CompTIA Cloud+
認定資格試験出題範囲

試験番号：**CV0-003**

CompTIA

試験について

CompTIA Cloud+認定資格試験は、以下の必要な知識とスキルを持っていることを証明します：

- クラウドのアーキテクチャと設計を理解している
- クラウドサービスとソリューションをデプロイすることができる
- クラウド環境の保守、セキュリティ維持、および最適化を行える
- クラウド管理に関係する一般的な問題のトラブルシューティングを行える

CompTIACloud+は、システム管理者としての2～3年の実務経験で得られる知識とスキルを目安に設計されています。

出題範囲に掲載された項目は、認定資格試験の目的を明確にするためのものであり、試験の出題内容を完全に網羅したものではありません。

試験開発

CompTIAの認定資格試験は、ITプロフェッショナルに必要とされるスキルと知識に関して検討する、専門分野のエキスパートによるワークショップ、および業界全体へのアンケートの調査結果に基づいて策定されています。

CompTIA認定教材の使用に関するポリシー

CompTIA Certifications, LLCは、無許可の第三者トレーニングサイト（通称「ブレインダンプ」）とは提携関係がなく、これらが提供するいかなるコンテンツも公認・推薦・容認しません。CompTIAの認定資格試験の受験準備にこのような教材を使用した個人は、CompTIA受験者同意書の規定に基づいて資格認定を取り消され、その後の受験資格を停止されます。CompTIAでは、無許可教材の使用に関する試験実施ポリシーをよりよく理解していただくための取り組みを進めています。認定資格試験を受験される方は、CompTIA認定資格試験実施ポリシーをご一読ください。CompTIAの認定資格試験を受験するための学習を始める前には、必ずCompTIAが定めるすべてのポリシーをご確認ください。受験者には、CompTIA受験者同意書の規定を遵守することが求められています。個々の教材が無許可扱いになるかどうかを確認するには、CompTIA **(examsecurity@comptia.org)** までメールにてご確認ください。

注意事項

箇条書きで挙げられた項目は、すべての試験内容を網羅するものではありません。この出題範囲に掲載がない場合でも、各分野に関連する技術、プロセス、あるいはタスクを含む問題が出題される可能性があります。CompTIAでは、提供している認定資格試験の内容に現在必要とされているスキルを反映するため、また試験問題の信頼性維持のため、継続的な試験内容の検討と問題の改訂を行っています。必要に応じて、現在の出題範囲を基に試験を改訂する場合があります。この場合、現在の試験に関連する資料・教材等は、継続的にご利用いただくことが可能です。

試験情報

試験番号	CV0-003
質問数	最大90問
出題形式	単一/複数選択、パフォーマンスベーステスト
試験時間	90分
推奨経験	• ITシステム管理またはITネットワーキングにおける最低2～3年間の業務経験 • CompTIA Network+およびServer+、またはそれに相当する知識 • サーバーの仮想化に関する主要なハイパーバイザーテクノロジーに精通している • クラウドサービスモデルに関する知識 • ITサービス管理に関する知識 • パブリックまたはプライベートのIaaSでの業務経験
合格スコア	750（100～900のスコア形式）

試験の出題範囲（試験分野）

下表は、この試験における試験分野（ドメイン）と出題比率の一覧です：

試験分野	出題比率
1.0 クラウドのアーキテクチャと設計	13%
2.0 セキュリティ	20%
3.0 デプロイ	23%
4.0 運用とサポート	22%
5.0 トラブルシューティング	22%
計	**100%**

1.0 クラウドのアーキテクチャと設計

1.1 様々な種類のクラウドモデルを比較検討することができる。

- 導入モデル
  - パブリック
  - プライベート
  - ハイブリッド
  - コミュニティ
  - Cloud within a cloud
  - マルチクラウド
  - マルチテナント
- サービスモデル
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- 高度なクラウドサービス
  - Internet of Things
    （IoT/モノのインターネット）
  - サーバーレス
  - 機械学習/人工知能 (AI)
- 責任共有モデル

