



ztC Edge ユーザ ガイド



For an **Always-On** World

www.stratus.com

通知

このドキュメントに記載の情報は通知なしに変更される可能性があります。

Stratus は、許可を受けた Stratus Technologies 担当者が署名した書面による合意で明示的に記述されている場合を除き、本書に記載の情報についてその市販性および特定目的への適合性を含むいかなる種類の保証または明言も行いません。

Stratus Technologies は、本書に含まれるすべての誤り、および本書の提供、パフォーマンス、または使用に関連するいかなる種類の責任あるいは義務を負いません。Stratus のマニュアルで説明されているソフトウェアは、(a) Stratus Technologies Ireland, Ltd. またはサードパーティの所有物であり、(b) ライセンスの元に提供され、(c) ライセンスの条項により明示的に許可されている方法でのみ複製または使用できるものとします。

Stratus マニュアルにはユーザ インタフェースおよび Stratus が開発したアプリケーション プログラミング インタフェース (API) でサポートされるすべての機能が説明されています。これらのインタフェースの機能のうち記載されていないものは、Stratus 従業員が使用する目的で提供されており、通知なしに変更される可能性があります。

このマニュアルは著作権で保護されています。All rights are reserved. Stratus Technologies は、使用者がすべての著作権通知、その他の記載制限事項、およびコピーされた文書に含まれる通知を保持することを条件として、本書 (またはその一部) を内部使用の目的のみでダウンロードし、変更を加えずに適度な数のコピーを作成する制限付きの許可をユーザに付与します。

著作権

Stratus、Stratus ロゴ、および Stratus Cloud は Stratus Technologies Ireland, Ltd. の登録商標です。Stratus Technologies ロゴ、Stratus 24 x 7 ロゴ、および ztC は Stratus Technologies Ireland, Ltd. の商標です。

UNIX は米国およびその他の国における The Open Group の登録商標です。

Intel および Intel Inside ロゴは米国その他の国や地域における Intel Corporation またはその関連会社の登録商標です。Xeon は米国その他の国や地域における Intel Corporation またはその関連会社の商標です。

Microsoft、Windows、Windows Server、および Hyper-V は、米国その他の国や地域における Microsoft Corporation の登録商標または商標です。

VMware、vSphere、および ESXi は米国およびその他の地域における VMware, Inc. の登録商標または商標です。

登録商標の Linux は、そのワールドワイドの所有者 Linus Torvalds の独占ライセンスである Linux Mark Institute からのサブライセンスに従い使用されています。

Google および Google ロゴは Google Inc. の登録商標で、許可を得て使用されています。Chrome ブラウザは Google Inc. の商標で、許可を得て使用されています。

Mozilla および Firefox は Mozilla Foundation の登録商標です。

Red Hat は米国およびその他の国における Red Hat, Inc. の登録商標です。

Debian は Software in the Public Interest, Inc. の登録商標で、Debian プロジェクトによって管理されています。

その他すべての商標および登録商標は、それぞれの所有者に帰属します。

マニュアル名称: ztC Edge ユーザガイド

製品リリース番号: Stratus Redundant Linux リリース 2.3.0.0

発行日: 2021年9月10日

Stratus Technologies, Inc.

5 Mill and Main Place, Suite 500

Maynard, Massachusetts 01754-2660

©2021 Stratus Technologies Ireland, Ltd. All rights reserved.

目次

第 1 部: ztC Edge ユーザ ガイド	1
第 1 章: ztC Edge システムの概要	1
ztC Edge システムの概要	1
ztC Edge システムの説明	2
物理マシンと仮想マシン	3
管理操作	3
アラート	4
リモート サポート	4
Lights-Out Management (LOM)	5
サードパーティ製の管理ツール	5
運用モード	6
高可用性運用	6
フォールト トレラント運用	7
ALSR 構成	8
ALSR とクォーラム サービス	8
クォーラム サーバ	9
ネットワーク アーキテクチャ	10
A-Link ネットワークとプライベート ネットワーク	10
ビジネス ネットワークと管理ネットワーク	11
ネットワーク セグメンテーション違反の検知と修復	12
システム使用の制限事項	12
QEMU	13
ホスト オペレーティング システムにアクセスする	13
第 2 章: 作業の開始	15
計画	16
安全上の注意事項	16
システム要件の概要	17
システム ハードウェア	17
IP アドレス	20
ポート	20
設置スペースに関する推奨事項	20
システム仕様	21
システム仕様: ztC Edge 250i システム	21

システム仕様: ztC Edge 200i システム	23
システム仕様: ztC Edge 110i システム	24
システム仕様: ztC Edge 100i システム	26
DIN レール マウントおよび壁かけブラケットの組み立て	28
DIN レール マウントおよび壁かけブラケットの組み立て: ztC Edge 110i システム	28
DIN レール マウントおよび壁かけブラケットの組み立て: ztC Edge 100i システム	30
製品コンプライアンス	31
全般的なネットワーク要件と構成	32
ビジネス ネットワークと管理ネットワークの要件	32
A-Link ネットワークとプライベート ネットワークの要件	34
ztC Edge コンソールの要件	35
対応しているインターネット ブラウザ	35
電源の要件と考慮事項	35
展開	35
電源を接続する	36
UPS (オプション)	36
システムを展開する	38
イーサネット ケーブルを接続する	40
キーボードをマッピングする	42
展開後にキーボード レイアウトを構成するには	43
管理 IP アドレスを記録する	43
展開後のタスク	43
システム IP 情報を取得する	44
ztC Edge コンソールに初めてログオンする	45
システムを登録して恒久ライセンスを入手する	47
ztC Edge システムを再展開する	52
単一ノード システムにノードを追加する	54
2 番目のビジネス ネットワークを接続する	56
第 3 章: ztC Edge コンソールを使用する	59
ztC Edge コンソール	60
ztC Edge コンソールにログオンする	61
ユーザ情報を編集する	63
[ダッシュボード] ページ	64
ダッシュボードで未対応のアラートを解決する	65
[システム] ページ	65

システムの電源をオンにする	66
システムをリブートする	67
システムをシャットダウンする	68
[基本設定] ページ	69
所有者情報を指定する	73
製品ライセンスを管理する	73
ソフトウェア更新を管理する	77
IP 設定を構成する	79
可用性の設定を構成する	81
クォーラム サーバを構成する	82
日付と時刻を構成する	84
メール サーバを構成する	85
ユーザとグループを構成する	86
ローカル ユーザ アカウントを管理する	88
ドメイン ユーザ アカウントを管理する	90
Active Directory を構成する	92
セキュアな接続を構成する	93
VM デバイスを構成する	97
iptables を管理する	98
ログイン バナーを構成する	104
ztC Advisor を有効化する	104
システム基本設定を保存または復元する	105
e アラートを構成する	117
SNMP 設定を構成する	118
OPC 設定を構成する	124
OPC 出力を表示する	126
リモート サポート設定を構成する	135
インターネットプロキシ設定を構成する	138
[アラート履歴] ページ	138
[監査ログ] ページ	139
[サポート ログ] ページ	140
診断ファイルを作成する	140
診断ファイルをカスタマ サポートにアップロードする	141
診断ファイルを削除する	142
[物理マシン] ページ	143

物理マシンのアクション	144
物理マシンの状態とアクティビティ	145
[仮想マシン] ページ	146
仮想マシンのアクション	148
仮想マシンの状態とアクティビティ	151
[ボリューム] ページ	152
[ネットワーク] ページ	154
MTU を設定する	155
[仮想 CD] ページ	156
[アップグレードキット] ページ	157
システム ソフトウェアの USB メディアを作成する	158
第 4 章: Stratus Redundant Linux ソフトウェアをアップグレードする	161
アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレー ドする	161
第 5 章: 物理マシンを管理する	167
メンテナンス モード	168
物理マシンの電源をオンにする	169
物理マシンを識別する	170
物理マシンをリブートする	170
物理マシンをシャットダウンする	171
負荷分散	173
運用モード	174
物理マシンのトラブルシューティングを行う	174
故障した物理マシンを復旧する (手動)	175
第 6 章: 仮想マシンを管理する	181
仮想マシンのリソースを計画する	182
仮想マシンの vCPU を計画する	183
仮想マシンのメモリを計画する	184
仮想マシンのストレージを計画する	185
仮想マシンのネットワークを計画する	186
仮想マシンを作成/マイグレーションする	187
新しい仮想マシンを作成する	188
仮想マシンをコピーする	193
物理マシンまたは仮想マシンをシステムにマイグレーションする	196
OVF または OVA ファイルをインポートする	207

OVF ファイルから仮想マシンを交換/復元する	218
仮想マシンをエクスポートする	223
ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする	229
Windows ドライブのラベルを管理する	231
Windows ベースの仮想マシンを構成する	232
VirtIO ドライバを更新する (Windows ベースの VM)	233
ディスクを作成して初期化する (Windows ベースの VM)	236
アプリケーションをインストールする (Windows ベースの VM)	237
Linux ベースの仮想マシンを構成する	238
ディスクを作成して初期化する (Linux ベースの VM)	239
アプリケーションをインストールする (Linux ベースの VM)	239
仮想マシンの運用を管理する	240
仮想マシンを起動する	240
仮想マシンをシャットダウンする	241
仮想マシンの電源をオフにする	243
仮想マシン コンソールのセッションを開く	243
仮想マシンの名前を変更する	248
仮想マシンを削除する	249
仮想マシンのリソースを管理する	250
仮想マシンのリソースを再プロビジョニングする	250
仮想マシンのボリュームを作成する	254
仮想マシンにボリュームを接続する	255
仮想マシンからボリュームを切断する	256
仮想マシンからボリュームを削除する	257
ztC Edge システムのボリュームの名前を変更する	259
ztC Edge システム上のボリュームを拡張する	259
仮想マシンのリソースを復旧する	261
仮想 CD を管理する	261
仮想 CD を作成する	262
仮想 CD を挿入する	263
仮想 CD を取り出す	264
仮想 CD からブートする	265
仮想 CD の名前を変更する	266
仮想 CD をダウンロードする	266

仮想 CD を削除する	267
高度なトピック (仮想マシン)	267
仮想マシンに特定の MAC アドレスを割り当てる	268
仮想マシンの優先 PM を選択する	269
VM を強制的にブートする	270
仮想マシンの保護レベルを変更する (HA または FT)	274
仮想マシンのブート シーケンスを構成する	274
故障した仮想マシンの MTBF をリセットする	276
仮想マシンに USB デバイスを接続する	277
第 7 章: 物理マシンのメンテナンスを行う	281
物理マシンを交換する (自動)	281
物理マシンを交換する (手動)	284
第 8 章: システム、Windows ベースの VM、およびアプリケーションをモニタリングする	291
ztC Edge システムをモニタリングする	291
Windows ベースの仮想マシンをモニタリングする	293
Windows ベースの仮想マシン上のアプリケーションをモニタリングする	296
第 2 部: 関連ドキュメント	301
第 9 章: Stratus Redundant Linux リリース 2.3.0.0 リリース ノート	302
新しい機能と機能強化	302
Stratus Redundant Linux リリース 2.3.0.0 の新機能	302
Stratus Redundant Linux リリース 2.2.0.0 の新機能	303
Stratus Redundant Linux リリース 2.1.0.0 の新機能	303
修正されたバグ	303
Stratus Redundant Linux リリース 2.3.0.0 で修正されたバグ	303
Stratus Redundant Linux リリース 2.2.0.0 で修正されたバグ	304
Stratus Redundant Linux リリース 2.1.0.0 で修正されたバグ	304
修正された CVE	304
重要な考慮事項	304
リリース 2.3.0.0 へのアップグレード	304
システム ソフトウェアのバージョンを特定する	305
アップグレードの処理中、ブラウザをリフレッシュして新しい証明書を受容する	305
ztC Edge 展開に関する機能強化	305
Intel Active Management Technology (AMT) for Lights-Out のサポートを使用する	306
ztC Edge ノードを個別の物理サイトで展開する	306
ztC Advisor を有効化する	306

テスト済みのゲスト オペレーティング システム	306
既知の問題	307
デュアルノード構成のシステムにアップグレードした後、VM に警告アイコンが表示される	307
リムーバブル メディアと、P2V クライアントを使用した PM または VM のマイグレーション	307
P2V クライアントの実行中に「VM <名前> の起動に失敗しました」というアラートが表示される (正常な動作)	307
VM のインポート時の最大パス長	307
RHEL 8.1 VM をインポートできない	308
UEFI VM コンソール セッションの最大解像度	308
vmgenid サポートを有効にするには VM を再起動する	308
Microsoft Edge コンソール ブラウザを使用した VCD の作成が失敗する	308
単一ノード システムで、VM 作成ウィザードの追加された vCPU の表示が誤っている	308
IE10、IE11、Firefox のコンソールでの日本語キーボード 106 および 109 のマッピングが正しくない	308
トラップのない SNMP 要求を有効化できない	309
モニタリングを有効にして VM をマイグレーションすると "応答なし" になる	309
A-Link がオフラインの場合、VM がパフォーマンス劣化ではなく破損として報告される	309
取り出した VCD が Linux ベースの VM でコンソールに引き続き表示される	309
一部のブラウザで https の使用中に VNC を接続できない	309
ノード IP アドレスやネットマスク ネットワーク設定を変更するとリブートが必要になる	310
Stratus ナレッジ ベースの記事にアクセスする	310
ヘルプ情報	311
第 10 章: システム リファレンス情報	312
テスト済みのゲスト オペレーティング システム	312
物理マシンと仮想マシンの重要な考慮事項	314
仮想マシンの推奨事項と制限	314
システムと HA または FT 運用	314
推奨される CPU コアの数	315
重要な考慮事項	316
ALSR 構成を作成する	316
構成を作成する	321
一般的な ztC Edge システム	321

クォーラム サーバのある ALSR 構成	322
ALSR VLAN の要件	323
初期展開から ALSR 構成の完了まで	323
ネットワークの要件を満たす	325
クォーラム サーバの場所を決めて作成する	327
クォーラム コンピュータの場所を決める	327
代替クォーラム コンピュータを追加する	328
クォーラム コンピュータの要件	329
クォーラム サービス ソフトウェアをダウンロードしてインストールする	329
構成を完了する	330
クォーラム サービス ポートを構成する	330
クォーラム サービス ポートを確認する	331
ztC Edge コンソール内でクォーラム サーバを構成する	331
構成を確認して VM を (再) 接続する	332
クォーラムがシステム動作に与える影響を理解する	333
例 1: クォーラム サーバなしのシステムではスプリット ブレイン状態が発生する	333
致命的な障害	334
障害処理	334
復旧と修復	335
例 2: クォーラム サーバのある ALSR システムではスプリット ブレイン状態を回避でき る	336
致命的な障害	336
障害処理	336
復旧と修復	337
例 2 (応用編): 致命的な障害時にクォーラム サーバがアクセス不可の場合	337
例 2 (応用編): 致命的な障害のない時にクォーラム サーバがアクセス不可の場合	338
停電から復旧する	339
ナレッジ ベースの記事にアクセスする	339
修正された CVE	340
Stratus Redundant Linux リリース 2.3.0.0 で修正された CVE	340
Stratus Redundant Linux リリース 2.2.0.0 で修正された CVE	346
Stratus Redundant Linux リリース 2.1.0.0 で修正された CVE	350
Stratus Redundant Linux リリース 2.0.1.0 で修正された CVE	355
Stratus Redundant Linux リリース 2.0.0.0 で修正された CVE	358
REST API	359

第 11 章: セキュリティ	362
セキュリティの強化	362
セキュリティ ガイドライン	363
ポートとプロトコル	364
ネットワークセグメンテーション	365
IP テーブルとファイアウォール	365
ユーザ アカウントの作成	365
パスワードの作成	366
最小権限	366
Active Directory	367
時間の同期	367
セキュアな接続	367
SSL 証明書を更新する	368
SNMP の構成	368
バックアップ	369
自動ローカル サイト復旧	369
監査	370
ログイン バナー通知	370
アップグレード	370
物理的なセキュリティ	371
高度なセキュリティ ガイドライン	371
パスワードの質に関する推奨事項	371
同時ユーザの管理	373
ウイルス対策	373
SSH アクセスの制限	373
標準化団体のベスト プラクティスと標準	375
第 12 章: SNMP	380
snmptable でシステム情報を取得する	380

第 1 部: ztC Edge ユーザ ガイド

『ztC Edge ユーザ ガイド』では、ztC Edge システムの概要およびシステムを展開して使用方法について説明します。

運用モードおよびストレージとネットワーク アーキテクチャを含むシステムの説明については、次を参照してください。

- [「ztC Edge システムの概要」](#)

計画と展開に関する情報は、次を参照してください。

- [「作業の開始」](#)

次のトピックでは、ztC Edge システムを管理する方法について説明します。

- [「ztC Edge コンソールを使用する」](#)
- [「Stratus Redundant Linux ソフトウェアをアップグレードする」](#)
- [「物理マシンを管理する」](#)
- [「仮想マシンを管理する」](#)
- [「物理マシンのメンテナンスを行う」](#)
- [「システム、Windows ベースの VM、およびアプリケーションをモニタリングする」](#) (適切なモニタリングのライセンスが適用されたシステム)

1

第 1 章: ztC Edge システムの概要

ztC Edge システムの概要については、次のトピックを参照してください。

- [「ztC Edge システムの概要」](#)
- [「運用モード」](#)
- [「ネットワーク アーキテクチャ」](#)
- [「システム使用の制限事項」](#)

ztC Edge システムの概要

2 つのノードを持つ ztC Edge システムは、ハードウェア障害が発生した場合にデータを失うことなく自動的に復旧する機能を提供します。単一または 2 つのノードを持つ ztC Edge システムは、(適切なライセンスがある場合は) ローカル システムやリモート システムを監視することによってシステム情報を確認する機能を提供します。

システムの機能と容量の説明については、次を参照してください。

- [「ztC Edge システムの説明」](#)
- [「物理マシンと仮想マシン」](#)
- [「管理操作」](#)
- [「アラート」](#)
- [「リモート サポート」](#)
- [「Lights-Out Management \(LOM\)」](#)
- [「サードパーティ製の管理ツール」](#)

ztC Edge システムの説明

Stratus Redundant Linux ソフトウェアは単一の ztC Edge コンピュータ上で稼働します。このコンピュータは物理マシン (PM) またはノードとも呼ばれます。単一ノードの ztC Edge システムは、インストール、仮想化、監視を簡単に行える機能を提供します。単一ノードのシステムに 2 台目の PM を追加して、デュアルノードの ztC Edge システムを構成できます (このシステム再構成を行う場合、その後で更新されたライセンスを適用する必要があります)。デュアルノード システムでは、フォールトトレラントまたは高可用性の仮想マシン (VM) を作成することができます。(単一ノード システムはシンプルクスなので、VM はフォールトトレラントでも高可用性でもありません。)デュアルノード システムでは両方の PM が次のようになります。

- 同じホスト オペレーティング システム (CentOS) を実行します。
- 複製された仮想マシンとストレージを含んでいます (2 台の PM は直接イーサネット リンク経由で同期されます)。
- テスト済みのゲスト オペレーティング システムを実行する仮想マシンをサポートします。

ztC Edge システム内の PM の構成の詳細については、[「システム要件の概要」](#)を参照してください。

ztC Edge システムではホスト オペレーティング システムの情報を監視することができ、Windows ベースの VM では Windows オペレーティング システムおよび Windows ベースの VM で実行しているアプリケーションに関する情報を監視できます ([「システム、Windows ベースの VM、およびアプリケーションをモニタリングする」](#)を参照)。また、システムの稼働状態に関する情報をリモートで監視することもできます ([「ztC Advisor を有効化する」](#)を参照)。

ztC Edge システムではセキュアな Out-Of-Box Experience (OOBE) が提供されます。また、セキュリティに関連する追加の構成を実装するオプションもあります。詳細については、[「セキュリティ」](#)を参照してください。

関連トピック

[「システム要件の概要」](#)

[「テスト済みのゲスト オペレーティング システム」](#)

[「ネットワーク アーキテクチャ」](#)

物理マシンと仮想マシン

1 台の物理マシン (PM) 上で稼働している Stratus Redundant Linux ソフトウェアはノードとも呼ばれます。このソフトウェアは仮想マシン (VM) を新しく作成できる単一ノードの ztC Edge システムを作成します。このシステムは、既存の VM を他の環境からインポートして、ゲスト VM に変換することもできます。単一ノードのシステムにノードを追加して、デュアルノード構成の ztC Edge システムを作成することができます。デュアルノードシステムでは、管理ソフトウェアが、選択した VM の同一のインスタンスを 2 台目のホスト PM 上に作成することにより、VM に (その構成に基づいて) 高可用性 (HA) または FT クラスの保護を自動的に提供します。システム管理者は、ztC Edge コンソールと呼ばれる個別のブラウザ ベースの管理コンソールを使用して、この単一の VM エンティティを管理します。

2 台のホスト PM に存在するコンピューティング リソースの冗長性は、アプリケーションやユーザには認識されません。アプリケーションに対しては 1 つのホスト名、VM に提示される各ネットワークにつき 1 つの MAC アドレス、そして VM に提示される各 VM ネットワークにつき 1 つの IP アドレスのみが使用されます。システム管理者は、物理サーバに読み込むのと同じ方法で、ゲスト VM (PVM) 上でアプリケーションの読み込みと構成を行います。ディスクやネットワーク デバイスで故障や障害が発生した場合、ソフトウェアは運用継続のために I/O をペアの残りのホスト PM に自動的にリダイレクトします。障害が修復されるまでは冗長性が失われますが、VM は通常どおりの運用を継続できます。アプリケーションは、何も問題が発生していないかのように継続して実行されます。冗長性、フォールト検知、特定、そして管理の各機能性は、Windows や Linux 環境およびそこで実行されているアプリケーションに対して完全に透過的に処理されます。同様に PM の修復も透過的かつ自動的行われます。PM で障害の起きたコンポーネントが修復されると、ソフトウェアはその修復済みのコンポーネントをゲスト VM の保護された環境に自動的に取り入れて、透過的に冗長性を復元します。

関連トピック

[「ztC Edge コンソールを使用する」](#)

[「\[物理マシン\] ページ」](#)

[「\[仮想マシン\] ページ」](#)

管理操作

ztC Edge システムに対するすべての管理操作は、ztC Edge コンソールから実行できます。このブラウザ ベースのインタフェースを使用して、システム全体および個々の物理マシン (PM)、仮想マシン (VM)、およびその他のリソースにアクセスできます。詳細については、[「ztC Edge コンソール」](#) を参照してください。






アラート

ztC Edge システムのアラート メッセージは、システム管理者に対処が必要な項目について通知します。たとえば以下のような項目があります。

- 実行する必要がある構成タスク
- システムの運用状態に関する通知
- 対処が必要なシステムの問題

アラート メッセージとその説明を表示するには、左側のナビゲーション パネルで **[ダッシュボード]** をクリックします。アラート ログを表示するには、左側のナビゲーション パネルで **[アラート]** をクリックします。

次のアイコンはそれぞれアラート メッセージの状態を示します。

-  情報目的
-  正常または OK の状態
-  軽度、警告、または一貫しない状態
-  中程度の状態
-  破損、故障、または深刻な状態

リモート サポート

ztC Edge システムのリモート サポート機能にアクセスするには、左側のナビゲーション パネルで **[基本設定]** をクリックします。このページで次を選択してサポートおよびプロキシの設定を構成できます。

- **サポート構成** — Stratus 認定サービス業者によるシステムのリモート サポート機能を許可し、システムが Stratus 認定サービス業者に稼動状態とステータスに関する通知を送信できるようにする設定を構成します。詳細については、[「リモート サポート設定を構成する」](#)を参照してください。
- **プロキシ構成** — インターネットへのアクセスに使用するプロキシ サーバを構成できます。詳細については、[「インターネットプロキシ設定を構成する」](#)を参照してください。

Lights-Out Management (LOM)

ztC Edge システムには Intel[®] Active Management Technology (AMT) lights-out のサポートが組み込まれていますが、デフォルトでは無効にされています。このサポートを有効にして構成するには、システムの起動中に BIOS 初期画面が表示されている間に **Ctrl-P** を押します。AMT 構成および制限に関する重要な情報については、ナレッジベースにアクセスして、「AMT and Remote Access in ztC Edge (ztC Edge の AMT およびリモートアクセス)」という記事 (KB-8219) を検索してください。[「ナレッジベースの記事にアクセスする」](#)を参照してください。

AMT 機能にはシステムの **P1** ネットワークポート上でアクセスできます。

サードパーティ製の管理ツール

ztC Edge システムにサードパーティ製の管理ツールをインストールできます。これには、ベンダー固有の管理・モニタリングユーティリティ、企業専用の管理・モニタリングユーティリティ、およびその他の各種の管理・モニタリングソフトウェアがあります。以下の点に注意してください。

- 一般的に言って、ホストオペレーティングシステム (CentOS) 上で実行できる管理ツールは ztC Edge システムでも実行できます。ただし、CentOS KVM ベースの仮想化を管理/モニタリングするツールは例外となる場合があります。ztC Edge の仮想化を管理/モニタリングするには、付属の ztC Edge 管理ツールを使用してください。
- Stratus では、ztC Edge システムを展開する前に、インストール済みの管理ツールとシステムが連携動作することを確認するよう推奨します。
- Stratus では、サードパーティ製管理ツール用として root 以外のアカウントを設定することをお勧めします。
- ztC Edge システムには、インストールの実行時に指定した (または、インタフェースで DHCP を使用するようインストール時に構成した場合は DHCP サーバから提供された) IP アドレスを使用して、管理ネットワーク経由でアクセスできます。
- サードパーティ製の管理ツールを物理マシン (PM) のホストオペレーティングシステムにインストールしていて、後日 PM の交換が必要となった場合、交換 PM にツールを再インストールする必要があるので注意してください。



注: サードパーティ製の管理ツールを使用すると、ホストオペレーティングシステムおよびシステムソフトウェアの環境が不安定になる可能性があります。RAM やディスク容量を過剰に消費したり、製品の動作を不安定にするとされる管理ツールは、削除する必要があります。Stratus 認定サービス業者が推奨する手順に従ってください。

ホスト オペレーティング システムへのアクセスに関する情報は、[「ホスト オペレーティング システムにアクセスする」](#)を参照してください。

関連トピック

[「作業の開始」](#)

[「システム リファレンス情報」](#)

運用モード

2 つのノードで構成されている ztC Edge システムでは、システム モデルに応じて、VM の可用性レベルを 1 つまたは 2 つのモードから選択することができます。

- [「高可用性運用」](#)
- [「フォールトトレラント運用」](#)

HA 運用と FT 運用はどちらも物理マシン (PM) のペアを使用することで、特定レベルの冗長性を提供します。FT 運用ではより多くのシステム リソースが消費されるため、アプリケーションの処理速度が遅くなる可能性があります。

Stratus では、HA 運用と FT 運用の両方でクォーラム サービスを構成することをお勧めします。クォーラム サービスによって、HA 運用や FT 運用のペアを構成する両方の PM が互いに独立して動作する "スプリットブ레인" 状態の発生を防ぐことができます。詳細については、[「クォーラム サーバ」](#)を参照してください。

高可用性運用

デュアルノードの ztC Edge システムの場合、ユーザが VM に定義できる可用性レベルとして高可用性 (HA) とフォールトトレラント (FT) の 2 つが Stratus Redundant Linux ソフトウェアで提供されます。

HA 運用では、Stratus Redundant Linux が大半のハードウェア障害を自動的に検知してその場所を特定し、対処することにより、アプリケーションを継続して実行できるようにします。HA のリモートサポートテクノロジーによって、ソフトウェアが Stratus サポート センターにさまざまな問題について通知を行い、障害のタイプとその正確な場所を知らせます。このように自動障害検知、特定、リモートサポートの各テクノロジーを組み合わせることで、専門知識を持つサポート技術者へのアクセスと迅速な問題解決が確実になります。

VM の可用性レベルの選択は、ztC Edge コンソールを使用して VM を作成またはインポートするときに行います。

有効にした場合、HA 運用は基本的なフェールオーバーと復旧機能が提供されます。一部の障害では復旧と HA 運用の復元のために (自動の) VM リブートが必要です。

- CPU、メモリ、I/O、その他の物理マシン (PM) の障害によるダウンタイムをほぼゼロにします。
- IT 担当者が介入することなく障害に対処できます。
- すべてのコンポーネントに継続したアクティブな有効性確認機能を提供します。
- 冗長性と回復性が常に保証されます。

HA は、数分程度の中断がときおり発生しても支障のないアプリケーションに適しています。

(サポートされる VM 可用性のレベルは、システム モデルによって異なります。詳細については、[「仮想マシンの推奨事項と制限」](#) を参照してください。)

関連トピック

[「\[仮想マシン\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

フォールトトレラント運用

デュアルノードの ztC Edge システムの場合、ユーザが VM に定義できる可用性レベルとして高可用性 (HA) とフォールトトレラント (FT) の 2 つが Stratus Redundant Linux ソフトウェアで提供されます。FT 運用では、障害発生時にもダウンタイムなしに継続してアプリケーションが実行されます。FT は、最高レベルの可用性を必要とするアプリケーションに使用します。

VM の可用性レベルの選択は、ztC Edge コンソールを使用して VM を作成またはインポートするときに行います。

FT 運用では ztC Edge ソフトウェアが、2 台の物理マシン (PM) で実行される VM 用に冗長な環境を作成することによりアプリケーションを透過的に保護します。ztC Edge ソフトウェアは、選択した VM と同一のインスタンスを 2 台目のホスト PM に作成して、VM に FT クラスの保護を提供します。

FT 運用を有効にした場合、VM はすべての障害から透過的に保護され、ダウンタイムが発生することはありません。また、FT では次のメリットも得られます。

- CPU、メモリ、I/O、その他の物理マシン (PM) の障害によるダウンタイムが一切なくなります。
- IT 担当者が介入しなくても障害に対処できます。
- データの損失がなくなります。
- すべてのコンポーネントに継続したアクティブな有効性確認機能を提供します。
- 完全な冗長性と回復性が常に保証されます。

(サポートされる VM 可用性のレベルは、システム モデルによって異なります。詳細については、[「仮想マシンの推奨事項と制限」](#) を参照してください。)

関連トピック

[「\[仮想マシン\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

ALSR 構成

"自動ローカル サイト復旧 (ALSR) 構成" は、2 つの別々のサイトにある 2 台の物理マシンを接続します。これはディザスタトレラントな展開方法で、ハードウェアの冗長性だけでなく、それを含む物理的なコンピュータ室や建物の冗長性も維持されます。地理的に離れているため、ALSR 構成にはコンポーネント配置の入念な計画と、より複雑なネットワーク トポロジが必要とされます。**ALSR 構成の場合、Stratus ではクォーラム サービスの使用を強く推奨します。ALSR 構成では A-Link ネットワークが他の障害発生シナリオにさらされる可能性があります。**(1 つのノードで構成されているシステムでは ALSR 構成は利用できません。)

ALSR 構成のネットワークの必要条件の一覧は、[「ネットワークの要件を満たす」](#) に記載されています。

ALSR とクォーラム サービス

ALSR 構成では、クォーラム展開に推奨されるベストプラクティス ([「クォーラム サーバ」](#) および [「クォーラム サーバの場所を決めて作成する」](#) を参照) に従って、2 台のクォーラム サービス コンピュータを構成します。すべての ALSR 構成において、優先クォーラム サービス コンピュータは第 3 のファシリティに配置し、代替コンピュータは第 4 サイトに配置します (第 3 サイトに配置する場合には適切な場所を選択してください)。これらのネットワークは相互に接続されています。

クォーラム サービス コンピュータはできる限り分離する必要があります。両方を同じ (つまり第 3 の) サイトに配置しなければならない場合、各コンピュータが同じ電源に依存しないように気を付ける必要があります。

また、ztC Edge PM とクォーラム サービス コンピュータ間の物理的な接続が、もう片方の PM のサイトを経由しないようにします。

クォーラム サービス コンピュータを ztC Edge PM の一方と同じサイトに配置することによって、データの整合性が確保されます。ただしその場合、発生したサイト障害によっては、手動で復旧されるまで VM をシャットダウンする必要があります。

管理ネットワークは ztC Edge の PM とクォーラム サービス コンピュータを物理的に接続します。これが正しく機能するためには各 ztC Edge PM が異なるゲートウェイを使用してクォーラム サービス コン

ピュータにアクセスするよう、PM を構成する必要があります。2 台の PM が同じゲートウェイを経由してクォーラム サービス コンピュータにアクセスする場合、障害時にデータの整合性が確保されます。ただしその場合、発生したサイト障害によっては、手動で復旧されるまで VM をシャットダウンする必要があります。

関連トピック

[「ALSR 構成を作成する」](#)

[「ネットワーク アーキテクチャ」](#)

クォーラム サーバ

"クォーラム サービス" は、デュアルノード ztC Edge システムの 2 台のサーバ (物理マシン、つまり PM) とは別個のサーバ上に展開する、Windows オペレーティング システム ベースのサービスです。クォーラム サーバによってデータの整合性が保証され、ztC Edge 環境で特定の障害が生じた場合に自動で再起動する機能が提供されます。Stratus では、ALSR 運用の場合は特に、クォーラム サーバを使用することを推奨します。ztC Edge システムの 2 台の PM に 0、1、または 2 個のクォーラム サーバを構成することができます。

クォーラム サーバは、スプリット ブレーンを含む複数のネットワーク障害が発生するシナリオで VM の完全性を確保し、特定の障害発生後に自動で再起動する機能を提供します。クォーラム サーバの通信は管理ネットワーク経由で行われます。

クォーラム サーバは、ALSR 構成では特に重要です。ALSR のベスト プラクティスとして、優先クォーラム コンピュータを第 3 のファシリティに設置し、代替クォーラム コンピュータは第 4 ファシリティに設置することが推奨されます。ただし、代替クォーラム サービス コンピュータを優先クォーラム コンピュータと同じファシリティに設置しても、十分な結果は得られます。詳細については、[「ALSR 構成」](#)を参照してください。

使用できるサイトが 2 つしかない場合 (つまり上記のベスト プラクティスによる構成が不可能な場合) で、一方の PM がダウンしていてもう片方の PM がクォーラム サーバと通信できない場合 (たとえばダウンした PM と同じサイトにある場合) には、スプリット ブレーン状態での実行を避けるため、正常なサイトにある VM は自動的にシャットダウンされます。

関連トピック

[「ALSR 構成を作成する」](#) (クォーラム サーバについての説明)

[「クォーラム サーバを構成する」](#)

ネットワーク アーキテクチャ

イーサネット ネットワークはシステムに通信手段を提供します。イーサネット ネットワークには次の主な種類があります。

- (青 (**A2** または ●●) と黄色 (**A1** または ●) のネットワーク ポート上の) 2 つのノードで構成されている ztC Edge システム上の "アベイラビリティ リンク ネットワーク" あるいは "A-Link ネットワーク" は、仮想マシン (VM) に割り当てられ、2 台の PM 間のデータの同期や VM のマイグレーションに使用されます。A-Link ネットワークのうち 1 つ (青い (**A2** または ●) ネットワーク ポート上) は、2 台の ztC Edge PM を接続する "プライベート ネットワーク" (priv0) です。詳細については、[「A-Link ネットワークとプライベート ネットワーク」](#) を参照してください。(1 つのノードで構成されているシステムは、A-Link ネットワークの機能を提供しません。)
- すべての ztC Edge システム上の "ビジネス ネットワーク" (**P1** ネットワーク ポート上、および有効な場合は **P2** 上) は、アプリケーションが既存のネットワークに接続できるようにします。ビジネス ネットワークのうち 1 つ (**P1** ネットワーク ポート上) は、"管理ネットワーク" でもあります。これは ibiz0 または network0 と呼ばれ、ztC Edge コンソールに接続してクォーラム サーバで使用されます。詳細については、[「ビジネス ネットワークと管理ネットワーク」](#) を参照してください。

ztC Edge システムにはネットワーク セグメンテーションの検知機構も用意されています。詳細については、[「ネットワーク セグメンテーション違反の検知と修復」](#) を参照してください。

A-Link ネットワークとプライベート ネットワーク

2 台の物理マシン (PM、またはノードとも呼ばれます) で構成されているすべての ztC Edge システムに、2 台の PM 間のプライベートな管理トラフィックに使用するためのネットワークが必要です。このプライベート ネットワークは "priv0" として参照されます。これはノード間の物理接続、直接イーサネット接続、または VLAN 接続のいずれかです。priv0 はピア ノードの検出に使用され、IPv4 ブロードキャストに応答するエンティティを他に構成することはできません。

2 つのノードで構成されている各システムには、priv0 に加え、PM 間におけるデータ複製のパフォーマンスを向上させる A-Link ネットワークが含まれます。A-Link ネットワークによって、ディスクの同期、ネットワークの分路、VM のマイグレーション、ハートビート チェックの実行、およびフォールトトレラント メモリの同期が可能になります。

A-Link と priv0 は PM 間で同じ方法によって接続されます。A-Link は各 PM の青と黄色のネットワーク ポート間で接続され、priv0 は青いネットワーク上の A-Link と共有されます。

最も単純な priv0 は、各サーバの内蔵イーサネット ポートを接続する 1 つのイーサネット ケーブル (クロス ケーブルまたはストレート ケーブル) で構成されます。priv0 に単一イーサネット ケーブル以外の ネットワーク デバイスを使用する場合、[「ALSR 構成」](#)を参照してください。

関連トピック

[「ビジネス ネットワークと管理ネットワーク」](#)

[「A-Link ネットワークとプライベート ネットワークの要件」](#)

[「ネットワーク アーキテクチャ」](#)

ビジネス ネットワークと管理ネットワーク

デュアルノード構成の ztC Edge システム上の A-Link ネットワークおよびプライベート ネットワークにより使用されるものを除いて、すべてのイーサネット ポートがビジネス ネットワーク ポートと見なされます。ゲスト オペレーティング システムはビジネス ネットワーク ポートを使用してネットワークに接続します。

1 つのビジネス ネットワークは "管理" ネットワークであり、各 PM が 1 つの管理ネットワークを持ちます。このネットワークは "ibiz0" と呼ばれ、**P1** というラベルのネットワークを使用します。管理ネットワークは、ztC Edge コンソールにアクセスして各種の管理タスクとクォーラム サーバの処理を行います。これらの管理タスクには以下が含まれます。

- call-home メッセージと e アラートの送信
- ライセンスのステータスのチェック
- 各 PM の ztC Edge コンソールとの通信
- priv0 のフェールオーバー機能 (デュアルノード構成のシステムの場合)
- 2 ノード間の通信 (デュアルノード構成のシステムの場合)
- クォーラム サーバとの通信 (存在する場合)

管理ネットワークの設定は、システムを展開するときに行います。また、展開中に、物理的に接続されているすべてのビジネス ネットワーク ポート用のビジネス ネットワークを設定することもできます。展開が完了した後で 2 番目のビジネス ネットワークを接続するには、[「2 番目のビジネス ネットワークを接続する」](#)を参照してください。

関連トピック

[「A-Link ネットワークとプライベートネットワーク」](#)

[「ビジネス ネットワークと管理ネットワークの要件」](#)

[「ネットワーク アーキテクチャ」](#)

ネットワーク セグメンテーション違反の検知と修復

共有ネットワークにおいて、それぞれが外部ネットワークに接続できてもネットワークの両端が互いに通信できなくなるようなネットワーク障害のことを "ネットワーク セグメンテーション違反" と呼びます。

デュアルノード構成の ztC Edge システムに用意されている "ネットワーク セグメンテーション違反の検知機構" は、この違反が検知された時点で、外部ネットワークとの接続が優れている方のノードにアクティブな VM を配置します。この機能の一環として、ztC Edge システムはアクティブなノードとスタンバイ ノードの間でビジネス ネットワーク インタフェースを介して UDP パケットを常時送信します。ネットワークの両側がアクティブなネットワーク リンクを維持している間にこのパケットの流れが中断されると、システムのネットワーク セグメンテーション ロジックによってエラーが検知されます。このエラー シナリオでは、どちらのノードもアクティブなネットワーク接続を保っているため、エラーの原因は ztC Edge システムの外部のスイッチにあります。

この状況が検知されると、ztC Edge システムはこのうちどちらの外部接続が優れているかを判断するロジックに基づいて、エラーを処理します。ztC Edge システムは、ブロードキャスト/マルチキャストの受信トラフィックを継続的に監視してどちらのノードの受信トラフィックが多いかを判断することにより、エラー処理判定を行います。このエラー条件では、ネットワーク トラフィックが多い方のノードで VM が既にアクティブになっていない場合、ztC Edge システムは VM ネットワークをこのノードにフェールオーバーします。この違反検知機能ではシステムで通常発生するトラフィックに基づいて判定が行われるので、ユーザが構成を行う必要はありません。

関連トピック

[「ネットワーク アーキテクチャ」](#)

システム使用の制限事項

次のトピックで説明されている、システム使用に関する制限事項に従ってください。

- [「QEMU」](#)
- [「ホスト オペレーティング システムにアクセスする」](#)

QEMU

ztC Edge デュアルノードシステムおよび単一ノードシステムは、ハードウェア仮想化を実行するオープンソースのハイパーバイザ QEMU ("Quick EMUlator") をサポートしています。仮想化に使用する場合、QEMU はゲストコードをホスト CPU 上で直接実行し、高レベルのパフォーマンスを実現します。

ztC Edge ユーザは QEMU の仮想化エンジンやその構成に変更を加えないでください。

ホスト オペレーティング システムにアクセスする

ztC Edge の展開を完了した後、PM の物理コンソールでローカルに、あるいはセキュア シェル (SSH) クライアントを使ったリモート操作によって、ホスト オペレーティング システム (CentOS) にアクセスできます。

SSH クライアントを使ってホスト オペレーティング システムにログオンする場合、展開の処理中に指定された (または、インタフェースで DHCP を使用するよう展開時に構成した場合には DHCP サーバから提供された) 管理用 IP アドレスを使用します。必要な場合はこのトピックの説明に従って PM の管理用 IP アドレスを取得できます。



注意事項: ztC Edge システムの CentOS ホスト オペレーティング システムを、Stratus 以外のソースから更新しないでください。Stratus Redundant Linux ソフトウェアと一緒にインストールされる CentOS リリースのみを使用してください。



注: 管理コマンドが確実に正しく機能するように、物理コンソールまたはプライマリ PM の IP アドレスにログオンしてください (ただし、デュアルノードシステムのセカンダリ PM 内のコンポーネントに対する操作が必要な場合は例外です)。PM 間で移動する可能性があるため、システム IP アドレスには接続しないでください。



注: ルート アカウントのデフォルトパスワードは **KeepRunning** です。システムのセキュリティを確保するため、各 PM で root のパスワードをできるだけ早く変更してください。PM に初めて root としてログオンする場合、システムにパスワードの変更を求めるプロンプトが自動的に表示されます。初回ログオンの後にパスワードを再度変更するには、各 PM で `passwd` コマンドを実行します。

CentOS でのサードパーティ製管理ツールの使用については、「[サードパーティ製の管理ツール](#)」を参照してください。

ztC Edge コンソール内の各 PM の IP アドレスを見つけるには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[システム]** の下で **[IP 構成]** をクリックします。
3. 各 PM、つまり **node0** と **node1** (存在する場合) の **[IP アドレス]** を記録します。
4. 左側のナビゲーション パネルで **[物理マシン]** をクリックして **[物理マシン]** ページを表示します。
5. どちらの PM がシステムのプライマリ ノードかを記録します。これは **noden (プライマリ)** と表示されます。通常の場合、管理コマンドが正しく機能するようにするには、プライマリ ノードの IP アドレスにログオンします。

Windows ベースのシステムからホスト オペレーティング システムにアクセスするには

オープンソース SSH クライアントの PuTTY を次からダウンロードして使用できます。

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

具体的には、`putty.exe` クライアントによって、シェルにアクセスしてホスト オペレーティング システムのコマンドラインでプログラムを実行することが可能になります。PuTTY には、リモートシステムからホスト オペレーティング システムにファイルをセキュアに転送できる `pscp.exe` コマンドライン ユーティリティも含まれています。

グラフィカル ユーザ インタフェースのあるセキュア コピー (SCP) クライアントが必要な場合、オープンソースの WinSCP ユーティリティを使用するオプションもあります。

<http://winscp.net/eng/index.php>

Linux ベースのシステムからホスト オペレーティング システムにアクセスするには

多くの Linux ベースや UNIX ベースのシステムでは、SSH ユーティリティが既にインストールされていてデフォルトで有効にされています。これらのユーティリティの使用方法の詳細については、`ssh(1)` および `scp(1)` を参照してください。

2

第 2 章: 作業の開始

次のトピックでは、ztC Edge の計画、展開、および展開後のタスクについて説明します。

- [「計画」](#)
- [「展開」](#)
- [「展開後のタスク」](#)

計画

システム構成の計画に関する情報は、次のトピックを参照してください。

- [「安全上の注意事項」](#)
- [「システム要件の概要」](#)
- [「設置スペースに関する推奨事項」](#)
- [「システム仕様」](#)
- [「DIN レール マウントおよび壁かけブラケットの組み立て」](#)
- [「製品コンプライアンス」](#)
- [「全般的なネットワーク要件と構成」](#)
- [「ビジネス ネットワークと管理ネットワークの要件」](#)
- [「A-Link ネットワークとプライベートネットワークの要件」](#)
- [「ztC Edge コンソールの要件」](#)
- [「対応しているインターネット ブラウザ」](#)
- [「電源の要件と考慮事項」](#)
- [「ALSR 構成を作成する」](#)（お使いの構成に該当する場合）

システム構成を計画したら、[「展開」](#)を続けて行います。

安全上の注意事項

作業を始める前に、次の安全上の注意事項をお読みください。



警告: 製品を接続する前に電源の電圧が正しいことを確認してください。



警告: 修理・点検は認定を受けたサービス担当者が行う必要があります。ユーザによる修理が可能なコンポーネントは使用しないでください。

警告: 誤ったタイプのバッテリーに交換すると爆発する危険があります。使用済みのバッテリーを廃棄する場合は指示に従ってください。



IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMEMENT AUX INSTRUCTIONS



警告: 高温注意。表面に触れないでください。

次の情報は ztC Edge 110i システムのみに適用されます。

- これらのデバイスは、環境に適した筐体内に設置する必要のあるオープンタイプです。内部のコンパートメントにアクセスするにはツールを使用する必要があります。
- クラス I、ディビジョン 2、グループ A ～ D の危険区域、あるいは非危険区域での使用のみに適しています。



警告: 爆発の危険があります。周囲に発火性物質がないことがわかっている場合を除き、回路がアクティブな間に機器を切断しないでください。

システム要件の概要


ztC Edge システムでは、複数の仮想マシン (VM) と、ztC Edge コンソールを実行できる 1 台のリモート管理コンピュータ (つまり汎用の PC) がサポートされます。

ztC Edge の「[システムハードウェア](#)」の仕様と要件を、物理マシン (PM) のタイプごとに次にまとめています。PM の推奨される配置については「[設置スペースに関する推奨事項](#)」、追加のシステム仕様については「[システム仕様](#)」を参照してください。


ゲストオペレーティングシステムの詳細については、「[テスト済みのゲストオペレーティングシステム](#)」を参照してください。

システム ハードウェア

機能	ztC Edge 200i PM	ztC Edge 250i PM
RAM (物理メモリ)	32 GB	64 GB

機能	ztC Edge 200i PM	ztC Edge 250i PM
ディスク容量	1 テラバイト (TB) のソリッドステートドライブ (SSD)	2 TB の SSD
ネットワークポート	<p>各 PM に 4 つの 1 Gb イーサネットポートが搭載されていること。</p> <p>2 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> • A1 (黄色いラベル) は A-Link 1 • A2 (青いラベル) は priv0 <p>2 つのノードまたは 1 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> • P1 はビジネス ネットワークと管理ネットワークの組み合わせ • P2 はオプションのビジネス ネットワーク 	<p>各 PM に、メイン シャーシに 6 つの 1-Gb ポート (P1 ~ P6)、拡張ユニットに 2 つの 10-Gb ポート (A1 と A2) の、合計 8 つのネットワークポートがあること。</p> <p>2 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> • A1 (黄色いラベル) は A-Link 1 • A2 (青いラベル) は priv0 <p>2 つのノードまたは 1 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> • P1 はビジネス ネットワークと管理ネットワークの組み合わせ • P2 ~ P6 はオプションのビジネス ネットワーク
<div>  注: P1 は network0 または ibiz0、P2 は network1 または ibiz1、P3 は network3 または ibiz3 と呼ばれます。それ以降も同様です。 </div>		

機能	ztC Edge 100i PM	ztC Edge 110i PM
RAM (物理メモリ)	32 GB	32 GB または 64 GB

機能	ztC Edge 100i PM	ztC Edge 110i PM
ディスク容量	512 GB のソリッドステート ドライブ (SSD) があり、うち約 475 GB を VM で利用できること。	2 テラバイト (TB) の SSD があり、うち約 1.9 TB を VM で利用できること。
ネットワーク ポート	<p>各 PM に 4 つの 1 Gb イーサネットポートが搭載されていること。</p> <p>2 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> 青 (●) は A-Link と priv0 プライベートの組み合わせネットワーク 黄色 (●●) は 2 番目の A-Link 専用ネットワーク <p>2 つのノードまたは 1 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> P1 はビジネス ネットワークと管理ネットワークの組み合わせ P2 はオプションのビジネス ネットワーク 	<p>各 PM に、前面に 6 つの 1-Gb ポート (P1 ~ P6)、背面に 2 つの 10-Gb ポート (A1 と A2) の、合計 8 つのネットワークポートがあること。</p> <p>2 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> A1 (黄色いラベル) は A-Link 1 A2 (青いラベル) は priv0 <p>2 つのノードまたは 1 つのノード用に構成されているシステムでは、次を使用します。</p> <ul style="list-style-type: none"> P1 はビジネス ネットワークと管理ネットワークの組み合わせ P2 ~ P6 はオプションのビジネス ネットワーク
	<div>  <p>注: P1 は network0 または ibiz0、P2 は network1 または ibiz1、P3 は network3 または ibiz3 とも呼ばれます。それ以降も同様です。</p> </div>	

システムは、Intel[®] Active Management Technology (AMT) lights-out のサポートも提供します。これには各 PM の **P1** ポートからアクセスできます。

ALSR 構成の場合はネットワーク要件が異なります。詳細については、「[ネットワークの要件を満たす](#)」を参照してください。

詳細については、「[ネットワークアーキテクチャ](#)」、「[A-Link ネットワークとプライベート ネットワーク](#)」、「[ビジネス ネットワークと管理ネットワーク](#)」を参照してください。

IP アドレス

各 ztC Edge システムに管理ソフトウェアで使用される静的な IPv4 IP アドレスが必要です。管理ネットワークの DNS プライマリおよびセカンダリ サーバの IP アドレス、およびゲートウェイとサブネット マスク情報は、担当の IT ネットワーク管理者に問い合わせてください。詳細については、「[システム IP 情報を取得する](#)」を参照してください。

ポート

ztC Edge システムは、ローカル ファイアウォールでの HTTPS 通信にポート 443、ssh にポート 22、また各 VM に関連付けられたアクティブな各 VNC 用に 5900-59nn を使用します。ファイアウォールで、適切なポートを経由したトラフィックが許可されている必要があります。VM が UDP ポート 4557 を使用してクォーラム サービス コンピュータにアクセスできるよう、ファイアウォールの許可が必要です。TCP および UDP ポートの詳細については、ナレッジ ベースにアクセスして、「TCP and UDP ports used by ztC Edge (ztC Edge で使用される TCP および UDP ポート)」という記事 (KB-[9357](#)) を検索してください。「[ナレッジ ベースの記事にアクセスする](#)」を参照してください。

関連トピック

[「物理マシンと仮想マシンの重要な考慮事項」](#)

[「仮想マシンの推奨事項と制限」](#)

[「仮想マシンのリソースを計画する」](#)

[「IP 設定を構成する」](#)

設置スペースに関する推奨事項

ztC Edge システムのインストール サイトでは、設備、冷却、および設置間隔について適切な環境を確実に提供できるよう、設置スペースに関する以下の推奨事項を考慮してください。

デスク上に設置するノードに推奨される設置間隔は次のとおりです。

- ノードの左右にそれぞれ少なくとも 2 インチ (5.08 cm) 空ける
- ノードの上に少なくとも 3 インチ (7.62 cm) 空ける

- ノードの前後にそれぞれ少なくとも 5 インチ (12.7 cm) 空ける
- ノードの間に少なくとも 2 インチ (5.08 cm) 空ける

DIN レール マウントを使って取り付けるノードに推奨される設置間隔は次のとおりです。

- ノードの左右にそれぞれ少なくとも 2 インチ (5.08 cm) 空ける
- ノードの上下にそれぞれ少なくとも 5 インチ (12.7 cm) 空ける
- ノードの間に少なくとも 2 インチ (5.08 cm) 空ける

上記に加え、設置スペースについての以下の推奨事項を考慮してください。

- ノードは水平方向 (平らな面に置く) または垂直方向 (壁に取り付ける) に設置できます。垂直に設置する場合、Stratus ロゴのある面を上に向けてください。
- システムのケーブルが破損するのを避けるため、すべてのケーブルの曲げ半径を最小でも 2 インチ (5.08 cm) に保つ必要があります。
- ノードの下に発熱の可能性があるものを設置しないでください。
- ノードの操作環境限度を超えないようにしてください。
- 最適な伝熱効果を得るには、各ノードのヒートシンク上に少なくとも 100 LFM (0.51 m/s) の空気循環が必要です。

上記の推奨事項に加えて、サイトに固有の設置ニーズについても検討してください。さらに詳しい情報が必要な場合は、Stratus 認定サービス業者までお問い合わせください。

システム仕様

ztC Edge システムの仕様については、以下を参照してください。

- [「システム仕様: ztC Edge 250i システム」](#)
- [「システム仕様: ztC Edge 200i システム」](#)
- [「システム仕様: ztC Edge 110i システム」](#)
- [「システム仕様: ztC Edge 100i システム」](#)

システム仕様: ztC Edge 250i システム

次の表はシステムの仕様を一覧したものです。

コンポーネント	説明
---------	----

CPU	
CPU	Intel Xeon W-1250TE、1.8 GHz、20 MB キャッシュ、10 x HT コア、35W
システム メモリ	2 x 260 ピン バッファなし DDR4-2666 MHz ECC、SO-DIMM ソケット、合計 64 GB
I/O	
ディスプレイ	1 x HDMI 1 x VGA ポート
イーサネット	6 x 10/100/1000 イーサネット ポート 2 x 10 Gb イーサネット ポート
USB ポート	2 x USB 3.2、第 2 世代 (10 Gbps) 4 x USB 3.2、第 1 世代 (5 Gbps)
ストレージ	1 NVMe SSD、2 TB
インジケータ	1 x 緑の LED (電源スイッチ) - PWR ステータスを示す 1 x 黄色の LED - SYS ステータスを示す
システム	
供給電源	オプションの AC 電源モジュール 100 ~ 240V AC、50/60 Hz、2.5A
入力電源	9V ~ 36V (DC)
環境	
動作環境温度	-20℃ ~ 60℃ (-4°F ~ 140°F)
ストレージ環境温度	-40℃ ~ 85℃ (-40°F ~ 185°F)
湿度	40℃ で 95% (結露しないこと)

耐久衝撃	IEC 60068-2-27 (SSD: 壁かけ型 20G、正弦半波パルス、時間 11 ms)
耐久振動	IEC 60068-2-64 (SSD: 3Grms STD、ランダム、5 ~ 500 Hz、1 時/軸)
外形寸法	
重量	4.6 kg (10.2 lb)
高さ	192 mm (7.55 インチ)
幅	127 mm (5.00 インチ)
奥行き	230 mm (9.05 インチ)

システム仕様: ztC Edge 200i システム

次の表はシステムの仕様を一覧したものです。

コンポーネント	説明
CPU	
CPU	Intel Xeon W-1250TE、2.4 GHz、12 MB キャッシュ、6 x HT コア、35W
システム メモリ	2 x 260 ピン バッファなし DDR4-2666 MHz ECC、SO-DIMM ソケット、合計 32 GB
I/O	
ディスプレイ	1 x HDMI 1 x VGA ポート
イーサネット	6 x 10/100/1000 イーサネット ポート
USB ポート	2 x USB 3.2、第 2 世代 (10 Gbps) 4 x USB 3.2、第 1 世代 (5 Gbps)

ストレージ	1 NVMe SSD、1 TB
インジケータ	1 x 緑の LED (電源スイッチ) - PWR ステータスを示す 1 x 黄色の LED - SYS ステータスを示す
システム	
供給電源	オプションの AC 電源モジュール 100 ~ 240V AC、50/60 Hz、2.5A
入力電源	9V ~ 36V (DC)
環境	
動作環境温度	-20℃ ~ 60℃ (-4°F ~ 140°F)
ストレージ環境温度	-40℃ ~ 85℃ (-40°F ~ 185°F)
湿度	40℃ で 95% (結露しないこと)
耐久衝撃	IEC 60068-2-27 (SSD: 壁かけ型 20G、正弦半波パルス、時間 11 ms)
耐久振動	IEC 60068-2-64 (SSD: 3Grms STD、ランダム、5 ~ 500 Hz、1 時/軸)
外形寸法	
重量	3.3 kg (7.2 lb)
高さ	192 mm (7.55 インチ)
幅	77 mm (3.07 インチ)
奥行き	230 mm (9.05 インチ)

システム仕様: ztC Edge 110i システム

次の表はシステムの仕様を一覧したものです。

コンポーネント	説明
---------	----

CPU	
CPU	Intel Core I7-8700T プロセッサ、35W
システム メモリ	2 x 260 ピン バッファなし DDR4-2400 MHz SO-DIMM ソケット、合計 32 GB または 64 GB
I/O	
ディスプレイ	1 x HDMI 1 x DVI ポート
イーサネット	6 x 10/100/1000 イーサネット ポート 2 x 10 Gb イーサネット ポート
USB ポート	2 x USB 3.2 Gen 2 (10 Gbps) (旧称 USB 3.1 Gen 2) 2 x USB 3.2 Gen 1 (5 Gbps) (旧称 USB 3.1 Gen 1)
ストレージ	1 SATA SSD、2 TB
インジケータ	1 x 緑の LED (PWR ステータス) 1 x 緑の LED (SYS ステータス) 1 x 緑の LED (SDD アクティブ)
スイッチ	1 x 電源スイッチ 1 x リセットスイッチ
システム	
供給電源	24V DC 入力 オプションの AC 電源モジュール 100 ~ 240V AC、50/60 Hz、5A ¹
標準的な消費電力と熱	62 W、213 BTU/時

¹AC アダプタ用 DIN 壁かけブラケットをインドに配送することはできません。

出力	
環境	
動作環境温度	-20°C ~ 55°C (-4°F ~ 131°F)
ストレージ環境温度	-40°C ~ 80°C (-40°F ~ 176°F)
湿度	10% ~ 95% (結露なし)
耐久衝撃	IEC 60068-2-27 (SSD: 壁かけ型 25G、正弦半波パルス、時間 11 ms)
耐久振動	IEC 60068-2-64 (SSD: 3Grms STD、ランダム、5 ~ 500 Hz、1 時/軸)
外形寸法	
重量	5.2 kg (11.46 lb) パッケージを除く 6.2 kg (13.67 lb) パッケージを含む
高さ	86.9 mm (3.42 インチ)
幅	280 mm (11.02 インチ)
奥行き	210 mm (8.26 インチ)

システム仕様: ztC Edge 100i システム

次の表はシステムの仕様を一覧したものです。

コンポーネント	説明
CPU	
CPU	Intel Core I7-6700TE プロセッサ、35W
システム メモリ	2 x 260 ピン バッファなし DDR4-2400 MHz SO-DIMM ソケット、合計 32 GB

I/O	
ディスプレイ	1 x HDMI 1 x DVI ポート
イーサネット	4 x 10/100/1000 イーサネット ポート
USB ポート	2 x USB 2.0 6 x USB 3.2 Gen 1 (5 Gbps) (旧称 USB 3.1 Gen 1)
ストレージ	1 SATA SSD、512 GB
インジケータ	1 x 緑の LED (PWR ステータス) 1 x 緑の LED (SYS ステータス) 1 x 緑の LED (SSD アクティブ)
スイッチ	1 x 電源スイッチ 1 x リセットスイッチ
システム	
供給電源	9 ~ 36V DC 入力 オプションの AC 電源モジュール 100 ~ 240V AC、50/60 Hz、5A
標準的な消費電力と熱出力	41 W、140 BTU/時
環境	
動作環境温度	-40°C ~ 60°C (-40°F ~ 140°F)
ストレージ環境温度	-40°C ~ 80°C (-40°F ~ 176°F)
湿度	10% ~ 95% (結露なし)
耐久衝撃	IEC 60068-2-27 (SSD: 壁かけ型 50G、正弦半波パルス、時間 11 ms)

耐久振動	IEC 60068-2-64 (SSD: 3Grms STD、ランダム、5 ~ 500 Hz、1 時/軸)
外形寸法	
重量	4.8 kg (10.58 lb) パッケージを除く 5.6 kg (12.34 lb) パッケージを含む
高さ	75 mm (2.95 インチ)
幅	280 mm (11.02 インチ)
奥行き	190 mm (7.48 インチ)

DIN レール マウントおよび壁かけブラケットの組み立て

ztC Edge システムにマウント キットを取り付けるため手順については、以下を参照してください。

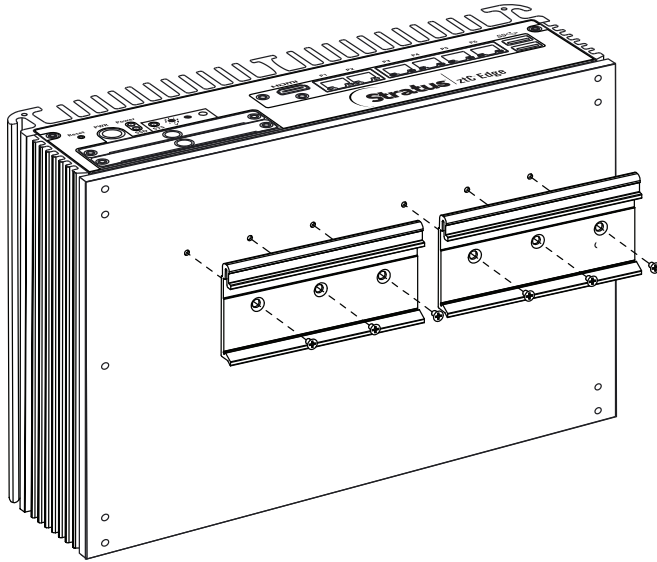
- [「DIN レール マウントおよび壁かけブラケットの組み立て: ztC Edge 110i システム」](#)
- [「DIN レール マウントおよび壁かけブラケットの組み立て: ztC Edge 100i システム」](#)

DIN レール マウントおよび壁かけブラケットの組み立て: ztC Edge 110i システム

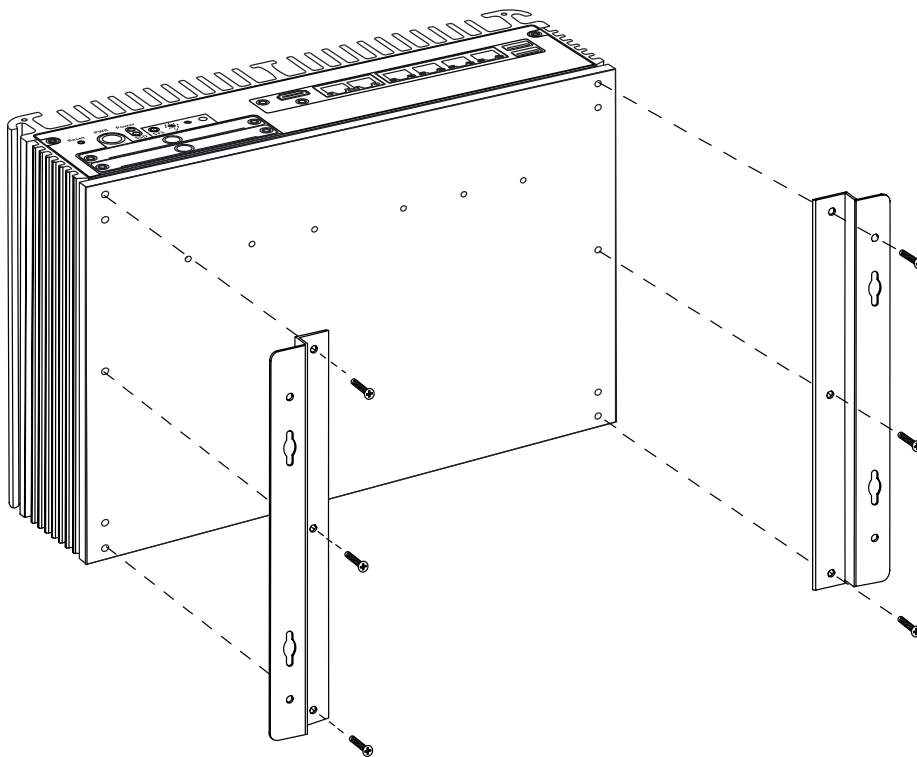


注: DIN レール マウントまたは壁かけキットを ztC Edge ノードに取り付ける際は、Stratus ロゴの付いた面が上を向いていることを確認してください。

DIN レール マウント キットを取り付けるには、アクセサリ ボックスにある 6 本の皿ネジ M3 x 6 mm を使用します。



壁かけキットを取り付けるには、ノードの底面にある 6 本の皿ネジ M3 x 12 mm (左右 3 本ずつ) を取り外します。これらのネジを使って、壁かけキットを取り付けます。





注: 石膏ボードにネジを打ち込む場合、アンカーを使用して、ケーブルや電源コネクタからの重みによってユニットが壁から抜け落ちることのないようにしてください。使用できるネジの直径は最大 0.166 インチ (3.5 mm)、ネジ頭の直径は最小 0.216 インチ (5.5 mm) です。

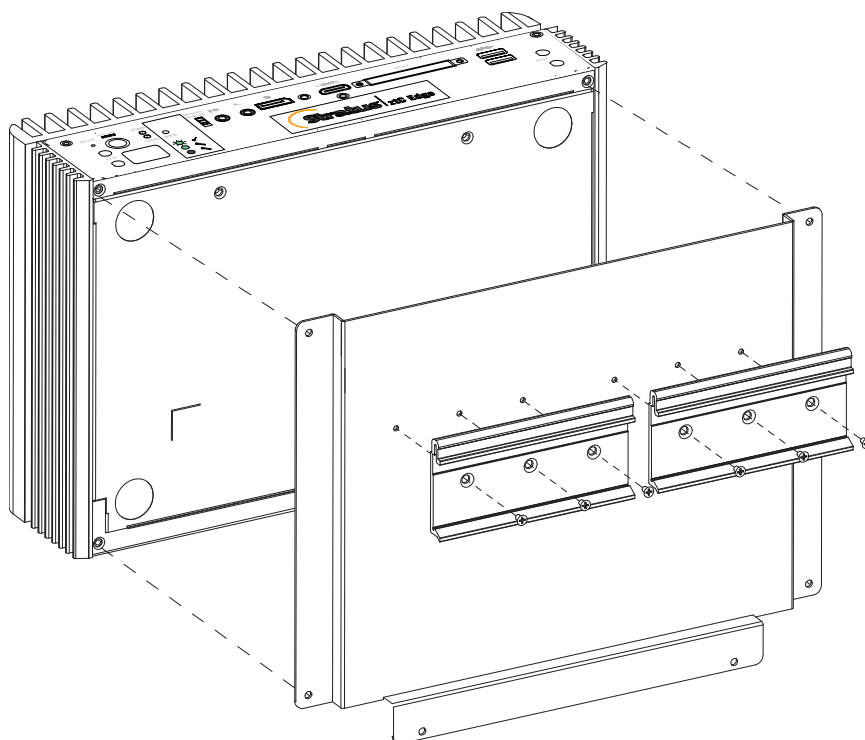
DIN レール マウントおよび壁かけブラケットの組み立て: ztC Edge 100i システム



注: DIN レール マウントまたは壁かけキットを ztC Edge ノードに取り付ける際は、Stratus ロゴの付いた面が上を向いていることを確認してください。

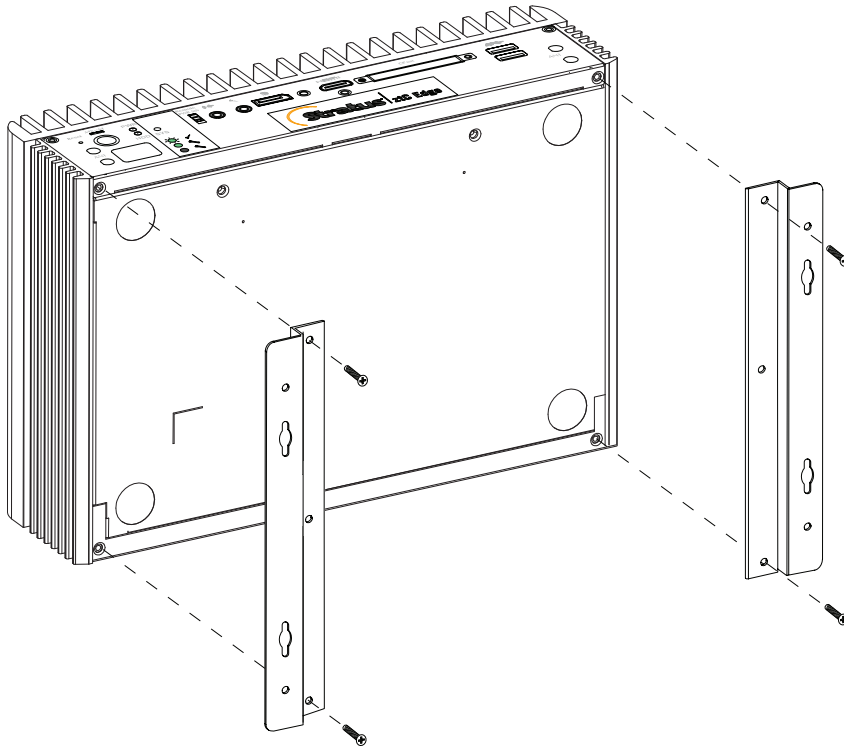
DIN レール マウント キットを取り付けるには

- ノードの底面から 4 本の皿ネジ M3 x 6mm (左右 2 本ずつ) を取り外します。
- アクセサリ ボックスにある 4 本の丸ネジ M3 x 6mm を使って、DIN レール マウント プレートを ノードに固定します。
- アクセサリ ボックスにある 6 本の皿ネジ M3 x 6mm を使って、DIN レール マウント ブラケットを DIN レール マウント プレートに固定します。



壁かけキットを取り付けるには

- ノードの底面から 4 本の皿ネジ M3 x 6mm (左右 2 本ずつ) を取り外します。
- アクセサリ ボックスにある 4 本の丸ネジ M3 x 6mm を使って、壁かけブラケットをノードに固定します。



注: 石膏ボードや類似した材質にユニットをマウントする場合、ケーブルの重みによってユニットが壁から抜け落ちることのないようにアンカーを使用してしてください。使用できるネジの直径は最小 0.138 インチ (3.5 mm)、長さは最小 1.5 インチ (38.1 mm)、ネジ頭の直径は最小 0.216 インチ (5.5 mm) です。選択した壁用アンカーに対応するネジを必ず使用してください。

製品コンプライアンス

ztC Edge システムに関するコンプライアンス情報は、次のサイトに記載されています。

https://stratadoc.stratus.com/compliance_info/Compliance_Information_for_Stratus_Products.htm

全般的なネットワーク要件と構成



注: ALSR ネットワークの場合、追加の異なるネットワーク要件が適用されます。以下の情報に加えて、[「ALSR 構成を作成する」](#) も参照してください。

ztC Edge システムを展開する前に、お使いのネットワークで以下の要件が満たされていることを確認してください。

- ztC Edge システムは IPv6 マルチキャストを含む、完全な IPv4 および IPv6 プロトコル アクセスを使用します。このトラフィックが妨げられた場合、展開が失敗したり、ztC Edge システムを実行できなくなる可能性があります。

上記に加え、各ネットワーク タイプに固有の以下のトピックを参照してください。

- [「A-Link ネットワークとプライベートネットワークの要件」](#)
- [「ビジネス ネットワークと管理ネットワークの要件」](#)

ビジネス ネットワークと管理ネットワークの要件

単一ノード システムとデュアルノード システムで使用されるビジネス ネットワークおよび管理ネットワークには、以下の要件が適用されます。

- ネットワークは IPv6 ローカル リンク アドレス指定を使用します。
- ネットワークでは最大 9000 の MTU 値がサポートされます。
- ネットワークでボンディングまたは VLAN トランキングはサポートされません。
- 仮想マシン (VM) は IPv4、IPv6、またはその他のイーサネット プロトコルを使用できます。
- サイトで SLAAC または DHCPv6 が有効にされている場合、IPv6 ホスト アクセスにすべてのビジネス ネットワークを使用できます。
- ztC Edge コンソールにアクセスするには、ibiz0 を使用します。これはプライマリ管理物理マシン (PM) にマイグレーションする IPv4 アドレスです。デュアルノード システムの各 PM は管理ネットワーク上で独自の ibiz0 IPv4 アドレスも有しています。
- 各 PM に少なくとも 1 つのビジネス ネットワーク (これは管理ネットワークです) が必要です。

イーサネットトラフィックがデュアルノードシステムの各 PM と VM の間を妨げなく通信できるようにするには、次を行います。

- ビジネス ネットワークに接続されているスイッチ ポートが ARP パケット (余分な ARP パケットも含みます) をフィルタリングしないようにします。ztC Edge システムは、イーサネットスイッチにそのポート転送テーブルを更新して VM トラフィックを正しい PM 上の適切な物理イーサネットポートに転送するよう指示するために、ゲスト VM の代理で余分な ARP パケットを送信します。
- ビジネス ネットワークに接続されたスイッチ ポートは、イーサネット タイプ 0x8807 でレイヤ 2 のマルチキャスト (アドレス 01:E0:09:05:00:02) を許可する必要があります。
- RHEL または CentOS ゲストを構成して同じサブネットに複数の NIC を設定する場合、非対称ルーティングに起因するゲスト ネットワークの接続問題が発生することがあります。この問題を回避するには、ゲスト仮想マシン (VM) の **/etc/sysctl.conf** ファイルを変更します。以下の行を追加してファイルを保存したうえで PVM をリブートしてください。

- `net.ipv4.conf.default.rp_filter = 2`

- `net.ipv4.conf.all.rp_filter = 2`

- PM のホスト OS から `ifdown` コマンドを実行して一時的に VM のビジネス ネットワーク接続 (ibizx) を切断することはしないでください。この操作を行うと、物理インタフェースがそのブリッジから切断され、ネットワークを介して VM にアクセスできなくなります。代わりに `ifconfig down` コマンドを使用してください。
- ビジネス ネットワークに接続されたスイッチで、特定のビジネス リンクからもう片方の PM の対応するビジネス リンクへの MAC アドレスの移動を無効化するような MAC アドレスのセキュリティ機能が有効になってはいけません。
- フェールオーバー応答を最適化するには、システムに接続されているすべてのスイッチで、MAC のエイジング期限の値を 1 秒未満に設定します。

これらの要件を満たしていない場合や、VM がデュアルノードシステムの片方の ztC Edge PM からもう一方の PM にマイグレーションするときにスイッチがその転送テーブルを正しく更新できない場合には、VM で停電が発生し、VM との間でネットワークトラフィックが正しくやり取りされない可能性があります。

関連トピック

[「ネットワーク アーキテクチャ」](#)

[「ビジネス ネットワークと管理ネットワーク」](#)

A-Link ネットワークとプライベート ネットワークの要件

デュアルノード システムのみで利用可能な A-Link ネットワークおよびプライベート ネットワークには、以下の要件が適用されます。

- ネットワークは IPv6 ローカル リンク アドレス指定を使用します。
- ztC Edge システムの特定の PM 上のすべての A-Link ネットワークとプライベート ネットワークは、プロトコル フィルタリングなしでもう一方の物理マシン (PM) 上の対応するリンクと同じ L2 ブroadcast ドメインになければなりません。
- システムの 2 台の PM 間で送信されるイーサネット パケットは、通信が妨げられたりレート制限を受けないようにします。これらが L3 ネットワーク インフラストラクチャによってルーティングやスイッチングされていないことを確認してください。
- A-Link ネットワークの速度は、ビジネス ネットワークまたは管理ネットワークの速度と同じかそれ以上でなければなりません。
- PM 間におけるストレージ複製のためのネットワーク トラフィックは A-Link ネットワークを介して送信されます。
- プライベート ネットワークに ztC Edge エンドポイント以外のネットワーク ホストは接続されません。

関連トピック

[「A-Link ネットワークとプライベート ネットワーク」](#)

ztC Edge コンソールの要件

ztC Edge コンソールは、ztC Edge システム、その物理マシン (PM)、および仮想マシン (VM) をブラウザを使ってリモート管理する機能を提供します。

- 使用するコンピュータは、ztC Edge 管理ネットワークを含むサブネットにアクセスできなければなりません (これは **P1** というラベルのネットワーク ポートで有効にします)。
- サポートされるブラウザを使用してください。 [「対応しているインターネット ブラウザ」](#) を参照してください。

詳細については、 [「ztC Edge コンソールを使用する」](#) を参照してください。

対応しているインターネット ブラウザ

ブラウザを使用して ztC Edge コンソールに接続します。ztC Edge システムに対応しているブラウザのみを使用してください。対応していないブラウザを使用すると、内容が正しく表示されなかったり、ウィザードの一部が表示されないことがあります。

ztC Edge システムに対応しているブラウザは次のとおりです。

対応しているブラウザ	リリース
Microsoft Internet Explorer™	11.0.648 以上
Microsoft Edge	42.17134 以上
Mozilla® Firefox®	65.0 以上
Google® Chrome™	73.0 以上

電源の要件と考慮事項

Stratus では可用性を最大限に高めるため、ztC Edge のフォールトトレラント (FT) ソフトウェアを冗長な電源装置から電力を得る物理マシン (PM) つまりノードで実行することを強く推奨します。また、各 PM の電源装置をそれぞれ個別の電源に接続する必要があります。

同じ電源に接続する場合の構成例については、 [「電源を接続する」](#) の図解を参照してください。

展開

システムの展開を初めて行う場合、次を実行します。



注: システムの展開と構成が済んでいて、これを新しいサイトでの展開用に準備する必要がある場合、「[ztC Edge システムを再展開する](#)」を参照してください。

1. ネットワークケーブルの接続に関する情報を確認します。必要に応じて、ネットワークを変更します。「[イーサネットケーブルを接続する](#)」を参照してください。
2. システムを展開します。「[システムを展開する](#)」を参照してください。

展開が完了したら、「[展開後のタスク](#)」を参照してください。

関連トピック

[「Stratus Redundant Linux ソフトウェアをアップグレードする」](#)

電源を接続する

電源を接続するには、2 つのノードで構成されている ztC Edge システムに、それぞれ別の電源に接続された冗長な電源装置を構成します。オプションで下記に示すように無停電電源装置 (UPS) を使用することもできます。単一ノードシステムの 1 つのノードを UPS に接続する方法を示す図は、「**2 台の UPS**」の下にある node0 の接続を参照してください。

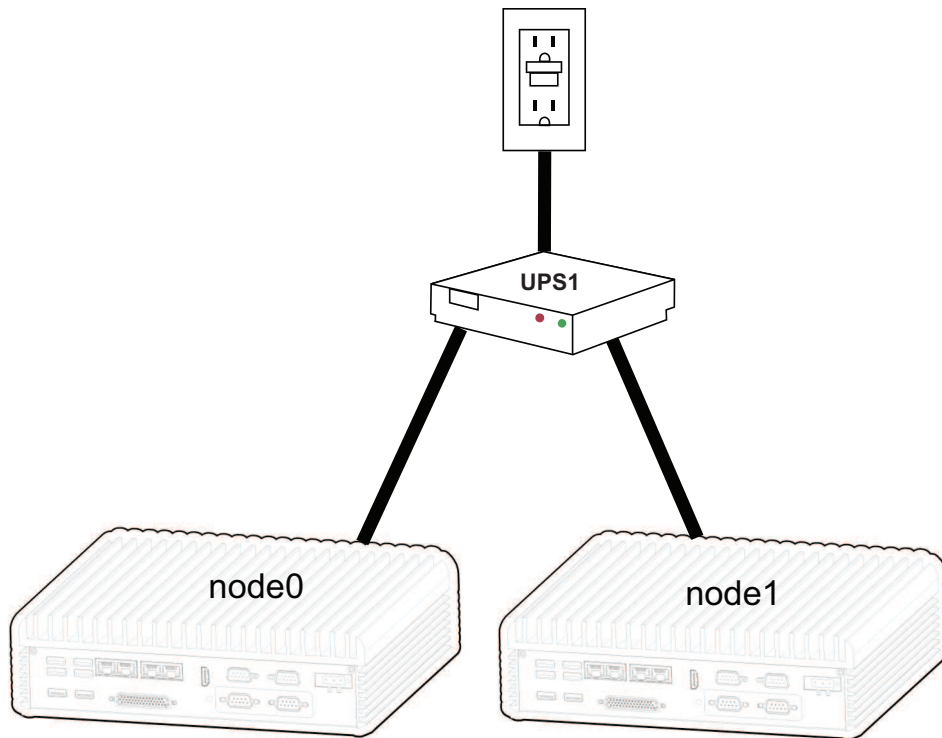
電源を接続した後、「[システムを展開する](#)」に戻ります。

UPS (オプション)

