Windows Server の入門ドキュメント

Windows Server は、ワークグループからデータ センターまで接続されたアプリ、ネットワーク、Web サービス インフラストラクチャを構築し、オンプレミスと Azure を橋渡しします。

Overview

概要

Windows Serverとは

Windows Server 2025 の新機能

Windows Server Insiders プレビュー

概念

エディション機能の比較

ハードウェア要件

Windows Server で削除または開発されなくなった機能

Plan

概念

インストール、アップグレード、または移行

Server Core とデスクトップ エクスペリエンスを備えたサーバー

サービス チャネルの比較

概念

Microsoft サーバー アプリケーションの互換性

Windows Server 向け Azure ハイブリッド特典

インストールとアップグレード

デプロイ

インストール メディアから Windows Server をインストールする

Windows Server のアップグレードを計画する

インプレース アップグレードの実行

攻略ガイド

エディションとライセンスの種類を変換する

Server Core アプリの互換性をインストールする

Activation

概念

VM の自動アクティブ化

KMS ライセンス認証計画

攻略ガイド

KMS ホストを作成する

KMS クライアントのアクティブ化

Windows ボリュームアクティベーションのトラブルシューティング

Azure Arc 対応サーバー

概念

Azure Connected Machine エージェントのデプロイ オプション

攻略ガイド

Windows Server を Azure Arc に接続する

拡張セキュリティ更新プログラムの取得

Azure Arc を使用した拡張セキュリティ更新プログラムの提供

Azure Arc 対応サーバーのホットパッチを有効にする

Windows Serverとは

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

> **ヒント**
>
> Windows Server に関する知識は既にありますか? **Windows Server 2025 の新機能**に移動して、最新の機能と拡張機能について学習します。

Windows Server は、組織がオンプレミス、ハイブリッド、クラウド環境全体でアプリケーション、サービス、ワークロードを実行してセキュリティで保護できるようにする、Microsoft のエンタープライズ サーバー プラットフォームです。

小規模ビジネスを実行している場合でも、エンタープライズ インフラストラクチャを管理する場合でも、Windows Server は、組織に合わせて拡張される、セキュリティで保護されたスケーラブルで高パフォーマンスのコンピューティングの基盤を提供します。 数十年にわたる Windows イノベーションに基づいて構築されたこのソリューションは、世界中の何百万もの組織のバックボーンとして機能し、ファイル サーバーや Web アプリケーションから複雑なエンタープライズ ワークロードや AI 駆動型ソリューションまで、あらゆる機能を強化しています。

https://learn-video.azurefd.net/vod/player?id=715f723f-0644-4b9d-b7df-6e708da43242&locale=ja-jp&embedUrl=%2Fwindows-server%2Fget-started%2Foverview

Windows Server を選択する理由

Windows Server は、セキュリティ、パフォーマンス、信頼性を維持しながら、組織がインフラストラクチャを最新化するのに役立つ包括的な機能を提供します。

Windows Server は次の目的に使用します。

- **混在環境**: Windows、Linux、コンテナーのワークロードの統合管理。
- **エンタープライズ統合**: SQL Server、System Center、Exchange、SharePoint、Project、および既存の Windows インフラストラクチャとのシームレスな統合。
- **商用サポート**: アクティブな技術コミュニティによるエンタープライズ レベルのサポート。
- **コンプライアンス シナリオ**: 規制対象の業界 (医療、財務、政府) 向けの組み込み機能。
- **柔軟なライセンス**: 従量課金制、永続的ライセンス、サブスクリプション ベースのライセンスのいずれかを選択します。

Windows Server は、セキュリティ、パフォーマンス、クラウド統合を強化する新機能を備えたこの基盤上に構築されています。 次のセクションでは、Windows Server の主な利点と機能について説明します。