1.2 キャパシティプランニングに関連する要因を説明することができる。

- 要件
  - ハードウェア
  - ソフトウェア
  - 予算
  - ビジネスニーズ分析
- 標準テンプレート
- ライセンス
  - ユーザーごと
  - ソケットベース
  - ボリュームベース
  - コアベース
  - サブスクリプション
- ユーザー密度
- システム負荷
- トレンド分析
  - ベースライン
  - パターン
  - アノマリ
- パフォーマンスキャパシティプランニング

1.3 クラウド環境における高可用性とスケーリングの重要性を説明することができる。

- ハイパーバイザー
  - アフィニティ
  - アンチアフィニティ
- オーバーサブスクリプション
  - コンピュート
  - ネットワーク
  - ストレージ
- リージョンとゾーン
- アプリケーション
- コンテナー
- クラスター
- ネットワーク機能の高可用性
  - スイッチ
  - ルーター
  - ロードバランサー
  - ファイアウォール
- 単一障害点の回避
- 拡張性
  - オートスケーリング
  - 水平スケーリング
  - 垂直スケーリング
  - クラウドバースティング

1.4 与えられたシナリオに基づいて、ソリューション設計を分析し、事業要件をサポートすることができる。

- 要件分析
  - ソフトウェア
  - ハードウェア
  - インテグレーション
  - 予算
  - コンプライアンス
  - サービスレベルアグリーメント (SLA)
  - ユーザーニーズとビジネスニーズ
  - セキュリティ
  - ネットワーク要件
    - サイジング
    - サブネッティング
    - ルーティング
- 環境
  - 開発
  - 品質保証 (QA)
  - ステージング
  - ブルー/グリーン
  - 本番環境
  - 災害復旧 (DR)
- テスト技術
  - 脆弱性テスト
  - ペネトレーションテスト
  - パフォーマンステスト
  - 回帰テスト
  - 機能テスト
  - ユーザビリティテスト

2.0 セキュリティ

2.1 与えられたシナリオに基づいて、認証管理とアクセス管理を構成することができる。

- 認証と承認
  - 特権アクセス管理
  - 論理アクセス管理
  - アカウントライフサイクル管理
    - アカウントのプロビジョニングとデプロビジョニング
  - アクセス制御
    - ロールベース
    - 任意アクセス制御
    - 非任意アクセス制御
    - 強制アクセス制御
- ディレクトリサービス
  - Lightweight Directory Access Protocol (LDAP)
- フェデレーション
- 証明書マネジメント
- 多要素認証 **(MFA)**
- シングルサインオン **(SSO)**
  - Security Assertion Markup Language (SAML)
- 公開鍵インフラストラクチャ **(PKI)**
- 秘密管理
- 鍵管理

2.2 与えられたシナリオに基づいて、クラウド環境内のネットワークを保護することができる。

- ネットワークのセグメンテーション
  - Virtual LAN (VLAN)/Virtual extensible LAN (VXLAN)/Generic network virtualization encapsulation (GENEVE)
  - マイクロセグメンテーション
  - 階層化
- プロトコル
  - ドメイン名サービス (DNS)
    - DNS over HTTPS (DoH)/DNS over TLS (DoT)
    - DNS Security (DNSSEC)
  - Network Time Protocol (NTP)
    - Network Time Security (NTS)
  - 暗号化
    - IPSec
    - Transport Layer Security (TLS)
    - Hypertext Transfer Protocol Secure (HTTPS)
  - トンネリング
    - Secure Shell (SSH)
    - Layer 2 Tunneling Protocol (L2TP)/Point-to-Point Tunneling Protocol (PPTP)
    - Generic Routing Encapsulation (GRE)
- ネットワークサービス
  - ファイアウォール
    - ステートフル
    - ステートレス
  - Webアプリケーションファイアウォール (WAF)
  - アプリケーションデリバリーコントローラー (ADC)
  - 侵入保護システム (IPS)/侵入検出システム (IDS)
  - データ損失防止 (DLP)
  - ネットワークアクセスコントロール (NAC)
  - パケットブローカー
- ログとイベントのモニタリング
- ネットワークフロー
- ハードニングと設定変更
  - 不要なポートとサービスの無効化
  - 脆弱なプロトコルと暗号化の無効化
  - ファームウェアのアップグレード
  - イングレストラフィックとエグレストラフィックの制御
    - 許可リスト（旧名ホワイトリスト）とブロックリスト（旧名ブラックリスト）
    - プロキシサーバー
  - 分散型サービス拒否 (DDoS) 保護

