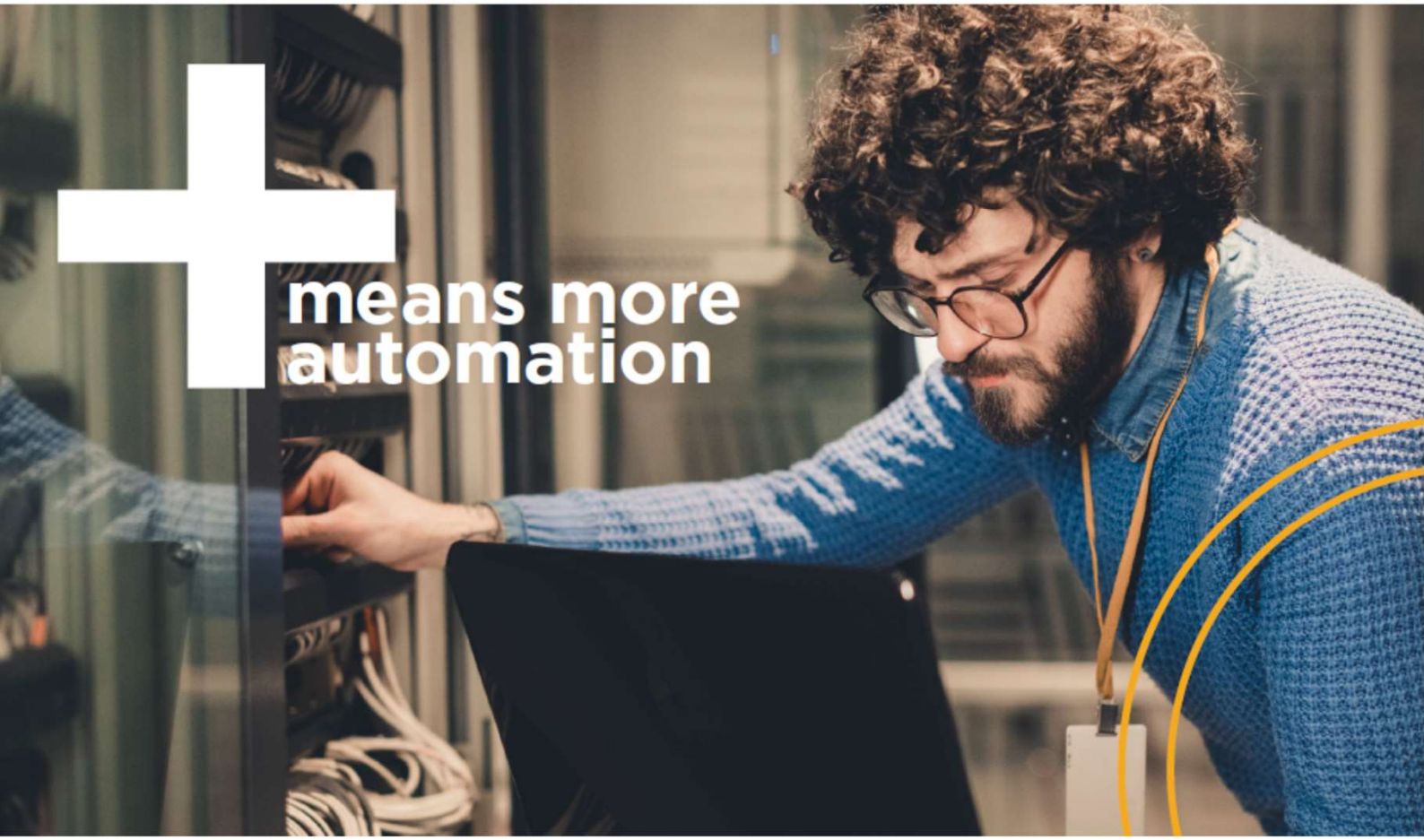
CompTIA



CompTIA Server+ SK0-004とSK0-005 出題範囲の比較

企業や組織は、今まで以上にインフラストラクチャへの投資、戦略を再検討しています。多くの企業でクラウドが利用が推進される一方で、ハイブリットソリューションへの信頼性の高まりも受け、オンプレミスとクラウドの両方のインフラストラクチャを理解し、セキュアに運用できるスキルを持った人材の必要性が高まっています。

今回のCompTIA Serer+の改訂では、企業のゴールを達成するためのインフラストラクチャ運用を業務とするプロフェッショナルに必要とされるスキルを反映しています。

改訂CompTIA Server+ SK0-005試験では、サーバー管理者、データセンターエンジニアといった職務において、サーバをセキュアにデプロイ、保守、トラブルシューティングするために必要となるスキルを評価します。出題範囲では、実践的なスキルの評価に重点を置き、テクノロジーの新旧の入れ替えを行っています。また、データセキュリティ、仮想化、クラウドソリューションの観点から必要とされる出題内容が含まれています。

CompTIA
Server+

CompTIA

出題範囲の比較

改訂試験SK0-005では、4つの出題範囲の分野で構成されています。（以前の試験は、7つの出題範囲に分かれていました。）SK0-005試験では、出題のターゲットをサーバー管理者により明確に絞ったため、いくつかの出題項目の取り扱いがなくなっています。
下記の表は、CompTIA Server+ SK0-005とSK0-004の出題範囲の比較表です