高度な多層セキュリティ

進化し続ける脅威に対する保護の強化、多層保護、回復性の向上。

- **高度な ID 保護**: Windows、Linux、Mac システム全体で一元的な認証、承認、ポリシー管理を提供するエンタープライズ ディレクトリ サービス (Active Directory)。
- **仮想化ベースのセキュリティ**: VBS エンクレーブを使用した Hyper-V セキュリティの強化と、コンフィデンシャル コンピューティングのキー保護。
- **セキュリティで保護されたネットワーク**: TLS 1.3 暗号化、QUIC 経由の SMB、および高度なマイクロセグメント化により、横攻撃の拡散を防ぎます。

クラウドの機敏性

Azure Arc を使用して、エッジとハイブリッド クラウド環境に Azure の機能を提供します。クラウド、データセンター、エッジでのハイブリッドなど、完全な柔軟性を備えたデプロイ。

- **デプロイの柔軟性**: オンプレミス、ハイブリッド、または統合管理を使用して Azure にデプロイする場合でも、一貫性のある Windows Server エクスペリエンス。
- **ホットパッチ**: 再起動せずにセキュリティ更新プログラムを適用します。生産性を向上させるために、年間 12 回の再起動が必要な回数から 4 回に短縮されます。
- **Azure Arc 統合**: Azure Arc は、Azure の管理機能をオンプレミス サーバーに拡張し、データが Azure、データセンター、その他のクラウド内にあるかどうかに関係なく、クラウドスタイルのガバナンス、セキュリティ ポリシー、監視を提供します。
- **従量課金制ライセンス**: Azure Arc を使用した柔軟なサブスクリプション ベースの価格。

高パフォーマンスで将来対応可能なインフラストラクチャ

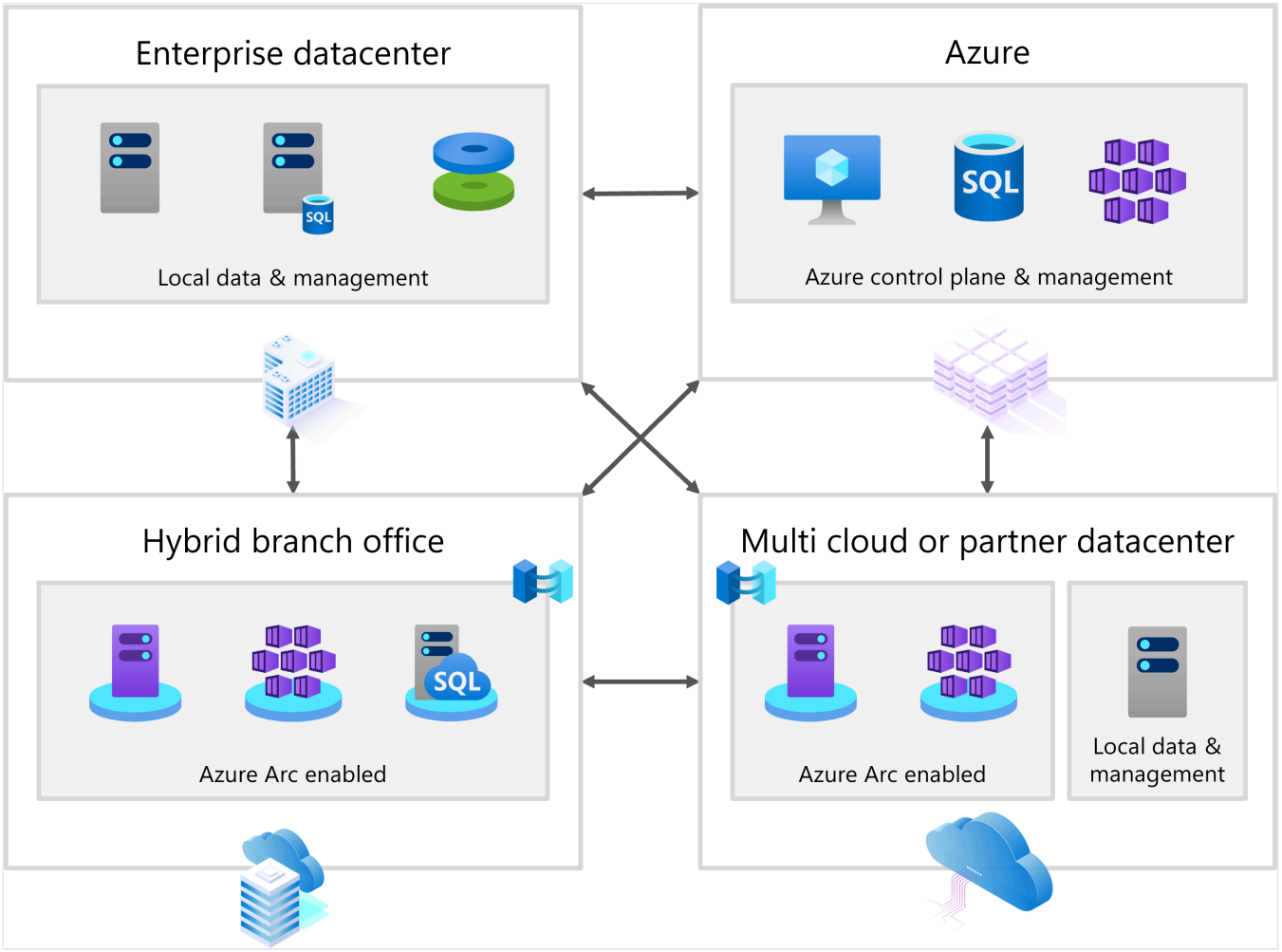
スケーラビリティ、パフォーマンス、ストレージ、および AI と ML をサポートする機能が飛躍的に向上します。