2.3 与えられたシナリオに基づいて、OSとアプリケーションの適切なセキュリティ制御を適用することができる。

- ポリシー
  - パスワードの複雑さ
  - アカウントのロックアウト
  - アプリケーション承認リスト（旧名ホワイトリスト）
  - ソフトウェアの機能
  - ユーザー/グループ
- ユーザーパーミッション
- アンチウイルス/アンチマルウェア/エンドポイントでの検出と対応 **(EDR)**
- ホスト型**IDS (HIDS)**/ホスト型IPS **(HIPS)**
- ベースラインのハードニング
  - 単一の機能
- ファイルの完全性
- ログとイベントのモニタリング
- 構成管理
- ビルド
  - ステーブル
  - 長期サポート (LTS)
  - ベータ
  - カナリア
- オペレーティングシステム **(OS)** のアップグレード
- 暗号化
  - Application Programming Interface (API) エンドポイント
  - アプリケーション
  - OS
  - ストレージ
  - ファイルシステム
- 強制アクセス制御
- ソフトウェアファイアウォール

2.4 与えられたシナリオに基づいて、クラウド環境内でデータセキュリティ制御とコンプライアンス制御を適用することができる。

- 暗号化
- 整合性
  - ハッシュ化アルゴリズム
  - デジタル署名
  - ファイル完全性モニタリング (FIM)
- クラシフィケーション
- セグメンテーション
- アクセスコントロール
- 法律と規制の影響
  - 訴訟ホールド
- レコードマネジメント
  - バージョン管理
  - 保持
  - 破壊
  - WORM (Write Once Read Many)
- データ損失防止 **(DLP)**
- クラウドアクセスセキュリティブローカー **(CASB)**

2.5 与えられたシナリオに基づいて、セキュリティ要件を満たすための対策を実施することができる。

- ツール
  - 脆弱性検査ツール
  - ポートスキャナ
- 脆弱性アセスメント
  - 初期値および一般的なクレデンシャルスキャン
  - クレデンシャルスキャン
  - ネットワークベーススキャン
  - エージェントベーススキャン
  - サービスの可用性
- セキュリティパッチ
  - ホットフィックス
  - スケジュールされたアップデート
  - 仮想パッチ
  - 署名のアップデート
  - ロールアップ
- リスク登録簿
- パッチアプリケーションの優先順位決定
- 初期設定されているアカウントの無効化
- セキュリティツールがシステムおよびサービスに及ぼす影響
- クラウドサービスモデルがセキュリティ実装に及ぼす影響

2.6 インシデントレスポンス手順の重要性を説明することができる。

- 準備
  - ドキュメンテーション
  - 連絡網
  - トレーニング
  - 机上演習
  - 文書化されたインシデントの種類/カテゴリー
  - 役割と責任
- インシデントレスポンス手順
  - 識別
    - 範囲
  - 調査
  - 封じ込め、根絶、および復旧
    - 分離
    - 証拠の取得
    - 証拠の連鎖
  - インシデント後の教訓の管理
    - 根本原因分析 (RCA: Root cause analysis)