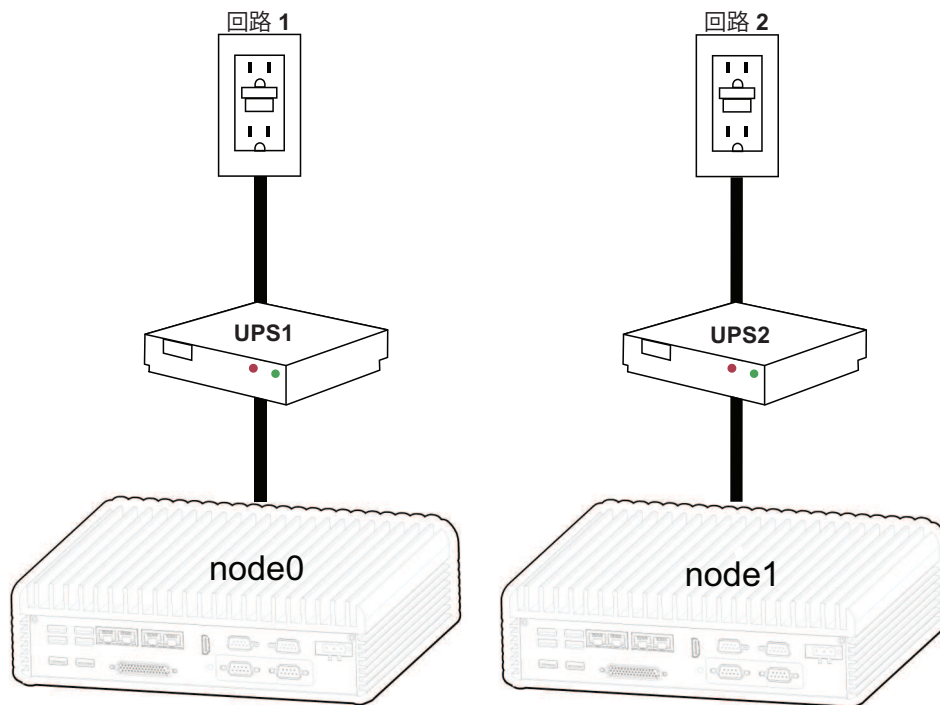
次の図は、1 台または 2 台のオプションの UPS ユニットを、2 つのノードで構成されている ztC Edge システムに接続する方法を示します。



注: Stratus では、個別の独立した電源に接続されている 2 台の UPS ユニットの使用を推奨します。2 つの電源を使うことにより、一方に障害が発生しても、システムには継続して電源が供給されます。

1 台の UPS:

2 台の UPS:



関連トピック

[「電源の要件と考慮事項」](#)

システムを展開する

このトピックでは ztC Edge システムを展開する方法について説明します。これは、お使いのシステムの [展開ガイド](#)にある情報を補足するものです。(1 つのノードをもつシステムでは、システムが既に実行中で 2 つ目のノードを追加する必要がある場合、[「単一ノードシステムにノードを追加する」](#)を参照してください。)



前提条件: 以下の手順では、リリース 2.3 以降でインストールされた工場出荷時状態のノードを展開する方法を説明します。廃止されたシステムからの既存のノードや、以前のソフトウェアリリースでインストールされたノードを展開する必要がある場合は、展開する前にノードを工場出荷時の状態にリセットする必要があります。必要な場合は、担当の Stratus 認定サービス業者にヘルプを依頼してください。

システムを展開するには

1. キーボードとモニタをノードに接続し、P1 ポートを既存の LAN に接続した後、ノードに電源を接続します (お使いのシステムの[展開ガイド](#)のステップ 1)。
2. ノードは自動的に電源がオンになります。オンにならない場合、電源ボタンを押します (お使いのシステムの[展開ガイド](#)のステップ 2)。ブート中にノードがビープ音を発する場合がありますが、これは正常な動作です。
3. **ztC Edge 展開ウィザード**で、**Enter** を押してシステムの展開を開始し、画面の指示に従います (お使いのシステムの[展開ガイド](#)のステップ 3)。
4. キーボード マップの選択を求めるウィンドウが表示されます。**Tab**、矢印、または **Esc** キーを使って次のいずれかを選択します。

- **Germany - map = DE (ドイツ)**
- **Japan - map = JP106 (日本)**
- **USA - map = US (米国) (デフォルト)**

Tab キーを使って **[OK]** に移動し、**Enter** キーを押します。



注: キーボード マップは初期展開の後でも選択したり変更できます。詳細については、「[キーボードをマッピングする](#)」を参照してください。

5. このノードのネットワークアドレスを構成する方法の選択を求めるメッセージが画面に表示されます。**Tab**、矢印、または **Esc** キーを使って次のいずれかを選択します。
 - **Automatic configuration via DHCP (DHCP による自動構成)** (デフォルト) — P1 を動的な IP 構成として構成するにはこの方法を選択します。
 - **Manual configuration (Static Address) (手動構成 (静的アドレス))** — P1 の IP アドレスを提供する場合はこの方法を選択します。値を入力するダイアログ ボックスが開きます。値は担当のネットワーク管理者から入手してください (これらのアドレスはお使いのシステムの[展開ガイド](#)の「[ユーザが提供するコンポーネント](#)」セクションに記録されている場合もあります):
 - このノードの IP アドレス
 - このノードのサブネット マスク
 - デフォルト ゲートウェイ (オプション)

入力した情報が無効な場合、有効な情報が入力されるまで同じダイアログ ボックスが再表示されます。

Tab キーを使って **[OK]** (または **[戻る]**) に移動し、次に **Enter** キーを押します。

6. 確認のダイアログ ボックスが表示されます。矢印キーまたは **Tab** キーを使用して、**[保存]** (デフォルト) に移動して表示された値を保存します (あるいは前のウィンドウに戻るには **[戻る]** に移動します)。次に、**Enter** キーを押します。

値を保存した場合、青い画面が数秒間表示されます。

7. 画面には最大 5 分間さまざまなステータス メッセージが引き続き表示されます。
8. 画面に Web ブラウザの IP アドレスに接続する指示が表示されます (お使いのシステムの[展開ガイド](#)のステップ 4)。IP アドレスをメモします。これは ztC Edge コンソールにログインする際に必要となります。

ノードに接続されたモニタには追加のプロンプトが表示されません。P1 を動的な IP 構成として構成した (ノードのネットワーク アドレスの上で **[Automatic configuration via DHCP (DHCP による自動構成)]** を選択した) 場合、[「管理 IP アドレスを記録する」](#)の説明に従って、その IP アドレスを記録します。



注: ネットワーク設定の構成を誤った場合 (たとえば IP アドレスの入力ミスなど) には、**[1]** キーを押して手順をやり直し、問題を修正することが可能です。

展開を完了するには、[「ztC Edge コンソールに初めてログオンする」](#)を参照してください。

展開ガイド

[ztC Edge 100i/110i システム: 単一ノード システムを展開する \(R014Z\)](#)

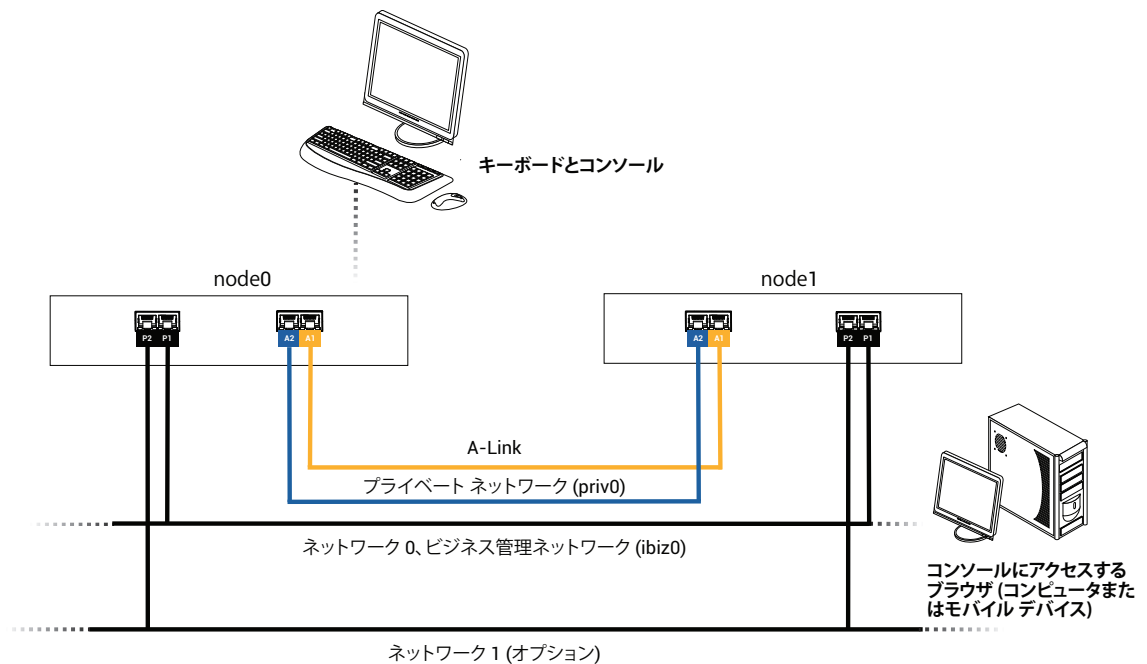
[ztC Edge 200i/250i システム: 単一ノード システムを展開する \(R017Z\)](#)

イーサネット ケーブルを接続する

ztC Edge システムを展開する場合、イーサネット ケーブルを接続する必要があります。次の図は、2 つのノード用に構成されているシステムのネットワーク構成のためのイーサネット ケーブルの接続を示しています。(キーボードとコンソールは node0 と node1 のどちらにでも接続できます。この図では node0 に接続されています。)1 つのノード用に構成されているシステムでは、下記の手順に従ってイーサネット ケーブルを network0 (ibiz0) の **P1** に接続し、オプションで network1 (ibiz1) の **P2** に接続します。



注: イーサネットポート **P1** および **P2** と、ポート **A1** および **A2** は、ノードの機種によってノードの前面または後面にあります。また、ノードのモデルによってはノードに **P1** と **P2** 以外のポートがある可能性もあります。



システムを展開する際 (「[システムを展開する](#)」を参照)、次を接続します。

- **priv0** の青いケーブルで node0 上の内蔵ポート **A2** を node1 上の同じ内蔵ポートにつなぎます。
- A-Link1 の黄色いケーブルで node0 上の内蔵ポート **A1** を node1 上の同じ内蔵ポートにつなぎます。

network0 (ibiz0) では、イーサネットケーブルで各ノード上の **P1** を、リモート管理コンピュータからアクセス可能なネットワークに接続します。オプションの network1 (ibiz1) では、イーサネットケーブルで各ノード上の **P2** を、追加のネットワークに接続できます。

これらの接続の準備として、ネットワーク内に必要な変更がある場合、これらの変更を行います。その後、「[システムを展開する](#)」にある次の手順を実行します。

関連トピック

[「展開」](#)

[「A-Link ネットワークとプライベートネットワークの要件」](#)

[「ビジネス ネットワークと管理ネットワークの要件」](#)

[「ztC Edge コンソールの要件」](#)

キーボードをマッピングする

展開後に、キーボードを構成してレイアウトを変更できます。

以下のキーボード レイアウトがサポートされています。

レイアウト	言語
de	ドイツ語
de-latin1	ドイツ語 (latin1)
de-latin1-noddeadkey	ドイツ語 (latin1 デッド キーなし)
dvorak	Dvorak
jp106	日本語
sg	ドイツ語 - スイス
sg-latin1	ドイツ語 - スイス (latin1)
uk	英国
us	英語 - 米国
us-acentos	米国 (インターナショナル)

展開後にキーボード レイアウトを構成するには

1. 1 台目の PM に root としてログインします。
2. コマンド ラインから `localectl` コマンドを実行して正しいキーボード レイアウトを構成します。次はドイツ語のキーボード レイアウトを構成する場合の例です。

```
# localectl set-keymap de
```

3. 2 台目の PM (存在する場合) で上記の手順を繰り返します。

関連トピック

[「展開後のタスク」](#)

管理 IP アドレスを記録する

システム IP アドレスを構成するために、ネットワーク管理者が各物理マシン (PM) の管理 IP アドレスを必要とする場合があります。この手順は、動的な IP アドレスを使用するように管理ネットワークが構成されている場合に実行します。(管理ネットワークに静的な IP アドレスを使用している場合、ネットワーク管理者は既にこの情報を把握しています。)

1. PM のインストールとリブートが完了すると、次のような画面が表示されます。

```
ztC Edge

IPv4 address 10.84.52.117

IPv6 address 3d00:feed:face:1083:225:64ff:fe8d:1b6e

IPv6 address fe80::225:64ff:fe8d:1b6e
```

2. 画面に表示された IPv4 アドレスを記録します。
3. この IP アドレスをネットワーク管理者に提供します。

[「システムを展開する」](#) に戻って展開を続行します。

関連トピック

[「ビジネス ネットワークと管理ネットワークの要件」](#)

展開後のタスク

システムの展開が完了した後、次のような展開後のタスクをいくつか実行する必要があります。

- 「システム IP 情報を取得する」
- 「ztC Edge コンソールに初めてログオンする」
- 「システムを登録して恒久ライセンスを入手する」
- 必要なシステムの基本設定を構成する
 - 「日付と時刻を構成する」
 - 「リモート サポート設定を構成する」
 - 「クォーラム サーバを構成する」
 - 「所有者情報を指定する」
- 「Active Directory を構成する」
- 「ローカル ユーザ アカウントを管理する」



注: パスワードを忘れた場合の回復機能を有効にするには、**admin** も含めて各ユーザ アカウントに電子メール アドレスを指定する必要があります。電子メール アドレスを指定していないユーザがコンソールのログイン ページで「**パスワードをお忘れですか?**」リンクをクリックした場合、システムは **user@example.com** に電子メールを送信します。ユーザの追加、ユーザ アカウントの編集、電子メール アドレスの追加を行う方法については、「**ローカル ユーザ アカウントを管理する**」を参照してください。

- 「ダッシュボードで未対応のアラートを解決する」
- 「2 番目のビジネス ネットワークを接続する」

状況によっては、以下の追加の作業が必要になります。

- 「ztC Edge システムを再展開する」
- 「単一ノード システムにノードを追加する」

システム IP 情報を取得する

システムを展開した後、ztC Edge コンソールに初めてログオンするために node0 の IP アドレスが必要になります (「**ztC Edge コンソールに初めてログオンする**」を参照してください)。初めてのログオンを完了させるには、システム IP 情報も必要です。この情報はネットワーク管理者から提供されます。ネットワーク管理者がシステム IP 情報を特定できるよう、node0 と node1 (存在する場合) の IP アドレス

をネットワーク管理者に提供します (「[管理 IP アドレスを記録する](#)」を参照してください)。システム IP アドレスは静的な IP アドレスでなければなりません。動的な IP アドレスは使用しないでください。

関連トピック

[「展開」](#)

[「展開後のタスク」](#)

ztC Edge コンソールに初めてログオンする

システムを展開する際、ztC Edge コンソールにログオンしてエンドユーザ ライセンス契約 (EULA) に同意し、ネットワーク情報を提供します。このときシステムを登録して恒久ライセンスを入手できます。ただし、これは後日改めて行うことも可能です。システムの初回インストール時には、期限が 30 日以内に指定された一時的なライセンスが設定されています。

ztC Edge コンソールに初めてログオンするには

1. ネットワークに接続された PC またはラップトップから、ブラウザのアドレス バーに node0 (プライマリ) の IP アドレスを入力します (お使いのシステムの[展開ガイド](#)のステップ 5)。



注: セキュリティ メッセージが表示されたら、Web サイトに進みます。後でセキュリティ例外を追加して、メッセージを表示せずにサイトの読み込みを許可することもできます (「[セキュアな接続を構成する](#)」を参照)。

ztC Edge コンソールのログオン ページが表示されます。

2. **[ユーザ名]** に **admin**、**[パスワード]** に **admin** (または提供されている場合はその他の資格情報) を入力し、**[ログイン]** をクリックします。

Stratus ztC Edge エンド ユーザ ライセンス契約 (EULA) が表示されます。

3. EULA を読み、その内容に同意する場合は **[同意する]** をクリックします。EULA に同意しない場合、展開が中止されます。

[初期の構成] ページが **[構成]** の下に表示されます。

4. デフォルトでは **[通知]** の下の **[サポート通知の有効化]** ボックスがオンになっています。ztC Edge システムから Stratus 認定サービス業者に稼動状態とスタータスの通知が送信されないようにするには、このチェック ボックスをオフにします。この設定は後でも変更できます (「[リモート サポート設定を構成する](#)」を参照してください)。

5. **[システム IP]** の下で、**[静的なシステム IP]** ボックスに、ネットワーク管理者から受け取った静的なシステム IP アドレスを入力します (お使いのシステムの[展開ガイド](#)の、「**ユーザが提供するコンポーネント**」セクションを参照してください)。(システム IP アドレスは、クラスタ IP アドレスとも呼ばれます。)

6. また、**[システム IP]** の下で、**[DHCP]** (デフォルト) または **[静的]** を選択します。**[DHCP]** の場合、追加の情報を入力する必要はありません。

[静的] を選択した場合、展開処理中に入力した node0 の静的 IP アドレスが表示されます。次の値を指定します (お使いのシステムの[展開ガイド](#)で、「**ユーザが提供するコンポーネント**」セクションを参照してください)。

- プライマリおよびセカンダリ DNS
- ネットマスク
- node0 のゲートウェイ アドレス

ネットワークの情報を入力したら、**[続行]** をクリックします。数秒後に **[ライセンス情報]** ウィンドウが表示されます。

7. このときシステムを登録して恒久ライセンスをインストールできます (お使いのシステムの[展開ガイド](#)のステップ 6)。この作業は後で行うこともできます。「[システムを登録して恒久ライセンスを入手する](#)」を参照してください。
8. 登録が完了したら **[完了]** をクリックします。**[アカウントのセキュリティ]** ウィンドウが表示されます。
9. **[アカウントのセキュリティ]** ウィンドウの **[新しいパスワード]** に、ユーザ **admin** の新しいパスワードを入力します。**[パスワードの確認]** にもう一度パスワードを入力します。パスワードはシステムのパスワード ポリシーに準拠しなければなりません (詳細は「[パスワード ポリシー](#)」を参照してください)。

注:



- セキュリティ上の理由から、このとき **admin** のパスワードを変更する必要があります。パスワードは後で再変更できます。また、**admin** アカountのデフォルトのユーザ ログイン名も変更することをお勧めします。これらの変更は **[ユーザとグループ]** ページで行います (**[ユーザとグループを構成する]** を参照してください)。
- セキュリティをさらに強化するため、展開の後にはできるだけ早く各 PM のホストオペレーティングシステムで **root** のパスワードを変更します (**[ホストオペレーティングシステムにアクセスする]** を参照)。

10. **[完了]** をクリックします。

ztC Edge コンソールが表示されて初回ログオンが完了します。今後コンソールにログオンする際に使用できるよう、このシステム IP アドレスはブックマークに保存するか、メモします。

必要に応じて、**[展開後のタスク]** の追加のタスクを実行します。

関連トピック

[「展開」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

展開ガイド

[ztC Edge 100i/110i システム: 単一ノード システムを展開する \(R014Z\)](#)

[ztC Edge 200i/250i システム: 単一ノード システムを展開する \(R017Z\)](#)

ノードを追加するためのガイド

[ztC Edge 100i/110i システム: ノードを追加する \(R015Z\)](#)

[ztC Edge 200i/250i システム: ノードを追加する \(R018Z\)](#)

システムを登録して恒久ライセンスを入手する

恒久ライセンスの入手も含め、システムを登録する必要があります。システムの初回展開時には、期限が 30 日以内に指定された一時的なライセンスが設定されています。(一時ライセンスはマストヘッドの **[アセット ID]** に **UNREGISTERED_TRIAL** として表示されます。) システムの登録は ztC Edge コン

ソールに初めてログオンするとき、その後で行うことができます。この作業はインターネット アクセスの有無に関わらず実行することができます。

インターネット アクセスのないシステムの場合、(インターネット アクセスのない) コンソールのロケーションと、インターネット アクセスのあるロケーションの間でファイルを移動する必要があります。以下に 2 つの方法を示しますが、他の方法で行うことも可能です。

- USB フラッシュ ドライブ – (システムに接続可能な) 管理 PC と、インターネット アクセスのあるコンピュータの間で USB フラッシュ ドライブを移動します。
- ラップトップやスマートフォンなどのモバイル デバイス – ztC Edge コンソールにログインできるロケーションと、インターネット アクセスのあるロケーションとの間でモバイル デバイスを移動します。



前提条件: システムを登録する前に、「[登録ポータルの手順を完了するには](#)」を読み、必要な情報がすべて手元にあることを確認してください。

登録ポータルの手順を完了するには

Step 1: General Information (ステップ 1: 一般情報) — 次の情報を入力します。

- **First Name (名)** および **Last Name (氏)**
- **Company Email (会社電子メール)** — 最終展開サイトである会社の所在地を使用します。個人の電子メール アドレスは使用しないでください。

Service Terms (契約条件) を確認して同意する必要もあります。

Step 2: Location Info (ステップ 2: ロケーション情報) — 次の情報を入力します。

- **End User Company Name (エンドユーザの会社名)** — システムを展開する会社の名前を入力します。
- **Deployment Shipping Address (展開の配送住所)** — 交換パーツの配送先となる住所を入力します。最終展開サイトである会社の所在地を使用します。私書箱は使用しないでください。次のフィールドがあります。
 - **[Address 1 (番地 1)]** と **[Address 2 (番地 2)]**
 - **[City (市区町村)]**、**[State (都道府県)]**、**[Postal Code (郵便番号)]**、**[Country (国)]**
 - **[Special Instructions (特記事項)]** (たとえば「発送センター 2 に配達すること」など)

Step 3: Contact Detail (ステップ 3: 連絡先詳細) — 次の情報を入力します:

- **Primary Technical Contact (1 次技術担当)** および **Secondary Technical Contact (2 次技術担当)** — Stratus 認定サービス業者との連絡を担当する技術者の名前を入力します。
- **Service Renewal Contact (サービス更新担当者)** — 毎年のサービス契約更新業務担当者の名前を入力します。

各担当者につき **[First Name (名)]**、**[Last Name (氏)]**、**[Email Address (電子メール アドレス)]**、**[Desk Phone (社内電話番号)]**、および **[Mobile (optional) (携帯 (オプション))]** を入力します。後で **Stratus カスタマ サービス ポータル** (<https://support.stratus.com>) を使用して連絡先を追加できます。

ページ下部の **[Next (次へ)]** をクリックすると、Stratus が情報を検証します。

情報に問題がある場合、**[Problem Encountered (問題が発生しました)]** パネルが開いて問題の説明が表示されます。可能であれば、**[Back (戻る)]** をクリックして問題を修正します。問題

が解決しない場合は **[Next (次へ)]** をクリックして続行すると、登録を完了するためのファイルをダウンロードできるようになります。問題を解決してアカウントを正しく設定できるよう、Stratus 認定サービス業者から連絡を差し上げます。

[Information Verification (情報検証)] ページが表示されます。ここで情報を確認することができます。情報を変更するには **[Back (戻る)]** をクリックします。情報を送信して登録を完了するには **[Next (次へ)]** をクリックします。

[Step 4: License Key (ステップ 4: ライセンス キー)] — インターネット アクセスのあるシステムの場合、ztC Edge コンソールの **[製品ライセンス]** ページをチェックしてライセンスが自動的に恒久ライセンスに更新されることを確認します。インターネット アクセスのないシステムの場合、**[Download License (ライセンスのダウンロード)]** をクリックしてライセンス キー ファイルをダウンロードし、これを ztC Edge システムにインストールします。ファイルをダウンロードした場所は必ずメモしてください。

システムを登録して恒久ライセンスを入手するには

インターネット アクセスのあるシステムの場合

1. コンソールに初めてログインしてシステムを登録する場合、次の手順から開始します。展開後にシステムを登録する場合、次の手順を実行します。
 - a. ztC Edge コンソールで、左側のナビゲーション パネルの **[基本設定]** をクリックします。
 - b. **[基本設定]** ページで **[製品ライセンス]** をクリックします。
2. **[オンラインのライセンス登録とアクティベーション]** で、**[オンライン登録]** をクリックして、新しいブラウザ タブを開いて Stratus 登録 Web ポータルを表示します。その後、[登録 Web ポータルの手順](#)を完了します。

ステップ 4 で、ztC Edge コンソールの **[製品ライセンス]** ページをチェックしてライセンスが自動的に恒久ライセンスに更新されることを確認します。必要に応じて **[ライセンスを今すぐチェック]** をクリックします。**[ステータス]** が **[ライセンスはアクティベートされています。有効期限はありません]** に変わり、登録が完了します。ライセンスが 5 分以内に正しく更新されない場合、登録用 Web ポータルの **[Download License (ライセンスのダウンロード)]** をクリックしてライセンス キー ファイルをダウンロードし、次のステップに進みます。

3. ztC Edge コンソールの **[製品ライセンス]** ページで、**[オフラインのライセンス チェックとライセンスの手動インストール]** を展開します。

4. **[アクティベート済みライセンス キーのシステムへのインストール]** で、**[ファイルの選択]** をクリックし、ファイルを保存した場所に移動します。
5. ファイルを選択して **[開く]** をクリックし、次に **[アップロード]** をクリックしてシステムにファイルをアップロードします。ライセンスが恒久ライセンスに更新されることを確認します。**[ステータス]** が **[ライセンスはアクティベートされています。有効期限はありません]** に変わり、登録が完了します。

インターネット アクセスのないシステムの場合

システムがインターネットにアクセスできない場合、ztC Edge コンソールの (インターネット アクセスのない) ロケーションと、インターネット アクセスのあるロケーションの間でファイルを移動する必要があります。次の手順は 1 つの方法を示しますが、他の方法で行うことも可能です。

ztC Edge コンソールにアクセスできるコンピュータまたはモバイル デバイスでの手順

1. 管理 PC を使用する場合、USB ポートに USB フラッシュ ドライブを挿入します。
モバイル デバイスを使用する場合、これが ztC Edge コンソールにアクセスできることを確認します。
2. コンソールに初めてログインしてシステムを登録する場合、次の手順から続行します。展開後にシステムを登録する場合、次の手順を実行します。
 - a. ztC Edge コンソールにログオンします。
 - b. 左側のナビゲーション パネルで **[基本設定]** をクリックします。
 - c. **[基本設定]** ページで **[製品ライセンス]** をクリックします。
3. ステップ 1、**[URL ファイルによるオフラインのライセンス登録]** (**[オフラインのライセンス登録とライセンスの手動インストール]** バーの下) で、**[URL ファイルのダウンロード]** をクリックして **register_site_file.html** ファイルを USB フラッシュ ドライブまたはモバイル デバイスに保存します。USB フラッシュ ドライブを使用している場合はドライブを取り出します。
4. インターネット アクセスのある場所に移動します。

インターネット アクセスのある場所での手順

1. USB フラッシュ ドライブを使用している場合、これをインターネット アクセスのあるコンピュータの USB ポートに挿入します。

2. 保存したファイルに移動し、ファイル名をクリックします。ブラウザでファイルが開き、Stratus 登録 Web ポータルにリダイレクトされます。[登録 Web ポータルの手順](#)を完了します。

ステップ 4 で、恒久ライセンスのキー ファイルをダウンロードして USB フラッシュ ドライブまたはモバイル デバイスに保存します。USB フラッシュ ドライブを使用している場合はドライブを取り出します。

3. コンソールにアクセスできる場所に戻ります。

ztC Edge コンソールにアクセスできるコンピュータまたはモバイル デバイスでの手順

1. USB フラッシュ ドライブを使用している場合、これを管理 PC の USB ポートに挿入します。

モバイル デバイスを使用する場合、これが ztC Edge コンソールにアクセスできることを確認します。

2. コンソールで、左側のナビゲーション パネルの **[基本設定]** をクリックします。
3. **[基本設定]** ページで **[製品ライセンス]** をクリックします。
4. ステップ 2、**[アクティベート済みライセンス キーのシステムへのインストール]** (**[オフラインのライセンス登録とライセンスの手動インストール]** バーの下) で、**[ファイルの選択]** をクリックして、ライセンス キー ファイルを保存した場所に移動します。
5. ファイルを選択して **[開く]** をクリックし、次に **[アップロード]** をクリックしてシステムにファイルをアップロードします。

コンソールに初めてログインしている場合、ライセンスをアップロードした後で「[ztC Edge コンソールに初めてログオンする](#)」の最後の手順に戻ります。

関連トピック

[「ztC Edge コンソールに初めてログオンする」](#)

[「製品ライセンスを管理する」](#)

ztC Edge システムを再展開する

システムの展開と構成が既に完了していて、新しいロケーションなどで異なるネットワークやサブネットに展開するための準備としてシステムのネットワーク設定をリセットする必要がある場合、ztC Edge システムを再展開します。

通常、新しい ztC Edge システムの再展開は、エンド ユーザのために設定と仮想マシン (VM) を準備した後で、エンド ユーザが自分のサイトに初めてシステムを展開できるように、ネットワークの設定をリセットしなければならない場合に行います (これは Windows の Sysprep ユーティリティを使ってエンド ユーザの初回展開や Out-Of-Box Experience (OOBE) のために Windows システムを準備するのと同じです)。

エンド ユーザのためにシステムを構成した後、ztC Edge コンソールで再展開を開始します。その後システムは、システムとノードのネットワーク設定をクリアして、実行中のすべての VM をシャットダウンし、システムの電源を切ります。システムではネットワーク以外のシステム設定と構成した VM が維持されますが、システムに適した[展開ガイド](#)で説明されているように、展開の準備が完了します。

注:

ztC Edge システムを再展開する場合、以下の問題と解決方法に注意してください。

- システムを再展開する前に NFS/CIFS 共有を無効にします。

アクティブな NFS/CIFS 共有は再展開機能に干渉します。新しいネットワークでのネットワーク設定構成を完了するまで共有を無効にしてください。

- 新しい静的なシステム IP アドレスを設定する際はシステムのリブートが必要です。

システムを再展開してからシャットダウンし、新しいロケーションで起動した後で新しい静的なシステム IP アドレスを構成した場合、システムはセカンダリ ノードへのアクセスを失います。セカンダリ ノードへのアクセスを再取得するには、**[システム]** ページを開いて **[リブート]** をクリックし、システムをリブートします。システムをリブートするとセカンダリ ノードのゲートウェイ設定がリフレッシュされ、システムに接続できるようになります。

- 新しいネットワークに移動済みのシステムで、その前に再展開を行わなかった場合には、KB-[8283](#) でシステムを再展開する手順を参照してください。
- 単一の使用ノードを新しいネットワークの最初のノードとして、あるいは別のシステムで 2 つ目のノードとして再展開する必要がある場合、KB-[9391](#) の手順を参照してください。

ztC Edge システムを再展開するには

1. エンド ユーザのためにシステムを準備します。ztC Edge システムの設定を構成して必要に応じて VM を作成します。(システムを再展開すると、ネットワーク設定のみがクリアされます。)

2. システムの準備が完了したら、ztC Edge コンソールで **[基本設定]** ページを開いて **[IP 構成]** をクリックし、次に **[再展開]** をクリックします。
3. システムは、システムとノードのネットワーク設定をクリアして、実行中のすべての VM をシャットダウンし、システムの電源を切ります。
4. これでエンド ユーザによるシステム展開の準備が完了します。システムを展開するには、システムに適した **展開ガイド** を参照してください。(必要な場合、詳細については「**システムを展開する**」を参照してください。)

関連トピック

[「展開」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

展開ガイド

[ztC Edge 100i/110i システム: 単一ノード システムを展開する \(R014Z\)](#)

[ztC Edge 200i/250i システム: 単一ノード システムを展開する \(R017Z\)](#)

単一ノード システムにノードを追加する

このトピックでは、システムに 2 つ目のノードを追加して、冗長なシステムを作成する方法を説明します。これは、「[ノードを追加するためのガイド](#)」にある、お使いのシステム用の情報を補足するものです。(システムを初めて展開する必要がある場合には、「[展開](#)」を参照してください。)

前提条件: この手順を完了するには次のものがが必要です。



- Stratus Redundant Linux リリース 2.3.0.0 以降がインストールされ、1 つ目 (稼働中) のノードのモデルと一致する、2 つ目の工場出荷時状態の ztC Edge ノード。廃止されたシステムの既存のノードや、以前のソフトウェア リリースでインストールされたノードを使用する必要がある場合は、展開する前にノードを工場出荷時の状態にリセットする必要があります。必要な場合は、担当の Stratus 認定サービス業者にヘルプを依頼してください。
- 最初のノードを静的な IP アドレスで構成した場合、2 つ目のノード用の静的な IP アドレス。(現在のネットワーク構成は、ztC Edge コンソールの **[基本設定]** ページの **[IP 構成]** で確認できます。)

ノードを追加するには

1. 最初のノードが実行されていて正常である (SYS LED が点滅している) ことを確認します。最初のノードにネットワーク接続している PC またはラップトップで ztC Edge コンソールに接続し、**[ダッシュボード]** ページに緑のチェックマークが表示されていて未解決の問題がないことを確認します。2 つ目のノードを追加する前に、すべての問題を解決してください。



注: ステップ 6 で VM を再起動するまでは VM のパフォーマンスが低下するため、次の手順は計画的なメンテナンス期間まで待ってから実行することを検討してください。

2. 2 つ目のノードの P1 ポートを既存の LAN に接続し、青色と黄色のネットワークケーブルで最初のノードと 2 つ目のノード (A2 と A1 ポート) を接続します。2 つ目のノードに電源を接続し、ノードの電源がオンになることを確認します。ネットワーク構成に関する追加の情報については、**「イーサネットケーブルを接続する」** を参照してください。
3. 最初のノードに接続している ztC Edge コンソールで、**[基本設定]** を開いて **[可用性]** をクリックし、**[+]** (プラス記号) をクリックして 2 つ目のノードを追加します。ノードの追加ウィザードを完了し、ノードをペアリングしてシステムを冗長化します。以下は概要です:
 - a. **[準備]** タブで **[続行]** をクリックし、接続した 2 つ目のノードを検索します。
 - b. **[検出]** タブに、ウィザードで新しく検出された 2 つ目のノードに関する情報が表示されます。
 - ノードがペアリングに適した互換タイプの場合、**[続行]** をクリックしてペアリングの処理を開始します。
 - ノードがペアリングに適していない場合、**[キャンセル]** をクリックし、ウィザードに報告された問題をすべて修正してからウィザードを再起動します。



注: ノードのペアリングをする前に、**[ペアリングとサポート レベルの確認]**

ポップアップに表示される新しいサポート契約に同意する必要があります。契約に同意してペアリングを開始するには **[続行]** をクリックします。

- c. **[ペアリング]** タブで、システムがペアリングの処理を完了するのを待ちます。
 - d. **[完了]** ページで、ノードが冗長構成で正しくペアリングされたことを確認します。
4. ペアリングの完了には最大で 30 分かかります。その後、2 つ目のノードの SYS LED が点滅して正常な状態であることが示され、ノードの追加ウィザードの各タブに緑色のチェックマークが表示されてペアリングが成功したことを確認できます。**[閉じる]** をクリックしてウィザードを終了し、**[可用性]** ページを表示します。このページには **[冗長構成]** が **[有効]** であることが示され、

冗長な構成が表示されます。

5. ztC Edge コンソールの **[基本設定]** ページで、**[IP 構成]** をクリックしてネットワークの設定を確認します。必要に応じて、2 つ目のノード (**node1**) の静的 IP アドレスを入力し、**[保存]** をクリックします。
6. 既存の VM は数時間同期する可能性があります。その後、VM を再起動して冗長性を有効化し、警告を解除する必要があります。フォールトトレラント (FT) 運用をサポートするシステムでは、VM がダウンしている間にその保護レベルの設定 (HA/FT) を更新することを検討してください。詳細は、「[仮想マシンの保護レベルを変更する \(HA または FT\)](#)」を参照してください。システムが同期され、VM が実行されている場合、未解決の問題がないことを示す緑のチェックマークが **[ダッシュボード]** に表示されます。
7. まだ登録していない場合は、「[システムを登録して恒久ライセンスを入手する](#)」の説明に従って、システムを登録して製品の恒久ライセンスを取得してください。

システムが既に登録されていて、インターネットにアクセスできる場合は、2 つ目のノードのシリアル番号で製品ライセンスが自動的に更新されます。システムがインターネットにアクセスできない場合や、ライセンスをチェックするようアラートが表示された場合は、「[製品ライセンスを管理する](#)」の説明に従ってライセンスを更新してください。



注: 製品ライセンスが更新されるまで、システム ソフトウェアのアップグレードを行うことはできません。

ノードを追加するためのガイド

ztC Edge 100i/110i システム: [ノードを追加する \(R015Z\)](#)

ztC Edge 200i/250i システム: [ノードを追加する \(R018Z\)](#)

2 番目のビジネス ネットワークを接続する

ztC Edge システムを初めて展開する場合、各ノードの P1 ポートから既存のネットワークにネットワーク ケーブルをつなぎ、network0 という共有ビジネス/管理ネットワーク (ibiz0 と呼ばれます) を 1 つ作成します。

展開後に 2 番目の専用ビジネス ネットワーク (network1、あるいは ibiz1) を追加するには、ネットワーク ケーブルで各ノードの P2 ポートを既存のネットワークにつなぐことができます。

2 番目のビジネス ネットワークを追加することで、仮想マシン (VM) を個別のビジネス ネットワークに割り当てることが可能になり、複数の VM をもつシステムにおける負荷分散の改善に役立ちます。

network0 は管理トラフィックとビジネス トラフィックの両方を処理するため、network0 の負荷を減らすことでパフォーマンスの改善にもつながります。

2 番目のビジネス ネットワークを接続するには

1. ネットワーク ケーブルで各ノードの **P2** ポートを既存のネットワークにつなぎます。
2. ztC Edge コンソールで、**[ネットワーク]** ページを表示します。
 - a. 通常は 1 以内に新しい **network1** という接続が表示されます。
 - b. 新しい接続 **network1** に緑のチェックマークが表示されることを確認します。
3. 必要に応じて、**仮想マシンの再プロビジョニング** ウィザードを使って各 VM で **network1** を有効にします (場合によっては **network0** を無効にします)。詳細については、[「仮想マシンのリソースを再プロビジョニングする」](#) を参照してください。

関連トピック

[「イーサネット ケーブルを接続する」](#)

[「A-Link ネットワークとプライベート ネットワークの要件」](#)

[「ビジネス ネットワークと管理 ネットワークの要件」](#)

[「全般的な ネットワーク要件と構成」](#)

3

第 3 章: ztC Edge コンソールを使用する

ztC Edge コンソールは、ztC Edge システムの管理とモニタリングをリモートの管理コンピュータから行う機能を提供するブラウザベースのインターフェースです。このコンソールの概要については、[「ztC Edge コンソール」](#) を参照してください。

ztC Edge コンソール内の各ページに関する情報については、以下のトピックを参照してください。

- [「\[ダッシュボード\] ページ」](#)
- [「\[システム\] ページ」](#)
- [「\[基本設定\] ページ」](#)
- [「\[アラート履歴\] ページ」](#)
- [「\[監査ログ\] ページ」](#)
- [「\[サポート ログ\] ページ」](#)
- [「\[物理マシン\] ページ」](#)
- [「\[仮想マシン\] ページ」](#)
- [「\[ボリューム\] ページ」](#)
- [「\[ネットワーク\] ページ」](#)
- [「\[仮想 CD\] ページ」](#)
- [「\[アップグレードキット\] ページ」](#)

ztC Edge コンソール

ztC Edge コンソールは、ztC Edge システムの管理とモニタリングをリモートの管理コンピュータから行う機能を提供するブラウザベースのインタフェースです。システムに対するすべての管理操作をコンソールから実行でき、システム全体および個々の物理マシン (PM)、仮想マシン (VM)、およびその他のリソースにアクセスすることができます。

ztC Edge コンソールで実行されるリモート管理コンピュータの要件については、[「ztC Edge コンソールの要件」](#)を参照してください。

ztC Edge コンソールを使用して、次のさまざまな管理機能を実行できます。

- ダッシュボードからシステム アラートを確認します。[「\[ダッシュボード\] ページ」](#)を参照してください。
- [システム] ページから、VM、CPU、メモリ、およびストレージに関する統計を表示し、システムのリブートまたはシャットダウンを実行します。[「\[システム\] ページ」](#)を参照してください。
- システム、通知 (e アラートと SNMP 構成)、およびリモート サポート (通知とアクセス) の基本設定を指定して、セキュアな接続を作成できる管理ツールにアクセスします。システムの基本設定には、所有者情報と IP アドレス、クォーラム サービス、日付と時刻、などの構成値が含まれます。[「\[基本設定\] ページ」](#)を参照してください。
- アラートおよび監査ログを表示します。[「\[アラート履歴\] ページ」](#)、[「\[監査ログ\] ページ」](#)、[「\[サポート ログ\] ページ」](#)を参照してください。
- 以下のリソースのモニタリング、管理、およびメンテナンスを行います。
 - PM のステータス、ストレージ (ディスクも含む)、ネットワーク、VM、および USB デバイス。[「\[物理マシン\] ページ」](#)を参照してください。
 - VM のステータスおよび管理タスク。VM の作成、インポート/リストア、管理、およびメンテナンスを含みます。[「\[仮想マシン\] ページ」](#)を参照してください。
 - ボリューム。その状態、名前、データ同期のステータス、サイズ、状態、およびその他の情報を含みます。[「\[ボリューム\] ページ」](#)を参照してください。
 - ネットワーク。状態、リンク状況、名前、内部名、タイプ (A-Link など)、VM 速度、MAC アドレス、およびネットワーク帯域幅を含みます。[「\[ネットワーク\] ページ」](#)を参照してください。
 - 仮想 CD。その状態、名前、サイズ、および VCD が削除可能かどうかを含みます。[「\[仮想 CD\] ページ」](#)を参照してください。

- アップグレードキットのモニタリングと管理を行います。[「\[アップグレードキット\] ページ」](#)を参照してください。

ユーザ情報を編集 ([「ユーザ情報を編集する」](#)を参照) したり、ユーザとグループを構成 ([「ユーザとグループを構成する」](#)を参照) することもできます。

関連トピック

[「ztC Edge コンソールに初めてログインする」](#)

[「ztC Edge コンソールにログインする」](#)

[「ztC Edge コンソールを使用する」](#)

ztC Edge コンソールにログインする

ztC Edge コンソールにログインして、ztC Edge システムを管理します。コンソールを使用して、システムの物理マシン (PM)、仮想マシン (VM)、ストレージ、ネットワークなどを管理できます。アラートとログの確認や、その他の管理タスクを実行することもできます。

注:



1. 使用しない場合、ログインセッションは 1 時間後にタイムアウトします。
2. システムのログインセッション数は 10 に制限されています。
3. パスワードはシステムの [「パスワード ポリシー」](#) に準拠しなければなりません。
4. ztC Edge コンソールのログイン ページにカスタム コンテンツを提供するログイン バナーを構成できます。[「ログイン バナーを構成する」](#)を参照してください。

ztC Edge コンソールにログインするには

1. ブラウザのアドレス バーに、ztC Edge システムの IP アドレスまたは完全修飾ドメイン名 (FQDN) を次のように入力します。

http://<IP アドレス>

または

http://<FQDN 名>

<IP アドレス> は ztC Edge システムの静的 IP アドレスで、展開の処理中に指定されます。

<FQDN 名> はその IP アドレスに対応する FQDN 名です。

2. ログイン ページが表示されたら、**ユーザ名**と**パスワード**を入力します。

パスワードを忘れた場合、**[パスワードをお忘れですか?]** をクリックして **[パスワードのリセット]** ページを表示します。パスワードのリセットに必要な情報を入力します。



注: パスワードのリセットするには、ローカル ユーザ アカウントで構成されているように (**「ローカル ユーザ アカウントを管理する」** を参照)、システム上に電子メール アドレスのある電子メール アカウントを持っている必要があります。電子メールを受信できない場合、システム管理者に問い合わせてパスワード リセットの要求を代理で行ってもらいます。(システム管理者は、ホスト OS の管理者にパスワードの変更を依頼しなければなりません。ホスト OS の管理者はプライマリ ノードでコマンドを使ってパスワードを変更します。)

パスワードのリセットするには



注: パスワードのリセット時に電子メールを受信するには、メール サーバが構成されていなければなりません。 **「メール サーバを構成する」** を参照してください。

- a. **[パスワードのリセット]** ページが表示されたら、**[ユーザ名]** を入力して **[続行]** をクリックします。ローカル ユーザ アカウントに設定されている電子メール アドレスに電子メールが送信されます。電子メールにはパスワードのリセット ページへのリンクが含まれています。
- b. 電子メール アカウント内で、パスワード リセット リンクの含まれた電子メールを開き、リンクをクリックします。**[パスワードのリセット]** ページが再び表示されます。
- c. **[新しいパスワード]** と **[パスワードの確認]** に、新しいパスワードを入力します。新しいパスワードはシステムの **「パスワード ポリシー」** に準拠しなければなりません。
[続行] をクリックします。
- d. ページが開き、パスワードが正しくリセットされ、システムに新しいパスワードでログインできることを知らせるメッセージが表示されます。**[完了]** をクリックします。

3. **[ログイン]** をクリックします。

パスワード ポリシー

システムのパスワード ポリシーでは、パスワードが以下の条件を満たしている必要があります。

- パスワードは最低 8 文字です。
- 大文字と小文字の両方を含めなければなりません。
- ユーザ名と同じであってははいけません。



注: ログイン試行の間隔は 500 ms です。したがって、ログインを試行した後で少なくとも 0.5 秒待ってから再試行してください。

関連トピック

[「ztC Edge コンソールに初めてログオンする」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

ユーザ情報を編集する

ユーザ名、電子メール アドレス、実名、およびパスワードを変更してユーザ情報 (つまりユーザ プロファイル) を編集します。

ユーザ情報を編集するには

1. コンソールの右上角にあるユーザ名をクリックします。

[ユーザの編集] ダイアログ ボックスが開きます。

2. 次の値を入力または変更します。

- ユーザ名
- 電子メール アドレス
- 実名
- パスワード



注: パスワードはシステムの「パスワード ポリシー」に準拠しなければなりません。

- パスワードの確認

3. **[保存]** をクリックします。(または、変更をキャンセルするには **[キャンセル]** をクリックします。)


関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[ダッシュボード] ページ

[ダッシュボード] ページには、ztC Edge システムの未対応のアラートのサマリが表示されます。このページを開くには、左側のナビゲーション パネルで **[ダッシュボード]** をクリックします。

未処理のアラートに関する追加の情報を表示するには、ztC Edge システム図でアラート記号 (たとえば ) をクリックするか、システム図の下のアラートのリストでエントリをクリックします。アラート リストは、アラートの種類によってシステム図の下に **[すべて]**、**[システム]**、**[無視]** などのタブとして表示されることもあります。アラート情報には次が含まれます。

- 問題に関連するコンポーネント (たとえば ztC Edge システム、物理マシン (PM)、仮想マシン (VM) など)
- 対処が必要なアクティビティまたはタスクの説明
- 問題の解決が必要な理由 (該当する場合)

アクティブなアラートはできるだけ早期に解決してください ([「ダッシュボードで未対応のアラートを解決する」](#) を参照)。

ztC Edge システム図を理解する

[ダッシュボード] ページのシステム図は、システムのステータスを視覚的に示すものです。星印はプライマリ PM を表します。アラート記号がある場合、これは情報目的のアラートか、対処が必要な重要なアラートを表します。アラート記号をクリックすると、そのアラートに関する情報が表示されます。

関連トピック

[「\[物理マシン\] ページ」](#)

[「\[システム\] ページ」](#)

[「\[仮想マシン\] ページ」](#)

ダッシュボードで未対応のアラートを解決する

システムの展開を完了した後、[ダッシュボード] ページに表示される未対応のアラートをすべて解決します。

未対応のアラートを解決するには

ztC Edge コンソールの [ダッシュボード] ページの下部に表示されるアラートを確認します。次のオプションがあります。

- アラートを解決します。

たとえば、「**Stratus によるサポートを最大限に活用するには、サポート通知サービスを有効にする必要があります**」というメッセージが表示されている場合はサポート通知サービスを有効にします。

- ([**アクション**] 列で) [**無視**] をクリックして、アラートを無視してリストから削除します。軽度のアラートは解決せずに無視することができます。[**無視**] をクリックするとアラートが表示されなくなります。

無視したアラートをリストに再び表示するには、アラート リストの上にある [**無視**] をクリックしてから、[**アクション**] 列で [**リストア**] をクリックします。

関連トピック

[「\[ダッシュボード\] ページ」](#)

[システム] ページ

[**システム**] ページには、ztC Edge システムに関する情報が表示されます。このページからシステムのリブートやシャットダウンを行えます。このページには、ztC Edge システムの[統計](#)とリソースの割り当てが表示されます。このページを開くには、左側のナビゲーション パネルで [**システム**] をクリックします。

[**システム**] ページを使用して、次のような管理タスクを実行できます。

- [「システムをリブートする」](#)
- [「システムをシャットダウンする」](#)

システムの電源を (PM の物理コンソールで) オンにするには、[「システムの電源をオンにする」](#)を参照してください。

このほかにも ztC Edge システムの多くの管理タスクを ztC Edge コンソールを使用して実行します。詳細については、「[ztC Edge コンソール](#)」を参照してください。

統計を表示する

[システム] ページでは、システムの使用状況および PM と VM に関する情報と統計が以下のセクションに表示されます。

- **システム名** — 円グラフにシステムの CPU 割り当て、メモリ割り当て、ディスク (R/W)、およびネットワーク使用状況が表示されます。
- **node0** および **node1** (存在する場合) — 円グラフに各ノードの CPU 使用状況、メモリ使用状況、ディスク使用状況、およびネットワーク使用状況が表示されます。ディスク使用状況とネットワーク使用状況の場合、統計を表示したい論理ディスクまたはネットワークを選択できます。

関連トピック

[「ztC Edge コンソールを使用する」](#)

システムの電源をオンにする

ztC Edge システムの電源は各物理マシン (PM) またはノードの物理コンソールでオンにします。これを行うと、まずシステム ソフトウェアをブートしてからシステム上の仮想マシン (VM) を起動することにより、システムが正常に起動します。(システムの電源をオフにするには、「[システムをシャットダウンする](#)」を参照してください。)



注意事項: システムを初めて電源オンにして展開する場合、お使いのシステムの展開ガイドの手順に従います。(必要な場合、詳細については「[システムを展開する](#)」を参照してください。)



注: 電源コードを抜いたために PM の電源が失われたり、メインの AC 電源が失われた場合、デュアルノードシステム内の各 PM および単一ノードシステム内の 1 台の PM が、電源回復の直後に自動で電源オンになるよう設定されます。システム ソフトウェアと VM は自動的に再起動されます。

ztC Edge システムの電源をオンにするには

1. 必要なネットワークケーブルがすべて接続されていることを確認します。デュアルノードシステムの場合、両方の PM にネットワークケーブルが接続されていることを確認します。

2. システム内の PM でフロント パネルの電源ボタンを押します。
3. PM のフロント パネルの **PWR** LED または電源ボタンが点灯することを確認します。

関連トピック

[「ztC Edge コンソール」](#)

[「\[システム\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

システムをリブートする

ztC Edge コンソールを使用した ztC Edge システムのリブートでは、VM に影響を与えずに両方の PM を安全に再起動できます。単一ノード システムの場合、リブート中に仮想マシンがシャットダウンされて再起動されるため、システムのリブートは計画的なメンテナンス期間中のみに行ってください。



注意事項: それ以外の方法 (たとえば各 PM を個別にリブートするなど) を使って ztC Edge システムをシャットダウンすると、データを損失する可能性があります。



注: 2 台の PM で構成されているシステムをリブートできるのは、両方の PM が正常に実行されていて、メンテナンス モードに入っていない場合のみです。1 台の PM で構成されているシステムをリブートできるのは、その PM が正常に実行されていて、メンテナンス モードに入っていない場合のみです。



前提条件: 2 つのノードで構成されているシステムでは、リブートを行う前に、両方の PM が実行中であることを確認してください。単一ノード システムの場合、リブートする前にその PM が実行中であることを確認してください。

ztC Edge システムをリブートするには

1. 左側のナビゲーション パネルで **[システム]** を選択します。
2. **[リブート]** ボタンをクリックします。リブートを確認するメッセージが表示されます。**[はい]** をクリックして続行します。

リブートには最長 15 分かかります。進捗状況を ztC Edge コンソールの **[ダッシュボード]** およびマストヘッドで確認できます。システムの PM で順次メンテナンス モードが有効になってから

解除されます (メンテナンス モードの詳細については、[「メンテナンス モード」](#)を参照してください)。

3. PM が再起動され、すべての VM が引き続き正常に実行されることを確認します。

リブートを開始すると、マストヘッドのメッセージにリブートの進捗状況が表示されます。リブートをキャンセルするには、マストヘッドの **[リブートのキャンセル]** をクリックします。



注意事項: リブートをキャンセルするとシステムはその時点の状態のままになるため、手動で正常な状態に復元する必要があります。

関連トピック

[「ztC Edge コンソール」](#)

[「\[システム\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

システムをシャットダウンする

ztC Edge システムをシャットダウンするには ztC Edge コンソールを使用します。この方法では、まず仮想マシン (VM) をシャットダウンしてから物理マシン (PM) をシャットダウンすることにより、正常なシャットダウンが実行されます。ztC Edge システムをシャットダウンするには、この方法のみを使用してください。シャットダウンする前に、2 ノードで構成されているシステムの両方の PM か、あるいは 1 つのノードで構成されているシステムの (1 台の) PM が実行されていることを確認してください。

注意事項:



1. ztC Edge システムをシャットダウンすると VM がオフラインになるので、システムのシャットダウンは計画的なメンテナンス期間中のみに行ってください。
2. それ以外の方法で ztC Edge システムをシャットダウンすると (たとえば両方の PM の電源を遮断するなど)、データを損失する可能性があります。



注: システムをシャットダウンする際、スタンバイ電源が LOM のためにオンのままになります。ただし、電源コードを抜いたりメインの AC 電源がオフにされた場合は例外です。

ztC Edge システムをシャットダウンするには

1. 2つのノードで構成されているシステムでは、ディスクがノード間で同期されるように、両方のPMが実行中であることを確認します。
2. 左側のナビゲーション パネルで **[システム]** を選択します。
3. **[シャットダウン]** ボタンをクリックします。次の警告が表示されます:「システム全体がシャットダウンされ、1つ以上のVMが停止します! シャットダウンするには **[はい]** を、シャットダウンをキャンセルするには **[いいえ]** をクリックします。」 **[はい]** をクリックすると2つ目の警告メッセージが表示され、シャットダウンを確認するよう求められます。シャットダウンするには **[はい]** をもう1度クリックし、シャットダウンをキャンセルするには **[いいえ]** をクリックします。

ztC Edge コンソールの **[ダッシュボード]** およびマストヘッドでシャットダウン処理の一部を確認できます。システムのPMが順次メンテナンス モードに切り替わります (メンテナンス モードの詳細については、[「メンテナンス モード」](#)を参照してください)。ただし、システムが完全にシャットダウンするとztC Edge コンソールが使用不可能になり、マストヘッドに「**通信が失われました**」と表示されます。

システムのシャットダウンが完了すると、コンソールに接続できなくなります。ztC Edge システムを完全にシャットダウンできない場合、VMが正しくシャットダウンされていない可能性があります。VMをシャットダウンするには、次のいずれかを実行します。

- VM コンソールまたはリモートデスクトップ アプリケーションを使用して、VMにログオンします。オペレーティング システム コマンドを使用してVMをシャットダウンします。
- ztC Edge コンソールにログオンします。左側のナビゲーション パネルで **[仮想マシン]** をクリックし、VMを選択してから **[電源オフ]** を選択します。

関連トピック

[「仮想マシンの運用を管理する」](#)

[「ztC Edge コンソール」](#)

[「\[システム\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

[基本設定] ページ

[基本設定] ページでは、ztC Edge システムの設定を構成できます。このページを開くには、左側のナビゲーション パネルで **[基本設定]** をクリックします。

次の表は基本設定の各項目とその説明を一覧したものです。

基本設定	説明
システム	
所有者情報	ztC Edge システム管理者の名前と連絡先を指定したり表示できます。この情報は、簡易ネットワーク管理プロトコル (SNMP) 要求への応答としても提供されます。「 所有者情報を指定する 」を参照してください。
製品ライセンス	ztC Edge の製品ライセンスを表示したり管理できます。「 製品ライセンスを管理する 」を参照してください。
ソフトウェア更新	システム ソフトウェアの現行バージョンを確認し、新しいバージョンが利用可能かどうかをチェックできます。新しいバージョンが利用できる場合、ダウンロードしてリリース ノートを読むことができます。また、更新が利用可能になった場合にアラートを送信したり、更新を自動的にダウンロードするようにも指定できます。「 ソフトウェア更新を管理する 」を参照してください。
IP 構成	システムのインターネットプロトコル (IP) アドレスおよびネットワーク設定を表示や指定し、システムを展開できます。「 IP 設定を構成する 」を参照してください。
可用性	システムの冗長な構成を確認し、オプションで 2 つ目のノードを展開して可用性を向上させることができます。「 可用性の設定を構成する 」を参照してください。
クォーラム サーバ	既存および新規のクォーラム サーバを表示できます。クォーラム サーバによってデータの整合性が保証され、ztC Edge 環境で特定の障害が発生した場合に自動で再起動する機能が提供されます。「 クォーラム サーバ 」および「 クォーラム サーバを構成する 」を参照してください。
日付と時刻	システム時刻を表示したり、システムでネットワーク タイム プロトコル (NTP) の値を指定したり (推奨)、日付と時刻を手動で設定することができます。「 日付と時刻を構成する 」を参照してください。

基本設定	説明
メール サーバ	メール サーバを構成して、たとえばパスワードのリセットが必要な場合などに ztC Edge システムで電子メールを送信できるようにします。 「メールサーバを構成する」 を参照してください。
管理ツール	
ユーザとグループ	ztC Edge システム上のユーザ アカウントの追加、変更、削除を行えます。また、Active Directory を有効にしてその許可を与えたり、ユーザを選択してそのユーザのパスワードが最後に更新された時刻を表示することもできます。管理者はこのページを使用して、ユーザを選択して次のログイン時にパスワードの変更を強制することもできます。 「ユーザとグループを構成する」 を参照してください。
セキュアな接続	システムへの HTTPS 接続のみを有効にすることができます。 「セキュアな接続を構成する」 を参照してください。
VM デバイスの構成	すべての VM への仮想 CD (VCD) の挿入機能や、すべての VM への USB デバイスの接続機能を有効化したり無効化することができます。 「VM デバイスを構成する」 を参照してください。
iptables セキュリティ	管理ツール iptables を使用した IP パケット フィルタリングを管理できます。 「iptables を管理する」 を参照してください。
ログイン バナー通知	ログイン バナーを構成できます。 「ログイン バナーを構成する」 を参照してください。
ztC Advisor	ztC Advisor を有効化して、管理者が ztC Advisor ダッシュボードを使ってシステムの稼働状態をリモートで監視できるようにします。 「ztC Advisor を有効化する」 を参照してください。
システム基本設定の保存	[基本設定] ページの設定を、ローカル コンピュータまたはクラウド上のファイルに保存できます。 「システム基本設定を保存または復元する」 を参照してください。

基本設定	説明
基本設定の復元	基本設定 ページの設定を、バックアップ ファイルから復元できます。 「システム基本設定を保存または復元する」 を参照してください。
通知	
e アラート	システム管理者用の電子メール アラート (e アラート) を有効にできます。 「e アラートを構成する」 を参照してください。
SNMP 構成	システムをリモートでモニタリングするために、簡易ネットワーク管理プロトコル (SNMP) 要求およびトラップを有効にできます。 「SNMP 設定を構成する」 を参照してください。
OPC 構成	Open Platform Communication (OPC) の設定を構成して OPC サーバの機能を有効にし、ztC Edge システムを他の産業機械と一緒にモニタリングできるようにします。 「OPC 設定を構成する」 を参照してください。
リモート サポート	
サポート構成	リモート アクセスおよび通知機能を構成できます。リモート アクセスにより、Stratus 認定サービス業者がトラブルシューティングの目的でシステムにリモート接続できるようになります。有効にすると、ztC Edge システムが Stratus 認定サービス業者にシステムの問題に関する通知を送信できます。 「リモート サポート設定を構成する」 を参照してください。
プロキシ構成	組織でインターネット アクセスにプロキシ サーバを使用する必要がある場合、ztC Edge あるいは他の認定 Stratus サービス業者とサービス契約を交わしている場合、ztC Edge システムのプロキシ設定を構成できます。Stratus Redundant Linux ソフトウェアは、サポート通知メッセージおよびリモート サポートのアクセス機能にプロキシ サーバ情報を使用します。 「インターネット プロキシ設定を構成する」 を参照してください。

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

所有者情報を指定する

ztC Edge システムの管理者または所有者の名前と連絡先情報を指定して、サポートの目的でこの情報を提供します。

所有者情報は ztC Edge コンソールで利用でき、簡易ネットワーク管理プロトコル (SNMP) 要求に応じて提供されます。

システムの所有者情報を指定するには

1. 左側のパネルで **[基本設定]** をクリックします。
2. **[基本設定]** ページで **[所有者情報]** をクリックします。
3. **[フル ネーム]**、**[電話番号]**、**[電子メール]**、**[サイト アドレス]** の各フィールドに情報を入力します。
4. **[保存]** をクリックします。

関連トピック

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソール」](#)

製品ライセンスを管理する

システムの製品ライセンスの管理では、次のことを行います。

- 展開の最中またはその後に恒久ライセンスを取得する
- [既存のライセンスのステータスを確認し、必要に応じて更新する](#)
- ステータスおよび有効期限など、現在のライセンス情報を表示する

システムの初回インストール時には、期限が 30 日以内に指定された一時的なライセンスが設定されています。(一時ライセンスはマストヘッドの **[アセット ID]** に **UNREGISTERED_TRIAL** として表示されます。)恒久ライセンスの入手も含め、システムを登録する必要があります。システムの登録は、初期展開の直後か、後日改めて行うことができます。システムの登録の詳細については、[「システムを登録して恒久ライセンスを入手する」](#)を参照してください。

システムに恒久ライセンスが適用されると、インターネットに接続できるシステムの場合は 24 時間ごとにライセンス サーバに更新がないかどうかを確認します。システムがインターネットにアクセスできない場合でも、ユーザがライセンスを更新してそのステータスを確認できます。これを行うには、ztC Edge コンソールの (インターネット アクセスのない) ロケーションと、インターネット アクセスのあるロケーションとの間でファイルを移動する必要があります。以下に 2 つの方法を示しますが、他の方法で行うことも可能です。

- USB フラッシュ ドライブ – (システムに接続可能な) 管理 PC と、インターネット アクセスのあるコンピュータの間に USB フラッシュ ドライブを移動します。
- ラップトップやスマートフォンなどのモバイル デバイス – ztC Edge コンソールにログインできるロケーションと、インターネット アクセスのあるロケーションとの間でモバイル デバイスを移動します。

次から条件に適した手順を選択します (必要に応じてドロップダウンをクリックしてください)。

ライセンスのステータスをチェックするには

システムがインターネットにアクセスできる場合は次の手順を使用します。この手順では必要に応じてライセンスの更新も自動的に行われます。システムがインターネットにアクセスできない場合は「[インターネット アクセスのないシステムの場合](#)」の手順を使用してください。ライセンスを手動で更新する必要がある場合、「[新しいライセンスを手動で更新するには](#)」を参照してください。

1. ztC Edge コンソールで、マストヘッドにある ([**アセット ID: asset_ID**] の) **asset_ID** をクリックします。

あるいは、登録済みのシステムではコンソールの左側のナビゲーション パネルで [**基本設定**] をクリックしてから、次を行います。

- a. [**基本設定**] ページで [**製品ライセンス**] をクリックします。
 - b. [**オンライン ライセンス チェック**] で [**ライセンスを今すぐチェック**] をクリックします。
2. コンソールにライセンスのステータスが表示されます (日付の形式はロケーションによって異なります)。

ステータス

ライセンスはアクティベートされています。有効期限はありません。

前回のチェック

曜日、月 dd、20yy、時刻

サービスの有効期限	曜日、月 <i>dd</i> 、20yy、時刻
アセット ID	<i>asset_ID</i>
製品 UUID	XXXXXXXX-XXXX-XXXX-XXXX- XXXXXXXXXXXX
FT 有効	<i>Yes_or_No</i>
ALSR 許可	<i>Yes_or_No</i>
ゲスト モニタリング許可	<i>Yes_or_No</i>
システム基本設定の保存/復元の許可	<i>Yes_or_No</i>
システム基本設定の保存/復元の有効期限	曜日、月 <i>dd</i> 、20yy、時刻_ま たは_ライセンスなし

新しいライセンスを手動で更新するには (登録済みシステムの場合)

インターネットに接続できる登録済みのシステムでは、ライセンスが自動的に更新されます。必要な場合、ライセンスを手動で更新することもできます。

インターネット アクセスのあるシステムの場合

1. コンソールで、左側のナビゲーション パネルの **[基本設定]** をクリックします。
2. **[基本設定]** ページで **[製品ライセンス]** をクリックします。
3. **[オフラインのライセンス チェックとライセンスの手動インストール]** バーをクリックして、オプションが表示されていない場合はこれを表示します。
4. **[URL ファイルによるオフラインのライセンス チェック]** の下で、**[URL ファイルのダウンロード]** をクリックしてファイルを保存します。
5. ファイル名をクリックします。Web ブラウザが開き、Stratus ライセンス サーバがライセンス ファイルのステータスを確認します。必要な場合、新しいライセンス .key ファイルが自動でダウンロードされます。
6. 次に、**[アップロード]** をクリックします。

インターネット アクセスのないシステムの場合

次の手順を使用して、ライセンスを確認し、必要な場合はインターネット アクセスのない登録済みシステム上で新しいライセンスを手動で取得します。ztC Edge コンソールの (インターネット アクセスのない) ロケーションと、インターネット アクセスのあるロケーションの間でファイルを移動する必要があります。次の手順は 1 つの方法を示しますが、他の方法で行うことも可能です。

ztC Edge コンソールにアクセスできるコンピュータまたはモバイル デバイスでの手順

1. 管理 PC を使用する場合、USB ポートに USB フラッシュ ドライブを挿入します。

モバイル デバイスを使用する場合、これが ztC Edge コンソールにアクセスできることを確認します。
2. ztC Edge コンソールにログオンします。
3. 左側のナビゲーション パネルで **[基本設定]** をクリックします。
4. **[基本設定]** ページで **[製品ライセンス]** をクリックします。
5. **[オフラインのライセンス チェックとライセンスの手動インストール]** バーをクリックして、オプションが表示されていない場合はこれを表示します。
6. **[URL ファイルによるオフラインのライセンス チェック]** で、**[URL ファイルのダウンロード]** をクリックしてファイルをモバイル デバイスまたは USB フラッシュ ドライブに保存します。USB フラッシュ ドライブを使用している場合はドライブを取り出します。インターネット アクセスのある場所に移動します。

インターネット アクセスのある場所での手順

1. USB フラッシュ ドライブを使用している場合、これをインターネット アクセスのあるコンピュータの USB ポートに挿入します。
2. 保存したファイルに移動し、ファイル名をクリックします。
3. Web ブラウザが開き、Stratus ライセンス サーバがライセンス ファイルのステータスを確認します。必要な場合、新しいライセンス .key ファイルが自動でダウンロードされます。USB フラッシュ ドライブを使用している場合、新しいライセンスの .key ファイルをそこにコピーしてから、USB フラッシュ ドライブを取り出します。
4. コンソールにアクセスできる場所に戻ります。

ztC Edge コンソールにアクセスできるコンピュータまたはモバイル デバイスでの手順

1. USB フラッシュ ドライブを使用している場合、これを管理 PC の USB ポートに挿入します。

モバイル デバイスを使用する場合、これが ztC Edge コンソールにアクセスできることを確認します。
2. コンソールで、左側のナビゲーション パネルの **[基本設定]** をクリックします。
3. **[基本設定]** ページで **[製品ライセンス]** をクリックします。

4. **[オフラインのライセンス チェックとライセンスの手動インストール]** バーをクリックして、オプションが表示されていない場合はこれを表示します。
5. **[アクティベート済みライセンス キーのシステムへのインストール]** で **[ファイルの選択]** をクリックし、ライセンス ファイルを保存した場所に移動します。
6. ファイルを選択して **[開く]** をクリックし、次に **[アップロード]** をクリックしてシステムにファイルをアップロードします。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

ソフトウェア更新を管理する

システム ソフトウェアの現行バージョンを確認し、ソフトウェア更新が利用可能かどうかをチェックすることにより、ソフトウェア更新を管理できます。また、オプションで以下を有効にすることもできます。

- システム ソフトウェアの更新が利用可能になると、**[アラート履歴]** ページにメッセージが送信されるようにする。
- システム ソフトウェアの更新が利用可能になると、システム管理者に電子メール アラート (e アラート) が送信されるようにする。
- システムが更新を自動的にダウンロードする (ただしインストールは行わない) ようにする。

更新を自動的にチェックするようにシステムを構成すると、システムは毎日 1 回、ローカル時間の深夜ごろにチェックを行います。利用可能な更新がある場合、システムは、更新されたソフトウェアがないかチェックした直後に、これをシステムのステージング領域にダウンロードします。ステージング領域へのダウンロードが正しく完了した場合、システムは、設定されている構成に応じて **[アラート履歴]** ページにメッセージを送信したり、ソフトウェアのインストール準備ができたことを知らせる e アラートを送信します。ダウンロードに失敗した場合、更新は削除されます。



前提条件: 更新が利用可能になるとシステム管理者が e アラートを受け取るようにするには、メール サーバと e アラートがまだ構成されていない場合はこれを構成する必要があります。
[「メールサーバを構成する」](#) および [「e アラートを構成する」](#) を参照してください。

ソフトウェア更新を管理するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで (**[システム]** の下にある) **[ソフトウェア更新]** をクリックします。
3. **[利用可能なシステム ソフトウェア更新]** に、次の情報が表示されます。

- 現在のシステム ソフトウェアのバージョン番号
- システム ソフトウェアの新しいバージョンが利用可能な場合、そのバージョン番号

システム ソフトウェアの新しいバージョンが利用できる場合、次のリンクから適切なものを 1 つまたは両方クリックします。

- **ソフトウェアのダウンロード** — 利用可能なバージョンをダウンロードするにはこのリンクをクリックします。
- **リリース ノートの確認** — リリース ノートを確認し、利用可能なバージョンのユーザ ガイド全体を表示するには、このリンクをクリックします。

4. **[システム ソフトウェア更新の管理]** に、次のオプションが表示されます。

- **システム ソフトウェア更新が利用可能になった場合、アラートを受け取る** — 更新が利用可能になったことを知らせるメッセージを **[アラート履歴]** ページに送るには、このオプションを選択します。電子メールをシステム管理者に送信して、システム ソフトウェアの更新が利用可能になったことを通知するには、e アラートを構成する必要があります。
- **システム ソフトウェア更新が利用可能になった場合、自動的にダウンロードする (システムにダウンロードするだけでインストールは行いません)** — 新しいシステム更新が利用可能になったらこれをシステムで自動的にダウンロードするには、このオプションを選択します。ダウンロードされたソフトウェアは、**[アップグレード キット]** ページにアップグレード キットとして表示され、ここからソフトウェアをインストールすることができます。詳細については、「[\[アップグレード キット\] ページ](#)」および「[アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする](#)」を参照してください。

5. **[保存]** をクリックします。

関連トピック

[「\[アラート履歴\] ページ」](#)

IP 設定を構成する

ztC Edge システムのインターネット プロトコル (IP) 設定を構成して、システムやノードの IP アドレスの値、およびネットワーク マスク、ゲートウェイ アドレス、Domain Name System (DNS) サーバなどの該当する設定の値を指定したり変更します。(ネットワーク設定は、**[再展開]** ボタンを使ってシステムを再展開する際にも変更します。[「ztC Edge システムを再展開する」](#)を参照してください。)

展開中および展開後に、システムの IP アドレスを構成します。2 つのノードで構成されているシステムでは、システム用に 1 つと各ノード (node0 と node1) 用に 1 つずつ、合計 3 つの IP アドレスを構成します。1 つのノードで構成されているシステムでは、システム用に 1 つ、ノード (node0) 用に 1 つの合計 2 つの IP アドレスを構成します。これらの IP アドレスやその他の IP 設定は、展開を完了した後も以下のうち適切な手順を使って変更できます。ztC Edge システムには静的な IPv4 アドレスを指定する必要があります。

警告:



1. 特に VM が稼働中のシステムでは、担当のネットワーク管理者の了解とアドバイスなしに IP 構成の設定を変更することは避けてください。IP 構成を変更すると、システムとそのすべての VM にアクセスできなくなる可能性があります。
2. **[静的なシステム IP]** のアドレスを変更する場合、VM がリブートすると、VM に自動で割り当てられているすべての MAC アドレスが変更されます。これは、Stratus Redundant Linux ソフトウェアがシステム IP アドレスに基づいて VM の MAC アドレスを生成するためです。VM の MAC アドレスが変更されないようにするには (たとえば、MAC アドレス ベースのライセンスを使用するソフトウェア アプリケーションをサポートする場合など)、固定された MAC アドレスを設定します。[「仮想マシンに特定の MAC アドレスを割り当てる」](#)の説明を参照してください。
3. IP アドレスの変更には ztC Edge コンソールを使用する必要があります。Linux のツールは使用しないでください。

注:

1. IP 設定の構成に使用する手順は、ztC Edge システムが同じサブネット上にとどまるか、新しいサブネットに移動するかによって異なります。ztC Edge システムを新しいネットワークに移動する必要がある場合、移動する前にシステムを "再展開" してその設定をクリアした後で移動します。手順については、[「ztC Edge システムを再展開する」](#)を参照してください。
2. 通常の場合、新しいサブネット用に IP 設定を変更するには、ノードの物理的なネットワーク接続を変更する必要があります (たとえば、PM を移動する場合はネットワークケーブルをいったん抜いてから差し込み直します)。ノードからケーブルを取り外す前に、ノードをシャットダウンする必要があります。これには **[基本設定]** ページの **[IP 構成]** セクションにある **[保存してシャットダウン]** ボタンを使うオプションがあります。
3. 1 つのノードで構成されているシステムでは、**[IP 構成]** ページに 1 つのノードのみの設定が表示されます。

システムやノードの IP 設定を、同じサブネット上のシステムの設定に変更するには

この手順は ztC Edge システムおよびすべての仮想マシン (VM) を実行したままの状態で行います。ただし、システムの IP アドレスを変更する場合は ztC Edge コンソールとシステムとの接続が一時的に失われることがあります。新しいシステム IP アドレスにある ztC Edge コンソールには 1 ~ 2 分以内にアクセスできるようになります。(各ノードのノード IP アドレスはそれぞれ個別に変更でき、その場合コンソールの接続は失われません。)

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[IP 構成]** をクリックします。
3. **[静的なシステム IP]** ボックスに、ネットワーク管理者から受け取った静的なシステム IP アドレスを入力します。
4. **[静的]** ボタンをクリックし、**[プライマリ DNS]** と **[セカンダリ DNS]** に、有効かつ一意の値を入力します。
5. 表示された**ネットマスク**値が正しいことを確認します。

6. **[node0]** と **[node1]** (存在する場合) に、**[IP アドレス]** と **[ゲートウェイ IP]** の適切な値を入力します。
7. **[保存]** をクリックして値を保存するか、以前の値に戻すには **[リセット]** をクリックします。

システム IP アドレスを変更した場合、**[システム IP が更新されました]** というメッセージボックスが表示されます。数秒後にブラウザが新しいシステム IP アドレスに自動的にリダイレクトされます。

関連トピック

[「展開」](#)

[「システム IP 情報を取得する」](#)

[「ztC Edge コンソールに初めてログオンする」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

可用性の設定を構成する

[可用性] ページを使ってシステムの冗長な構成を確認したり、オプションで 2 つ目のノードを展開して可用性を向上させることができます。

[可用性] ページにはお使いのシステムの現在の **[冗長構成]** が表示されます。

- **[有効]** — 両方のノードがオンラインです。システムは冗長化されています。どちらかのノードが故障したりオフラインにされた場合、仮想マシン (VM) は自動的に正常なノードにフェールオーバーします。(ztC Edge システムの可用性のレベルとフェールオーバーの概要は、[「運用モード」](#) を参照してください。)
- **[無効]** — 1 つのノードだけが構成されています。システムは冗長化されていません。ノードが故障したりオフラインにされた場合、VM を利用することはできません。システムを冗長化して可用性を向上させるには、2 つ目のノードを追加してください。

[可用性] ページには、お使いのシステム内の各ノードに関する情報も表示されます。ノードが 1 つしかない場合、**[+]** (プラス記号) をクリックして 2 つ目のノードを追加し、冗長化することができます。詳細については、お使いのシステムに該当するノードの追加ガイド (または [「単一ノード システムにノードを追加する」](#)) を参照してください。

ノードを追加するためのガイド

ztC Edge 100i/110i システム: ノードを追加する (R015Z)

ztC Edge 200i/250i システム: ノードを追加する (R018Z)

関連トピック

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

クォーラム サーバを構成する

ztC Edge システムに初めてログオンするときに、クォーラム サーバを構成します。

前提条件:



1. クォーラム サーバを構成するには 2 つのノードで構成されているシステムが必要です。
2. クォーラム サーバを構成する前に、「[クォーラム サーバ](#)」および「[ALSR 構成を作成する](#)」を参照してください。クォーラム サーバについて説明されています。

注:



1. VM にクォーラム サーバ構成の変更を認識させるには、VM をシャットダウンしてから再起動して、マシンをリブートする必要があります。「[仮想マシンをシャットダウンする](#)」および「[仮想マシンを起動する](#)」を参照してください。
2. クォーラム サーバ上で Windows Update を実行すると、サーバの運用が中断されて障害復旧動作に影響する場合があります。クォーラム サーバでは Windows Update をメンテナンス期間中にスケジュールするか、Windows Update を無効にしてください。

クォーラム サーバを構成するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[クォーラム サーバ]** をクリックします。
3. **[クォーラム サーバの追加]** をクリックします。

4. **[優先クォーラム サーバの追加]** ダイアログ ボックスで、次の値を入力します (既に優先クォーラム サーバが存在する場合は **[代替クォーラム サーバの追加]** ダイアログ ボックスが表示されます)。

- **DNS または IP アドレス** — 優先クォーラム サーバの完全修飾 **DNS** ホスト名または **IP アドレス** を入力します。
- **ポート** (デフォルト値は 4557 です) — デフォルト値以外のポートを使用する場合、その番号を入力します。

[保存] をクリックして値を保存します。

5. ステップ 4 および 5 を繰り返して 2 台目の代替クォーラム サーバを構成します。Stratus では、クォーラム サーバを 2 台構成することを推奨します。
6. クォーラム サービスを有効にするには、**[有効]** チェック ボックスをオンにして **[保存]** をクリックします。

クォーラム サーバを削除するには



注意事項: 優先クォーラム サーバを削除すると、代替クォーラム サーバが優先クォーラム サーバになります。代替クォーラム サーバがない場合、優先クォーラム サーバを削除すると自動的にクォーラム サービスが無効になります。

1. ztC Edge コンソールの **[基本設定]** ページに移動します。
2. **[クォーラム サーバ]** をクリックします。
3. 削除するクォーラム サーバのエントリを見つけます。
4. 一番右の列で **[削除]** をクリックします。



注: VM で使用されているクォーラム サーバを削除する場合、削除の操作を完了させるには、VM をリブートしてクォーラム サーバが認識されないようにする必要があります。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

日付と時刻を構成する

ztC Edge システムに初めてログオンするときに、日付と時刻を設定してネットワーク タイム プロトコル (NTP) サービスを有効にします。NTP サービスを使用するとシステム クロックが自動的に設定され、実際の時刻とのずれが生じないようになります。



注意事項: 日付と時刻の設定を変更すると、システム時刻が実際の時刻と一致しない場合にプライマリの物理マシン (PM) がリブートされ、セカンダリ PM が (存在する場合は) シャットダウンすることがあります。リブートが完了するまですべての仮想マシン (VM) が停止され、ビジネス プロセスは中断されます。



注: VM のマイグレーションや再起動が行われると、クロックのタイムゾーンが切り替わります。VM のタイムゾーンが変更されないようにするには、次を行います。

- すべての VM のタイムゾーンを、ztC Edge システム用に構成したタイムゾーンと一致するように設定します。
- すべての仮想マシンを、ztC Edge システム用に構成されたのと同じ NTP サーバを使用するように構成します。

日付と時刻の設定を構成するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[日付と時刻]** をクリックします。
3. **[日付と時刻]** の表示の **[タイムゾーンの構成]** はデフォルトで **米国ニューヨーク州** に設定されています。必要に応じて地域に適したタイムゾーンを選択してください。
4. **[日付と時刻の構成]** で、次のいずれかを選択します。
 - **[自動 (推奨設定)]** を選択すると、NTP サービスが有効になります。テキスト領域で、NTP サーバのアドレスを 1 行に 1 つずつ入力します。複数の NTP サーバを指定すると冗長性が得られます。
 - **[手動]** を選択すると、設定を手動で入力できます。



注: この方法で構成すると、ztC Edge システム時刻が実時刻と一致しなくなることがあります。

5. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

時刻のずれが生じたためにシステムのリブートが必要な場合、ztC Edge コンソールのマストヘッドにシステムがリブートされるというメッセージが表示されます。その場合には、プライマリ物理マシン (PM) がリブートされ、セカンダリ PM が (存在する場合は) シャットダウンします。プライマリ PM のリブート中は ztC Edge コンソールへの接続が失われます。リブートが完了すると PM がコンソールとの接続を再確立し、セカンダリ PM の再起動を求めるアラートが表示されます。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

メール サーバを構成する

メール サーバを構成して、たとえばパスワードのリセットが必要な場合などに ztC Edge システムで電子メールを送信できるようにします。

メール サーバを構成するには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[システム]** の下で **[メール サーバ]** をクリックします。
3. **[メール サーバの有効化]** ボックスをクリックします。以下の設定を指定や選択するためのボックスが表示されます。
 - **SMTP サーバ (必須)** — 企業が電子メールの送信に利用している簡易メール転送プロトコル (SMTP) サーバの名前を入力します。
 - **ポート番号 (オプション)** — e アラートの送信に使用するポート番号を入力します。ポート番号を指定しない場合、デフォルトの SMTP ポート 25 が使用されます。(SMTP ポートを含むすべての TCP および UDP ポートの詳細については、ナレッジ ベースにアクセスして、「TCP and UDP ports used by ztC Edge (ztC Edge で使用される TCP および UDP ポート)」という記事 (KB-9357) を検索してください。[「ナレッジ ベースの記事にアクセスする」](#)を参照してください。)
 - **送信者の電子メール アドレス** — 次のいずれかが該当する場合、送信者の有効な電子メールアドレスを指定して e アラートの配信を有効にします。