- **AI と ML 対応**: ライブ マイグレーションをサポートし、AI ワークロードとエッジ推論のパフォーマンスを強化した VM 間での GPU パーティション分割。
- **大規模**: Hyper-V を使用して、最も要求の厳しいワークロードに対して最大 240 TB の RAM と VM あたり 2,048 個の仮想プロセッサをサポートしてワークロードを仮想化します。
- **ストレージの最適化**: ソフトウェア定義ストレージの重複除去と圧縮が最適化された強化された ReFS。

新機能の詳細については、「 Windows Server 2025 の新機能」を参照してください。

Windows Server はどこに展開できますか?

Windows Server を使用すると、ビジネス ニーズに基づいてアプリケーションとデータの場所を柔軟に選択できます。 各展開オプションには、組織の成長とイノベーションを促進するのに役立つ固有の利点があります。 Windows Server は、クラウド、データセンター、または異なる環境のエッジでハイブリッド ソリューションとして展開できます。



Windows Server の展開:

- **☁ クラウド内**

  最大のスケーラビリティとグローバルリーチを実現するために、Azure に Windows Server 仮想マシンをデプロイします。 新しいアプリケーション、開発環境、または迅速にスケーリングする必要がある場合に最適です。

  最適な対象: 新しいプロジェクト、可変ワークロード、グローバル アプリケーション、ディザスター リカバリー シナリオ。

- **データセンター内**

環境を完全に制御するために、既存のインフラストラクチャを Windows Server にアップグレードします。 特定のコンプライアンス要件、既存のハードウェア投資、エアギャップ環境が必要な場合に最適です。

最適: 規制対象の業界、既存のインフラストラクチャ、特殊なハードウェア要件、完全なデータ制御。

- 🌐 **エッジでのハイブリッド**

  ワークロードをローカルで実行したまま、Azure Arc を使用してデータセンターを Azure に拡張します。 クラウド管理とサービスを使用したローカル パフォーマンスという両方の長所を最大限に活用できます。