3.0 デプロイ

3.1 与えられたシナリオに基づいて、クラウドソリューションの構成要素を統合することができる。

- サブスクリプションサービス
  - ファイルサブスクリプション
  - コミュニケーション
    - Eメール
    - Voice over IP (VoIP)
    - メッセージング
  - コラボレーション
  - 仮想デスクトップインフラストラクチャ (VDI)
  - ディレクトリと認証サービス
  - クラウドリソース
    - IaaS
    - PaaS
    - SaaS
- リソースのプロビジョニング
  - コンピュート
  - ストレージ
  - ネットワーク
- アプリケーション
  - サーバーレス
- 仮想マシン **(VM)** とカスタムイメージのデプロイ
- テンプレート
  - OSテンプレート
  - ソリューションテンプレート
- 認証管理
- コンテナー
  - 変数の設定
  - シークレットの設定
  - 永続ストレージ
- オートスケーリング
- デプロイ後の検証

3.2 与えられたシナリオに基づいて、クラウド環境内でストレージをプロビジョニングすることができる。

- 種類
  - ブロック
    - Storage Area Network (SAN)
      - ゾーニング
  - ファイル
    - Network Attached Storage (NAS)
  - オブジェクト
    - テナント
    - バケット
- 階層
  - フラッシュ
  - ハイブリッド
  - スピニングディスク
  - 長期
- **Input/output Operations Per Second (IOPS)** とリード/ライト
- プロトコル
  - Network File System (NFS)
  - Common Internet File System (CIFS)
  - Internet Small Computer System Interface (iSCSI)
  - ファイバーチャネル (FC)
  - Non-volatile Memory express over Fabrics (NVMe-oF)
- **Redundant Array of Inexpensive Disks (RAID)**
  - 0
  - 1
  - 5
  - 6
  - 10
- ストレージシステムの機能
  - 圧縮
  - 重複排除
  - シンプロビジョニング
  - シックプロビジョニング
  - レプリケーション
- ユーザークォータ
- ハイパーコンバージド
- ソフトウェア定義ストレージ **(SDN)**

3.3 与えられたシナリオに基づいて、クラウドネットワーキングソリューションをデプロイすることができる。

- サービス
  - Dynamic Host Configuration Protocol (DHCP)
  - NTP
  - DNS
  - Content Delivery Network (CDN)
  - IPアドレス管理 (IPAM：IP address management)
- 仮想プライベートネットワーク**(VPN)**
  - site-to-site
  - point-to-point
  - point-to-site
  - IPSec
  - Multiprotocol Label Switching (MPLS)
- 仮想ルーティング
  - 動的および静的ルーティング
  - 仮想ネットワークインターフェイスコントローラー (vNIC)
  - サブネッティング
- ネットワークアプライアンス
  - ロードバランサー
  - ファイアウォール
- 仮想プライベートクラウド **(VPC)**
  - ハブアンドスポーク
  - ピアリング
- **VLAN/VXLAN/GENEVE**
- **Single Root Input/Output Virtualization (SR-IOV)**
- ソフトウェア定義ネットワーク **(SDN)**

3.4 与えられたシナリオに基づいて、デプロイに向けた適切なコンピューティングサイジングを構成することができる。

- 仮想化
  - ハイパーバイザー
    - Type 1
    - Type 2
  - 同時マルチスレッディング (SMT)
  - 動的割り当て
  - オーバーサブスクリプション
- **Central Processing Unit (CPU)**/仮想**CPU (vCPU)**
- **Graphics Processing Unit (GPU)**
  - 仮想
    - 共有
  - パススルー
- クロック速度/サイクルあたりの命令実行数 **(IPC)**
- ハイパーコンバージド
- メモリ
  - 動的割り当て
  - バルーニング

3.5 与えられたシナリオに基づいて、クラウドの移行を実施することができる。

- **Physical to Virtual (P2V)**
- **Virtual to Virtual (V2V)**
- クラウド間の移行
  - ベンダーロックイン
  - PaaSまたはSaaS移行
    - アクセス制御リスト (ACL)
    - ファイアウォール
- ストレージ移行
  - ブロック
  - ファイル
  - オブジェクト
- データベース移行
  - サービス間移行
  - 相関的
  - 非相関的