- ztC Edge システムに DNS サーバが指定されておらず、**なおかつ** SMTP サーバがドメイン リテラル (noreply@<IP アドレス> という形式の差出人アドレス) を受け入れるように構成されていない場合。
- e アラートの差出人メール アドレスとして、noreply@company.com などの別のアドレスを使用する場合。

SMTP サーバで受け入れられる任意の電子メール アドレスを使用できます。

- **暗号化接続** — プルダウン メニューから、SMTP サーバに必要な暗号化プロトコルの値を選択します。

- **なし** — 暗号化なし。デフォルトではポート番号 25 が使用されます。
- **TLS** — Transport Layer Security (TLS: トランスポート層セキュリティ) プロトコル。TLS の場合、**[ポート番号]** にはデフォルトで 25 が使用されますが、Stratus では 587 を指定することを推奨します。
- **SSL** — Secure Sockets Layer (SSL) プロトコル。SSL の場合、**[ポート番号]** にはデフォルトで 25 が使用されますが、Stratus では 465 を指定することを推奨します。

- **認証の有効化** — 電子メールを送信するために SMTP サーバが認証を必要とする場合にこのボックスをオンにします。その後、SMTP アカountの **[ユーザ名]** と **[パスワード]** を入力します。

パスワードを指定しない場合、以前のパスワードが引き続き必須になります。以前のパスワードが空で、新しいパスワードも入力しない場合、パスワードは空のままになります。

4. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

ユーザとグループを構成する

[ユーザとグループ] ページでは、ztC Edge システムのユーザ アカountの追加、変更、削除、または Active Directory ユーザへのアクセスの許可を行います。ユーザを選択してそのユーザのパスワードが

最後に更新された時刻を確認できます。管理者はこのページを使用して、ユーザを選択して次のログイン時にパスワードの変更を強制することもできます。

このページを開くには、左側のナビゲーション パネルで **[基本設定]** をクリックしてから、**[基本設定]** ページで **[管理ツール]** の下から **[ユーザとグループ]** を選択します。

ローカル ユーザ アカウントを管理するには

新しいユーザを追加するには、下部パネルにある **[追加]** をクリックします。既存のユーザに変更を加えるには、ユーザ アカウントの名前をクリックして **[編集]** または **[削除]** をクリックします。

ユーザが最後にユーザのパスワードを変更した時刻を調べるには、選択したユーザの **[前回のパスワード更新時刻]** 列を確認します。ユーザに次のログイン時にパスワードの変更を強制するには、管理者がそのユーザを選択して **[パスワードの失効]** をクリックします。

詳細については、「[ローカル ユーザ アカウントを管理する](#)」を参照してください。

ドメイン ユーザ アカウントを管理するには

ztC Edge システムで Active Directory サービスを有効にする手順については、「[Active Directory を構成する](#)」を参照してください。ドメイン ユーザが ztC Edge システムを管理するためのアクセスを許可したり削除するには、「[ドメイン ユーザ アカウントを管理する](#)」を参照してください。



注: Active Directory ユーザまたはグループが構成されたシステムに管理者としてログインしている場合、**[ユーザとグループ]** ページの右上角に **[アクセスの許可]** ボタンが表示されます。**[アクセスの許可]** ボタンをクリックすると、アクセスの許可ウィザードが起動します。アクセスの許可ウィザードの使い方については、「[ドメイン ユーザ アカウントを管理する](#)」を参照してください。

ユーザ アカウントをソートおよび検索するには

アカウントの数が多い場合、列見出しをクリックしてアカウントを特定のパラメータによってソートできます。アカウントのソート基準には**タイプ**、**ユーザ名**、**実名**、**電子メール** アドレス、または**ロール**を使用できます。

関連トピック

[「ドメイン ユーザ アカウントを管理する」](#)

[「ローカル ユーザ アカウントを管理する」](#)

[「Active Directory を構成する」](#)

[「セキュリティの強化」](#)

ローカル ユーザ アカウントを管理する

ztC Edge コンソールの **[ユーザとグループ]** ページで、ローカル ユーザ アカウントのユーザの追加、編集、削除、パスワードの指定、およびユーザ ロールの割り当てを行えます。ユーザを選択してそのパスワードが最後に更新された時刻を表示することもできます。また、管理者は、ユーザを選択して次のログイン時にパスワードを変更するよう強制できます。管理者ではないユーザに "ドメインにコンピュータを接続する" タスク (または権限) を割り当てることができます。(Active Directory ドメイン内の設定済みユーザによるアクセスを許可したり拒否するには、[「ドメイン ユーザ アカウントを管理する」](#)を参照してください。)

ローカル ユーザ アカウントは、中央のドメイン サーバではなく ztC Edge システム自体に保存されます。**[ユーザとグループ]** ページでローカル アカウントを検索するには、**[タイプ]** 列の値が **[ローカル ユーザ]** になっているエントリを探します。

次のユーザ ロールがあります。

- **管理者:** 完全なシステム管理者権限
- **プラットフォーム マネージャー:** ユーザの追加、削除、および変更を除く、システム管理者権限
- **VM マネージャー:** VM の管理権限 (詳細は、[「仮想マシンを管理する」](#)を参照)
- **読み取り専用:** システム構成を表示する権限 (構成の変更権限はありません)、およびシステム ソフトウェアをインストールする権限

以下の手順では、まず **[ユーザとグループ]** ページを次のように開きます: 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを開き、次に **[管理ツール]** の下で **[ユーザとグループ]** を選択します。

ユーザ アカウントを追加するには

1. 下部パネルで **[追加]** をクリックします。
2. **[ロール]** ドロップダウン ウィンドウで **[管理者]**、**[プラットフォーム マネージャー]**、**[VM マネージャー]**、**[読み取り専用]** のいずれかを選択します。
3. **[ユーザ名]**、**[パスワード]** (および **[パスワードの確認]**)、**[電子メール アドレス]**、**[実名]** の各フィールドに値を入力します。ユーザ名は 1 ~ 64 文字にし、スペースを含めることはできません。パスワードはシステムの **「パスワード ポリシー」** に準拠しなければなりません。
4. **[保存]** をクリックします。

ユーザ アカウントを編集するには

1. 編集するアカウントを選択します。
2. 下部パネルで **[編集]** をクリックします。
3. 必要に応じてユーザの情報を編集します。たとえば、ユーザのロールを変更するには、**[ロール]** ドロップダウン ウィンドウで **[管理者]**、**[プラットフォーム マネージャー]**、**[VM マネージャー]**、**[読み取り専用]** のいずれかを選択します。
4. **[保存]** をクリックします。

ユーザにユーザ パスワードの変更を強制するには

1. パスワードを失効させるユーザを選択します。
2. **[パスワードの失効]** をクリックします。
3. 確認のダイアログ ボックスで **[はい]** をクリックします。

管理者以外のユーザに "ドメインにコンピュータを接続する" タスクを割り当てるには

1. 管理者ではないユーザを AD サーバに追加して、**ドメインにコンピュータを接続する** タスク (権限) をそのユーザに委任します。詳細については、お使いの AD サーバのマニュアルを参照してください。
2. ztC Edge システムで、`/etc/resolv.conf` ファイルを編集して AD ドメイン コントローラの IP アドレスを追加します。次の行はその例です。

```
nameserver 123.456.28.910
```
3. ztC Edge コンソールで、AD が有効になっていない場合はこれを有効化します。**「Active Directory を構成する」** を参照してください。

ユーザ アカウントを削除するには

1. 削除するアカウントを選択します。
2. 下部パネルで **[削除]** をクリックします。
3. 確認のダイアログ ボックスで **[はい]** をクリックします。

注:

1. デフォルトの **admin** アカウントを編集して名前とパスワードを変更する必要がありますが、このアカウントを削除することはできません。
2. パスワードを忘れた場合の回復機能を有効にするには、**admin** も含めて各ユーザ アカウントに電子メール アドレスを指定する必要があります。電子メール アドレスを指定していないユーザがコンソールのログイン ページで「**パスワードをお忘れですか?**」リンクをクリックした場合、システムは **user@example.com** に電子メールを送信します。

関連トピック

[「Active Directory を構成する」](#)

[「ドメイン ユーザ アカウントを管理する」](#)

[「ユーザとグループを構成する」](#)

ドメイン ユーザ アカウントを管理する

Active Directory (AD) ドメイン ユーザ アカウントに ztC Edge コンソールへのアクセスを許可することができます。ドメイン ユーザ アカウントは、ローカルの ztC Edge システムではなく中央の AD ドメイン サーバ上で管理します。

ドメイン アカウントにアクセスを許可した後は、[ユーザとグループ] ページにあるアクセスの許可ウィザードを使ってシステムへのアクセス許可のある AD アカウントの表示、管理、およびソートを行うことができます。



前提条件: ドメイン アカウントを管理するには、その前に ztC Edge システムを Active Directory ドメインに追加する必要があります。(「[Active Directory を構成する](#)」を参照してください。)Active Directory が構成されていない場合や、インタフェースにログインしているユーザが管理者の権限を持たない場合には、[ユーザとグループ] ページの [アクセスの許可] ボタンはグレー表示されます。

以下の手順を行うには **ztC Edge のアクセスの許可ウィザード**を開きます。

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で **[ユーザとグループ]** を選択します。
3. **[アクセスの許可]** をクリックします。

ドメイン ユーザ アカウントにアクセスを許可するには

1. **ztC Edge - アクセスの許可ウィザード** の **[Search for (検索対象)]** メニューで検索範囲を指定します。
2. 検索する名前またはグループを入力します。名前やテキストの一部を入力することができます。
3. **[検索]** をクリックします。
4. システムの ztC Edge コンソール グローバル ユーザまたはグループとして追加する、ユーザまたはグループの隣りにある緑色のプラス記号 (+) をクリックします。
5. **[ロール]** 列のドロップダウン メニューを使用して、上記の手順でアクセスを許可したユーザまたはグループにロールを割り当てます。割り当てが可能なロールは以下のとおりです。
 - **管理者** — システム管理者が行うすべての操作の実行権限が有効になります。
 - **プラットフォーム管理者** — 管理者の権限からユーザ アカウントの管理権限を除いたものが有効になります。
 - **VM マネージャー** — VM の管理権限が有効になります (詳細は、[「仮想マシンを管理する」](#)を参照)。
 - **読み取り専用** — 読み取りアクセスは有効になりますが、管理機能は許可されません。
6. **[完了]** をクリックします。アクセスの許可ウィザードに新しいドメイン ユーザが表示されます。

ドメイン ユーザ アカウントからアクセスを削除するには

1. **ztC Edge - アクセスの許可ウィザード** で、削除するユーザまたはグループの隣のチェックボックスをオンにします。
2. **[Deny Access (アクセスの拒否)]** をクリックし、**[完了]** をクリックします。

関連トピック

[「Active Directory を構成する」](#)

Active Directory を構成する

ztC Edge システムの Active Directory を構成して、Active Directory ドメインからの既存のユーザまたはグループが自身の Active Directory 資格情報を使って ztC Edge コンソールにログオンする操作を許可することが可能です。

ztC Edge システムを Active Directory ドメインに追加した後、**アクセスの許可**ウィザードを使ってドメイン ユーザに管理者権限を割り当てることができます。このウィザードは **[ユーザとグループ]** ページから起動できます (**[ユーザとグループを構成する]** を参照してください)。

Active Directory ドメインに ztC Edge システムを追加するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[ユーザとグループ]** をクリックします。
3. 下部パネルの **[Active Directory の有効化]** ボタンをクリックします。
4. **[Active Directory ドメイン]** の隣に、使用するドメインの名前を入力します。
5. 次のいずれかをクリックして、"全員" ロールの自動割り当てを禁止するか、許可します。
 - **すべての AD ユーザに "全員" ロールが自動的に割り当てられないようにする** (デフォルト設定)
 - **すべての AD ユーザの認証と、"全員" ロール アクセスの承認を許可する**
6. **[Active Directory へのシステムの追加]** をクリックします。
7. この ztC Edge システムをドメインに追加するには、Active Directory 管理者の **[ユーザ名]** と **[パスワード]** を入力します。
8. **[追加]** をクリックします。
9. **[ユーザとグループ]** ページで管理者権限を割り当てます。 **[ドメイン ユーザ アカウントを管理する]** を参照してください。

Active Directory ドメインから ztC Edge システムを削除するには

1. ztC Edge コンソールで、左側のパネルの **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[ユーザとグループ]** をクリックします。
3. 下部パネルの **[Active Directory からのシステムの削除]** ボタンをクリックします。

4. そのドメインの管理権限が付与されている **[ユーザ名]** および **[パスワード]** を入力します。
5. **[削除]** をクリックします。

ドメイン認証を無効にするには

1. ztC Edge コンソールで、左側のパネルの **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[ユーザとグループ]** をクリックします。
3. 下部パネルの **[Active Directory の無効化]** ボタンをクリックします。



注: Active Directory を無効にすると、ztC Edge システムの管理者を認証するためのドメイン認証が使用できなくなりますが、システムがドメインから削除されることはありません。ドメイン認証を再び使用できるようにするには、**[Active Directory の有効化]** をクリックします。**[ユーザとグループ]** ページでコントローラの名前を再入力したり、ドメイン ユーザを復元する必要はありません。

関連トピック

[「ユーザとグループを構成する」](#)

[「ドメイン ユーザ アカウントを管理する」](#)

[「ローカル ユーザ アカウントを管理する」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソール」](#)

[「セキュリティの強化」](#)

セキュアな接続を構成する

セキュリティのため、デフォルトでは ztC Edge システムは HTTPS 接続のみを許可します。HTTP 接続を許可するには、セキュアな接続を構成することができます。

注:



下記の手順で **[HTTPS のみ有効化 / HTTP を無効化]** の横のボックスをオンやオフにしてから **[保存]** をクリックすると、ユーザがシステムから自動的に ztC Edge コンソールからログアウトされるので、ログインし直す必要があります。

HTTPS 接続が有効にされている場合、スクリプトを使ってカスタム証明書をホスト マシンにインストールすることができます。「[カスタム証明書をインストールするには](#)」を参照してください。

HTTP 接続と HTTPS 接続の両方を有効にするには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で **[セキュアな接続]** をクリックします。
3. **[HTTPS のみ有効化 / HTTP を無効化]** の横のチェック ボックスをオフにします。
4. **[保存]** をクリックします。

ztC Edge コンソールから自動的にログアウトされ、ブラウザが HTTPS ログイン ページにリダイレクトされます。HTTP ログイン ページにアクセスするには、ブラウザのアドレス バーで **https** を **http** に手作業で変更すると、ログインできるようになります。

システムで HTTP と HTTPS 接続が許可されている場合に HTTPS 接続のみが許可されるようにするには、このチェック ボックスをオンにする必要があります。

HTTPS 接続のみを有効にするには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で **[セキュアな接続]** をクリックします。
3. **[HTTPS のみ有効化 / HTTP を無効化]** の横のチェック ボックスをオンにします。
4. **[保存]** をクリックします。

ztC Edge コンソールから自動的にログアウトされ、ブラウザが HTTPS ログイン ページにリダイレクトされるので、再度ログインする必要があります。

カスタム証明書をインストールするには

カスタム証明書をインストールするには、[certificate_installer](#) スクリプトを使用します。このスクリプトを使用して、次のようにカスタムの SSL 証明書をインストールしたり、以前に使用した証明書や組み込み証明書を復旧したり、現在使用中の証明書や以前使用していた証明書に関する情報を表示することができます。

- カスタム証明書をインストールするには (HTTPS のみのモードを除く)
 - i. 証明書をホスト マシンの `/tmp` フォルダにコピーします。
 - ii. コマンドは次のように入力します。

```
certificate_installer install -c /tmp/server.crt -k  
/tmp/server.key
```

- カスタム証明書をインストールするには (HTTPS のみのモード)

- i. 証明書をホスト マシンの /tmp フォルダにコピーします。
- ii. コマンドは次のように入力します。

```
certificate_installer install -c /tmp/server.crt -k  
/tmp/server.key -f
```

- カスタム証明書を以前使用していた証明書に戻すには

```
certificate_installer recover -p
```

- カスタム証明書を組み込み証明書に戻すには

```
certificate_installer recover -b
```

- 現在使用中の証明書に関する情報を一覧するには

```
certificate_installer list -c
```

- 以前使用していた証明書に関する情報を一覧するには

```
certificate_installer list -p
```

カスタム証明書のインストールの詳細については、ナレッジ ベースにアクセスして、「Adding Certificates to ca-bundle.crt in ztC Edge (ztC Edge で ca-bundle.crt に証明書を追加する)」という記事 (KB-[9792](#)) を検索してください。「[ナレッジ ベースの記事にアクセスする](#)」を参照してください。

certificate_installer スクリプト

使用方法

```
certificate_installer [command command_options] [script_  
options]
```

コマンドとコマンド オプション

<code>install command_options</code>	<p>カスタム証明書をインストールします。次のコマンド オプションがあります。</p> <ul style="list-style-type: none">• <code>-c</code>、<code>--cert=certificate_path</code>: 証明書が保存されるパス。• <code>-k</code>、<code>--key=private_key_path</code>: キーが保存されるパス。• <code>-f</code>、<code>--[no-]force</code>: 使用中の SSL 証明書を強制的に置換します。
<code>recover command_options</code>	<p>カスタム証明書を復旧します。次のコマンド オプションがあります。</p> <ul style="list-style-type: none">• <code>-b</code>、<code>--[no-]built-in</code> (デフォルト): 組み込み証明書に戻します。• <code>-p</code>、<code>--[no-]previous</code>: 以前使用していた証明書に戻します。
<code>list command_options</code>	<p>カスタム証明書の一覧を表示します。次のコマンド オプションがあります。</p> <ul style="list-style-type: none">• <code>-a</code>、<code>--[no-]all</code> (デフォルト): ホスト マシン上のすべての SSL 証明書を表示します。• <code>-c</code>、<code>--[no-]current</code>: 現在の使用中の証明書を表示します。• <code>-p</code>、<code>--[no-]previous</code>: 以前使用していた証明書を表示します。• <code>-L</code>、<code>--location=location</code>: 指定の場所にある証明書の情報を表示します。

スクリプトのオプション

<code>-v, --[no_]verbose</code>	詳細モード。スクリプトがすべての情報を表示します。
<code>-l, --log=log_file</code>	ログを STDOUT の代わりにファイル <i>log_file</i> に出力します。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

[「セキュリティの強化」](#)

VM デバイスを構成する

VM デバイスを構成して、すべての VM への仮想 CD (VCD) の挿入機能や、すべての VM への USB の接続機能を有効にしたり無効にします。デフォルトでは、これらの VM デバイスを挿入や接続することが可能です。構成を変更するには **[基本設定]** ページの **[VM デバイスの構成]** を使用します。

VM デバイスの挿入や接続が有効にされている場合 (デフォルト設定)、すべての VM に VCD を挿入したり、すべての VM に USB デバイスを接続することができます。VM デバイスの挿入や接続が無効にされている場合、これらのデバイスを挿入したり接続することはできません。

VM デバイスの挿入または接続を無効にするには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[管理ツール]** の下の **[VM デバイスの構成]** をクリックします。
3. 次のいずれか、または両方のチェック ボックスをオンにします。
 - **すべての VM での CD の挿入の無効化** — VM への CD の挿入を無効にするにはチェック ボックスをオンにします。
 - **すべての VM への USB デバイスの接続の無効化** — VM への USB デバイスの接続を無効にするにはチェック ボックスをオンにします。
4. **[保存]** をクリックします。

VM デバイスの挿入または接続を有効にするには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[管理ツール]** の下の **[VM デバイスの構成]** をクリックします。
3. 次のいずれか、または両方のチェック ボックスをオンにします。
 - **すべての VM での CD の挿入の無効化** — VM への CD の挿入を有効にするにはチェック ボックスをオフにします。
 - **すべての VM への USB デバイスの接続の無効化** — VM への USB デバイスの接続を有効にするにはチェック ボックスをオフにします。
4. **[保存]** をクリックします。

関連トピック

[「仮想 CD を挿入する」](#)

[「仮想マシンに USB デバイスを接続する」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

iptables を管理する

Linux オペレーティング システムで IP パケットのフィルタリングを管理するツールのことを通称 "iptables" と呼びます。ztC Edge システムで行う iptables の作業タスクが合理化され、簡単になりました。**[iptables のセキュリティ]** ページを使用して、さまざまなフィルター テーブルチェーンとその基本ルールの設定、保守、および検査を行うことができます。必要なパケット フィルタリング ルールを適用するための 3 つの主要チェーン (**INPUT**、**OUTPUT**、**FORWARD**) にアクセスできます。ztC Edge システムでは、ルールが IPv4 パケットと IPv6 パケットの両方で各物理マシン (PM) 上のホスト オペレーティング システムに適用され、リブートした後もルールが保持されます。

ルールを挿入する際、チェーン (**INPUT**、**OUTPUT**、または **FORWARD**) と **[ルール ID]** を指定します。受信パケットの処理ではカーネルが **INPUT** チェーンに関連付けられているルールを適用し、送信パケットの処理時には **OUTPUT** チェーンに関連付けられているルールを適用します。別のホストへのルーティングが必要な受信パケットを処理する場合、カーネルは **FORWARD** チェーンに関連付けられているルールを適用します。ルールは **[ルール ID]** の順序に従って適用されます。(**[ルール ID]** は行 ID と似ています。たとえば、**ルール ID** が 1 の場合、1 行目に相当します。) ルールを作成する代わりに、ルールのデフォルト設定を読み込むこともできます。

[iptables セキュリティ] ページに、3 つのチェーンとその関連ルールについてそれぞれ個別の表が表示されます。特定のチェーンに設定されているルールは、チェーンごとに **[ルール ID]** によってソートされます。列にはネットワーク名、ネットワークのタイプ、プロトコル、およびその他の情報が表示されます。必要な場合は、ページの右側にあるスクロールバーを使ってすべてのルールを表示したり、下部にあるスクロールバーを使ってすべての列を表示できます。iptables の機能の詳細については、Linux マニュアル (man) ページで iptables を参照してください。

オプションとして、ホストに加えてゲスト オペレーティング システムへのルールの適用を有効化することができます。デフォルトでは、ルールがホスト オペレーティング システムのみに適用され、ゲスト オペレーティング システムには適用されません。ルールがゲストにも適用されるよう有効化する際は、すべての既存のルール、インポートされたルール、および追加の新しく挿入されたルールも、すべてのゲスト オペレーティング システムに適用されます (ゲストに割り当てられた同じビジネス ネットワークに基づくルールについて)。

注:

1. ztC Edge ソフトウェアが使用するポートの詳細については、[「システム要件の概要」](#)を参照してください。
2. ztC Edge TCP および UDP ポートの詳細については、ナレッジ ベースにアクセスして、「TCP and UDP ports used by ztC Edge (ztC Edge で使用される TCP および UDP ポート)」という記事 (KB-[2123](#)) を検索してください。[「ナレッジ ベースの記事にアクセスする」](#)を参照してください。

iptables を管理するには、まず iptables セキュリティを有効化します (まだ行っていない場合)。

iptables セキュリティを有効にするには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[iptables セキュリティ]** をクリックします。
3. **[iptables セキュリティの有効化]** の横のチェック ボックスをオンにします。

[iptables セキュリティの有効化] ウィンドウが数分間グレーになります。このウィンドウが再びアクティブになると、**[iptables セキュリティの有効化]** が選択されています。

デフォルトではルールがホストのみに適用されます。ただし、ホストに加えてゲストにもルールを適用することが可能です。

ホストに加えてゲストにもルールを適用するには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[iptables セキュリティ]** をクリックします。
[iptables セキュリティの有効化] が選択されていることを確認します。
3. デフォルトでは **[ホストに適用]** が選択されています。
[ホストとゲストに適用] を選択して、ルールをホストとゲストの両方のオペレーティングシステムに適用します。**[ポート管理の有効化]** ウィンドウが数分間グレーになります。
[ホストとゲストに適用] が選択されている場合、すべての既存のルール、インポートされたルール、および追加の新しく挿入されたルールも、すべてのゲスト オペレーティングシステムに適用されます (ゲストに割り当てられた同じビジネス ネットワークに基づくルールについて)。

新しいルールの挿入、ルールの削除、デフォルト設定の読み込み、ルールのインポート、またはルールのエクスポートから、適切な操作を選んで続行します。

新しいルールを挿入するには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[iptables セキュリティ]** をクリックします。
[iptables セキュリティの有効化] が選択されていることを確認します。
3. **[新しいルールの挿入]** ボタンをクリックして **[新しいルールの挿入]** ポップアップ ウィンドウを開きます。
4. **[新しいルールの挿入]** ウィンドウで、次の値を設定します。
 - **チェーン** — ドロップダウン リストで **[INPUT]**、**[OUTPUT]**、または **[FORWARD]** を選択します。
 - **ルール ID** — ルールの処理順序を指定する数値を入力します。入力できる最小値は 1、最大値はチェーンに含まれるルールの総数に等しい値です。**[ルール ID]** の値は一意でなければなりません。
他のルールに既に割り当てられている数値を入力すると、既存のルール (および該当する場合はその後のすべてのルール) の番号が 1 つ増え、入力した数値は新しいルールに割り当てられます。したがって、たとえば **ルール ID 1** が既に存在する場合、

新しいルールに **1** を指定すると、既存のルール **ID 1** がルール **ID 2** に変わり、さらに該当する場合は既存の **ルール ID 2** がルール **ID 3** となります。

- **共有ネットワーク** — 利用可能なすべての共有ネットワークが表示されたドロップダウン リストからネットワークを選択します。
- **プロトコル** — **[udp]**、**[tcp]**、または **[すべて]** を選択します。
[すべて] を選択すると、ポート番号の範囲設定が不要になり、**[グループ化]** フィールドと **[ポート番号]** フィールドが非アクティブ (グレー) になります。
- **ターゲット** — ルールの仕様に一致するパケットに適用するアクションとして、**[ドロップ]**、**[受容]**、または **[拒否]** を選択します。
- **ポート番号 (開始)** — 範囲の最初のポートには、0 ～ 65535 の範囲内で **[ポート番号 (終了)]** 以下の数値を入力します。
- **ポート番号 (終了)** — 範囲の最後のポートには、0 ～ 65535 の範囲内で **[ポート番号 (開始)]** 以上の数値を入力します。
- **IP アドレス (開始)** — 範囲の最初の IPv4 アドレスには、0.0.0.0 ～ 255.255.255.255 の範囲内で **[IP アドレス (終了)]** 以下の数値を入力します。
- **IP アドレス (終了)** — 範囲の最後の IPv4 アドレスには、0.0.0.0 ～ 255.255.255.255 の範囲内で **[IP アドレス (開始)]** 以上の数値を入力します。
- **IPv6 アドレス (開始)** — 範囲の最初の IPv6 アドレスには、
0000:0000:0000:0000:0000:0000:0000:0000 ～
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff の範囲内で **[IPv6 アドレス (終了)]** 以下の数値を入力します。
- **IPv6 アドレス (終了)** — 範囲の最後の IPv6 アドレスには、
0000:0000:0000:0000:0000:0000:0000:0000 ～
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff の範囲内で **[IPv6 アドレス (開始)]** 以上の数値を入力します。

[挿入] をクリックして新しいルールを挿入します。

5. デフォルトで、挿入されたルールはホストのみに適用されます。ルールをホストとゲストの両方に適用するには、[「ホストに加えてゲストにもルールを適用するには」](#)を参照してください。

6. ページの一番下にある **[保存]** をクリックするか、保存されていない変更をすべてキャンセルして前回の保存済みセッションの状態にルールを復元するには **[リセット]** をクリックします。

保存された新しいルールは **[iptables セキュリティ]** ページの適切なチェーンに表示されます。

ルールを削除するには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[iptables セキュリティ]** をクリックします。
[iptables セキュリティの有効化] が選択されていることを確認します。
(**[ホストに適用]** および **[ホストとゲストに適用]** は、ルールの削除には影響しません。)
3. 削除するルールを選択します。
4. 選択したルールの **[削除]** (一番右の列) をクリックします。
5. ページの一番下にある **[保存]** をクリックするか、保存されていない変更をすべてキャンセルして前回の保存済みセッションの状態にルールを復元するには **[リセット]** をクリックします。

ルールが削除されると、**[iptables セキュリティ]** ページに表示されなくなります。

デフォルト設定を読み込むには



注意事項: デフォルト設定を読み込むと、現在の設定がオーバーライドされます。

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[iptables セキュリティ]** をクリックします。
[iptables セキュリティの有効化] が選択されていることを確認します。
3. ページの一番下にある **[デフォルト設定の読み込み]** をクリックします。

次の警告が表示されます: 「現在の設定が初期設定でオーバーライドされます。」 デフォルト設定を読み込むには **[OK]** を、読み込みをキャンセルするには **[キャンセル]** をクリックします。 **[OK]** をクリックすると、**[ポート管理の有効化]** ウィンドウが数分間グレーになり、**[デフォルト設定を読み込み中...]** メッセージが表示されます。

4. デフォルトのルールは、ホストのみに適用されます。ルールをホストとゲストの両方に適用するには、[「ホストに加えてゲストにもルールを適用するには」](#)を参照してください。

ルールをインポートまたはエクスポートするには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[基本設定]** ページで **[iptables セキュリティ]** をクリックします。

[iptables セキュリティの有効化] が選択されていることを確認します。

3. ページの一番下にある **[インポート]** または **[エクスポート]** をクリックします。

- **インポート** — **iptables セキュリティ ルールのインポート/リストア ウィザード**が開きます。インポートする XML ファイルを参照して選択します。インポートした XML ファイル内で共有ネットワークのタイプに関連付けられている全ルールが、同じタイプをもつシステム上の既存の各共有ネットワーク用に生成されます。

XML ファイルを選択すると、次のメッセージが表示されます。

[追加] を選択すると現在のルール セットが維持されます。現在のルールをすべて消去するには **[上書き]** を選択します。

次から適切なボタンをクリックします。

- **追加** — 選択した XML ファイルは既存の XML ファイルに追加され、既存のルールが維持されます。
- **上書き** — 選択した XML ファイルが既存の XML ファイルを上書きし、既存のルールは消去されます。

- **エクスポート** — **エクスプローラー ウィンドウ**が開きます。ローカル システム上で、エクスポートしたルールのファイルを保存するロケーションを参照します。表内のすべてのルールが XML ファイルにエクスポートされた後、選択したロケーションにそのファイルがダウンロードされます。

4. デフォルトでは、インポートしたルールはホストのみに適用されます。ルールをホストとゲストの両方に適用するには、[「ホストに加えてゲストにもルールを適用するには」](#)を参照してください。
5. ファイルをインポートした場合、**[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

関連トピック

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソール」](#)

[「セキュリティの強化」](#)

ログイン バナーを構成する

ztC Edge コンソールのログイン ページにカスタム コンテンツを提供するログイン バナーを構成できます。たとえば、メッセージを追加できます。

ログイン バナーを構成するには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。

2. **[管理ツール]** の下で **[ログイン バナー通知]** をクリックします。

3. **[ログイン バナー通知の有効化]** ボックスをオンにします。ボックスが表示されます。

このボックスに、コンソールのログイン ページに表示したい情報を入力します。たとえば、社名やメッセージを入力できます。

4. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

ztC Advisor を有効化する

ztC Advisor を ztC Edge システム用に有効化して、管理者が ztC Advisor ダッシュボードを使ってシステムの稼働状態をリモートで監視できるようにします。

ztC Advisor は、ztC Edge システムのフリート全体を一括表示できるセキュアな Web ベースのポータルです。使いやすい直観的なダッシュボードから各システムの稼働状態、リソースの使用状況、およびソフトウェアバージョンを一目で確認できます。ztC Advisor の登録と使用の詳細については、

<https://www.stratus.com/solutions/ztc-advisor> にある Web ページを参照してください。



前提条件: ztC Advisor で監視するには、ztC Edge システムが Stratus で登録されていて、インターネットに接続されていなければなりません。ztC Advisor はいつでも有効化することができますが、システムの稼働状況に関する情報がダッシュボードに表示されるのは、システムが Stratus に登録済みでインターネットに接続されている場合のみです。

次の手順で ztC Advisor を有効化した後、ztC Advisor ダッシュボードにログインして次の Web ページでシステムのステータスを表示できます: <https://ztcadvisor.stratus.com>

ztC Edge システム用に ztC Advisor を有効化するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で **[ztC Advisor]** をクリックします。
3. **[ztC Advisor の有効化]** の横のチェック ボックスをオンにします。
4. オプションとしてシステムの **[エイリアス名]** を入力できます。

デフォルトでは、各システムがそのアセット ID に基づいてダッシュボードに一覧されますが、システムにエイリアスを割り当ててわかりやすい名前を付け、フィルターや検索で簡単に見つけるようにすることができます。エイリアス名の長さは最大 64 文字で、文字、数字、特殊文字の任意の組み合わせを使用できます。

5. **[保存]** をクリックして設定を保存し、モニタリングを有効にします。

変更を保存すると、数分以内にシステムが ztC Advisor ダッシュボードに表示されます。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

システム基本設定を保存または復元する

適切なライセンスが適用されている ztC Edge システムでは、完全なシステム管理者権限をもつユーザが ztC Edge コンソールの **[基本設定]** ページの設定 (つまりバックアップ ファイル) を保存することができます。このファイルはローカル コンピュータ上の保存先フォルダか、クラウドのフォルダに保存できます。その後で必要に応じ、保存したファイルを選択して、同じノード、交換ノード、または 1 つ以上の別のノードに **[基本設定]** の設定を復元することができます。この機能を使用すると、1 つ以上のシステムをすばやくセットアップできます。たとえば、システムの復元ファイルが保存されているクラウドア

カウントに既にログインしている場合、1 度クリックするだけでノードのシステム基本設定を復元できます。

注:

- クラウドには ztC Edge システムごとに最大 50 個のファイルを保存できます。
- ファイルをクラウドに保存したり、クラウドからファイルを復元するには、インターネットにアクセスできるシステムで、有効な資格情報を使ってクラウド アカウントにログインする必要があります。
- 単一ノード システムでは冗長性が提供されないため、システムの基本設定を保存しておくことが特に重要です。

システムには **[基本設定]** の設定を保存および復元するための適切なライセンスが必要です。システムの最初のインストール時には、この機能が無効にされています。**[基本設定]** ページの **[システム基本設定の保存]** および **[システム基本設定の復元]** ウィンドウに、**[基本設定]** の設定を保存および復元するにはライセンスをアクティベートする必要があるというメッセージが表示されます。この機能を使用するには、ライセンスのアクティベーションを行う必要があります。

ライセンスをアクティベートするには

前提条件: ライセンスのアクティベーションには次の情報が必要です。



- **First Name (名) および Last Name (氏)**
- **Company Email (会社電子メール)** — ライセンスが適用されるシステムを所有している会社の電子メール アドレスを入力します。個人の電子メール アドレスは使用しないでください。
- **Company Name (会社名)** — ライセンスが適用されるシステムを所有している会社の名前を入力します。
- **Company Phone Number (会社の電話番号)** — ライセンスが適用されるシステムを所有している会社の電話番号を入力します。個人の電話番号は使用しないでください。
- **Asset ID (アセット ID)** — ztC Edge コンソールのマストヘッドに記載のアセット ID を入力します。

システムがインターネットにアクセスできる場合は次のステップ 1 に進みます。システムがインターネットにアクセスできない場合、インターネット アクセスのあるロケーションと、(インター

ネット アクセスのない) ztC Edge コンソールのロケーション間でライセンス ファイルを移動させる必要があります。次の手順では USB フラッシュ ドライブを使う方法を示しますが、他の方法で行うことも可能です。USB フラッシュ ドライブを使用している場合、この手順を開始する前にドライブを入手して、ztC Edge コンソールを実行しているリモート管理 PC の USB ポートに挿入します。

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で、**[システム基本設定の保存]** または **[システム基本設定の復元]** をクリックします。
3. ウィンドウに、**[基本設定]** を保存および復元するには個別のライセンスのアクティベーションが必要であることを伝えるメッセージが表示されます。
4. メッセージを読みます。システムがインターネットにアクセスできる場合、ライセンスの Web ページを開くリンクをクリックします。



注: システムを登録してその恒久ライセンスを入手する必要がある場合には、[「システムを登録して恒久ライセンスを入手する」](#)を参照してください。

システムがインターネットにアクセスできない場合、次の手順を実行してライセンスの Web ページを開きます。

インターネット アクセスのないシステムの場合

- a. ライセンスの Web ページを開くリンクをクリックし、お使いのブラウザに適した方法でライセンス Web ページの URL をコピーします。
- b. テキスト ファイルに URL を貼り付けて、そのテキスト ファイルを USB フラッシュ ドライブに保存します。
- c. USB フラッシュ ドライブを取り出し、インターネット アクセスのあるコンピュータに移動します。
- d. このコンピュータの USB ポートに、USB フラッシュ ドライブを挿入します。
- e. テキスト ファイルを見つけて開き、ライセンス Web ページの URL をコピーします。

- f. ブラウザを開いてアドレス バーに URL を貼り付け、Web ページにアクセスします。
5. Web ページに情報を入力して **[Submit (送信)]** をクリックします。
6. **[Download License (ライセンスのダウンロード)]** ボタンが表示されたら、クリックします。システムがインターネットにアクセスできる場合は次のステップに進みます。
- システムがインターネットにアクセスできない場合、ダウンロードしたライセンス ファイルを USB フラッシュ ドライブに保存して、フラッシュ ドライブを取り出します。コンソールを実行しているリモート管理コンピュータに戻り、USB フラッシュ ドライブを挿入します。
7. ライセンスをシステムにアップロードします。まず、**[基本設定]** ページの **[製品ライセンス]** をクリックします。次に、システムに応じて次のいずれかの手順を実行します。
- インターネット アクセスのあるシステムでライセンスを自動的にアップロードするには、まず **[基本設定]** ページの **[製品ライセンス]** をクリックした後、**[オンラインのライセンス チェック]** の **[ライセンスを今すぐチェック]** をクリックします。新しくダウンロードされたライセンスは、自動的にシステムに適用されます。
 - インターネット アクセスのないシステムでライセンスをアップロードするには
 - a. **[基本設定]** ページの **[製品ライセンス]** をクリックします。
 - b. **[オフラインのライセンス チェックとライセンスの手動インストール]** バーのオプションが表示されていない場合は、バーをクリックして表示します。
 - c. **[アクティベート済みライセンス キーのシステムへのインストール]** で **[ファイルの選択]** をクリックし、ファイルを保存した場所に移動します。
 - d. ファイルを選択して **[開く]** をクリックし、次に **[アップロード]** をクリックしてシステムにファイルをアップロードします。

これで **[基本設定]** の設定を保存および復元するための適切なライセンスがシステムに適用されます。

デフォルトでは、保存したファイルに次の基本設定が含まれています。

所有者情報	VM デバイスの構成
ソフトウェア更新	iptables セキュリティ
IP 構成	ログイン バナー通知

クォーラム サーバ (デュアルノード システムのみ)	ztC Advisor
日付と時刻	e アラート
メール サーバ	SNMP 構成
ユーザとグループ	OPC 構成
セキュアな接続	サポート構成
	プロキシ構成

システム基本設定を保存するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で **[システム基本設定の保存]** をクリックします。
3. **[システム基本設定の保存]** の下で、次のいずれかを選択します。

- **このコンピュータ上のファイルにシステム基本設定を保存する**
- **クラウドのファイルにシステム基本設定を保存する** — これを選択すると、ztC Edge コンソールを実行しているリモート管理コンピュータがインターネットに接続している場合は、次のメッセージが表示されます。

Stratus カスタマ サービス ポータルにログインしてアカウントを認証します。

Stratus カスタマ サービス アカウントのユーザ名とパスワードを入力します。リモート管理コンピュータがインターネットに接続していない場合、ログイン用のフィールドは表示されません。代わりに、インターネット接続が利用不可であるためファイルを保存できないことを示すメッセージが表示されます。

クラウド アカウントにログインすると、クラウド アカウントにログインしたユーザの名前と、現在クラウドに保存されているファイルの数が表示されます。クラウドにはシステムごとに最大 50 個のファイルを保存できます。50 個のファイルが保存されている場合、それ以上ファイルを保存することはできません。ファイルは削除できないので、ファイルを削除するには担当の Stratus 認定サービス業者に問い合わせる必要があります。

クラウド アカウントのログイン セッションは、コンソール セッションがアクティブな間継続されます。コンソール セッションを閉じるか、セッションがタイムアウトした場合は自動的にログアウトされます。

4. 必要に応じて、次のフィールドに情報を入力します。

- **ファイル名** — このフィールドにはデフォルトのファイル名が表示されます。形式は **ztC_<アセット ID>_preferences_yyyy-mm-dd-hh-mm.zip** です。ファイルを保存した後でも、必要に応じてファイル名は変更できます。ファイル名に使用できる文字は、英文字、数字、ハイフン (-)、およびアンダースコア (_) です。
- **説明** — 説明を入力します (オプション)。
- **キーワード** — デフォルトではキーワード <システム ID> が表示されます。デフォルトのキーワードを変更したり、キーワードを追加することができます。合計 3 つのキーワードを指定できます。

5. 次のいずれかのボタンをクリックします。

- **保存** — ファイルがデフォルトのファイル名で保存されます。あるいは必要に応じてファイル名を変更できます。

ファイルをローカル コンピュータに保存する場合、デフォルトの場所を使用するか、別の場所に移動します。(デフォルトの保存場所はブラウザで設定されています。)

ファイルをクラウドに保存している場合、ユーザ名とパスワードが正しく検証されると、ファイルが作成されてユーザのクラウド アカウントに保存されます。フォルダの名前は **<アセット ID>** です。

- **クリア** — **[説明]** フィールドと **[タグ]** フィールドをクリアします。また、ファイルをクラウドに保存している場合、ファイル名はデフォルトの名前にリセットされ、ユーザ名とパスワードがクリアされます。

正しく保存されると、「システム基本設定が保存されました。」というメッセージが表示されます。

システム基本設定を保存した後で、同じシステムまたは別のシステムに設定を復元したい場合、まずリストア操作に関する注意事項、前提条件、および注記に目を通し、準備をする必要があります。

システム基本設定の復元の準備をするには

保存したシステム基本設定ファイルを復元する前に、以下の注意事項、前提条件、注記について知っておく必要があります。

注意事項: 復元したシステム基本設定によって以下のいずれかの設定が変更される場合、システムと ztC Edge コンソールの接続が失われます。

- IP 構成
- セキュアな接続 (HTTP を有効にしてログインしていて、復元ファイルによって HTTP が無効化される場合)
- 日付と時刻



接続が失われると、復元処理は引き続きバックグラウンドで実行されますが、その進捗状況やステータスを表示することはできません。接続が失われた場合には、もう一度ログインしてください。(IP 構成の設定方法の詳細については、[「IP 設定を構成する」](#)を参照してください。セキュアな接続の設定方法の詳細については、[「セキュアな接続を構成する」](#)を参照してください。日付と時刻の設定方法の詳細については、[「日付と時刻を構成する」](#)を参照してください。)

前提条件:

- Active Directory (AD) の設定: 復元した基本設定によって AD が有効化される場合、ログイン時に AD の資格情報を提供する必要があります。AD を有効にする手順の詳細については、[「Active Directory を構成する」](#)を参照してください。

- **クォーラム サーバ**の設定:



- **[有効]** ステータスが復元されます。
- VM が既存のクォーラム サーバを使用することはできません。基本設定を復元する前に、使用中のすべての VM の電源をオフにしなければなりません。復元操作の最中にクォーラム サーバを使用している VM がある場合、**クォーラム サーバ**の復元は失敗します。
- この設定は単一ノードシステムには復元されません。

クォーラム サーバを有効にする手順の詳細については、[「クォーラム サーバを構成する」](#)を参照してください。

注: システム基本設定を復元する前に、以下を考慮してください。

- 基本設定を復元するターゲットのシステムと、復元に使用する保存済みの基本設定ファイルの元のシステムは、以下の点が同じでなければなりません。
 - 同じハードウェア モデル — 基本設定を復元するターゲットのシステムは、復元に使用する保存済みの基本設定ファイルの下のシステムと同じハードウェア モデルでなければなりません。
 - デュアルノード/単一ノード構成の一致 — デュアルノードのシステムに復元できるのは、デュアルノード システムで保存された基本設定だけです。単一ノードのシステムに復元できるのは、単一ノード システムで保存された基本設定だけです。
- システム基本設定を、元のバックアップより古いリリースやそれより新しいリリースを実行しているシステム上で復元する場合、古い方のリリースでサポートされる基本設定のみを復元できます。
- **iptables セキュリティ** — iptables の設定を復元するには、**[追加]** (復元ファイルの設定を既存のルール セットの後に追加する場合) または **[上書き]** (既存のルール セットを復元ファイルの設定で上書きする場合) のどちらかを選択する必要があります。(iptables の詳細については、[「iptables を管理する」](#)を参照してください。)
- **IP 構成** — 選択されている場合、すべてのネットワーク構成データが復元されます。(詳細については、[「IP 設定を構成する」](#)を参照してください。)
- **日付と時刻** — 直ちに復元されるのは **[自動]** の設定のみです。**[手動]** の設定や、異なるタイムゾーンと複数の NTP サーバをもつ設定を復元する場合、物理マシンの電源がオフになり、復元された日付と時刻の設定はシステムのリブート後に有効になります。(詳細は、[「日付と時刻を構成する」](#)を参照してください。)
- **[ユーザとグループ]** では、以下について考慮してください。
 - **[ユーザとグループ]** の設定を復元するには AD の資格情報を提供する必要があります。
 - ユーザ アカウントが現在のシステム上と復元ファイルの両方にある場合、現在のシステムはそのユーザ アカウントを編集されるものと見なします。



- ユーザ アカウントが復元ファイルにあり、現在のシステムにはない場合、現在のシステムはそのユーザ アカウントを追加されるものと見なします。
 - 以下の状況では現在のシステムが復元ファイルの AD エントリをスキップします。
 - 復元ファイルの AD エントリが、復元時に現在のシステム用に構成されている AD がない場合。
 - 復元ファイルの AD エントリが、復元時に現在のシステム用に構成されている AD エントリと一致しないユーザ タイプである場合。
- (ユーザとグループの詳細については、「[ユーザとグループを構成する](#)」を参照してください。)

注意事項、前提条件、および注記の内容を理解したら、システム基本設定の復元を行うことができます。

システム基本設定を復元するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[管理ツール]** の下で **[システム基本設定の復元]** をクリックします。
3. **[システム基本設定の復元]** の下で、次のいずれかを選択します。
 - このコンピュータ上に保存されたファイルからシステム基本設定を復元する —
 - a. **[ファイルの選択]** をクリックして、デフォルトの保存ディレクトリにあるファイルのリストを、保存されている zip ファイルも含めて表示します。必要な場合は別のディレクトリに移動してください。
 - b. 復元する**基本設定**を含むファイルをスクロールして選択し、ファイル名をクリックします。次のような表が表示されます。

システム基本設定を次から復元しています:

ファイル名	ztC_<アセット ID>_preferences_yyyy-mm-dd-hh-mm-ss.zip
-------	---

ソフトウェア バージョン	<バージョン番号>
説明	<説明>
キーワード	<キーワード>

復元された**基本設定**に「ユーザとグループ」が含まれる場合、次の情報も表示されます。

Active Directory の資格情報	「 ユーザとグループ 」の設定を復元するには、Active Directory の資格情報が必要です。
------------------------	--

選択したファイルにある設定を復元するには、**[次へ]** をクリックします。

- クラウドに保存されたファイルからシステム基本設定を復元する** — これを選択すると、リモート管理コンピュータがインターネットに接続している場合は、「Stratus カスタマ サービス ポータルにログオンしてアカウントを認証します。」というメッセージと、**[ユーザ名]** ボックスおよび **[パスワード]** ボックスが表示されます (アカウントにまだログインしていない場合)。リモート管理コンピュータがインターネットに接続していない場合は、インターネット接続が利用不可であることを示すメッセージが表示されます。(クラウド アカウントにログインした後、セッションはコンソール セッションがアクティブな間継続されます。コンソール セッションを閉じると、セッションがタイムアウトすると、自動的にログアウトされます。)

Stratus カスタマ サービス アカウントのユーザ名とパスワードを入力して **[ログイン]** をクリックします。

接続が確立されると、次の表に 1 つ以上のファイルが一覧されます。表示されるファイルの最大数は、保存ファイルの総数です。

アセット ID の選択 [ID の検索]	システム基本設定を復元する元のファイルを選択	
アセット ID	ファイル名	作成日
<アセット ID>	<ファイル名>	<時刻>

[**アセット ID**] 列には <アセット ID> フォルダのリストが表示されます。[**ファイル名**] 列には <アセット ID> フォルダ内にあるファイルが表示され、[**時刻**] 列にはファイルの保存時刻が表示されます。さらに、[「システム基本設定を次から復元しています:」](#)の表も表示されます。

[**アセット ID**] のリストの最初に現在のシステムの ID が表示され、[**ファイル名**] のリストの最初にその復元ファイル (存在する場合) が表示されます。この場合、一番上のファイル名をクリックして [**基本設定**] の設定を現在のシステムに復元します。

ファイルを検索するには、[ID の検索] ボックスにその "ファイル名" を入力します。

ファイルを選択するには、該当する <アセット ID> をクリックし、次に適切な <ファイル名> をクリックします。[**次へ**] をクリックして、選択したファイルから [**基本設定**] の設定を復元します。

4. [**復元するシステム基本設定を選択します**] ウィンドウが開いて基本設定のリストが表示されます。

デフォルトでは、次の基本設定が復元されます。

所有者情報	ztC Advisor
ソフトウェア更新	e アラート
クォーラム サーバ (デュアルノード システムのみ)	SNMP 構成
メール サーバ	OPC 構成
VM デバイスの構成	サポート構成
ログイン バナー通知	プロキシ構成

注:

次の基本設定はポップアップ メッセージの表示やシステムの再起動の原因となるため、デフォルトでは選択されていません。



- **日付と時刻** — 設定が変更されるとシステムがリブートします。
- **ユーザとグループ** — Active Directory (AD) が有効にされている場合、AD の資格情報を入力するウィンドウが表示されます。
- **セキュアな接続** — HTTP でログインしている場合に HTTP が復元ファイルによって無効化されると、システムへの接続が失われ、再度ログインが必要になります。
- **iptables セキュリティ** — 現在のルール セットを上書きするか、または復元されたルールを現在のルール セットに付加するかを選択するウィンドウが表示されます。
- **IP 構成** — IP 構成が変更されると、システムへの接続が失われ、再度ログインが必要になります。

復元対象ではない基本設定のチェックボックスはすべてオフにします。まだ選択されていない場合は追加の基本設定をすべて選択します。

5. **[リストア]** をクリックして選択した基本設定をシステムに復元するか、**[戻る]** をクリックして前のウィンドウに戻ります。いったん **[リストア]** をクリックすると、処理をキャンセルすることはできません。復元操作が完了するには約 1 分かかります。復元操作の処理中に ztC Edge コンソール ウィンドウ内で別の画面に移動することはできません。復元操作が完了するまで待ってから、別のコンソール ウィンドウを表示してください。

[復元ステータス] 列に、復元のステータスが**進行中**、**完了済み**、**一部完了**、または**失敗**として一覧されます。復元操作が完了すると、次のメッセージが表示されます。

完了。上記の基本設定が正常に復元されました。

6. **[完了]** をクリックします。最初の **[システムの基本設定の復元]** 画面が再び表示されます。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

e アラートを構成する

電子メール アラート (e アラート) を構成して、システムで管理者による対処が必要なイベントが発生したときに、ztC Edge システムが管理者に電子メールを送信できるようにします。



前提条件: e アラートが正しく機能するようにするには、メール サーバを構成する必要があります。「[メール サーバを構成する](#)」を参照してください。

e アラートを有効にするには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[通知]** の下で **[e アラート]** をクリックします。
3. **[e アラートの有効化]** ボックスをクリックします。以下の設定を指定や選択するためのボックスが表示されます。
 - **e アラートの言語** — プルダウン メニューから言語を選択します。
 - **受信者リスト** (必須) — すべての e アラート受信者の電子メール アドレスを入力します。
4. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。



注: e アラートの構成を有効にしたり更新した場合、テスト アラートを作成して、アラートを受信できることを確認します。

テスト アラートを作成するには

[テスト アラートの作成] をクリックします。Stratus Redundant Linux ソフトウェアがテスト アラートを作成して「テスト アラート」という件名のサンプル電子メールをすべての電子メール 受信者に送信します。SNMP が構成されている場合、SNMP がトラップの受信者にトラップを送信します (「[SNMP 設定を構成する](#)」を参照)。また、構成されている場合はサポート構成が Stratus 認定サービス業者に通知を送信します (「[リモート サポート設定を構成する](#)」を参照)。配信ステータスはアラート履歴ログ (「[アラート履歴](#)」ページ) を参照) で確認できます。

セカンダリ物理マシンをいったんメンテナンス モードにしてから (「[メンテナンス モード](#)」を参照) メンテナンス モードを解除することによって e アラートをテストすることもできます。両方のメンテナンス モード イベントに関する e アラートが受信されることを確認してください。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

SNMP 設定を構成する

ztC Edge システム用に簡易ネットワーク管理プロトコル (SNMP) の設定を構成して、SNMP 管理アプリケーションがシステムをリモートでモニタリングできるようにします。(SNMP 情報は個々の PM ではなく、システムのみに関する情報です。) SNMP 要求および SNMP トラップを次のように有効にできます。

- SNMP 要求 — Stratus Redundant Linux ソフトウェアでサポートされる MIB に登録されているオブジェクトの値を取得するために、システムに送信される要求。これには、ztC Edge システムを記述するオブジェクトの集合であるシステム固有の MIB が含まれます。MIB ファイルのコピーは、**[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) の **[Drivers and Tools (ドライバとツール)]** セクションからダウンロードできます。
- SNMP トラップ — アラートなどのイベントが発生した後、ztC Edge システムのいずれかのノードによって作成されるメッセージ。このメッセージは、通常ネットワーク管理ステーション (NMS) などの所定の受信者リスト宛てに送信されます。

適切な手順に従い、SNMP 要求またはトラップを有効化します。

SNMP 要求を有効にするには

SNMP 要求を有効にするには、次のいずれかの操作を実行します。

- **[基本設定]** ページから SNMP 要求を有効にします。
 - SNMPv3 要求を有効にできる、ztC Edge システムの完全な MIB への読み取り専用アクセスを持つ SNMPv3 ユーザを追加します。
 - SNMPv1 要求と SNMPv2 要求のアクセス制御を構成します。ここでは全ユーザに要求の送信を禁止 (**制限あり**) するか、あるいはデフォルトの public コミュニティを使用して全ユーザに許可 (**制限なし**) します。
- `snmpd.conf` ファイルを編集して SNMP 要求の機能をカスタマイズします。SNMPv1 要求と SNMPv2 要求のアクセス制御をカスタマイズできます。SNMPv3 要求のユーザのリス

トもカスタマイズすることができます。詳細については、下記の「[SNMP 要求の機能をカスタマイズするには](#)」を参照してください。


[基本設定] ページから SNMP 要求を有効にするには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[通知]** の下で **[SNMP 構成]** をクリックします。
3. **[SNMP 要求の有効化]** の横のチェック ボックスをオンにします。
4. **[SNMP 要求のユーザ リスト (バージョン 3)]** が表示されます。

[SNMP 要求のユーザ リスト (バージョン 3)] の下にユーザ名が表示される場合、そのユーザのセキュリティ レベルと、snmpd.conf ファイルの読み取り専用コピーも表示されます。ユーザは完全な MIB への読み取り専用アクセスをもっています。システムでサポートされる **SNMP 要求 (バージョン 3)** ユーザは 1 人だけであることに注意してください。

ユーザ名が表示されない場合、SNMPv3 ユーザを追加できます。

SNMPv3 ユーザを追加するには

- a.  **[追加]** ボタンをクリックすると、**ユーザの追加**ウィザードが起動します。
- b. 次の値を入力します。

ユーザ名 — SNMPv3 エージェントにアクセスできるユーザの名前。名前は一意でなければなりません。

セキュリティ レベル — ユーザのセキュリティ レベル。有効な値は次のとおりです。

- **認証なし・プライバシーなし** — メッセージにセキュリティが適用されず、認証も暗号化も行われません。
- **認証あり・プライバシーなし** — メッセージは認証されますが、暗号化はされません。**[認証タイプ]** と **[認証パスワード]** に値を入力する必要があります。
- **認証あり・プライバシーあり** — メッセージは認証され暗号化されます。**[認証タイプ]**、**[認証パスワード]**、**[暗号化タイプ]**、および **[暗号化パスワード]** に値を入力する必要があります。

セキュリティ レベルに認証またはプライバシーが含まれる場合、次のフィールドが表示されます。

認証タイプ — ユーザの認証のタイプ。有効な値は次のとおりです。

- **MD5:** メッセージ ダイジェスト アルゴリズム (MD5) をユーザの認証タイプとして構成します。
- **SHA:** セキュア ハッシュ アルゴリズム (SHA) をユーザの認証タイプとして構成します。

認証パスワード — ユーザの必須のパスワード。認証秘密鍵の生成に使用されます。パスワードは 8 文字以上でなければなりません。

暗号化タイプ — ユーザの暗号化のタイプ。有効な値は次のとおりです。

- **AES:** 高度暗号化標準 (AES) をユーザの暗号化タイプとして構成します。
- **DES:** データ暗号化標準 (DES) をユーザの暗号化タイプとして構成します。

暗号化パスワード — ユーザの必須のパスワード。暗号化秘密鍵の生成に使用されます。パスワードは 8 文字以上でなければなりません。

c. **[保存]** をクリックして変更を保存します。

5. アクセス オプションを選択します。

制限あり (デフォルト) — SNMPv1 要求と SNMPv2 要求の送信を全ユーザに禁止します。

制限なし — デフォルトの public コミュニティを使用して SNMPv1 要求と SNMPv2 要求の送信を全ユーザに許可します。

カスタム (snmpd.conf をユーザが手作業で編集した場合に利用可能。下記の「[SNMP 要求の機能をカスタマイズするには](#)」を参照) — カスタムのアクセスを可能にします。

6. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

snmpd.conf ファイルを編集して SNMP 要求の機能をカスタマイズするには

snmpd.conf ファイルを編集して SNMP 要求の機能をカスタマイズします。

SNMPv1 要求と SNMPv2 要求のアクセス制御をカスタマイズするには、次のように /etc/snmp/snmpd.conf ファイルを編集します。

1. ホストにログインします。
2. 両方のノードで標準の `/etc/snmp/snmpd.conf` ファイルを手作業で編集します。
3. ファイルを保存します。
4. **`systemctl restart snmpd`** コマンドを入力して各ノードで `snmpd` プロセスを再起動します。

SNMPv3 要求のユーザのリストをカスタマイズするには、次のように

`/etc/snmp/snmpd.conf` ファイルと `/var/lib/net-snmp/snmpd.conf` ファイルを編集します。

1. ホストにログインします。
2. 両方のノードで標準の `/etc/snmp/snmpd.conf` ファイルを手作業で編集します。
3. 両方のノードで標準の `/var/lib/net-snmp/snmpd.conf` ファイルを手作業で編集します。
4. ファイルを保存します。
5. **`systemctl restart snmpd`** コマンドを入力して各ノードで `snmpd` プロセスを再起動します。

SNMP トラップを有効にするには

注:




1. **SNMP トラップ (バージョン 3)** の受信者を追加する場合、受信サーバ上のトラップ ユーザのエンジン ID が `0x80001370017F000001` であることを確認する必要があります。
2. SNMP トラップの構成を有効にしたり更新した場合、テスト アラートを作成して、トラップを受信できることを確認します。

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[通知]** の下で **[SNMP 構成]** をクリックします。
3. **[SNMP トラップの有効化]** の横のチェック ボックスをオンにします。
4. SNMP コミュニティの名前を入力するか、デフォルト値 (**public**) のままにします。

5. **[SNMP トラップの受信者リスト (バージョン 3)]** の下に、トラップ ユーザのリストと、トラップ ユーザがいる受信サーバの IP アドレスが表示されます。ztC Edge システムは受信サーバ上のトラップ ユーザに SNMPv3 トラップを送信します。必要に応じて受信者を追加します。

受信者を追加するには

- a.  **[追加]** ボタンをクリックして、**受信者の追加**ウィザードを起動します。
- b. 次の値を入力します。

受信者アドレス — 受信サーバのホスト名または IPv4 アドレス。

ユーザ名 — 受信サーバ上のトラップ ユーザの名前。名前はその受信者に一意でなければなりません。

セキュリティ レベル — ユーザのセキュリティ レベル。有効な値は次のとおりです。

- **認証なし・プライバシーなし** — メッセージにセキュリティが適用されず、認証も暗号化も行われません。
- **認証あり・プライバシーなし** — メッセージは認証されますが、暗号化はされません。**[認証タイプ]** と **[認証パスワード]** に値を入力する必要があります。
- **認証あり・プライバシーあり** — メッセージは認証され暗号化されます。**[認証タイプ]**、**[認証パスワード]**、**[暗号化タイプ]**、および **[暗号化パスワード]** に値を入力する必要があります。

セキュリティ レベルに認証またはプライバシーが含まれる場合、次のフィールドが表示されます。

認証タイプ — ユーザの認証のタイプ。有効な値は次のとおりです。

- **MD5:** メッセージ ダイジェスト アルゴリズム (MD5) をユーザの認証タイプとして構成します。
- **SHA:** セキュア ハッシュ アルゴリズム (SHA) をユーザの認証タイプとして構成します。

認証パスワード — ユーザの必須のパスワード。認証秘密鍵の生成に使用されます。パスワードは 8 文字以上でなければなりません。

暗号化タイプ — ユーザの暗号化のタイプ。有効な値は次のとおりです。

- **AES**: 高度暗号化標準 (AES) をユーザの暗号化タイプとして構成します。
- **DES**: データ暗号化標準 (DES) をユーザの暗号化タイプとして構成します。

暗号化パスワード — ユーザの必須のパスワード。暗号化秘密鍵の生成に使用されます。パスワードは 8 文字以上でなければなりません。

c. **[保存]** をクリックして変更を保存します。

6. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。
7. 組織のファイアウォールを構成して、SNMP 操作を許可して SNMP 管理システムが ztC Edge システムとの間でアラートの受信とトラップの送信を行えるようにします。そのためには、SNMP ポートを開くように組織のファイアウォールを構成します。

メッセージ タイプ: SNMP

プロトコル: SNMP

ポート: 161 (Get/Walk) 162 (トラップ)

8. **[テスト アラートを作成]** をクリックしてテスト アラートを作成します。

Stratus Redundant Linux ソフトウェアがテスト アラートを生成し、SNMP がトラップを SNMP トラップの受信者に送信します。構成されている場合には e アラートが「テスト アラート」という件名のサンプル電子メールを e アラートのすべての電子メール受信者に送信します ([「e アラートを構成する」](#) を参照)。さらに、構成されている場合はサポート構成によって Stratus 認定サービス業者に通知が送信されます ([「リモート サポート設定を構成する」](#) を参照)。配信ステータスはアラート履歴ログ ([「\[アラート履歴\] ページ」](#) を参照) で確認できます。

関連トピック

[「SNMP」](#)

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

[「セキュリティの強化」](#)

OPC 設定を構成する

Open Platform Communication (OPC) の設定を構成して、OPC サーバの機能を有効にします。この機能は OPC クライアントによって受信され表示される ztC Edge システムのパフォーマンス データを発行します。これにより、ztC Edge システムを他の産業機械と一緒にモニタリングできるようになります。

OPC 機能を使用するには、OPC クライアント ソフトウェアを選択して個別のコンピュータにインストールしてから、OPC クライアントを構成してください (「[OPC クライアントをインストールおよび構成するには](#)」を参照)。OPC クライアントは、OPC 用に構成する ztC Edge システム上のポートからデータを受信するように構成しなければなりません。デフォルトのポートは 4840 ですが、それ以外のポート番号も指定できます。

OPC 設定を構成するには

1. 左側にあるナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[通知]** の下で **[OPC 構成]** をクリックします。
3. **[OPC サーバの有効化]** の横のチェック ボックスをオンにします。
4. デフォルトのポート番号は **4840** です。必要に応じて別の番号を指定します。
5. システムに合わせて次のチェック ボックスのうち 1 つまたは両方をオンにします。

匿名 OPC クライアント接続の許可 — OPC クライアントは ztC Edge システム上の OPC サーバに接続する際にユーザ名とパスワードを必要としません。(チェック ボックスがオンにされていない場合、OPC クライアントがユーザ名とパスワードを提供する必要があります。)

[ユーザとグループ] で構成されたユーザ名とパスワードによる OPC クライアント接続の許可 — OPC クライアントは ztC Edge へのログインに使用するのと同じユーザ名とパスワードを使って ztC Edge コンソールシステム上の OPC サーバに接続することができます。(チェック ボックスをオンにしない場合、OPC クライアントは、**[ユーザとグループ]** ページで指定したローカル ユーザ アカウントのユーザ名とパスワードを使って OPC サーバにログインすることができません。

「[ローカル ユーザ アカウントを管理する](#)」を参照してください。)

6. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

OPC クライアントをインストールおよび構成するには

OPC クライアント ソフトウェアは個別のコンピュータにインストールして構成する必要があります。数多くの市販製品から好みの OPC クライアント ソフトウェアを選択できます。下記の手順では、Unified Automation 社の UaExpert[®] ソフトウェアを使用して OPC クライアントをインストールして構成する方法を説明します。

UaExpert ソフトウェアを使用して OPC クライアントをインストールおよび構成する



注: 以下の手順だけでなく、UaExpert ソフトウェアに付属の操作手順にも従ってください。

1. UaExpert ソフトウェアの Windows バージョンをダウンロードしてインストールします。
<https://www.unified-automation.com/products/development-tools/uaexpert.html> を参照してください。
2. UaExpert ソフトウェアを初めて起動する場合、ソフトウェアを初回起動する際の指示に従ってください。
3. UaExpert ソフトウェアを実行します。

[Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject (Unified Automation UaExpert - OPC Unified Architectureクライアント - 新規プロジェクト)] というメイン ウィンドウが開きます。

4. メニュー バーの **[Server (サーバ)]** をクリックして **[Add (追加)]** を選択します。 **[Add Server (サーバの追加)]** ダイアログ ボックスが表示されます。
5. **[Advanced (詳細)]** タブをクリックします。
6. **[Endpoint Url (エンドポイント URL)]** ボックスにエンドポイントの URL を入力します。これは ztC Edge システムのクラスタ IP アドレスです (例: **opc.tcp://tcp_cluster_ip_address:4840/**)。
7. **[Security Settings (セキュリティ設定)]** で、**[Security Policy (セキュリティ ポリシー)]** と **[Message Security Mode (メッセージ セキュリティ モード)]** の両方に **[None (なし)]** を選択します。
8. **[Authentication Settings (認証設定)]** で、お使いの構成に適したものを次から 1 つ選択します。

Anonymous (匿名) — 匿名 OPC クライアント接続を許可するチェック ボックスをオンにした場合、これを選択します。

Username (ユーザ名) および **Password (パスワード)** — ユーザ名とパスワードを使用した OPC クライアント接続を許可するチェック ボックスをオンにした場合、値を入力します。入力するユーザ名とパスワードは、ztC Edge システム上で OPC アクセス用に読み取り専用ユーザのために追加されるユーザ名とパスワードに一致していなければなりません。

ん。ztC Edge システムにユーザを追加する方法の詳細については、「[ローカルユーザアカウントを管理する](#)」を参照してください。

9. **[OK]** をクリックして **[Add Server (サーバの追加)]** ダイアログ ボックスを閉じます。

メイン ウィンドウが再び表示されます。左側のパネルで、**[Servers (サーバ)]** の下の **[Project (プロジェクト)]** ボックスにサーバの名前が表示されます。

10. 新しいサーバを選択してから、ツール バーでマイナス記号のアイコンの右に表示される接続ボタンをクリックします。

クライアントがサーバに正しく接続すると、メイン ウィンドウの **[Address Spaces (アドレス空間)]** ボックスにサーバのエンド ポイントが表示されます。

[Address Spaces (アドレス空間)] ボックスで最上位レベルをクリックして展開表示すると、利用できるデータ値を検査できます。**[Attributes (属性)]** ボックスの **[Value (値)]** 列に、選択した項目の現行値が表示されます。

関連トピック

[「OPC 出力を表示する」](#)

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

OPC 出力を表示する

ztC Edge システム上で OPC サーバの機能を有効化した後、(ztC Edge システムではないコンピュータ上の) OPC クライアントから、システムのパフォーマンス データを発行することができます。このデータは複数のアドレス空間に分割され、その各アドレス空間がいくつかのデータ項目を含むサブオブジェクトに分かれています。ztC Edge システム上の OPC サーバ機能がデータ項目の値を OPC クライアントに渡し、クライアントがデータを表示します。

このトピックでは、Unified Automation の UaExpert[®] ソフトウェアで作成された OPC クライアントを使って ztC Edge システムの情報を表示する方法を説明します。

OPC 出力を表示する

1. OPC クライアントを作成したコンピュータ上で、OPC クライアントを開きます。
2. 左側の **[Project (プロジェクト)]** パネルで、**[Project (プロジェクト)]**、**[Servers (サーバ)]**、**[ztC OPC Server (ztC OPC サーバ)]** の順にクリックします。

[Project (プロジェクト)] の下の左パネルに **[Address Space (アドレス空間)]** が表示されます。**[ztC OPC Server (ztC OPC サーバ)]** を選択すると、**[Address Space (アドレス空間)]** パネルに **[Root (ルート)]** の階層が表示されます。

3. **[Address Space (アドレス空間)]** パネルで、**[Root (ルート)]** の下の **[Objects (オブジェクト)]** をクリックします。**[Objects (オブジェクト)]** の下で、**[Server (サーバ)]** と **[ztC]** を選択できます。

■ サーバ

現在 OPC サーバを実行しているノードに関する情報は、**[BuildInfo (ビルド情報)]** サブオブジェクトで確認できます。**[Server (サーバ)]**、**[ServerStatus (サーバステータス)]** の順にクリックします。

[BuildInfo (ビルド情報)] サブオブジェクトに、次のデータ項目の値が表示されます。

データ項目	説明
ProductUrl	「 http://www.stratus.com/ 」と表示されます。
ManufacturerName	「 Stratus Technologies Ireland, Ltd 」と表示されます。
ProductName	ハードウェアの製品名 (ztC Edge) が表示されます。
SoftwareVersion	Stratus Redundant Linux ソフトウェアのバージョン番号が表示されます。
BuildNumber	Stratus Redundant Linux ソフトウェアのビルド番号が表示されます。
BuildDate	Stratus Redundant Linux ソフトウェアのビルドの

データ項目	説明
	日付が表示されます。

Server オブジェクトのその他の情報は、『OPC Unified Architecture Specification』の「Part 5: Information Model」を参照してください。この文書は opcfoundation.org から入手できます。

- **ztC** — ztC オブジェクトは、アドレス空間を、次の各表に示すデータ項目を含むサブオブジェクトに分割します。

アプリケーション

アプリケーションのデータ項目は、アプリケーションの稼働状態に関する情報を提供します。

データ項目	説明
AlertedApplicationsCount	AlertedApplicationsList にあるアプリケーションの数を表示します。 データ型: UInt32
AlertedApplicationsList	現在モニタリング対象のアプリケーションのうち、ステータスが正常でないか、利用不可のもの (<i>Not Running</i> (停止中)、 <i>Not Responding</i> (応答なし)、 <i>Unavailable</i> (利用不可)、および <i>Not found</i> (検出不可)) を一覧します。このリストには停止している VM のアプリケーションが含まれます。アクティブでないモニタ ([Monitor (モニタ)] タブの [Applications (アプリケーション)] パネルにある、 [Enabled (有効)] ボックスがオフになっているアプリケーション モニタ) はリストに含まれません。

データ項目	説明
	データ型: 動的な文字列配列
AllApplicationsHealthy	<p>モニタリング対象のアプリケーションに警告があるかどうかを示します。<i>true</i> の場合は警告がなく、<i>false</i> の場合は 1 つ以上のモニタリング対象アプリケーションに警告があります。</p> <p>データ型: Boolean</p>
ApplicationMonitoringEnabled	<p>アプリケーションのモニタリングにライセンスが適用され有効になっているかを示します。<i>true</i> の場合は有効です。<i>false</i> の場合は有効にされていません。</p> <p>データ型: Boolean</p>
ApplicationsCount	<p>現在モニタリング対象となっているアプリケーションの数を示します。この値は ApplicationsList のアプリケーションの数と一致します。</p> <p>データ型: UInt32</p>
ApplicationsList	<p>現在モニタリング対象となっているアプリケーションを一覧します。これは 1 次元の配列で、モニタリング対象のアプリケーションが追加や削除されると、それに応じて増減します。アクティブでないモニタ (Monitor (モニタ)) タブの Applications (アプリケーション) パネルにある、Enabled (有効) ボックスがオフになっているアプリケーション モニタ) はリストに含まれません。リストされ</p>

データ項目	説明
	る名前には、アプリケーション名の前に接頭辞として VM 名が含まれています (例: vm1/testapp.exe)。 データ型: 動的な文字列配列

物理マシン

物理マシンのデータ項目は、システム内の個々のノードが正常かどうかについての情報を提供します。

データ項目	説明
AllPhysicalMachinesHealthy	両方のノードが正常かどうかを示します。 <i>true</i> の場合は両方のノードが存在し、緑のチェックマーク付きで実行され、メンテナンス モードになっていません。 <i>false</i> の場合は片方または両方のノードが存在しないか、緑のチェックマーク付きで実行されていないか、メンテナンス モードになっていません。 データ型: Boolean
node0 および node1	NodenHostState: ホストの状態。有効な値には次が含まれます: <i>exiled</i> (除外済み)、 <i>failed</i> (失敗)、 <i>firmware</i> (ファームウェア)、 <i>imaging</i> (イメージング)、 <i>lost</i> (損失)、 <i>nfc</i> 、 <i>off</i> (オフ)、 <i>proto</i> (プロト)、 <i>running</i> (実行中)、 <i>starting</i> (開始中)、 <i>stopping</i> (停止中)、 <i>unlicensed</i> (ライセンスなし)、 <i>unreachable</i> (アクセス不可)。

データ項目	説明
	<p>NodenIPAddress: ノードの IP アドレス。</p>
	<p>NodenMaintenanceMode: ホストのメンテナンス モード。有効な値には次が含まれます: <i>evacuating</i> (退去中)、<i>maintenance</i> (メンテナンス)、<i>normal</i> (正常)。</p>
	<p>NodenExists: ノードがシステムで認識されているかどうかを示します。 <i>true</i> の場合はノードがシステムに正しく接続しています。 <i>false</i> の場合は 2 つ目のノードがシステムに追加されていないか、2 つ目のノードが追加された後で削除されています。この値が <i>false</i> の場合、<i>noden</i> の他のすべての情報は無視してください。</p>
	<p>NodenVirtualMachineList: このノードで実行中の仮想マシン (VM) を一覧します。</p>
	<p>NodenCombinedState: NodenMaintenanceMode、 NodenExists、NodenHostState の組み合わせを次のように示します。</p> <ul style="list-style-type: none"> ◦ NodenExists が <i>false</i> の場合、 NodenCombinedState は <i>missing</i> (不在) です。 ◦ NodenExists が <i>true</i>、

データ項目	説明
	<p>NodenHostState が <i>running</i> (実行中)、および</p> <p>NodenMaintenanceMode が <i>evacuating</i> (退去中) または <i>maintenance</i> (メンテナンス) の場合、NodenCombinedState は <i>evacuating</i> (退去中) または <i>maintenance</i> (メンテナンス) です。</p> <p>◦ NodenCombinedState がそれ以外の値の場合、これは NodenHostState の値を示します。NodenHostState の有効値の範囲は上記のとおりです。</p>
PhysicalMachinesList	<p>存在するノードを一覧します。</p> <p>データ型: 動的な文字列配列</p>
PhysicalMachinesWarningCount	<p>緑のチェックマークが付いていない物理マシンの数を表示します。</p> <p>データ型: UInt32</p>
PhysicalMachinesWarningList	<p>問題を報告している物理マシンを一覧します。このリストは通常、両方のノードを含みます。たとえば、セカンダリがメンテナンス モードにあり、プライマリが安全でない場合など。</p> <p>データ型: 動的な文字列配列</p>
PrimaryPhysicalMachine	<p>現在のプライマリ ノードの名前を表示します。</p>

データ項目	説明
	データ型: 文字列

仮想マシン

仮想マシンのデータ項目は、システム上で実行中の VM のステータスについての情報を提供します。

データ項目	説明
AllVirtualMachinesHealthy	警告またはエラーのステータスをもつ VM があるかどうかを示します。 <i>true</i> の場合、すべての VM に緑のチェックマークが付いています。 <i>false</i> の場合、緑のチェックマークが付いていない VM が 1 つ以上あります。 データ型: Boolean
FTVirtualMachinesList	システム上に存在する FT VM の名前を一覧します。 データ型: 動的な文字列配列
GetPhysicalMachine	指定の VM をどの物理マシンが実行しているかを示します。 データ型: 1 つの文字列を受け入れて 1 つの文字列を返す関数 (関数の入力引数は VM 名を示す文字列、出力は入力引数に指定された VM を現在実行している物理マシンを示す文字列、つまり node0 または node1 です)
HAVirtualMachinesList	システム上に存在する HA VM の名前を一覧します。

データ項目	説明
	データ型: 動的な文字列配列
RunningVirtualMachinesCount	RunningVirtualMachinesList にある VM の数を表示します。 データ型: UInt32
RunningVirtualMachinesList	<i>running</i> (実行中) とマークされている VM の名前を一覧します。 データ型: 動的な文字列配列
StoppedVirtualMachinesCount	StoppedVirtualMachinesList にある VM の数を表示します。 データ型: UInt32
StoppedVirtualMachinesList	<i>stopped</i> (停止) とマークされている VM の名前を一覧します (<i>booting</i> (ブート中) など推移中の状態は無視します)。 データ型: 動的な文字列配列
VirtualMachinesCount	システム上に存在する VM の数を表示します。 データ型: UInt32
VirtualMachinesList	システム上に存在する VM の名前を一覧します。 データ型: 動的な文字列配列

システム

システムのデータ項目は、高レベルのステータス情報に加え、システム全体のアクセス メソッドに関する情報も提供します。

データ項目	説明
ManagementConnectionGood	OPC サーバが ztC Edge システムから情報を取得できるかどうかを示します。 <i>true</i> の場合、サーバがシステムから情報を取得できます。 <i>false</i> の場合、サーバは情報を取得できません。 データ型: Boolean
ManagementIP	ztC Edge システムの、システムの IP アドレスを示します。 データ型: 文字列
ManagementURL	ztC Edge コンソールの HTTP URL を示します。 データ型: 文字列
OutstandingSeverity	ログイン ページのシステム全体のステータス アイコンに対応します。 データ型: 文字列
SecureManagementURL	ztC Edge コンソールの HTTPS URL を示します。 データ型: 文字列

関連トピック

[「OPC 設定を構成する」](#)

リモート サポート設定を構成する

ztC Edge システムに初めてログインするときに、サポート構成を設定して、注意の必要なイベントが発生すると ztC Edge システムがサポート通知 (アラート) を Stratus 認定サービス業者に送信する機能を有効にします。

サポート構成の設定を行うには



注: [リモート サポート アクセスの有効化] または [通知の有効化] の設定を有効にしたり変更する際は、Stratus 認定サービス業者が担当のシステムからのシステム稼動状態に関するメッセージを受信できることを確認するテスト アラートを作成します。

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[リモート サポート]** の下で **[サポート構成]** をクリックします。
3. システムに応じて、適切な設定に変更します。
 - **[リモート サポート アクセスの有効化]** を使用すると、Stratus 認定サービス業者 がトラブルシューティングの目的で ztC Edge システムにリモート接続できます。この設定は、有効にした後でも必要に応じて無効にすることができます。
 - **[通知の有効化]** を使用すると、ztC Edge システムから Stratus 認定サービス業者に稼動状態とステータスの通知を送信できます。
 - **[サポート通知の有効化]** は、注意が必要なすべてのイベントに関してアラートを送信します。また、Stratus 認定サービス業者に定期的な "ハートビート" call-home メッセージも送信します。
 - **[定期レポートの有効化]** を使用すると、システム情報のサマリを毎日送信し、製品およびサービスの品質向上に役立てることができます。
4. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。
5. 組織のファイアウォールを構成して、サポート メッセージが許可されるようにします。

サポート メッセージが許可されるようにファイアウォールを構成するには

次の情報を使用して、企業のファイアウォールを、Stratus 認定サービス業者との通信が許可されるように構成します。

メッセージ タイプ: Call-home とライセンス

プロトコル: TCP

ポート: 443

Stratus サポート サーバ アドレス: *.stratus.com

メッセージ タイプ: サポート診断

プロトコル: TCP

ポート: 443

Stratus サポート サーバ アドレス: *.stratus.com

メッセージタイプ: Dial-in

プロトコル: TCP

ポート: 443、デフォルトプロキシポート: 3128 (デフォルトプロキシポート番号は変更できます。)

Stratus サポート サーバ アドレス: *.ecacsupport.com

メッセージタイプ: e アラート

プロトコル: SMTP

ポート: 25

(TCP および UDP ポートの詳細については、ナレッジベースにアクセスして、「TCP and UDP ports used by ztC Edge (ztC Edge で使用される TCP および UDP ポート)」という記事 (KB-9357) を検索してください。[[ナレッジベースの記事にアクセスする](#)] を参照してください。)

SNMP 管理システムを有効にして、アラートを受信して ztC Edge システムにトラップを送信するには、ファイアウォールを以下のように構成します。

メッセージタイプ: SNMP

プロトコル: SNMP

ポート: 161 (Get/Walk) 162 (トラップ)

6. テストアラートを作成します。

テストアラートを作成するには

[[テストアラートの作成](#)] をクリックします。Stratus Redundant Linux ソフトウェアがテストアラートを生成し、サポート構成が Stratus 認定サービス業者に通知を送信し、構成されている場合は e アラートが「テストアラート」という件名のサンプル電子メールを e アラートのすべての電子メール受信者に送信します ([[e アラートを構成する](#)] を参照)。さらに、構成されている場合は SNMP によって SNMP トラップの受信者にトラップが送信されます ([[SNMP 設定を構成する](#)] を参照)。配信ステータスはアラート履歴ログ ([[アラート履歴](#)] ページ) を参照) で確認できます。サポート通知に失敗すると、後続のアラートが作成されます。

関連トピック

[[ztC Edge コンソール](#)]