  Azure Arc を通じてクラウド管理、監視、サービスを利用しながら、コンプライアンス、パフォーマンス、またはコスト上の理由から機密性の高いワークロードをオンプレミスに保持します。完全なクラウド コミットメントやデータ所在地の懸念なしにクラウドの利点を必要とする組織に最適です。

  ベスト:クラウドの段階的な導入、分散した場所、エッジ コンピューティングのシナリオ、クラウド機能を獲得しながら既存の投資を使用する。

エディション

Windows Server には、さまざまなスケールと仮想化のニーズに合わせて設計された 2 つのエディションが用意されています。

⛶ **テーブルを展開する**

エディション	Standard	データセンター
環境	仮想化のニーズが限られている物理サーバーまたは環境	高度に仮想化された環境とクラウド シナリオ
仮想化の権限	ライセンスごとに 2 台の仮想マシンと 1 つの Hyper-V ホスト	無制限の仮想マシンとライセンスごとに 1 つの Hyper-V ホスト
最適な用途	小規模から中規模のデプロイ、特定のワークロード、コスト重視の環境	大規模なデータセンター、クラウドデプロイ、広範な仮想化

どちらのエディションにも、同じ機能の多くが含まれています。 詳細な比較については、以下を参照してください。

- Windows Server エディションの比較
- Windows Server でのロックと制限の比較

デプロイのアプローチ

現在の環境と要件に基づいて、Windows Server を実装するための適切なアプローチを選択します。

テーブルを展開する

方法	説明	最適な対象者
クリーン インストール	新しいハードウェアにインストールするか、既存の OS を完全に置き換える	新しいデプロイ、最大パフォーマンス、複雑な構成
既存環境でのアップグレード	設定、ロール、データを保持しながらアップグレードする	VM、安定した構成、最小限のダウンタイム
移行	役割と機能を新しいインストールに段階的に移動する	複雑な環境、ミッション クリティカルなシステム
クラスターのローリング アップグレード	クラスター ノードを一度に 1 つずつアップグレードする	Hyper-V クラスター、Scale-Out ファイル サーバー、厳密な SLA