4.0 運用とサポート

4.1 与えられたシナリオに基づいて、ロギング、モニタリング、およびアラートを構成し、稼働状態を維持することができる。

- ロギング
  - コレクター
    - Simple Network Management Protocol (SNMP)
    - Syslog
  - 分析
  - 深刻度の分類
  - 監査
  - タイプ
    - アクセス/認証
    - システム
    - アプリケーション
  - 自動化
  - トレンド化
- モニタリング
  - ベースライン
  - しきい値
  - タグ付け
  - ログスクラブ
  - パフォーマンスのモニタリング
    - アプリケーション
    - インフラストラクチャの構成要素
  - リソースの活用
  - 可用性
    - SLAが定義する稼働時間要件
  - 継続的モニタリング活動の検証
  - サービス管理ツールの統合
- 警告
  - 一般的なメッセージング手法
  - アラートの有効化/無効化
    - メンテナンスモード
  - 適切な対応
  - 警告の分類と伝達に関するポリシー

4.2 与えられたシナリオに基づいて、クラウド環境の効率的な運用を維持することができる。

- バックアップの完了を確認する
- ライフサイクル管理
  - ロードマップ
  - 旧/現行/新バージョン
  - システムのアップグレードと移行
  - 廃止予定または寿命
- 変更管理
- 資産マネジメント
  - Configuration Management Database (CMDB)
- パッチの適用
  - 機能と拡張
  - 稼働しない重要なインフラストラクチャ、アプリケーションの修復
  - パッチが適用されるべきクラウド要素の範囲
    - ハイパーバイザー
    - VMs
    - 仮想アプライアンス
    - ネットワーキングコンポーネント
    - アプリケーション
    - ストレージコンポーネント
    - ファームウェア
    - ソフトウェア
    - OS
  - ポリシー
    - n-1
  - ロールバック
- システムのプロセス改善による影響
- アップグレードの手法
  - ローリングアップグレード
  - ブルー/グリーン
  - カナリア
  - アクティブ・パッシブ
  - 開発/QA/本番環境/DR
- ダッシュボードとレポート
  - タグ付け
  - 費用
    - チャージバック
    - ショーバック
  - 使用量
  - 接続性
  - レイテンシー
  - キャパシティ
  - インシデント
  - 健全性
  - 全体の使用状況
  - 可用性

4.3 与えられたシナリオに基づいて、クラウド環境を最適化することができる。

- ライトサイジング
  - オートスケーリング
  - 水平スケーリング
  - 垂直スケーリング
  - クラウドバースティング
- コンピュート
  - CPU
  - GPU
  - メモリ
  - コンテナー
- ストレージ
  - 階層
    - 適応最適化
  - IOPS
  - キャパシティ
  - 重複排除
  - 圧縮
- ネットワーク
  - 帯域幅
  - Network Interface Controller (NIC)
  - レイテンシー
  - SDN
  - エッジコンピューティング
    - CDN
- 配置
  - 地理
  - クラスター型配置
  - 冗長性
  - コロケーション
- デバイスのドライバとファームウェア
  - 市販
  - ベンダー
  - オープンソース

4.4 与えられたシナリオに基づいて、適切な自動化技術とオーケストレーション技術を適用することができる。

- **Infrastructure as Code**
  - インフラストラクチャの構成要素とその統合
- **Continuous Integration/ Continuous Deployment (CI/CD)**
- バージョンコントロール
- 構成管理
  - プレイブック
- コンテナー
- 自動化アクティビティ
  - ルーチンオペレーション
  - 更新
  - スケーリング
  - シャットダウン
  - 再起動
  - 内部APIの作成
- セキュアなスクリプティング
  - ハードコードされたパスワードが存在しない
  - 個別サービスアカウントの使用
  - パスワードボールト
  - 鍵ベースの認証
- オーケストレーションのシーケンシング