[[基本設定](#)] ページ]

[[ztC Edge コンソールを使用する](#)]

インターネットプロキシ設定を構成する

組織でインターネット アクセスにプロキシ サーバを使用する必要がある、ztC Edge あるいは他の認定 Stratus サービス業者とサービス契約を交わしている場合は、ztC Edge システムのプロキシ設定を構成します。

プロキシ サーバは ztC Edge システムとインターネットとの間のセキュアなブリッジとして機能します。Stratus Redundant Linux ソフトウェアは、サポート通知メッセージまたはリモート サポートのアクセス機能に関連する発信 HTTP トラフィック用としてのみプロキシ サーバ情報を使用します。

インターネットプロキシ設定を構成するには

1. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
2. **[リモート サポート]** の下で **[プロキシ構成]** をクリックします。
3. プロキシ サービスを有効にするには、**[プロキシの有効化]** ボックスをクリックします。
4. **[プロキシ サーバ]** ボックスにプロキシ サーバの完全修飾ホスト名か、IP アドレスを入力します。
5. デフォルトのポート番号 (3128) と異なるポートを使用する場合は、**[ポート番号]** ボックスにポート番号を入力します。
6. プロキシ サーバに認証が必要な場合、**[認証の有効化]** ボックスをクリックし、**[ユーザ名]** と **[パスワード]** を入力します。

パスワードを指定しない場合、以前のパスワードが引き続き必須になります。以前のパスワードが空で、新しいパスワードも入力しない場合、パスワードは空のままになります。
7. **[保存]** をクリックするか、以前の保存値に戻すには **[リセット]** をクリックします。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

[アラート履歴] ページ

[アラート履歴] ページには、ztC Edge システムで発生したイベントに関するメッセージが表示されます。

[アラート履歴] ページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで **[アラート履歴]** をクリックします。(ztC Edge システムにおけるユーザ アクティビティのログを表示するには、[「\[監査ログ\] ページ」](#) を参照してください。)

注: サポート通知アラート、e アラート、および SNMP トラップが生成されるのは、ztC Edge コンソールでこれらを有効にした場合のみです。詳細については、次を参照してください。



- [「リモート サポート設定を構成する」](#)
- [「e アラートを構成する」](#)
- [「SNMP 設定を構成する」](#)

アラートに関する情報を表示するには、アラートを下にスクロールします。デフォルトでは一番新しいものから順に表示されます。アラートをクリックすると、アラートが発生した日時、問題とその解決策 (該当する場合) に関する情報、およびこのアラートに対して **[サポート通知]**、**[e アラート]**、**[SNMP トラップ]** のうちどれが送信されたかが表示されます。(アラート情報の表示には `snmptable` を使用することもできます。[「snmptable でシステム情報を取得する」](#) を参照してください。)

アラートを削除するには、アラートを選択して **[削除]** をクリックします。

アラートをすべて削除するには、**[すべてページ]** をクリックします。

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[監査ログ] ページ

[監査ログ] ページには、ztC Edge コンソールにおけるユーザ アクティビティのログが表示されます。このページを開くには、左側のナビゲーション パネルで **[監査ログ]** をクリックします。(ztC Edge システムで発生したイベントのログを表示するには、[「\[アラート履歴\] ページ」](#) を参照してください。)

ログに関する情報を表示するには、ログ エントリを下にスクロールします。デフォルトでは一番新しいものから順に表示されます。次の情報が表示されます。

- **時刻** — アクションの日付と時刻。
- **ユーザ名** — アクションを開始したユーザの名前。

- **発信元ホスト** — ztC Edge コンソールを実行していたホストの IP アドレス。
- **アクション** — ztC Edge コンソールで実行されたアクション。

監査ログ情報の表示には `snmptable` を使用することもできます ([「snmptable でシステム情報を取得する」](#) を参照してください)。

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[「セキュリティの強化」](#)

[サポート ログ] ページ

[サポート ログ] ページでは、診断ファイルの生成を行えます。診断ファイルには、特定時点における ztC Edge システムのログ ファイルと構成情報が含まれます。Stratus 認定サービス業者はこの情報を使用して、システムの問題を解決することができます。

詳細については、次を参照してください。

- [「診断ファイルを作成する」](#)
- [「診断ファイルを削除する」](#)
- [「診断ファイルをカスタム サポートにアップロードする」](#)

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[「\[基本設定\] ページ」](#)

診断ファイルを作成する

診断ファイルは特定時点における ztC Edge システムのログ ファイルと構成情報を提供します。診断ファイルを作成すると、Stratus 認定サービス業者によるシステムの問題解決に役立ちます。



注: Stratus Redundant Linux ソフトウェアは診断ファイル用に一定容量のストレージを割り当てます。診断ファイルの作成時に十分な空き容量がない場合、システムは以前に作成されたファイルを削除します。

診断ファイルを作成するには

1. 左側のナビゲーション パネルで **[サポート ログ]** をクリックして **[サポート ログ]** ページを表示します。
2. **[診断ファイルの生成]** をクリックします。
3. Stratus 認定サービス業者にファイルをアップロードします。手順については、[「診断ファイルのカスタマ サポートにアップロードする」](#) を参照してください。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

診断ファイルをカスタマ サポートにアップロードする

Stratus ztC Edge カスタマ サポート Web サイトに診断ファイルをアップロードして、システムの問題解決に役立てます。(診断ファイルを作成するには、[「診断ファイルを作成する」](#) を参照してください。)

診断ファイルをカスタマ サポートにアップロードするには

1. 左側のナビゲーション パネルで **[サポート ログ]** をクリックして **[サポート ログ]** ページを表示します。
2. 次のいずれかを実行します。
 - ztC Edge システムがインターネットに接続している場合、**[アップロード]** をクリックして診断ファイルを Stratus ztC Edge カスタマ サポート Web サイトに直接アップロードします。アップロードが成功した場合、診断ファイルが正しくアップロードされたことを伝えるメッセージが表示されます。
 - ztC Edge システムがインターネットに接続されていない場合や、**アップロード** に失敗した場合、診断ファイルを **[Stratus Diagnostic Upload (Stratus 診断のアップロード)]** Web ページに手動でアップロードできます。まず、ztC Edge コンソールで **[ダウンロード]** をクリックして診断ファイルをローカル コンピュータに .zip ファイルとしてダウンロードします。zip 形式の診断ファイルを、インターネットに接続しているコンピュータに転送します。Web ブラウザを開いてアドレス バーに [「http://diags.stratus.com/DiagUpload.html」](http://diags.stratus.com/DiagUpload.html) と入力します。**[Stratus Diagnostic**

Upload (Stratus 診断のアップロード)] ページで **[Choose File (ファイルの選択)]** をクリックし、コンピュータ上のファイルを選択して **[Submit (送信)]** をクリックします。

この手順の詳しい説明が必要な場合、ztC Edge カスタマ サポートまでお問い合わせください。電話番号は **ztC Edge サポート** ページ (<https://www.stratus.com/services-support/customer-support/?tab=ztcedge>) に記載されています。

ファイルが一切不要になった時点で (たとえば、カスタマ サポートによりファイルが正しくアップロードされたことが確認された時点で)、オプションで「**診断ファイルを削除する**」の説明に従って、ファイルを ztC Edge システムから削除することができます。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

診断ファイルを削除する

診断ファイルを Stratus 認定サービス業者にアップロードした後、ztC Edge システムから削除します。

診断ファイルを削除するには

1. 左側のナビゲーション パネルで **[サポート ログ]** をクリックして **[サポート ログ]** ページを表示します。
2. 診断ファイルを選択し、**[削除]** をクリックします。

関連トピック

[「ztC Edge コンソール」](#)

[「\[基本設定\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

[物理マシン] ページ

[物理マシン] ページでは、ztC Edge システムの物理マシン (PM) を管理できます。(PM はノードとも呼ばれます。)このページを開くには、左側のナビゲーション パネルで **[物理マシン]** をクリックします。

[物理マシン] という見出しとマストヘッドのすぐ下に、**[状態]**、**[アクティビティ]**、**[名前]**、**[モデル]**、**[VM の数]** の各列が表示されます。特定の PM を管理するには、**[名前]** の下で **[node0 (プライマリ)]** または **[node1]** (存在する場合) をクリックします。PM の状態とアクティビティの意味については、[「物理マシンの状態とアクティビティ」](#) を参照してください。ノードに関する情報の表示には、`snmptable` コマンドを使用します ([「snmptable でシステム情報を取得する」](#) を参照してください)。

下部パネルにはアクション ボタンおよび選択したノードの詳細情報が表示されます。

- アクション ボタン: 選択したノードの状態に応じてさまざまなアクション ボタンが表示されます。非アクティブなボタンはグレー表示されています。通常の場合、メンテナンス タスクを実行するには **[作業開始]** をクリックしてノードをメンテナンス モードに切り替える必要があります (詳細については、[「メンテナンス モード」](#) を参照してください)。メンテナンス モードで利用できる追加の PM アクションについては、[「物理マシンのアクション」](#) か、実行するタスクのヘルプ トピックを参照してください。
- 詳細情報: 選択したノードの詳細や統計を表示するには、次のいずれかのタブをクリックします。
 - **[サマリ]** (初期表示) には、選択したノードについて、メーカー、モデル、シリアル番号、総合状態、アクティビティ、および構成 (メモリおよび論理ディスク) などの該当する情報が表示されます。
 - **[説明]** には、ノードに関する情報を入力できるウィンドウが表示されます。
 - **[ストレージ]** には、ストレージの状態、論理 ID、サイズ、および使用サイズが表示されます。SSD ドライブの余命も表示されます。
 - **[ネットワーク]** には、ネットワークの状態、名前、速度、および MAC アドレスが表示されます。
 - **[センサー]** には、センサーの名前、状態、および CPU とシステム (ノード) の電圧と温度を含む現在のセンサー値が表示されます。
 - **[仮想マシン]** には、仮想マシンの状態、アクティビティ、および名前が表示されます。
 - **[USB デバイス]** には、ノードに挿入されている USB デバイスがすべて一覧されます。
 - **[モニタ]** には、システムに関する情報 (CPU 使用率、メモリ使用状況など) が表示されます。詳細については、[「ztC Edge システムをモニタリングする」](#) を参照してください。

関連トピック

[「ztC Edge コンソール」](#)





[「ztC Edge コンソールを使用する」](#)




物理マシンのアクション

物理マシン (PM) を選択すると、PM の状態とアクションに応じて以下のアクション ボタンまたはこの一部が表示されます。非アクティブなボタンはグレー表示されています。



注意事項: PM のメンテナンスを行うには、ztC Edge コンソールの **[物理マシン]** ページを使用します。コンピュータのコントロールは使用しないでください。ztC Edge コンソールは、サービスの中断につながる可能性のある大半のアクションから ztC Edge システムを守ります。

コマンド	説明
 検出	[名前] の下で選択されているノードの SYS LED を点滅させます。 「物理マシンを識別する」 を参照してください。
 作業開始	PM をメンテナンス モードにします。この PM で実行中の VM は、もう片方の PM が存在し、サービスに使用されている場合はそちらにマイグレーションされます。(そうでない場合、要求を再確認して VM をシャットダウンするよう求められます。)VM がマイグレーションまたはシャットダウンされると、PM に「 実行中 (メンテナンス中) 」と表示されます。 「メンテナンス モード」 を参照してください。
[作業開始] ボタンをクリックすると、PM がメンテナンス モードになった後、一部のシステムでは次のアクションを実行できるようになります。	
 最終処理	PM の「 実行中 (メンテナンス中) 」の状態を解除します。 「メンテナンス モード」 を参照してください。
 シャット	PM をシャットダウンします。PM は「 オフ (メンテナンス中) 」に切り替わります。 「物理マシンをシャットダウンする」 を参照してください。

コマンド	説明
ダウン	
 リブート	PM をリブートします。PM は「 リブート準備中 (メンテナンス中) 」に切り替わります。「 物理マシンをリブートする 」を参照してください。
 削除	PM やそのコンポーネントを交換できるよう、Stratus Redundant Linux ソフトウェアが PM を ztC Edge システムのデータベースから削除します。「 物理マシンを交換する (手動) 」を参照してください。
以下のアクションは、障害率が高いために PM が故障したり Stratus Redundant Linux ソフトウェアが PM をサービスから除外し、電源をオフにした場合に使用できます。	
 リカバリ	故障した PM を復旧します。状況によっては、ztC Edge コンソールに故障した PM の状態が「 アクセス不可能 (同期/退去中...) 」と表示されることもあります。「 故障した物理マシンを復旧する (手動) 」を参照してください。

関連トピック





[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[「\[物理マシン\] ページ」](#)

物理マシンの状態とアクティビティ

物理マシン (PM) には以下の状態とアクティビティがあります。各状態とアクティビティに応じて特定のアクションが有効になります。

状態	アクティビティ	使用できるコマンド	説明
	 実行中	作業開始	PM は正常に稼働しています。
	 退去中	最終処理	仮想マシンがこの PM からパートナー マシンに

状態	アクティビティ	使用できるコマンド	説明
			マイグレーションしています。
	 実行中	作業開始	PM は故障が予想されます。
	 実行中	作業開始	PM が故障しました。
	 電源オフ	作業開始	障害率が高すぎるため、ztC Edge が PM の電源をオフにしました。
	 ブート中	最終処理	PM がブートしています。
	 リブート中	最終処理	PM がリブートしています。
	 実行中	最終処理 シャットダウン リブート リカバリ 交換	PM はメンテナンス モードで実行中です。「 メンテナンス モード 」を参照してください。

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[「\[物理マシン\] ページ」](#)

[仮想マシン] ページ

[仮想マシン] ページを使用して、ztC Edge システムで実行中の仮想マシン (VM) を管理します。このページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで **[仮想マシン]** をクリックし

ます。

特定の VM を管理するには、**[仮想マシン]** ページの上部パネルで VM の名前をクリックします。下部のパネルに、その VM を管理するためのコントロールと情報が表示されます。

[仮想マシン] ページに表示される VM の状態とアクティビティの意味については、[「仮想マシンの状態とアクティビティ」](#) を参照してください。このページに表示されるコントロールの詳細については、[「仮想マシンのアクション」](#) か、特定のタスクのヘルプ トピックを参照してください。

[仮想マシン] ページを使用して、次のような管理タスクを実行できます。

- VM に関する情報 (VM の名前、オペレーティング システム、説明、および下部パネルのタブに表示されるリソースなど) を表示する
- VM を作成、コピー、エクスポート、インポート、復元する ([「仮想マシンを作成/マイグレーションする」](#) を参照)
- [「仮想マシン コンソールのセッションを開く」](#)
- [「仮想マシンのリソースを再プロビジョニングする」](#)
- VM の電源を制御する
 - [「仮想マシンを起動する」](#)
 - [「仮想マシンをシャットダウンする」](#)
 - [「仮想マシンの電源をオフにする」](#)
- [「仮想マシンを削除する」](#) または [「仮想マシンの名前を変更する」](#)
- 高度なタスクやトラブルシューティングを実行する ([「高度なトピック \(仮想マシン\)」](#) を参照)
- USB デバイスまたはネットワークマウント フォルダをマウントしてゲスト オペレーティング システムで使用する ([「ztc Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」](#) を参照)
- USB デバイスと VM を接続 (または切断) する ([「仮想マシンに USB デバイスを接続する」](#) を参照)
- Windows ベースの VM とアプリケーションをモニタリングする ([「システム、Windows ベースの VM、およびアプリケーションをモニタリングする」](#) を参照)

管理者または**プラットフォーム マネージャー**のロールが割り当てられているユーザは、**[仮想マシン]** ページのすべてのタスクを実行できます。**[VM マネージャー]** のロールが割り当てられているユーザはすべてのタスクを実行できますが、ボリュームを拡張することができません。**VM マネージャー**の権限

の詳細については、「[仮想マシンを管理する](#)」を参照してください。これらのロールの割り当ての詳細については、「[ローカル ユーザ アカウントを管理する](#)」を参照してください。




関連トピック


[「仮想マシンを管理する」](#)






[「ztC Edge コンソールを使用する」](#)

仮想マシンのアクション

仮想マシン (VM) を選択すると、VM の状態とアクションに応じて以下のアクション ボタンが表示されます。非アクティブなボタンはグレー表示されています。

アクション	説明
 作成	VM 作成ウィザードを起動します。「 新しい仮想マシンを作成する 」を参照してください。
 コピー	システム上の既存の VM をコピーして新しい VM を作成するか、トラブルシューティングの目的で VM を複製します。「 仮想マシンをコピーする 」を参照してください。
 インポート/ リストア	<p>OVF および VHD ファイルのセットから VM をインポートします。「仮想マシンを作成/マイグレーションする」を参照してください。</p> <p>インポート ウィザードでは、VM を "インポート" してその VM の新しいインスタンスを作成するか、あるいは VM を "リストア" して OVF および VHD ファイルに指定されているのと同じハードウェア ID が設定された同一の VM を作成することができます。</p> <p>Open Virtual Machine Format (OVF) は、物理マシンまたは仮想マシン データをパッケージングして配布するためのオープン スタンドards です。OVF フォーマットは VM に関するメタデータ情報を含みます。仮想ハード ディスク (VHD) は、仮想ディスク情報を含むファイルです。</p>
VM が稼働している場合、次のアクションを使用できます。	

アクション	説明
 マウント	USB デバイスまたはネットワーク マウント フォルダ (つまりディレクトリ) をマウントして、ゲスト オペレーティング システムで利用できるようにします。その後、マウントしたロケーションに VM をエクスポートできます。 「ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」 を参照してください。
 アンマウント	USB デバイスまたはネットワークマウント フォルダをアンマウントします。 「ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」 を参照してください。
 コンソール	選択した VM のコンソールを開きます。 「仮想マシン コンソールのセッションを開く」 を参照してください。
 シャットダウン	選択した VM をシャットダウンします。 「仮想マシンをシャットダウンする」 を参照してください。
 電源オフ	選択した VM の処理を直ちに停止して、そのメモリの状態を破棄します。これは、VM を正常にシャットダウンできない場合の最後の手段としてのみ使用してください。 「仮想マシンの電源をオフにする」 を参照してください。
VM がシャットダウンまたは停止している場合、次のアクションを使用できます。	
 構成	仮想マシンの再プロビジョニング ウィザードを起動します。このウィザードを起動する前に VM がシャットダウンされている必要があります。 「仮想マシンのリソースを再プロビジョニングする」 を参照してください。
 リストア	OVF または VHD ファイルの以前のバックアップ コピーから VM を上書きすることで、お使いの ztC Edge システム上の既存の VM を復旧します。 「OVF ファイルから仮想マシンを交換/復元する」 を参照してください。

アクション	説明
 エクスポート	OVF および VHD ファイルのセットに VM のイメージを保存します。これらのファイルを別のシステムにインポートしたり、同じ ztC Edge システムにインポートし直して元の VM を復元や複製することもできます。 「仮想マシンをエクスポートする」 を参照してください。
 起動	選択した VM をブートします。 「仮想マシンを起動する」 を参照してください。
 CD からブート	選択した CD から VM をブートします。 「仮想 CD からブートする」 を参照してください。
 削除	VM を削除します。 「仮想マシンを削除する」 を参照してください。
次のアクションは、障害率が高いために Stratus Redundant Linux ソフトウェアが VM をサービスから除外し、電源をオフにした場合に使用できます。	
 デバイスのリセット	<p>VM の平均故障間隔 (MTBF) カウンタをリセットしてサービスに戻せるようにします。「故障した仮想マシンの MTBF をリセットする」を参照してください。</p> <p>VM がクラッシュすると、MTBF しきい値に達している場合は Stratus Redundant Linux ソフトウェアがその VM を自動的に再起動します。VM が MTBF のしきい値を下回る場合、Stratus Redundant Linux ソフトウェアはそのマシンをクラッシュした状態のまま維持します。必要に応じて [デバイスのリセット] をクリックし、VM を再起動して MTBF カウンタをリセットできます。</p>

関連トピック









[「仮想マシンの運用を管理する」](#)

[「\[仮想マシン\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

仮想マシンの状態とアクティビティ

仮想マシン (VM) では、以下のように状態とアクティビティに応じて特定のアクションが有効になります。

状態	アクティビティ	有効なアクション	説明
	 インストール中		Stratus Redundant Linux ソフトウェアが新しい VM のブートボリュームをインストールしています。
	 停止	起動 コピー 構成 エクスポート CD からブート 削除	VM はシャットダウンされたか電源オフになっています。
	 ブート中	コンソール 電源オフ	VM が起動しています。
	 実行中	コンソール シャットダウン 電源オフ	VM は冗長な物理マシンで正常に稼動しています。
	 実行中	コンソール シャットダウン	VM は正常に稼動していますが、完全に冗長なリソースで実行されてい

状態	アクティビティ	有効なアクション	説明
		電源オフ	ません。
	 停止中	電源オフ 削除	VM は シャットダウン アクションが実行されたためシャットダウンしている最中か、もう片方の物理マシンがメンテナンス モードに推移しているためにシャットダウンされています。
	 クラッシュ		VM がクラッシュし、再起動しています。有効な場合、e アラートとサポート通知メッセージが送信されます。
	 クラッシュ		VM がクラッシュした回数が多く、その MTBF しきい値を超えました。 [デバイスのリセット] をクリックするまで VM はクラッシュ状態のままになります。 「故障した仮想マシンの MTBF をリセットする」 を参照してください。

関連トピック

[「仮想マシンの運用を管理する」](#)

[「\[仮想マシン\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

[ボリューム] ページ

[ボリューム] ページには、ztC Edge システム内の仮想マシン (VM) に接続されているボリュームに関する情報が表示されます。このページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで **[ボリューム]** をクリックします。**[ボリューム]** ページの上部パネルに、ボリュームに関する以下の列と情報が表示されます。

- **状態**
- **名前**
- **ディスクの同期** (存在する場合)
- **サイズ**
- **ブート可能**
- **用途**。次のいずれかが表示されます。
 - ボリュームを VM が使用している場合、その VM へのリンク。
 - ボリュームが **root** または **swap** の場合、物理マシン (PM) ページ (**node0** または存在する場合は **node1**) へのリンク。
 - 共有ボリューム (**shared.fs**) の場合は「システム」。
 - ボリュームがシステム ボリュームではなく、VM でも使用されていない場合は「なし」。

[ボリューム] ページの上部パネルでボリュームの名前をクリックすると、下部パネルにそのボリュームに関する追加の情報が表示されます。(ボリューム情報の表示には `snmptable` コマンドを使用することもできます。[「snmptable でシステム情報を取得する」](#)を参照してください。)下部パネルでは、ボリュームに対して次のような管理タスクを実行できます。

- **[説明]** テキスト ボックスに各ボリュームの説明を追加する
- ボリュームの名前を変更する ([「ztC Edge システムのボリュームの名前を変更する」](#)を参照)
- **[削除]** をクリックしてボリュームを削除するただし、VM がボリュームを使用している場合、**[削除]** ボタンはグレー表示されます。

その他のボリューム管理タスクは、[仮想マシン] ページから実行します。これには以下のタスクが含まれます。

- [「仮想マシンにボリュームを接続する」](#)
- [「仮想マシンのボリュームを作成する」](#)
- [「仮想マシンからボリュームを切断する」](#)
- [「仮想マシンからボリュームを削除する」](#)

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[ネットワーク] ページ

[ネットワーク] ページには、ztC Edge システムに接続されている共有ネットワークに関する情報が表示されます。このページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで **[ネットワーク]** をクリックします。

[ネットワーク] ページを使用して特定のネットワークに関する情報を表示できます。これにはネットワークの状態、リンク状況、名前、内部名、タイプ、接続されている仮想マシン (VM) の数、MTU などが含まれます。また、下部パネルの **[説明]** タブでネットワークの説明を追加することもできます。

特定のネットワークを管理したり、単にその情報を表示するには、**[ネットワーク]** ページの上部パネルで **[名前]** または **[内部名]** にあるネットワークの名前をクリックするか、**[サマリ]** タブのネットワーク接続図にあるポートをクリックします。下部のパネルに、そのネットワークのノードに関する追加の情報が表示されます。**[サマリ]** タブの列にはノードの状態、物理インタフェース、速度、MAC アドレス、スロット、およびポートに関する情報が表示されます。列の表示/非表示を切り替えるには、カーソルを列見出しの右に移動して、表示された下矢印をクリックし、**列** をクリックして表示/非表示する列を選択または選択解除します。

[ネットワーク] ページを使用して、次のような管理タスクを実行できます。

- **[サマリ]** タブで、ネットワークを構成する物理アダプタのリストを確認する
- **[説明]** タブで、ネットワークの説明を追加する
- **[仮想マシン]** タブで、ネットワークを使用する仮想マシンのリストを確認する
- **[名前]** 列で、名前をダブルクリックして名前を変更する
- A-Link およびビジネス ネットワークの **「MTU を設定する」**

ネットワークに関するその他の情報については、以下を参照してください。

- **「ネットワーク アーキテクチャ」**
- **「イーサネット ケーブルを接続する」**
- **「全般的なネットワーク要件と構成」**
- **「ネットワークの要件を満たす」** (ALSR 構成)



注: **[ネットワーク]** ページには、両方の物理マシンに物理的に接続されているネットワークのみが表示されます。存在するはずのネットワークが表示されない場合、両方のネットワーク接続が正しく配線されていて、そのリンクがアクティブであることを確認します。

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

MTU を設定する

ネットワークでサポートされる最大転送単位 (MTU) が大きいほど、ネットワークのパフォーマンスが向上します。ztC Edge コンソールの **[ネットワーク]** ページを使用して、A-Link およびビジネス (biz) ネットワークに MTU の値を設定することができます。



注: デュアルノードシステム上のビジネス ネットワーク ibiz0 (network0 と呼ばれます) または ibiz1 (network1 と呼ばれます) のいずれかの MTU を変更すると、システムによって VM が自動的に一方のノードからもう片方のノードにマイグレーションされます。特に、ibiz0 の MTU を変更した場合、システムはプライマリ ノードからセカンダリ ノードへのフェールオーバーも自動的に行います。この問題を回避するには、ビジネス ネットワークの MTU を変更しないようにするか、計画的なメンテナンス期間中のみに MTU を変更するようにします。

単一ノードシステムでは、VM がシャットダウンされるので、MTU の変更は避けてください。変更がどうしても必要な場合には計画的なメンテナンス期間中のみに行うようにします。



前提条件: 単一ノードシステムのビジネス ネットワーク上の MTU を変更する場合、そのネットワークを使用するすべての VM をシャットダウンしてから MTU を変更してください。

A-Link またはビジネス ネットワークの MTU を設定するには

1. 左側のナビゲーション パネルで **[ネットワーク]** をクリックして **[ネットワーク]** ページを表示します。
2. 上部パネルで、MTU を設定する A-Link またはビジネス ネットワークを選択します。
3. **[構成]** をクリックします。
4. **[共有ネットワークの構成]** ウィンドウで、**[ネットワーク ロール]** に **[ビジネス]** または **[A-Link]** を選択します。

5. **[MTU]** の下で 1280 ～ 65535 のバイト値を入力します。デフォルト値は次のとおりです。

システム モデル	イーサネット ポートの MTU 値	
	ポート A1 (A-Link1) および ポート A2 (priv0) (デュアルノード システムのみ)	ポート P1 ～ P6 (ibiz0 ～ ibiz5)
100i	1500	1500
110i	9000	1500
200i	9000	1500
250i	9000	1500

6. **[保存]** をクリックします。

関連トピック

[「\[ネットワーク\] ページ」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[仮想 CD] ページ

[仮想 CD] ページを使用して仮想 CD (VCD) を作成します。VCD を使用して、システム上の仮想マシンで使用する、ソフトウェア インストール メディアまたはリカバリ メディアを作成できます。このページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで **[仮想 CD]** をクリックします。

特定の VCD を管理するには、**[仮想 CD]** ページの上部パネルで VCD の名前をクリックします。下部のパネルに、その VCD の説明が表示されます。

[仮想 CD] ページを使用して、次のような管理タスクを実行できます。

- [「仮想 CD を作成する」](#)
- [「仮想 CD を削除する」](#)
- [「仮想 CD の名前を変更する」](#)
- **[説明]** テキスト ボックスに各ボリュームの説明を追加する

その他の VCD 管理タスクを実行するには、「[仮想 CD を管理する](#)」を参照してください。

関連トピック

[「仮想 CD を挿入する」](#)

[「仮想 CD を取り出す」](#)

[「ztC Edge コンソールを使用する」](#)

[アップグレード キット] ページ

ztC Edge の [アップグレード キット] ページでは、お使いのシステムを新しいバージョンの Stratus Redundant Linux ソフトウェアにアップグレードするためのアップグレード キットのアップロードと管理を行えます。システム ソフトウェアの新しいバージョンが利用可能かどうかを確認し、利用できる場合はダウンロードすることができます。USB メディアにアップグレード キットをコピーして、このメディアをシステム ソフトウェアの再インストールに使用することもできます。

[アップグレード キット] ページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで [アップグレード キット] をクリックします。



注: 利用できるアップグレード キットを自動でダウンロードするように指定できます。電子メール アラート (e アラート) をシステム管理者に送信して、システム ソフトウェアの更新が利用可能になると通知するようにも設定できます。「[ソフトウェア更新を管理する](#)」を参照してください。

システム ソフトウェアの新しいバージョンをチェックしてダウンロードするには



注: この手順を実行するユーザのロールは [管理者] または [プラットフォーム マネージャー] でなければなりません。

1. 左側のナビゲーション パネルで [アップグレード キット] をクリックして [アップグレード キット] ページを表示します。
2. マストヘッドの下にある [更新のチェック] ボタンをクリックします。
メッセージ ボックスが開き、システム ソフトウェアの新しいバージョンが利用可能かどうかが表示されます。
3. 更新を利用できる場合、[利用可能なソフトウェア更新] ボックスが開くので、[ソフトウェアのダウンロード] をクリックして、ソフトウェアをダウンロードします。または、[リ

リース ノートの確認] をクリックして、更新に関する情報の英語版を確認することもできます。



注: [アップグレード キット] ページで利用できる保存済みキットは 2 つだけです。ページに 2 つのキットが表示されているときに、もう 1 つ別のキットをダウンロードするには、その前にキットを 1 つ削除する必要があります。

[ソフトウェアのダウンロード] をクリックすると、次が行われます。

- ztC Edge システムがインターネットに接続している場合、ソフトウェア更新を含む **.kit** ファイルがシステムに直接ダウンロードされ、**[アップグレード キット]** ページに一覧されます。**[利用可能なソフトウェア更新]** ボックスに、ダウンロードの進捗状況を示すさまざまなステータス メッセージが表示されます。
- システムがインターネットに接続していない場合、**.kit** ファイルは ztC Edge コンソールを実行しているリモートの管理コンピュータにダウンロードされます。ファイルをブラウザの既定のダウンロード フォルダに保存するか、別の保存場所に移動します。システム ソフトウェアの新しいバージョンが利用可能で、システムへのアップロードが必要なことを知らせる e アラート (設定されている場合) が届きます。

4. 続けてアップグレードを行うには、**「アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする」** を参照してください。

Stratus Redundant Linux ソフトウェアのアップグレードの詳細については、**「Stratus Redundant Linux ソフトウェアをアップグレードする」** を参照してください。

(USB メディアの作成の詳細については、**「システム ソフトウェアの USB メディアを作成する」** を参照してください。)

関連トピック

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

システム ソフトウェアの USB メディアを作成する

[アップグレード キット] ページを使用して、システム ソフトウェア Stratus Redundant Linux の展開用 ISO ファイルのコピーが含まれた USB メディアを作成できます。その後、この USB メディアを使用

して障害のあるノードを手動で復旧したり交換する必要がある場合にソフトウェアを再インストールします。



注: USB メディアにアップグレード キットをコピーすると、ファイル システムがある場合はこれがメディアからアンマウントされます。

システム ソフトウェアの USB メディアを作成するには

1. まだ行っていない場合はアップグレード キットをダウンロードします。[「アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする」](#)を参照してください。
2. プライマリ ノードに USB メディアを挿入します。[\[物理マシン\]](#) ページで、デバイス一覧のある [\[USB デバイス\]](#) タブをクリックします。
3. ztC Edge コンソールの左側のナビゲーション パネルで [\[アップグレード キット\]](#) をクリックします。
4. [\[アップグレード キット\]](#) ページに複数のキットが表示される場合、コピーする ISO のあるバージョンを選択します。
5. [\[USB メディアの作成\]](#) ボタン (マストヘッド下部にあります) をクリックします。
[\[USB メディアの作成\]](#) ダイアログ ボックスが開きます。
6. ノードに複数の USB メディアがある場合、ドロップダウン リストからメディアを選択する必要があります。その後、[\[続行\]](#) をクリックします (または、手順をキャンセルするには [\[キャンセル\]](#) をクリックします)。
[\[USB メディアの作成\]](#) ダイアログ ボックスに進捗状況のパーセントが表示されます。コピーが完了するとウィンドウが閉じます。

この USB メディアを使用して障害のあるノードを手動で復旧したり交換する必要がある場合にソフトウェアを再インストールします。[「故障した物理マシンを復旧する \(手動\)」](#) または [「物理マシンを交換する \(手動\)」](#) を参照してください。

関連トピック

[「\[アップグレード キット\] ページ」](#)

4

第 4 章: Stratus Redundant Linux ソフトウェアをアップグレードする

Stratus Redundant Linux ソフトウェアをアップグレードするには、アップグレード キットを使用します。[「アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする」](#)を参照してください。

関連トピック

[「ソフトウェア更新を管理する」](#)

[「\[アップグレード キット\] ページ」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする

このトピックでは、Stratus Redundant Linux ソフトウェアのアップグレード キットを使用してシステム ソフトウェアをアップグレードする方法を説明します。また、システムをアップグレードする前に、キットをダウンロードしてからシステムにアップロードする必要がある場合、その方法についても説明します。2 つのノードで構成されているシステムでは、オプションで一時停止を有効にしてアップグレードを制御することもできます (1 つのノードで構成されているシステムで一時停止を有効にすることはできません)。一時停止中のシステムの検査は、システムで管理されていないサードパーティ製ツールやその他のサービスを確認したり再構成する場合に役立ちます。



注意事項: ztC Edge システムの CentOS ホスト オペレーティング システムを、Stratus 以外のソースから更新しないでください。Stratus Redundant Linux ソフトウェアと一緒にインストールされる CentOS リリースのみを使用してください。

前提条件:



- システム ソフトウェアをアップグレードする前に、すべての PM と VM が正常な稼働状態になければなりません。アップグレードを開始する前に、ztC Edge コンソールで PM または VM の問題を示すアラートが発生していないことを確認してください。
- システム ソフトウェアのアップグレードを行う前に、すべての VCD および USB メディアを VM から取り出してください。VCD または USB メディアが VM に接続されたままの場合、システムがアップグレードプロセスのために VM をマイグレーションして PM をメンテナンス モードに切り替えることはできません。
- システムがアップグレード キットの要件を満たしていることを確認するには、このトピックの説明に従って **[評価]** ボタンを使用します。
- 単一ノード用に構成されているシステムをアップグレードする前に、VM をバックアップしてください。その後、下記の手順に従いソフトウェアをアップグレードして評価します。最後に、「**1 つのノードで構成されているシステムをアップグレードするには**」の手順を使用して、システムの 1 台の PM をアップグレードします。アップグレードの操作中にシステムがリブートする際、ztC Edge コンソールとの通信が少なくとも 15 分間失われます。

次に手順を示します。

[I. アップグレード キットをダウンロードするには]

[II. システムにアップグレード キットをアップロードするには]

[III. ソフトウェアを評価するには] (オプション)

[IV. システム ソフトウェアをアップグレードするには]

I. アップグレード キットをダウンロードするには

利用可能な更新がある場合、新しいシステム ソフトウェアを含むアップグレード キットがまだダウンロードされていない場合には、ダウンロードすることができます。**[アップグレード キット]** ページから、**[利用可能なソフトウェア更新]** ウィンドウで **[ソフトウェアのダウンロード]** をクリックします (**[アップグレード キット] ページ** を参照)。

あるいは、ソフトウェアを Stratus の **ダウンロード** ページからダウンロードすることもできます。



注: ztC Edge コンソールの **[アップグレード キット]** ページで利用できる保存済みキットは 2 つだけです。ページに 2 つのキットが表示されているときに、もう 1 つ別のキットをダウンロードするには、その前にキットを 1 つ削除する必要があります。

1. **[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) を開きます。
2. アップグレード セクションにスクロールして、アップグレード リンクをクリックしてキットをダウンロードします。
3. ローカル コンピュータでファイルを保存するロケーションに移動します。必要な場合、ztC Edge コンソールを実行しているリモート管理コンピュータにファイルを転送します。

II. システムにアップグレード キットをアップロードするには

必要な場合、ztC Edge コンソールを実行しているリモート管理コンピュータから、ztC Edge システムにアップグレード キットを転送します。

1. ztC Edge コンソールの左側のナビゲーション パネルで **[アップグレード キット]** をクリックします。
2. **[アップグレード キット]** ページでマストヘッドの下にある **[キットの追加]** ボタンをクリックして、**ztC Edge - キットのアップロード ウィザード**を開きます。
3. **ztC Edge - キットのアップロード ウィザード** ダイアログ ボックスで、Google Chrome の場合は **[ファイルの選択]**、Firefox または Internet Explorer の場合は **[参照]** をクリックしてから、.kit ファイルを参照して選択します。
4. .kit ファイルを選択した後、**[アップロード]**、**[インポート]**、または **[完了]** をクリックします (実行される機能は同じです)。ファイルをアップロードする間、「**ファイルをアップロードしています (ウィザードを閉じないでください)**」というメッセージが表示されます。アップロードの所要時間は、ローカルに保存されているファイルで最大 2 分間、ネットワーク経由で保存されているファイルの場合は 10 分以上かかることがあります。アップロードに失敗した場合、ウィザードに「**ファイルのアップロードに失敗しました。**」というメッセージが表示されます。
5. アップロードが完了すると、ウィザードが閉じて **[アップグレード キット]** ページにアップグレードキットの状態とバージョン番号が表示されます。また、**[キットの追加]** ボタンに加え、**[評**

価]、[アップグレード]、および[削除] ボタンも表示されます。

6. 複数のアップグレード キットが読み込まれている場合、どれを使用するか選択してください。

III. ソフトウェアを評価するには

ソフトウェアを評価して、システムがアップグレード キットの要件を満たしているかどうかを確認します。(この手順は推奨しますが、必須ではありません。)

これを行うには、[アップグレード キット] ページで評価するアップグレード キットを選択して、[評価] をクリックします。

評価の所要時間は最大 6 分です。評価に成功した場合、次のステップに進みます。

評価に失敗した場合は、ポップアップ ウィンドウが開いてエラーの原因を示すメッセージが表示されます。これらのメッセージには、リリースがサポートされない、ストレージが不足している、パーティションに問題がある、VM のシャットダウンが必要、あるいはその他のシステム アップグレードに関する情報が示されます。たとえば、システムのディスク領域が不足していてアップグレードを完了できない場合、**空き容量の不足**を示すメッセージに必要な容量が報告されます。評価の問題を解決するための詳しい情報は、**Stratus カスタマ サービス ポータル** (<https://support.stratus.com>) の**ナレッジ ベース**で該当する評価エラー メッセージを検索してください。

IV. システム ソフトウェアをアップグレードするには

1. まず [アップグレード キット] ページの [アップグレード] をクリックして、アップグレードを開始します。

システムのアップグレードが選択されたことを示す **[確認]** ウィンドウが開き、選択したアップグレード キットへのアップグレードの確認を求めるメッセージが表示されます。このウィンドウには、アップグレードを制御するために一時停止を有効にするチェック ボックスも表示されます。一時停止を有効にするには、**[各ノードのアップグレード後に一時停止]** ボックスをオンにします。

2. **[はい]** をクリックしてアップグレードを続行します。

アップグレードが開始されます。一時停止を有効にした場合、アップグレードのステップを示す図に、アップグレードの現在の状態が表示されます。アップグレードが一時停止された場合、続行するには **[最終処理]** をクリックする必要があります。

ノードがアップグレードされた後、もう片方のノード (存在する場合) をアップグレードするまでは、2 つのノードで異なるバージョンのソフトウェアが実行されています。この間、マストヘッドに「**システムは次の状態で稼働中: バージョン不一致**」というメッセージが表示されます。

アップグレードが完了した後は、すべての Windows ベースの VM で更新された virtIO ドライバをチェックします。手順については、[「VirtIO ドライバを更新する \(Windows ベースの VM\)」](#)を参照してください。

1 つのノードで構成されているシステムをアップグレードするには

1. ztC Edge システムで稼働しているすべての VM をシャットダウンします。
2. 上記のステップの手順を使用して、アップグレード キットでシステムをアップグレードします。



注: アップグレードの操作中にシステムがリブートする際、ztC Edge コンソールとの通信が少なくとも 15 分間失われます。

3. システムが正常に稼働していることを確認します。
4. すべての VM を起動します。

関連トピック

[「ソフトウェア更新を管理する」](#)

[「\[アップグレード キット\] ページ」](#)

[「ztC Edge コンソール」](#)

[「ztC Edge コンソールを使用する」](#)

[「ztC Edge システムの説明」](#)

5

第 5 章: 物理マシンを管理する

物理マシン (PM) つまりノードを管理して、その運用を制御しメンテナンスを行います。

PM の表示と管理には ztC Edge コンソールの **[物理マシン]** ページを使用します。詳細については、[「\[物理マシン\] ページ」](#) を参照してください。

[物理マシン] ページから行う多くのタスクはメンテナンス モードで実行する必要があります。詳細については、[「メンテナンス モード」](#) を参照してください。

メンテナンス モードで PM の運用状態を管理するには、次を参照してください。

- [「物理マシンをリブートする」](#)
- [「物理マシンをシャットダウンする」](#)
- [「負荷分散」](#)

PM の電源を (その物理コンソールで) オンにするには、[「物理マシンの電源をオンにする」](#) を参照してください。

障害のある PM を復旧したり、MTBF をリセットして PM のトラブルシューティングを行うには、[「物理マシンのトラブルシューティングを行う」](#) を参照してください。

PM の交換など PM ハードウェアの保守タスクを実行するには、[「物理マシンのメンテナンスを行う」](#) を参照してください。

適切なモニタリングのライセンスが適用されたシステムで、ztC Edge システムのホスト オペレーティング システムをモニタリングするには、[「ztC Edge システムをモニタリングする」](#) を参照してください。

メンテナンス モード

物理マシン (PM) がメンテナンス モードに切り替わると、メンテナンスを行えるようマシンがオフラインになります。メンテナンス後に最終処理すると、PM のメンテナンス モードが解除されて再びオンラインになり、仮想マシン (VM) を実行できるようになります。

2 つのノード (つまり 2 台の PM) で構成されているシステムでは、以下の点に注意してください。

- PM がメンテナンス モードになると、その PM は実行中の VM をもう片方の PM にマイグレーションします。これにより、サービスに起因する中断から VM を保護できます。両方の PM がメンテナンス モードに入る場合、これらの PM はすべての VM を正常にシャットダウンします。したがって、PM がシャットダウンやリブートされる前に VM のメモリ状態は保護されます。
- 物理マシン (**nodex (プライマリ)**) がメンテナンス モードに切り替わると、もう片方の PM がブライマリになります。
- 両方の物理マシンをメンテナンス モードにするには、まずセカンダリ PM をメンテナンス モードにした後で、プライマリ PM をメンテナンス モードにします。この順序を守ることで、VM の不要なマイグレーションを回避できます。

1 つのノード (つまり 1 台の PM) で構成されているシステムの場合、PM はメンテナンス モードに入るときに VM をシャットダウンします。したがって、PM をメンテナンス モードにするのは、計画的なメンテナンス期間中のみに行ってください。

PM のシャットダウンは、PM がメンテナンス モードにある状態で **[物理マシン]** ページから行う必要があります。これは ztC Edge コンソールが、PM の電源を手動でオフにした結果生じる可能性のあるサービス中断からシステムを保護するためです。


注意事項:



1. PM がメンテナンス モードになっている間、システムはフォールト トレラントではありません。ダウンタイムの発生を回避するには、PM のメンテナンス モードを解除して再びオンラインに戻せるよう、サービスをできるだけ早く最終処理します。
2. すべての PM をメンテナンス モードにするのは、すべてのビジネス プロセスをシャットダウンできる場合に限られます。2 台の PM で構成されているシステム上で VM の運用を継続する必要がある場合には、両方の PM を同時にメンテナンス モードにすることは避けてください。VM の運用を継続するには、少なくとも 1 台の PM が正常に稼働している必要があります。(ztC Edge システム全体をシャットダウンする必要がある場合、**「物理マシンをシャットダウンする」**を参照してください。)

PM をメンテナンス モードにするには

1. **[物理マシン]** ページから PM を選択します。
2. **[作業開始]** をクリックします。

PM がメンテナンス モードになると、その状態が  と表示されます。

PM を最終処理してメンテナンス モードを解除するには

1. **[物理マシン]** ページから PM を選択します。
2. **[最終処理]** をクリックして、PM のメンテナンス モードを解除します。

関連トピック

[「ztC Edge コンソール」](#)

[「物理マシンを管理する」](#)

[「物理マシンと仮想マシン」](#)

[「\[物理マシン\] ページ」](#)

[「\[仮想マシン\] ページ」](#)

物理マシンの電源をオンにする

物理マシン (PM) の電源はその PM の物理コンソールでオンにします。



注: 電源コードを抜いたために PM の電源が失われたり、メインの AC 電源が失われた場合、ztC Edge システム内の各 PM が電源回復の直後に自動で電源オンになるよう設定されます。

PM の電源をオンにするには

1. PM のフロントパネルにある電源ボタンを押します。
2. フロントパネルの **PWR** LED または電源ボタンが点灯することを確認します。

システムの電源をオンにするには、システム内の各 PM でフロントパネルの電源ボタンを押します。手順については、[「システムの電源をオンにする」](#)を参照してください。

関連トピック

[「メンテナンス モード」](#)

[「ztC Edge コンソール」](#)

[「物理マシンを管理する」](#)

[「\[物理マシン\] ページ」](#)

物理マシンを識別する

ユーザ アカウントに**管理者**または**プラットフォーム管理者**のロールが割り当てられている場合、物理マシン (PM) の SYS LED を点滅させてマシンを識別することができます。

物理マシンを識別するには

1. 識別したい PM (node0 または存在する場合は node1) を決定します。
2. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
3. 適切な PM (node0 または存在する場合は node1) を選択してから **[検出]** をクリックします。すると、選択した PM の SYS LED が 30 秒間高速点滅します。

関連トピック

[「ztC Edge コンソール」](#)

[「\[物理マシン\] ページ」](#)

[「ztC Edge コンソールを使用する」](#)

物理マシンをリブートする

物理マシン (PM) をリブートして Stratus Redundant Linux ソフトウェアを再起動し、オプションで PM のメンテナンス モードを解除します。(2 つのノードで構成されているシステムの両方の PM をリブートする必要がある場合には、[「システムをリブートする」](#)を参照してください。)

PM をリブートすると VM がシャットダウンされ、これらは手動で再起動しなければなりません。したがって、単一ノードシステムの PM をリブートする場合には、計画的なメンテナンス期間中のみにリブートしてください。

PM をリブートするには

1. リブートする PM (node0 または存在する場合は node1) を決定します。必要に応じて **[検出]** ボタンを使用します ([「物理マシンを識別する」](#)を参照してください)。

2. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
3. 作業する PM (node0 または存在する場合は node1) を選択して **[作業開始]** をクリックします。
PM の総合状態が「**メンテナンス モード**」に変わり、**アクティビティ** 状態が「**実行中 (メンテナンス中)**」に変わります。
4. **[リブート]** をクリックします。PM がリブートし **[アクティビティ]** 状態が表示されます。
 - **リブート準備中 (メンテナンス中)**
 - **リブート中 (メンテナンス中)**
 - **ブート中 (メンテナンス中)**
 - **実行中 (メンテナンス中)**
5. PM のメンテナンス モードを解除して仮想マシンを実行できるようにするには、**[最終処理]** をクリックします。

単一ノード システムでは、VM を手動で再起動する必要があります。

関連トピック

[「メンテナンス モード」](#)

[「ztC Edge コンソール」](#)

[「物理マシンを管理する」](#)

[「\[物理マシン\] ページ」](#)

物理マシンをシャットダウンする

物理マシン (PM)、つまりノードをシャットダウンして、修復や交換の必要がある場合に PM の実行を停止します。次の手順を使用して、から ztC Edge コンソールまたは PM の電源ボタンを使って 1 台の PM だけをシャットダウンします。

注意事項:

1. 次の手順を使って 2 ノードで構成されている ztC Edge システムの両方の PM をシャットダウンしたり、1 つのノードで構成されているシステムの (1 台の) PM をシャットダウンしたりすると、データが失われます。2 ノードで構成されているシステムの両方の PM、あるいは 1 ノードで構成されているシステムの (1 台の) PM を停止する必要がある場合、「システムをシャットダウンする」の説明に従って、システムをシャットダウンします (これにより仮想マシン (VM) もシャットダウンされます)。
2. -f (強制) オプションは、PM のホスト オペレーティング システムの halt、poweroff、または reboot コマンドで使用しないでください。これにより、同じ PM 上でアクティブな ゲストがハングします。
3. PM をシャットダウンすると、2 つのノードで構成されている ztC Edge システムがフォールトトレラントではなくなります。アップタイムを継続させるには、オフラインの PM をできるだけ早くサービスに戻します。




注: PM をシャットダウンする際、スタンバイ電源が LOM のためにオンのままになります。ただし、電源コードを抜いたりメインの AC 電源がオフにされた場合は例外です。

ztC Edge コンソールで PM をシャットダウンするには

PM をシャットダウンするには、PM をメンテナンス モードにする必要があります。すると、その PM で実行中のすべての VM がもう片方の PM (存在する場合) にマイグレーションされます。2 つのノードをもつシステムでは、このプロセス (1 ~ 2 分かかります) の間も VM が引き続き実行されます。

1. シャットダウンする PM を決定します。必要に応じて **[検出]** ボタンを使用します (「物理マシンを識別する」を参照してください)。
2. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
3. 作業する PM (node0 または存在する場合は node1) を選択して **[作業開始]** をクリックします。PM の総合状態が「メンテナンス モード」に変わり、アクティビティ状態が「実行中 (メンテナンス中)」に変わります。
4. この PM の状態が「実行中 (メンテナンス中)」になった後、**[シャットダウン]** をクリックします。

PM がシャットダウンした後はアクティビティが  「オフ (メンテナンス中)」になります。この PM は手動で再起動する必要があります。

電源ボタンで PM をシャットダウンするには

電源ボタンを使って PM をシャットダウンするには

PM の電源ボタンを使用して PM をシャットダウンすることもできます。2 つのノードで構成されているシステムでは、このプロセス (1 ~ 2 分かかります) の間も VM が引き続き実行されます。

1. 両方の PM が実行を継続している間に、シャットダウンする PM のフロントパネルの電源ボタンを押し、放します。
2. システムが PM を自動的にメンテナンス モードに切り替え、その結果その PM で実行中の VM がもう片方の PM にマイグレーションされます。
3. PM が自動的にシャットダウンします。

PM がシャットダウンすると、フロントパネルの **PWR** LED または電源ボタンは消灯しますが、スタンバイ電源はオンのままです。この PM は手動で再起動する必要があります。

電源ボタンを使って PM を強制的に電源オフにするには



注意事項: [シャットダウン] をクリックした後や電源ボタンを押した後に PM がオフにならない場合、PM の電源を強制的にオフにする必要があります。PM の電源オフを強制的に行うとメモリの状態情報が失われるため、これは最後の手段としてのみ使用します。

強制的に電源を切断するには、PM の電源ボタンを数秒間押し続けます。

PM がシャットダウンすると、フロントパネルの **PWR** LED または電源ボタンは消灯しますが、スタンバイ電源はオンのままです。この PM は手動で再起動する必要があります。

関連トピック

[「メンテナンス モード」](#)

[「ztC Edge コンソール」](#)

[「物理マシンを管理する」](#)

[「\[物理マシン\] ページ」](#)

負荷分散

2 つのノードで構成されているシステムの場合、HA 負荷分散は VM を両方の PM に分散させることによりパフォーマンスと可用性の改善を図ります。負荷分散は VM ごとに構成され、ztC Edge システム上で自動的に有効化されます。(1 つのノードで構成されているシステムは、負荷分散を提供しません。)

の PM が使用不可となった場合、もう片方の PM ですべての VM が実行されます。VM は、それを実行するターゲットの PM がサービスに復帰して完全に同期されると、すぐに自動的にマイグレーションされて戻ります。

運用モード

負荷分散は **[仮想マシン]** ページにある、VM の **[負荷分散]** タブで設定します。次のモードがサポートされています。

- **[自動で分散]**。VM の自動負荷分散機能を提供します。自動負荷分散が設定された VM は、最も多くのリソースがある使用可能な PM 上で実行されます。自動設定された 1 つ以上の VM を移動することにより負荷分散の効果が向上するとシステムで判定された場合、アラートが生成されます。ダッシュボードにアラートが表示され、マストヘッドに負荷分散の通知が表示されます。アラートへの応答として、マストヘッドで **[負荷分散]** をクリックして VM の自動負荷分散を開始します。

[仮想マシン] ページの **[現在の PM]** 列のアイコンに、次にマイグレーションする VM が表示されます。

- **[nodeN に手動で配分]**。上級ユーザの場合、自動ポリシーに依存する代わりに、個々の VM に特定の PM (ノード) を手動で割り当てることができます。

[仮想マシン] ページで、各 VM の **[現行 PM]** 列にグラフィックが表示されます。このグラフィックは、VM の現在の負荷分散状態、VM を実行している PM、およびその優先 PM を示します。

次のサンプルグラフィックは、VM が現在 PM 0 で実行されていて、優先マシンは PM 1 であることを示しています。



ztC Edge ポリシーは VM を常に稼動状態に保ちます。一方の PM で故障が予想されていたり、メンテナンス中または使用不可となっている場合、VM は正常な方の PM 上で実行されます。両方の PM が正常な状態にある場合、VM はその優先 PM にマイグレーションします。

関連トピック

[「仮想マシンの優先 PM を選択する」](#)

物理マシンのトラブルシューティングを行う

次のトピックでは、PM のトラブルシューティングの手順について説明します。

- 「故障した物理マシンを復旧する (手動)」

上記のソフトウェアベースのトラブルシューティング手順を使って PM を復旧できない場合、「物理マシンのメンテナンスを行う」にある PM ハードウェアを物理的に交換する方法を参照してください。

故障した物理マシンを復旧する (手動)



注意事項: ztC Edge システム内の 1 台の PM を復旧または交換する必要がある場合、『ztC Edge 100i/110i システム: ノードを交換する (R013Z)』または『ztC Edge 200i/250i システム: ノードを交換する (R019Z)』の手順を使用してください。(必要な場合、「物理マシンを交換する (自動)」を参照してください。) Stratus 認定サービス業者から特に指示を受けた場合を除き、このトピックに記載されている手動の手順は使用しないでください。

物理マシン (PM)、つまりノードの復旧は、PM がブート不可能になったり、ztC Edge システムで PM として機能しなくなった場合に行います。状況によっては、ztC Edge コンソールに故障した PM の状態が「アクセス不可能 (同期中/退去中)」と表示されることもあります。

PM を復旧するには、PM が実行していた Stratus Redundant Linux リリースを再インストールする必要があります。ただし、故障した PM の復旧は最初に行うソフトウェアのインストールとは異なります。復旧操作ではすべてのデータが維持されますが、/boot および root ファイルシステムの再作成、Stratus Redundant Linux システム ソフトウェアの再インストール、および既存のシステムへの接続試行が行われます。(システム ソフトウェアの復旧ではなく物理的な PM ハードウェアの交換が必要な場合、「物理マシンを交換する (手動)」を参照してください。)

システム ソフトウェアを再インストールするには、システムが交換ノードをプライマリ PM 上の一時的な Preboot Execution Environment (PXE) サーバから自動的にブートできるように設定します。各 PM に一番最近インストールされたソフトウェア キットの完全なコピー (ztC Edge コンソールの **[アップグレード キット]** ページに記載) が含まれている限り、PXE ブート インストールを使ってどちらの PM からでもそのパートナー PM の復旧を開始できます。必要な場合、交換ノードを USB インストール メディアから手動でブートすることもできます。

インストールに使用するメディアに応じて、**PXE** または **USB** インストールのいずれかの手順を使用します。



注意事項: 復旧手順を行うと、PM のホスト オペレーティング システムにインストールされている全ソフトウェアと、復旧前に入力したすべての PM 構成情報が削除されます。この手順を完了した後は、ホストレベルの全ソフトウェアを手動で再インストールして、元の設定に一致するよう PM を再構成する必要があります。

前提条件:

1. 復旧が必要な PM を判断します。
2. USB メディアを使って交換 PM にシステム ソフトウェアをインストールする場合、
「[システム ソフトウェアの USB メディアを作成する](#)」の説明を参照してブート可能な USB メディアを作成します。



USB メディアを作成する際は、必ず一番最後にインストールしたアップグレード キットを含めてください。たとえば、ztC Edge コンソール ウィンドウのマストヘッドに表示されたリリースが 1.2.0-550 である場合、550 がビルド番号となり、**[アップグレード キット]** ページで USB メディアの作成用を選択するキットのバージョンは 1.2.0-550 にする必要があります。システムでターゲット PM 上に異なるビルドが検出された場合、ユーザ操作なしで自動的に復旧プロセスがオーバーライドされ、ターゲット PM 上の**すべてのデータを初期化**して、PXE ブート インストールを使って一番最近インストールされたソフトウェア キットが PM に再インストールされます。

3. USB メディアを使用する場合、キーボードとモニタを交換 PM に接続してインストール手順を監視し、設定を指定します。

PM を復旧するには (PXE ブート インストール)

次の手順を使用して PM を復旧します。ここでは PXE ブート インストールにより、プライマリ PM 上のソフトウェア キットからシステム ソフトウェアを再インストールします。

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
2. 作業する PM (node0 または node1) を選択して **[作業開始]** をクリックします。PM の**総合状態**が "メンテナンス モード" に変わり、**アクティビティ**状態が "実行中 (メンテナンス中)" に変わります。
3. PM が「**実行中 (メンテナンス中)**」になった後、**[リカバリ]** をクリックします。
4. 修復のタイプを選択するよう求められたら、**[PXE PM リカバリ - データの維持]** をクリックします。



注意事項: このとき **[PXE PM リカバリ - データの維持]** を選択しないと、インストール プロセスによってターゲット PM のデータが削除される可能性があるので注意してください。

5. **[続行]** をクリックして、復旧プロセスを開始します。システム ソフトウェアの再インストールの準備として、システムがターゲット PM をリブートします。
6. リカバリ プロセスがユーザによる操作なしで次のように続行されます。
 - ターゲット PM が、プライマリ ノードで一時実行される PXE サーバからのブートを開始します。
 - ターゲット PM が、システム ソフトウェアのインストールを自動的に開始します。これはプライマリ ノード上のインストールキットのコピーから実行されます。
 - インストールプロセスが、データをすべて維持したままシステム ソフトウェアを再インストールします。

ターゲット PM の物理コンソールでソフトウェア インストールの進捗状況を監視したり、プロンプトに応答する必要はありません。リカバリ プロセスは自動化されており、ソフトウェアのインストール処理中 PM に空白の画面が長時間表示されるのは正常な動作です。

7. ソフトウェアのインストールが完了すると、ターゲット PM が新しくインストールされたシステム ソフトウェアからリブートします。
8. ターゲット PM のブート中、ztC Edge コンソールの **[物理マシン]** ページでそのアクティビティを確認できます。復旧が完了すると、**[アクティビティ]** 列の PM の状態が「**(メンテナンス中)**」として表示されます。
9. 必要に応じて、アプリケーションおよびすべてのホストレベルのソフトウェアを手動で再インストールし、元の設定に一致するよう PM を再構成してください。
10. ターゲット PM をオンラインに戻す準備が完了したら、**[最終処理]** をクリックしてメンテナンス モードを終了します。両方の PM が「**実行中**」の状態に戻り、PM の同期が完了することを確認します。



注: ターゲット PM がメンテナンス モードを終了すると、システムはリカバリ プロセスに使用したプライマリ ノード上の PXE サーバを自動的に無効にします。

PM を復旧するには (USB インストール)

次の手順を使用して、USB メディアからシステム ソフトウェアを再インストールすることにより、PM を復旧します。

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。

2. 作業する PM (node0 または node1) を選択して **[作業開始]** をクリックします。PM の総合状態が **"メンテナンス モード"** に変わり、**アクティビティ** 状態が **"実行中 (メンテナンス中)"** に変わります。
3. PM が **「実行中 (メンテナンス中)」** になった後、**[リカバリ]** をクリックします。
4. 修復のタイプを選択するよう求められたら、**[USB PM リカバリ - データの維持]** をクリックします。



注意事項: このとき **[USB PM リカバリ - データの維持]** を選択しないと、インストール プロセスによってターゲット PM のデータが削除される可能性があるため注意してください。

5. **[続行]** をクリックして、復旧プロセスを開始します。システム ソフトウェアの再インストールの準備として、システムがターゲット PM をシャットダウンします。
6. ターゲット PM にブート可能な USB メディアを接続し、次に手動で PM の電源をオンにします。
7. ターゲット PM の電源がオンになったら、ファームウェア (UEFI) のセットアップ ユーティリティを起動します。**[Save & Exit (保存して終了)]** メニューの **[Boot Override (ブート オーバーライド)]** で、USB メディアに **[UEFI]** エントリを選択して、次のブートシーケンスでこのデバイスから 1 回ブートするようにします。PM が再起動します。



注: **[Boot (ブート)]** メニューで恒久的な **BOOT ORDER Priorities (ブート順序の優先度)** を変更する代わりに、ブート デバイスを一時的に変更するには **[Boot Override (ブート オーバーライド)]** プロパティを使用します。ztC Edge システムで通常実行されるノードの自動交換をサポートするため、最上位のブート優先度は **UEFI Network** (デフォルト) のままにする必要があります。

8. ターゲット PM の物理コンソールでインストールのプロセスを監視します。
9. **[Welcome (ウェルカム)]** 画面で、矢印キーを使ってインストール用に国のキーボードマップを選択します。
10. **[インストールまたはリカバリ]** 画面で、**[Recover PM, Join system: Preserving data (PM のリカバリ、システムの結合: データの維持)]** を選択し、**Enter** キーを押します。リカバリ プロセスがユーザによる操作なしで続行されます。



注意事項: このとき **[Recover PM, Join system: Preserving data (PM のリカバリ、システムの結合: データの維持)]** を選択しないと、インストールプロセスによってターゲット PM のデータが削除される可能性があるので注意してください。

11. ソフトウェアのインストールが完了すると、ターゲット PM が新しくインストールされたシステム ソフトウェアからリブートします。
12. ターゲット PM のブート中、ztC Edge コンソールの **[物理マシン]** ページでそのアクティビティを確認できます。復旧が完了すると、**[アクティビティ]** 列の PM の状態が「**(メンテナンス中)**」として表示されます。
13. 必要に応じて、アプリケーションおよびすべてのホストレベルのソフトウェアを手動で再インストールし、元の設定に一致するよう PM を再構成してください。
14. ターゲット PM をオンラインに戻す準備が完了したら、**[最終処理]** をクリックしてメンテナンス モードを終了します。両方の PM が「**実行中**」の状態に戻り、PM の同期が完了することを確認します。

関連トピック

[「メンテナンス モード」](#)

[「物理マシンを管理する」](#)

[「ztC Edge コンソール」](#)

[「\[物理マシン\] ページ」](#)

6

第 6 章: 仮想マシンを管理する

仮想マシン (VM) を管理して、その運用の制御、リソースのプロビジョニング、またはゲスト オペレーティング システムとアプリケーションの構成を行います。

VM の表示と管理は ztC Edge コンソールの **[仮想マシン]** ページで行えます。このページにアクセスする方法は、**「[仮想マシン] ページ」** を参照してください。特定の管理タスクの実行手順については次のトピックを参照してください。

VM の運用状態を管理するには、次を参照してください。

- **「仮想マシンを起動する」**
- **「仮想マシンをシャットダウンする」**
- **「仮想マシンの電源をオフにする」**
- **「仮想マシン コンソールのセッションを開く」**
- **「仮想マシンの名前を変更する」**
- **「仮想マシンを削除する」**

VM に関する情報の表示には、snmptable コマンドを使用します (**「snmptable でシステム情報を取得する」** を参照してください)。

VM の作成または構成を行うには、次を参照してください。

- **「仮想マシンのリソースを計画する」** (仮想 CPU、メモリ、ストレージ、およびネットワーク)
- **「仮想マシンを作成/マイグレーションする」**
- **「仮想 CD を管理する」**
- **「Windows ベースの仮想マシンを構成する」**

- [「Linux ベースの仮想マシンを構成する」](#)
- [「仮想マシンのリソースを管理する」](#)

USB デバイスを VM に接続するには、[「仮想マシンに USB デバイスを接続する」](#)を参照してください。

高度なタスクを実行するには、次を参照してください。

- [「仮想マシンに特定の MAC アドレスを割り当てる」](#)
- [「仮想マシンの優先 PM を選択する」](#)
- [「仮想マシンの保護レベルを変更する \(HA または FT\)」](#)
- [「仮想マシンのブート シーケンスを構成する」](#)
- [「故障した仮想マシンの MTBF をリセットする」](#)

VM マネージャーのローカルユーザ ロールはこれらのタスクの多くを実行できます。具体的には、**VM マネージャー**で次のことを行えます。

- [「\[仮想マシン\] ページ」](#)にある利用可能な機能ボタンとアクションのタスクを実行する
- [「\[仮想マシン\] ページ」](#)にあるすべての利用可能なタブを表示する
- [「\[仮想 CD\] ページ」](#)から VCD の作成と削除を行う

VM マネージャーのロールの割り当ての詳細については、[「ローカル ユーザ アカウントを管理する」](#)を参照してください。

仮想マシンのリソースを計画する

仮想マシンを作成するときは、システムのパフォーマンスと可用性を最大限にできるようなシステム リソースの割り当て方法を計画してください。

仮想マシンへのリソース割り当てを計画するには、次を参照してください。

- [「仮想マシンの vCPU を計画する」](#)
- [「仮想マシンのメモリを計画する」](#)
- [「仮想マシンのストレージを計画する」](#)
- [「仮想マシンのネットワークを計画する」](#)

仮想マシンの vCPU を計画する

仮想 CPU (vCPU) の割り当てによって、ztC Edge システムの仮想マシン (VM) にコンピューティング リソースを割り当てます。

VM に vCPU を割り当てるときは、以下の情報と制限事項に配慮してください。

- 各 vCPU は処理能力の仮想単位を表します。システムで利用可能な vCPU の合計数は、システム内で処理能力が低い方の物理マシン (PM) が表すハードウェア スレッドの数に一致します。たとえば、1 台の PM にそれぞれ 2 つのスレッドで構成されるコアが 4 つ (つまり vCPU が 8 個) あり、同じシステム内の 2 台目の PM にそれぞれ 2 つのスレッドで構成されるコアが 8 つ (つまり vCPU が 16 個) ある場合、利用できる vCPU の合計数は 8 個 (つまり処理能力が小さい方の PM のスレッド数) となります。
- VM に割り当てることのできる vCPU の数は、システム内にある vCPU の合計数に等しくなります。
- 1 つの VM に割り当てることのできる vCPU の最大数は、システム内にある vCPU の合計数に等しくなります。
- Windows ベースの VM: 割り当て済み vCPU の数を 1 から n または n から 1 に変更した場合、再プロビジョニングの完了時に VM を再起動した後で ([「仮想マシンのリソースを再プロビジョニングする」](#)を参照)、VM をもう一度シャットダウンして再起動する必要があります。これにより、VM が対称型マルチプロセッシング (SMP) のために正しく再構成されます。この VM は、再起動されるまで異常な動作を示し、使用不可になります。
- ztC Edge コンソールの **[システム]** ページ ([「\[システム\] ページ」](#)を参照) に、vCPU の合計容量、ztC Edge システム ソフトウェアに割り当てられた vCPU の数、実行中の VM により使用される vCPU の数、および利用可能な vCPU の数が表示されます。
- Stratus Redundant Linux ソフトウェアでは vCPU のオーバープロビジョニングが許可されません。**[システム]** ページに表示された空き vCPU の数がゼロ未満の場合、vCPU のオーバープロビジョニングが発生したことを示します。これはコンソールにも表示され、vCPU がどの程度オーバープロビジョニングされているかも表示されます。
- vCPU をオーバープロビジョニングしても VM の作成や起動には支障はありませんが、オーバープロビジョニングが発生した状態でシステムを稼動するのは避けることを推奨します。

仮想 CPU のオーバープロビジョニングに関する考慮事項



注: 一般に、VM リソースのオーバープロビジョニングは避けてください。各 VM のリソースは隔離して、VM をリソース リークや予期しないパフォーマンス ピークの発生し得る他の VM から保護するのが理想的です。VM を作成して構成する際は、他の VM では使用できない専用のリソースを割り当てるようにします。

物理 CPU のオーバープロビジョニングは、次の状況が当てはまる場合のみに行います。

- すべての VM によって消費されるピーク時 vCPU リソースが、ztC Edge システムの物理リソースを超えていない場合。
- 1 つ以上の VM を異なる時間に使用している場合 (オフピーク時のバックアップなど)。
- 1 つ以上の VM を、別の VM の稼動中に停止する場合 (VM のアップグレード中、VM のバックアップや復旧時など)。
- VM で使用されるピーク時合計 CPU が、サービス レベル アグリーメントまたは必要な応答時間に影響を及ぼさない場合。
- 各 VM の CPU 使用状況をよく把握していて、そのアプリケーションにリソース リークの傾向がない場合。CPU がオーバープロビジョニングされた場合、1 つの VM で発生したリークが他の VM のパフォーマンスに影響を及ぼすことがあります。

関連トピック

[「システム要件の概要」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

仮想マシンのメモリを計画する

メモリの割り当てによって、ztC Edge システムの仮想マシン (VM) に物理メモリを割り当てます。

VM にメモリを割り当てるときは、以下の情報と制限事項に配慮してください。

- VM に割り当てることのできる合計メモリは、ztC Edge システムで使用可能な合計メモリ ([「システム要件の概要」](#)を参照) から、ztC Edge システム ソフトウェアに割り当てられたメモリ容量を差し引いたものです。たとえば、メモリの合計容量が 32 GB あり、システム ソフトウェアに 2 GB を割り当てた場合、VM で使用可能なメモリは 30 GB になります。

- 2つのノードで構成されているシステムでは、1台のVMに、最大ですべてのVMに利用できるメモリ合計容量までのメモリをプロビジョニングすることができます。各VMは、その要求されたメモリ容量に20%のオーバーヘッドを加算した容量を使用します。
- 許容される最小のメモリ割り当ては256 MBですが、64ビットオペレーティングシステムでは少なくとも600 MBが必要です。ゲストオペレーティングシステムのメモリの要件を必ず確認してください。
- ztC Edge コンソールの **[システム]** ページ ([「\[システム\] ページ」](#) を参照) に、メモリの合計容量、ztC Edge システム ソフトウェアに割り当てられたメモリ、実行中のVMにより使用されるメモリ、および空きメモリの容量が表示されます。このページを使用してメモリの割り当てを確認します。
- Stratus Redundant Linux ソフトウェアでは、**実行中の** VM のオーバープロビジョニングが許可されないため、物理マシンの合計物理メモリ容量を超える VM を起動することはできません。メモリのオーバープロビジョニングの発生を許可しても安全なのは、たとえば VM のアップグレードやポイントインタイム バックアップまたは復旧の最中などの、VM のうち1つ以上が**停止中**で、なおかつ別のVMが実行中の場合のみです。
- 必要な場合には使用度の低い仮想マシンを1つ以上シャットダウンするか再構成し、使用度の高いVMに利用可能なリソースを割り当て直すことによって、メモリを手動で再配分することができます。

関連トピック

[「システム要件の概要」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

仮想マシンのストレージを計画する

ztC Edge システムのストレージ割り当てを計画して、仮想マシン (VM) とシステム管理のニーズを満たすのに十分な空き容量を確保します。

ストレージを仮想マシン (VM) に割り当てる際、以下の点について考慮してください。

- ストレージの最大容量を考慮する

Stratus Redundant Linux ソフトウェアはストレージのオーバプロビジョニングを許可しません。すべての VM および VCD に必要なストレージの合計は、ztC Edge システムで利用可能なストレージの合計未満でなければなりません。

- 追加の VCD 用にストレージ容量を残しておく

追加の VM やアプリケーションをインストールするための VCD 用として、少なくとも 5 GB の空き容量を残しておきます。(このストレージ容量を確保するため、使用し終わった VCD を削除することを検討してください。)

- 各 VM に個別のブート ボリュームとデータ ボリュームを作成する

ゲストオペレーティングシステムとアプリケーションを最初の (ブート) ボリュームにインストールし、その関連データ用には別のボリュームを作成します。ブート ボリュームとデータ ボリュームを区別しておくことでデータの保護に役立ち、ブート ボリュームがクラッシュした際に VM を簡単に復旧できます。

- ゲストオペレーティングシステムにオーバーヘッドを追加した容量を持つブート ボリュームを作成する

ゲストオペレーティングシステムの容量の最小要件に従い、ボリュームのフォーマット後の容量と使用容量を考慮して、容量を大めに割り当てることを検討します。たとえば、VM の作成時にブートドライブに 5 GB 割り当てた場合、そのブートボリュームのフォーマット後の容量は、使用開始前に約 4.8 GB となり、5 GB の要件を満たすには不十分な可能性があります。

- 最大ボリューム サイズを確認する

ボリュームのエクスポート、インポート、または復元を行う際、最大ボリューム サイズを確認しておきます (「[重要な考慮事項](#)」を参照してください)。

関連トピック

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

仮想マシンのネットワークを計画する

ネットワークリソースを計画して、利用可能な仮想ネットワークを ztC Edge システム上の仮想マシン (VM) に割り当てる方法を決定します。

2 台の物理マシン (PM) で構成されているシステムを展開すると、ソフトウェアが 2 台の PM をまたぐ物理ネットワークポートのペアをバインディングして、冗長性のある仮想ネットワークを形成します。ztC

Edge システム上に VM を作成または再プロビジョニングする際は、物理ネットワーク ポートではなく、これらの仮想ネットワークに VM を接続します。

VM を仮想ネットワークに接続するときは、以下の情報と制限事項に配慮してください。

- 1 台の VM を複数の仮想ネットワークに接続できます。複数の VM を同じ仮想ネットワークに接続することもできます。
- Stratus Redundant Linux ソフトウェアでは、ネットワーク リソースのオーバープロビジョニングに制限がありません。したがって、仮想ネットワークを割り当てる際は VM のネットワーク帯域幅および応答時間の必要条件を考慮します。
- 複数の VM で同じ仮想ネットワークを共有する場合、利用可能なネットワーク帯域幅はこれらの VM 間で均等に共有されます。vCPU 容量と異なり、帯域幅リソースを比例して割り当てる方法はありません。したがって、1 台の VM によるネットワーク リソースの使用度が高い場合、当該ネットワーク上のすべての VM のパフォーマンスが劣化することがあります。VM の帯域幅要件が大きい場合、その VM に専用の仮想ネットワークを接続することを検討してください。

関連トピック

[「全般的なネットワーク要件と構成」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

仮想マシンを作成/マイグレーションする

新しい VM を作成するか、既存の VM または物理マシン (PM) をネットワーク経由で直接マイグレーションする、あるいは OVF (Open Virtualization Format) ファイルまたは Open Virtualization Appliance (OVA) ファイルを既存の VM からインポートする方法で、システムに新しい仮想マシン (VM) を作成します。

既存のソース VM または PM を使用せずに新しい VM を作成するには、[「新しい仮想マシンを作成する」](#)を参照してください。

新しい VM を作成するためや、トラブルシューティングの目的で VM を複製するためにシステム上の既存の VM をコピーするには、[「仮想マシンをコピーする」](#)を参照してください。

別のシステムから VM をマイグレーションやインポートしたり、同じ システム上の VM を復元するには、次のいずれかのトピックを参照してください。

- [「物理マシンまたは仮想マシンをシステムにマイグレーションする」](#)

"P2V クライアント" (**virt-p2v**) を使用して、PM または VM をネットワーク経由で直接 システム上の新しい VM に転送します。

- [「仮想マシンをエクスポートする」](#)

ztC Edge コンソールを使用してソース VM をネットワーク共有上の OVF および VHD ファイルにエクスポートします。

- [「OVF または OVA ファイルをインポートする」](#)

ztC Edge コンソールを使用して、OVF または VHD ファイルを別の ztC Edge システムから ztC Edge システムにインポートするか、OVF および VHD ファイルまたは OVA ファイルを VMware vSphere ベースのシステムから ztC Edge システムにインポートします。

- [「OVF ファイルから仮想マシンを交換/復元する」](#)

ztC Edge コンソールを使用して、OVF および VHD ファイルを同じシステムにインポートし、既存の VM を以前のバックアップ コピーで上書きして復元します。

関連トピック


[「仮想マシンを管理する」](#)

新しい仮想マシンを作成する

新しい仮想マシン (VM) を作成して、ztC Edge システムにゲスト オペレーティング システムをインストールします。(既存の VM または物理マシン (PM) をマイグレーションすることもできます。説明は、[「仮想マシンを作成/マイグレーションする」](#)を参照してください。)

[仮想マシン] ページの **[作成]** をクリックして、**VM 作成ウィザード**を起動します。ウィザードに VM のリソース割り当てのプロセスが順を追って表示されます。

前提条件:

- 「[仮想マシンのリソースを計画する](#)」および「[仮想マシンの推奨事項と制限](#)」のリストを参照し、VM への CPU、メモリ、ストレージ、およびネットワーク リソースの割り当てに関する前提条件と考慮事項を確認します。後者のリストには、高可用性 (HA) およびフォールトトレラント (FT) 運用が可能なシステムも一覧されています。
- サポートされるゲストオペレーティングシステムおよびブートインターフェースを実行する VM を作成できます。詳細については、「[テスト済みのゲストオペレーティングシステム](#)」を参照してください。
-  VM をブートするソースとして、リモートの ISO またはブート可能な仮想 CD (VCD) を選択できます。リモート ISO の場合、レポジトリの URL またはパス名が必要です。また、共有ネットワークドライブ上のリモート ISO の場合は、ユーザ名とパスワードが必要となります。Windows または Linux インストールメディアのブート可能な VCD が必要な場合、「[仮想 CD を作成する](#)」の説明を参照して作成してください。ブート可能な VCD は単一の CD または DVD でなければなりません。複数の CD または DVD はサポートされていません。
- ztC Edge システムの両方の PM がオンラインになっていることと、ネットワークに接続していることを確認します。そうでない場合、システムが VM を正しく作成できません。

新しい VM を作成するには

1. 2 つのノードで構成されているシステムの **[物理マシン]** ページ (「[\[物理マシン\] ページ](#)」を参照) で、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンスモードではなく、同期の実行中でもないことを確認します。
2. **[仮想マシン]** ページ (「[\[仮想マシン\] ページ](#)」を参照) で、**[作成]** をクリックして **VM 作成ウィザード**を開きます。
3. **[名前、説明、保護および OS]** ページで、次を行います。
 - a. VM に ztC Edge コンソールで表示される **[名前]** を入力し、オプションで **[説明]** を入力します。VM 名は、以下の要件を満たす必要があります。

- VM 名は単語または数字で始める必要があり、名前に特殊文字 (たとえば #、%、または \$) を含めることはできません。
 - VM 名に Zombie- や migrating- などのハイフン付きのプレフィックスは使用できません。
 - VM 名には最大 85 文字を使用できます。
- b. VM で使用する保護のレベルを選択します。
- **フォールトトレラント (FT)** — 2 台の物理マシンで実行される VM に冗長な環境を作成することにより、アプリケーションを透過的に保護します。FT は、HA で提供される以上のダウンタイム保護を必要とするアプリケーションに使用します。
 - **高可用性 (HA)** — 基本的なフェールオーバーと復旧機能を提供し、発生した障害によっては復旧に (自動の) VM リブートが必要です。HA は、ある程度のダウンタイムが許容され、FT が提供する高レベルのダウンタイム保護を必要としないアプリケーションに使用してください。

保護のレベルの詳細については、「[運用モード](#)」を参照してください。

- c. **[ブートインタフェース]** に次のいずれかを選択します。
- **BIOS** — Basic Input/Output System
 - **UEFI** — Unified Extensible Firmware Interface

注:



1. 選択した **[ブートインタフェース]** がゲストオペレーティングシステムでサポートされていることを確認します。そうでない場合、ゲストオペレーティングシステムを正しくブートできません。ztC Edge システムでサポートされているゲストオペレーティングシステムとブートインタフェースのリストは、「[テスト済みのゲストオペレーティングシステム](#)」を参照してください。
2. **[ブートインタフェース]** を設定できるのは VM の作成時のみです。後で設定を変更することはできません。

- d. **[ブートのソース]** で、ブートソースとして次のいずれかを選択します。
- **VCD** – ブートソースはVCDです。プルダウンメニューからソースを選択します。
 - **Windows 共有経由のリモート ISO (CIFS/SMB)** – ブートソースは共有ネットワークドライブ上のリモート ISO ファイルです。**[ユーザ名]** と **[パスワード]** に値を入力する必要があります。**[レポジトリ]** に、「**¥¥<マシンの URL>¥<共有名>**」の形式で値を入力します (例: **¥¥192.168.1.34¥MyISO_Folder**)。
 - **NFS 経由のリモート ISO** – ブートソースは NFS 経由でアクセスする ISO ファイルです。**[レポジトリ]** に、リモートシステムの URL を「**nnn.nnn.nnn.nnn**」の形式で入力します (**http://** や **https://** は含めません)。

利用可能な ISO レポジトリのリストを表示するには、**[ISO のリスト]** をクリックして ISO ファイルを選択します。選択した ISO ファイルの完全パス名が **[レポジトリ]** の下に表示されます。表示された ISO URL を編集することはできません。

- e. **[次へ]** をクリックします。

4. **[vCPU とメモリ]** ページで次を行います。

- a. VM に割り当てる **vCPU** の数と**メモリ**の容量を指定します。詳細については、「[仮想マシンの vCPU を計画する](#)」および「[仮想マシンのメモリを計画する](#)」を参照してください。
- b. **[次へ]** をクリックします。