SK0-005	SK0-004	コメント
1.1 与えられたシナリオに基づいて、 物理的なハードウェアをインストール できる。	1.1 サーバーフォームファクターの機能と役割について説明することができる。	現在のサーバー管理者に必要とされるより実践的で高いレベルのスキル項目を追加。
1.1 与えられたシナリオに基づいて、 物理的なハードウェアをインストール できる。	1.2 与えられたシナリオに基づいて、サーバーコンポーネントの設置、設定、管理を実施することができる。	
1.1 与えられたシナリオに基づいて、 物理的なハードウェアをインストール できる。	1.3 電力と冷却のコンポーネントを比較対照することができる。	現在のサーバー管理者に必要とされるより実践的で高いレベルのスキル項目を追加。
1.2 与えられたシナリオに基づいて、 ストレージを導入し管理することができる。	3.1 与えられたシナリオに基づいて、特定の仕様とインターフェースを使用しプライマリストレージデバイスをインストール、展開することができる。	
1.3 与えられたシナリオに基づいて、サーバーのハードウェア のメンテナンスを実行することができる。	2.4 与えられたシナリオに基づいて、適切なサーバー管理手法を実施することができる。	
2.1 与えられたシナリオに基づいて、サーバーオペレーティングシステムを インストールできる。	2.1 サーバー用 OS のインストールと設定をすることができる。	
2.2 与えられたシナリオに基づいて、ネットワークインフラストラクチャサービス を使用するようにサーバーを構成できる。	5.1 与えられたシナリオに基づき、IP アドレッシングとネットワークインフラストラクチャサービスを利用してサーバーを設定することができる。	
2.3 与えられたシナリオに基づいて、サーバーの機能と特性を 構成し維持できる。	2.2 サーバーの役割と必要条件を比較対照することができる。	現在のサーバー管理者に必要とされるより実践的で高いレベルのスキル項目を追加。
2.4 サーバーの高可用性の主なコンセプトを説明できる。	2.4 与えられたシナリオに基づいて、適切なサーバー管理手法を実施することができる。	サーバーの高可用性の重要性が増していることを反映し、基本的なレベルのスキルを追加。
2.5 仮想化の目的とオペレーションを要約できる。	2.6 仮想化コンポーネントの目的と運用方法を説明することができる	
2.6 サーバー管理向けのスクリプティングの基本を要約できる。		自動化と仮想化のためのスクリプトのスキルを習得する重要性が増したため追加された項目。今回の改訂にあたり重要な変更点の一つ。
2.7 資産管理と文書化の重要性を説明できる。	2.5 資産管理と文書化の重要性を説明することができる。	
2.8 ライセンス付与のコンセプトを説明できる。		IaaSモデルと継続的なスケーラビリティの必要性が増したため追加された新しい項目の一つ。

SK0-005	SK0-004	コメント
3.1 データセキュリティの概要を要約できる。	4.5 データセキュリティの方法とセキュアストレージの処分テクニックを実行することができる。	重要度の変化により、SK0-004の出題内容の一部は、SK0-005の他の項目でもカバーされています。
3.2 物理的なセキュリティの概要を要約できる。	4.1 物理セキュリティの方法と概念を比較対照することができる。	
3.2 物理的なセキュリティの概要を要約できる。	4.4 企業のポリシーに基づいて、論理的なアクセス制御の方法を実装することができる。	
3.3 サーバー管理におけるアイデンティティアクセス管理に関する 重要なコンセプトを説明できる。	4.1 物理セキュリティの方法と概念を比較対照することができる。	
3.4 データセキュリティリスクと緩和戦略について説明できる。		データセキュリティの重要性とビジネスリスクに焦点をあてた新しい出題分野。脆弱性を軽減し、コンプライアンスの概念を理解することで違反の防止につなげます。
3.5 与えられたシナリオに基づいて、サーバーのハードニング方法を 適用できる。	4.2 与えられたシナリオに基づいて、サーバー要塞化の手法を適用することができる。	
3.6 適切なサーバーのデコミッショニングのコンセプトを要約できる。		データセキュリティの重要性の高まりを受け、大幅に更新された出題分野。
3.7 バックアップと復旧の重要性を説明できる。	6.2 与えられたシナリオに基づき、適切なバックアップの手法を実行することができる。	職務の変化を反映し、出題分野の重要度を変更。
3.8 災害復旧の重要性について説明できる。	6.1 災害復旧原則の重要性を説明することができる。	
4.1 トラブルシューティングの理論と方法論について説明できる。	7.1 トラブルシューティングの理論と方法を説明することができる。	
4.2 与えられたシナリオに基づいて、 一般的なハードウェアの障害を トラブルシューティングすることができる。	7.2 与えられたシナリオに基づき、適切なツールと方法を選択した上で、ハードウェアに関連する問題のトラブルシ ューティングを実施することができる。	
4.3 与えられたシナリオに基づいて、 ストレージの問題を トラブルシューティングすることができる。	7.5 与えられたシナリオに基づき、適切なツールと方法を選択し、ストレージに関連する障害を効果的にトラブルシ ューティングすることができる。	
4.4 与えられたシナリオに基づいて、 一般的なOSとソフトウェアの問題を トラブルシューティングすることができる。	7.3 与えられたシナリオに基づいて、適切なツールと方法を選択し、ソフトウェアに関連する障害を効果的にトラブ ルシューティングすることができる。	
4.5 与えられたシナリオに基づいて、ネットワークの接続性の問題を トラブルシューティングすることができる。	7.4 与えられたシナリオに基づき、適切なツールと方法を選択し、ネットワークに関連する障害を効果的に診断する ことができる。	
4.6 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。	7.6 与えられたシナリオに基づき、適切なツールと方法を選択し、セキュリティ関連する障害を効果的に診断するこ とができる。	