4.5 与えられたシナリオに基づいて、適切なバックアップ作業と復旧作業を実施することができる。

- バックアップの種類
  - インクリメンタル
  - 差分
  - フル
  - 合成フル
  - スナップショット
- オブジェクトのバックアップ
  - アプリケーションレベルのバックアップ
  - ファイルシステムのバックアップ
  - データベースダンプ
  - 設定ファイル
- バックアップターゲット
  - テープ
  - ディスク
  - オブジェクト
- バックアップと復旧のポリシー
  - 保持
  - スケジュール
  - ロケーション
  - SLA
  - 目標復旧時間 (RTO)
  - 目標復旧時点 (RPO)
  - 平均復旧時間 (MTTR)
  - 3-2-1ルール
    - データの3つのコピー
    - 2つの異なるメディア
    - オフサイトの1つのコピー
- 復旧の手法
  - インプレイス
  - 代替ロケーション
  - ファイルの復元
  - スナップショット

4.6 与えられたシナリオに基づいて、災害復旧タスクを実施することができる。

- フェールオーバー
- フェールバック
- バックアップの復元
- レプリケーション
- ネットワーク設定
- オンプレミスとクラウドサイト
  - ホット
  - ウォーム
  - コールド
- 要件
  - RPO
  - RTO
  - SLA
  - 企業ガイドライン
- 文書化
  - DRキット
  - プレイブック
  - ネットワークダイアグラム
- 地理的データセンターの要件

5.0 トラブルシューティング

5.1 与えられたシナリオに基づいて、トラブルシューティングの方法論を活用し、クラウド関連の問題を解決することができる。

- 変更を実施する際は、必ず前もって会社のポリシー、手順、および影響を検討する。

1. 問題を特定する
   - ユーザーに質問し、ユーザーによるコンピューターへの変更を明確にして、バックアップを実施してから変更を行う
   - 環境またはインフラストラクチャの変更に関する問い合わせ
2. 推定される原因の仮説を立てる（明白と思われる点も確認する）
   - 必要な場合は、症状に応じた外部または内部調査を実施する
3. 仮説を検証して原因を特定する
   - 仮説が証明された場合、問題解決に向けた今後の対応を決定する
   - 仮説が証明されなかった場合、仮説を立て直すか、エスカレーションする
4. 問題解決のための対応計画を策定し、実行に移す
5. システム全体の機能を検証し、該当する場合は予防対策を実施する
6. プロセス全体を通じた発見内容、対応、および結果を文書化する。

5.2 与えられたシナリオに基づいて、セキュリティの問題をトラブルシューティングすることができる。

- 特権
  - 喪失
  - 不完全
  - エスカレーション
  - 鍵
- 認証
- 承認
- セキュリティグループ
  - ネットワークセキュリティグループ
  - ディレクトリセキュリティグループ
- 鍵と証明書
  - 期限切れ
  - 取り消し
  - 信頼性
  - 不正アクセス
  - 設定ミス
- ポリシーの設定ミスまたは適用ミス
- データセキュリティの問題
  - 暗号化されていないデータ
  - 情報侵害
  - 分類ミス
  - プロトコルの暗号化不足
  - セキュアでない暗号
- 暴露されたエンドポイント
- セキュリティアプライアンスの設定ミスまたは障害
  - IPS
  - IDS
  - NAC
  - WAF
- サポートされていないプロトコル
- 外部/内部攻撃

5.3 与えられたシナリオに基づいて、デプロイの問題をトラブルシューティングすることができる。

- 接続性の問題
  - クラウドサービスプロバイダ (CSP) またはインターネットサービスプロバイダ (ISP) の機能停止
- パフォーマンスの低下
  - レイテンシー
- 構成
  - スクリプト
- コンテナー内のアプリケーション
- テンプレートの構成ミス
- 欠けている、または正しくないタグ
- 不十分なキャパシティ
  - スケーリング構成
  - コンピュート
  - ストレージ
  - 帯域幅の問題
  - オーバーサブスクリプション
- ライセンスの問題
- ベンダー関連の問題
  - ベンダーまたはプラットフォームの移行
  - ベンダーまたはプラットフォームの統合
  - APIリクエストの制限
  - 費用または請求に関する問題