5. **[ボリューム]** ページで次を行います。

- a. ztC Edge コンソールに表示されるブートボリュームの**[名前]**を入力します。
- b. 作成するボリュームの**[ボリューム サイズ]**をギガバイト (GB) 単位で入力します。ストレージ割り当ての詳細については、「[仮想マシンのストレージを計画する](#)」を参照してください。
- c. 必要に応じて、**[新しいボリュームの追加]** をクリックして各ボリュームのパラメータを指定し、追加のデータ ボリュームを作成します。(VM を作成した後、**仮想マシンの再プロビジョニング** ウィザードを使用してボリュームを追加することもできます。詳細については、「[仮想マシンのボリュームを作成する](#)」を参照してください。)
- d. **[次へ]** をクリックします。

6. **[ネットワーク]** ページで、VM に接続する共有ネットワークを選択します (詳細については、「[仮想マシンのネットワークを計画する](#)」を参照してください)。ネットワークを有効化や無効化して、MAC アドレスを指定することもできます。続行するには **[次へ]** をクリックします。

7. **[作成サマリ]** ページで次を行います。

- a. 作成サマリの内容を確認します。変更が必要な場合、**[戻る]** をクリックします。
- b. コンソール セッションの自動開始を避け、ソフトウェアのインストール処理をモニタリングできるようにするには、**[コンソールの起動]** の選択を解除します。
- c. VM のプロビジョニング内容を受け入れてソフトウェアのインストールを開始するには、**[完了]** をクリックします。

VM 作成ウィザードに作成の進捗状況が表示され、状況に応じてコンソール ウィンドウが開きます。コンソール ウィンドウが開く際、コンソールが VM に接続するのに 1 分ほどかかることがあります。

8. Windows ベースの VM では、VM コンソールが開いたら、コンソール ウィンドウ内をクリックし、VCD またはリモート ISO から **Windows セットアップ** を実行するために任意のキーを押す準備をしてください。

```
Press any key to boot from CD or DVD...
```

UEFI ブート タイプの Windows ベースの VM では、1 ～ 2 秒以内にキーを押す必要があります。そうでないと、**[UEFI Interactive Shell (UEFI インタラクティブ シェル)]** が表示されます。その場合には、次のように **Windows セットアップ** を実行することができます。

- a. **[UEFI Interactive Shell (UEFI インタラクティブ シェル)]** で、Shell> プロンプトに「exit」と入力して **Enter** キーを押します。

```
Shell> exit
```

- b. 矢印キーを使用して **[Continue (続行)]** を選択し、**Enter** キーを押します。

```
Select Language

Device Manager

Boot Manager

Boot Maintenance Manager

Continue

Reset
```

- c. VM が再起動したら、任意のキーを押して、VCD またはリモート ISO から **Windows セットアップ** を実行します。

```
Press any key to boot from CD or DVD...
```

- d. 任意のキーを押すタイミングが合わず **[UEFI Interactive Shell (UEFI インタラクティブ シェル)]** が再び表示された場合は、ステップ a ～ c を繰り返します。
9. 必要に応じて、VM コンソール セッションでオペレーティング システムのインストールの進行状況を確認したり (必要な場合はブラウザでポップアップを許可してください)、任意のプロンプトに応答できます。
10. オペレーティング システムをインストールした後、稼動時に必要となる追加のリソースとソフトウェアを構成します。詳細については次を参照してください。
- [「Windows ベースの仮想マシンを構成する」](#)
 - [「Linux ベースの仮想マシンを構成する」](#)



注意事項: インストール処理が完了した後、最後のリブートを実行する前にプライマリ PM で障害が生じたり VM がクラッシュした場合、VM のインストールを再開しなければならないことがあります。

次のいずれかのインストールが中断した場合、VM がリブートしないことがあります。

- 構成手順を含む、ゲスト オペレーティング システム
- システム ファイルを処理する任意のミドルウェアまたはアプリケーション

関連トピック

[「仮想マシンをコピーする」](#)

[「仮想マシンの名前を変更する」](#)

[「仮想マシンを削除する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンをコピーする

ztC Edge システム上の既存の VM を複製するには、仮想マシン (VM) をコピーします。たとえば、正常な VM をコピーして新しい VM を作成したり、不具合のある VM をコピーしてトラブルシューティングに使用することができます。(VM を別のシステムからインポートしたりマイグレーションする場合は、[「仮想マシンを作成/マイグレーションする」](#)を参照してください。)

VM をコピーするには、**[仮想マシン]** ページで VM を選択して **[コピー]** をクリックします。ウィザードに新しい VM の名前変更とリソース割り当てのプロセスが順を追って表示されます。

VM のコピー操作では、一意の SMBIOS UUID、システム シリアル番号、MAC アドレス、およびハードウェア ID を持つ、同一の VM が作成されます。

注:

- ソース VM との競合を避けるため、コピー ウィザードは新しい VM にある各ネットワーク インタフェースに新しい MAC アドレスを自動的に割り当てますが、場合によっては IP アドレスとホスト名を手動で更新しなければなりません。
- VM のコピー中に ztC Edge システムがプライマリ PM からセカンダリ PM に切り替わった場合、そのコピー プロセスは失敗します。これはシステムの継続運用には影響しませんが、コピーした VM に関連付けられているすべてのボリュームを削除してから、コピーを再起動する必要があります。
- システムがサポートしている運用モードの詳細については、[「仮想マシンの推奨事項と制限」](#) を参照してください。
- 1 つのノード用に構成されているシステム上の VM をコピーすることができます。

前提条件:

- コピーを実行する前に VM をシャットダウンする必要があります。
- 2 つのノードで構成されているシステムでは、コピー プロセスが正しく機能するためには、ztC Edge システムの両方の PM がオンラインでなければなりません。

ztC Edge システム上の VM をコピーするには

1. 2 つのノードで構成されているシステムの **[物理マシン]** ページ ([「\[物理マシン\] ページ」](#) を参照) で、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンス モードではなく、同期の実行中でもないことを確認します。1 つのノードで構成されているシステムでは、PM が「**実行中**」の状態にあることを確認してください。
2. **[仮想マシン]** ページ ([「\[仮想マシン\] ページ」](#) を参照) で、コピーする VM を選択して **[シャットダウン]** をクリックします。
3. VM が停止したら **[コピー]** をクリックしてコピー ウィザードを開きます。

4. **[名前、説明および保護]** ページで、次を行います。

- a. VM に ztC Edge コンソールで表示される **[名前]** を入力し、オプションで **[説明]** を入力します。
- b. VM で使用する保護のレベルを選択します。
 - **フォールトトレラント (FT)**
 - **高可用性 (HA)**

これらの保護レベルの詳細については、「[新しい仮想マシンを作成する](#)」と、「[運用モード](#)」を参照してください。

- c. **[次へ]** をクリックします。

5. **[vCPU とメモリ]** ページで次を行います。

- a. VM に割り当てる **vCPU** の数と**メモリ**の容量を指定します。詳細については、「[仮想マシンの vCPU を計画する](#)」および「[仮想マシンのメモリを計画する](#)」を参照してください。
- b. **[次へ]** をクリックします。

6. **[ボリューム]** ページで、次を行います。

- **[名前]** にボリューム名を入力します。
- 各ボリュームの **[ボリューム サイズ]** を指定します。
- **[新しいボリュームの追加]** をクリックして新しいデータ ボリュームを作成します。(ボタンが表示されない場合、ウィザード ページの一番下までスクロールします。)

詳細については、「[仮想マシンのストレージを計画する](#)」を参照してください。続行するには **[次へ]** をクリックします。

7. **[ネットワーク]** ページで、この VM に接続する各共有ネットワークのチェック ボックスをオンにします。

8. **[コピー サマリ]** ページで次を行います。

- a. 構成サマリの内容を確認します。変更が必要な場合、**[戻る]** をクリックします。
- b. VM のコピーを続行するには **[完了]** をクリックします。

コピー プロセスの完了後、ztC Edge システムは HA または FT 運用を有効にするため、PM 間のデータ同期を続行することがあります。

トラブルシューティング

コピー プロセスで発生した問題を解決するには、必要に応じて以下の情報を参照してください。

コピー操作をキャンセルしたり、コピーが失敗した後にクリーンアップするには

コピーした VM に関連付けられているすべてのボリュームを削除します。

関連トピック

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

物理マシンまたは仮想マシンをシステムにマイグレーションする

物理マシン (PM) または仮想マシン (VM) のマイグレーションでは、A-Link ネットワークを経由して システムの新しい VM にマシンを転送します。(Open Virtualization Format (OVF) または Open Virtualization Appliance (OVA) ファイルをシステムにインポートすることもできます。概要は、[「仮想マシンを作成/マイグレーションする」](#)を参照してください。)

下の手順では、PM または VM をネットワーク経由でマイグレーションし、ソース PM または VM で "P2V クライアント" (**virt-p2v**) ISO ファイルをダウンロードし、P2V クライアント ISO ファイルをブートした後、このクライアントを使用してソース側からセキュアなネットワーク転送の構成、開始、およびモニタリングを行う方法を示します。マイグレーションが完了するまではシステムで構成手順を行う必要はありませんが、ztC Edge コンソールの **[ボリューム]** ページに新しい VM に関連付けられたボリュームが順次表示されるので、マイグレーションが進行中であることを確認できます。



注意事項: マイグレーションの準備を行う前に、ソース PM または VM のバックアップを取ることを検討してください。VM をバックアップするには、これをエクスポートします ([「仮想マシンをエクスポートする」](#)を参照してください)。VM や PM のバックアップの詳細については、[「セキュリティの強化」](#)を参照してください。

注:

- マイグレーション プロセスでは、次のオペレーティング システムを実行する PM または VM のみがサポートされます。
 - CentOS/RHEL 7.5
 - Microsoft Windows 10 Desktop、または Windows Server 2012、2016、2019
 - Ubuntu 18.04 サーバー この VM をマイグレーションした後は、追加の手順を行う必要があります。[「Ubuntu VM のマイグレーションを完了するには」](#)を参照してください。
 - VMware リリース 6.x
- "休止状態" や "高速スタートアップ" モードをサポートする Windows ベースの VM では、マイグレーション プロセスの前にこれらの機能を無効にする必要があります。休止や高速スタートアップ モードを完全に無効にするには、下記の「**トラブルシューティング**」で、「Failed to mount '/dev/sda1: Operation not permitted ('/dev/sda1 をマウントできません。操作が許可されていません)」というエラー メッセージが表示されて失敗したマイグレーションから復旧する手順を参照してください。
- Linux ベースの PM または VM の場合、マイグレーション プロセスの前に `/etc/fstab` ファイルを編集してデータ ボリュームのエントリをコメントアウトし、ブート ボリュームのみがマウントされるようにすることを検討してください。Linux ベースの VM は ztC Edge システム上で異なるデバイス名を使用するので、元のデバイス名のボリュームをマウントできない場合、新しい VM がシングルユーザ モードでブートされることがあります。マイグレーションの後、`/etc/fstab` のエントリを正しいデバイス名に戻すことができます。詳細については、下記の「**トラブルシューティング**」を参照してください。
- VMware VM をマイグレーションする場合、VMware のコンソールから電源をオフにするのに加え、オペレーティング システムのシャットダウン コマンドを使って VM をシャットダウンする必要があります。VMware のコンソールだけを使って VM をシャットダウンすると、マイグレーションは失敗します。





- マイグレーション プロセスの進行中はソース PM または VM をオフラインにする必要があります。マイグレーションのために計画的なメンテナンス期間を設定することを検討してください。
- VM を everRun または ztC Edge システムからマイグレーションしている処理の最中に、「VM <名前> の起動に失敗しました」というアラートが表示された場合、これは正常な動作です。これは、ソース VM の電源がオンになっていて P2V クライアントを実行していても、ゲスト オペレーティング システムが起動しないためです。
- マイグレーションにかかる時間は、ソース システムにあるボリ्यूムのサイズと数、およびソースとターゲット システム間のネットワーク帯域幅によって異なります。たとえば、20 GB のブート ボリ्यूムが 1 つあるソース システムを 1 Gb ネットワークで転送するには約 30 分かかります。
- 1 度に複数の PM や VM のマイグレーションを行えますが、ネットワーク帯域幅を共有すると、マイグレーションの処理時間は長くなります。
- 元の PM または VM との競合を避けるため、P2V クライアントは新しい VM にある各ネットワーク インタフェースに新しい MAC アドレスを自動的に割り当てますが、IP アドレスとホスト名は必要に応じて手動で更新する必要があります。
- マイグレーションの処理中にシステムがプライマリ PM からセカンダリ PM に切り替わった場合、そのマイグレーション プロセスは失敗します。これはシステムの継続運用には影響しませんが、ソース PM または VM の P2V クライアントをリブートして再実行する必要があります。詳細については、下記の「**トラブルシューティング**」を参照してください。
- PM や VM をマイグレーションした後、ネットワーク ドライバが正しくインストールされないことがあります。この問題が発生した場合は、ドライバを手動でインストールしてください。詳細については、下記の「**トラブルシューティング**」を参照してください。



前提条件: 2 つのノードで構成されているシステムの場合、マイグレーション プロセスが正しく機能するためには、システムの両方の PM がオンラインになっている必要があります (1 つのノードで構成されているシステム上で PM や VM のマイグレーションは行えません)。ztC Edge コンソールの **[物理マシン]** ページで、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンス モードではなく、同期も行われていないことを確認します。

次のマイグレーション手順を実行します (必要に応じてドロップダウン メニューをクリックしてくださ

い)。

ztC Edge システムへの PM のマイグレーションを準備するには

1. P2V クライアントの ISO ファイルを **[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) からダウンロードします。
 - a. **[Downloads (ダウンロード)]** ページで **ztC Edge** をクリックし (まだ表示されていない場合)、次に適切なバージョンを選択します。
 - b. **[Drivers and Tools (ドライバとツール)]** にスクロールし、さらに **[ztC Edge P2V Client for Virtual or Physical Machine Migration (仮想マシンまたは物理マシン マイグレーション用の everRun P2V クライアント)]** までスクロールします。
 - c. **P2V クライアント (virt-p2v)** ファイルを選択します。
2. ISO イメージの整合性を検証する場合、MD5 のチェックサム ハッシュ関数を使用します。コマンドプロンプト ウィンドウを管理者として開き、次を入力します。

CertUtil -hashfile *path_to_file* MD5

CertUtil コマンドによって、コマンドの実行が正しく完了したかどうかを示すメッセージが表示されます。コマンドが成功した場合、次のステップに進みます。コマンドが失敗した場合はもう一度ダウンロードを行います。

3. ソース PM のブートに使用する CD-ROM に、P2V クライアントの ISO ファイルを書き込みます。
4. P2V クライアント CD を、ソース PM の CD または DVD ドライブに挿入します。
5. PM をシャットダウンして、P2V クライアントをブートする準備をします。

ztC Edge システムへの VM のマイグレーションを準備するには

1. P2V クライアントの ISO ファイルを、**[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) の **[Drivers and Tools (ドライバとツール)]** セクションからダウンロードします。VM をマイグレーションするターゲットの ztC Edge システム バージョンに一致するバージョンの P2V クライアントをダウンロードしてください。
2. ISO イメージの整合性を検証する場合、MD5 のチェックサム ハッシュ関数を使用します。コマンドプロンプト ウィンドウを管理者として開き、次を入力します。

CertUtil -hashfile *path_to_file* MD5

CertUtil コマンドによって、コマンドの実行が正しく完了したかどうかを示すメッセージが表示されます。コマンドが成功した場合、次のステップに進みます。コマンドが失敗した場合はもう一度ダウンロードを行います。

3. P2V クライアント ISO ファイルをソース VM に挿入または接続し、関連するハイパーバイザで仮想 CD ドライブをブートデバイスに設定します。
4. VM をシャットダウンして、P2V クライアントをブートする準備をします。

ztC Edge システムに PM または VM をマイグレーションするには

1. ソース PM または VM の電源をオンにして P2V クライアントをブートします。約 1 分後に **virt-p2v** ウィンドウが開きます。
2. P2V クライアントは DHCP からネットワーク設定を自動的に取得します。静的な設定はマイグレーション プロセスに必要ありませんが、オプションとして **[Configure network (ネットワークの構成)]** をクリックして設定を指定することもできます。(必要な場合は、後で ztC Edge システム上でターゲット VM のネットワーク設定を構成します。)
3. **変換サーバ** (ztC Edge システム) の接続設定を入力します。システムのホスト名または IP アドレスと **root** アカウントの **[Password (パスワード)]** を入力します。(「[ホストオペレーティングシステムにアクセスする](#)」にあるように、ztC Edge ホスト オペレーティングシステムの **root** アカウントを使用する必要があります。)
4. **[Test connection (接続のテスト)]** をクリックします。P2V クライアントが ztC Edge システムに接続できる場合、**[Next (次へ)]** をクリックして操作を続行します。**[Target properties (ターゲット プロパティ)]**、**[Fixed hard disks (固定ハード ディスク)]**、およびその他の設定用のセクションを含むページが開きます。

P2V クライアントが接続できない場合には、接続設定を確認してから接続を再試行してください。

5. **[Target properties (ターゲット プロパティ)]** セクションで、ztC Edge コンソールに表示されるターゲット VM の **[Name (名前)]** を入力します。(ztC Edge システムのすべての既存の VM と異なる名前を指定する必要があります。)
6. **[# vCPUs (vCPU の数)]** および **[Memory(MB) (メモリ (MB))]** の値は自動的に検知されて入力されますが、ztC Edge システムの VM にソース PM または VM よりも多くの CPU やメモリを割り当てたい場合には、これらの値を変更することもできます。

7. ターゲット VM の **[Virt-v2v output options (Virt-v2v 出力オプション)]** を次のように指定します。
 - a. **[Output to (出力先)]** の横で **[HA]** (高可用性) または **[FT]** (フォールトトレラント) のどちらかの運用モードを選択します。(運用オプションの詳細については、[「新しい仮想マシンを作成する」](#) および [「運用モード」](#) を参照してください。)
 - b. **[Output format (出力フォーマット)]** の横で、ディスクイメージのフォーマットに **[raw]** または **[qcow2]** を選択します。
8. マイグレーションプロセスからのデバッグメッセージを保存する場合、オプションで **[Enable server-side debugging (サーバサイド デバッグの有効化)]** チェックボックスをオンにします。(Stratus 認定サービス業者用に診断ファイルを作成する場合、そのファイルにデバッグメッセージも含まれています。 [「診断ファイルを作成する」](#) を参照してください。)
9. マイグレーションに含める **[Fixed hard disks (固定ハードディスク)]** (ボリューム) を選択するには、各デバイスの横のチェックボックスをオンにします。

ブートボリュームを含めて 1 つ以上のボリュームを選択する必要があります。(P2V クライアントは Linux ベースのユーティリティなので、すべてのデバイスが Linux デバイス名を使って表示されます。したがって **sda** または **vda** はブートボリュームを表します。)
10. マイグレーションに含める **[Network Interfaces (ネットワーク インタフェース)]** を選択するには、各デバイスの横のチェックボックスをオンにします。

ターゲットの ztC Edge システムに複数の共有ネットワークがある場合、各ネットワークインタフェースに接続する共有ネットワークを選択することもできます。ネットワークインタフェースをダブルクリックして **[Configure Network (ネットワークの構成)]** ダイアログボックスを開き、ドロップダウン リストから共有ネットワークを選択します。

[Configure Network (ネットワークの構成)] ダイアログボックスで、特定のネットワークインタフェースに MAC アドレスを指定することもできます。アドレスを指定しない場合、各ネットワークインタフェースの MAC アドレスがシステムによって自動的に設定されます。

ネットワーク インタフェースの構成を完了したら **[OK]** をクリックします。
11. ztC Edge システムに PM または VM をマイグレーションする準備が完了したら、**[Start conversion (変換の開始)]** をクリックします。(何らかの理由でマイグレーションをキャンセルする必要がある場合はこの後の「[トラブルシューティング](#)」を参照してください。)

12. マイグレーションが完了すると、P2V クライアントに処理が成功したというメッセージが表示されます。該当する場合は CD または仮想 CD を取り出し、**[電源オフ]** をクリックしてソース PM または VM をシャットダウンします。



注: マイグレーションの後、ztC Edge システムの新しい VM はプライマリ PM 上に配置され、停止中の状態のままになります。VM を起動する前に、次の手順を実行してマイグレーションの処理を完了してください。

ztC Edge システムのマイグレーションを完了させるには

1. ztC Edge コンソールで **[仮想マシン]** ページを開きます ([「\[仮想マシン\] ページ」](#) を参照してください)。
2. 上部パネルで新しい VM を選択して **[構成]** をクリックし、**仮想マシンの再プロビジョニング** ウィザードを開きます。 [「仮想マシンのリソースを再プロビジョニングする」](#) を参照してください。ウィザードを使用して VM に必要な vCPU、メモリ、ストレージ、およびネットワーク設定を構成します。
 - ソース PM または VM に複数のネットワーク インタフェースがある場合、マイグレーション プロセスに含まれないその他のネットワーク インタフェースを構成します。
 - ソース PM または VM を引き続き実行する場合、新しい VM で各ネットワーク インタフェースの MAC アドレスが、ソース PM または VM のものとは異なることを確認してください。

ウィザードの最後のページで **[完了]** をクリックし、変更を有効にします。

3. **[起動]** をクリックして、新しい VM をブートします。
4. **[コンソール]** をクリックして VM のコンソールを開き、ゲスト オペレーティング システムにログオンします。(コンソールの使用方法については、 [「仮想マシン コンソールのセッションを開く」](#) を参照してください。)
5. ztC Edge システムで操作に不要なゲスト オペレーティング システムのサービスをすべて無効にします。
 - PM ソースからマイグレーションを行った場合、ハードウェアと直接やり取りを行うすべてのサービスを無効にします。例:

- Dell OpenManage (OMSA)
- HP Insight Manager
- Diskeeper
- VM ソースからマイグレーションを行った場合、他のハイパーバイザに関連付けられているすべてのサービスを無効にします。例:
 - VMware ツール
 - Hyper-V ツール
 - 仮想マシン用 Citrix ツール

これらのサービスを無効にした後、ゲスト オペレーティング システムを再起動して変更を実装します。

6. 必要に応じてゲスト オペレーティング システムのネットワーク構成の設定を更新し、再起動して設定を有効にします。

7. ゲスト オペレーティング システムに追加の Windows または Linux ベースのシステム設定を構成済みであることを確認します。次を参照してください。

- [「Windows ベースの仮想マシンを構成する」](#)
- [「Linux ベースの仮想マシンを構成する」](#)

新しい VM が正しく機能することを確認できたら、マイグレーション プロセスは完了します。ただしシステムは、高可用性 (HA) 運用を有効にするため、PM 間のデータの同期を続行することがあります。

Ubuntu VM のマイグレーションを完了するには

Ubuntu リリースを実行するベア メタル マシンから P2V を使って VM をマイグレーションした後、VM でアクティブ ネットワークがないなどの問題が発生する場合があります。問題を修正するには、Ubuntu VM をマイグレーションした後で、以下のうち適切な手順を実行してください。

Ubuntu 18.04 VM のマイグレーションの後で行う手順

1. ztC Edge コンソールから、VM のコンソール ウィンドウを開きます。
2. VM にログインしてターミナルに移動します。
3. 次のコマンドを入力します: `cd /etc/netplan`
4. 次のコマンドを入力します: `sudo vi 01-netcfg.yaml`
5. 01-netcfg.yaml ファイルで、eno1 を ens3f0 に変更します。

6. 次のコマンドを入力します: `sudo netplan apply`

7. 次のコマンドを入力します: `ifconfig`

これらのコマンドを実行した後は VM がその構成済み IP アドレスを使ってネットワーク上に存在するため、VM をリブートする必要はありません。

トラブルシューティング

必要に応じて以下の情報を参照し、マイグレーション プロセスで発生した問題を解決してください。

マイグレーション プロセスをキャンセルするには

P2V クライアントを実行しているソース PM または VM の電源をオフにします。

キャンセルしたマイグレーションや失敗したマイグレーションをクリーンアップするには

ztC Edge コンソールを開いてソース PM または VM に関連するマイグレーション済みボリュームをすべて削除します。マイグレーション プロセスを再開するには、ソース PM または VM で P2V クライアントをリブートします。

失敗したマイグレーションから復旧するには

マイグレーション プロセスが失敗した場合、ソース PM または VM で P2V クライアントにエラーメッセージが表示されます。また、ztC Edge システムにもメッセージが表示されることがあります。これらのメッセージに基づいて問題を特定します。

その後もマイグレーションが失敗する場合、可能であればサーバサイド デバッグを有効にします。マイグレーションの後、Stratus 認定サービス業者に送信する診断ファイルを作成します。詳細については、[「診断ファイルを作成する」](#)を参照してください。診断ファイルには、マイグレーション プロセスで生成されたサーバサイドのデバッグ メッセージが含まれています。

「Failed to mount '/dev/sda1: Operation not permitted ('/dev/sda1 をマウントできません。操作が許可されていません)」というエラー メッセージが表示されて失敗したマイグレーションから復旧するには

Windows ベースの PM または VM で次のエラー メッセージが表示されてマイグレーション プロセスが失敗する場合、"休止状態" または "高速スタートアップ" モードが有効になっている可能性があります。

```
Failed to mount '/dev/sda1': Operation not permitted
The NTFS partition is in an unsafe state. Please resume and
shutdown Windows fully (no hibernation or fast restarting), or
mount the volume read-only with the 'ro' mount option.
```

この問題を解決するには、ソース PM または VM で休止機能と高速スタートアップを無効にします。

1. ソース PM または VM のオペレーティング システムにログオンします。
2. **[Power Options (電源オプション)]** コントロール パネルを開いて **[Choose what the power buttons do (電源ボタンの動作の選択)]** をクリックします。
3. **[When I press the power button (電源ボタンを押したとき)]** の横で、(**[Hibernate (休止)]** や **[Sleep (スリープ)]** ではなく) **[Shutdown (シャットダウン)]** を選択します。
4. **[Shutdown Settings (シャットダウンの設定)]** の下で、**[Turn on fast startup (recommended) (高速スタートアップをオンにする (推奨))]** の横のチェック ボックスをオフにします。
5. **[Save changes (変更の保存)]** をクリックします。
6. **[Administrator Power Shell (管理者)]** を開いて次のコマンドを実行します。

```
> powercfg /h off
```
7. オペレーティング システムをシャットダウンしてマイグレーション プロセスを再開します。

新しくマイグレーションした Linux ベースの VM が「ブート中」の状態から戻らない場合に復旧するには

VM のネットワークがオフラインの場合、Linux ベースの VM が ztC Edge コンソールで**ブート中**の状態のままになることがあります。

マイグレーション プロセス中に P2V クライアントは各ネットワーク インタフェースに新しい MAC アドレスを設定して、元の VM との競合を回避しようとします。Linux ベースの一部のオペレーティング システムは新しい MAC アドレスを検出し、元のインタフェースを維持したまま、その新しいネットワーク インタフェースを自動的に作成します。ゲスト オペレーティング システムはブートしますが、ネットワーク設定を手動で構成するまではネットワークがオフラインのままになることがあります。

この問題を解決するには、VM コンソールを開き、ゲスト オペレーティング システムにログオンしてネットワーク スタートアップ スクリプトを更新します。各ネットワーク インタフェースにつき 1 つのエントリだけを残すようにし、各インタフェースが環境に適した一意の MAC アドレスと正しいネットワーク設定を使用していることを確認してください。

ztC Edge システムの VM で見つからないデータ ボリュームを復旧するには

インポートの完了後に ztC Edge システムの VM にデータ ボリュームが表示されない場合、次の手順に従ってこれらのボリュームを手作業で復元できます。

- VM をシャットダウンして**仮想マシンの再プロビジョニング** ウィザードを実行し、**[ボリューム]** ページで正しいボリュームを含めたことを確認します。
- Windows ベースの VM では**ディスク管理**を使用してデータ ボリュームをオンラインにします。
- Linux ベースの VM では `/etc/fstab` ファイルを編集して、ストレージ デバイスを (`/dev/vda ~ /dev/vdh`) の新しいデバイス名に更新します。たとえばインポートにボリュームが含まれなかった場合、デバイス名が一致しなくなることもあります。

ztC Edge システムの VM で見つからないネットワーク デバイスを復旧するには

インポートの完了後に ztC Edge システムの VM にネットワーク デバイスが表示されない場合、次の手順に従ってこれらのデバイスを手作業で復元できます。

- VM をシャットダウンして**仮想マシンの再プロビジョニング** ウィザードを実行し、**[ネットワーク]** ページで正しいネットワークを含めます。
- Linux ベースの VM の場合、ネットワーク スタートアップ スクリプトを再構成して、ネットワーク インタフェースに新しいデバイス名を反映させます。

新しいネットワーク ドライバを手動でインストールするには

PM や VM をマイグレーションした後、ネットワーク ドライバが正しくインストールされないことがあります (たとえば、**[デバイス マネージャー]** に警告 (⚠️) 付きのドライバが一覧される場合があります)。この問題が発生した場合は、ドライバを手動でインストールしてください。

1. VM コンソール ウィンドウで、ゲスト オペレーティング システムの **[デバイス マネージャー]** を開きます。
2. **[ネットワーク アダプタ]** を展開して **[Red Hat VirtIO Ethernet Adapter]** を右クリックします (ドライバが正しく機能していません)。

3. **[ドライバ ソフトウェアの更新]** を選択します。
4. ポップアップ ウィンドウで **[コンピュータを参照してドライバ ソフトウェアを検索する]** をクリックします。
5. **[コンピュータ上のデバイス ドライバの一覧から選択する]** をクリックします。
6. **[Red Hat VirtIO Ethernet Adapter]** を選択します。
7. **[次へ]** をクリックしてネットワーク ドライバをインストールします。

ドライバがインストールされたら、ztC Edge コンソールで VM の状態を確認します。状態が実行中 (✓) であればドライバが正しく機能しています。

関連トピック

[「仮想マシンを作成/マイグレーションする」](#)

[「Windows ベースの仮想マシンを構成する」](#)

[「Linux ベースの仮想マシンを構成する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

OVF または OVA ファイルをインポートする

VM をあるシステムから別のシステムに転送する必要がある場合や、作成したイメージを同じシステムに転送して戻すことにより元の VM を復元または複製する場合、システムから Open Virtualization Format (OVF) または Open Virtual Appliance (or Application) (OVA) ファイルをインポートします。(OVF または OVA ファイルを使用せずに物理マシン (PM) または仮想マシン (VM) をシステムにマイグレーションするには、[「物理マシンまたは仮想マシンをシステムにマイグレーションする」](#)を参照してください。)

VM は "インポート" または "リストア" することができます。VM をインポートすると、一意のハードウェア ID が設定された VM の新しいインスタンスが作成されます。VM をリストア (復元) する場合、同じハードウェア ID (SMBIOS UUID、システム シリアル番号、および VM イメージに指定されている場合は MAC アドレス) が設定された同一の VM が作成されます。これらの ID はゲスト オペレーティング システムやアプリケーションのソフトウェア ライセンスに必要となる場合があります。元の VM との競合を避けるため、VM のリストアはこれを ztC Edge システムに転送した後ソース システム上での使用を停止する場合のみに行ってください。

このトピックでは、OVF または OVA ファイルをローカル コンピュータ、USB デバイス、または NFS エクスポートや Windows 共有 (Samba など、CIFS 共有とも呼ばれます) などのリモート ファイル システムからインポートする方法を説明します。既存の VM を同じ システム上に復元して VM を上書きし、これを以前のバックアップ コピーから復元する場合は、[「OVF ファイルから仮想マシンを交換/復元する」](#)を参照してください。

注:

- VM のインポートは、正常な状態のイメージから VM を作成したりクローンする場合に行います。VM のインポート中、システムによって一意のハードウェア ID と MAC アドレスが割り当てられます。(正常な状態のイメージは、通常、複数回コピーするために作成されたテンプレートの VM です。)ソース VM との競合を避けるため、インポートウィザードは新しい VM にある各ネットワーク インタフェースに新しい MAC アドレスを自動的に割り当てますが、必要に応じて IP アドレスとホスト名を手動で更新しなければなりません。
- インポートできるのは、サポートされるゲスト オペレーティング システムおよびブート インタフェースを実行している VM のみです。詳細については、[「テスト済みのゲスト オペレーティング システム」](#)を参照してください。

VM をインポートする際、システムはブート インタフェースの設定 (BIOS または UEFI) を OVF あるいは OVA ファイルからインポートします。この設定は変更できません。



- VM を VMware ソースからインポートできるのは、ソースが VMware リリース 6.x を実行している場合のみです。

VMware VM をインポートする場合、VMware のコンソールから電源をオフにするのに加え、オペレーティング システムのシャットダウン コマンドを使って VM をシャットダウンする必要があります。VMware のコンソールだけを使って VM をシャットダウンすると、インポートは失敗します。

- VMware OVA ファイルから VM をインポートする場合、操作を行うのに十分なディスク容量がシステムにあることを確認してください。システムに必要なディスク容量は、「OVA ファイルのサイズ + 作成する VM ボリュームの合計サイズ + 圧縮 OVA ファイルの解凍と処理用に一時予約される 100 GB のディスク容量」の総計に等しくなります。たとえば、3 GB の OVA ファイルを、32 GB ボリュームを要する VM のためにインポートするには、最低限 $3\text{ GB} + 32\text{ GB} + 100\text{ GB} = 135\text{ GB}$ のストレージが必要です。

システム上の**空き**ディスク容量は、ztC Edge コンソールの **[システム]** ページの、**[ストレージ割り当て]** で確認できます。お使いのシステムで、VMware OVA ファイルをインポートするのに十分なディスク容量がない場合、ディスク容量を解放するか、代わりに VM をネットワーク経由で (OVF や OVA ファイルを使わずに) 直接マイグレー

ションすることができます。詳細については、「[物理マシンまたは仮想マシンをシステムにマイグレーションする](#)」を参照してください。

- VM を同じシステムにインポートし直して VM を複製する際、VM の名前を変更して、エクスポートまたはインポートの処理中にボリュームを複製する必要があります。VM の名前を変更しなかった場合、ソース VM との競合を避けるため、インポートウィザードによって新しい VM と新しいボリュームの名前が自動的に変更されます。ウィザードは VM 名とボリューム名に数字を追加して、VM に複製が追加されるたびにその数字を増やします (**MyVM**、**MyVM0**、**MyVM1** など)。
- OVA ファイルのインポートを開始した後にノードがメンテナンス モードに切り替わったり電源が切断された場合、OVA のインポートが失敗し、それ以降に試行されるすべての OVA ファイルのインポートも失敗します。この問題を解決する方法の詳細については、KB-[10034](#) を参照してください。
- VM のインポートにかかる時間はソース VM にあるボリュームのサイズと数、およびネットワーク帯域幅によって異なります。たとえば、20 GB のブート ボリュームが 1 つある VM を 1 Gb ネットワークで転送するには約 30 分かかります。
- インポートの処理中にシステムがプライマリ PM からセカンダリ PM に切り替わった場合、そのプロセスは失敗します。これはシステムの継続運用には影響しませんが、システムで不完全な VM とその関連ボリュームを削除してから、もう一度インポートを実行する必要があります。
- PM や VM をマイグレーションした後、ネットワークドライバが正しくインストールされないことがあります。この問題が発生した場合は、ドライバを手動でインストールしてください。詳細については、下記の「[トラブルシューティング](#)」を参照してください。
- Linux VMware OVA ファイルをインポートした後、ネットワーク情報を手動で構成する必要があります。「[Linux VMware OVA ファイルをインポートした後はネットワーク情報を手動で構成する](#)」を参照してください。



前提条件:

OVF ファイルから VM イメージをインポートする前に、ソース システム上で ztC Edge コンソールを使用して、サポートされるネットワーク共有または USB デバイス上の OVF および仮想ハード ディスク (VHD) ファイルに VM をエクスポート (「[仮想マシンをエクスポートする](#)」を参照) します。これらのファイルはお使いの管理 PC にコピーするか、ターゲットの ztC Edge システム上の USB デバイスまたはネットワーク共有にマウントします。手順については、「[ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする](#)」を参照してください。その後、ターゲット システム上の ztC Edge コンソールを使って OVF および VHD ファイルをインポートします。

OVA ファイルから VM イメージをインポートする前に、VMware システム上に OVA ファイルを作成します。ztC Edge システムは、1 つのメタデータ ファイルと 1 つ以上のディスク イメージ ファイルを含む VMware OVA ファイルをサポートしています。

OVF または OVA ファイルをインポートするには

1. ターゲット システム上で ztC Edge コンソールにログインします。
2. 2 つのノードで構成されているシステムの **[物理マシン]** ページ (「[\[物理マシン\] ページ](#)」を参照) で、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンス モードではなく、同期の実行中でもないことを確認します。
3. (ztC Edge コンソールを実行している PC ではなく) USB デバイスまたはネットワーク共有から VM をインポートしている場合、デバイスまたは共有を ztC Edge システム上にマウントします。手順については、「[ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする](#)」を参照してください。
4. **[仮想マシン]** ページ (「[\[仮想マシン\] ページ](#)」を参照) で、**[インポート/リストア]** をクリックして**仮想マシンのインポート/リストア** ウィザードを開きます。
5. 次のいずれかを選択します。
 - **PC からインポート** — ztC Edge コンソールを実行している PC から VM をインポートします。



注: PC からインポートする際には VMware OVF および OVA の参照がサポートされませんが、その他の方法を使用して VMware OVF および OVA をインポートすることができます。

[次へ]、[参照] の順にクリックして、ローカル コンピュータ上の適切なファイルを見つけます。

- **USB からインポート** — ztC Edge システム上にマウントされた USB デバイスから VM をインポートします。

[次へ] をクリックし、プルダウン メニューからパーティションを選択します。

[OVF/OVA のリスト] をクリックし、プルダウン メニューから適切なファイルを選択します。オプションとして、[ファイルの検索] ボックスにファイル名またはその一部を入力してファイルを検索できます。このボックスには、入力された名前に一致する、さまざまなディレクトリに保存されている OVA ファイルが一覧されます。

- 親 (ルート) ディレクトリが検索ディレクトリである場合、一覧されるファイルは、親 (ルート) ディレクトリに加えて、サブディレクトリにも保存されています。
- サブディレクトリが検索ディレクトリである場合、一覧されるファイルは、サブディレクトリに加えて、親 (ルート) ディレクトリにも保存されています。

- **リモートまたはネットワーク Windows 共有からインポート (CIFS/SMB)** — ローカル ネットワーク上の Windows 共有から VM をインポートします。VM のパスの最大長は、VM 名を含めて 4096 文字であることに注意してください。

[次へ] をクリックし、[ユーザ名] と [パスワード] に値を入力します。[レポジトリ] に、「¥¥<マシンの URL>¥¥<共有名>」の形式で値を入力します (例:

¥¥192.168.1.34¥¥MyOVFsForImport)。次に、[OVF/OVA のリスト] をクリックしてリストから適切なファイルを選択します。

- **リモートまたはネットワーク NFS からインポート** — ローカル ネットワーク上の NFS 共有から VM をインポートします。VM のパスの最大長は、VM 名を含めて 4096 文字であることに注意してください。

[次へ] をクリックし、[レポジトリ] に、リモート システムの URL を

「*nnn.nnn.nnn.nnn*/*<フォルダ名>*」の形式で入力します (*http://* や *https://* は含めません)。

[OVF/OVA のリスト] をクリックしてリモート フォルダにあるすべてのファイルのリストを表示します。インポートする適切なファイルを選択してください。オプションとして、[ファイルの検索] ボックスにファイル名またはその一部を入力してファイルを検索できます。あるいは、列の見出し (名前、変更日、サイズなど) をクリックしてファイルを並べ替

えることも可能です。ファイル名をクリックしてファイルを選択し、**[次へ]** をクリックします。

OVA ファイルを選択した場合、次のステップに進んでください (OVA ファイルで行えるのはインポートのみです)。

OVF ファイルを選択した場合、**[次へ]** をクリックします。これが ztC Edge で作成されたファイルかどうか、および VM のインポートとリストアを行えるかどうかを確認するメッセージが表示されます。ztC Edge で作成した OVF ファイルを選択する際は、オプションとして、ファイルをインポートまたはリストアすることができ、次のメッセージの表示も可能です。

VM を復元すると、全ネットワーク インタフェースのハードウェア ID と MAC アドレスの維持が試行されます。**[リストア]** は、VM の特定インスタンスを指定して復元する場合で、そのインスタンスがネットワーク上のすべてのシステムで実行されるこの VM の唯一のコピーである場合のみに選択してください。通常の場合、**リストア** は過去のバックアップから VM を復旧させるために使用します。正常な状態のイメージから VM を作成したりクローンする場合には、**インポート** を選択します。この操作では一意のハードウェア ID と MAC アドレスが割り当てられます。

6. **[インポート]** を選択します (必要な場合はウィンドウを下にスクロールしてください)。 (ztC Edge で作成された OVF の場合、**[リストア]** を選択することもできます。詳細については、[「OVF ファイルから仮想マシンを交換/復元する」](#) を参照してください。)
7. ウィザードの **[仮想マシンのインポートの準備]** ウィンドウが開き、必要に応じて追加のファイルをアップロードするプロンプトが表示されます。プロンプトが表示されたら、VM に関連付けられている各ボリュームについて含める適切なファイルを選択します。
8. OVF ファイルを選択した場合、情報を確認し、必要な場合は編集することができます (必要に応じてウィンドウを下にスクロールしてください):

■ 名前、ブート インタフェース、CPU、メモリ

VM の名前、ブート インタフェース、vCPU の数、または VM が利用できる合計メモリが表示されます。必要に応じて情報を編集します。(ブート インタフェースは変更できません。この設定はシステムによって OVF または OVA ファイルからインポートされます。)

■ ストレージ

各ボリュームの名前およびサイズが表示されます。**[作成]** 列で、システム上のボリューム用にストレージを割り当てるには、ボリュームのボックスを選択します (ブート ボリューム

ムは必須です)。[データの復元] 列で、VHD ファイルからボリュームのデータをインポートする場合はボックスを選択します。

■ ネットワーク

利用可能なネットワークが表示されます。既存のネットワークを削除したり、まだ割り当てられていない新しいネットワークを追加することも可能です。選択した各ネットワークに 1 つの静的な IP アドレスを指定することもできます。少なくとも 1 つのネットワークが必要です。

ネットワークの総数は、ztC Edge システム上のビジネス ネットワークの数を超えることができません。VM を OVF ファイルからインポートする場合、ウィザードでどのネットワークを削除するかを選択できます。VM を OVA ファイルからインポートする場合、システムはインポートの処理中に余分なネットワークを自動的に無視します。どちらの場合も、VM をインポートする前や後に追加のビジネス ネットワークを ztC Edge システムに接続して、ネットワーク接続を復元することができます。

9. 初めて起動する前に VM の再プロビジョニングが必要な場合、オプションで **[インポート後に仮想マシンを自動的に起動]** チェック ボックスをオフにすることもできます。
10. **[インポート]** をクリックして、VM のインポートを開始します。オプションとして、**[キャンセル]** をクリックして手順をキャンセルできます。

ウィザードに進捗状況が表示されます。転送が完了したら **[完了]** をクリックしてウィザードを閉じます。



注: インポートの処理中、ztC Edge コンソールの **[ボリューム]** ページにインポートされたボリュームが順次表示されます。インポート ウィンドウに処理が完了したことが示されるまで、インポートされたボリュームを接続したり削除しないでください。そうでない場合、インポートは失敗します。

11. 該当する場合は**仮想マシンの再プロビジョニング** ウィザードを使用して VM に追加のリソースを割り当てます。「[仮想マシンのリソースを再プロビジョニングする](#)」を参照してください。
VM の再プロビジョニングが完了したら、**[起動]** をクリックして VM をブートします。
12. **[コンソール]** をクリックして VM のコンソールを開き、ゲスト オペレーティング システムにログインします。

13. Windows ベースの VM の場合のみ、VirtIO ドライバをダウンロードして、サポートされる最新のバージョンに更新します。手順については、「[VirtIO ドライバを更新する \(Windows ベースの VM\)](#)」を参照してください。(Linux ベースの VM には既に正しい VirtIO ドライバがインストールされています。)



注: ドライバを更新した後、ゲスト オペレーティング システムの再起動が必要となる場合があります。

14. 必要に応じてゲスト オペレーティング システムのネットワーク設定を更新します。

新しい VM が正しく機能することを確認できたら、インポートプロセスは完了します。ただしシステムは、高可用性 (HA) またはフォールトトレラント (FT) 運用を有効にするため、PM 間のデータの同期を続行することがあります。



注: データが同期されて VirtIO ドライバが稼動するまでの間、新しい VM とその関連ボリュームに警告マークが表示される場合があります。

トラブルシューティング

エクスポートプロセスやインポートプロセスで発生した問題を解決するには、必要に応じて以下の情報を参照してください。

インポートをキャンセルしたり、インポートが失敗した後でクリーンアップするには

ターゲットシステム上の ztC Edge コンソールで、インポートした VM およびそれに関連するすべてのボリューム (存在する場合) を削除します。

ターゲット VM で見つからないデータ ボリュームを復旧するには

インポートの完了後にターゲットシステムの VM にデータ ボリュームが表示されない場合、次の手順でこれらのボリュームを手作業で復元できます。

- VM をシャットダウンして**仮想マシンの再プロビジョニング**ウィザードを実行し、**[ボリューム]** ページで正しいボリュームを含めたことを確認します。
- Windows ベースの VM では**ディスク管理**を使用してデータ ボリュームをオンラインにします。
- Linux ベースの VM の場合、`/etc/fstab` ファイルを編集して、ストレージデバイスに新しいデバイス名を反映させます。インポートにボリュームを含めなかった場合には、デバイス名が一致しなくなることがあります。

ztC Edge システムの VM で見つからないネットワーク デバイスを復旧するには

インポートの完了後にターゲット システムの VM にネットワーク デバイスが表示されない場合、次の手順でこれらのデバイスを手作業で復元できます。

- VM をシャットダウンして**仮想マシンの再プロビジョニング** ウィザードを実行し、**[ネットワーク]** ページで正しいネットワークを含めます。VM がウィザードに表示される数よりも多くのネットワークを必要とする場合、追加のビジネス ネットワークを ztC Edge システムに接続してから、VM を再プロビジョニングして新しいネットワークを含めてください。
- Linux ベースの VM の場合、ネットワーク スタートアップ スクリプトを再構成して、ネットワーク インタフェースに新しいデバイス名を反映させます。

新しいネットワーク ドライバを手動でインストールするには

PM や VM をインポートした後、ネットワーク ドライバが正しくインストールされないことがあります (たとえば、**[デバイス マネージャー]** に警告 (⚠) 付きのドライバが一覧される場合があります)。この問題が発生した場合は、ドライバを手動でインストールしてください。

1. VM コンソール ウィンドウで、ゲスト オペレーティング システムの **[デバイス マネージャー]** を開きます。
2. **[ネットワーク アダプタ]** を展開して **[Red Hat VirtIO Ethernet Adapter]** を右クリックします (ドライバが正しく機能していません)。
3. **[ドライバ ソフトウェアの更新]** を選択します。
4. ポップアップ ウィンドウで **[コンピュータを参照してドライバ ソフトウェアを検索する]** をクリックします。
5. **[コンピュータ上のデバイス ドライバの一覧から選択する]** をクリックします。
6. **[Red Hat VirtIO Ethernet Adapter]** を選択します。
7. **[次へ]** をクリックしてネットワーク ドライバをインストールします。

ドライバがインストールされたら、ztC Edge コンソールで VM の状態を確認します。状態が**実行中** (✅) であればドライバが正しく機能しています。

Linux VMware OVA ファイルをインポートした後はネットワーク情報を手動で構成する

Linux VMware OVA ファイルをインポートすると、ネットワーク インタフェースおよび `networks-scripts` ファイルが変更されます。ファイルをインポートした後、以下の手順を使ってネットワーク情報を手動で構成する必要があります。

1. **[仮想マシン]** ページで、VM を選択します。
2. 下部パネルの **[コンソール]** をクリックして VM のログイン ページを開きます (詳細については、「[仮想マシン コンソールのセッションを開く](#)」を参照してください)。
3. VM にログインします。
4. コマンド プロンプト ウィンドウを開きます。
5. `ifconfig` コマンドを実行します。コマンドの出力で、`ip address` が仮想ネットワーク インタフェース `eth0` に割り当てられているかどうか確認します。
6. `ip address` が `eth0` に割り当てられていない場合、`/etc/sysconfig/network-scripts` ディレクトリの内容をリスト表示します。
7. `ifcfg-xxxx` (ただし `ifcfg-lo` を除く) の値を書き留めます。
8. `ifcfg-xxxx` の名前を `ifcfg-eth0` に変更します。
9. `ifcfg-eth0` ファイルを編集し、`DEVICE` と `ONBOOT` の値を次のように変更します。

```
DEVICE=eth0
```

```
ONBOOT=yes
```

ファイルを保存します。

10. 次のコマンドを実行してネットワーク サービスを再起動します。

```
systemctl restart network
```

11. `ifconfig` コマンドを使用して IP の割り当てを確認します。コマンドの出力で、`ip address` が `eth0` に割り当てられていることを確認します。

関連トピック

[「ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「Windows ベースの仮想マシンを構成する」](#)

[「Linux ベースの仮想マシンを構成する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

OVF ファイルから仮想マシンを交換/復元する

ztC Edge で作成した Open Virtualization Format (OVF) ファイルから仮想マシン (VM) を交換して、VM を以前のバックアップ コピーで上書きすることにより ztC Edge システム上の VM を復元 (つまり復旧) します。(VM を別のシステムからインポートする場合は、[「仮想マシンを作成/マイグレーションする」](#)を参照してください。)

通常の場合、VM をインポートすると、一意のハードウェア ID が設定された VM の新しいインスタンスが作成されます。VM をリストア (復元) する場合、SMBIOS UUID、システム シリアル番号、および VM イメージに指定されている場合は MAC アドレスがそれぞれ同じ値に設定された、同一の VM が作成されます。この情報は、ゲスト オペレーティング システムやアプリケーションのソフトウェア ライセンスに必要となる場合があります。ただし、復元された VM のハードウェア ID は一意です。ztC Edge システム上に同一の VM が既に存在する場合、VM を復元することで VM を置換して前のコピーで上書きできます。

ztC Edge システム上の既存の VM を復元できるのは、既に VM を ztC Edge システム ([「仮想マシンをエクスポートする」](#)を参照) から、サポートされるネットワーク共有または USB デバイス上の OVF および仮想ハード ディスク (VHD) ファイルにエクスポートしてある場合のみです。これらのファイルはお使いの管理 PC にコピーするか、ターゲットの ztC Edge システム上の USB デバイスまたはネットワーク共有にマウントします。手順については、[「ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」](#)を参照してください。その後、ターゲット ztC Edge システム上の ztC Edge コンソールを使って管理 PC から OVF および VHD ファイルを復元します。



注意事項: 上書きと復元を行う前に、ztC Edge システム上の既存の VM をバックアップすることを検討してください。VM をエクスポートしてバックアップを作成する場合、復元対象の OVF および VHD ファイルを上書きしないよう注意してください。

注:

- VM を復元できるのは、ztC Edge システムで作成された OVF からだけです。サードパーティ システムで作成された OVF から VM を復元することはできません。OVA ファイルから VM を復元することもできません。
- 通常、リストアは過去のバックアップから VM を復旧させるために使用します。VM を復元すると、システムは全ネットワーク インタフェースのハードウェア ID と MAC アドレスを維持しようとします。
- VM のリストアは、ztC Edge VM の特定インスタンスを指定して復元するために行い、復元された VM が、ネットワーク内のすべての ztC Edge サーバで実行されるこの VM の唯一のコピーになる場合のみに実行します。
- VM の復元にかかる時間はソース VM にあるボリュームのサイズと数、およびネットワーク帯域幅によって異なります。たとえば、20 GB のブート ボリュームが 1 つある VM を 1 Gb ネットワークで転送するには約 30 分かかります。
- 既存の VM を上書きして復元すると、ztC Edge システムによって既存の VM とそのボリュームが削除されます。
- VM の復元処理中に ztC Edge システムがプライマリ PM からセカンダリ PM に切り替わった場合、その復元プロセスは失敗します。これはシステムの継続運用には影響しませんが、ztC Edge システムで不完全な VM とその関連ボリュームを削除してから、もう一度復元を実行する必要があります。

前提条件:

- ztC Edge システムから VM イメージを交換 (つまり復元) する前に、ソース ztC Edge システム上で ztC Edge コンソールを使用して、サポートされるネットワーク共有または USB デバイス上の OVF および仮想ハード ディスク (VHD) ファイルに、VM をエクスポート (「[仮想マシンをエクスポートする](#)」を参照) します。これらのファイルはお使いの管理 PC にコピーするか、ターゲットの ztC Edge システム上の USB デバイスまたはネットワーク共有にマウントします。手順については、「[ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする](#)」を参照してください。その後、ターゲット ztC Edge システム上の ztC Edge コンソールを使って OVF および VHD ファイルを復元します。
- 復元プロセスが正しく機能するためには、ztC Edge システムの両方の PM がオンラインになっている必要があります。

VM を復元するには

1. ターゲット ztC Edge システム上で ztC Edge コンソールにログインします。
2. 2 つのノードで構成されているシステムの **[物理マシン]** ページ (「[\[物理マシン\] ページ](#)」を参照) で、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンス モードではなく、同期の実行中でもないことを確認します。
3. (ztC Edge コンソールを実行している PC ではなく) USB デバイスまたはネットワーク共有から VM を復元している場合、デバイスまたは共有を ztC Edge システム上にマウントします。手順については、「[ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする](#)」を参照してください。
4. **[仮想マシン]** ページ (「[\[仮想マシン\] ページ](#)」を参照) で、上部パネルから復元する VM を選択します。
5. 下部パネルで、**[リストア]** をクリックするか、**[インポート/リストア]** をクリックします (上部パネルの近く)。
6. 次のいずれかを選択します。
 - **PC からインポート** — ztC Edge コンソールを実行している PC から VM をインポートします。
 - a. **[次へ]** をクリックします。
 - b. **[参照]** をクリックしてローカル コンピュータ上の適切なフォルダを見つけます。

c. 目的のファイルの名前をクリックします。

d. **[開く]** をクリックします。

- **USB からインポート** — ztC Edge システム上にマウントされた USB デバイスから VM をインポートします。

[次へ] をクリックし、プルダウン メニューからパーティションを選択します。

[OVF/OVA のリスト] をクリックし、プルダウン メニューから適切なファイルを選択します。オプションとして、**[ファイルの検索]** ボックスにファイル名またはその一部を入力してファイルを検索できます。このボックスには、入力された名前に一致する、さまざまなディレクトリに保存されている OVA ファイルが一覧されます。

- 親 (ルート) ディレクトリが検索ディレクトリである場合、一覧されるファイルは、親 (ルート) ディレクトリに加えて、サブディレクトリにも保存されています。
- サブディレクトリが検索ディレクトリである場合、一覧されるファイルは、サブディレクトリに加えて、親 (ルート) ディレクトリにも保存されています。

- **リモートまたはネットワーク Windows 共有からインポート (CIFS/SMB)** — ローカルネットワーク上の Windows 共有から VM をインポートします。

[次へ] をクリックし、**[ユーザ名]** と **[パスワード]** に値を入力します。**[レポジトリ]** に、「**¥¥<マシンの URL>¥¥<共有名>**」の形式で値を入力します (例:

¥¥192.168.1.34¥¥MyOVFsForImport)。次に、**[OVF/OVA のリスト]** をクリックしてリストから適切な OVF ファイルを選択します。

- **リモートまたはネットワーク NFS からインポート** — ローカルネットワーク上の NFS 共有から VM をインポートします。

[次へ] をクリックし、**[レポジトリ]** に、リモートシステムの URL を

「**nnn.nnn.nnn.nnn/<フォルダ名>**」の形式で入力します (**http://** や **https://** は含めません)。

[OVF/OVA のリスト] をクリックしてリモートフォルダにあるすべてのファイルのリストを表示します。適切な OVF ファイルを選択します。オプションとして、**[ファイルの検索]** ボックスにファイル名またはその一部を入力してファイルを検索できます。あるいは、列の見出し (名前、変更日、サイズなど) をクリックしてファイルを並べ替えることも可能です。ファイル名をクリックしてファイルを選択し、**[次へ]** をクリックします。

7. **[リストア]** を選択します。(必要な場合はウィンドウを下にスクロールしてください。)**[リストア]** によって既存のデータと構成の詳細がすべて上書きされるために注意を促す警告メッセージが表示されます。
8. **[続行]** をクリックします。
9. プロンプトが表示されたら、VHD ファイルを追加します。
10. 次の情報を確認し、必要に応じて編集します。

- **名前、ブート インタフェース、CPU、メモリ**

VM の名前、ブート インタフェース、vCPU の数、または VM が利用できる合計メモリが表示されます。必要に応じて情報を編集します。(ブート インタフェースは変更できません。この設定はシステムによって OVF ファイルからインポートされます。)

- **ストレージ**

各ボリュームの名前およびサイズが表示されます。**[作成]** 列で、ztC Edge システム上のボリューム用にストレージを割り当てるには、ボリュームのボックスを選択します (ブート ボリュームは必須です)。**[データの復元]** 列で、VHD ファイルからボリュームのデータをインポートする場合はボックスを選択します。

- **ネットワーク**

利用可能なすべてのネットワークが表示されます。既存のネットワークを削除したり、まだ割り当てられていない新しいネットワークを追加することも可能です。少なくとも 1 つのネットワークが必要です。

ネットワークの総数は、ztC Edge システム上のビジネス ネットワークの数を超えることができません。ウィザードで、削除するネットワークを選択したり、VM やネットワーク接続を復元する前や後に追加のビジネス ネットワークを ztC Edge システムに接続して、ネットワーク接続を復元することができます。

11. システムで最初に起動する前に VM の再プロビジョニングが必要な場合、オプションで **[復元後に仮想マシンを自動的に起動]** チェック ボックスをオフにすることもできます。
12. **[リストア]** をクリックして、VM のリストアを開始します。転送が完了したら **[完了]** をクリックしてウィザードを閉じます。



注: 復元の処理中、ztC Edge コンソールの **[ボリューム]** ページに復元されたボリュームが順次表示されます。リストア ウィンドウに処理が完了したことが示されるまで、復元したボリュームを接続したり削除しないでください。これを行うと、復元操作が失敗します。

13. 該当する場合は**仮想マシンの再プロビジョニング** ウィザードを使用して VM に追加のリソースを割り当てます。「[仮想マシンのリソースを再プロビジョニングする](#)」を参照してください。

VM の再プロビジョニングが完了したら、**[起動]** をクリックして VM をブートします。

復元した VM が正しく機能することを確認したら、復元プロセスが完了します。ただし ztC Edge システムは、高可用性 (HA) またはフォールト トレラント (FT) 運用を有効にするため、PM 間のデータの同期を続行することがあります。



注: データが同期されて VirtIO ドライバが稼動するまでの間、復元した VM とその関連ボリュームに警告マークが表示される場合があります。

トラブルシューティング

復元プロセスで発生した問題を解決するには、必要に応じて以下の情報を参照してください。

復元操作をキャンセルしたり、復元が失敗した後でクリーンアップするには

ターゲット システム上の ztC Edge コンソールで、復元した VM およびそれに関連するすべてのボリューム (存在する場合) を削除します。

関連トピック

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンをエクスポートする

システムから仮想マシン (VM) をエクスポートして、ネットワークにマウントされたフォルダ (つまりディレクトリ) または USB デバイスに VM のイメージを保存します。ztC Edge システムから VM をエクスポートすると、VM イメージを別のシステムにインポートしたり、同じ ztC Edge システムへインポートし直して元の VM の復元や複製を行えるようになります。エクスポートした VM は元の VM のバックアップとして機能します。このトピックで説明されている手順で ztC Edge システムから VM を直接エクスポートできます。



注: 1つのノードで構成されているシステム上の VM の場合、VM をバックアップとしてエクスポートすることは特に重要です。元の VM の故障や損失が発生した場合、エクスポートした VM を使って、失われた VM を復元することができます。

VM のエクスポートを準備するには、エクスポートした VM を環境内に保存するための USB デバイスを挿入するか、ネットワーク マウントされたフォルダを作成します。USB デバイスを使用する場合、システムの現在のプライマリ ノード (**[物理マシン]** ページに **noden (プライマリ)** として表示されます) にデバイスを挿入します。フォルダを使用している場合、Windows 共有またはネットワーク ファイル システム (NFS) エクスポート用にフォルダを作成します。Windows 共有は Common Internet File System (CIFS) 共有とも呼ばれます (たとえば Samba など)。次に、フォルダまたは USB デバイスを、このトピックの説明に従って ztC Edge システムのホスト オペレーティング システムにマウントします。ztC Edge コンソールでエクスポートを開始すると、ztC Edge システムによって VM が標準の Open Virtualization Format (OVF) および仮想ハード ディスク (VHD) ファイルとして保存されます。

注:



- ソース VM をエクスポートするにはこれをシャットダウンする必要があるので、このプロセスのために計画的なメンテナンス期間を設けることを検討してください。
- エクスポートにかかる時間はソース VM にあるボリュームのサイズと数、およびネットワーク帯域幅によって異なります。たとえば、20 GB のブート ディスクが 1 つある VM を 1 Gb ネットワークで転送するには約 30 分かかります。
- エクスポートした後で VM を引き続き使用する場合には、ターゲットシステムへのインポート時に必ず別の MAC アドレスおよび IP アドレスを設定してください。
- エクスポートの処理中に ztC Edge システムがプライマリ PM からセカンダリ PM に切り替わった場合、そのプロセスは失敗します。この操作はシステムの継続運用に影響することはありません。ネットワークマウントされたフォルダから部分的にエクスポートされたファイルを削除して、もう一度ファイルをエクスポートすることができます。
- エクスポートできる vfat ファイルの最大サイズは 4 GB です。4 GB を超えるサイズの vfat ファイルをエクスポートしようとすると、操作が失敗します。
- Linux ベースの VM では、VM を別のシステムにエクスポートするときに `/etc/fstab` ファイルを変更する必要はありません。
- 古いリリースの Ubuntu を実行している Ubuntu ベースの VM では、必要に応じて VM をエクスポートする前に `/boot/grub/grub.cfg` ファイルを編集して `gfxmode` パラメータを `text` に変更する必要があります (たとえば `set gfxmode=text`)。これを行わないと、新しい VM のコンソールが別のシステムでハングすることがあります。マイグレーションの後、ソース VM で元の設定を復元できます。

前提条件:

- エクスポートを実行する前に VM をシャットダウンする必要があります。
- エクスポートの保存先を準備します。
 - USB デバイスを使用する場合、システムの現在のプライマリ ノード (**[物理マシン]** ページに **noden (プライマリ)** として表示されます) にデバイスを挿入します。システムに USB デバイスが表示されることを確認します。**[物理マシン]** ページに移動します。デバイスを挿入したノードをクリックして、下部パネルで **[USB デバイス]** タブを選択します。挿入した USB デバイスがタブに表示されることを確認します。
 - Windows/CIFS 共有または NFS エクスポート用のネットワークマウント フォルダを使用している場合、環境内のエクスポートされた VM を保存できる場所にそのフォルダを作成します。ファイルの転送が許可されるよう、ネットワークマウント フォルダの完全な読み書き権限を設定するか、Windows/CIFS 共有の場合は、その共有をホストするシステム/ドメインの特定のユーザに読み書きのアクセス許可を割り当てます。NFS エクスポートや CIFS 共有の URL またはパス名、および CIFS 共有のユーザ名とパスワードを記録します。これは VM をエクスポートするときに使用します。

エクスポートする VM を保存するのに十分なストレージがあることを確認します。


また、Windows ベースの VM には Windows 固有の準備を行う必要があります。

VM のエクスポート準備をするには (Windows ベースの VM)

1. ztC Edge コンソールを使用して ztC Edge システムにログインします。
2. **[仮想マシン]** ページで、エクスポートする VM を選択します。
3. **[コンソール]** をクリックして VM のコンソールを開き、Windows ゲスト オペレーティング システムにログインします。
4. **「Windows ドライブのラベルを管理する」** を参照して、すべてのボリュームのラベルが正しいことを確認します。
5. Windows システム準備ツール (Sysprep) を実行してゲスト オペレーティング システムを再展開用に準備します。

VM をエクスポートするには

1. ztC Edge コンソールを使用して ztC Edge システムにログインします。
2. **[仮想マシン]** ページで、エクスポートする VM を選択して **[シャットダウン]** をクリックします。VM がシャットダウンするのを待ちます。[「\[仮想マシン\] ページ」](#) を参照してください。
3. VM を選択した状態で、**[エクスポート]** をクリックしてエクスポートウィザードを開きます。
4. 次のいずれかを選択します。

 **注:** **[マウント]** ボタンを使ってロケーションを既にマウントしてある場合 (「ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」を参照)、エクスポートウィザードに、マウントされているデバイスの URL が緑で表示されます。これを変更するには、**[変更]** ボタンをクリックします。

■ **Windows 共有経由でデバイスをマウント (CIFS/SMB)**

エクスポートの保存先は CIFS 共有上のフォルダ内です。**[ユーザ名]**、**[パスワード]**、および **[レポジトリ]** に値を入力します。**[レポジトリ]** に、「**¥¥<マシンの URL>¥¥<共有名>**」の形式で値を入力します (例:
¥¥192.168.1.34¥¥MyExportVMs)。

■ **NFS 経由でデバイスをマウント**

エクスポートの保存先は NFS 経由でアクセスするリモートシステム上のフォルダ内です。**[レポジトリ]** の値はリモートシステムの URL で、「**nnn.nnn.nnn.nnn**」の形式で入力します (**http://** や **https://** は含めません)。

■ **USB をマウント**

[USB パーティション リスト] で、プルダウン メニューからパーティションを選択します。

5. **[エクスポート パス: /mnt/ft-export:]** で、VM をエクスポートしてその OVF および VHD ファイルを保存する場所のパスを入力します。たとえば、VM を ocean1 という新しいフォルダにエクスポートするには、ocean1 と入力します。
6. **[マウント]** をクリックします。

マウントに成功した場合、[デバイス URL] の下にレポジトリが表示されて [VM のエクスポート] ボタンがアクティブになります。そうでない場合はアラートが表示されます。

7. [エクスポートするブート ボリューム] および [エクスポートするデータ ボリューム] の下で、含めるボリュームを選択します。(ブート ボリュームは必須です。)

8. [VM のエクスポート] をクリックして VM をエクスポートします。

エクスポートする VM の [サマリ] タブの [エクスポート ステータス] で、エクスポート状況を監視できます。進捗状況はエクスポート全体および各ボリュームにおける比率 (%) で報告されます。プロセスが完了すると、[エクスポートを正しく完了しました] というステータスに変わります。

エクスポートをキャンセルするには、[エクスポート進捗状況] のパーセント値の横の [キャンセル] をクリックします。ダイアログ ボックスが開き、キャンセルを確認するよう求められます。キャンセルするには [はい] をクリックします。

ztC Edge システムは、まず VHD ファイル (ボリューム) をエクスポートしてから、OVF ファイルをエクスポートします。フォルダに OVF ファイルが表示された段階でプロセスの完了を確認できます。

エクスポートプロセスの後に ztC Edge システム上の OVF ファイルや VHD ファイルをインポートしたり復元するには、[「OVF または OVA ファイルをインポートする」](#)を参照してください。

デバイスをアンマウントするには、[「ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする」](#)を参照してください。

トラブルシューティング

エクスポートプロセスで発生した問題を解決するには、必要に応じて以下の情報を参照してください。

ztC Edge システムからのエクスポートをキャンセルしたり、エクスポートが失敗した後でクリーンアップするには

エクスポート フォルダから VM ファイルを削除するか、その後で行うエクスポート用に新しいフォルダを作成します。

関連トピック

[「仮想マシンに USB デバイスを接続する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

ztC Edge システム上の USB デバイスまたはネットワークマウント フォルダをマウントする

ztC Edge システム上の USB デバイスまたはネットワーク マウント フォルダ (つまりディレクトリ) をマウントおよびアンマウントするには、**[マウント]** (または **[アンマウント]**) ボタンを使用します。これは **[仮想マシン]** ページにあります。ロケーションをマウントすると、プライマリ ノードのマウント ポイント `/mnt/ft-export/` で利用可能になります。その後、プライマリ ノード上の VM を、マウントした場所にエクスポートしたり、マウントした場所から VM を ztC Edge システムインポートすることができます。エクスポートまたはインポートが完了したら、**[アンマウント]** ボタンを使ってそのロケーションをアンマウントします。

(VM のゲスト オペレーティング システムでデバイスにアクセスするために USB デバイスをマウントする必要がある場合、[「仮想マシンに USB デバイスを接続する」](#) を参照してください。)

注:



1. 使用中のロケーションをアンマウントしたりマウントすることはできません。たとえば、VM のエクスポートやインポートの処理中にロケーションをアンマウントすることはできません。
2. ztC Edge システム上の Stratus Redundant Linux ソフトウェアは、exFAT ファイル システムをサポートしていません。USB メディアをマウントする前に、デバイスを NTFS で書式設定します。(デフォルトではほとんどの USB メディアが FAT ファイル システム用に書式設定されていますが、ファイル サイズが 4 GB に制限されるため大半の VM では不十分です。)

前提条件: マウント ロケーションを準備します。



- USB デバイスを使用して VM のエクスポートやインポートを行っている場合、デバイスをシステムの現在のプライマリ ノードに接続します (これは **[物理マシン]** ページに **noden (プライマリ)** として表示されます)。システムに USB デバイスが表示されることを確認します。**[物理マシン]** ページに移動してデバイスを接続したノードをクリックし、下部のパネルで **[USB デバイス]** タブを選択します。接続した USB デバイスがタブに表示されることを確認します。
- Windows/CIFS 共有または NFS エクスポート用のネットワークマウント フォルダを使用している場合、環境内のエクスポートされた VM を保存できる場所にそのフォルダを作成します。ファイルの転送が許可されるよう、ネットワークマウント フォルダの完全な読み書き権限を設定するか、Windows/CIFS 共有の場合は、その共有をホストするシステム/ドメインの特定のユーザに読み書きのアクセス許可を割り当てます。NFS エクスポートや CIFS 共有の URL またはパス名、および CIFS 共有のユーザ名とパスワードを記録します。これは CIFS 共有の NFS エクスポートをマウントするときに使用します。

USB デバイスまたはネットワークマウント フォルダをマウントするには

1. **[仮想マシン]** ページで、VM を選択します。
2. 下部パネルで **[マウント]** ボタンをクリックします。
3. マウント ポイント **/mnt/ft-export/** に次のいずれかを選択します

- **Windows 共有経由でデバイスをマウント (CIFS/SMB)**

マウントする場所は CIFS 共有上のフォルダ内です。**[ユーザ名]**、**[パスワード]**、および **[レポジトリ]** に値を入力します。**[レポジトリ]** に、「**¥¥<マシンの URL>¥<共有名>**」の形式で値を入力します (例: **¥¥192.168.1.34¥MyMountLocation**)。

- **NFS 経由でデバイスをマウント**

マウントする場所は NFS 経由でアクセスするリモートシステム上のフォルダ内です。**[レポジトリ]** に、リモートシステムの URL を「**nnn.nnn.nnn.nnn**」の形式で入力します (**http://** や **https://** は含めません)。

- **USB をマウント**

[USB パーティション リスト] で、プルダウン メニューからパーティションを選択しま

す。

4. **[マウント]** をクリックします。

ロケーションがプライマリ ノードにマウントされ、**[マウント]** ボタンが **[アンマウント]** に変わります。

USB デバイスまたはネットワークマウント フォルダをアンマウントするには

1. **[仮想マシン]** ページで、VM を選択します。
2. 下部パネルで **[アンマウント]** ボタンをクリックします。
3. **[確認]** ダイアログ ボックスが開き、ロケーションのアンマウントを確認するメッセージが表示されます。アンマウントするには **[はい]** をクリックします。

ロケーションがアンマウントされ、**[アンマウント]** ボタンが **[マウント]** に変わります。

関連トピック

[「仮想マシンをエクスポートする」](#)

[「仮想マシンを管理する」](#)

Windows ドライブのラベルを管理する

Windows ベースの仮想マシンにあるボリュームにラベルを付けて、仮想マシンをエクスポートする前に、仮想マシンが正しくマッピングされていることを確認します。



注意事項: (エクスポートまたはスナップショットの準備のため) を実行する前に、各ボリュームに識別可能な一意のラベルが付いていることを確認します。この手順を実行するには管理者の権限が必要です。

コマンド プロンプトからラベルを設定するには、次を入力します。

```
C:\>label C:c-drive
```

すべてのボリューム ラベルを一覧して確認するには、**diskpart** ユーティリティを使用します。

```
C:\> diskpart
```

```
DISKPART> list volume
```

```
...
```

```
DISKPART> exit
```

仮想マシンをインポートした後、**ディスク マネージャー**を使ってドライブ名を割り当て直します。エクスポートを実行する前にラベルを付けることで、ドライブの識別が容易になります。Windows システムにおけるドライブ文字の再割り当て手順については、Microsoft サポート Web サイトを検索してください。

関連トピック

[「仮想マシンを作成/マイグレーションする」](#)

[「Windows ベースの仮想マシンを構成する」](#)

Windows ベースの仮想マシンを構成する

Windows ベースの仮想マシンをインストールした後、以下を参照して稼動時に必要となる追加のリソースとソフトウェアを構成します。

- [「VirtIO ドライバを更新する \(Windows ベースの VM\)」](#)
- [「ディスクを作成して初期化する \(Windows ベースの VM\)」](#)
- [「アプリケーションをインストールする \(Windows ベースの VM\)」](#)

また、以下の設定も構成する必要があります。

- ゲスト オペレーティング システムのタイム ゾーンを、ztC Edge コンソールの **[日付と時刻]** の基本設定ページに構成されているタイムゾーンに対応するよう変更します ([「日付と時刻を構成する」](#)を参照)。これを行わないと、VM の再起動やマイグレーションを実行するたびに VM のタイムゾーンが変更されます。VM と ztC Edge システムの両方で、ネットワーク タイム プロトコル (NTP) を使用することを推奨します。
- ゲスト オペレーティング システムが省エネルギー状態になるのを防ぐため、休止機能を無効にします (これはデフォルトで有効になっている場合があります)。
- ゲスト オペレーティング システムの電源ボタンのアクションを、ゲストを "休止" する代わりに "シャットダウン" するように構成して、ztC Edge コンソールの VM の **[シャットダウン]** ボタンが正しく機能するようにします ([「仮想マシンをシャットダウンする」](#)を参照してください)。
- システムがクラッシュしたときにクラッシュ ダンプ ファイルが生成されるようにゲスト オペレーティング システムを構成します。Microsoft の記事「[How to generate a complete crash dump file or a kernel crash dump file by using an NMI on a Windows-based system \(Windows ベースのシステムで NMI を使用して、完全クラッシュ ダンプ ファイルまたはカーネル クラッシュ ダンプ ファイルを生成する方法\)](#)」(記事 ID: 927069) の指示に従います。「**More Information (詳細)**」セクションの手順を実行します。

適切なモニタリングのライセンスが適用されたシステムで Windows ベースの VM をモニタリングする場合の詳細については、[「Windows ベースの仮想マシンをモニタリングする」](#)を参照してください。

関連トピック

[「仮想マシンを管理する」](#)

VirtIO ドライバを更新する (Windows ベースの VM)

Windows ベースの仮想マシン (VM) の Red Hat VirtIO ドライバを最新の対応バージョンに更新して、VM が正常に稼働するようにします。たとえば、システムソフトウェアをアップグレード ([「Stratus Redundant Linux ソフトウェアをアップグレードする」](#)) した後や、P2V クライアントを使って VM または 物理マシン (PM) を ztC Edge システムにマイグレーション ([「物理マシンまたは仮想マシンをシステムにマイグレーションする」](#)) した後に、VirtIO ドライバを更新します。

VirtIO ドライバの ISO ファイルが保存された VCD は、システムソフトウェアのインストール時とアップグレード時にシステムにインストールされます。VCD の存在を確認するには、名前に **virtio** が含まれている VCD の **[仮想 CD]** ページをチェックします ([「\[仮想 CD\] ページ」](#)を参照)。VCD が存在する場合、VirtIO ドライバを更新します ([「Windows ベースの仮想マシンで VirtIO ドライバを更新するには」](#)を参照)。VCD が存在しない場合、これを作成します ([「VirtIO ドライバをダウンロードして VCD を作成するには」](#)を参照)。その後、ドライバを更新します。

注:

- 操作を正しく行うには、次の手順に従って必ず **ztC Edge サポート** ページから VirtIO ドライバをダウンロードしてください。サポート ページの VirtIO ファイルには、Stratus Redundant Linux ソフトウェアでテスト済みのバージョンの VirtIO ドライバが含まれており、正しく動作することが既に確認されています。その他のソースから入手した VirtIO ドライバでは互換性の問題が生じる可能性があります。
- VirtIO ドライバを更新する場合、**[コンピュータを参照してドライバソフトウェアを検索する]** オプションのみを使用して、ゲスト オペレーティング システムに適用される特定のフォルダまたは .inf ファイルを選択します。**[自動的に更新されたドライバソフトウェアを検索します]** オプションを使用したり、VirtIO VCD の最上位レベルのみを選択すると、Windows によって自動的に誤ったドライバがインストールされる可能性があります。
- 場合によっては、ドライバ更新の後にゲスト オペレーティング システムの再起動を求められることがあります。その場合にはゲスト オペレーティング システムを再起動します。

VirtIO ドライバをダウンロードして VCD を作成するには

1. **[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) から VirtIO の ISO ファイルをダウンロードします。
 - a. **[Downloads (ダウンロード)]** ページで **ztC Edge** をクリックし (まだ表示されていない場合)、次に適切なバージョンを選択します。
 - b. **[Drivers and Tools (ドライバとツール)]** にスクロールして、さらに **[ztC Edge VirtIO Driver Update (everRun VirtIO ドライバの更新)]** までスクロールします。
 - c. 適切なファイルのリンクをクリックします。

必ずお使いの ztC Edge システムのバージョンに一致する VirtIO ISO ファイルをダウンロードしてください。

2. ISO イメージの整合性を検証する場合、MD5 のチェックサム ハッシュ関数を使用します。

コマンド プロンプト ウィンドウを管理者として開き、次を入力します。

CertUtil -hashfile *path_to_file* MD5

CertUtil コマンドによって、コマンドの実行が正しく完了したかどうかを示すメッセージが表示されます。コマンドが成功した場合、次のステップに進みます。コマンドが失敗した場合はもう一度ダウンロードを行います。

3. ztC Edge コンソールを開いて VirtIO ISO ファイルの VCD を作成します (「[仮想 CD を作成する](#)」を参照)。

Windows ベースの仮想マシンで VirtIO ドライバを更新するには

1. ztC Edge コンソールを開いて Windows ベースの VM に VCD を挿入します (「[仮想 CD を挿入する](#)」を参照)。
2. VM コンソールウィンドウで、ゲスト オペレーティング システムの **[デバイス マネージャー]** を開きます。

デバイス マネージャーを開く方法はゲスト オペレーティング システムのバージョンによって異なります。たとえば、コントロールパネルを開いて **[デバイス マネージャー]** を選択するのも 1 つの方法です。あるいは検索ウィンドウを開いて「**デバイス マネージャー**」と入力することもできます。

3. **[ネットワーク アダプタ]** を展開して **[Red Hat VirtIO Ethernet Adapter]** を見つけます。VM 内のネットワーク インタフェースの数によっては、複数のアダプタが存在する場合があります。

Red Hat VirtIO Ethernet Adapter が存在しない場合、VirtIO ドライバがインストールされていません。**[その他のデバイス]** を展開して不明の **[イーサネット コントローラ]** デバイスを見つけてみます。このデバイス用にドライバを更新します。

- a. **[Red Hat VirtIO Ethernet Adapter]** (または **[イーサネット コントローラ]**) を右クリックして、**[ドライバ ソフトウェアの更新]** を選択します。**[コンピュータを参照してドライバ ソフトウェアを検索する]** をクリックし、ゲスト オペレーティング システムの VirtIO イーサネット ドライバ (**netkvm**) の場所を指定して、ドライバの更新を完了します。(たとえば、Windows Server 2012 R2 ゲストのドライバを更新するには、VirtIO VCD 上の NetKVM¥2k12R2¥amd64¥**netkvm.inf** ファイルを選択します。)
 - b. その他の各 **Red Hat VirtIO Ethernet Adapter** (または **イーサネット コントローラ**) デバイスについて、ドライバの更新を繰り返します。
4. **[ストレージ コントローラ]** を展開して **[Red Hat VirtIO SCSI controller]** が存在することを確認します。VM 内のボリュームの数によっては、複数のコントローラが存在する場合があります。**Red Hat VirtIO SCSI controller** が存在しない場合、VirtIO ドライバがインストールされ

ていません。不明の **SCSI コントローラ** を見つけて、このデバイス用にドライバを更新します。

- a. **[Red Hat VirtIO SCSI]** コントローラ (または **[SCSI コントローラ]**) を右クリックして、**[ドライバ ソフトウェアの更新]** を選択します。**[コンピュータを参照してドライバー ソフトウェアを検索します]** をクリックし、ゲスト オペレーティング システムの VirtIO SCSI ドライバ (**viostor**) の場所を指定して、ドライバの更新を完了します。(たとえば、Windows Server 2012 R2 ゲストのドライバを更新するには、VirtIO VCD 上の **viostor¥2k12R2¥amd64¥viostor.inf** ファイルを指定します。)
- b. 追加の各 **Red Hat VirtIO** (または **SCSI コントローラ**) デバイスについてドライバの更新を繰り返します。



注意事項: デバイス名は **Red Hat VirtIO SCSI** コントローラですが、**vioscsi** ではなく (存在する場合)、**viostor** というラベルのストレージ ドライバー ファイルを選択する必要があります。**vioscsi** ドライバをインストールすると VM がクラッシュする場合があります。

5. 必要に応じてゲスト オペレーティング システムを再起動し、更新されたドライバを読み込みます。

関連トピック

[「Windows ベースの仮想マシンを構成する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

ディスクを作成して初期化する (Windows ベースの VM)

ディスクを作成して初期化し、Windows ベースの仮想マシンでボリュームにパーティションできるように準備します。

Windows ベースの仮想マシンでディスクを作成して初期化するには

1. ztC Edge コンソールで、ztC Edge システムに新しいボリュームを作成します。詳細については、[「仮想マシンのボリュームを作成する」](#) を参照してください。
2. Windows ゲスト オペレーティング システムで、**ディスク管理** または類似したユーティリティを開きます。