各方法の詳細な手順については、「インストール、アップグレード、および移行のオプション」を参照してください。

インストール オプション

Windows Server をインストールする場合は、サーバーの管理方法に基づいて、次の 2 つのオプションから選択します。

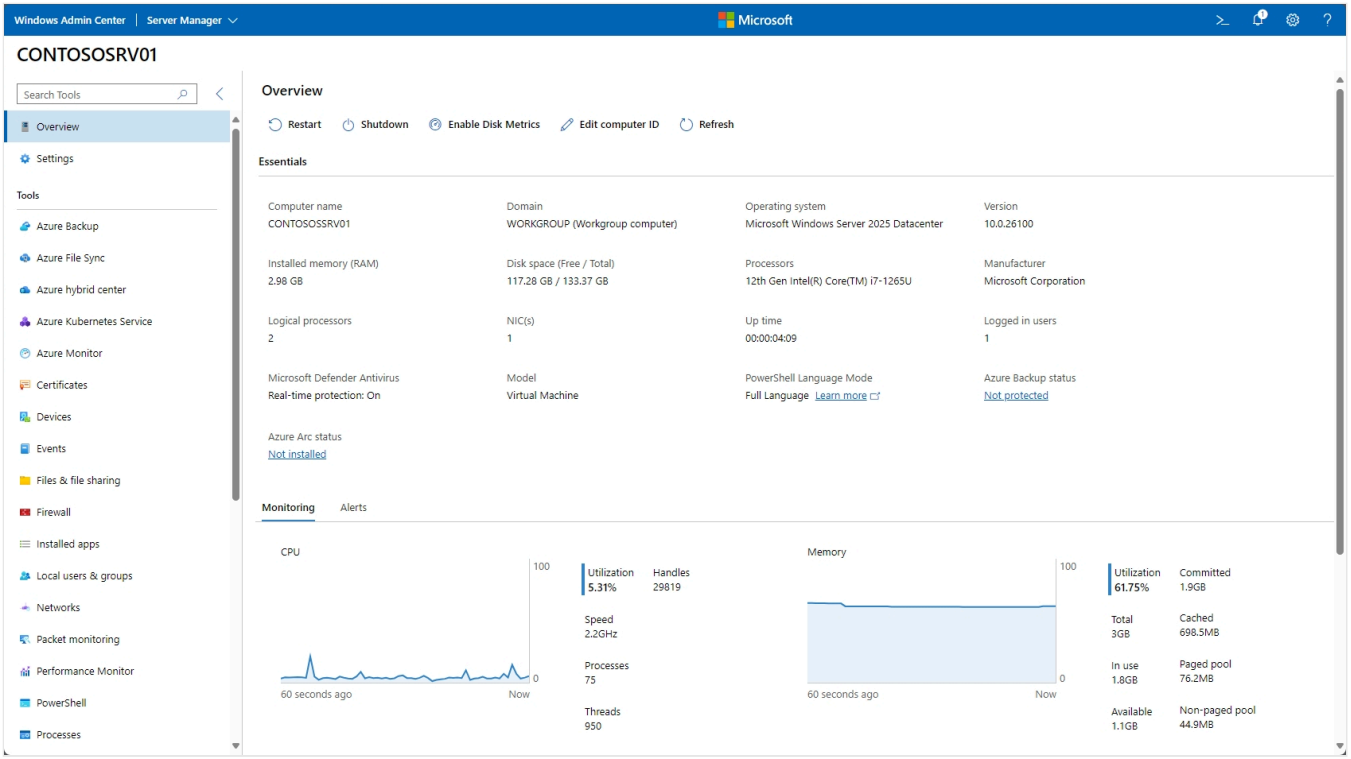
テーブルを展開する

インストール オプション	サーバー コア	デスクトップ エクスペリエンス搭載サーバー
説明	グラフィカル インターフェイスを使用しない最小限のインストール。 PowerShell、SConfig、またはリモート ツールを使用して管理されます。 フットプリントが小さく、攻撃面が減少し、パフォーマンスが向上します。	標準の Windows デスクトップとすべての GUI 管理ツールを使用した完全インストール。 使い慣れたインターフェイスとローカルのグラフィカル管理を提供します。
Best For	ほとんどのサーバー ワークロード (特にリモート管理を使用する場合)	ローカル GUI アクセスまたはデスクトップ依存アプリケーションを必要とするサーバー

相違点と詳細なガイダンスの詳細については、 Server Core とデスクトップ エクスペリエンスを備えた Server を参照してください。

Windows Server の管理

Windows Server には、単一サーバーからエンタープライズ データセンターにスケーリングする複数の管理ツールが用意されています。



Windows Server は、次の 1 つ以上の方法を使用して管理できます。

🌐 **Windows Admin Center**: 日常的なサーバー管理のための最新のブラウザー ベースの管理。 ハイブリッド シナリオでは、ローカルで動作するか、Azure portal と統合します。

☁️ **Azure Arc**: データセンター、他のクラウド、またはエッジの場所の任意の場所のサーバーに対して、Azure のガバナンス、セキュリティ、監視を拡張するクラウドベースの管理。

🔧 **ローカル ツール**: サーバー マネージャー (GUI 管理)、PowerShell (オブジェクト指向のコマンド シェルとスクリプト言語)、サーバーへの直接アクセスと自動化のためのリモート サーバー管理ツールなどの従来の管理。

🏢 **System Center**: 包括的な監視、デプロイ、構成管理を必要とする大規模データセンター向けのエンタープライズ規模の管理。

環境のサイズとクラウド戦略に基づいて、管理アプローチを選択します。 詳細なガイダンスについては、「 Windows Server 管理の概要」を参照してください。