5.4 与えられたシナリオに基づいて、接続性の問題をトラブルシューティングすることができる。

- ネットワークセキュリティグループの構成ミス
  - ACL
  - 継承
- ネットワーク構成の一般的な問題
  - ピアリング
  - 不正確なサブネット
  - 不正確なIPアドレス
  - 不正確なIP空間
  - ルーティング
    - デフォルト
    - 静的
    - ダイナミック
  - ファイアウォール
    - 管理が不適切なマイクロセグメンテーション
  - ネットワークアドレス変換 (NAT)
    - VPN
    - ソース
    - 宛先
  - ロードバランサー
    - 方式
    - ヘッダー
    - プロトコル
    - 暗号化
    - バックエンド
    - フロントエンド
  - DNSの記録
  - VLAN/VXLAN/GENEVE
  - プロキシ
  - Maximum Transmission Unit (MTU)
  - Quality of Service (QoS)
  - 時刻同期の問題
- ネットワークトラブルシューティングツール
  - ping
  - tracert/traceroute
  - flushdns
  - ipconfig/ifconfig/ip
  - nslookup/dig
  - netstat/ss
  - route
  - arp
  - curl
  - パケットキャプチャ
  - パケットアナライザー
  - OpenSSLクライアント

5.5 与えられたシナリオに基づいて、一般的なパフォーマンスの問題をトラブルシューティングすることができる。

- リソースの活用
  - CPU
  - GPU
  - メモリ
  - ストレージ
    - I/O
    - キャパシティ
  - ネットワーク帯域幅
  - ネットワーク遅延
  - レプリケーション
  - スケーリング
- アプリケーション
  - メモリ管理
  - サービスの過負荷
- ロードバランシングの不正確な構成または障害

5.6 与えられたシナリオに基づいて、自動化もしくはオーケストレーションの問題をトラブルシューティングすることができる。

- アカウントのミスマッチ
- 変更管理の不履行
- サーバー名の変更
- IPアドレスの変更
- ロケーションの変更
- バージョン/機能のミスマッチ
- 自動化ツールの非互換性
  - 非推奨の機能
  - 互換性のないAPIバージョン
- ジョブ検証の問題
- パッチの失敗

CompTIA Cloud+(CV0-003) 略語リスト

下記はCompTIA Cloud+認定資格試験で使用される略語の一覧です。
包括的な試験準備の一環として、リストを復習し、知識の習得に努めてください。

略語	定義
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ADC	Application Delivery Controller
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
ARP	Address Resolution Protocol
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
CAB	Change Advisory Board
CAS	Content Addressed Storage
CASB	Cloud Access Security Broker
CD	Continuous Deployment
CDN	Content Delivery Network
CI	Continuous Integration
CIFS	Common Internet File System
CIIS	Client Integration Implementation Service
CMDB	Configuration Management Database
CMS	Content Management System
CNA	Converged Network Adapter
COLO	Co-location
COOP	Continuity of Operations Plan
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSP	Content Service Provider
DAC	Discretionary Access Control
DAS	Direct Attached Storage
DBaaS	Database as a Service
DBMS	Database Management Server
DDoS	Distributed Denial of Service
DFS	Distributed File System

略語	定義
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DNSSEC	DNS Security
DoH	DNS over HTTPS
DoT	DNS over TLS
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSA	Distributed Services Architecture
EDR	Endpoint Detection and Response
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
FTPS	FTP over SSL
GENEVE	Generic Network Virtualization Encapsulation
GPT	GUID Partition Table
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HA	High Availability
HBA	Host Bus Adapter
HIDS	Host-Based IDS
HIPS	Host-Based IPS
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICMP	Internet Control Management Protocol
IDS	Intrusion Detection System
IFCP	Internet Fibre Channel Protocol

