在のところ回避策はありません。

Admin/Superuser アカウントのパスワードをリセットできない

現象

管理者/スーパー管理者ユーザがログインパスワードを忘れた場合、そのアカウントのパスワードを自分でリセットすることはできません。

解決策

スーパー管理者ユーザがパスワードを忘れた場合、再インストールする必要があります。

管理者ユーザがパスワードを忘れた場合、スーパーユーザがパスワードをリセットできます。

Arcserve Cyber Resilient Storage のリビルド

インストールが動作しなくなった場合、または OS ディスクのハードウェア障害またはその他のオペレーティングシステムの問題が原因で起動できない場合、データストアディスクが分離されている場合は、いつでも修復インストールを実行して Arcserve Cyber Resilient Storage ボックスをリビルドできます。

詳細については、「[インストール環境の復旧](#)」を参照してください。

UDP のリビルド

UDP RPS サーバがクラッシュしても Arcserve Cyber Resilient Storage が破損していない場合は、データストアのインポート オプションを使用してデータストアを再作成できます。UDP をリビルドするには、以下の手順に従います。

- UDP を再インストールする
- 新しいアクセス キー ID/シークレット キーの組み合わせを作成する
- UDP サーバで新しい認証プロファイルを作成する
- 新しい認証プロファイルを使用して、既存のプール、ファイルシステム、およびポートを指定して、データストアをインポートする

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

logs コマンドが実行されている限り、ターミナルはタイムアウトしません

現象

logs コマンドが実行されている限り、ターミナルはタイムアウトしません。

解決策

これは Arcserve Cyber Resilient Storage v1.0 の正常な動作です。

第17章: 付録

このセクションには、以下のトピックが含まれます。

コマンド リファレンス	116
-----------------------------------	-----

コマンド リファレンス

Arcserve Cyber Resilient Storage ドキュメントには、コマンド リファレンス ガイドも含まれています。このガイドには、使用可能なシェルコマンドのリスト、構文、説明が記載されています。詳細については、「[コマンド リファレンス ガイド](#)」を参照してください。