3. 新しく追加したディスクを初期化します。(これを自動で行うプロンプトが表示されることもあります。)
4. ディスクをダイナミック ディスクに変換します。
5. ディスク上に 1 つ以上のシンプル ボリュームを作成します。
6. Windows ゲスト オペレーティング システムを再起動します。

詳しい手順は Windows のマニュアルを参照してください。



注: Stratus Redundant Linux ソフトウェアは既に物理レベルでデータのミラーリングを行っているため、Windows ゲスト オペレーティング システムにおけるボリュームの冗長性は必要ありません。

関連トピック

[「仮想マシン コンソールのセッションを開く」](#)

[「Windows ベースの仮想マシンを構成する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

アプリケーションをインストールする (Windows ベースの VM)

Windows ベースの仮想マシンにアプリケーションをインストールするには、次のいずれかを実行します。

- ゲスト オペレーティング システムに、インストールプログラムを実行可能ファイルまたは ISO ファイルとしてダウンロードします。
- インストールプログラムを含むネットワーク ドライブをマウントします。
- インストールプログラムを含む仮想 CD (VCD) を作成して挿入します。 [「仮想 CD を管理する」](#) を参照してください。

(適切なモニタリングのライセンスが適用されたシステムで) Windows ベースの VM 上のアプリケーションをモニタリングする場合の詳細については、 [「Windows ベースの仮想マシン上のアプリケーションをモニタリングする」](#) を参照してください。

関連トピック

[「仮想マシン コンソールのセッションを開く」](#)

[「Windows ベースの仮想マシンを構成する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

Linux ベースの仮想マシンを構成する

Linux ベースの仮想マシンをインストールした後、次を参照して稼動時に必要となる追加のリソースとソフトウェアを構成します。

- [「ディスクを作成して初期化する \(Linux ベースの VM\)」](#)
- [「アプリケーションをインストールする \(Linux ベースの VM\)」](#)

また、以下の設定も構成する必要があります。

- ゲスト オペレーティング システムが省エネルギー状態になるのを防ぐため、休止機能を無効にします (これはデフォルトで有効になっている場合があります)。
- ゲスト オペレーティング システムの電源ボタンのアクションを、ゲストを "休止" にする代わりに "シャットダウン" するように構成して、ztC Edge コンソールの VM の **[シャットダウン]** ボタンが正しく機能するようにします。最小サーババージョンの Ubuntu Linux の場合、オプションで `acpid` パッケージをインストールして **[シャットダウン]** ボタンを有効にします。[「仮想マシンをシャットダウンする」](#) を参照してください。
- `kexec-tools` パッケージをインストールして、システムがクラッシュしたときにクラッシュ ダンプ ファイルが生成されるようにゲスト オペレーティング システムを構成します。
- Ubuntu Linux ゲスト オペレーティング システムの場合、VM コンソールが ztC Edge コンソールでハングする問題を避けるため、`/boot/grub/grub.cfg` ファイルを編集して `gfxmode` パラメータを `text` に変更します (例: `set gfxmode=text`)。VM コンソールがハングしてパラメータを設定できない場合、[「仮想マシン コンソールのセッションを開く」](#) のトラブルシューティング情報を参照し、問題を解決してください。

これらの設定の詳細については、お使いの Linux のマニュアルを参照してください。

関連トピック

[「仮想マシンを管理する」](#)

ディスクを作成して初期化する (Linux ベースの VM)

ディスクを作成して初期化し、Linux ベースの仮想マシンでデータを保存できるようにします。

Linux ベースの仮想マシンでディスクを作成して初期化するには

1. ztC Edge コンソールで、新しいボリュームを作成します。詳細については、[「仮想マシンのボリュームを作成する」](#)を参照してください。
2. Linux ベースの仮想マシンでは、必要に応じてボリューム管理ツールを使用するか、適切なファイルを編集して、ボリュームを初期化してマウントします。詳しい手順は Linux のマニュアルを参照してください。

Linux ベースの仮想マシンのディスク デバイス名は `/dev/vda` ～ `/dev/vdh` です。標準の `/dev/sda` ～ `/dev/sdh` ではありません。ztC Edge 仮想ディスク ボリュームはゲスト オペレーティング システムに表示され、物理ディスクであるかのように使用されます。

関連トピック

[「仮想マシン コンソールのセッションを開く」](#)

[「Linux ベースの仮想マシンを構成する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

アプリケーションをインストールする (Linux ベースの VM)

Linux ベースの仮想マシンにアプリケーションをインストールするには、次のいずれかを実行します。

- ゲスト オペレーティング システムに、インストール パッケージを実行可能ファイルまたは ISO ファイルとしてダウンロードします。
- インストール パッケージを含むネットワーク ドライブをマウントします。
- インストール パッケージを含む仮想 CD (VCD) を作成して挿入します。[「仮想 CD を管理する」](#)を参照してください。

関連トピック

[「仮想マシン コンソールのセッションを開く」](#)

[「Linux ベースの仮想マシンを構成する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンの運用を管理する

仮想マシンの運用を管理する方法は次を参照してください。

- [「仮想マシンを起動する」](#)
- [「仮想マシンをシャットダウンする」](#)
- [「仮想マシンの電源をオフにする」](#)
- [「仮想マシン コンソールのセッションを開く」](#)
- [「仮想マシンの名前を変更する」](#)
- [「仮想マシンを削除する」](#)

構成とトラブルシューティングの詳細については、[「高度なトピック \(仮想マシン\)」](#)を参照してください。

仮想マシンを起動する

仮想マシン (VM) を起動して VM のゲスト オペレーティング システムをブートします。ztC Edge システムのブート時に VM の起動モードを構成することもできます。

仮想マシンを起動するには

1. [\[仮想マシン\]](#) ページで、VM を選択します。
2. 下部のパネルで [\[起動\]](#) をクリックします。

システム ブート時の仮想マシンの起動モードを構成するには

1. [\[仮想マシン\]](#) ページで、VM を選択します。
2. 下部のパネルで [\[ブート\]](#) タブをクリックします。
3. [\[自動起動モード\]](#) に次のいずれかを選択します。

- **最終** — VM をシステムがシャットダウンされたときの状態に戻します。VM が稼働していた場合、システムのブート時に VM が再起動されます。VM が停止していた場合はシステムのブート時に VM は起動されません。
- **オン** — システムのブート時に VM を起動します。
- **オフ** — システムのブート時に VM を起動しません。

4. **[保存]** をクリックします。

関連トピック

[「仮想マシンをシャットダウンする」](#)

[「仮想マシンの電源をオフにする」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンをシャットダウンする

仮想マシン (VM) をシャットダウンして、ゲスト オペレーティング システムの正常なシャットダウンを開始します。



注: VM のシャットダウンにはゲスト オペレーティング システムのコマンドを使用できます。一部のゲスト OS では ztC Edge コンソールを使用した VM のシャットダウンが許可されています (または許可されるよう構成できます)。

ztC Edge コンソールを使って VM をシャットダウンする操作は、物理マシンの電源ボタンを押す場合と似ており、通常はオペレーティング システムが正常にシャットダウンされます。場合によっては、ゲスト オペレーティング システムでこの機能を有効に設定する必要があります。例:

- すべてのゲストで、電源ボリュームのアクションが、ゲスト オペレーティング システムの休止ではなくシャットダウンを実行するように設定されていることを確認します。ztC Edge コンソールで、休止するように設定されているゲストの **[シャットダウン]** をクリックすると、その VM は **「停止中」** のままの状態になり、正しくシャットダウンされません。
- ゲストによっては、ユーザがオペレーティング システムにログオンしていないと、電源ボタンを使ってシステムをシャットダウンすることができません。その場合、セキュリティ設定を更新して、ログイン セッションがない場合でも電源ボタンを有効にできることがあります。
- Ubuntu の最小サーバ バージョンの一部には、電源ボタンを有効にする acpid パッケージがデフォルトのインストールに含まれていません。このパッケージを手動でインストールして電源ボタンを有効にするには、次のコマンドを使用できます (またはゲスト オペレーティング システム

のマニュアルを参照してください)。

```
sudo apt-get install acpid
```

デスクトップを実行している Ubuntu のバージョンの場合、ztC Edge コンソールの **[シャットダウン]** ボタンを押すと VM の Ubuntu デスクトップに中断、スリープ、シャットダウンの 3 つのアイコンのいずれかを選択するようプロンプトが表示されます。Ubuntu VM がデスクトップ プロンプトなしでシャットダウンできるようにするには、powerbtn ファイルを変更する必要があります。

powerbtn ファイルを変更するには

1. VM で /etc/acpi/events/powerbtn ファイルを編集します。
2. 次のラインをコメントアウトします。

```
event=button[ /]power  
action=/etc/acpi/powerbtn.sh
```

3. 次のラインを追加します。

```
event=button/power (PWR.||PBTN)  
action==/sbin/poweroff
```

4. 次のコマンドを実行して acpid を再起動します。

```
systemctl restart acpid
```

[シャットダウン] ボタンが ztC Edge コンソールで機能するようにシステム電源ボタンの動作を構成する方法は、ゲスト オペレーティング システムのマニュアルを参照してください。

ztC Edge コンソールで VM をシャットダウンするには

1. **[仮想マシン]** ページで、VM を選択します。
2. 下部のパネルで **[シャットダウン]** をクリックします。

シャットダウンを確認するための警告メッセージが表示されます。シャットダウンする場合は **[はい]** を、シャットダウンを中断する場合は **[いいえ]** をクリックします。

VM が応答しない場合、仮想マシンを**電源オフ**にして、ゲスト オペレーティング システムを正常にシャットダウンせずに VM を停止することもできます。

関連トピック

[「仮想マシンを起動する」](#)

[「仮想マシンの電源をオフにする」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンの電源をオフにする

ゲスト オペレーティング システムの正常なシャットダウンを行わずに仮想マシン (VM) を停止するには、仮想マシンを電源オフにします。



注意事項: **[電源オフ]** コマンドは、**[シャットダウン]** コマンドやゲスト オペレーティング システムのコマンドが失敗した場合のみに使用してください。VM を電源オフにする操作は、電源コードをコンセントから引き抜く場合と似ており、データ損失の原因となる可能性があります。

仮想マシンの電源をオフにするには

1. **[仮想マシン]** ページで、VM を選択します。
2. 下部のパネルで **[電源オフ]** をクリックします。

関連トピック

[「仮想マシンを起動する」](#)

[「仮想マシンをシャットダウンする」](#)

[「仮想マシンの運用を管理する」](#)


[「高度なトピック \(仮想マシン\)」](#)

仮想マシン コンソールのセッションを開く

仮想マシン (VM) コンソール セッションを開いて、VM で実行中のゲスト オペレーティング システムのコンソールを表示します。

次に示すのは ztC Edge コンソールで VM コンソール セッションを開く手順ですが、リモートデスクトップ アプリケーションを使用することもできます。

VM コンソール セッションを開くには

1. **[仮想マシン]** ページで、VM を選択します。
2. VM が稼動状態にあることを確認します。
3. 下部のパネルで **[コンソール]** () をクリックします。

注:

[コンソール] をクリックした後、ブラウザが HTTPS でシステムに接続していて、そこにセキュリティ例外がない場合には、コンソール セッションが空白になることがあります。その場合、セッション ウィンドウの右上角にある **[IP アドレス]** をクリックします。この IP アドレスは `https://system_IP_address:8000` という形式で、システム IP アドレスをブラウザのセキュリティ例外として追加します。セキュリティ例外によって、ブラウザがサイトを開けるようになります。

ブラウザによっては、追加のセキュリティ警告のウィンドウやメッセージが表示される場合もあります。一部のブラウザでは、セキュリティ メッセージがいくつか表示されるので、これらのメッセージをクリックする必要があります。その他のブラウザでは、アドレス バーが赤くなるだけでメッセージは表示されず、その場合はアドレスをクリックして操作を続行する必要があります。次に具体的な例を示します。



- アドレス バーに **[Certificate error (証明書のエラー)]** が表示されたら、(1) アドレスをクリックし、(2) **[The website cannot display the page (Web サイトでこのページは表示できません)]** と表示されたページで **[More information (詳細情報)]** をクリックしてから、(3) **[This site is not secure (このサイトは安全ではありません)]** と表示されたページで **[Go on to the webpage (not recommended) (Web ページに移動 (非推奨))]** をクリックします。
- **[Warning: Potential Security Risk Ahead (警告: 潜在的なセキュリティ リスクがあります)]** というページが表示されたら、**[Advanced (詳細)]** をクリックして、次のウィンドウで **[Accept Risk and Continue (危険性を承知で続行)]** をクリックします。
- **Error code 405 (エラー コード 405)** の **[Error response (エラー応答)]** が表示された場合は、ウィンドウまたはタブを閉じます。




すると、このセキュリティ例外がすべての VM に適用されます。これらのアクションを行う必要があるのは、各ブラウザで 1 度だけです。それ以降は、**[コンソール]** をクリックすると、VM へのコンソール セッションが問題なく開きます。

VM コンソール セッションを開いた後、ブラウザ ウィンドウと VM コンソール セッションのサイズを変更できます。キーボード ショートカットを使用することもできます。

ブラウザ ウィンドウと VM セッションのサイズを変更するには

1. 上記の手順を参照して VM コンソール セッションを開きます。

ウィンドウの左端にアイコンが表示されます。アイコンを表示するには、ウィンドウの左端にあるタブ内の矢印をクリックしてください。







2. ブラウザ ウィンドウを全画面表示にするには、全画面のアイコン () をクリックします。
全画面で表示されているときに全画面のアイコン () をもう一度クリックすると、ブラウザが小さいウィンドウに戻ります。
3. ブラウザ内の VM セッションのサイズを変更するには、設定アイコン () をクリックして **[拡大縮小モード]** を選択します (現在のモードをクリックすると、その他の設定を含むプルダウン メニューが表示されます)。

- **リモート サイズ変更** (デフォルト) — ゲスト OS の解像度を変更すると VM セッションのサイズが変わります。
- **ローカル拡大縮小** — VM セッションのサイズは、元の幅と高さの比率で全画面に収まるよう自動的に変更されます。

キーボード ショートカットを使用するには

1. 上記の手順を参照して VM コンソール セッションを開きます。

ウィンドウの左端にアイコンが表示されます。アイコンを表示するには、ウィンドウの左端にあるタブ内の矢印をクリックしてください。

2. ウィンドウの左端にある **A** アイコン () をクリックして、キーボード ショートカットの選択アイコンを表示します。
3. 次のアイコンが表示されます。
 -  — **Ctrl** キーの機能を使用する場合に選択します。
 -  — **Alt** キーの機能を使用する場合に選択します。
 -  — **Tab** キーの機能を使用する場合に選択します。
 -  — **Esc** キーの機能を使用する場合に選択します。
 -  — **Ctrl+Alt+Delete** キーの機能を使用する場合に選択します。

トラブルシューティング

VM コンソール ウィンドウが開かない場合に問題を解決するには

6900 から 6999 まで (両者を含む) のポートを開くように、ネットワーク管理者に依頼してください。

VM コンソール ウィンドウが空白の場合に問題を解決するには

VM に電源が入っていて、ブート中でないことを確認します。また、コンソール ウィンドウをクリックして任意のキーを押し、スクリーン セーバーを無効にします。

複数の VM コンソール ウィンドウが表示されていて、その動作が不安定な場合に問題を解決するには

すべてのコンソール ウィンドウを閉じてから、コンソール ウィンドウを 1 つだけ開きます。

VM コンソール ウィンドウが ztC Edge システムでハングする問題を解決するには

Ubuntu ベースの VM では、`gfxmode` パラメータが正しく設定されていないと VM コンソールが ztC Edge コンソールでハングします。ゲスト オペレーティング システムで、`/boot/grub/grub.cfg` ファイルを編集して `gfxmode` パラメータを `text` に変更します (例: `set gfxmode=text`)。

コンソールがハングしてパラメータを設定できない場合、次を行います。

1. ztC Edge コンソールで VM を再起動します。
2. GRUB メニューで `e` を押して、`grub` コマンドを編集します。
3. 次の画面の `gfxmode` 行で、`$linux_gfx_mode` を `text` に変更して次のようにします。

```
gfxmode text
```

4. **Ctrl-x** または **F10** を押してゲスト オペレーティング システムをブートします。
5. リブートした後も設定が維持されるように更新するには、`/boot/grub/grub.cfg` ファイルを編集して `gfxmode` パラメータを `text` に変更します。行が次のようになります。

```
set gfxmode=text
```

6. `/boot/grub/grub.cfg` ファイルを保存します。

コンソール画面が判読不能な場合に Linux ベースの VM でターミナル タイプを変更するには

デフォルトでは、Linux オペレーティング システムは ztC Edge コンソールで VM コンソールの基盤である `vncterm` プログラムでは正しくサポートされない `vt100-nav` に `TERM` 変数を設定します。コマンド ライン以外の方法を利用すると、画面が判読不能になります。この問題を解決するには、次の手順に従い Linux ゲスト オペレーティング システムのターミナルのタイプを変更します。

1. ゲスト オペレーティング システムの `inittab` ファイルを開きます。
2. 以下の行で、行の末尾にある `-nav` を削除して、`vt100-nav` を `vt100` に変更します。更新後の行は次のようになります。

```
# Run gettys in standard runlevels co:2345:respawn:/sbin/agetty xvc0
9600 vt100
```
3. **inittab** ファイルを保存します。

関連トピック

[「仮想マシンを起動する」](#)

[「仮想マシンをシャットダウンする」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンの名前を変更する

[**仮想マシン**] ページに表示される仮想マシン (VM) の名前を変更します。

VM で実行されるゲスト オペレーティング システムのホスト名を変更する必要がある場合は、ゲスト オペレーティング システムのツールを使用します。



前提条件: VM の名前を変更するには、VM をシャットダウンする必要があります。

仮想マシンの名前を変更するには

1. [**仮想マシン**] ページで、VM を選択します。
2. [**シャットダウン**] をクリックして VM がシャットダウンするまで待ちます。
3. VM の名前をダブルクリックします。
4. 新しい名前を入力します。VM 名は、以下の要件を満たす必要があります。

- VM 名は単語または数字で始める必要があり、名前に特殊文字 (たとえば #、%、または \$) を含めることはできません。
- VM 名に Zombie- や migrating- などのハイフン付きのプレフィックスは使用できません。
- VM 名には最大 85 文字を使用できます。

5. **Enter** キーを押します。

関連トピック

[「仮想マシンを削除する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンを削除する

ztC Edge システムから仮想マシン (VM) を永久に削除して、オプションでその関連ボリュームも削除するには、仮想マシンの削除を行います。



前提条件: VM を正しく削除するには、ztC Edge システムの両方の PM がオンラインでなければなりません。ztC Edge コンソールの **[物理マシン]** ページで、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンス モードではなく、同期も行われていないことを確認します。

仮想マシンを削除するには

1. **[仮想マシン]** ページで、VM を選択します。
2. 下部のパネルで **[シャットダウン]** をクリックします。
3. VM が停止したら、**[削除]** をクリックします。
4. **[仮想マシンの削除]** ダイアログ ボックスで、削除するボリュームの横のチェック ボックスをオンにします。ボリュームをアーカイブとして保存する場合や別の VM への接続用に保存する場合は、このチェック ボックスをオフにします。



注意事項: 削除の対象として正しい VM とボリュームを選択してください。**[VM の削除]** をクリックすると、これらの項目は永久に削除されます。

5. VM および選択した任意のボリュームを永久に削除するには、**[VM の削除]** をクリックします。

関連トピック

[「仮想マシンの名前を変更する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンのリソースを管理する

仮想マシンのリソースを管理して、既存の仮想マシンの vCPU、メモリ、ストレージ、またはネットワーク リソースを再構成します。

仮想マシンのリソースを再構成するには、**仮想マシンの再プロビジョニング** ウィザードを使用します。説明は次を参照してください。

- [「仮想マシンのリソースを再プロビジョニングする」](#)

仮想マシンのボリュームを再構成するには、タスクに応じて以下のトピックを参照してください。

- [「仮想マシンのボリュームを作成する」](#)
- [「仮想マシンにボリュームを接続する」](#)
- [「仮想マシンからボリュームを切断する」](#)
- [「仮想マシンからボリュームを削除する」](#)
- [「ztC Edge システム上のボリュームを拡張する」](#)

仮想マシンのリソースを復旧し、新しいボリュームや仮想 CD 用に容量を解放するには、次を参照してください。

- [「仮想マシンのリソースを復旧する」](#)

仮想マシンのリソースを再プロビジョニングする

仮想マシン (VM) を再プロビジョニングして、その仮想 CPU (vCPU)、メモリ、ストレージ、またはネットワークのリソースの割り当てを変更します。

[仮想マシン] ページの下部パネルで **[構成]** をクリックして、**仮想マシンの再プロビジョニング** ウィザードを起動します。ウィザードに VM のリソース再割り当てのプロセスが順を追って表示されます。

前提条件:

- 「[仮想マシンのリソースを計画する](#)」のリストを参照し、VM への vCPU、メモリ、ストレージ、およびネットワークのリソースの割り当てに関する前提条件と考慮事項を確認します。ストレージ リソースの詳細については、「[仮想マシンのストレージを計画する](#)」を参照してください。
- VM を再プロビジョニングするには、その VM をシャットダウンする必要があります。

仮想マシンを再プロビジョニングするには

1. **[仮想マシン]** ページを開きます (「[\[仮想マシン\] ページ](#)」を参照してください)。
2. VM を選択して **[シャットダウン]** をクリックします。
3. VM が停止したら、**[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを表示します。
4. **[名前および説明] [名前、説明および保護]** ページで、次を行います。
 - a. VM に ztC Edge コンソールで表示される **[名前]** を入力し、オプションで **[説明]** を入力します。

VM 名は、以下の要件を満たす必要があります。

 - VM 名は単語または数字で始める必要があります、名前に特殊文字 (たとえば #、%、または \$) を含めることはできません。
 - VM 名に Zombie- や migrating- などのハイフン付きのプレフィックスは使用できません。
 - VM 名には最大 85 文字を使用できます。
 - b. VM で使用する保護のレベルを選択します。
 - **フォールトトレラント (FT)**
 - **高可用性 (HA)**

これらの保護レベルの詳細については、「[新しい仮想マシンを作成する](#)」と、「[運用モード](#)」を参照してください。
 - c. **[次へ]** をクリックします。

5. **[vCPU とメモリ]** ページで次を行います。

- a. VM に割り当てる **vCPU** の数と**メモリ**の容量を指定します。詳細については、「[仮想マシンの vCPU を計画する](#)」および「[仮想マシンのメモリを計画する](#)」を参照してください。
- b. **[次へ]** をクリックします。

6. **[ボリューム]** ページで、次を行えます。

注:



VM ブート ボリュームは変更できません。変更できるのはデータ ボリュームだけです。ただし、ブート ボリュームを切断することは可能です。

- **[ブート ボリューム]** をクリックして、ブート ボリュームを切断します。



注意事項: ブート ボリュームを切断すると、VM がブート不可能になります。

ブート ボリュームを切断すると VM がブート不可能になることを知らせるメッセージが表示されます。ブート ボリュームの切断を取り消すには、**[切断を元に戻す]** をクリックします。

- ボリュームを VM から切断し、後日使用できるように維持しておくには、**[切断]** をクリックします。
- ボリュームを ztC Edge システムから完全に削除するには、**[削除]** をクリックします。
- プルダウン メニューが表示される場合、メニューから未接続のボリュームを選択し、**[接続]** をクリックします。

あるいは、該当する場合は **[新しいボリュームの追加]** をクリックして新しいデータ ボリュームを作成します。(ボタンが表示されない場合、ウィザード ページの一番下までスクロールします。)

未接続のボリュームや新しいボリュームの場合、ボリュームのパラメータを指定します。

- a. ボリュームの **[名前]** を入力します。
- b. ボリュームの **[ボリューム サイズ]** をギガバイト (GB) 単位で入力します。ストレージ割り当ての詳細については、および「[仮想マシンのストレージを計画する](#)」を参照してください。
- c. 該当する場合、**[接続]** をクリックしてボリュームを VM に接続します。

続行するには **[次へ]** をクリックします。

7. **[ネットワーク]** ページで、この VM に接続する各共有ネットワークのチェック ボックスをオンにします。

接続する各共有ネットワークについて、オプションで次を指定することもできます。

- カスタムの MAC アドレスを設定する (詳細は、[「仮想マシンに特定の MAC アドレスを割り当てる」](#) を参照してください)
- **[状態]** を **[有効]** または **[無効]** に設定して、選択したネットワークへのトラフィックを許可したりブロックする

詳細については、[「仮想マシンのネットワークを計画する」](#) を参照してください。続行するには **[次へ]** をクリックします。

8. **[構成サマリ]** ページで次を行います。



注意事項: 削除対象としてマークされているボリュームが正しいことを確認します。

[完了] をクリックすると、削除対象としてマークされたディスクのデータは永久に失われます。

- a. 構成サマリの内容を確認します。変更が必要な場合、**[戻る]** をクリックします。
 - b. VM のプロビジョニング構成を受け入れるには、**[完了]** をクリックします。
9. **[起動]** をクリックして、VM を再起動します。
 10. Windows ベースの VM で、割り当て済み仮想 CPU の数を 1 から n に変更したり n から 1 に変更した場合、再プロビジョニングの完了時に VM を再起動した後で、VM をもう一度シャットダウンして再起動する必要があります。これにより、VM が対称型マルチプロセッシング (SMP) のために正しく再構成されます。この VM は、再起動されるまで異常な動作を示し、使用不可になります。

関連トピック

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンのリソースを計画する」](#)

[「仮想マシンを管理する」](#)

仮想マシンのボリュームを作成する

ボリュームを作成して、新しい空白のボリュームを仮想マシン (VM) に接続します。(未接続の既存のボリュームを接続することもできます。詳細については、「[仮想マシンにボリュームを接続する](#)」を参照してください。)



前提条件: VM にボリュームを作成する前に、その VM をシャットダウンする必要があります。

VM に新しいボリュームを作成するには

1. **[仮想マシン]** ページを開きます (「[\[仮想マシン\] ページ](#)」を参照してください)。
2. VM を選択して **[シャットダウン]** をクリックします。
3. VM が停止したら、**[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを表示します。
4. ウィザードの各ページで **[次へ]** をクリックして、**[ボリューム]** ページに進みます。(必要な場合、「[仮想マシンのリソースを再プロビジョニングする](#)」を参照し、追加の VM リソースを構成します。)
5. **[ボリューム]** ページで、**[新しいボリュームの追加]** をクリックします。(ボタンが表示されない場合、ウィザード ページの一番下までスクロールします。)
6. **[作成予定]** の下で、次のいずれかを実行します。
 - a. ztC Edge コンソールに表示されるボリュームの **[名前]** を入力します。
 - b. 作成するボリュームの **[ボリューム サイズ]** をギガバイト (GB) 単位で入力します。ストレージ割り当ての詳細については、および「[仮想マシンのストレージを計画する](#)」を参照してください。
7. ウィザードの各ページで **[次へ]** をクリックして、**[構成サマリ]** ページに進みます。構成の変更内容を確認します。
8. **[完了]** をクリックして、ボリュームを作成します。
9. VM を起動して、ゲスト オペレーティング システムで使用するボリュームを準備します。次を参照してください。
 - 「[ディスクを作成して初期化する \(Windows ベースの VM\)](#)」
 - 「[ディスクを作成して初期化する \(Linux ベースの VM\)](#)」

関連トピック

[「仮想マシンからボリュームを切断する」](#)

[「仮想マシンからボリュームを削除する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンのリソースを計画する」](#)

[「仮想マシンを管理する」](#)

仮想マシンにボリュームを接続する

ボリュームを接続して、未使用のボリュームを仮想マシンに接続します。



注: 既にブート ボリュームを持つ VM にブート ボリュームを接続しようとする、新しく追加したボリュームはデータ ボリュームとして接続されます。この方法でボリュームを接続して、ブート問題の診断や、別の VM のブート ボリュームにあるデータ破損を診断することもできます。ゲスト オペレーティング システムのツールを使ってこの問題を解決した後、ボリュームを切断し、元の VM に再び接続します。



前提条件: 仮想マシンにボリュームを接続するには、その前に仮想マシンをシャットダウンする必要があります。

仮想マシンにボリュームを接続するには

1. 他の仮想マシンで使用されているボリュームを接続することはできません。**[ボリューム]** ページを開いてボリュームを見つけ、**[用途]** 列の値が **[なし]** であることを確認します。
2. **[仮想マシン]** ページを開きます ([「\[仮想マシン\] ページ」](#) を参照してください)。
3. VM を選択して **[シャットダウン]** をクリックします。
4. VM が停止したら、**[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを表示します。
5. ウィザードの各ページで **[次へ]** をクリックして、**[ボリューム]** ページに進みます。(必要な場合、[「仮想マシンのリソースを再プロビジョニングする」](#) を参照し、追加の VM リソースを構成します。)

6. **[ボリューム]** ページで、**[新しいボリュームの追加]** ボタンの横のプルダウン メニューを見つけます。プルダウン メニューから未接続のボリュームを選択し、**[接続]** をクリックします。
(プルダウン メニューが表示されない場合、ウィザード ページの一番下までスクロールします。プルダウン メニューが表示されるのは、ztC Edge システムに未接続のボリュームがある場合のみです。)
7. ウィザードの各ページで **[次へ]** をクリックして、**[構成サマリ]** ページに進みます。構成の変更内容を確認します。
8. **[完了]** をクリックして、選択したボリュームを接続します。

関連トピック

[「仮想マシンのボリュームを作成する」](#)

[「仮想マシンからボリュームを切断する」](#)

[「仮想マシンからボリュームを削除する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンのリソースを計画する」](#)

[「仮想マシンを管理する」](#)

仮想マシンからボリュームを切断する

仮想マシンからボリュームを切断して、後日使用のために保持したり、別の仮想マシンに接続することができます。手順については、[「仮想マシンにボリュームを接続する」](#)を参照してください。)(ボリュームを ztC Edge システムから永久に削除することもできます。詳細については、[「仮想マシンからボリュームを削除する」](#)を参照してください。)



注: VM からブート ボリュームを切断すると、その VM がブート不可になりますが、ブート ボリュームを切断してブートの問題やボリューム内のデータ破損についての診断を行う場合もあります。ブート ボリュームを一時的に別の VM にデータ ボリュームとして接続することができます。詳細については、[「仮想マシンにボリュームを接続する」](#)を参照してください。ゲストオペレーティングシステムのツールを使ってこの問題を解決した後、ボリュームを切断し、元の VM に再び接続します。



前提条件: 仮想マシンからボリュームを切断するには、その前に仮想マシンをシャットダウンする必要があります。

仮想マシンからボリュームを切断するには

1. **[仮想マシン]** ページを開きます ([「\[仮想マシン\] ページ」](#) を参照してください)。
2. VM を選択して **[シャットダウン]** をクリックします。
3. VM が停止したら、**[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを表示します。
4. ウィザードの各ページで **[次へ]** をクリックして、**[ボリューム]** ページに進みます。(必要な場合、[「仮想マシンのリソースを再プロビジョニングする」](#) を参照し、追加の VM リソースを構成します。)
5. **[ボリューム]** ページで、切断するボリュームを見つけます。(ボリュームが表示されない場合、ウィザード ページを下にスクロールします。)
6. ボリューム名の横の **[切断]** をクリックしてボリュームを切断の対象としてマークします。



注意事項: 正しいボリュームをマークする必要があります。現在使用中のボリュームはマークしないでください。

7. ウィザードの各ページで **[次へ]** をクリックして、**[構成サマリ]** ページに進みます。構成の変更内容を確認します。
8. **[完了]** をクリックして、選択したボリュームを切断します。

関連トピック

[「仮想マシンにボリュームを接続する」](#)

[「仮想マシンからボリュームを削除する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンのリソースを計画する」](#)

[「仮想マシンを管理する」](#)

仮想マシンからボリュームを削除する

仮想マシン (VM) のボリュームを削除して、ボリュームを ztC Edge システムから永久に削除します。

(VM からボリュームを切断して後日使用できるよう残しておくこともできます。詳細については、[「仮想マシンからボリュームを切断する」](#) を参照してください。)



前提条件: 仮想マシンに接続されているボリュームを削除するには、その前に仮想マシンをシャットダウンする必要があります。

仮想マシンに接続されているボリュームを削除するには

1. **[仮想マシン]** ページを開きます ([「\[仮想マシン\] ページ」](#) を参照してください)。
2. VM を選択して **[シャットダウン]** をクリックします。
3. VM が停止したら、**[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを表示します。
4. ウィザードの各ページで **[次へ]** をクリックして、**[ボリューム]** ページに進みます。(必要な場合、[「仮想マシンのリソースを再プロビジョニングする」](#) を参照し、追加の VM リソースを構成します。)
5. **[ボリューム]** ページで、削除するボリュームを見つけます。(ボリュームが表示されない場合、ウィザード ページを下にスクロールします。)
6. ボリューム名の横の **[削除]** をクリックしてボリュームを削除の対象としてマークします。



注意事項: 正しいボリュームをマークする必要があります。現在使用中のボリュームはマークしないでください。

7. ウィザードの各ページで **[次へ]** をクリックして、**[構成サマリ]** ページに進みます。構成の変更内容を確認します。
8. **[完了]** をクリックして、選択したボリュームを永久に削除します。

未接続のボリュームを削除するには



注意事項: ボリュームを削除する前に、他の管理者がそのボリュームを必要としていないことを確認します。

1. **[ボリューム]** ページで次を行います。
2. 未接続のボリュームを選択します。(**[用途]** 列の値が **[なし]** の場合のみ、**[削除]** ボタンが表示されます。)
3. **[削除]** をクリックします。

関連トピック

[「仮想マシンからボリュームを切断する」](#)

[「仮想マシンにボリュームを接続する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンのリソースを計画する」](#)

[「仮想マシンを管理する」](#)

ztC Edge システムのボリュームの名前を変更する

ztC Edge システム上のボリュームの名前を変更します。ボリューム名は **[ボリューム]** ページに表示されます。

仮想マシンで実行されるゲスト オペレーティング システムにあるディスクまたはボリュームの名前を変更する必要がある場合は、ゲスト オペレーティング システムのツールを使用します。

ztC Edge システム上のボリュームの名前を変更するには

1. **[ボリューム]** ページでボリュームを見つけます。
2. ボリュームの名前をダブルクリックします。
3. 新しい名前を指定して **Enter** キーを押します。

関連トピック

[「仮想マシンのボリュームを作成する」](#)

[「仮想マシンからボリュームを切断する」](#)

[「仮想マシンからボリュームを削除する」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンのリソースを計画する」](#)

[「仮想マシンを管理する」](#)

ztC Edge システム上のボリュームを拡張する

仮想マシン (VM) ボリュームを拡張して、プログラムやデータ用の追加の容量をゲスト オペレーティング システムに割り当てます。

ボリュームは拡張できますが、サイズを小さくすることはできません。VM が停止している場合のみ、次の手順に従ってボリュームを拡張します。

前提条件:

- VM を含むボリュームを拡張する場合、その前に VM をシャットダウンする必要があります。
- ztC Edge システムの両方の PM がオンラインになっていることを確認します。そうでない場合、システムはボリュームを正しく拡張できません。

ボリュームを拡張するには

1. 2つのノードで構成されているシステムの **[物理マシン]** ページ ([「\[物理マシン\] ページ」](#) を参照) で、両方の PM が「**実行中**」の状態にあり、どちらの PM もメンテナンス モードではなく、同期の実行中でもないことを確認します。
2. **[仮想マシン]** ページで ([「\[仮想マシン\] ページ」](#) を参照)、拡張するボリュームを含む VM を選択します。VM が**停止**していることを確認します。
3. 下部パネルで **[ボリューム]** タブをクリックして、拡張するボリュームを選択します。**[アクション]** 列で、**[ボリュームの拡張]** をクリックします。
4. **[追加するサイズ]** の横に、ボリュームに追加するストレージ容量をギガバイト (GB) 単位で入力します。値を入力すると、この操作の実行後に得られる **[拡張後のボリューム サイズ]** を示すダイアログ ボックスが表示されます。



注: **[追加するサイズ]** に入力する値には注意してください。ボリュームは一度拡張すると、その後でサイズ変更を取り消したり、サイズを小さくすることはできません。ボリュームのサイズは拡張することしかできません。

5. **[ボリュームの拡張]** をクリックして変更を確定し、ボリュームを拡張します。ダイアログ ボックスに拡張処理の進捗状況が表示されます。操作が完了すると、このダイアログ ボックスは自動的に閉じます。

関連トピック

- [「仮想マシンのボリュームを作成する」](#)
- [「仮想マシンからボリュームを切断する」](#)
- [「仮想マシンからボリュームを削除する」](#)
- [「仮想マシンのリソースを管理する」](#)
- [「仮想マシンのリソースを計画する」](#)
- [「仮想マシンを管理する」](#)

仮想マシンのリソースを復旧する

ストレージ容量を節約するため、不要になった VM リソースは削除してください。また、ボリュームや VCD の作成など、特定のタスクに必要な容量が不足している場合には、ストレージ容量を直ちに復旧しなければならないことがあります。

ストレージ容量を復旧するには、次のトピックを参照して未使用のリソースを削除します。

- [「仮想マシンを削除する」](#)
- [「仮想マシンからボリュームを削除する」](#)
- [「仮想 CD を削除する」](#)

関連トピック

- [「仮想マシンのリソースを管理する」](#)
- [「仮想マシンのリソースを計画する」](#)
- [「仮想マシンを管理する」](#)

仮想 CD を管理する

仮想 CD (VCD) を作成および管理して、ISO 形式のソフトウェア インストール メディアを ztC Edge システム上の仮想マシンで使用できるようにします。

VCD は、読み取り専用の ISO イメージ ファイルで、ztC Edge システムのストレージデバイス上にあります。(ztC Edge コンソールの) **仮想 CD の作成ウィザード**を使用して、既存の ISO ファイルをアップロードします。詳細については、[「仮想 CD を作成する」](#)を参照してください。

VCD を作成すると、そこからブートして Windows や Linux ゲスト オペレーティング システムをインストールしたり、ブート可能な復旧 VCD から VM を起動することができます。VCD はローカル コン

コンピュータにダウンロードできます。稼働中の VM に VCD を挿入してソフトウェア アプリケーションをインストールすることもできます。

VCD の管理については、次を参照してください。

- [「仮想 CD を作成する」](#)
- [「仮想 CD を挿入する」](#)
- [「仮想 CD を取り出す」](#)
- [「仮想 CD からブートする」](#)
- [「仮想 CD の名前を変更する」](#)
- [「仮想 CD をダウンロードする」](#)
- [「仮想 CD を削除する」](#)

管理者または**プラットフォーム マネージャー**のロールが割り当てられているユーザは、VCD のすべてのタスクを実行できます。**VM マネージャー**のロールを割り当てられているユーザは、VCD の名前変更を除くすべての VCD タスクを実行できます。(これらのロールの割り当ての詳細については、[「ローカル ユーザ アカウントを管理する」](#)を参照してください。)

仮想 CD を作成する

仮想 CD (VCD) を作成して、ソフトウェア インストール メディアを ztC Edge システム上の仮想マシン (VM) で使用できるようにします。

VCD を作成するには、**仮想 CD の作成ウィザード**を使用して ISO ファイルを ztC Edge システム上のストレージ デバイスにアップロードまたはコピーします。すると、その VCD からブートして ([「仮想 CD からブートする」](#)を参照) ゲスト オペレーティング システムをインストールしたり、ブート可能な復旧 VCD から VM を起動できるようになります。稼働中の VM に VCD を挿入して ([「仮想 CD を挿入する」](#)を参照) ソフトウェア アプリケーションをインストールすることもできます。

注:






1. 定期的に使用する VCD を除いて、不要になった VCD は削除してください。
2. インストール用にブート可能な VCD を作成する場合、これは単一の CD または DVD でなければなりません。複数の CD または DVD はサポートされていません。

VCD を作成するには

1. 必要に応じて、VCD を作成するすべての物理メディアの ISO ファイルを作成します。
2. ztC Edge コンソールで **[仮想 CD]** ページを開きます。
3. **[VCD の作成]** をクリックして**仮想 CD の作成ウィザード**を開きます。
4. VCD の名前を入力します。
5. 次から VCD のソースを 1 つ選択します。
 - **[ISO ファイルのアップロード]** は、ztC Edge コンソールを実行しているシステムからファイルをアップロードします。**[参照]** をクリックしてシステム上の ISO ファイルを選択し、**[開く]** をクリックします。
 - **[ネットワーク ソースから CD ISO をコピーする]** は、ファイルを Web URL からコピーします。ISO ファイルの URL を指定します。
6. **[完了]** をクリックして、アップロードするか、指定のソースから ISO ファイルをコピーします。

仮想 CD の作成ウィザードにアップロードの進捗状況が表示されます。

VCD のステータスは、**[仮想 CD]** ページの **[状態]** 列で確認できます。

- 同期中のアイコン () は、VCD がまだ作成中であることを示します。
- 破損のアイコン () は、VCD の作成に失敗したことを示します。VCD を削除してから、作成を再試行してください。
- 正常のアイコン () は、転送が完了し VCD を使用する準備が整ったことを示します。

関連トピック

[「仮想 CD を挿入する」](#)

[「仮想 CD を取り出す」](#)

[「仮想 CD を管理する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

仮想 CD を挿入する

仮想 CD (VCD) を仮想マシン (VM) に挿入して、ゲスト オペレーティング システムでのアプリケーションのインストール時にインストール メディアにアクセスします。(USB デバイスを接続するには、[「仮想マシンに USB デバイスを接続する」](#)を参照してください。仮想マシンを VCD からブートするには、[「仮想 CD からブートする」](#)を参照してください。)



注意事項: 稼働中の VM に VCD を挿入すると、障害が発生した場合に Stratus Redundant Linux ソフトウェアが VM を別の物理マシンにマイグレーションすることができなくなります。冗長性を復元するには、VCD の使用が完了した時点で直ちに VCD をアンマウントし、取り外してください。



注: デフォルトでは、VCD の VM への挿入が有効にされています。この構成を変更するには、「[VM デバイスを構成する](#)」を参照してください。

VCD を VM に接続するには

1. 必要に応じて、アクセスが必要なソフトウェアのインストール メディアとして VCD を作成できます (「[仮想 CD を作成する](#)」を参照)。
2. **[仮想マシン]** ページで、VM を選択します。
3. 下部パネルで **[CD ドライブと USB デバイス]** タブをクリックします。
4. **[CD の挿入]** をクリックして VCD を選択します。プルダウン メニューが表示された場合はこれを終了します。

システムが VCD を挿入すると、その名前が **CD-ROM** の右に表示されます。

関連トピック

[「仮想 CD を作成する」](#)

[「仮想 CD を取り出す」](#)

[「仮想 CD からブートする」](#)

[「仮想 CD を管理する」](#)

仮想 CD を取り出す

仮想 CD (VCD) を取り出して、VCD を仮想マシン (VM) から切断します。VCD を取り出すと、その VM に別の VCD を挿入できるようになります。また、取り出した VCD を他の VM に挿入することもできます。

VM から VCD を取り出すには

1. ゲスト オペレーティング システムから VCD をアンマウントして、その使用を確実に停止します。

2. **[仮想マシン]** ページで、VM を選択します。
3. 下部パネルにある **[CD ドライブと USB デバイス]** タブをクリックします。
4. **[CD ドライブ]** タブで **[CD の取り出し]** をクリックします。

関連トピック

[「仮想 CD を作成する」](#)

[「仮想 CD を挿入する」](#)

[「仮想 CD からブートする」](#)

[「仮想 CD を管理する」](#)

仮想 CD からブートする

仮想マシンを仮想 CD (VCD) からブートして、ゲスト オペレーティング システムをインストールしたり、メンテナンスを実行します。

VCD からブートするには、その前に仮想マシンをシャットダウンする必要があります。

VCD から仮想マシンをブートするには

1. 必要な場合はブート可能な CD/DVD から VCD を作成します ([「仮想 CD を作成する」](#) を参照)。
2. **[仮想マシン]** ページで、仮想マシンを選択します。
3. 仮想マシンが実行中の場合、**[シャットダウン]** をクリックします。
4. 仮想マシンのステータスが「**停止**」になったら、下部パネルで **[CD からブート]** をクリックします。
5. ブート可能な VCD を選択して **[ブート]** をクリックします。



注: VCD からブートされた Windows ベースの仮想マシンは、ハードウェア仮想マシン (HVM) としてブートされ、最初の 3 つのディスク ボリュームのみにアクセスできます。

関連トピック

[「仮想 CD を作成する」](#)

[「仮想 CD を挿入する」](#)

[「仮想 CD を取り出す」](#)

[「仮想 CD を管理する」](#)

[「仮想マシンを作成/マイグレーションする」](#)

[「仮想マシンの運用を管理する」](#)

仮想 CD の名前を変更する

仮想 CD (VCD) の名前を変更します。VCD の名前は **[仮想 CD]** ページに表示されます。

VCD の名前を変更するには

1. **[仮想 CD]** ページで、VCD を見つけます。
2. VCD の名前をダブルクリックします。
3. 新しい名前を指定して **Enter** キーを押します。

関連トピック

[「仮想 CD を削除する」](#)

[「仮想 CD を挿入する」](#)

[「仮想 CD を取り出す」](#)

[「仮想 CD を作成する」](#)

[「仮想 CD を管理する」](#)

仮想 CD をダウンロードする

仮想 CD (VCD) をダウンロードして、VCD 上のソフトウェアを後日アップロードできるようにします。



前提条件: まだ行っていない場合は、まず VCD を作成する必要があります。 [「仮想 CD を作成する」](#) を参照してください。

VCD をダウンロードするには

1. ztC Edge コンソールで **[仮想 CD]** ページを開きます。
2. ダウンロードする VCD の名前をクリックします。
3. **[ダウンロード]** をクリックします。ウィンドウが開き、ローカル コンピュータ上のフォルダが表示されます。
4. ファイルの保存先を選択し、**[保存]** をクリックします。

ファイルのサイズによってはダウンロードが完了するまで数分かかります。

関連トピック

[「仮想 CD を管理する」](#)

仮想 CD を削除する

ztC Edge システムから仮想 CD (VCD) を永久に削除するには、VCD の削除を行います。

VCD を削除するには

1. ztC Edge コンソールで、**[仮想 CD]** をクリックします。
2. リストで削除する VCD を見つけます。
3. VCD の **[削除可能]** 列が **[はい]** になっていることを確認します。値が **[いいえ]** の VCD は現在使用中です。
4. VCD を選択して下部パネルで **[削除]** をクリックします。

関連トピック

[「仮想 CD の名前を変更する」](#)

[「仮想 CD を挿入する」](#)

[「仮想 CD を取り出す」](#)

[「仮想 CD を作成する」](#)

[「仮想 CD を管理する」](#)

高度なトピック (仮想マシン)

次のトピックでは、上級ユーザのための手順と情報を説明します。

- 「仮想マシンに特定の MAC アドレスを割り当てる」
- 「仮想マシンの優先 PM を選択する」
- 「VM を強制的にブートする」
- 「仮想マシンの保護レベルを変更する (HA または FT)」
- 「仮想マシンのブートシーケンスを構成する」
- 「故障した仮想マシンの MTBF をリセットする」
- 「仮想マシンに USB デバイスを接続する」

仮想マシンの運用を管理するには、「[仮想マシンの運用を管理する](#)」を参照してください。

仮想マシンに特定の MAC アドレスを割り当てる

仮想マシン (VM) のデフォルトのメディア アクセス制御 (MAC) アドレスをオーバーライドするには、VM に特定の MAC アドレスを割り当てます。

警告:



1. デフォルトでは Stratus Redundant Linux ソフトウェアが VM の MAC アドレスを自動的に割り当てます。特定の必要条件がある場合 (たとえば MAC アドレスに基づいてライセンスされているソフトウェア アプリケーションをサポートする場合など) を除き、デフォルト設定をオーバーライドしないでください。
2. **[静的なシステム IP]** のアドレスを変更する場合、VM がリブートすると、VM に自動で割り当てられているすべての MAC アドレスが変更されます。これは、Stratus Redundant Linux ソフトウェアがシステム IP アドレスに基づいて VM の MAC アドレスを生成するためです。VM の MAC アドレスが変更されないようにするには、下記の手順に従って固定 MAC アドレスを設定します。お使いの環境に有効な MAC アドレスを生成するには、担当のネットワーク管理者に連絡してください。また、新しい MAC アドレスに基づいてファイアウォール ルールを適宜更新することも忘れないでください。



前提条件: 仮想マシンの MAC アドレスを上書きする前に、その VM をシャットダウンする必要があります。

VM に特定の MAC アドレスを割り当てるには

1. **[仮想マシン]** ページを開きます ([「\[仮想マシン\] ページ」](#) を参照してください)。
2. VM を選択して **[シャットダウン]** をクリックします。
3. VM が停止したら、**[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを表示します。
4. ウィザードの各ページで **[次へ]** をクリックして、**[ネットワーク]** ページに進みます。(必要な場合、[「仮想マシンのリソースを再プロビジョニングする」](#) を参照し、追加の VM リソースを構成します。)
5. **[ネットワーク]** ページで、変更するネットワークを見つけ、必要に応じて元に戻せるように、その現在の MAC アドレスをメモします。
6. **[MAC アドレス]** 列に新しいアドレスを入力するか、Stratus Redundant Linux ソフトウェアによって MAC アドレスを自動で割り当てるには、テキスト領域を空白のままにします。
7. **[完了]** をクリックします。

関連トピック

[「高度なトピック \(仮想マシン\)」](#)

[「仮想マシンのリソースを管理する」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンの優先 PM を選択する

2 つのノードで構成されているシステムの場合、仮想マシンが ztC Edge システム内の特定の物理マシンで実行されるようにするには、優先物理マシンを選択します。



注: デフォルトでは、システムが仮想マシンの負荷を 2 台の物理マシンに自動で分散させます。負荷分散に特定の要件が課される場合を除き、この設定は変更しないでください。

優先物理マシンを選択するには

1. **[仮想マシン]** ページで、仮想マシンを選択します。
2. 下部パネルで **[負荷分散]** タブをクリックします。
3. ドロップダウン リストから、優先させるマシンを選択し、**[保存]** をクリックします。

関連トピック

[「高度なトピック \(仮想マシン\)」](#)

[「仮想マシンの運用を管理する」](#)

VM を強制的にブートする

[仮想マシン] ページの **[ブートの強制]** ボタンを使用して、VM を強制的にブートすることができます。ただし、**[ブートの強制]** ボタンがアクティブになるのは、ztC Edge コンソールにパートナー ノードが電源オフまたはアクセス不可の状態にあることが報告されている場合のみです。**[ブートの強制]** を使用して VM をオンラインにする際は、データを保護するためのシステムの安全チェックを手動でバイパスするため、**[ブートの強制]** の使用にあたっては細心の注意を払い、その条件と影響について完全に理解しておく必要があります。



注意事項: **[ブートの強制]** を使用する前に、このトピック全体をよく読んで、Stratus 認定サービス業者までお問い合わせください。サービス業者は、お使いのシステムについて最後のボリューム同期日時などの詳細な情報を確認し、**[ブートの強制]** がもたらす影響のすべてについて詳しく説明することができます。その後、担当のサービス業者と協議したうえで VM の強制ブートを行うかどうかを決定してください。

[ブートの強制] を使って VM を強制的にオンラインにする際は、VM のブートを強制するノード (これはアクセス可能なノードです) を選択します。データの実際の状態 (たとえば、データの状態、前回の同期、ボリュームの状態など) とは関係なく、そのノードの全データが有効としてマークされます。

[ブートの強制] の処理中、VM のボリュームにはその強制ブート処理が開始された日時を示すタグが付けられます。VM の AX コンポーネント (VM の AX ペア) は、VM のボリューム上のデータを使用してそのデータの状態を通信し、どの AX に最新のボリューム情報が含まれているかを判断します。**[ブートの強制]** 処理は、スプリットブレイン状態での実行から VM を保護するための組み込みロジックをオーバーライドします。AX ペアが通信できない場合、スプリット ブレイン状態が発生してデータの整合性が失われます (スプリットブレイン状態の詳細については、[「ALSR 構成を作成する」](#)を参照してください)。

警告: 次の状況では **[ブートの強制]** を使用しないでください。



- 1 つ以上のボリュームが **[ブートの強制]** を実行するノード上にある未完了のミラー コピーのターゲットである。
- 未完了のミラー コピーのターゲットが良好でなく、**[ブートの強制]** を使用しても利用可能にならない。
- ボリュームが同期されていない。次にその例を 2 つ示します。
 - VM の AX の両方が VM のすべてのデータ ボリュームにアクセスを必要とする。
 - 複数のボリュームをもつシステム上で、VM がそのすべてのボリュームにアクセスするには、両方の AX が実行されている必要がある。これは、各ノードが別のボリュームの緑のチェックマークが付いたコピーをもち、もう片方のノード上にあるボリュームのミラー コピーに緑のチェックマークが付いていないために起こります。
- 複数の VM が劣化していて、反対側のノードで緑のチェックマークが付いている (たとえば、node0 ではブート ボリュームが良好でデータ ボリュームは不良であり、node1 ではブート ボリュームが不良でデータ ボリュームは良好である場合など) ために、両方のノードが必要である。
- システムが 1 つのノードで構成されている。

古いボリュームのあるシステムで **[ブートの強制]** を実行する場合には、Stratus 認定サービス業者まで直ちに連絡してください。両方のノードで電源がオンになりデータの同期が開始されている場合、システムは強制ブートした VM からのデータを使用するため、アクセス不可だったノード上のデータは復旧できません。

ただし、状況によっては、古いボリュームをもつシステムで **[ブートの強制]** を使用した後にデータを復旧することも可能です。

- アクセス不可のノードの電源がまだオフになっている場合は、電源をオンにしないでください。
- **[ブートの強制]** をクリックする前にアクセス不可のノードの電源をオフにした場合は、電源オフのノード上で VM の AX が維持され、以下の条件下ではデータを失わずに **[ブートの強制]** を元に戻すことができます。

- ブートを強制した VM に新しいデータがない (つまり、VM をまだ稼働していない) 場合。
- VM のブートを強制する前に、アクセス不可のノードにある VM の AX が、ブートを強制する VM の AX とステータスを交換しなかった場合。
- アクセス不可のノードにある VM の AX のブートを阻止している問題が解決した場合。
- 2 ノード間のすべての VM データが正しく同期されている場合。システムには、各 VM の 2 つの AX コンポーネントにおいて、一方のノードの VM の AX のデータが、もう片方のノードの VM の AX のデータと異なる状態にあるような VM がありません。

お使いのシステムがこれらすべての条件を満たしている場合、Stratus 認定サービス業者に連絡し、復旧プロセスについてのヘルプを依頼してください。

VM の強制ブートを行うことに決定した場合、前提条件となる手順を必ず実行して適切な準備を行ってください。

前提条件:



- すべてのボリュームを手動でチェックして、これらをオーバーライドしても安全であることを確認します。たとえば、ボリュームに緑のチェックマークが付いていて、ディスクの同期が完了している必要があります。
- VM の両方の AX コンポーネントが通信可能で、システム プロセスによる各ボリュームの状態の判定を許可できるかどうかを判定します。スプリット ブレーン状態を回避するには、VM の 2 つの AX コンポーネントが状態を通信でき、良好なデータ ボリュームと良好なブート ボリュームをもつのがどちらの AX かを判断できることが確実でなければなりません。
- システムが 2 つのノードで構成されていることを確認します。
- Stratus 認定サービス業者に連絡してください。

VM を強制的にブートするには

Stratus 認定サービス業者と協議したうえで VM の強制ブートを決定した場合、以下の手順を実行してください。この例では、node0 がオフライン、node1 がプライマリ、VM-1 が停止中であると仮定します。

1. 2 つのノードで構成されているシステムの ztC Edge コンソールで、左側のパネルにある **[仮想マシン]** をクリックします。
2. **[仮想マシン]** ページに移動します。
3. **[仮想マシン]** ページで、ブートを強制する停止中の VM を選択します (例: VM-1)。

4. 下部パネルで **[起動]** ボタンをクリックします。

VM のブートが開始されます。タイムアウト期限に達するまで最大 5 分間、ブート処理が継続します。タイムアウト期限が経過すると、**[ブートの強制]** ボタンがアクティブになります。

5. VM のブートを強制するには、**[ブートの強制]** をクリックします。

警告が表示され、最新の VM データが保存されているノードを確実に特定できるかどうか確認されます。また、データが失われる可能性があることを示す警告も表示されます。さらに、VM のブートを強制できるノードを知らせるメッセージが表示されます。



注意事項: **[ブートの強制]** を行うときに誤ったノードを選択すると、データが破損されます。

ノードはメッセージに示されているとおりに入力する必要があります (node0 または node1)。次にメッセージの例を示します。

ブートの強制 VM-1



最新の VM データがどちらのノードに保存されているかが
確実な場合のみ、操作を続行してください。データが
失われる可能性があります。

ブートを強制できるのは node1 だけです。

node1 の VM をブートするには、"**node1**" と入力します。

[OK ボタン]

[キャンセル ボタン]

6. **[OK]** をクリックして、ノード (たとえば node1) を強制的にブートします。(キャンセルするには **[キャンセル]** をクリックします。) 強制ブートのプロセスが開始されます。VM が起動してデータが有効であることがシステムにマークされるまでの間、追加の確認メッセージが表示されます。

VM が稼働し始めます。**[仮想マシン]** ページに、VM が警告付きで表示されます。これは、ノード (たとえば node0) がまだオフラインになっているためです。

セカンダリ ノードがシステムに復帰すると、VM を実行しているノードからすべてのデータが同期されます。この例では、すべてのデータが node1 から node0 に同期されます。

関連トピック

[「高度なトピック \(仮想マシン\)」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンの保護レベルを変更する (HA または FT)

ゲスト VM の保護レベルを高可用性 (HA) からフォールトトレランス (FT)、または FT から HA に変更できます。

保護レベルを変更するには

1. **[仮想マシン]** ページで、停止している (つまり **[アクティビティ]** 列に「停止」とマークされている) VM を選択します。(VM の停止の詳細については、[「仮想マシンをシャットダウンする」](#)を参照してください。)
2. 下部パネルで **[構成]** をクリックして**仮想マシンの再プロビジョニング** ウィザードを開きます。
3. **[名前、説明および保護]** ページで、**[HA]** ボタンか **[FT]** ボタンを選択します。
4. クリックしてウィザードの最後のページまで進みます。**[完了]** をクリックし、(再構成が成功した場合は) **[OK]** をクリックします。

関連トピック

[「運用モード」](#) (HA または FT)

[「高度なトピック \(仮想マシン\)」](#)

[「仮想マシンの運用を管理する」](#)

仮想マシンのブート シーケンスを構成する

仮想マシンのブート シーケンスを構成して、ztC Edge システムにおけるゲスト オペレーティング システムおよびアプリケーションの起動順序を設定します。

まず必須のブート シーケンスを決定してから、それに応じて各仮想マシンのブート設定を構成します。

仮想マシンのブート シーケンスを設定するには

1. **[仮想マシン]** ページで、仮想マシンを選択します。
2. 下部パネルで **[ブート シーケンス]** タブをクリックします。

3. 以下の説明に従ってブート設定を構成します。

4. **[保存]** をクリックします。

ブート設定は次のとおりです。

- **[優先度グループ]** を使用して、ztC Edge システムに電源を投入した後や、VM の再起動が必要となるフェールオーバーの後の、仮想マシンのブート順序を指定できます。一部のビジネスソリューションでは、他の VM を起動する前に、特定の VM を作動させなければならない場合があります。優先度がもっとも高いのはグループ「1」で、もっとも低いのが「なし」です。Stratus Redundant Linux ソフトウェアは、**OS およびアプリケーションの起動時間**が経過するまで待つから、次の優先度グループに含まれる仮想マシンを起動します。

ブートシーケンスの例:

VM	優先度グループ	OS およびアプリケーションの起動時間
DNS	1	2 分
App	2	30 秒
DB	2	10 分
Web	3	0

- 1 ztC Edge が DNS VM をブートします。
- 2 ztC Edge は、DNS VM が起動した 2 分後に、グループ 2 の App サーバおよび DB サーバを起動します。
- 3 ztC Edge は、DB VM が起動した 10 分後に、グループ 3 の Web VM を起動します。

- **[OS およびアプリケーションの起動時間]** には、仮想マシンが起動してから、ゲスト オペレーティング システムとアプリケーションが完全な動作状態になるまでの所要時間を設定します。

関連トピック

[「高度なトピック \(仮想マシン\)」](#)

[「仮想マシンの運用を管理する」](#)

故障した仮想マシンの MTBF をリセットする

仮想マシンの平均故障間隔 (MTBF) カウンタをリセットして、故障した仮想マシンの再起動を試行します。

仮想マシンのゲスト OS がクラッシュした場合、ztC Edge は、その MTBF しきい値を下回る場合を除き、OS を自動的に再起動します。仮想マシンが MTBF のしきい値を下回る場合、ztC Edge はそのマシンをクラッシュした状態のまま維持します。必要な場合は MTBF カウンタをリセットして、仮想マシンを再起動できます。



注意事項: Stratus 認定サービス業者から指示を受けた場合を除き、MTBF カウンタはリセットしないでください。リセットを行うと、システムのフォールトトレランスに影響することがあります。

注:



1. **[デバイスのリセット]** ボタンは、仮想マシンがその MTBF しきい値に満たない場合にのみ表示されます。
2. **[MTBF のクリア]** ボタンは、1 台の物理マシンで VM をサポートしているシステムソフトウェアが、その MTBF しきい値に満たない場合にのみ表示されます。

仮想マシンの MTBF カウンタをリセットするには

1. **[仮想マシン]** ページで、仮想マシンを選択します。
2. **[デバイスのリセット]** をクリックします。

一方の物理マシンで VM をサポートしているシステムソフトウェアで、あまり多くの障害が発生する場合、以下の手順に従ってその MTBF カウンタをリセットします。

1 台の物理マシン上の VM の MTBF カウンタをリセットするには

1. **[仮想マシン]** ページで、仮想マシンを選択します。
2. **[MTBF のクリア]** をクリックします。

関連トピック

[「高度なトピック \(仮想マシン\)」](#)

[「仮想マシンの運用を管理する」](#)

[「診断ファイルを作成する」](#)

仮想マシンに USB デバイスを接続する

USB デバイスを仮想マシン (VM) に接続して、VM がデバイスを使用できるようにします。たとえば、ゲストオペレーティングシステムにアプリケーションをインストールするために USB ベースのライセンスが要求される場合などは、USB デバイスが必要です。USB デバイスが不要になったらデバイスを切断します。

(USB デバイスを使用して VM のエクスポートやインポートを行うために、そのデバイスを ztC Edge システムにマウントする必要がある場合、[「ztC Edge システム上の USB デバイスまたはネットワークマウントフォルダをマウントする」](#)を参照してください。)

注意事項:



稼働中のフォールトトレラント (FT) VM に USB デバイスを接続すると、障害が発生した場合に Stratus Redundant Linux ソフトウェアが VM を別の物理マシンにマイグレーションすることができなくなります。フォールトトレラント運用を復元するには、USB デバイスの使用が完了した時点で直ちにデバイスを切断し、取り外してください。

注:

1. ゲスト オペレーティング システムには、サポートされている USB デバイスのみを接続できます。ztC Edge システムでサポートされる USB デバイスのリストについては、「[システム仕様](#)」を参照してください。

ztC Edge システムは、ゲスト オペレーティング システムで USB 3.2 Gen 2 (10 Gbps) またはそれ以上のデバイスをサポートしないことに注意してください。ここで Gen 2 またはそれ以上のデバイスを USB 3.2 Gen 1 (5 Gbps) 1 ホスト ポートに挿入することはできますが、デバイスは Gen 1 (5 Gbps) の速度で稼働します。この場合、デバイスをゲスト オペレーティング システムに接続できます。(USB 3.2 Gen 1 (5 Gbps) デバイスは以前 USB 3.1 Gen 1 デバイスと呼ばれ、USB 3.2 Gen 2 (10 Gbps) デバイスは USB 3.1 Gen 2 デバイスと呼ばれていました。)

2. USB 接続 SCSI (UAS) 準拠のデバイスを VM に接続しないでください。システムでは UAS デバイスがサポートされません。



3. USB デバイスを接続するには、その VM が稼働していなければなりません。
4. デフォルトでは、USB デバイスの VM 接続は有効にされています。この構成を変更するには、「[VM デバイスを構成する](#)」を参照してください。
5. サポートされる USB デバイスを Windows ベースの VM から切断する (つまり取り出す) には、次のいずれかの方法を使用します。
 - エクスプローラーで [Eject (取り出し)] をクリックする — エクスプローラーからデバイスを取り出す場合、ztC Edge コンソールで下記の手順を使用して切断する必要があります。その後、ztC Edge システムから物理的に取り除き、同じ VM や別の VM に再接続する前に、挿入し直さなければなりません。
 - タスクバーで [ハードウェアの安全な取り外し] および [メディアの取り出し] をクリックする — タスクバーからデバイスを取り出す場合、ztC Edge コンソールで下記の手順を使用して切断する必要があります。同じ VM や別の VM に再接続する前に ztC Edge システムから物理的に取り除く必要はありません。

USB デバイスを VM に接続するには

1. USB デバイスを VM のプライマリ (アクティブ) ノードに挿入します。

[**仮想マシン**] ページに、各 VM のプライマリ ノードが [**現行 PM**] として表示されます。(このノードは、[**物理マシン**] ページに表示される ztC Edge システムの現在のプライマリ ノードとは異なる場合があります。)

システムに USB デバイスが表示されることを確認します。[**物理マシン**] ページに移動します。デバイスを挿入したノードをクリックして、下部パネルで [**USB デバイス**] タブを選択します。挿入した USB デバイスがタブに表示されることを確認します。

2. [**仮想マシン**] ページで、VM を選択します。
3. 下部パネルで [**CD ドライブと USB デバイス**] タブをクリックします。
4. [**CD ドライブと USB デバイス**] タブの [**USB**] 行で、プルダウン メニューから USB デバイスを選択します。
5. [**USB の接続**] をクリックして、VM に USB デバイスを接続します。
6. [**確認**] ダイアログ ボックスが表示され、デバイスの接続を確認するメッセージと、USB デバイスの使用中はゲストがシンプレックス モードになることを示す警告が表示されます。[**はい**] をクリックしてデバイスを接続します。

システムが VM に USB デバイスを接続すると、[**CD ドライブと USB デバイス**] タブで、その VM の USB デバイスのリストに USB デバイスの名前が表示されるようになります。

USB デバイスを VM から切断するには

1. [**仮想マシン**] ページで、USB デバイスが接続されている VM を選択します。
2. 下部パネルで [**CD ドライブと USB デバイス**] タブをクリックします。
3. [**CD ドライブと USB デバイス**] タブの [**USB**] 行で、[**USB デバイスの切断**] をクリックします。必要な場合、プルダウン メニューから USB デバイスを選択します。
4. [**確認**] ダイアログ ボックスが開き、デバイスの切断を確認するメッセージが表示されます。[**はい**] をクリックしてデバイスを切断します。

システムが VM から USB デバイスを切断すると、[**CD ドライブと USB デバイス**] タブで、その VM の USB デバイスのリストに USB デバイスの名前が表示されなくなります。

関連トピック

[「仮想マシンを管理する」](#)

7

第 7 章: 物理マシンのメンテナンスを行う

ztC Edge システム内の物理マシン (PM) つまりノードのメンテナンスを行うには、これを交換するか復旧します。

故障した PM を交換するには、次のいずれかの手順を使用します。

- [「物理マシンを交換する \(自動\)」](#) (推奨)

自動ノード交換プロセスを使用して故障した PM を交換する方法について説明します。このヘルプ トピックは、各交換ノードに付属している『[ztC Edge 100i/110i システム: ノードを交換する \(R013Z\)](#)』または『[ztC Edge 200i/250i システム: ノードを交換する \(R019Z\)](#)』の情報を補足するものです。

- [「物理マシンを交換する \(手動\)」](#)

ユーザによる手動交換プロセスを使用して故障した PM を交換する方法について説明します。この操作は ztC Edge コンソールから開始して監視します。Stratus 認定サービス業者から特に指示を受けた場合を除き、ユーザによる手動プロセスは使用しないでください。

PM のハードウェアを交換する代わりに故障した PM のシステム ソフトウェアを復旧するには、[「故障した物理マシンを復旧する \(手動\)」](#)を参照してください。

1 つのノードで構成されているシステムにノードを追加するには、[「単一ノードシステムにノードを追加する」](#)を参照してください。

物理マシンを交換する (自動)

このトピックでは、自動ノード交換プロセスを使用してデュアルノードの ztC Edge システムで故障した物理マシン (PM)、つまりノードを交換する方法について説明します。これは、お使いのシステム用の「[ノードを交換するためのガイド](#)」にある情報を補足するものです。

システムの実行中にデュアルノード システム内の 1 つのノードを交換します。

前提条件: 交換 ztC Edge ノードをリクエストするには、**Stratus カスタマ サービス ポータル**にログインし、**[Customer Support (カスタマ サポート)]**を展開して**[Add Issue (問題の追加)]**をクリックします。問題を作成する場合、次の情報を準備してください。



- **Asset ID (アセット ID)** — ztC Edge コンソール ウィンドウのマストヘッドにあるシステムの **[アセット ID]**を確認します。
- **診断ファイル** — ztC Edge コンソールの **[サポート ログ]** ページで診断ファイルを生成してダウンロードします。**「診断ファイルを作成する」**を参照してください。サービスポータルで追加する問題に診断ファイルを添付します。

問題を診断して必要な場合は交換ノードを提供するために弊社のカスタマ サービス担当者から連絡を差し上げます。



前提条件: 交換用のノードは、工場出荷時の状態でリリース 2.3 以降がインストールされており、正常に稼働しているノードと同じモデルである必要があります。廃止されたシステムからの既存のノードや、以前のソフトウェア リリースでインストールされたノードを使用する必要がある場合は、展開する前にノードを工場出荷時の状態にリセットする必要があります。必要な場合は、担当の Stratus 認定サービス業者にヘルプを依頼してください。

ztC Edge システム内のノードを交換するには

1. 交換するノードの位置を確認します。障害のあるノードは電源が (自動で) オフにされるか、電源がオンで SYS LED がオフまたは緑あるいは黄色 (非正常) に点灯しています。ノードの電源が既にオフになっている場合はステップ 3 に進みます。
2. 障害のあるノードの電源がオンになっている場合、ztC Edge コンソールを開いてシャットダウンを妨げている問題を解決します。たとえば、正常なノード上でエラーとなったネットワーク接続は、障害のあるノードへの依存の原因となり得ます。問題をすべて解決して障害のあるノードをシャットダウンします。
3. 障害のあるノードから電源ケーブルを切断し、次にネットワーク ケーブルを切断してシステムからノードを取り除きます。
4. システムに交換ノードを追加します。ネットワーク ケーブルを差し込み直し、電源を再接続してノードを自動的に電源オンにします。これでノードの交換が完了します。ユーザによる入力なしでシステムが同期を開始します。

5. 20 分後に SYS LED がオフから緑または黄色の点灯に切り替わり、交換ノード上のソフトウェアが起動したことを示します。さらに 15 分後、SYS LED が点滅し始めてシステムが正常であることを示します。
6. ztC Edge コンソールにログオンしてシステムの正常性を確認します。仮想マシンの同期には数時間かかる場合があります。同期が正常に完了すると、未解決の問題がないことを示す緑のチェックマークが **[ダッシュボード]** に表示されます。
7. 必要に応じて、ztC Edge システムの製品ライセンスを再アクティベートすることで、交換用のノードをアクティベートしてください。ライセンスのアクティベーションを自動で行うには、**[基本設定]** ページで **[製品ライセンス]**、**[ライセンスを今すぐチェック]** の順にクリックします。システムがインターネットにアクセスできない場合は、**「製品ライセンスを管理する」** の説明に従ってライセンスをアクティベートしてください。



注: 新しいノードは、ztC Edge ライセンスを再アクティベーションしない限り、メンテナンス モードを終了して VM を実行することができません。

8. 必要に応じて、交換したノードをオンラインに戻す準備が完了したら、**[最終処理]** をクリックしてメンテナンス モードを終了します。両方の PM が「**実行中**」の状態に戻り、ノードの同期が完了することを確認します。

ノードを交換するためのガイド

ztC Edge 100i/110i システム: [ノードを交換する \(R013Z\)](#)

ztC Edge 200i/250i システム: [ノードを交換する \(R019Z\)](#)

関連トピック

[「メンテナンス モード」](#)

[「物理マシンのメンテナンスを行う」](#)

[「ztC Edge コンソール」](#)

[「物理マシンと仮想マシン」](#)

[「\[物理マシン\] ページ」](#)

物理マシンを交換する (手動)



注意事項: ztC Edge システム内の 1 台の PM を復旧または交換する必要がある場合、『ztC Edge 100i/110i システム: ノードを交換する (R013Z)』または『ztC Edge 200i/250i システム: ノードを交換する (R019Z)』の手順を使用してください。(必要な場合、『物理マシンを交換する (自動)』を参照してください。) Stratus 認定サービス業者から特に指示を受けた場合を除き、このトピックに記載されている手動の手順は使用しないでください。

システムの実行中にデュアルノードの ztC Edge システム内の 1 つの物理マシン (PM)、つまりノードを交換します。(PM のハードウェアを交換する代わりに、故障した PM のシステム ソフトウェアを復旧する必要がある場合、『故障した物理マシンを復旧する (手動)』を参照してください。)

PM を削除して交換する場合、システムは Stratus Redundant Linux システム ソフトウェアの完全インストールを行う準備として、交換 PM にあるすべてのディスクを完全に消去します。ソフトウェアをインストールするには、システムが交換ノードをプライマリ PM 上の一時的な Preboot Execution Environment (PXE) サーバから自動的にブートできるように設定します。各 PM に一番最近インストールされたソフトウェアキットの完全なコピー (ztC Edge コンソールの [アップグレード キット] ページに記載) が含まれている限り、PXE ブート インストールを使ってどちらの PM からでもそのパートナー PM の交換を開始できます。必要な場合、交換ノードを USB インストール メディアから手動でブートすることもできます。

インストールに使用するメディアに応じて、**PXE** または **USB** インストールのいずれかの手順を使用します。



注意事項: 交換手順を行うと、PM のホスト オペレーティング システムにインストールされている全ソフトウェアと、交換前に入力したすべての PM 構成情報が削除されます。この手順を完了した後は、ホストレベルの全ソフトウェアを手動で再インストールして、元の設定に一致するよう PM を再構成する必要があります。



注意事項: データの損失を避けるため、ディスク ミラーのアセンブリに手動の操作が必要なことがシステム ログに示されている場合には、Stratus 認定サービス業者に連絡してヘルプを依頼してください。再同期を強制的に行ってミラー内の一番新しいディスクを上書きすると、貴重なデータが失われる可能性があります。

前提条件: 交換 ztC Edge ノードをリクエストするには、**Stratus カスタマ サービス ポータル**にログインし、**[Customer Support (カスタマ サポート)]**を展開して**[Add Issue (問題の追加)]**をクリックします。問題を作成する場合、次の情報を準備してください。



- **Asset ID (アセット ID)** – ztC Edge コンソール ウィンドウのマストヘッドにあるシステムの**[アセット ID]**を確認します。
- **診断ファイル** – ztC Edge コンソールの**[サポート ログ]**ページで診断ファイルを生成してダウンロードします。**「診断ファイルを作成する」**を参照してください。サービスポータルで追加する問題に診断ファイルを添付します。

問題を診断して必要な場合は交換ノードを提供するために弊社のカスタマ サービス担当者から連絡を差し上げます。



前提条件: 交換用のノードは、工場出荷時の状態でリリース 2.3 以降がインストールされており、正常に稼働しているノードと同じモデルである必要があります。廃止されたシステムからの既存のノードや、以前のソフトウェア リリースでインストールされたノードを使用する必要がある場合は、展開する前にノードを工場出荷時の状態にリセットする必要があります。必要な場合は、担当の Stratus 認定サービス業者にヘルプを依頼してください。



前提条件: USB メディアを使って交換 PM にシステム ソフトウェアをインストールする場合

- ブート可能な USB メディアを作成します。手順は、**「システム ソフトウェアの USB メディアを作成する」**を参照してください。

USB メディアを作成する際は、必ず一番最後にインストールしたアップグレード キットを含めてください。たとえば、ztC Edge コンソール ウィンドウのマストヘッドに表示されたリリースが 1.2.0-550 である場合、550 がビルド番号となり、**[アップグレード キット]**ページで USB メディアの作成用に選択するキットのバージョンは 1.2.0-550 にする必要があります。システムで交換 PM 上に異なるビルドが検出された場合、ユーザ操作なしで自動的に交換プロセスが再開され、交換 PM 上のすべてのデータを初期化して、PXE ブート インストールを使って一番最近インストールされたソフトウェア キットが PM に再インストールされます。

- キーボードとモニタを交換 PM に接続してインストール手順を監視し、設定を指定します。

注:

PM の交換後は ztC Edge システムの製品ライセンスを再度アクティベートする必要があります。

故障した PM を削除して交換するには (PXE ブート インストール)

次の手順を使用して、故障した PM を交換し、プライマリ PM 上のソフトウェアキットからの PXE ブート インストールを使ってシステム ソフトウェアを再インストールします。

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
2. 作業する PM (node0 または node1) を選択して **[作業開始]** をクリックします。PM の**総合状態**が **"メンテナンス モード"** に変わり、**アクティビティ**状態が **"実行中 (メンテナンス中)"** に変わります。
3. PM が **「実行中 (メンテナンス中)」** になった後、**[リカバリ]** をクリックします。
4. 修復のタイプを選択するよう求められたら、**[PXE PM 交換 - 全ディスクの初期化]** をクリックします。



注意事項: **[PXE PM 交換 - 全ディスクの初期化]** を選択すると、交換 PM 上のすべてのデータが削除されます。

5. 次の PXE 設定のいずれかを選択します。

■ **現在のパートナー ノードからの PXE 要求のみに応答する。**

現在のパートナー ノードの MAC アドレスからの PXE ブート要求を待機します。このオプションは、既存の PM を完全にワイプして再インストールする方法で復旧する場合に選択します。この手順では PM 上の全データが削除されますが、その現在のネットワーク構成が復元されます。

■ **次の MAC アドレスからの PXE 要求のみに応答する。**

ユーザが指定する MAC アドレスからの PXE ブート要求を待機します。このオプションは、PM を新しい PM に交換する場合に選択します。PXE ブートを開始する、特定のネットワーク アダプタの MAC アドレスを入力します。

- **priv0 上のすべてのシステムからの PXE 要求を受け入れる。**

2 つの ztC Edge ノードを接続するプライベートネットワーク priv0 からの PXE ブート要求を待機します。このオプションは、PM を新しい PM に交換する場合で、新しい PM の MAC アドレスが不明な場合に選択します。

6. **[続行]** をクリックして、交換プロセスを開始します。システムが PM をシャットダウンして電源をオフにします。
7. PM の電源がオフになった後、交換 PM を必要に応じてインストールします。
 - a. 古い PM を切断して削除し、次に交換 PM をインストールします。
 - b. ネットワークケーブルを元のポートにつなぎ直してから、電源を接続します。
8. PM が自動的に電源オンにならない場合、電源ボタンを押します。
9. 交換プロセスがユーザによる操作なしで次のように続行されます。
 - 交換 PM が、プライマリ ノードで一時実行される PXE サーバからのブートを開始します。
 - システムが交換 PM のディスク上にあるすべてのデータを自動的に削除します。
 - 交換 PM がもう一度リブートし、システム ソフトウェアのインストールを自動的に開始します。これはプライマリ ノード上のインストールキットのコピーから実行されます。

交換 PM の物理コンソールでソフトウェア インストールの進捗状況を監視したり、プロンプトに応答する必要はありません。交換プロセスは自動化されており、ソフトウェアのインストール処理中 PM に空白の画面が長時間表示されるのは正常な動作です。

10. ソフトウェアのインストールが完了すると、交換 PM が新しくインストールされたシステム ソフトウェアからリブートします。



注: システム ソフトウェアのインストール後、交換 PM がシステムに結合して ztC Edge コンソールに表示されるようになるには最大 20 分かかる場合があります。

11. 交換 PM がシステムに結合する間、ztC Edge コンソールの **[物理マシン]** ページでそのアクティビティを確認できます。復旧が完了すると、**[アクティビティ]** 列の PM の状態が「**(メンテナンス中)**」として表示されます。

12. 交換 PM をアクティベートするには、ztC Edge システムの製品ライセンスの再アクティベーションを行います。ライセンスのアクティベーションを自動で行うには、**[基本設定]** ページで **[製品ライセンス]**、**[ライセンスを今すぐチェック]** の順にクリックします。システムがインターネットにアクセスできない場合は、**「製品ライセンスを管理する」** の説明に従ってライセンスをアクティベートしてください。



注: 新しい PM は、ztC Edge ライセンスを再アクティベーションしない限り、メンテナンス モードを終了して VM を実行することができません。

13. 必要に応じて、アプリケーションおよびすべてのホストレベルのソフトウェアを手動で再インストールし、元の設定に一致するよう交換 PM を再構成してください。
14. 交換した PM をオンラインに戻す準備が完了したら、**[最終処理]** をクリックしてメンテナンス モードを終了します。両方の PM が**「実行中」**の状態に戻り、PM の同期が完了することを確認します。初期の同期には、ストレージ容量や VM の数などの構成に応じて、数分から数時間かかります。



注: 交換 PM がメンテナンス モードを終了すると、システムは交換プロセスに使用したプライマリ ノード上の PXE サーバを自動的に無効にします。

故障した PM を削除して交換するには (USB インストール)

次の手順を使用して、故障した PM を交換し、USB メディアを使ってシステム ソフトウェアを再インストールします。

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
2. 作業する PM (node0 または node1) を選択して **[作業開始]** をクリックします。PM の**総合状態**が **"メンテナンス モード"** に変わり、**アクティビティ** 状態が **"実行中 (メンテナンス中)"** に変わります。
3. PM が **「実行中 (メンテナンス中)」** になった後、**[リカバリ]** をクリックします。
4. 修復のタイプを選択するよう求められたら、**[USB PM 交換 - 全ディスクの初期化]** をクリックします。