略語	定義
IGRP	Interior Gateway Routing Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IPAM	IP Address Management
IPC	Instructions Per Cycle
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
IPSec	IP Security
IQN	Initiator Qualified Name
iSCSI	Internet Small Computer Systems Interface
ISNS	Internet Storage Name Service
ISP	Internet Service Provider
JBOD	Just a Bunch of Disks
KVM	Kernel Virtual Machine
KVM	Keyboard Video Mouse
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTS	Long Term Support
LUN	Logical Unit Number
MAC	Mandatory Access Control
MBR	Master Boot Record
MDF	Main Distribution Facility
MFA	Multi-Factor Authentication
ML	Machine Learning
MPIO	MultiPath I/O
MPLS	Multiprotocol Label Switching
MSP	Managed Service Provider
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Controller
NIS	Network Information Service
NOC	Network Operations Center
NPIV	N_Port ID Virtualization
NTFS	New Technology File System
NTP	Network Time Protocol
NTS	Network Time Security
NVMe	Non-Volatile Memory Express
NVMe-oF	NVMe over Fabrics
ODBC	Open Database Connectivity

略語	定義
OLA	Operational Level Agreement
OS	Operating System
OSPF	Open Shortest Path First
P2P	Physical to Physical
P2V	Physical to Virtual
PaaS	Platform as a Service
PAT	Port Address Translation
PBX	Private (or Public) Branch Exchange
PIT	Point-in-Time
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
QA	Quality Assurance
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCP	Session Control Protocol
SCSI	Small Computer System Interface
SDLC	Software Development Life Cycle
SDN	Software Defined Network
SDN	Software-Defined Storage
SFTP	Secure FTP
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMB	Server Message Block
SMT	Simultaneous Multi-Threading
SNMP	Simple Network Management Protocol
SR-IOV	Single-Root Input/ Output Virtualization
SSD	Solid State Disk
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCO	Total Cost of Operations
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module

略語	定義
TTL	Time to Live
UAT	User Acceptance Testing
UDP	Universal Datagram Protocol
UPS	Universal Power Supply
V2P	Virtual to Physical
V2V	Virtual to Virtual
VAT	Virtual Allocation Table
VCPU	Virtual CPU
VDI	Virtual Desktop Infrastructure
vGPU	Virtual Graphics Processing Unit
VHD	Virtual Hard Disk
VLAN	Virtual LAN
VM	Virtual Machine
VMFS	Virtual Machine File System
VNC	Virtual Network Computing
VNIC	Virtual NIC
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VRAM	Virtual RAM
VSAN	Virtual SAN
vSwitch	Virtual Switch
VTL	Virtual Tape Library
VXLAN	Virtual ExtensibleLAN
WAF	Web Application Firewall
WAN	Wide Area Network
WMI	Windows Management Implementation
WWNN	World Wide Node Name
WWPN	World Wide Port Name
XaaS	Anything as a Service
ZFS	Z File System

CompTIA Cloud+のハードウェアとソフトウェア一覧

本リストは、CompTIA Cloud+の受験準備として役立てていただくためのハードウェアとソフトウェアのリストです。トレーニングを実施している企業でも、トレーニングの提供に必要なラボコンポーネントを作成したい場合に役立ちます。各トピックに箇条書きで挙げられた項目は例であり、すべてを網羅するものではありません。

ハードウェア

- 仮想化を実行できるコンピューター
- ネットワークスイッチ**
- ネットワークルーター**
- コンピュート（CPU、RAMなど）**
- NASまたはSAN**
- ケーブル**

ソフトウェア

- 自動化ツール
- ハイパーバイザー（Type1、Type2）
- クライアント（およびサーバー）OS
- 各種ウェブブラウザ
- CLI**
- 仮想化フォーマットコンバーター**

その他

- インターネットアクセス
- SaaS、PaaS、IaaS環境へのアクセス
- クラウドサービスプロバイダへのリモートアクセス（試用または無料のサービス）

**あれば望ましいですが、ラボのセットアップに必須ではありません