注意事項: **[USB PM 交換 - 全ディスクの初期化]** を選択すると、交換 PM 上のすべてのデータが削除されます。

5. **[続行]** をクリックして、交換プロセスを開始します。システム ソフトウェアの再インストールの準備として、システムが PM をシャットダウンします。
6. PM の電源がオフになった後、交換 PM を必要に応じてインストールします。
 - a. 古い PM を切断して削除し、次に交換 PM をインストールします。モニタとキーボードを接続します。
 - b. ネットワーク ケーブルを元のポートに接続し直します。
 - c. 交換 PM にブート可能な USB メディアを接続し、次に電源ケーブルを接続し直します。PM が自動的に電源オンにならない場合、電源ボタンを押します。
7. 交換 PM の電源がオンになったら、ファームウェア (UEFI) のセットアップ ユーティリティを起動します。**[Save & Exit (保存して終了)]** メニューの **[Boot Override (ブート オーバーライド)]** で、USB メディアに **[UEFI]** エントリを選択して、次のブート シーケンスでこのデバイスから 1 回ブートするようにします。PM が再起動します。



注: [Boot (ブート)] メニューで恒久的な **BOOT ORDER Priorities (ブート順序の優先度)** を変更する代わりに、ブート デバイスを一時的に変更するには **[Boot Override (ブート オーバーライド)]** プロパティを使用します。ztC Edge システムで通常実行されるノードの自動交換をサポートするため、最上位のブート優先度は **UEFI Network (デフォルト)** のままにする必要があります。

8. 交換 PM の物理コンソールでインストールのプロセスを監視します。
9. **[Welcome (ウェルカム)]** 画面で、矢印キーを使ってインストール用に国のキーボード マップを選択します。
10. **[インストールまたはリカバリ]** 画面で、**[Replace PM, Join system: Preserving data (PM の交換、システムの結合: データの維持)]** を選択し、**Enter** キーを押します。交換プロセスがユーザによる操作なしで続行されます。



注意事項: [Replace PM, Join system: Initialize data (PM 交換、システムの結合: データの初期化)] を選択すると、交換 PM 上のすべてのデータが削除されます。

11. ソフトウェアのインストールが完了すると、交換 PM が新しくインストールされたシステム ソフトウェアからリブートします。



注: システム ソフトウェアのインストール後、交換 PM がシステムに結合して ztC Edge コンソールに表示されるようになるには最大 20 分かかる場合があります。

12. 交換 PM がシステムに結合する間、ztC Edge コンソールの **[物理マシン]** ページでそのアクティビティを確認できます。復旧が完了すると、**[アクティビティ]** 列の PM の状態が「**(メンテナンス中)**」として表示されます。
13. 交換 PM をアクティベートするには、ztC Edge システムの製品ライセンスの再アクティベーションを行います。ライセンスのアクティベーションを自動で行うには、**[基本設定]** ページで **[製品ライセンス]**、**[ライセンスを今すぐチェック]** の順にクリックします。システムがインターネットにアクセスできない場合は、「**製品ライセンスを管理する**」の説明に従ってライセンスをアクティベートしてください。



注: 新しい PM は、ztC Edge ライセンスを再アクティベーションしない限り、メンテナンス モードを終了して VM を実行することができません。

14. 必要に応じて、アプリケーションおよびすべてのホストレベルのソフトウェアを手動で再インストールし、元の設定に一致するよう交換 PM を再構成してください。
15. 交換した PM をオンラインに戻す準備が完了したら、**[最終処理]** をクリックしてメンテナンス モードを終了します。両方の PM が「**実行中**」の状態に戻り、PM の同期が完了することを確認します。

関連トピック

[「メンテナンス モード」](#)

[「物理マシンのメンテナンスを行う」](#)

[「ztC Edge コンソール」](#)

[「物理マシンと仮想マシン」](#)

[「\[物理マシン\] ページ」](#)

8

第 8 章: システム、Windows ベースの VM、およびアプリケーションをモニタリングする

モニタリングのライセンスが適用されているシステムでは、パフォーマンスに関する情報 (たとえば CPU 使用状況など) をモニタリングすることができます。下限値と上限値を設定してモニタリングの対象となるパラメータ値の範囲を作成できます。また、パラメータの値が設定範囲を超えた場合に送信される **call-home** や **e アラート/トラップ** メッセージを設定することもできます。

以下に関する情報をモニタリングできます。

- ztC Edge システムのホスト オペレーティング システム – [「ztC Edge システムをモニタリングする」](#) を参照してください。
- Windows ベースの VM 上の Windows ベースのオペレーティング システム – [「Windows ベースの仮想マシンをモニタリングする」](#) を参照してください。
- Windows ベースの VM 上で実行しているアプリケーション – [「Windows ベースの仮想マシン上のアプリケーションをモニタリングする」](#) を参照してください。



注: システムにモニタリングのライセンスがない場合、**[モニタ]** タブの内容はグレー表示されます。この機能を有効にする方法については、アカウントの担当者までご連絡ください。

ztC Advisor (ztC Edge システムのフリート全体を一括表示できる Web ベースのセキュアなポータル) を使用したシステムの監視の詳細については、[「ztC Advisor を有効化する」](#) を参照してください。

ztC Edge システムをモニタリングする

ztC Edge システムのホスト オペレーティング システムにおける、OS パフォーマンスに関する情報 (CPU 使用状況など) をモニタリングします。モニタリング パラメータを設定すると、その後は値が 30

秒ごとに更新されます。

ホスト オペレーティング システムのモニタリングのパラメータを設定および表示するには

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[物理マシン]** をクリックします。
2. 下部パネルで **[モニタ]** タブをクリックします。
[モニタ] タブに、実行中の各ノードのモニタリング情報が表示されます。
3. 実行中の各ノードにおけるパラメータのモニタリングを有効にするには、そのパラメータの一番左の列で **[有効]** ボックスをオンにします。
4. 該当するパラメータ値を設定します。

パラメータ — **[CPU 使用]** および **[メモリ使用状況]**。表示値のため設定できません。

単位 — 比率 (%)。最大 100% です。表示値のため設定できません。

範囲:

低 — 範囲の下限值。値は 0 または正の数にできます。値は両方のノードに適用されます。

高 — 範囲の上限値。値は 0 または正の数にできます。値は **[低]** の値より大きくなければなりません。値は両方のノードに適用されます。

デフォルトでは範囲の値が空になっています。値を入力するには、パラメータ行の **[低]** または **[高]** 列のセル内の空白部分をクリックします。空白部分をクリックするとボックスが表示され、そこに値を入力できます。

call-home — どちらかのノードで範囲外の値が検知されると call-home メッセージが Stratus 認定サービス業者に送信されます。

e アラート/トラップ — どちらかのノードで範囲外の値が検知されると電子メール アラート (e アラート) と SNMP トラップが送信されます。

最初の検知 — 過去 24 時間以内に各ノードでパラメータ値が初めて検知された日付と時刻。表示値のため設定できません。

最後の検知 — 過去 24 時間以内にどちらかのノードでパラメータ値が最後に検知された日付と時刻。表示値のため設定できません。

最後のイベント — 各ノードにおける最後のしきい値違反 (**[低]** または **[高]**)。セルが空白の場合、しきい値違反が発生していないことを示します。表示値のため設定できません。

インシデント カウント — 過去 24 時間以内にどちらかのノードで範囲を超えた回数。表示値のため設定できません。

現行値 — 次のいずれかを示します (表示値のため設定できません)。

- 1 つのノードの現行値。
- **利用不可** — この値は現在利用できません。

ステータス — 1 つのノード上のパラメータのステータス。表示値のため設定できません。

- 予期値 (✓) — パラメータは過去 24 時間にその範囲を超えていません。
- 警告 (⚠) — パラメータは過去 24 時間にその範囲を超えていますが、現時点では発生が昇格されません。
- 範囲外 (✗) — 現在範囲外です。

5. **[保存]** をクリックして変更を保存するか、まだ保存していない値をキャンセルするには **[リセット]** をクリックします。

関連トピック

[「システム、Windows ベースの VM、およびアプリケーションをモニタリングする」](#)

[「e アラートを構成する」](#)

[「SNMP 設定を構成する」](#)

[「物理マシンを管理する」](#)

Windows ベースの仮想マシンをモニタリングする

Windows ベースの VM 上のオペレーティング システムについて OS パフォーマンスに関する情報 (たとえば CPU の使用状況) をモニタリングします。モニタリングは以下のオペレーティング システムを実行する VM で利用できます。

- Windows 10 Professional
- Windows 10 Enterprise
- Windows Server 2012 R2 Standard
- Windows Server 2016 Standard
- Windows Server 2019 Standard

Windows ベースの VM を作成した後、**[仮想マシン]** ページの **[モニタ]** タブでモニタリングのパラメータを表示して設定できます。モニタリング パラメータを設定すると、その後は値が 60 秒ごとに更新されます。

ゲスト モニタリング エージェントがまだインストールされていない場合は、まずこれをインストールする必要があります。

ゲスト モニタリング エージェントをインストールするには

1. ztC Edge コンソールで、**[仮想 CD]** をクリックします。
2. **guest_monitoring_agent_n.n.n.n** VCD がリストされることを確認します。
3. 左側のナビゲーション パネルで **[仮想マシン]** をクリックします。
4. **[仮想マシン]** の下で、ゲスト モニタリング エージェントをインストールする VM を選択します。
5. VCD を挿入します。 **[仮想 CD を挿入する]** を参照してください。
6. VM コンソール セッションを開きます。 **[仮想マシン コンソールのセッションを開く]** を参照してください。
7. VM コンソール セッションで、エクスプローラー ウィンドウを開いて *Monitoring Agent Installation* (モニタリング エージェントのインストール) CD に移動します。
8. CD をダブルクリックして、**Monitoring Agent Service Setup Wizard** (モニタリング エージェントサービスのセットアップ ウィザード) を開き、ウィザードで **[Next (次へ)]** をクリックします。
ウィザードがエージェントをインストールします。インストールが完了したら **[Finish (完了)]** をクリックします。
9. インストールが完了したら、VM から VCD を取り出します。 **[仮想 CD を取り出す]** を参照してください。

注:



1. VM の名前を変更するとモニタリング パラメータが非表示になりますが、1 ~ 2 分後に再び表示されます。
2. Guest Monitoring Agent (ゲスト モニタリング エージェント) によってプロセッサ、メモリ、ディスクの使用状況に関する情報を取得するには、ゲスト オペレーティング システムでパフォーマンス カウンタが有効にされ機能していることを確認する必要があります。

VM のモニタリングのパラメータを設定および表示するには

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[仮想マシン]** をクリックします。
2. 適切な VM を選択します。
3. 下部パネルで **[モニタ]** タブをクリックします。

[ゲスト OS] の下に、表示と設定が可能なパラメータを含むタブが表示されます。

4. パラメータのモニタリングを有効にするには、一番左の列で **[有効]** ボックスをオンにします。
5. 該当するパラメータ値を設定します。

パラメータ — **[CPU 使用]**、**[使用ディスク容量]**、および **[メモリ使用状況]**。表示値のため設定できません。

単位 — 比率 (%)。表示値のため設定できません。

範囲:

低 — 範囲の下限值。値は 0 ~ 100 (つまり 100%) の間の正の整数でなければなりません。

高 — 範囲の上限値。値は 0 ~ 100 (つまり 100%) の間の正の整数で、**[低]** より大きくなければなりません。

デフォルトでは範囲の値が空になっています。値を入力するには、パラメータ行の **[低]** または **[高]** 列のセル内の空白部分をクリックします。空白部分をクリックするとボックスが表示され、そこに値を入力できます。

call-home — 範囲外の値が検知されると Stratus 認定サービス業者に call-home メッセージが送信されます。

e アラート/トラップ — 範囲外の値が検知されると電子メール アラート (e アラート) および SNMP トラップが送信されます。

最初の検知 — 過去 24 時間以内にパラメータ値が初めて検知された日付と時刻。表示値のため設定できません。

最後の検知 — 過去 24 時間以内にパラメータ値が最後に検知された日付と時刻。表示値のため設定できません。

最後のイベント — 各ノードにおける最後のしきい値違反 (**[低]** または **[高]**)。セルが空白の場合、しきい値違反が発生していないことを示します。表示値のため設定できません。

インシデント カウント — 過去 24 時間以内に範囲を超えた回数。表示値のため設定できません。

現行値 — 次のいずれかを示します (表示値のため設定できません)。

- 現行値。
- **応答なし** — ゲスト モニタリング エージェントがインストールされていないか停止されているため、この VM 上で応答しません。ゲストをモニタリングするには、この VM にゲスト モニタリング エージェントを手動でインストールするか再起動する必要があります。
- **停止中** — ゲストが実行中の状態にありません。
- **利用不可** — この値は現在利用できません。

ステータス — 表示値のため設定できません。

- 予期値 (✓) — パラメータは過去 24 時間にその範囲を超えていません。
- 警告 (⚠) — パラメータは過去 24 時間にその範囲を超えていますが、現時点では発生が昇格されません。
- 範囲外 (✗) — 現在範囲外です。

6. **[保存]** をクリックして変更を保存するか、まだ保存していない値をキャンセルするには **[リセット]** をクリックします。

関連トピック

[「システム、Windows ベースの VM、およびアプリケーションをモニタリングする」](#)

[「e アラートを構成する」](#)

[「SNMP 設定を構成する」](#)

[「Windows ベースの仮想マシンを構成する」](#)

Windows ベースの仮想マシン上のアプリケーションをモニタリングする

Windows ベースの VM で実行しているアプリケーションのパフォーマンスに関する情報 (たとえば CPU 使用状況) をモニタリングします。

Windows ベースの VM を作成した後、**[仮想マシン]** ページの **[モニタ]** タブでアプリケーションを追加できます。その後、モニタリングのパラメータを表示して設定します。モニタリング パラメータを設定すると、その後は値が 60 秒ごとに更新されます。



注: VM の名前を変更するとモニタリング パラメータが非表示になりますが、1 ~ 2 分後に再び表示されます。

モニタリングするアプリケーション パラメータを追加や表示したり、パラメータを削除するには、アプリケーションの実行可能ファイルの名前 (拡張子なしで、たとえば `mysqld`) が必要です。この名前は Windows ユーティリティを使って調べます。たとえば、**[タスク マネージャ]** の **[プロセス]** タブにある名前のリストから、適切な名前を取得します。

アプリケーションとそのパラメータを追加、設定、表示するには

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[仮想マシン]** をクリックします。
2. 操作対象のアプリケーションを実行している VM を選択します。
3. 下部パネルで **[モニタ]** タブをクリックします。

[アプリケーション] パネルが **[ゲスト OS]** パネルの下に表示されます。**[アプリケーション]** 列にアプリケーションとその関連パラメータが一覧されます。リストの下にある追加と削除を行うボタンを使用して、アプリケーションとパラメータをリストに追加したり、削除することができます。

4. 必要に応じてアプリケーションとパラメータを追加します。

- a.  **[追加]** ボタンをクリックします。

2つのボックスが開き、最初 (左) のボックスにアクティブなカーソルが表示されます。

- b. 最初のボックスで、アプリケーションの実行可能ファイルの名前 (拡張子なしで、mysqld など) を入力するか、ドロップダウン リストから名前を選択します。
- c. 2 番目 (右) のボックスのドロップダウン リストから、モニタリングするパラメータを選択します。
- d. **[保存]** をクリックして変更を保存するか、まだ保存していない値をキャンセルするには **[リセット]** をクリックします。変更を保存すると、**[アプリケーション]** の下のリストに新しいアプリケーションが表示されます。

新しいアプリケーションが表示されるまで少し時間がかかります。

5. アプリケーションとパラメータのモニタリングを有効にするには、一番左の列で **[有効]** ボックスをオンにします。
6. 該当するパラメータ値を設定します。

アプリケーション — モニタリング対象として選択した、VM で実行中のアプリケーション。

パラメータ — **[CPU 使用]** および **[メモリ使用状況]**。表示値のため設定できません。

単位 — 比率 (%)。表示値のため設定できません。

範囲:

低 — 範囲の下限值。値は 0 ～ 100 (つまり 100%) の間の正の整数でなければなりません。

高 — 範囲の上限値。値は 0 ～ 100 (つまり 100%) の間の正の整数で、**[低]** より大きくなければなりません。

デフォルトでは範囲の値が空になっています。値を入力するには、パラメータ行の **[低]** または **[高]** 列のセル内の空白部分をクリックします。空白部分をクリックするとボックスが表示され、そこに値を入力できます。

call-home — 範囲外の値が検知されると Stratus 認定サービス業者に call-home メッセージが送信されます。

e アラート/トラップ — 範囲外の値が検知されると電子メール アラート (e アラート) および SNMP トラップが送信されます。

最初の検知 — 過去 24 時間以内にパラメータ値が初めて検知された日付と時刻。表示値のため設定できません。

最後の検知 — 過去 24 時間以内にパラメータ値が最後に検知された日付と時刻。表示値のため設定できません。

最後のイベント — 各ノードにおける最後のしきい値違反 (**[低]** または **[高]**)。セルが空白の場合、しきい値違反が発生していないことを示します。表示値のため設定できません。

インシデント カウント — 過去 24 時間以内に範囲を超えた回数。表示値のため設定できません。

現行値 — 次のいずれかを示します (表示値のため設定できません)。


- 現行値。
- **応答なし** — ゲスト モニタリング エージェントがインストールされていないか停止されているため、この VM 上で応答しません。ゲスト上のアプリケーションをモニタリングするには、この VM のゲスト モニタリング エージェントを手動でインストールするか再起動する必要があります。
- **停止中** — ゲストが実行中の状態にありません。
- **検出不可** — アプリケーションが見つからないか、ゲストで実行されていません。
- **利用不可** — この値は現在利用できません。

ステータス — 表示値のため設定できません。

- 予期値 (✓) – パラメータは過去 24 時間にその範囲を超えていません。
- 警告 (⚠) – パラメータは過去 24 時間にその範囲を超えていますが、現時点では発生が昇格されません。
- 範囲外 (✗) – 現在範囲外です。

7. **[保存]** をクリックして変更を保存するか、まだ保存していない値をキャンセルするには **[リセット]** をクリックします。数秒後、新しい値を入力した場合はこれが表示されます。

パラメータを削除するには

1. ztC Edge コンソールで、左側のナビゲーション パネルの **[仮想マシン]** をクリックします。
2. パラメータを削除するアプリケーションを実行している VM を選択します。
3. 下部パネルで **[モニタ]** タブをクリックします。**[アプリケーション]** パネルが **[ゲスト OS]** パネルの下に表示されます。
4. アプリケーション/パラメータ行を選択します。
5.  **[削除]** ボタンをクリックします。

アプリケーションのリストでアプリケーション/パラメータ行が非表示になります。

6. **[保存]** をクリックして変更を保存するか、まだ保存していない値をキャンセルするには **[リセット]** をクリックします。数秒後、アプリケーションのリストからアプリケーション/パラメータ行が再び非表示になります。

関連トピック

[「システム、Windows ベースの VM、およびアプリケーションをモニタリングする」](#)

[「e アラートを構成する」](#)

[「SNMP 設定を構成する」](#)

[「アプリケーションをインストールする \(Windows ベースの VM\)」](#)

[「Windows ベースの仮想マシンを構成する」](#)

第 2 部: 関連ドキュメント

リリース情報、およびリファレンスとトラブルシューティングについては、次の関連ドキュメントを参照してください。

- [「Stratus Redundant Linux リリース 2.3.0.0 リリース ノート」](#)
- [「システム リファレンス情報」](#)
- [「セキュリティ」](#)
- [「SNMP」](#)

9

第 9 章: Stratus Redundant Linux リリース 2.3.0.0 リリース ノート

これらのリリース ノート (2021/09/10 13:13 に更新) は、ztC Edge システム上で稼働する Stratus Redundant Linux リリース 2.3.0.0 を対象とします。(翻訳が完了した後の変更点のリストを含め、これらのリリース ノートの最新バージョンは、[StrataDOC](#) にある英語版を参照してください。) 次のセクションを参照してください。

- [新しい機能と機能強化](#)
- [修正されたバグ](#)
- [修正された CVE](#)
- [重要な考慮事項](#)
- [既知の問題](#)
- [Stratus ナレッジ ベースの記事にアクセスする](#)
- [ヘルプ情報](#)

新しい機能と機能強化

Stratus Redundant Linux リリース 2.3.0.0 の新機能

Stratus Redundant Linux リリース 2.3.0.0 の新機能は次のとおりです。

- ztC Edge 200i および 250i システム
- [展開に関する機能強化](#)

- 仮想マシン — RHEL 7.9、RHEL 8.2、CentOS 7.9、および Debian 10.9 ゲスト オペレーティング システムのサポート (完全なリストは「[テスト済みのゲスト オペレーティング システム](#)」を参照してください)。
- セキュリティの強化 — 337 個の CVE を修正。「[修正された CVE](#)」を参照してください。
- システムの初期インストール時とアップグレード時に VirtIO ドライバがシステム上に VCD としてインストールされます。
- ztC Edge コンソールのユーザ インタフェースに繁体字中国語をサポート。

Stratus Redundant Linux リリース 2.2.0.0 の新機能

詳細については、「[Stratus Redundant Linux リリース 2.2.0.0 の新機能](#)」を参照してください。

Stratus Redundant Linux リリース 2.1.0.0 の新機能

詳細については、「[Stratus Redundant Linux リリース 2.1.0.0 の新機能](#)」を参照してください。

修正されたバグ

Stratus Redundant Linux リリース 2.3.0.0 で修正されたバグ

ZTC-9370: 夏時間 (DST) を採用しているタイム ゾーンのサイトでは、[システム] ページの PM の詳細データの表示が不完全です。

ZTC-8354: バーチャルテクノロジー (VT) がサポートされ、有効になっているかどうかのチェックを修正しました。

ZTC-8097: マストヘッドの「サービスの期限切れ」のクロックをクリアする機能を追加しました。

ZTC-7532: [VM サマリ] タブの [ライブ ダンプのステータス] 行は、アクティビティのタイムアウトが発生したときには表示されません。

ZTC-5945: SNMP OID と値をすべての ztC プラットフォームで正しく識別し、すべての ztC プラットフォームで値が正しくなるように、プラットフォーム バリエーションの実装を修正しました。

ZTC-5872: アップグレードキットのダウンロード中にインターネット接続が失われると、それ以降のアップグレードキットをダウンロードできなくなることがあります。

ZTC-5824: システムがインターネットに接続されていない場合、更新のチェック機能が正しく終了するようになりました。

ZTC-5667: VM が再起動したノードにマイグレーションして戻った後、[システム] ページの VM 統計情報の表示に失敗することがあります。

ZTC-5218: VirtIO ドライバを virtio-win-0.1.171-1 に更新しました。

ZTC-4514: VM が使用しているビジネス ネットワーク ケーブルがピア ノード上で引っ張られた場合、ノードがメンテナンス状態に移行できません。

ZTC-4461: VM をインポートすると、ディスク イメージが 145 GB より大きい場合、無効なディスク イメージになることがあります。

ZTC-4458: アップグレード キットの評価機能が強化され、壊れたネットワークを検出し、適切な場合には評価を失敗させるようになりました。

ZTC-3888: GRUB2 は CVE-2020-10713 に対処するために更新されました。

ZTC-3590: root、swap、diagdata の各パーティションを初期ストレージ グループの 2 番目の論理ディスクにミラーリングする必要はなくなりました。

ZTC-3007: VirtIO ドライバの VCD がインストール時とアップグレード時に作成されるようになりました。

ZTC-459: 未使用のビジネス ネットワークに障害が発生した場合、ユニットの自動ローリング リブートは不可能です。

Stratus Redundant Linux リリース 2.2.0.0 で修正されたバグ

詳細については、「[Stratus Redundant Linux リリース 2.2.0.0 で修正されたバグ](#)」を参照してください。

Stratus Redundant Linux リリース 2.1.0.0 で修正されたバグ

詳細については、「[Stratus Redundant Linux リリース 2.1.0.0 で修正されたバグ](#)」を参照してください。

修正された CVE

修正された CVE のリストについては、「[修正された CVE](#)」を参照してください。

重要な考慮事項

リリース 2.3.0.0 へのアップグレード

Stratus Redundant Linux リリース 2.3.0.0 にアップグレードするには、システムで実行中のリリースに適したアップグレード パスに従ってください。

- リリース 2.2.0.0、2.1.0.0、2.0.1.0 および 2.0.0.0 – 「[アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする](#)」の手順に従って、リリース 2.3.0.0 に直接アップグレードします。
- 2.0.0.0 以前のリリース – まずリリース 2.0.1.0 にアップグレードしてから、リリース 2.3.0.0 にアップグレードします。リリース 2.0.1.0 にアップグレードする方法の詳細については、[リリース 2.0.1.0 リリース ノートおよびヘルプ](#)を参照してください。

システム ソフトウェアのバージョンを特定する

ztC Edge システムで稼働する Stratus Redundant Linux のバージョンを特定するには、そのシステムの ztC Edge コンソールにログオンし、マストヘッドでシステム情報をチェックします。

```
ocean.abc.com  
IP: 123.109.50.34 | Asset ID: ze-12345  
  
Version: n.n.n-nnn
```

あるいは、**[基本設定]** ページの **[ソフトウェア更新]** をクリックする方法でも、システム上の Stratus Redundant Linux ソフトウェアの現行バージョン番号を表示することができます。

ソフトウェア リリースの番号がリリース 2.3.0.0 よりも低い場合、Stratus Redundant Linux 2.3.0.0 アップグレード キットを **[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) からダウンロードして、システムのソフトウェアをアップグレードしてください。詳細は、「[アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする](#)」を参照してください。

アップグレードの処理中、ブラウザをリフレッシュして新しい証明書を受容する

Stratus Redundant Linux ソフトウェアのアップグレードの操作中、最初のノードがアップグレードされてプライマリ ノードになった後にアップグレード処理が停止しているというメッセージがブラウザに表示されることがあります。ブラウザに表示されたこのエラー メッセージは正しくありません。この問題は、ブラウザで Stratus からの新しい証明書の受容が必要となった場合に発生することがあります。プロンプトが表示された場合はブラウザをリフレッシュして、新しい証明書を受容してください。新しい証明書を受容すると、ブラウザにアップグレードの正しいステータスが表示されます。

ztC Edge 展開に関する機能強化

リリース2.3.0.0 以降では、ztC Edge のノード展開とインベントリ管理の柔軟性が強化されています。リリース 2.3.0.0 以降でインストールされた工場出荷時の状態にあるノードを、単一ノード システム、デュアルノード システムの 2 番目のノード、または交換ノードとして展開できるようになりました。

更新された手順については、「[システムを展開する](#)」、「[単一ノードシステムにノードを追加する](#)」、および「[物理マシンを交換する \(自動\)](#)」を参照してください。

Intel Active Management Technology (AMT) for Lights-Out のサポートを使用する

ztC Edge システムには、リモート電源管理、リモート コンソール、およびリモート メディアのための Intel Active Management Technology (AMT) lights-out のサポートが組み込まれています。AMT の構成と制限事項についての重要な情報は、KB-[8219](#) を参照してください。

ztC Edge ノードを個別の物理サイトで展開する

冗長なデュアルノード構成で ztC Edge システムを展開する際、同じサイトで両方のノードを展開して各ノード上の青 (A2) と黄色 (A1) のネットワークポート間の A-Link を直接接続する必要があります。冗長性を高めるために、各ノードが個別の物理サイトにある自動ローカル サイト復旧 (ALSR) 構成を用いて ztC Edge システムをセットアップしたい場合は、Stratus 認定サービス業者にヘルプを依頼してください。ALSR 構成は地理的に距離があることから、コンポーネントの配置とネットワーク トポロジを注意深く計画する必要があります。

ztC Advisor を有効化する

Stratus Redundant Linux リリース 2.2.0.0 以降、ztC Advisor がサポートされるようになりました。これは、ztC Edge システムのフリート全体を一括表示できる Web ベースのセキュアなポータルです。使いやすい直観的なダッシュボードから各システムの稼働状態、リソースの使用状況、およびソフトウェアバージョンを一目で確認できます。

ztC Advisor の登録と使用の詳細については、<https://www.stratus.com/solutions/ztc-advisor> にある Web ページを参照してください。システム用に ztC Advisor を有効化や無効化するには、「[ztC Advisor を有効化する](#)」を参照してください。

テスト済みのゲスト オペレーティング システム

現在のリリースでのテストが済んでいるゲスト オペレーティング システムのリストについては、「[テスト済みのゲスト オペレーティング システム](#)」を参照してください。以前のリリースでテスト済みまたはサポートされていたゲスト オペレーティング システムの詳細については、<http://ztcedgedoc.stratus.com> にアクセスして適切なリリースを選択してから、ゲスト オペレーティング システムを検索してください。

既知の問題

デュアルノード構成のシステムにアップグレードした後、VM に警告アイコンが表示される

1 つのノード用に構成されているシステムを、2 つのノード用に構成されているシステムにアップグレードする際、VM は実行中のままになりますが、ダッシュボードには VM の状態が警告アイコン (⚠) で表示されます。この警告は、アップグレード中には、システムが A-Link1 を追加しないため、VM が 1 または 0 個の A-Link で実行されていることを示します。

問題を回避するには、アップグレードの前に VM を停止し、アップグレードの後で VM を再起動します。この問題が発生したら、アップグレードの後に VM を停止してから再起動してください。

リムーバブル メディアと、P2V クライアントを使用した PM または VM のマイグレーション

ブート可能な P2V クライアント (**virt-p2v**) の ISO ファイルを使用して PM または VM をマイグレーションする前に、ソース イメージにリムーバブル メディア (フロッピー ディスク、DVD ドライブ、外付け USB ディスクなど) が接続されていないかどうかを確認します。PM または VM のマイグレーションを試行する際にリムーバブル メディアがソース イメージに接続されている場合、**変換に失敗した**というエラー メッセージが表示されます。この問題を未然に防ぐには、マイグレーションを開始する前に、**[virt-p2v]** ウィンドウでメディアの選択を解除してください。これを行うには、**[Target properties (ターゲットプロパティ)]** セクションと **[Fixed hard disks (固定ハード ディスク)]** セクションのある **[virt-p2v]** ウィンドウにアクセスしてから、**[Fixed hard disks (固定ハード ディスク)]** の下で、リムーバブル メディアの横の **[Convert (変換)]** 列のチェック ボックスをオフにします。**virt-p2v** の使用に関する詳細については、「[物理マシンまたは仮想マシンをシステムにマイグレーションする](#)」にある「ztC Edge システムに PM または VM をマイグレーションするには」を参照してください。

P2V クライアントの実行中に「VM <名前> の起動に失敗しました」というアラートが表示される (正常な動作)

P2V クライアントを使用して VM を everRun または ztC Edge システムからマイグレーションしている場合、マイグレーションの処理中にソース システムに「VM <名前> の起動に失敗しました」というアラートが表示された場合、これは正常な動作です。これは、ソース VM の電源がオンになっていて P2V クライアントを実行していても、ゲスト オペレーティング システムが起動しないためです。

VM のインポート時の最大パス長

仮想マシンのインポート/リストア ウィザードを使って VM をインポートする場合の VM の最大パス長は、**[リモートまたはネットワーク Windows 共有からインポート (CIFS/SMB)]** および **[リモートまたはネットワーク NFS からインポート]** オプションを使用する際は VM 名を含めて 4096 文字です。

RHEL 8.1 VM をインポートできない

(BIOS ブート ファームウェア使用の) RHEL 8.1 を実行している VM を、VMware ESXi 6.7.0 サーバから ztC Edge システムにインポートすることはできません。

UEFI VM コンソール セッションの最大解像度

ztC Edge コンソールの **【仮想マシン】** ページで、VM コンソール セッションを開いて VM で実行中のゲスト オペレーティング システムのコンソールを表示できます。コンソール セッションを開いて UEFI ブート タイプのゲスト VM にアクセスした場合、コンソール セッションの最大解像度は 800x600 です。これより高い解像度を得るには、リモートデスクトップ接続を使って VM に接続してください。

vmgenid サポートを有効にするには VM を再起動する

アップグレード キットを使用してシステムをリリース 2.0.1.0 以前から Stratus Redundant Linux リリース 2.2.0.0 以降にアップグレードした後、Windows Server 2019、Windows Server 2016、または Windows Server 2012 を実行する VM 上で vmgenid のサポートを有効にするには、VM を再起動する必要があります。したがって、そのような VM はアップグレード後に再起動して、vmgenid のサポートを有効にしなければなりません。リリース 2.1.0.0 からアップグレードする場合、リリース 2.1.0.0 を実行しているシステムで以前に再起動された VM を、あらためて再起動する必要はありません。

Microsoft Edge コンソール ブラウザを使用した VCD の作成が失敗する

Microsoft Edge を ztC Edge コンソール用のブラウザとして使用している場合、VCD を作成できず、処理が失敗します。代わりに、別の対応するブラウザを使用してください ([「対応しているインターネットブラウザ」](#) を参照)。

単一ノード システムで、VM 作成ウィザードの追加された vCPU の表示が誤っている

1 つのノード用に構成されているシステム上に VM を作成する際、**VM 作成ウィザード** には、指定した数の vCPU に 2 つの vCPU を追加していると表示されます。しかし、いったん VM が作成されると、ユーザが指定した数の vCPU が VM に接続されます。誤って表示された追加の 2 つの vCPU は追加されません。

IE10、IE11、Firefox のコンソールでの日本語キーボード 106 および 109 のマッピングが正しくない

IE10、IE11、Firefox を使用して ztC Edge コンソールにアクセスする場合、日本語キーボード 106 および 109 のマッピングが正しくない可能性があります。代わりに、Chrome またはリモート接続ソフト

ウェア (VNC または RDP) を使用してください。

トラップのない SNMP 要求を有効化できない

ztC Edge コンソールで SNMP 要求を作成する場合、トラップも作成する必要があります。そうでないと ztC Edge コンソールに「SNMP の更新中に問題が発生しました。設定が正しいことを確認してください。エラー: SNMP の構成に失敗しました。」というエラーが表示されます。回避策としては、新しい SNMP 要求を作成するときに、**[SNMP 要求の有効化]** と **[SNMP トラップの有効化]** をクリックし、バージョン 3 のユーザを定義せず、デフォルトの **[制限あり]** の要求のままにして、少なくとも 1 つのトラップ受信者を指定します。初期設定時にバージョン 3 のユーザを追加したり、**[制限なし]** をクリックすると、構成に失敗することがあります。初期設定が完了したら、必要な設定に変更することができます。

モニタリングを有効にして VM をマイグレーションすると "応答なし" になる

VM のモニタリングが 3 つすべてのパラメータ (CPU、メモリ、ディスク) に設定されている状態で VM をもう片方のノードにマイグレーションすると、**[モニタ]** タブに「**ゲスト エージェントから応答がありません。**」と表示されます。ゲスト エージェントが再接続するまで数分かかる場合があります。

A-Link がオフラインの場合、VM がパフォーマンス劣化ではなく破損として報告される

A-Link ケーブルまたはネットワークが 1 つのノードで切断されていると、VM に別のアクティブな A-Link 接続がある場合でも、ztC Edge コンソールでそのノード上の VM の状態が破損 (✖) として報告される可能性があります。VM の可用性に影響はありません。

取り出した VCD が Linux ベースの VM でコンソールに引き続き表示される

ztC Edge コンソールを使用して Linux ベースのゲスト オペレーティング システムを実行する VM から VCD を取り出した場合、ゲスト オペレーティング システムで VCD が表示されたままになることがあります。必要な場合はゲスト オペレーティング システムで VCD を取り出して、VCD を非表示にします。

一部のブラウザで https の使用中に VNC を接続できない

Microsoft Internet Explorer または Mozilla[®] FireFox[®] ブラウザで **https** URL を使って ztC Edge コンソールに接続している場合、**[仮想マシン]** ページで実行中の VM を選択してから **[コンソール]** をクリックすると、「**VNC: Unable to connect, retrying in n seconds** (VNC: 接続できません。n 秒後に再試行します)」というメッセージが表示されます。VNC 接続を有効にするには、マストヘッドの右上角にある VNC コンソール ページへの **https** リンクをクリックして、次の手順から適切なものを選択して続行します (お使いのブラウザのバージョンによって手順が異なる可能性があります)。

- Internet Explorer の場合、**セキュリティの警告**ウィザードが表示されます。
 - a. **[このサイトの閲覧を続行する (推奨されません)]** をクリックします。
 - b. **[OK]** をクリックします。
- FireFox の場合、**[安全な接続ではありません]** というウィンドウが表示されます。
 - a. **[詳細]** をクリックします。セキュリティ証明書が無効であるというメッセージが表示されます。
 - b. **[例外の追加]** をクリックします。**[セキュリティ例外の追加]** ダイアログ ボックスが開いて**[場所]** にコンソールの場所が表示されます。
 - c. **[セキュリティ例外を承認]** をクリックします。

VNC コンソールが表示されます。

ノード IP アドレスやネットマスク ネットワーク設定を変更するとリブートが必要になる

「[IP 設定を構成する](#)」の説明に従ってノードの IP アドレスやネットマスクの設定を変更する際、ノードをリブートするまでは古い設定と新しい設定の両方が有効になります。両方の設定が有効な場合、ルーティングや接続の問題につながる可能性があります。

Stratus ナレッジ ベースの記事にアクセスする

Stratus カスタマ サービス ポータルは、ztC Edge システムおよび Stratus Redundant Linux ソフトウェアを含む Stratus の全製品に関する技術的な記事を取めた検索可能な**ナレッジ ベース**を提供します。状況によっては、リリース ノートでこれらのナレッジ ベース記事を直接参照する場合もあります (例: KB-*nnnn*)。カスタマ サービス ポータルおよびナレッジ ベースの記事にアクセスするには、既存のサービス ポータル資格情報を使用するか、次の手順に従って新しいユーザ アカウントを作成してください。

ナレッジ ベースにアクセスするには

1. **Stratus カスタマ サービス ポータル** (<https://support.stratus.com>) にログオンします。

必要な場合は次の手順で新しいアカウントを作成します。

 - a. **[Register Account (アカウントの登録)]** をクリックします。
 - b. 勤務先の電子メール アドレスと連絡先情報を入力して **[Register (登録)]** をクリックします。

勤務先電子メール アドレスには Stratus の登録顧客企業のドメイン名 (たとえば「stratus.com」) を含める必要があります。

- c. Stratus から受け取った電子メールに記載されているリンクをクリックします。
- d. 新しいパスワードを入力してアカウントの構成を完了します。

アカウントの作成に関してヘルプが必要な場合は Stratus 認定サービス業者に連絡してください。

- 2. サービス ポータルで左側パネルにある **[Knowledge Base (ナレッジ ベース)]** をクリックします。
- 3. **[Keyword Search (キーワード検索)]** ボックスに、必要な情報に関連するキーワードを入力してから、**[Search (検索)]** をクリックします。

記事番号 (KB-*nnnn*) で記事を検索するには、**[Advanced Search (高度な検索)]** をクリックします。**[Search by ID (ID で検索)]** の横に記事の ID 番号 (*nnnn*) を入力して **[表示]** をクリックします。

ヘルプ情報

ztC Edge システムに関する技術的な質問がある場合、**[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) にある最新の技術情報およびオンライン マニュアルを参照してください。**ナレッジ ベース**は **Stratus カスタマ サービス ポータル** (<https://support.stratus.com>) でも検索できます。

オンライン マニュアルを参照しても疑問点が解決されず、システムにサービス契約が適用される場合には、Stratus 認定サービス業者まで問い合わせてください。詳細については、**ztC Edge サポート ページ** (<https://www.stratus.com/services-support/customer-support/?tab=ztcedge>) を参照してください。

10

第 10 章: システム リファレンス情報

リファレンス情報は、次のトピックを参照してください

- [「テスト済みのゲスト オペレーティング システム」](#)
- [「物理マシンと仮想マシンの重要な考慮事項」](#)
- [「ナレッジ ベースの記事にアクセスする」](#)
- [「ALSR 構成を作成する」](#)
- [「修正された CVE」](#)
- [「REST API」](#)

テスト済みのゲスト オペレーティング システム

次の表に Stratus Redundant Linux ソフトウェアの現在のリリースで Stratus によるテストが済んでいる仮想マシン (VM) 用のゲスト オペレーティング システムを一覧します。ここに一覧されていないゲスト オペレーティング システムは Stratus によるテストが済んでいないため、ローカルでテストを行う必要があります。

オペレーティング システム	バージョン	ブート ファームウェア インタフェース
CentOS 7	7.5、7.6、7.7、7.8、7.9 (すべて 64 ビット)	BIOS

オペレーティング システム	バージョン	ブート ファームウェア インタフェース
CentOS 6	6.9、6.10 (ともに 64 ビット)	BIOS
Debian 10	10.9.0-i386	BIOS
Microsoft Windows Server 2019 (Standard、Datacenter)	64 ビット	BIOS UEFI ¹
Microsoft Windows Server 2016 (Standard、Datacenter)	64 ビット	BIOS UEFI ²
Microsoft Windows Server 2012 (Standard、Datacenter)	64 ビット R2	BIOS
Microsoft Windows 10 Desktop	64 ビット	BIOS
Red Hat Enterprise Linux 8 (Workstation、 Server)	8.1、8.2 (ともに 64 ビット)	BIOS
Red Hat Enterprise Linux 7 (Workstation、 Server)	7.5、7.6、7.7、7.8、7.9 (すべて 64 ビット)	BIOS
Red Hat Enterprise Linux 6 (Workstation、 Server)	6.10 (64 ビット)	BIOS

¹VM が vSphere Release 6.7 を実行する VMware サーバからエクスポートされた場合に限り、UEFI ブート ファームウェア インタフェースをもち、Windows Server 2019 を実行している VMware VM を、Stratus Redundant Linux リリース 2.3.0.0 (以降) を実行するシステムにインポートできます。

²VM が vSphere Release 6.7 を実行する VMware サーバからエクスポートされた場合に限り、UEFI ブート ファームウェア インタフェースをもち、Windows Server 2016 を実行している VMware VM を、Stratus Redundant Linux リリース 2.3.0.0 (以降) を実行するシステムにインポートできます。

オペレーティング システム	バージョン	ブート ファームウェア インタフェース
SUSE Linux Enterprise Server (SLES)	12 SP2 64 ビット	BIOS
Ubuntu	18.042 サーバ 64 ビット	BIOS

物理マシンと仮想マシンの重要な考慮事項

物理マシンと仮想マシンを最適な方法で実装するには、以下のセクションで説明されている最大限の構成と必要条件に注意してください。

- [「仮想マシンの推奨事項と制限」](#)
- [「重要な考慮事項」](#)

仮想マシンの推奨事項と制限

仮想マシン (VM) には特定の [CPU コア リソース](#)が必要とされます。また、高可用性 (HA) とフォールトトレラント (FT) の両方の運用が可能なのはデュアルノードシステムの一部のモデルだけで、その他のモデルでは HA 運用のみを使用できます。単一ノードシステムでは HA 運用や FT 運用は許可されません。

システムと HA または FT 運用

システム モデル	HA 運用	FT 運用
100i	○	×
110i	○	○
200i	○	×
250i	○	○

詳細については、[「運用モード」](#)を参照してください。

推奨される CPU コアの数

Stratus では、ztC Edge システム上の物理スレッドと同数のみのスレッドをワークロードに使用することを推奨します。システムごとのスレッド数は次のとおりです。

ztC Edge システム モデル	物理スレッド総数
100i	8
110i	12
200i	12
250i	20

ztC Edge のワークロードに推奨されるコア数は、次で説明するように各 VM の vCPU の数および VM のタイプによって異なります。

例

以下の例はデュアルノードの ztC Edge 100i および 200i システムに適用されます。

- 4 つの 2-vCPU HA ゲストでは、通常合計 8 つのスレッドが必要です。
- 2 つの 3-vCPU HA ゲストと 1 つの 2-vCPU HA ゲストでは、通常合計 8 つのスレッドが必要です。
- 2 つの 4-vCPU HA ゲストでは、通常合計 8 つのスレッドが必要です。
- 1 つの 8-vCPU HA ゲストでは、通常合計 8 つのスレッドが必要です。

上記の例に加えて、以下の例はデュアルノードの ztC Edge 110i システムおよび 250i システムに適用されます。

- 1 つの 4-vCPU FT ゲストでは、通常合計 6 つのスレッドが必要です。
- 6 つの 2-vCPU HA ゲストでは、通常合計 12 つのスレッドが必要です。
- 1 つの 2-vCPU FT ゲストで 4 つのスレッド、2 つの 2-vCPU HA ゲストで 4 つのスレッド、合計 8 つのスレッドが必要です。

単一ノード システムでは、各 vCPU が 1 つのスレッドとしてカウントされます。以下の例は単一ノードの ztC Edge 100i および 200i システムに適用されます。

- 4 つの 2-vCPU ゲストでは、通常合計 8 つのスレッドが必要です。
- 2 つの 3-vCPU ゲストと 1 つの 2-vCPU ゲストでは、通常合計 8 つのスレッドが必要です。
- 2 つの 4-vCPU ゲストでは、通常合計 8 つのスレッドが必要です。
- 1 つの 8-vCPU ゲストでは、通常合計 8 つのスレッドが必要です。

上記の例に加えて、次の例は単一ノードの ztC Edge 110i システムおよび 250i システムに適用されます: 6 つの 2-vCPU ゲストでは、通常合計 12 つのスレッドが必要です。

重要な考慮事項

以下の重要な点について考慮してください。

機能	コメント
USB デバイス	VM のインポートとエクスポートおよびシステムの復元に USB キーボード、CD/DVD ドライブ、ディスク ドライブ、およびサムドライブを使用できます。
コンソールの接続	各 PM のテキスト コンソールを CentOS オペレーティング システムで使用できます。ただし、VGA モードはサポートされないため PM はランレベル 3 で実行する必要があり、ランレベル 5 には対応していません。以下の「システム管理」を参照してください。
システム管理	ztC Edge のシステム管理はランレベル 5 では機能しません。
ボリューム	たとえば、ボリュームのエクスポート、インポート、または復元を行う際、最大ボリューム サイズは 2 TB です。

ALSR 構成を作成する

このトピックのセクションでは、自動ローカル サイト リカバリ (ALSR) 構成を作成する方法について説明します。クォーラム サーバに関する一般的な情報は、[「クォーラム サーバ」](#) および、[「ALSR とクォーラム サービス」](#) を参照してください。



注: ALSR 構成を作成する前に、このトピックのすべてのセクションを読み、その説明に従って ALSR 構成を計画してください。構成を作成する前に、計画された構成がこのトピックの各セクションにある情報に準拠していることを確かめてください。

ALSR 構成は、次のいずれかが真の場合に存在します。

- デュアルノード システムの 2 つのノードが直接のケーブル接続ではなくネットワークインフラストラクチャを用いて接続されている。
- 2 つのノードを接続する A-Link (直接接続) ケーブルの長さが 10m を超えている (たとえば、同じキャンパス内の別々のビルにある場合など)。

これらの構成では、より優れたディザスタ レランスとハードウェア冗長性が得られるだけでなく、それを含む物理的なコンピュータ室や建物の冗長性も提供されます。

Stratus では、ALSR 構成にクォーラム サーバとなる 3 台目のコンピュータを含めることを推奨します。クォーラム サーバは、node0 と node1 の両方から物理的に離れた場所にあります。



注: このトピックの各セクションでは、クォーラム サーバのある ALSR 構成について説明します。Stratus では、ALSR 構成にクォーラム サーバを含めることを強く推奨します。クォーラム サーバなしの ALSR 構成の作成を検討している場合、ナレッジ ベースにアクセスして「Considerations if deploying ALSR without quorum (クォーラムなしで SplitSite を展開する場合の考慮事項)」という記事 (KB-9682) を参照したうえで、Stratus 認定サービス業者に連絡してください。ナレッジ ベースの記事のアクセスに関する情報は、「[ナレッジ ベースの記事にアクセスする](#)」を参照してください。

これらの物理マシンは地理的に離れているため、ALSR 構成を作成する際は、コンポーネント配置の入念な計画と、より複雑なネットワーク トポロジが必要とされます。

以下のトピックでは、ALSR 構成を作成する方法について説明します。トピックの手順を実行するには、ztC Edge ソフトウェアとその実行ハードウェアに関する知識と、システムのネットワーク インフラストラクチャおよびその場所を把握しておく必要があります。



注: ネットワーク スイッチやルータ、その他のハードウェアを提供するすべてのベンダーと機種についてこのトピックですべて説明することは不可能です。このヘルプ トピックにある要件に従ってハードウェアを構成する方法の詳細については、お使いのインフラストラクチャに関するマニュアルを参照してください。

- 「構成を作成する」
- 「ネットワークの要件を満たす」
- 「クォーラム サーバの場所を決めて作成する」
- 「構成を完了する」
- 「クォーラムがシステム動作に与える影響を理解する」

次の表は ALSR 構成の作成に関連する用語とその定義を一覧したものです。

用語	意味
アクティブ ノード	ゲスト VM が現在実行されているノード。各ゲスト VM が異なるアクティブ ノードをもつ場合もあります。"アクティブ" の逆は "スタンバイ" です (「 スタンバイ ノード 」を参照)。
A-Link	アベイラビリティ リンク。ztC Edge システムを形成する 2 台のコンピュータ間の直接ネットワーク接続。(システムの各コンピュータは "物理マシン" (PM) または "ノード" と呼ばれます。)A-Link はポイントツーポイント接続でなければならず、そのトラフィックをルーティングすることはできません。ztC Edge システムには 2 つの A-Link が必要です。一部のシステムではこれらの接続に青と黄色のケーブル (およびポート) が使われます。VLAN 接続は、分散されたローカル サイトの展開における A-Link に使用できます (「 VLAN 」を参照)。
代替クォーラム サーバ	代替クォーラム サーバは、優先クォーラム サーバが利用できない場合に使用されます (「 優先クォーラム サーバ 」を参照)。
自動ローカル サイト復旧 (ALSR)	ALSR 構成は、次のいずれかが真の場合に存在します。 <ul style="list-style-type: none">• ztC Edge システムの 2 つのノードが直接のケーブル接続ではなくネットワーク インフラストラクチャを用いて接続されている。• 2 つのノードを接続する A-Link (直接接続) ケーブルの長さが 10m を超えている (たとえば、同じキャンパス内の別々のビルにある場合など)。

	通常 ALSR 構成は、柔軟で細かいネットワーク セットアップと構成オプションを犠牲にして、代わりにより優れたディザスタ レランスを提供するために使用されます。ALSR 構成には、クォーラム サーバとなる 3 台目のコンピュータが必要です (「 クォーラム サーバ 」を参照)。
AX	ztC Edge システム内にある、ゲスト VM の動作を制御するコンテナ層。AX は、アクティブ ノードとスタンバイ ノード間の VM の同期を維持する役割を果たします。各 VM は独自の AX ペアをもちます (「 VM 」、「 アクティブ ノード 」、および「 スタンバイ ノード 」を参照)。
ビジネス ネットワーク (ibiz)	ztC Edge システムから LAN へのネットワーク接続。管理メッセージなどその他のトラフィック、およびアプリケーションとその他のクライアントやサーバのためのトラフィックも含むことがあります。通常 ztC Edge システムにはビジネス ネットワーク接続用に 2 つのポートがあります。ビジネス ネットワークは、使用する 1 台以上のゲスト VM に割り当てることができますが、ゲスト VM に一切割り当てない場合もあります。最初のビジネス ネットワーク (ibiz0) は、Web ブラウザからシステムを管理できるよう、LAN に接続しなければなりません。
障害	システムがゲスト VM (「 VM 」を参照) を実行する能力の劣化につながる可能性のある問題。ディスク エラー、ネットワークの損失、停電などは、すべてシステムにより検知される障害の例です。
node0 および node1	ztC Edge システムを形成する 2 台のコンピュータで、内部的には node0 および node1 としてラベル付けされています。(これらのコンピュータは物理マシンまたは PM とも呼ばれます。)node0 と node1 の選択は自由で、システムを最初に構成するときに選択します。node0 と node1 間に常時トラフィック フローがあり、システムや各ゲスト VM (「 VM 」を参照) の状態に関する情報がやり取りされます。
優先クォーラム サーバ	優先クォーラム サーバは、これが利用可能な場合に使用されます。優

	先クォーラム サーバが利用できない場合には、代替クォーラム サーバが使用されます (「 代替クォーラム サーバ 」を参照)。
プライマリ ノード	システムのコンピュータがペアとして設定される場合、管理メッセージにはそのうち 1 台のコンピュータのみが応答します。そのコンピュータがプライマリ ノードです。システムを最初に展開するときに割り当てられるシステム IP アドレスは、プライマリ ノードに適用されます。プライマリ ノードは、さまざまな障害条件の発生に伴い node0 と node1 の間で切り替えることが可能です (「 障害 」を参照)。プライマリ ノードは必ずしもゲスト VM のアクティブ ノードではないことに注意してください (「 アクティブ ノード 」および「 VM 」を参照)。
priv0	2 つのノード間におけるプライベート管理トラフィックを処理するネットワーク。詳細については、「 A-Link ネットワークとプライベート ネットワーク 」を参照してください。
クォーラム サーバ	各ゲスト VM についてどちらの AX をアクティブにするかの判別に役立つ 3 台目のコンピュータ (「 アクティブ ノード 」および「 VM 」を参照)。クォーラム サーバを正しく使用することでスプリット ブレーン状態を回避できます (「 スプリット ブレーン 」を参照)。
RTT	往復時間 (Round-trip time)。ネットワーク メッセージが開始点と宛先の間を往復するのに要する時間。時間は通常ミリ秒 (ms) 単位で計測されます。
スプリット ブレーン	ゲスト VM の AX ペアにおいて両方の AX が同時にアクティブになり、各アクティブ ゲスト内に食い違うデータのコピーが生成される状態のこと (「 AX 」および「 VM 」を参照)。スプリット ブレーンは node0 と node1 間のすべての通信パスが切断されたときに発生する可能性があります (「 node0 および node1 」を参照)。クォーラム サービスを使用してスプリット ブレーン状態の発生を回避できます (「 クォーラム サーバ 」を参照)。
スタンバイ ノード	ゲスト VM のアクティブでない方のノード。スタンバイ ノードは A-Link 接続による AX 通信を通じて同期が保たれます (「 AX 」および

	「A-Link」を参照)。どちらのノードがアクティブでどちらがスタンバイかは、各ゲスト VM の AX ペアによって決定されます (「 アクティブ ノード 」を参照)。
システム管理	システムの総合状態の維持を担当する、Stratus Redundant Linux ソフトウェア内の層。どちらのノードがプライマリかを判別する処理はシステム管理の一部です (「 プライマリ ノード 」を参照)。システム管理は、ztC Edge コンソール内の情報表示も行います。
UPS	無停電電源装置。短期間の停電による可用性への影響を防ぐ、電気機器用の外付けバッテリー バックアップ。
VLAN	仮想 LAN。VLAN は、1 つ以上の LAN 上にあるデバイスのセットで、異なる LAN セグメント上に配置されているにも関わらず、まるでケーブルでつながれた同じネットワークに接続されているかのように通信するよう構成されています。VLAN は ztC Edge システム内ではなく、ネットワーク インフラストラクチャ レベルで構成されます。「 自動 ローカル サイト復旧 (ALSR) 」構成では、A-Link 接続は隔離された VLAN として実装されます (「A-Link」を参照)。
VM	仮想マシン (ゲストとも呼ばれます)。システムには通常、1 つ以上の VM (ゲスト) と実行アプリケーションが、ゲスト オペレーティング システムを介して割り当てられています。

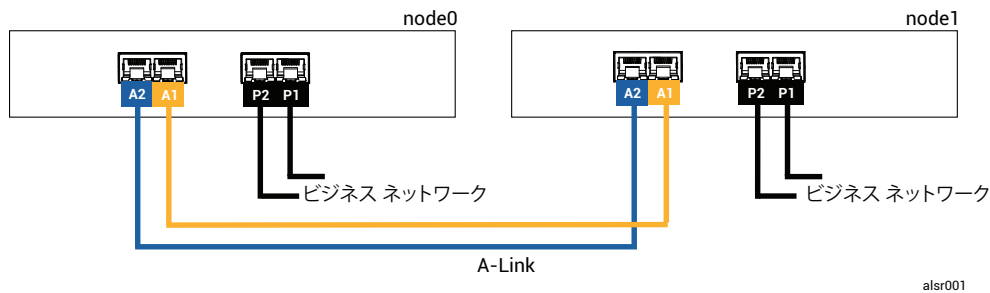
構成を作成する

ALSR 構成を作成するには、まず一般的な ztC Edge システムの構成と、ALSR 構成の VLAN 要件について検討します。その後、正しく計画された ALSR 構成 (クォーラム サーバを含みます) を観察し、VLAN 要件の構成を理解します。また、一般的な ztC Edge システムを展開してから ALSR 構成を作成するプロセス全体についても把握しなければなりません。以下のセクションではこの情報が提供されています。

一般的な ztC Edge システム

一般的な ztC Edge システム構成では、2 台の PM が A-Link 用のネットワーク ケーブルのペアで直接接続されています。1 つの A-Link は通常プライベート ネットワーク (priv0) として機能します。2 台の

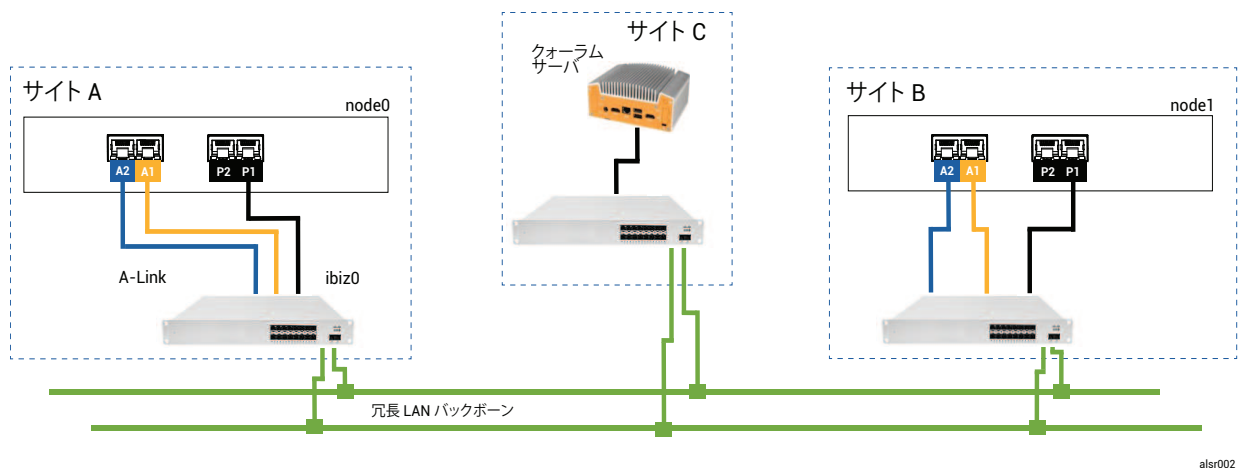
PM にはビジネス ネットワーク用の追加のネットワーク接続があり、これは ztC Edge コンソールおよびシステムでホストされるゲスト VM によって使用されます。次の図は一般的な構成を示すものです。



一般的な構成において PM 間の物理的な距離は 1 本の A-Link ネットワーク ケーブルの長さによって制限されます。これは約 33 ft (10m) です。物理的な環境と周囲の電気ノイズを考慮に入れると、この距離は大幅に短くなることもあります。

クォーラム サーバのある ALSR 構成

正しく計画された ALSR 構成は、2 箇所にある 2 つのノードと、3 つ目の箇所でクォーラム サービスを実行する 3 台目のコンピュータとで構成されています。ALSR 構成内には単一障害点が存在しないよう、これら 3 台すべてのコンピュータが適切なネットワーク スイッチ機器でネットワーク化されています。次の図はそのような構成の例です。ここではサイト A に node0、サイト B に node1、そしてサイト C にクォーラム サーバがあります。



注:

1. 各 A-Link は、スイッチ A とスイッチ B の間に構成された独自の VLAN に接続されます。
2. この図では便宜上 DNS サーバとゲートウェイは省略されていますが、ALSR 構成には DNS サーバへの接続と、ネットワーク故障に備えてゲートウェイを含めなければなりません。
3. 最大限の保護を確保するため、各サイトに冗長スイッチをインストールしますが、図にはこれらのスイッチが表示されていません。図に示す構成では、サイト A とサイト B の "それぞれに" 2 つのスイッチを含める必要があります。A-Link がその一方のスイッチを経由し、ビジネス ネットワークはもう片方のスイッチを経由します。可能であれば、短時間の停電による障害を回避できるよう、各スイッチに異なる回線からの電源を供給するか、UPS を使用してください。

ALSR VLAN の要件

スイッチ A とスイッチ B 間の A-Link 接続にはスイッチ上の VLAN 構成が必要となります。A-Link トラフィックはルーティングが不可能で、接続は 1 本の長いネットワークをエミュレートする必要があります。各 A-Link はその独自の VLAN 上で隔離されていなければなりません。

スイッチ機器間に VLAN を作成できない場合、イーサネットツーファイバのメディア コンバータを使用して 2 台の PM 間にさらに長いファイバー接続を作成できます。ただし、2 つの A-Link ファイバ接続を同じ物理的な導管には通さないでください。そうすると単一障害点が作成されます。

さらに、クォーラム サービス コンピュータは node0 と node1 のどちらともスイッチを共有できません。これは、スイッチの共有により単一障害点が作成されるためです。

A-Link およびクォーラム接続の遅延の要件に関する詳細については、[「ネットワークの要件を満たす」](#)を参照してください。

初期展開から ALSR 構成の完了まで

ALSR 構成を作成する際は、まず ztC Edge 構成なしで一般的な ALSR システムを展開して登録します。

[「一般的な ztC Edge システム」](#)の図は、そのようなシステムを示しています。作業を簡単にするには、提供されているケーブルを使用して、ノードを並べてインストールします。[「作業の開始」](#)を参照してください。

一般的なシステムが正常に作動するようになったら、ALSR 構成を作成します。

1. まだ行っていない場合、[「ALSR 構成を作成する」](#)のすべてのセクションを通読します。
2. クォーラム コンピュータをインストールしてクォーラム サーバを有効にします。次に記載されているすべての情報に従ってください。
 - [「クォーラム サーバのある ALSR 構成」](#)
 - [「ALSR VLAN の要件」](#)
 - [「ネットワークの要件を満たす」](#)
 - [「構成を完了する」](#)
3. クォーラム サーバが両方のノードにアクセスできることを確認します。
4. 1 つのノードを正常にシャットダウンします。[「物理マシンをシャットダウンする」](#)を参照してください。
5. シャットダウンしたノードを離れたサイトに移します。
6. インフラストラクチャを接続します。[上にある ALSR 構成の図](#)は、次を含む接続を示しています。
 - ポート **A2** への priv0 接続
 - ポート **A1** への 2 つ目の A-Link 接続
 - ポート **P1** への ibiz0 接続
7. 電源をオンにしてノードを (再) 接続します。[「物理マシンの電源をオンにする」](#)を参照してください。
8. 構成を確認します。以下のことを確かめてください。
 - 共有ネットワークが正しくペアリングされること — ztC Edge コンソールで **[ネットワーク]** ページに移動して、すべてのネットワークの状態が緑のチェックマークになっていることを確認します。必要に応じて、インフラストラクチャの問題のトラブルシューティングを行います。
 - クォーラム接続が再確立されること — コンソールで **[基本設定]**、**[クォーラム サーバ]** の順にクリックして **[クォーラム サーバ]** ページに移動します。クォーラム サーバの状態が緑のチェックマークになっていることを確認します。必要に応じて、インフラストラクチャの問題のトラブルシューティングを行います。
 - プライマリ ノードが node0 から node1 へ移行でき、コンソールが両方の構成で接続できること — 各ノードをメンテナンス モードにします ([「メンテナンス モード」](#)を参照)。

9. VM を (再) 接続する – VM をノード間でマイグレーションします (「[物理マシンまたは仮想マシンをシステムにマイグレーションする](#)」を参照)。VM ネットワークの正しいネットワーク フェールオーバーを確認します。
10. ネットワークのステータスを評価してイーサネット フェイルオーバーを検証します (「[\[ネットワーク\] ページ](#)」を参照)。

ネットワークの要件を満たす

このトピックでは、正しい ALSR 構成のための A-Link、ビジネス ネットワーク、クォーラム サーバ接続、および管理ネットワークにおけるネットワークの要件と考慮事項について説明します。(これらのネットワークの一般的な情報は、「[ネットワーク アーキテクチャ](#)」を参照してください。)



前提条件: ALSR 構成を計画して作成するには、(まだ行っていない場合は) まず「[ALSR 構成を作成する](#)」を読み、その手順に従います。

A-Link ネットワーク接続は、以下の要件を満たす必要があります。

- A-Link は IPv6 アドレス指定を使用します。
- 各 A-Link はその独自の VLAN 上で接続されていなければなりません。A-Link トラフィックはルーティングが不可能です。
 - FT VM の場合、RTT A-Link 遅延は 2 ms 未満でなければなりません (110i システムのみで利用可能)。
 - HA VM の場合、RTT A-Link 遅延は 10 ms 未満でなければなりません (すべての ztC Edge システムで利用可能)。
 - システム上のすべての VM のニーズを満たすのに十分な帯域幅を提供する必要があり、少なくとも各 A-Link につき 1Gb の速度を提供しなければなりません。
 - ネットワーク インフラストラクチャを計画する場合、スイッチと、そのスイッチ上の全ポートにわたるネットワーク バックボーンとの間のアップリンク帯域幅を考慮する必要があります。

これらの要件が満たされない場合、2 ノード間の同期帯域幅が制限されるためゲスト VM の実行速度が遅くなります。

最初のビジネス ネットワーク (ibiz0) は、ノード間およびクォーラム サーバとの通信に使用されます。ibiz0 ネットワークは、以下の要件を満たす必要があります。

- 2つのノードは同じサブネット上になければなりません。
- ネットワークは2つのノード間における IPv6 マルチキャスト トラフィックを許可しなければなりません。
- 2つのノードが IPv4 ネットワーク アドレス指定を使ってクォーラム サーバにアクセスできなければなりません。

クォーラム サーバのネットワーク接続は、以下の要件を満たす必要があります。

- クォーラム サービスへのアクセスは ibiz0 を使用し IPv4 ネットワーク アドレス指定を用いて提供しなければなりません。
- 2つの UDP ポートが開いていてノードとクォーラム サービス間の通信に利用可能でなければなりません。これにはファイアウォール内の通信も含まれます。デフォルトでは、これらのポートは 4557 と 4558 です。これらのポートを変更する場合、「[クォーラム サービス ポートを構成する](#)」(クォーラム コンピュータ上) および「[ztC Edge コンソール内でクォーラム サーバを構成する](#)」を参照してください。
- ztC Edge ノードとクォーラム コンピュータ間の遅延が 500 ms RTT 未満でなければなりません。
- スループットは重要な考慮事項ではありません。10 Mb イーサネット、または T1 帯域幅でも十分です。
- クォーラム コンピュータは同じ ztC Edge システム上のすべての VM に共通しています。
- クォーラム コンピュータは数多くの ztC Edge システム間で共有できます。
- クォーラム コンピュータは、それを使用する同じ ztC Edge システム上の VM として実装することは絶対にできません。
- 異なるネットワーク インフラストラクチャを使用するようにし、共有は避けてください。ztC Edge ノードが、クォーラム サービス コンピュータへのアクセスを維持するためにパートナー ノード サイト上のゲートウェイまたはスイッチ/ルータに依存してはいけません。

注: クォーラム サービスを異なるノード ペア上のゲスト VM として実装しないでください。これらのノードで障害が発生するとクォーラム サービスを実行している VM がフェールオーバーし、ネットワーク トポロジと障害管理が不必要に複雑化する結果を招きます。それだけでなく、クォーラム サービスを実行している ztC Edge システム用のクォーラムを管理するために 2 台目のクォーラム コンピュータが必要になります。

管理ネットワーク接続は、以下の要件を満たす必要があります。

- デフォルトでは管理ネットワークはビジネス ネットワークと共有されます。その場合、ビジネス ネットワークの要件のすべてが管理ネットワークにも適用されます。
- リモート管理用にビジネス LAN へのゲートウェイを構成します。

クォーラム サーバの場所を決めて作成する

正しく計画されている ALSR 構成では、3 台目のコンピュータがクォーラム サービスをホストします。クォーラム サービスの処理要件は厳しくないため、ネットワークと運用の要件をすべて満たす既存のコンピュータまたは VM であれば、クォーラム サービスをホストすることができます。クォーラム サーバの効果は、ネットワーク内のどこにクォーラム コンピュータを配置するかによって決まります。

クォーラム コンピュータ (および該当する場合は代替クォーラム コンピュータ) の効果的な場所を決定し、そのコンピュータがクォーラム サービスの要件を満たすことを確認したら、クォーラム コンピュータを作成できます。



前提条件: ALSR 構成を計画して作成するには、(まだ行っていない場合は) まず「[ALSR 構成を作成する](#)」を読み、その手順に従います。

クォーラム コンピュータの場所を決める

「[クォーラム サーバのある ALSR 構成](#)」に示されるように、1 台目のクォーラム コンピュータをネットワーク内の第 3 サイトに配置します。第 3 サイトが利用できない場合、node0 と node1 の両方から物理的に離れた場所にクォーラム コンピュータを配置してください。クォーラム コンピュータを専用のサイトに配置すると、両方のノードとクォーラム コンピュータが失われるような問題が発生してもシステムの生存確率を最大限にすることができます (たとえば、一時的な電力、配管、その他の問題によりネットワーク接続が失われる場合があります)。

クォーラム コンピュータは、node0 と node1 に電力を供給する回路とは異なる電気回路につないでください。また、クォーラム コンピュータは UPS ユニットに接続する必要があります。

注意事項: 両方の AX がクォーラム サーバとの接続を失った場合、それらは代替クォーラム サーバを選択しようとしています。クォーラム サーバを選択することができない場合、別の障害が発生したときにスプリットプレーン状態が起きるのを回避するため、VM はシンプレックス モードにダウングレードされます。



片方のノードがシャットダウンし、残ったノード上の VM (AX) がクォーラム サーバまたはそのピアにアクセスできない場合には、その VM はスプリットプレーン状態を回避するために自らシャットダウンします。

クォーラム コンピュータの場所を決める際、次のことに注意してください。

- クォーラム コンピュータは、node0 と node1 のどちらともスイッチ (またはルータ) を共有しないようにしてください。
- クォーラム サービスの実行には ztC Edge システム内のゲスト VM を**使用しない**でください。

システム動作と障害モードの説明については、[「クォーラムがシステム動作に与える影響を理解する」](#)を参照してください。

代替クォーラム コンピュータを追加する

もう 1 台のクォーラム コンピュータ (とそのスイッチ) をシステムに追加して、代替クォーラム サービスを作成することができます。代替クォーラム サーバを使用する最も一般的なケースは、たとえば優先クォーラム コンピュータにオペレーティング システムの更新を適用する場合などです。優先クォーラム コンピュータが再起動されると、代替クォーラム コンピュータが選択されて、ダウングレードの発生を防ぎます。優先クォーラム が復旧すると、元の優先クォーラム コンピュータが再び選択されます。

2 つ目のクォーラム サービスを作成する際は、ネットワークとクォーラム 配置のすべての要件に従わなければいけません。両方のノードが互いに通信でき、またこれらが同じクォーラム サーバ (優先または代替のクォーラム サーバ) と通信できる場合、1 台のクォーラム 接続が失われても、システムは VM の冗長性を維持できます。優先クォーラム サーバの選択は、両方のノードが相互に通信でき優先クォーラム サーバとも通信できる状況において発生します。したがって、ノードの損失と同時にクォーラム サービスが失われた場合には、2 つ目の非優先クォーラム サービスが利用可能であっても、残っているノードが VM をシャットダウンします。ただし、ノードを失う "前に" 優先クォーラム サービスが失われ、両方のノードが引き続き代替クォーラム サーバにアクセスできる場合には、選択対象が代替クォーラム サーバに移ります。障害処理は選択されたクォーラム サーバのコンテキスト内のみで行われます。

代替クォーラム サービスを作成する場合、ztC Edge コンソールでクォーラム サービスを追加するときに 2 つ目のクォーラム IP アドレスを追加する必要があります。

クォーラム コンピュータの要件

クォーラム サービス ソフトウェアは、Windows オペレーティング システムを実行していて以下の要件を満たす、すべての汎用コンピュータ、ラップトップまたは VM 上にインストールできます。

- ztC Edge システムの ibiz0 ネットワークが常にクォーラム サーバにアクセスできるよう、コンピュータは電源が常にオンでネットワークに接続された状態を維持できること。
- コンピュータに静的な IPv4 ネットワーク アドレスが割り当てられていること。DHCP は使用しないでください。
- オペレーティング システムが Windows Server 2016、Windows Server 2012、Windows 10 のいずれかであること。Windows OS の埋め込みバージョンはサポートされません。
- 最小 100 MB のディスク領域が利用可能であること。
- 2 つの UDP ポートが開いていてノードとクォーラム サービス間の通信に利用可能でなければなりません。これにはファイアウォール内の通信も含まれます。デフォルトでは、これらのポートは 4557 と 4558 です。これらのポートを変更するには、[「クォーラム サービス ポートを構成する」](#) (クォーラム コンピュータ上) および [「ztC Edge コンソール内でクォーラム サーバを構成する」](#) を参照してください。

クォーラム サービス ソフトウェアをダウンロードしてインストールする

クォーラム コンピュータの適切な場所を決定したら、クォーラム サーバの作成に必要なソフトウェアをダウンロードしインストールします。

クォーラム サーバ ソフトウェアをダウンロードしてインストールするには

1. **[Downloads (ダウンロード)]** ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) を開きます。
2. **[Drivers and Tools (ドライバとツール)]** セクションにスクロールして、**[Quorum Service (クォーラム サービス)]** をクリックし、クォーラム サーバ ソフトウェアのインストーラ ファイルをクォーラム サーバにダウンロードします。
3. クォーラム サーバでインストーラ ファイルをダブルクリックします。
4. ダウンロードしたファイルをアクセス可能な場所に移動します。

5. クォーラム コンピュータにログインします。
6. クォーラム サービス インストーラに移動し、これをダブルクリックします。
7. 表示される指示に従いインストールを完了します。

クォーラム サービスをインストールするときに製品名の "everRun" が表示されることがあります。



注: クォーラム サーバソフトウェアを新しいバージョンにアップグレードする場合、以前のバージョンをアンインストールする必要はありません。

構成を完了する

ALSR 構成を作成したら、必要に応じてクォーラム サービス ポートを変更します。その後、ztC Edge コンソール内でクォーラムを有効にします。最後に、構成を確認して VM を (再) 接続します。



前提条件: ALSR 構成を計画して作成するには、(まだ行っていない場合は) まず「[ALSR 構成を作成する](#)」を読み、その手順に従います。



注: クォーラム コンピュータ上でクォーラム サービス用に構成されているポートと、ztC Edge コンソール内でクォーラム サーバ用に構成されているポートは、ポート番号が同じでなければなりません。クォーラム コンピュータ上のクォーラム サービス ポートを変更する場合、そのクォーラム コンピュータに接続するすべての ztC Edge システム上で (ztC Edge コンソールを使用して) クォーラム サービス ポートを変更しなければなりません。これは、クォーラム コンピュータと ztC Edge システムの両方で同じポート番号が使用されるようにするためです。「[ztC Edge コンソール内でクォーラム サーバを構成する](#)」を参照してください。

クォーラム サービス ポートを構成する

デフォルトでは、クォーラム サービスは UDP ポート 4557 でリッスンします。

大半の場合、デフォルトのポートを変更する必要はありません。ただし、ポートを変更する場合には、ネットワーク構成のために次の操作が必要となります。

クォーラム サーバ上のポート番号を変更するには

1. 管理者権限のあるアカウントを使ってクォーラム コンピュータにログオンします。
2. コマンド プロンプト ウィンドウを管理モードで開きます。

3. 次を入力してクォーラム サービスを停止します。

```
net stop sraqserver
```

4. 次を入力してポートを変更します (*nnnn* を新しいポート番号で置き換えます)。

```
sraqserver -install nnnn
```

5. 次を入力してクォーラム サービスを再開します。

```
net start sraqserver
```

クォーラム サービス ポートを確認する

クォーラム サービス ポートを確認する必要がある場合、次の Windows レジストリ キーを調べます。

```
HKEY_LOCAL_  
MACHINE\SYSTEM\CurrentControlSet\Services\Sraqserver\Parameters\QS  
ServerPortForReceive
```

ztC Edge コンソール内でクォーラム サーバを構成する

クォーラム サービスが稼働したら、ztC Edge コンソール内でクォーラム サービスを有効にしてください。クォーラム サーバを削除することもできます。

クォーラム サービスを有効にするには

1. 管理者権限のあるアカウントを使って ztC Edge コンソールにログインします。
2. 左側のナビゲーション パネルで **[基本設定]** をクリックして **[基本設定]** ページを表示します。
3. **[クォーラム サーバ]** をクリックします。クォーラム構成のページが開きます。
4. ページの左側にある **[クォーラム サーバの追加]** をクリックします。
5. **[優先クォーラム サーバの追加]** ダイアログ ボックスで、次の値を入力します (既に優先クォーラム サーバが存在する場合は **[代替クォーラム サーバの追加]** ダイアログ ボックスが表示されます)。
 - **DNS または IP アドレス** — 優先クォーラム サーバの完全修飾 **DNS** ホスト名または **IP アドレス** を入力します。
 - **ポート** — デフォルトのポートは 4557 です。デフォルト以外のポートが必要な場合、ポート番号を入力します。入力が必要なポート番号は 1 つだけです。クォーラム サービスは、**[ポート]** およびその次のポートのポート番号 (たとえば 4557 と 4558) を開きます。



注: ポート番号はクォーラム サービスがリスンしているポートと一致しなければなりません。(必要な場合はクォーラム サーバのポートを変更できます。)

[保存] をクリックして値を保存します。

6. ステップ 4 および 5 を繰り返して 2 台目の代替クォーラム サーバを構成します。Stratus では、クォーラム サーバを 2 台構成することを推奨します。
7. クォーラム サービスを有効にするには、[有効] チェック ボックスをオンにして [保存] をクリックします。

クォーラム構成に行った変更は既に実行中の VM には反映されません。クォーラム構成を変更した後は、実行中のすべての VM を停止して再起動する必要があります。

クォーラム サーバを削除するには



注意事項: 優先クォーラム サーバを削除すると、代替クォーラム サーバが優先クォーラム サーバになります。代替クォーラム サーバがない場合、優先クォーラム サーバを削除すると自動的にクォーラム サービスが無効になります。

1. ztC Edge コンソールの [基本設定] ページに移動します。
2. [クォーラム サーバ] をクリックします。
3. 削除するクォーラム サーバのエントリを見つけます。
4. 一番右の列で [削除] をクリックします。



注: VM で使用されているクォーラム サーバを削除する場合、削除の操作を完了させるには、VM をリブートしてクォーラム サーバが認識されないようにする必要があります。VM はクォーラム サーバが構成されて再起動されるまでの間、シンプレックス モードにダウングレードします。

構成を確認して VM を (再) 接続する

構成を確認して VM を (再) 接続します。「初期展開から ALSR 構成の完了まで」の適切な手順に従います。

クォーラムがシステム動作に与える影響を理解する

ALSR システム内のクォーラム サーバによって、システムの可用性と復旧動作が変更されます。クォーラムがシステム動作に与える影響を理解するには、その前にクォーラム サーバをもたないシステムの動作を理解しておく必要があります。



前提条件: ALSR 構成を計画して作成するには、(まだ行っていない場合は) まず「[ALSR 構成を作成する](#)」を読み、その手順に従います。

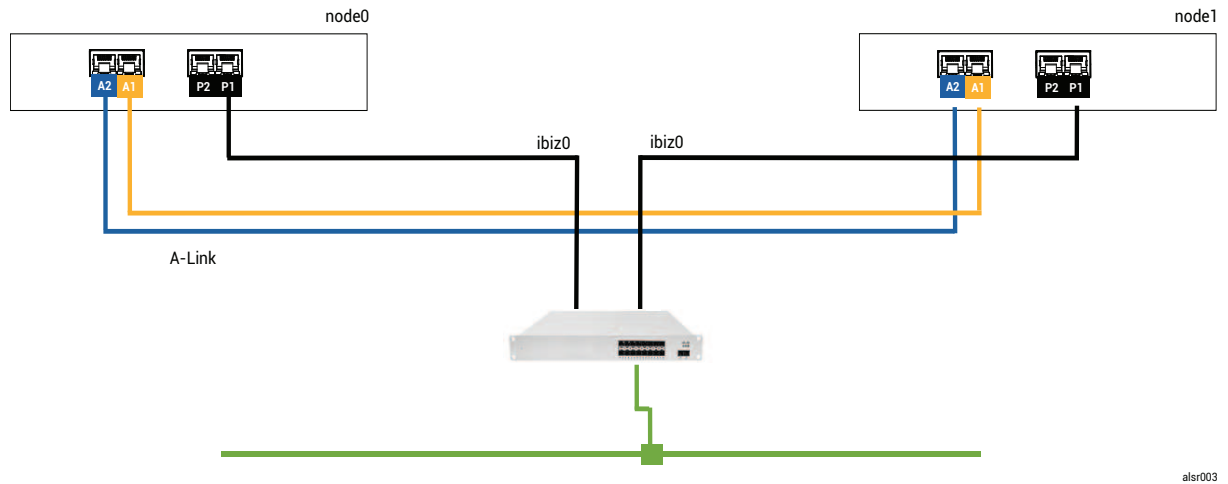
ztC Edge システムは、1 台以上のゲスト VM に高可用性を提供するよう設計されています。そのため、通常ならアプリケーションのダウンタイムを引き起こすような障害が発生した場合であっても、VM を継続して実行できるようになります。ztC Edge システムは、たとえば 1 つのネットワーク接続やハードディスク、あるいはコンピュータ全体が失われた場合でも、ゲスト VM を引き続き実行することができます。

ただし、さらに致命的な障害が発生した場合 (たとえば可能なネットワークパスすべての故障など)、ztC Edge システムはシステム全体の総合状態を判断しようとします。その後、システムはゲスト VM の整合性を保護するために必要なアクションを実行します。

次の例は、致命的な障害発生時のシステムのプロセスを示すものです。

例 1: クォーラム サーバなしのシステムではスプリット ブレーン状態が発生する

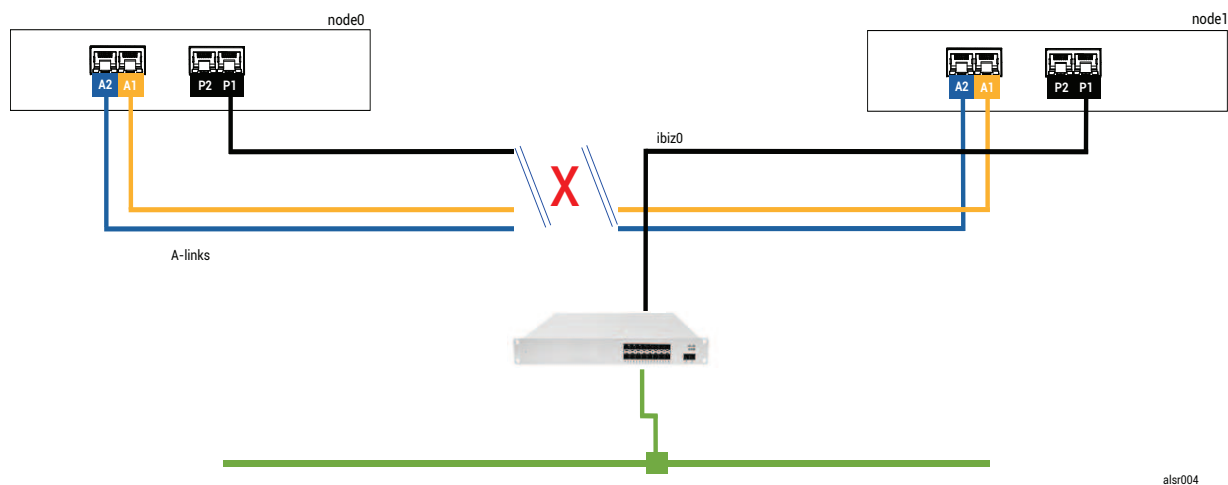
ALSR の例では、ztC Edge システムに node0 と node1 が含まれますが、クォーラム サーバは含まれません。動作は正常で、現在検知されている障害はありません。2 つのノードは正常な (障害のない) 動作のときと同様に、A-Link 接続を介してその状態と可用性をやり取りします。次の図は正常な接続を示すものです。



alsr003

致命的な障害

フォークリフトを運転する作業員が不注意から壁に衝突し、すべてのネットワーク接続 (ビジネスリンクと A-Link の両方) を切断してしまいました。ただし電源は残っており、システムも実行を継続しています。次の図は障害のある状態を示すものです。



alsr004

障害処理

2 つのノードは次のように障害を処理します。

- node0 — node0 の AX が、A-Link とその他のネットワークパスの両方が失われたことを検知します。node0 AX がそのパートナーの存在を検知できなくなると、node0 AX がアクティブになります。

ゲスト VM を実行します。ゲスト VM 内のアプリケーションは、ネットワーク損失のため、おそらく機能が制限された状態で実行を継続します。

- node1 — node1 の AX が、両方の A-Link が失われたことを検知しますが、ibiz0 は引き続き利用可能です。パートナーが ibiz0 内のメッセージに応答しないため、node1 AX がアクティブになります。ゲスト VM 内のアプリケーションは、おそらくシステムの問題を認識しない状態で、実行を継続します。

アプリケーション クライアントまたは外部オブザーバの観点からは、ゲスト VM の両方がアクティブであり、同じ返信アドレスでネットワーク メッセージを生成しています。両方のゲスト VM がデータを生成し、それぞれ異なる量の通信エラーを検知します。ゲスト VM の状態は、時間が経つにつれて相違が大きくなります。

復旧と修復

しばらくしてネットワーク接続が復元され、壁の修理が済みネットワーク ケーブルの配線もやり直しました。

AX ペアの各 AX は、それぞれのパートナーがオンラインに戻ったことを認識し、障害処理規則のある AX ペアが、アクティブな状態を続ける AX を選択します。この選択は予測が不可能であり、スプリット ブレーン状態の間にどちらのノードのパフォーマンスがより正確であったかを一切考慮に入れません。

(その時点での) スタンバイ ノードから生成されたデータはアクティブ ノードの再同期によって上書きされるため、(その時点での) スタンバイ ノードにあるデータは永久に失われます。

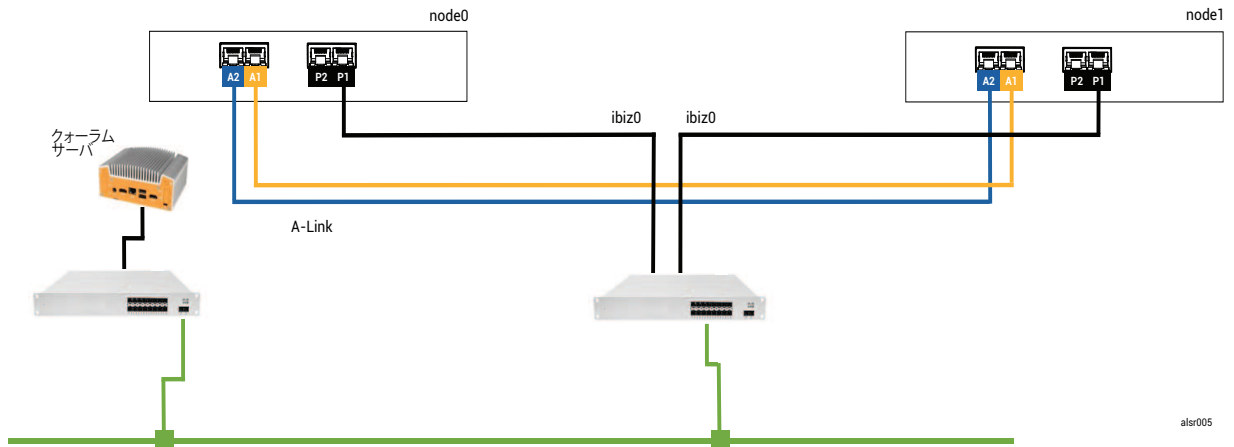
スプリット ブレーン状態の後、システムが再同期を完了するまで数分間かかります。この所要時間はスタンバイ ノードに送信が必要なディスク アクティビティの量によって決まります。異なるアクティブ ノードをもつゲスト VM がいくつか実行されている場合、両方向の同期トラフィックが生じることがあります。



注: 状況によっては、ztC Edge システムが致命的な障害の後取るべき最善の処理を判定できないこともあります。その場合、システムを手動で復旧する必要があります。復旧方法としては、片方のノードを実行し続けながら、ztC Edge コンソールを使ってもう一方のノードをシャットダウンし、リブートすることを推奨します。この方法では実行中のノードを強制的にプライマリとし、そのノード上の AX がアクティブになります。実行中のノードがプライマリになった後、もう一方のノードの電源を手動でオンにすることができます。既に再同期が進行中の場合には、どちらのノードもシャットダウンしないでください。

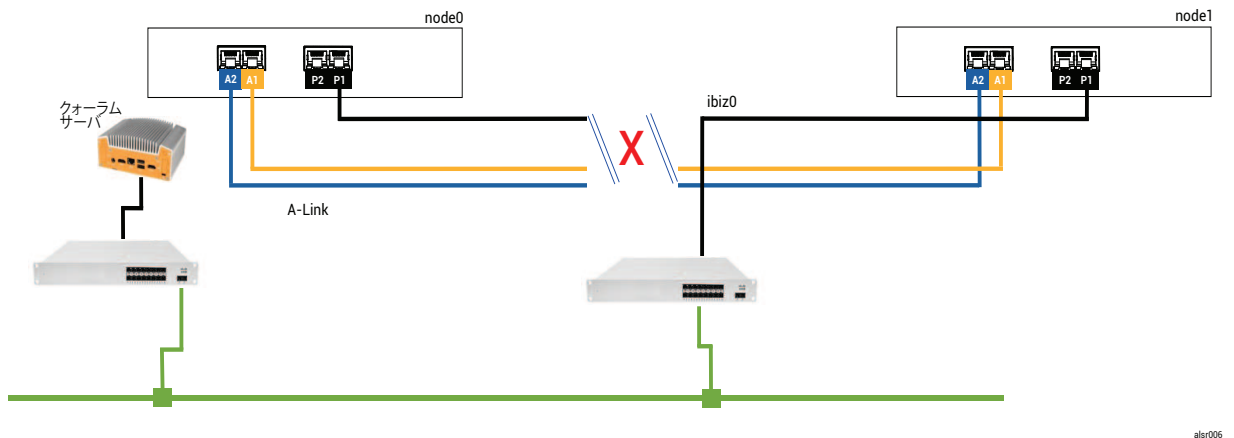
例 2: クォーラム サーバのある ALSR システムではスプリット ブレーン状態を回避できる

この ALSR の例では、ztC Edge システムに例 1 のシステムとまったく同じ接続をもつ node0 と node1 が含まれています。これに加えて、例 2 のシステムにはクォーラム サーバが含まれます。次の図はこれらの接続を示すものです。



致命的な障害

例の不注意な作業員が再びフォークリフトで壁に衝突し、ネットワーク接続をすべて切断してしまいました。ただし電源は残っており、システムも実行を継続しています。次の図は障害のある状態を示すものです。



障害処理

2 つのノードは次のように障害を処理します。

- node0 — node0 の AX が、A-Link とその他のネットワーク パスの両方が失われたことを検知します。node0 AX はそのパートナーの存在を検知できなくなったため、node0 AX はクォーラム サーバへの通信を試行します。この場合、クォーラム サーバも利用不可になります。したがって、node0 AX はシャットダウンを選択します。このシャットダウンは Windows の正常なシャットダウンではなく強制停止であるため、ゲスト VM 内のアプリケーションが停止されます。
- node1 — node1 の AX が、両方の A-Link が失われたことを検知しますが、ibiz0 は引き続き利用可能です。node1 AX がクォーラム サーバへの通信を試行し、サーバが応答するため、node1 AX はアクティブなままになります。ゲスト VM 内のアプリケーションはおそらくシステムの問題を認識していない状態で、実行されます。



注: node1 AX は以前アクティブではなく、ゲスト VM が HA VM であるため、場合によっては node1 のゲスト VM が node1 のハード ドライブからブートする必要があります。その場合、ゲスト VM のブート中、アプリケーションのダウンタイムが一時発生します。(FT VM は実行を継続します。)

アプリケーション クライアントまたは外部オブザーバの観点からは、node1 のゲスト VM はアクティブなままになり、node0 の VM がシャットダウンしている間もデータを生成します。スプリット ブレーン状態は存在しません。

復旧と修復

しばらくしてネットワーク接続が復元され、壁の修理が済みネットワーク ケーブルの配線もやり直しました。

node1 AX でそのパートナーがオンラインに戻ったことが認識されると、node0 AX がスタンバイになります。node0 は以前実行中ではなかったため、node1 から node0 へのデータ同期が開始されます。

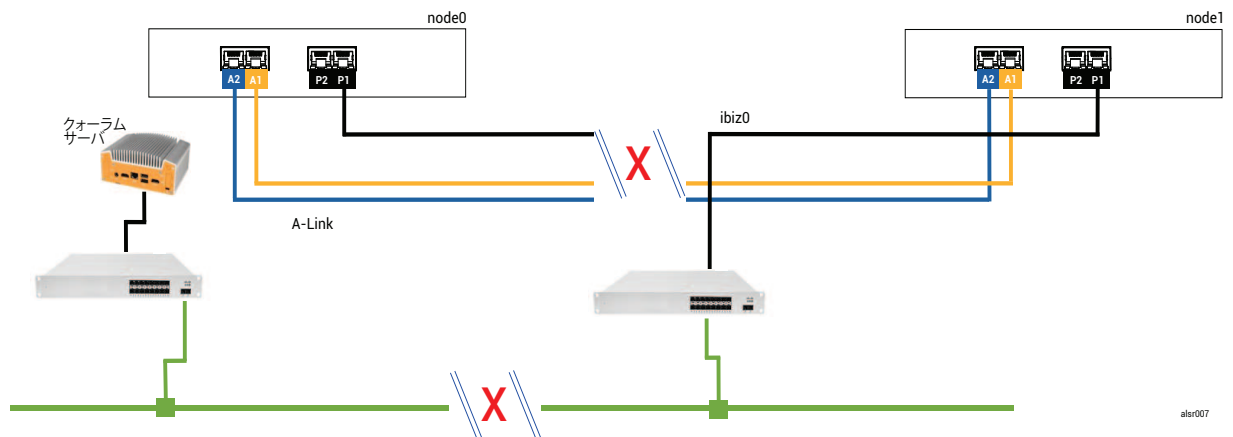
スプリット ブレーン状態は発生していないので、データ損失はありません。

システムが再同期を行うには数分間かかります。この所要時間はスタンバイ ノードに送信が必要なディスク アクティビティの量によって決まります。

例 2 (応用編): 致命的な障害時にクォーラム サーバがアクセス不可の場合

クォーラム サーバのある ALSR システムでは、電源は残っていてシステムが実行を継続している状態であっても、致命的な障害によりすべてのネットワーク接続が切断されてクォーラム サーバがオフライン

またはアクセス不可になる可能性があります。次の図は、このようなシステムでクォーラム サーバがオフラインになった状態を示すものです。



障害処理は例 2 の場合と似ていますが、node1 に重要な違いが 1 つあります。

node1 AX も、両方の A-Link が失われたことを検知しますが、ibiz0 は引き続き利用可能です。

node1 AX がクォーラム サーバへの通信を試行しますが、通信が失敗します。AX がゲスト VM を終了します。

この場合、ゲスト VM が node0 と node1 の両方でシャットダウンされ、スプリット ブレーンの発生は回避されます。トレードオフは、node0 とクォーラム サーバのどちらかへの接続が復元されるまでゲスト VM が利用不可になる点です。

その場合、運用しない方のノードを特定し、その電源を切ります。次に、運用する方のノードを強制ブートして、VM を強制ブートします。VM をシャットダウンしてから起動する方法については、[「仮想マシンの運用を管理する」](#)を参照してください。)

例 2 (応用編): 致命的な障害のない時にクォーラム サーバがアクセス不可の場合

場合によっては、致命的な物理的障害がなくてもクォーラム サーバがアクセス不可になる可能性があります。これはたとえば、OS パッチの適用などの定期的なメンテナンスのためにクォーラム コンピュータがリブートされる場合などです。こうした状況では、クォーラム サービスが応答していないことが AX で検知されるため、AX はクォーラム サーバへの接続が復元されるまで同期のトラフィックを中断します。ゲスト VM は、接続が失われた時点でアクティブだったノード上で実行を継続します。ただし、追加の障害が発生する可能性があるため、ゲスト VM はスタンバイ ノードに移行しません。クォーラム サービスが復元された後、クォーラム サーバへの接続が維持されていれば、AX は同期と通常の障害処理を再開します。

停電から復旧する

停電やシステム シャットダウンの後にシステムを再起動する場合、ztC Edge システムはゲスト VM の起動を行う前に、まずそのパートナーがブートして応答するまで待機します。以前アクティブだった AX がクォーラム サーバにアクセスできる場合には、AX がパートナー ノードのブートを待たずにゲスト VM を直ちに起動します。以前スタンバイだった AX が最初にブートした場合、この AX はパートナー ノードを待機します。

システムがパートナー ノードまたはクォーラム サーバのいずれかから応答を受け取ると、正常な運用が再開されて VM が起動します。その際、その他のケースと同じ障害処理規則が適用されます。

システムがクォーラム サーバからの応答を受け取らない場合や、システムにクォーラム サーバがない場合、ユーザが手作業でゲスト VM を強制的にブートする必要があります。これは AX または障害処理機能によって下されたすべての判断を上書きします。node0 と node1 でそれぞれ異なるユーザが同じゲスト VM をブートすることは避けてください。そうすると、誤ってスプリット ブレーン状態を引き起こす結果となります。

ナレッジ ベースの記事にアクセスする

Stratus カスタマ サービス ポータルは、ztC Edge を含む Stratus の全製品に関する技術的な記事を収めた検索可能な**ナレッジ ベース**を提供します。状況によっては、オンラインのヘルプがこれらのナレッジ ベース記事を直接参照する場合もあります (例: KB-*nnnn*)。カスタマ サービス ポータルおよびナレッジ ベースにアクセスするには、既存のサービス ポータル資格情報を使用するか、次の手順に従って新しいユーザ アカウントを作成してください。

ナレッジ ベースにアクセスするには

1. **Stratus カスタマ サービス ポータル** (<https://support.stratus.com>) にログインします。

必要な場合は次の手順で新しいアカウントを作成します。

- a. **[Register Account (アカウントの登録)]** をクリックします。
- b. 勤務先の電子メール アドレスと連絡先情報を入力して **[Register (登録)]** をクリックします。

勤務先電子メール アドレスには Stratus の登録顧客企業のドメイン名 (たとえば「stratus.com」) を含める必要があります。
- c. Stratus から受け取った電子メールに記載されているリンクをクリックします。
- d. 新しいパスワードを入力してアカウントの構成を完了します。

アカウントの作成に関してヘルプが必要な場合は Stratus 認定サービス業者に連絡してください。

- サービス ポータルで左側パネルにある **[Knowledge Base (ナレッジ ベース)]** をクリックします。
- [Keyword Search (キーワード検索)]** ボックスに、必要な情報に関連するキーワードを入力してから、**[Search (検索)]** をクリックします。

記事番号 (KB-*nnnn*) で記事を検索するには、**[Advanced Search (高度な検索)]** をクリックします。**[Search by ID (ID で検索)]** の横に記事の ID 番号 (*nnnn*) を入力して **[表示]** をクリックします。

関連トピック

[「関連ドキュメント」](#)

修正された CVE

以下に、それぞれのリリースで修正された共通脆弱性識別子 (CVE: Common Vulnerabilities and Exposures) を一覧します。

Stratus Redundant Linux リリース 2.3.0.0 で修正された CVE

次の表に、このリリースで修正された CVE を一覧します (必要に応じてドロップダウン アイコンをクリックしてください)。

このリリースで修正された CVE		
CVE-2013-2139	CVE-2015-2716	CVE-2015-6360
CVE-2016-5766	CVE-2017-12652	CVE-2017-15715
CVE-2017-18190	CVE-2017-18551	CVE-2018-1283
CVE-2018-1303	CVE-2018-11782	CVE-2018-15746
CVE-2018-19662	CVE-2018-20836	CVE-2018-20843
CVE-2019-2974	CVE-2019-5094	CVE-2019-5188

このリリースで修正された CVE		
CVE-2019-5482	CVE-2019-6237	CVE-2019-6251
CVE-2019-6978	CVE-2019-7572	CVE-2019-7573
CVE-2019-7574	CVE-2019-7575	CVE-2019-7576
CVE-2019-7577	CVE-2019-7578	CVE-2019-7635
CVE-2019-7636	CVE-2019-7637	CVE-2019-7638
CVE-2019-8506	CVE-2019-8524	CVE-2019-8535
CVE-2019-8536	CVE-2019-8544	CVE-2019-8551
CVE-2019-8558	CVE-2019-8559	CVE-2019-8563
CVE-2019-8571	CVE-2019-8583	CVE-2019-8584
CVE-2019-8586	CVE-2019-8587	CVE-2019-8594
CVE-2019-8595	CVE-2019-8596	CVE-2019-8597
CVE-2019-8601	CVE-2019-8607	CVE-2019-8608
CVE-2019-8609	CVE-2019-8610	CVE-2019-8611
CVE-2019-8615	CVE-2019-8619	CVE-2019-8622
CVE-2019-8623	CVE-2019-8625	CVE-2019-8644
CVE-2019-8649	CVE-2019-8658	CVE-2019-8666
CVE-2019-8669	CVE-2019-8671	CVE-2019-8672
CVE-2019-8673	CVE-2019-8674	CVE-2019-8675
CVE-2019-8676	CVE-2019-8677	CVE-2019-8678

このリリースで修正された CVE		
CVE-2019-8679	CVE-2019-8680	CVE-2019-8681
CVE-2019-8683	CVE-2019-8684	CVE-2019-8686
CVE-2019-8687	CVE-2019-8688	CVE-2019-8689
CVE-2019-8690	CVE-2019-8696	CVE-2019-8707
CVE-2019-8710	CVE-2019-8719	CVE-2019-8720
CVE-2019-8726	CVE-2019-8733	CVE-2019-8735
CVE-2019-8743	CVE-2019-8763	CVE-2019-8764
CVE-2019-8765	CVE-2019-8766	CVE-2019-8768
CVE-2019-8769	CVE-2019-8771	CVE-2019-8782
CVE-2019-8783	CVE-2019-8808	CVE-2019-8811
CVE-2019-8812	CVE-2019-8813	CVE-2019-8814
CVE-2019-8815	CVE-2019-8816	CVE-2019-8819
CVE-2019-8820	CVE-2019-8821	CVE-2019-8822
CVE-2019-8823	CVE-2019-8835	CVE-2019-8844
CVE-2019-8846	CVE-2019-9454	CVE-2019-9458
CVE-2019-10098	CVE-2019-10208	CVE-2019-11068
CVE-2019-11070	CVE-2019-11719	CVE-2019-11727
CVE-2019-11756	CVE-2019-12450	CVE-2019-12614
CVE-2019-12749	CVE-2019-14494	CVE-2019-14744

このリリースで修正された CVE		
CVE-2019-14822	CVE-2019-14834	CVE-2019-14866
CVE-2019-14907	CVE-2019-14973	CVE-2019-15217
CVE-2019-15691	CVE-2019-15692	CVE-2019-15693
CVE-2019-15694	CVE-2019-15695	CVE-2019-15807
CVE-2019-15903	CVE-2019-15917	CVE-2019-16231
CVE-2019-16233	CVE-2019-16707	CVE-2019-16935
CVE-2019-16994	CVE-2019-17006	CVE-2019-17023
CVE-2019-17053	CVE-2019-17055	CVE-2019-17498
CVE-2019-17546	CVE-2019-17563	CVE-2019-18197
CVE-2019-18282	CVE-2019-18808	CVE-2019-19046
CVE-2019-19055	CVE-2019-19058	CVE-2019-19059
CVE-2019-19062	CVE-2019-19063	CVE-2019-19126
CVE-2019-19332	CVE-2019-19447	CVE-2019-19523
CVE-2019-19524	CVE-2019-19530	CVE-2019-19532
CVE-2019-19534	CVE-2019-19537	CVE-2019-19767
CVE-2019-19807	CVE-2019-19956	CVE-2019-20054
CVE-2019-20095	CVE-2019-20382	CVE-2019-20386
CVE-2019-20388	CVE-2019-20485	CVE-2019-20636
CVE-2019-20811	CVE-2019-20907	CVE-2019-25013

このリリースで修正された CVE		
CVE-2020-0427	CVE-2020-1472	CVE-2020-1749
CVE-2020-1927	CVE-2020-1934	CVE-2020-1935
CVE-2020-1971	CVE-2020-1983	CVE-2020-2574
CVE-2020-2732	CVE-2020-2752	CVE-2020-2780
CVE-2020-2812	CVE-2020-3862	CVE-2020-3864
CVE-2020-3865	CVE-2020-3867	CVE-2020-3868
CVE-2020-3885	CVE-2020-3894	CVE-2020-3895
CVE-2020-3897	CVE-2020-3899	CVE-2020-3900
CVE-2020-3901	CVE-2020-3902	CVE-2020-5313
CVE-2020-6829	CVE-2020-7053	CVE-2020-7595
CVE-2020-8177	CVE-2020-8622	CVE-2020-8623
CVE-2020-8624	CVE-2020-8625	CVE-2020-8647
CVE-2020-8649	CVE-2020-8695	CVE-2020-8696
CVE-2020-8698	CVE-2020-9383	CVE-2020-10018
CVE-2020-10029	CVE-2020-10543	CVE-2020-10690
CVE-2020-10703	CVE-2020-10713	CVE-2020-10732
CVE-2020-10742	CVE-2020-10751	CVE-2020-10754
CVE-2020-10769	CVE-2020-10878	CVE-2020-10942
CVE-2020-11078	CVE-2020-11565	CVE-2020-11761

このリリースで修正された CVE		
CVE-2020-11763	CVE-2020-11764	CVE-2020-11793
CVE-2020-12243	CVE-2020-12321	CVE-2020-12351
CVE-2020-12352	CVE-2020-12400	CVE-2020-12401
CVE-2020-12402	CVE-2020-12403	CVE-2020-12723
CVE-2020-12770	CVE-2020-12825	CVE-2020-12826
CVE-2020-13765	CVE-2020-13935	CVE-2020-14305
CVE-2020-14308	CVE-2020-14309	CVE-2020-14310
CVE-2020-14311	CVE-2020-14314	CVE-2020-14318
CVE-2020-14323	CVE-2020-14331	CVE-2020-14345
CVE-2020-14346	CVE-2020-14347	CVE-2020-14351
CVE-2020-14355	CVE-2020-14360	CVE-2020-14361
CVE-2020-14362	CVE-2020-14363	CVE-2020-14364
CVE-2020-14372	CVE-2020-14385	CVE-2020-14779
CVE-2020-14781	CVE-2020-14782	CVE-2020-14792
CVE-2020-14796	CVE-2020-14797	CVE-2020-14803
CVE-2020-15436	CVE-2020-15705	CVE-2020-15706
CVE-2020-15707	CVE-2020-15862	CVE-2020-15999
CVE-2020-16092	CVE-2020-17507	CVE-2020-24394
CVE-2020-25211	CVE-2020-25212	CVE-2020-25632

このリリースで修正された CVE		
CVE-2020-25637	CVE-2020-25643	CVE-2020-25645
CVE-2020-25647	CVE-2020-25648	CVE-2020-25656
CVE-2020-25684	CVE-2020-25685	CVE-2020-25686
CVE-2020-25692	CVE-2020-25694	CVE-2020-25695
CVE-2020-25705	CVE-2020-25712	CVE-2020-27749
CVE-2020-27779	CVE-2020-28374	CVE-2020-29573
CVE-2020-29599	CVE-2020-29661	CVE-2020-35513
CVE-2021-2144	CVE-2021-2163	CVE-2021-3156
CVE-2021-20225	CVE-2021-20233	CVE-2021-20265
CVE-2021-20305	CVE-2021-25215	CVE-2021-27219
CVE-2021-27363	CVE-2021-27364	CVE-2021-27365
CVE-2021-27803		

Stratus Redundant Linux リリース 2.2.0.0 で修正された CVE

次の表に、このリリースで修正された CVE を一覧します (必要に応じてドロップダウン アイコンをクリックしてください)。

このリリースで修正された CVE		
CVE-2015-2716	CVE-2015-8035	CVE-2015-9289
CVE-2016-5131	CVE-2017-6519	CVE-2017-11166
CVE-2017-12805	CVE-2017-12806	CVE-2017-15412

このリリースで修正された CVE		
CVE-2017-15710	CVE-2017-17807	CVE-2017-18251
CVE-2017-18252	CVE-2017-18254	CVE-2017-18258
CVE-2017-18271	CVE-2017-18273	CVE-2017-18595
CVE-2017-1000476	CVE-2018-1116	CVE-2018-1301
CVE-2018-4180	CVE-2018-4181	CVE-2018-4300
CVE-2018-4700	CVE-2018-5712	CVE-2018-5745
CVE-2018-7191	CVE-2018-7418	CVE-2018-7584
CVE-2018-8804	CVE-2018-9133	CVE-2018-10177
CVE-2018-10360	CVE-2018-10547	CVE-2018-10804
CVE-2018-10805	CVE-2018-11362	CVE-2018-11439
CVE-2018-11656	CVE-2018-12599	CVE-2018-12600
CVE-2018-13139	CVE-2018-13153	CVE-2018-14340
CVE-2018-14341	CVE-2018-14368	CVE-2018-14404
CVE-2018-14434	CVE-2018-14435	CVE-2018-14436
CVE-2018-14437	CVE-2018-14567	CVE-2018-15518
CVE-2018-15587	CVE-2018-15607	CVE-2018-16057
CVE-2018-16328	CVE-2018-16749	CVE-2018-16750
CVE-2018-17199	CVE-2018-18066	CVE-2018-18544
CVE-2018-18751	CVE-2018-19622	CVE-22018-19869

このリリースで修正された CVE		
CVE-2018-19870	CVE-2018-19871	CVE-2018-19872
CVE-2018-19873	CVE-2018-19985	CVE-2018-20169
CVE-2018-20467	CVE-2018-20852	CVE-2018-21009
CVE-2019-2737	CVE-2019-2739	CVE-2019-2740
CVE-2019-2805	CVE-2019-3820	CVE-2019-3880
CVE-2019-3890	CVE-2019-3901	CVE-2019-5436
CVE-2019-6465	CVE-2019-6477	CVE-2019-7175
CVE-2019-7397	CVE-2019-7398	CVE-2019-9024
CVE-2019-9503	CVE-2019-9924	CVE-2019-9956
CVE-2019-9959	CVE-2019-10131	CVE-2019-10197
CVE-2019-10207	CVE-2019-10218	CVE-2019-10638
CVE-2019-10639	CVE-2019-10650	CVE-2019-10871
CVE-2019-11190	CVE-2019-11459	CVE-2019-11470
CVE-2019-11472	CVE-2019-11487	CVE-2019-11597
CVE-2019-11598	CVE-2019-11884	CVE-2019-12293
CVE-2019-12382	CVE-2019-12779	CVE-2019-12974
CVE-2019-12975	CVE-2019-12976	CVE-2019-12978
CVE-2019-12979	CVE-2019-13133	CVE-2019-13134
CVE-2019-13135	CVE-2019-13232	CVE-2019-13233

このリリースで修正された CVE		
CVE-2019-13295	CVE-2019-13297	CVE-2019-13300
CVE-2019-13301	CVE-2019-13304	CVE-2019-13305
CVE-2019-13306	CVE-2019-13307	CVE-2019-13309
CVE-2019-13310	CVE-2019-13311	CVE-2019-13454
CVE-2019-13648	CVE-2019-14283	CVE-2019-14815
CVE-2019-14980	CVE-2019-14981	CVE-2019-15090
CVE-2019-15139	CVE-2019-15140	CVE-2019-15141
CVE-2019-15221	CVE-2019-15605	CVE-2019-15916
CVE-2019-16056	CVE-2019-16708	CVE-2019-16709
CVE-2019-16710	CVE-2019-16711	CVE-2019-16712
CVE-2019-16713	CVE-2019-16746	CVE-2019-16865
CVE-2019-17041	CVE-2019-17042	CVE-2019-17540
CVE-2019-17541	CVE-2019-17666	CVE-2019-18634
CVE-2019-18660	CVE-2019-19338	CVE-2019-19527
CVE-2019-19768	CVE-2019-19948	CVE-2019-19949
CVE-2020-0543	CVE-2020-0548	CVE-2020-0549
CVE-2020-1938	CVE-2020-2754	CVE-2020-2755
CVE-2020-2756	CVE-2020-2757	CVE-2020-2773
CVE-2020-2781	CVE-2020-2800	CVE-2020-2803

このリリースで修正された CVE		
CVE-2020-2805	CVE-2020-2830	CVE-2020-2922
CVE-2020-5208	CVE-2020-5260	CVE-2020-5312
CVE-2020-7039	CVE-2020-8112	CVE-2020-8597
CVE-2020-8608	CVE-2020-8616	CVE-2020-8617
CVE-2020-9484	CVE-2020-10188	CVE-2020-10531
CVE-2020-10711	CVE-2020-10757	CVE-2020-10772
CVE-2020-11008	CVE-2020-12049	CVE-2020-12351
CVE-2020-12352	CVE-2020-12653	CVE-2020-12654
CVE-2020-12662	CVE-2020-12663	CVE-2020-12888
CVE-2020-14364	CVE-2020-14556	CVE-2020-14577
CVE-2020-14578	CVE-2020-14579	CVE-2020-14583
CVE-2020-14593	CVE-2020-14621	

Stratus Redundant Linux リリース 2.1.0.0 で修正された CVE

次の表に、このリリースで修正された CVE を一覧します (必要に応じてドロップダウン アイコンをクリックしてください)。

このリリースで修正された CVE		
CVE-2016-3186	CVE-2016-3616	CVE-2016-10713
CVE-2016-10739	CVE-2017-5731	CVE-2017-5732
CVE-2017-5733	CVE-2017-5734	CVE-2017-5735

このリリースで修正された CVE		
CVE-2017-14503	CVE-2017-17742	CVE-2018-0495
CVE-2018-0734	CVE-2018-1050	CVE-2018-1111
CVE-2018-1122	CVE-2018-1139	CVE-2018-1312
CVE-2018-3058	CVE-2018-3063	CVE-2018-3066
CVE-2018-3081	CVE-2018-3282	CVE-2018-3613
CVE-2018-5383	CVE-2018-5407	CVE-2018-5741
CVE-2018-6790	CVE-2018-6914	CVE-2018-6952
CVE-2018-7159	CVE-2018-7409	CVE-2018-7456
CVE-2018-7485	CVE-2018-7755	CVE-2018-8087
CVE-2018-8777	CVE-2018-8778	CVE-2018-8779
CVE-2018-8780	CVE-2018-8905	CVE-2018-9363
CVE-2018-9516	CVE-2018-9517	CVE-2018-10689
CVE-2018-10779	CVE-2018-10853	CVE-2018-10858
CVE-2018-10904	CVE-2018-10907	CVE-2018-10911
CVE-2018-10913	CVE-2018-10914	CVE-2018-10923
CVE-2018-10926	CVE-2018-10927	CVE-2018-10928
CVE-2018-10929	CVE-2018-10930	CVE-2018-10963
CVE-2018-11212	CVE-2018-11213	CVE-2018-11214
CVE-2018-11645	CVE-2018-11813	CVE-2018-12015

このリリースで修正された CVE		
CVE-2018-12121	CVE-2018-12181	CVE-2018-12327
CVE-2018-12404	CVE-2018-12641	CVE-2018-12697
CVE-2018-12900	CVE-2018-13053	CVE-2018-13093
CVE-2018-13094	CVE-2018-13095	CVE-2018-13346
CVE-2018-13347	CVE-2018-14348	CVE-2018-14498
CVE-2018-14598	CVE-2018-14599	CVE-2018-14600
CVE-2018-14625	CVE-2018-14647	CVE-2018-14651
CVE-2018-14652	CVE-2018-14653	CVE-2018-14654
CVE-2018-14659	CVE-2018-14660	CVE-2018-14661
CVE-2018-14734	CVE-2018-15473	CVE-2018-15594
CVE-2018-15686	CVE-2018-15853	CVE-2018-15854
CVE-2018-15855	CVE-2018-15856	CVE-2018-15857
CVE-2018-15859	CVE-2018-15861	CVE-2018-15862
CVE-2018-15863	CVE-2018-15864	CVE-2018-16062
CVE-2018-16396	CVE-2018-16402	CVE-2018-16403
CVE-2018-16646	CVE-2018-16658	CVE-2018-16838
CVE-2018-16842	CVE-2018-16866	CVE-2018-16881
CVE-2018-16885	CVE-2018-16888	CVE-2018-17100
CVE-2018-17101	CVE-2018-17336	CVE-2018-18074

このリリースで修正された CVE		
CVE-2018-18281	CVE-2018-18310	CVE-2018-18384
CVE-2018-18520	CVE-2018-18521	CVE-2018-18557
CVE-2018-18661	CVE-2018-18897	CVE-2018-19058
CVE-2018-19059	CVE-2018-19060	CVE-2018-19149
CVE-2018-19519	CVE-2018-19788	CVE-2018-20060
CVE-2018-20481	CVE-2018-20650	CVE-2018-20662
CVE-2018-20856	CVE-2018-20969	CVE-2018-1000073
CVE-2018-1000074	CVE-2018-1000075	CVE-2018-1000076
CVE-2018-1000077	CVE-2018-1000078	CVE-2018-1000079
CVE-2018-1000132	CVE-2018-1000876	CVE-2018-1000877
CVE-2018-1000878	CVE-2019-0154	CVE-2019-0155
CVE-2019-0160	CVE-2019-0161	CVE-2019-0217
CVE-2019-0220	CVE-2019-1125	CVE-2019-1387
CVE-2019-1559	CVE-2019-2503	CVE-2019-2529
CVE-2019-2614	CVE-2019-2627	CVE-2019-2945
CVE-2019-2949	CVE-2019-2962	CVE-2019-2964
CVE-2019-2973	CVE-2019-2975	CVE-2019-2978
CVE-2019-2981	CVE-2019-2983	CVE-2019-2987
CVE-2019-2988	CVE-2019-2989	CVE-2019-2992

このリリースで修正された CVE		
CVE-2019-2999	CVE-2019-3459	CVE-2019-3460
CVE-2019-3811	CVE-2019-3827	CVE-2019-3840
CVE-2019-3846	CVE-2019-3858	CVE-2019-3861
CVE-2019-3880	CVE-2019-3882	CVE-2019-3900
CVE-2019-5010	CVE-2019-5489	CVE-2019-6470
CVE-2019-7149	CVE-2019-7150	CVE-2019-7222
CVE-2019-7310	CVE-2019-7664	CVE-2019-7665
CVE-2019-9200	CVE-2019-9500	CVE-2019-9506
CVE-2019-9631	CVE-2019-9740	CVE-2019-9824
CVE-2019-9947	CVE-2019-9948	CVE-2019-10086
CVE-2019-10126	CVE-2019-10216	CVE-2019-11043
CVE-2019-11135	CVE-2019-11236	CVE-2019-11599
CVE-2019-11729	CVE-2019-11745	CVE-2019-11810
CVE-2019-11833	CVE-2019-12155	CVE-2019-13616
CVE-2019-13638	CVE-2019-13734	CVE-2019-14287
CVE-2019-14378	CVE-2019-14744	CVE-2019-14811
CVE-2019-14812	CVE-2019-14813	CVE-2019-14816
CVE-2019-14817	CVE-2019-14821	CVE-2019-14835
CVE-2019-14869	CVE-2019-14895	CVE-2019-14898

このリリースで修正された CVE		
CVE-2019-14901	CVE-2019-14906	CVE-2019-15239
CVE-2019-17133	CVE-2019-18397	CVE-2019-18408
CVE-2019-1000019	CVE-2019-1000020	CVE-2019-1010238
CVE-2020-2583	CVE-2020-2590	CVE-2020-2593
CVE-2020-2601	CVE-2020-2604	CVE-2020-2654
CVE-2020-2659		

Stratus Redundant Linux リリース 2.0.1.0 で修正された CVE

次の表に、このリリースで修正された CVE を一覧します (必要に応じてドロップダウン アイコンをクリックしてください)。

このリリースで修正された CVE		
CVE-2015-8830	CVE-2015-9262	CVE-2016-4913
CVE-2016-9396	CVE-2017-0861	CVE-2017-3735
CVE-2017-10661	CVE-2017-16997	CVE-2017-17805
CVE-2017-18198	CVE-2017-18199	CVE-2017-18201
CVE-2017-18208	CVE-2017-18232	CVE-2017-18267
CVE-2017-18344	CVE-2017-18360	CVE-2017-1000050
CVE-2018-0494	CVE-2018-0495	CVE-2018-0732
CVE-2018-0737	CVE-2018-0739	CVE-2018-1050
CVE-2018-1060	CVE-2018-1061	CVE-2018-1092

このリリースで修正された CVE		
CVE-2018-1094	CVE-2018-1113	CVE-2018-1118
CVE-2018-1120	CVE-2018-1130	CVE-2018-1139
CVE-2018-1304	CVE-2018-1305	CVE-2018-5344
CVE-2018-5391	CVE-2018-5407	CVE-2018-5729
CVE-2018-5730	CVE-2018-5742	CVE-2018-5743
CVE-2018-5803	CVE-2018-5848	CVE-2018-6485
CVE-2018-6764	CVE-2018-7208	CVE-2018-7568
CVE-2018-7569	CVE-2018-7642	CVE-2018-7643
CVE-2018-7740	CVE-2018-7757	CVE-2018-8014
CVE-2018-8034	CVE-2018-8781	CVE-2018-8945
CVE-2018-9568	CVE-2018-10322	CVE-2018-10372
CVE-2018-10373	CVE-2018-10534	CVE-2018-10535
CVE-2018-10733	CVE-2018-10767	CVE-2018-10768
CVE-2018-10844	CVE-2018-10845	CVE-2018-10846
CVE-2018-10852	CVE-2018-10858	CVE-2018-10878
CVE-2018-10879	CVE-2018-10881	CVE-2018-10883
CVE-2018-10902	CVE-2018-10906	CVE-2018-10911
CVE-2018-10940	CVE-2018-11236	CVE-2018-11237
CVE-2018-11784	CVE-2018-12126	CVE-2018-12127

このリリースで修正された CVE		
CVE-2018-12130	CVE-2018-12180	CVE-2018-12910
CVE-2018-13033	CVE-2018-13405	CVE-2018-13988
CVE-2018-14526	CVE-2018-14618	CVE-2018-14633
CVE-2018-14646	CVE-2018-14665	CVE-2018-15688
CVE-2018-15908	CVE-2018-15909	CVE-2018-15911
CVE-2018-16395	CVE-2018-16511	CVE-2018-16539
CVE-2018-16540	CVE-2018-16541	CVE-2018-16802
CVE-2018-16863	CVE-2018-16864	CVE-2018-16865
CVE-2018-16871	CVE-2018-16884	CVE-2018-17183
CVE-2018-17456	CVE-2018-17961	CVE-2018-17972
CVE-2018-18073	CVE-2018-18284	CVE-2018-18311
CVE-2018-18397	CVE-2018-18445	CVE-2018-18559
CVE-2018-18690	CVE-2018-19134	CVE-2018-19409
CVE-2018-19475	CVE-2018-19476	CVE-2018-19477
CVE-2018-1000007	CVE-2018-1000026	CVE-2018-1000120
CVE-2018-1000121	CVE-2018-1000122	CVE-2018-1000301
CVE-2019-2422	CVE-2019-2602	CVE-2019-2684
CVE-2019-2698	CVE-2019-2745	CVE-2019-2762
CVE-2019-2769	CVE-2019-2786	CVE-2019-2816

このリリースで修正された CVE		
CVE-2019-2842	CVE-2019-3813	CVE-2019-3815
CVE-2019-3835	CVE-2019-3838	CVE-2019-3839
CVE-2019-3855	CVE-2019-3856	CVE-2019-3857
CVE-2019-3862	CVE-2019-3863	CVE-2019-5953
CVE-2019-6116	CVE-2019-6133	CVE-2019-6454
CVE-2019-6778	CVE-2019-6974	CVE-2019-7221
CVE-2019-8322	CVE-2019-8323	CVE-2019-8324
CVE-2019-8325	CVE-2019-9636	CVE-2019-10132
CVE-2019-10160	CVE-2019-10161	CVE-2019-10166
CVE-2019-10167	CVE-2019-10168	CVE-2019-11085
CVE-2019-11091	CVE-2019-11477	CVE-2019-11478
CVE-2019-11479	CVE-2019-11811	CVE-2019-12735

Stratus Redundant Linux リリース 2.0.0.0 で修正された CVE

次の表に、このリリースで修正された CVE を一覧します (必要に応じてドロップダウン アイコンをクリックしてください)。

このリリースで修正された CVE		
CVE-2016-2183	CVE-2017-3636	CVE-2017-3641
CVE-2017-3651	CVE-2017-3653	CVE-2017-10268
CVE-2017-10378	CVE-2017-10379	CVE-2017-10384

このリリースで修正された CVE		
CVE-2017-11600	CVE-2017-13215	CVE-2018-1336
CVE-2018-2562	CVE-2018-2622	CVE-2018-2640
CVE-2018-2665	CVE-2018-2668	CVE-2018-2755
CVE-2018-2761	CVE-2018-2767	CVE-2018-2771
CVE-2018-2781	CVE-2018-2813	CVE-2018-2817
CVE-2018-2819	CVE-2018-2952	CVE-2018-3133
CVE-2018-3136	CVE-2018-3139	CVE-2018-3149
CVE-2018-3169	CVE-2018-3180	CVE-2018-3183
CVE-2018-3214	CVE-2018-3620	CVE-2018-3639
CVE-2018-3646	CVE-2018-3665	CVE-2018-3693
CVE-2018-5390	CVE-2018-5740	CVE-2018-7550
CVE-2018-7566	CVE-2018-8088	CVE-2018-10194
CVE-2018-10675	CVE-2018-10873	CVE-2018-10897
CVE-2018-10915	CVE-2018-11235	CVE-2018-11806
CVE-2018-12020	CVE-2018-12384	CVE-2018-14634
CVE-2018-15910	CVE-2018-16509	CVE-2018-16542
CVE-2018-1002200		

REST API

説明

物理マシンのプロパティ、統計、システム パフォーマンス、現在のアラート リストなどを含むシステム情報を取得します。多量 (約 14 KB) の情報が返されることがあります。

ヘッダ

ヘッダ	値	必須
Locale	de (ドイツ語)、en-US (英語)、ja (日本語)、zh-CN (中国語)、または pt-br (ポルトガル語)。デフォルトのロケールは en-US です。	いいえ
Content-type	application/json	はい

エンドポイント

GET /system/overview

例

要求 URL:

`https://{hostname or IP address}/restapi/system/overview`

11

第 11 章: セキュリティ

ztC Edge システムに最高レベルのセキュリティを提供するために設定できる追加の構成についての詳細は、[「セキュリティの強化」](#)を参照してください。

セキュリティの詳細については、以下のトピックを参照してください。

- [「修正された CVE」](#)
- [「iptables を管理する」](#)
- [「セキュアな接続を構成する」](#)
- [「ユーザとグループを構成する」](#)
- [「Active Directory を構成する」](#)
- [「\[監査ログ\] ページ」](#)

セキュリティの強化

Stratus ztC Edge システムではセキュアな Out-Of-Box Experience (OOBE) が提供されますが、以下の説明に従ってさらに追加の構成を行うことにより、最高レベルのセキュリティを確保することが可能です。

セキュリティの設定においては、保護と使いやすさのバランスを保つことが重要です。ztC Edge システムは、これらの要素のバランスを保つ一連のデフォルト設定が行われた状態で出荷されます。さらにセキュアなシステムを展開するには、以下のガイドラインに従ってください。計画から構成、運用、廃止に至るまで、システムのライフサイクル全体にわたって継続的にセキュリティを評価することができます。

下記の情報は、"CIS Controls" のバージョン 7.1 に基づくセキュリティ強化のための手引きです。これは、IT システムとデータのセキュリティ保護に関するベスト プラクティスのリーダーとして知られるコミュニティベースの非営利団体 Center for Internet Security (CIS) によって開発された、セキュリティ強化のための推奨事項です。"CIS ベンチマーク" は、セキュアな製品のベースラインを検証し作成するためにも使用されます。CIS Controls の一覧は、下記の「[標準化団体のベスト プラクティスと標準](#)」に記載されています。

以下の情報には、産業制御システムのサイバー セキュリティ標準 ISA/IEC 62443 に基づくセキュリティ強化の手引きも含まれています。この標準は国際計測制御学会 (ISA: International Society of Automation) によって当初作成されたもので、国際電気標準会議 (IEC: International Electrotechnical Commission) による改訂が続けられています。ISA/IEC 62443-4-2 にはデータの機密性や意図的な脅威の行為者・敵対者に基づいた各種のセキュリティ レベルがあり、推奨項目を実施し緩和制御を適用することによって、必要なセキュリティ レベルのコンプライアンスを達成するのに役立ちます。ISA/IEC 62443-4-2 の要件の概要は、下記の「[標準化団体のベスト プラクティスと標準](#)」に含まれています。

このトピックは以下のセクションで構成されています。

- [セキュリティ ガイドライン](#)
- [高度なセキュリティ ガイドライン](#)
- [標準化団体のベスト プラクティスと標準](#)

セキュリティ ガイドライン

次のセクションでは、ztC Edge システムのセキュリティ ガイドラインについて説明します。

注: Stratus では以下のガイドラインをテスト済みで、サポートしています。Stratus によって明示的に承認されていないその他すべての更新や変更は、システムの正常動作に影響する可能性があります。



これらのガイドラインに関して疑問な点があり、システムにサービス契約が適用される場合には、Stratus 認定サービス業者まで問い合わせてください。詳細については、**ztC Edge サポート ページ** (<https://www.stratus.com/services-support/customer-support/?tab=ztcedge>) を参照してください。

セキュリティ強化のガイドラインを実施する際、以下を考慮してください。

- このセキュリティ ガイドラインは、ztC Edge コンソールおよびホスト オペレーティング システムで実行される管理タスクに適用されます。ztC Edge コンソールは、ztC Edge システムの大半

の機能についての管理とモニタリングをリモートの管理コンピュータから行うことができる、ブラウザベースのインタフェースです ([「ztC Edge コンソール」](#) を参照)。ホスト オペレーティング システムは、システムの各ノード上で稼働します。ホスト オペレーティング システムのコマンド ラインには、PM の物理コンソールからローカルに、あるいはセキュア シェル (SSH) クライアントを用いてリモートでアクセスできます ([「ホスト オペレーティング システムにアクセスする」](#) を参照)。

- 構成を変更する前に、後で必要に応じて復元できるように現在の設定を記録しておきます。また、どのような変更を行うかもすべて記録してください。この情報はトラブルシューティングで必要となる可能性があります。
- 特にホスト オペレーティング システムにおいて、デフォルトのシステム設定を変更する際は、両方のノードで変更を行わなければなりません。そうでない場合、不整合が生じた結果システムの正常動作に影響を及ぼす可能性があります。同様に、root のパスワードやホスト オペレーティング システムのその他のユーザ アカウントの設定を変更する場合にも、両方のノードで行う必要があります。下記のガイドラインは、どのような状況でこれらの変更が必要となるかを示しています。
- システム ソフトウェアをアップグレードしたりシステム内のノードを交換するときに、システム強化のための変更がすべて移行されないことがあります。同様に、一部の設定は複数のノードで共有されるため、共有リソースに競合が生じる可能性もあります。したがって、これらの手順を完了した後は、システムの各ノードについて、正しい設定が適用され正しく動作していることを検証する必要があります。
- セキュリティ ガイドラインでは、ztC Edge システムと Stratus Redundant Linux ソフトウェアの構成に関する詳細が記載されているナレッジ ベース記事を直接参照する場合があります (例: KB-[nnnn](#))。Stratus のカスタマ サービス ポータルおよびナレッジ ベースにアクセスするには、既存のサービス ポータル資格情報を使用するか、[「ナレッジ ベースの記事にアクセスする」](#) の手順に従って新しいユーザ アカウントを作成してください。

ポートとプロトコル

システムに対してネットワーキングや通信に関する変更を行うすべての管理者は、Stratus Redundant Linux で使用されるポートやプロトコルについて精通する必要があります。詳細については、KB-[9357](#) を参照してください。

ネットワーク セグメンテーション

ztC Edge システムは、信頼済みのデバイスか、デバイス同士の通信に明示的な許可が必要とされるネットワークのみに接続してください。ネットワーク セグメンテーションの詳細については、NIST の特別刊行物 800-125B および 800-39 を参照してください。ztC Edge システムで利用できるイーサネットネットワークの詳細については、[「ネットワーク アーキテクチャ」](#)を参照してください。

IP テーブルとファイアウォール

システムの IP テーブル パケット フィルタ処理を有効化して、通常の操作で使用されないポートをすべてブロックします。悪意のある行為者が、未使用のインタフェースをバックドアとして潜在的なセキュリティ脆弱性を利用することがあります。未使用のポートの IP テーブルを有効化して、エクスポージャを制限してください。

IP テーブルの実装方法の詳細については、[「iptables を管理する」](#)を参照してください。

注:



- ztC Edge システム内の ping には ICMP プロトコルが使用されます。ICMP トラフィックをドロップするように IP テーブルを設定すると、フォールトトレランスやフェールオーバーのサポートが正しく機能しなくなります。
- ホスト オペレーティング システムへの接続には SSH プロトコルが使用されます。SSH トラフィックをブロックするように IP テーブルを設定すると、システム管理者がホスト オペレーティング システムにアクセスできなくなります。

ユーザ アカウントの作成

システムへのアクセスが承認されている各ユーザについて個別のユーザ アカウントを作成し、デバイスの使用に関するユーザのロールを検討します。個別のユーザ アカウントを維持することで監査や否認防止も可能になり、ログの確認によってデバイスにアクセスしたユーザや構成を変更したユーザを判定することができます。

ユーザの設定を構成する方法の詳細については、[「ユーザとグループを構成する」](#)を参照してください。

注:

- デフォルトの **admin** アカウントの設定を編集して名前とパスワードを変更する必要がありますが、このアカウントを削除することはできません。
- パスワードを忘れた場合の回復機能を有効にするには、**admin** も含めて各ユーザ アカウントの電子メール アドレスを指定する必要があります。また、メール サーバも有効化する必要があります。手順は「[メール サーバを構成する](#)」を参照してください。そうでないと、システムがパスワードのリセット メールを送信できません。

パスワードの作成

システムのデフォルトのパスワードは変更する必要があります。

ztC Edge コンソールの展開時、**admin** に新しいパスワードを指定するためのプロンプトが表示されます。ztC Edge コンソールのパスワード ポリシーでは、パスワードが以下の条件を満たしている必要があります。

- パスワードは最低 8 文字です。
- 大文字と小文字の両方を含めなければなりません。
- ユーザ名と同じであってははいけません。

ホスト オペレーティング システムの初回ログイン時、`root` に新しいパスワードを指定するためのプロンプトが表示されます。ホスト オペレーティング システムの `root` のパスワードを変更する際は、両方のノードで手作業によって変更する必要があります。詳細については、「[ホスト オペレーティング システムにアクセスする](#)」を参照してください。



注: ホスト オペレーティング システムの `root` のパスワードを変更する際は、パスワードを忘れないようにしてください。root のパスワードを紛失した場合、これを復旧するにはノードを交換するか再インストールしなければなりません。

ホスト オペレーティング システムにおけるパスワードの質を管理する方法の詳細については、「[高度なセキュリティ ガイドライン](#)」を参照してください。

最小権限

各ユーザのアクセスを、その役職やロールに該当する機能のみに制限します。

最小権限を実施することにより、権限のないユーザがそのロールより上のサービスにアクセスできないようにします。

各ユーザの権限を定義するロールの構成方法の詳細については、「[ユーザとグループを構成する](#)」を参照してください。

Active Directory

Active Directory 統合によって、認証と承認を一か所でまとめて行うことができます。Active Directory では、パスワードの複雑度を指定するグループ ポリシーを作成し、ローカルのセキュリティ ポリシーに基づいて適用できます。

ztC Edge システムを Active Directory ドメインに追加する方法の詳細については、「[Active Directory を構成する](#)」を参照してください。

時間の同期

時間の同期は重要です。これにより一括参照点が提供され、運用とセキュリティのプロセスが確実に同じ期間内で動作するようにできます。時間の参照によって、アプリケーションを更新する際にチェックと使用の時刻における信頼が得られ、日付と時刻に基づいてキーと証明書がまだ有効かどうかを確認できます。

ztC Edge システムに初めてログオンするときに、ネットワーク タイム プロトコル (NTP) サービスを有効化してシステム クロックを自動的に設定してください。NTP は、既知の信頼される NTP サーバを参照するように構成します。詳細は、「[日付と時刻を構成する](#)」を参照してください。



注: NTP の設定を正しく構成するには、必ず ztC Edge コンソールを使用してください。ホストオペレーティングシステム内で手動で構成することは避けてください。

セキュアな接続

デフォルトでは、ztC Edge コンソールは HTTPS プロトコルによるセキュアな接続のみをサポートするように構成されています。

ztC Edge システムで HTTPS を有効化すると、一般的な Web セキュリティ攻撃を防ぎ、個々の Web セッションにある程度の機密性を提供することが可能です。HTTPS は Web セッションのトラフィックを暗号化し、データの整合性を確保して、Web トラフィックの全体的なセキュリティを向上させます。

HTTPS が有効な場合、TLSv1.2 のみがサポートされます。これは現在推奨される最強の暗号化スイートです。暗号化方式には次が含まれます。

TLSv1.2:

暗号化方式:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 4096) - A
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 4096) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 4096) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 4096) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 4096) - A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 4096) - A
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 4096) - A
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 4096) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

また、メールサーバやその他のタイプのサーバソフトウェアを使用する際も、セキュアな暗号化接続を有効化してください。ztC Edge システム上でのメールサーバ用の暗号化された接続の構成と有効化の詳細については、[「メールサーバを構成する」](#)を参照してください。

SSL 証明書を更新する

ztC Edge システムには自己署名された SSL 証明書が付属していますが、これを任意の購入済みの、あるいは提供されている証明書に更新することができます。SSL 証明書の変更によって、信頼の元を顧客から指定されたものに更新できます。詳細については、KB-[9792](#) を参照してください。

SNMP の構成

簡易ネットワーク管理プロトコル (SNMP) は、アラームの受信、トラップの送信、およびシステムステータスのモニタリングに使用される標準プロトコルです。SNMP は、階層型に構成された管理情報ベース (MIB) に格納されているシステム定義情報を使用します。

セキュリティ上の理由から、顧客にとって ztC Edge システムのホストレベルで SNMP を無効化することが望ましい場合があります。必要な場合は iptables にルールを追加して ([「iptables を管理する」](#)を参照)、UDP ポート 162、161、199 および TCP ポート 162、199 をブロックし、すべての SNMP 接続を無効化することができます。

あるいは、SNMP の**制限あり**の構成を使用することもできます。すると SNMP 構成ファイルで SNMP v1 と v2 が無効化され、SNMPv3 のみが構成されます。詳細については、[「SNMP 設定を構成する」](#)を参照してください。



注: デフォルトでは、ztC Edge システムが SNMP v1 と v2 が有効な状態になっています。セキュリティ確保のためこれらのバージョンは無効化し、バージョン 3 のみを有効にする必要があります。

バックアップ

セキュリティ イベントが発生した場合のために、バックアップを準備しておくことが重要です。ユニットを既知の良好な状態に戻して運用を継続することができます。作成したすべてのバックアップはセキュアな場所に保存する必要があります。

VM とそのゲスト オペレーティング システムをバックアップするには、[「仮想マシンをエクスポートする」](#)を参照してください。SMBIOS UUID、システム シリアル番号、および MAC アドレスが元の VM と一致する同一の VM を復元するには、[「OVF ファイルから仮想マシンを交換/復元する」](#)を参照してください。

[基本設定] ページで構成した ztC Edge システムの基本設定をバックアップするには、設定をローカルのストレージデバイスかクラウドに保存します。詳細については、[「システム基本設定を保存または復元する」](#)を参照してください。

デュアルノード構成の冗長な ztC Edge システムでは、各ノードがもう片方のノードのバックアップとしても機能します。ノードに障害が発生した場合、システム内の現在ライセンスが適用されているノードを交換することができ、システムは稼働中のノードからの Stratus Redundant Linux ソフトウェアの正確なコピーと仮想マシンを使用して、そのノードを自動的に復元します。

自動ローカル サイト復旧

自動ローカル サイト復旧 (ALSR) 構成は、2 つの別々のサイトにある 2 台の物理マシンを接続します。これはディザスタ トレナントな展開方法で、ハードウェアの冗長性だけでなく、それを含む物理的なコンピュータ室や建物の冗長性も維持されます。地理的に離れているため、ALSR 構成にはコンポーネント配置の入念な計画と、より複雑なネットワーク トポロジが必要とされます。ALSR 構成にはクォーラム サービスを使用するよう、Stratus では強く推奨します。これは、ALSR 構成によって A-Link ネットワークが他の障害発生シナリオにさらされる可能性があるためです。ALSR 構成は、1 つのノード用に構成されているシステムでは利用できません。)

詳細については、[「ALSR 構成を作成する」](#)を参照してください。

監査

ローカル ポリシーによる監査を実施して、サイバー攻撃の検知、理解、およびそこから復旧に必要なイベントのログを定期的に収集し、管理します。

[監査ログ] ページには、ztC Edge コンソールにおけるユーザ アクティビティのログが表示されます。このページを開くには、左側のナビゲーション パネルで **[監査ログ]** をクリックします。(ztC Edge システムで発生したイベントのログを表示するには、[「\[アラート履歴\] ページ」](#)を参照してください。)

ログの情報には次が含まれています。

- 時刻 — アクションの日付と時刻。
- ユーザ名 — アクションを開始したユーザの名前。
- 発信元ホスト — ztC Edge コンソールを実行していたホストの IP アドレス。
- アクション — ztC Edge コンソールで実行されたアクション。

監査ログ情報の表示には `snmptable` を使用することもできます (詳細は、[「snmptable でシステム情報を取得する」](#)を参照してください)。

ログを使用して ztC Edge システムの継続的なモニタリングを行います。サービス コールの際に迅速なサービスを確保するため、システムのサポート通知と定期レポートも有効化して、Stratus にシステムの稼働状態に関する情報が随時提供されるようにします。詳細については、[「リモート サポート設定を構成する」](#)を参照してください。

ログイン バナー通知

ログイン バナー通知を構成して、ztC Edge コンソール ユーザ向けの重要な通知を含めます。詳細については、[「ログイン バナーを構成する」](#)を参照してください。

アップグレード

Stratus Redundant Linux を定期的にアップグレードして、古いコンポーネントに起因するセキュリティ脆弱性が悪用されるのを未然に防ぎます。アップグレードの頻度と方法についての情報は、ローカルのセキュリティ ポリシーを参照してください。



注意事項: ztC Edge システムの CentOS ホスト オペレーティング システムを、Stratus 以外のソースから更新しないでください。Stratus Redundant Linux ソフトウェアと一緒にインストールされる CentOS リリースのみを使用してください。

ztC Edge コンソールの **[アップグレード キット]** ページでは、お使いのシステムを新しいバージョンの Stratus Redundant Linux ソフトウェアにアップグレードするためのアップグレード キットのアップロードと管理を行えます。USB メディアにアップグレード キットをコピーして、このメディアをシステム ソフトウェアの再インストールに使用することもできます。

[アップグレード キット] ページを開くには、ztC Edge コンソールの左側のナビゲーション パネルで **[アップグレード キット]** をクリックします。

Stratus Redundant Linux ソフトウェアのアップグレードの詳細については、[「アップグレード キットを使用して Stratus Redundant Linux ソフトウェアをアップグレードする」](#)を参照してください。USB メディアの作成の詳細については、[「システム ソフトウェアの USB メディアを作成する」](#)を参照してください。

物理的なセキュリティ

悪意のあるユーザがノードにアクセスするのを未然に防ぐため、それぞれの ztC Edge システムをセキュアな場所にインストールしてください。

悪意のあるユーザを特定できるよう、該当エリアに立ち入るスタッフを識別する監査可能なシステムを導入してセキュリティを確保します。

ztC Edge ノードを含むあらゆるデバイスにとって、不正の検出やアラート機能だけでなく、物理的なセキュリティも重要な役割を果たします。

高度なセキュリティ ガイドライン

以下のセクションでは、ztC Edge システムの高度なセキュリティ ガイドラインについて説明します。

パスワードの質に関する推奨事項

パスワードを設定する際の推奨事項には次が含まれます。

- 最小のパスワード長を少なくとも 8 文字に設定し、大文字、小文字、数字、特殊文字の 4 種類のうち 3 種類の使用を義務付けます。

- パスワードを定期的のリセットするようユーザに義務付けます (30 日、60 日、または 90 日ごとなど)。パスワードの更新履歴の所定の期間内におけるパスワードの再利用を禁止することもできます。

ホスト オペレーティング システムのパスワードの質の設定を手動で更新するには



注: パスワードの質の設定はシステム内の両ノードに適用します。

1. ホスト オペレーティング システムにログオンします。手順は「[ホスト オペレーティング システムにアクセスする](#)」を参照してください。
2. テキスト エディタで `/etc/pam.d/system-auth` ファイルを開きます。
3. `pam_pwquality.so` モジュールを適切な設定に変更します。たとえば、次のような設定を使用します。

```
password requisite pam_pwquality.so try_first_pass local_
users_only retry=3 authtok_type= minlen=8 lcredit=-1
ucredit=-1 dcredit=-1 ocredit=-1 enforce_for_root
```

この例の場合、以下の値が設定されます。

`minlen=8` は、最小のパスワード長を 8 文字に設定します。

`lcredit=-1` は、パスワードに含まれる小文字の最小数を 1 に設定します。

`ucredit=-1` は、パスワードに含まれる大文字の最小数を 1 に設定します。

`dcredit=-1` は、パスワードに含まれる数字の最小数を 1 に設定します。

`dcredit=-1` は、パスワードに含まれる記号 (@、#、!、\$、% など) の最小数を 1 に設定します。

`enforce_for_root` は、`root` ユーザがパスワードを設定している場合でも、複雑度のポリシーが必ず適用されるようにします。

4. パスワード履歴を制限するには、`pam_pwhistory.so` モジュールを適切な設定で追加するか変更します。たとえば、次のような設定を使用します。

```
password requisite pam_pwhistory.so debug use_authtok
remember=10 retry=3
```

5. `/etc/pam.d/system-auth` ファイルを保存します。

ホストオペレーティングシステムでのパスワードポリシーの詳細については、次の CentOS マニュアルを参照してください。

https://wiki.centos.org/HowTos/OS_Protection#Password_Policies

同時ユーザの管理

監査ログを継続的に監視して、マシンにログオンしたユーザと、それらのユーザがまだアクティブかどうかを確認できます。

システムを現在操作しているユーザを識別し、その利用状況を正当化し監査します。

ウイルス対策

ウイルス対策やマルウェア検出のためにネットワークベースの分析を継続的に行います。

ネットワークベースの侵入検知システムは ztC Edge の機能を補うもので、セキュリティ機能の動作を検証するのに役立ちます。検知システムは、悪意のある操作を検証するために調査が必要となる、異常なネットワークトラフィックを検出しなければなりません。

SSH アクセスの制限

/etc/ssh/sshd_config のいくつかのパラメータは、SSH でシステムにアクセスできるユーザとグループを制限します。ファイルに以下のパラメータが 1 つも存在しない場合、ファイルを編集して 1 つ以上のパラメータを設定し、アクセスを制限します。

AllowUsers

AllowUsers パラメータは、特定のユーザが SSH を用いてシステムにアクセスすることを許可するオプションをシステム管理者に提供します。リストにはユーザ名をスペースで区切って指定します。このパラメータでは数字のユーザ ID が認識されません。許可されたユーザのみがホストからログインできるように指定してユーザアクセスをさらに制限する場合、エントリを user@host の形式で指定することができます。

AllowGroups

AllowGroups パラメータは、特定のユーザグループが SSH を用いてシステムにアクセスすることを許可するオプションをシステム管理者に提供します。リストにはグループ名をスペースで区切って指定します。このパラメータでは数字のグループ ID が認識されません。

DenyUsers

DenyUsers パラメータは、特定のユーザが SSH を用いてシステムにアクセスすることを拒否するオプションをシステム管理者に提供します。リストにはユーザ名をスペースで区切って指定します。このパラメータでは数字のユーザ ID が認識されません。システム管理者が特にホストからのユーザ アクセスを拒否してユーザ アクセスをさらに制限する場合、エントリを `user@host` の形式で指定することができます。

DenyGroups

DenyGroups パラメータは、特定のユーザ グループが SSH を用いてシステムにアクセスすることを拒否するオプションをシステム管理者に提供します。リストにはグループ名をスペースで区切って指定します。このパラメータでは数字のユーザ ID が認識されません。

SSH を使用してシステムにリモートでアクセスできるユーザを制限することによって、承認を受けたユーザだけがシステムにアクセスできるようにします。

MaxAuthTries

MaxAuthTries パラメータは、各接続ごとに許可される認証試行の最大回数を指定します。ログインエラーのカウントがこの半数に達すると、詳細を示すエラー メッセージが `syslog` ファイルに書き込まれます。

MaxAuthTries パラメータを小さい数に設定すると、SSH サーバに対するブルートフォース攻撃が成功する確率を最小限に抑えることができます。推奨される設定は 4 ですが、この値はサイトのポリシーに従って設定してください。例:

```
MaxAuthTries 4
```

IgnoreRhosts

IgnoreRhosts パラメータは、RhostsRSAAuthentication または HostbasedAuthentication で `.rhosts` ファイルと `.shosts` ファイルを使用しないように指定します。

このパラメータを設定すると、ユーザが SSH を使って認証する際にパスワードの入力が義務付けられます。例:

```
IgnoreRhosts yes
```

HostbasedAuthentication

HostbasedAuthentication パラメータは、認証が `.rhosts` または `/etc/hosts.equiv` で成功したパブリック キーのクライアント ホスト認証を使用して、信頼されるホストを介して許可されるかどうかを指定します。このオプションは SSH プロトコルのバージョン 2 のみに適用されます。

/etc/pam.conf でサポートが無効化されている場合、.rhosts ファイルは無効ですが、SSH で .rhosts ファイルを使用できないようにすることによって追加の保護層を提供できます。例:

```
HostbasedAuthentication no
```

sshd_config パラメータの詳細については、sshd_config(5) のマニュアル ページを参照してください。

標準化団体のベスト プラクティスと標準

このトピックに記載されている情報は、以下のベストプラクティスと標準に基づいています。

CIS Controls バージョン 7.1

CIS Controls は、現在最も一般的で危険度の高い脅威を食い止めるために作成された、優先すべきベストプラクティスと標準のセットです。これは各国のセキュリティ専門家によって編み出されたもので、その後も毎年改良と検証が続けられています。さらに詳しい情報は CIS のサイト <https://www.cisecurity.org> に記載されています。

CIS Controls は以下のとおりです。

Basic (基本)

1. ハードウェア資産のインベントリとコントロール
2. ソフトウェア資産のインベントリとコントロール
3. 継続的な脆弱性管理
4. 管理権限のコントロールされた使用
5. モバイル デバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアとソフトウェアのセキュアな構成
6. 監査ログの保守、監視および分析

Foundational (基盤)

7. 電子メールと Web ブラウザの保護
8. マルウェア対策
9. ネットワーク ポート、プロトコル、およびサービスの制限とコントロール
10. データ復旧能力
11. ファイアウォール、ルータ、スイッチなどのネットワーク デバイスのセキュアな構成

12. 境界防御
13. データ保護
14. Need-to-Know に基づいたアクセス コントロール
15. ワイヤレス アクセス コントロール
16. アカウントの監視とコントロール

Organizational (組織)

17. セキュリティ意識向上トレーニング プログラムの実施
18. アプリケーション ソフトウェア セキュリティ
19. インシデントの対応と管理
20. ペネトレーション テストおよびレッドチームの訓練

ISA/IEC 62443-4-2

ISA/IEC 62443-4-2 には、制御システム能力のセキュリティ レベルを満たすための 7 つの基本要件 (FR) に関連する技術的なコンポーネント要件 (CR) の詳細が記載されています。さらに詳しい情報は IEC のサイト <https://www.iec.ch/> に記載されています。

基本要件は以下のとおりです。

1. 識別と認証制御 (IAC)
2. 利用制御 (UC)
3. システム完全性 (SI)
4. データ機密性 (DC)
5. 制限されたデータ フロー (RDF)
6. イベントへのタイムリーな対応 (TRE)
7. リソース可用性 (RA)

1. 識別と認証制御 (IAC)

ユーザの識別と認証機構を組み合わせて使用し、コンポーネントのアクセス制御を実施します。アクセスを要求するユーザの身元確認は、不正なユーザによるコンポーネントへのアクセス取得を未然に防ぐために必要です。認証は、ログインを行いパスワードを使って ztC Edge システムに入る個々のユーザに対して、アクセス制御リストから行われます。

2. 利用制御 (UC)

ユーザの識別と認証が済んだ後、コンポーネントは、許可されるアクションをそのコンポーネントの承認される利用だけに制限する必要があります。ztC Edge システムには最小権限の概念を実施するロールが定義されています。さまざまなレベルのアクセス制御をもつ複数のユーザを作成することで、コンポーネントの承認される利用を定義することもできます。

3. システム完全性 (SI)

稼働時および非稼働時のソフトウェアと物理コンポーネントの両方において、デバイスの完全性が損なわれてはなりません。ztC Edge システムでは、ユニットが信頼される状態からブートまたは起動されることを確認するセキュア ブートを実装しているほか、アップグレードの前にはソフトウェア コンポーネントのデジタル署名が検証されます。データの不正な操作や変更を未然に防ぐには、システム完全性を確保することが重要です。

4. データ機密性 (DC)

通信チャネル上の情報やレポジトリに保管されているデータの機密性を確保し、不正な開示から保護することが目的です。ztC Edge システムは Web 通信用に TLS v1.2 を含む HTTPS に加え、暗号化付きの SSH と SMTP も提供しており、悪意のある人物から情報を確実に保護します。

5. 制限されたデータ フロー (RDF)

制限されたデータ フローによって、ゾーンや導管を介して制御システムをセグメント化し、不要なデータ フローを制限します。ztC Edge ネットワーク アーキテクチャでは、ネットワーキングの構成によって指定されるルーティングやスイッチングがサポートされます。これにより、担当のシステム エンジニアによる定義に基づいて情報フローの管理を行います。ztC Edge システムのネットワーキング能力を活用することで、ネットワーク セグメンテーションによるデータ フローの制限が可能になります。

6. イベントへのタイムリーな対応 (TRE)

システムがセキュアな状態から動作を開始した場合でも、脆弱性やセキュリティ イベントが発生する可能性はあります。ztC Edge システムではセキュリティ インシデントに対応して問題を迅速に解決し、調査結果を報告するため、製品セキュリティ インシデント対応 (PSIR) チームを用意しています。ztC Edge システムの提供するアラート ログを使用すると、適切なチャネルに通知して、セキュリティ インシデントを示す可能性のある構成変更を伝えることができます。ログには調査に十分な情報が含まれており、e アラート通知は電子メールで送信されます。

7. リソース可用性 (RA)

この制御は、コンポーネントがさまざまなサービスの拒否イベントから確実に回復できるようにすることが目的です。ztC Edge システムの高可用性は「always on」状態を提供するための基盤です。産業制御システムでは、ときに生命の安全に関わることもあるため、高可用性を維持することが不可欠となり

ます。組み込みの仮想化および可用性層、自動化されたデータ保護、アプリケーションの復旧といった機能を備えた Stratus Redundant Linux は、最新の仮想化されたコンピューティングにおける IT への依存度を大幅に削減します。自己保護および自己監視の機能を通じて計画外のダウンタイムを減らし、ビジネスクリティカルな産業アプリケーションに継続的な可用性を確実に提供します。

12

第 12 章: SNMP

簡易ネットワーク管理プロトコル (SNMP) は、アラームの受信、トラップの送信、およびシステムステータスのモニタリングに使用される標準プロトコルです。SNMP は、階層型に構成された管理情報ベース (MIB) に格納されているシステム定義情報を使用します。

ztC Edge システムが SNMP を使用するように構成するには、「[SNMP 設定を構成する](#)」を参照してください。

`snmptable` コマンドを実行して、システムに関するアラート、監査ログ、ノード、VM、ボリュームなどの情報を取得できます。「[snmptable でシステム情報を取得する](#)」を参照してください。

MIB ファイルのコピーは、[\[Downloads \(ダウンロード\)\]](#) ページ (<https://www.stratus.com/services-support/downloads/?tab=ztcedge>) の [\[Drivers and Tools \(ドライバとツール\)\]](#) セクションからダウンロードできます。

snmptable でシステム情報を取得する

`snmptable` コマンドを実行して、システムに関するアラート、監査ログ、ノード、VM、ボリュームなどの情報を取得できます。










アラート情報を表示するには

アラートに関する情報を表示するには、次のコマンドを実行します。

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c public  
localhost ztCEdgeAlertTable
```

コマンドの出力には以下が表示されます。

フィールド	説明												
ztCEdgeAlertIndex	アラート番号。												
ztCEdgeAlertSeverity	<p>アラートの重大度 (数値については ztCEdgeAlertSeverityNum を参照してください)。次の値があります。</p> <table><tr><td>クリア</td><td></td></tr><tr><td>情報目的</td><td></td></tr><tr><td>軽度</td><td></td></tr><tr><td>重度</td><td></td></tr><tr><td>深刻</td><td></td></tr><tr><td>重大</td><td></td></tr></table>	クリア		情報目的		軽度		重度		深刻		重大	
クリア													
情報目的													
軽度													
重度													
深刻													
重大													
ztCEdgeAlertType	<p>アラートのタイプ。例:</p> <ul style="list-style-type: none">• node_singleSystemDisk• ノード メンテナンス• ユニット が適切に負荷分散されていません												
ztCEdgeAlertSource	<p>アラートのソース。例:</p> <ul style="list-style-type: none">• node0 または node1• ztC Edge システム ネットワークの名前• ネットワーク ホストの名前												
ztCEdgeAlertDateTime	アラートの日時。yyyy-mm-dd hh:mm:ss 形式で yyyy が年、mm が月、dd が日付、hh が時、mm が分、ss が秒を表します (例: 2017-11-03 23:49:45)。												
ztCEdgeAlertCallHomeSent	true の場合は call-home が送信されました。false の場合は送信されていません。												

フィールド	説明																		
ztCEdgeAlertEAlertSent	true の場合は e アラートが送信されました。false の場合は送信されていません。																		
ztCEdgeAlertSNMPTrapSent	true の場合は SNMP トラップが送信されました。 false の場合は送信されていません。																		
ztCEdgeAlertInformation	アラートに関する情報。例： <ul style="list-style-type: none">• ノード node1 はメンテナンス中です• node0 は単一のシステム ディスクをもち、ポリシーはこのディスクの冗長性を仮定しています。そうでない場合は別の内蔵ディスクを追加してください• ビジネス ネットワーク net_728 がリンクの劣化を報告しています• ユニットが適切に負荷分散されていません																		
ztCEdgeAlertSNMPTrapOID	SNMP トラップ オブジェクト ID (OID) (例: COMPANY-MIB::nodeSingleSystemDisk)																		
ztCEdgeAlertSeverityNum	ztCEdgeAlertSeverity の数値。次の値があります。 <table><tr><td>0</td><td>クリア</td><td></td></tr><tr><td>1</td><td>情報目的</td><td></td></tr><tr><td>2</td><td>軽度</td><td></td></tr><tr><td>3</td><td>重度</td><td></td></tr><tr><td>4</td><td>深刻</td><td></td></tr><tr><td>5</td><td>重大</td><td></td></tr></table>	0	クリア		1	情報目的		2	軽度		3	重度		4	深刻		5	重大	
0	クリア																		
1	情報目的																		
2	軽度																		
3	重度																		
4	深刻																		
5	重大																		

監査ログ情報を表示するには

監査ログに関する情報を表示するには、次のコマンドを実行します。

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c public  
localhost ztCEdgeAuditTable
```

コマンドの出力には以下が表示されます。

フィールド	説明
ztCEdgeAuditIndex	番号 (1、2 など)。情報を表示している監査ログを示します。
ztCEdgeAuditDateTime	監査の生成日時。yyyy-mm-dd hh:mm:ss 形式で yyyy が年、mm が月、dd が日付、hh が時、mm が分、ss が秒を表します (例: 2017-11-03 23:49:45)。
ztCEdgeAuditUsername	監査を生成したユーザの名前 (例: audit や admin)。
ztCEdgeAuditOriginatingHost	監査を実行したホストの IP アドレス。
ztCEdgeAuditAction	監査対象となるアクションの説明。例: <ul style="list-style-type: none">"Login user \"audit\"""Start virtual machine \"manager1\"""Remove all cleared alert"

ノード情報を表示するには

ノード情報を表示するには、次のコマンドを実行します。

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c public  
localhost ztCEdgeNodeTable
```

コマンドの出力には以下が表示されます。

フィールド	説明
ztCEdgeNodeIndex	番号 (具体的には 1 または 2)。情報を表示しているノードを示します。
ztCEdgeNodeId	ノードのホスト ID (例: host:o34)。
ztCEdgeNodeDisplayName	ノード名。node0 または node1。
ztCEdgeNodeIsPrimary	true の場合、ノードはプライマリです。false の場合、ノードはセカンダリです。
ztCEdgeNodeStateNum	ノードの状態: 0 正常 (✓) 1 警告 (⚠) 2 ビジー (🔄) 3 破損 (✖) 4 メンテナンス (🛠)
ztCEdgeNodeActivityNum	ノードのアクティビティ: 0 イメージング 1 ブート中 2 実行中 3 停止中 4 リブート中 5 電源オフ 6 失敗 7 ファームウェア更新中 8 損失 9 除外済み 10 アクセス不可 11 プロト (初期化中)

フィールド	説明
	12 退去中

VM 情報を表示するには

VM 情報を表示するには、次のコマンドを実行します。

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c public  
localhost ztCEdgeVMTable
```

コマンドの出力には以下が表示されます。

フィールド	説明
ztCEdgeVMIndex	番号 (1、2 など)。情報を表示している VM を示します。
ztCEdgeVMId	VM の ID (例: vm:o1467)。
ztCEdgeVMDisplayName	VM 名 (例: MyVM)。
ztCEdgeVMRunningNode	VM を実行しているノード。node0 または node1。
ztCEdgeVMAvailability	VM の可用性。HA (高可用性) または FT (フォールトトレラント)。
ztCEdgeVMStateNum	VM の状態: 0 正常 (✓) 1 警告 (⚠) 2 ビジーまたは同期中 (🔄) 3 破損またはブラックリスト (✗)
ztCEdgeVMActivityNum	VM アクティビティ: 0 インストール中 1 ブート中 2 実行中

フィールド	説明
	3 移動中
	4 停止中
	5 停止
	6 エクスポート中
	8 一時停止
	9 読み込み中
	10 クラッシュ処理中
	11 クラッシュ
	12 ダンプ処理中
	13 待機中

ボリューム情報を表示するには

ボリューム情報を表示するには、次のコマンドを実行します。

```
snmptable -v2c -m+/usr/smd/STRATUS-ZTC-EDGE-MIB.txt -c public
localhost ztCEdgeVolumeTable
```

コマンドの出力には以下が表示されます。

フィールド	説明
ztCEdgeVolumeIndex	番号 (1、2 など)。情報を表示しているボリュームを示します。
ztCEdgeVolumeId	ボリュームの ID (例: volume:o588)。
ztCEdgeVolumeDisplayName	ボリューム名 (例: root)。
ztCEdgeVolumeSyncPercentage	同期されるボリュームのパーセント率。
ztCEdgeVolumeUsedBy	ボリュームを使用している VM またはホストの名前 (例: MyVM)。none はボリュームが使用されていないことを示します。

フィールド	説明
ztCEdgeVolumeStateNum	ボリュームの状態: 0 正常 (✓) 1 警告 (⚠) 2 ビジーまたは同期中 (🔄) 3 破損 (✖)