Windows Insider Program

Windows Server 用 Windows Insider Program には、Windows Server のプレビュー ビルドが用意されており、Windows Server の将来を学習、テスト、および形成するための早期アクセスが可能です。 詳細については、 Windows Server 用 Windows Insider Program の使用を開始し、 Windows Server Insider コミュニティ に参加できます。

Windows Server を始めてみましょう

Windows Server 体験を開始する準備はできましたか? 無料の評価から始めて、環境内でテストします。

- Windows Server 2025 評価版をダウンロードする
- システム要件を表示する
- アップグレードガイダンスを取得する
- Windows Server のラーニング パスを参照 して、新しいスキルを学習し、詳細なガイダンスを使用して展開を高速化します。

Windows Server の最新ニュースについては、 Windows Server のブログ を参照して、Windows Server エンジニアリング チームからの発表、機能、イベント、その他の情報を最新の状態に保ちます。 また、Windows Server コミュニティ にアクセスして、ベスト プラクティスの共有、最新のニュースの入手、Windows Server に関する専門家からの学習を行うこともできます。

ⓘ **注:** この記事には、AI で作成されたコンテンツが含まれています。 詳細情報

Last updated on 2025/08/13

Windows Server 2025 の新機能

適用対象: ✅ Windows Server 2025

この記事では、セキュリティ、パフォーマンス、柔軟性を向上させる高度な機能を備える Windows Server 2025 の最新の開発について説明します。 より高速なストレージ オプションとハイブリッド クラウド環境と統合する機能により、インフラストラクチャの管理が効率化されました。 Windows Server 2025 は、その前身の強力な基盤に基づいており、ニーズに合わせてさまざまな革新的な機能強化が導入されています。

デスクトップ エクスペリエンスとアップグレード

アップグレード オプションとデスクトップ エクスペリエンスについて確認します。

Windows Server 2012 R2 からのインプレース アップグレード

Windows Server 2025 では、一度に最大 4 つのバージョンをアップグレードできます。 Windows Server 2012 R2 以降から Windows Server 2025 に直接アップグレードできます。

デスクトップ シェル

初めてサインインすると、デスクトップ シェル エクスペリエンスは Windows 11 のスタイルと外観に準拠します。

Bluetooth

Windows Server 2025 のBluetoothを使用して、マウス、キーボード、ヘッドセット、オーディオ デバイスなどを接続できるようになりました。

DTrace

Windows Server 2025 には、ネイティブ ツールとして `dtrace` が搭載されています。 DTrace は、ユーザーがシステムのパフォーマンスをリアルタイムで監視およびトラブルシューティングできるようにするコマンド ライン ユーティリティです。 DTrace を使用すると、カーネル コードとユーザー空間コードの両方を動的にインストルメント化できます。コード自体を変更する必要はありません。 この汎用性の高いツールは、集計、ヒストグラム、ユーザー レベルのイベントのトレースなど、さまざまなデータ収集と分析の手法をサポートします。 詳細については、コマンドラインヘルプについて DTrace をご覧ください。その他の機能については Windows 上での DTrace を参照してください。

電子メールとアカウント

Windows Server 2025 の [**アカウント**]> の [Windows **設定**] で、次の種類のアカウントを追加できるようになりました。

- Microsoft Entra ID
- Microsoft アカウント
- 職場または学校アカウント

ドメイン参加は、ほとんどの状況で引き続き必要です。

フィードバックハブ

Windows Server 2025 の使用時に発生したフィードバックや問題を報告するには、Windows フィードバック ハブを使用します。 問題の原因となったプロセスのスクリーンショットや記録を含めると、お客様の状況を把握し、Windows エクスペリエンスを向上させる提案を共有できます。 詳細については、フィードバック ハブを参照してください。

ファイル圧縮

Windows Server 2025 には、新しい圧縮機能があります。 アイテムを圧縮するには、右クリックして [**圧縮して**へ] を選択します。 この機能では、ZIP 、7z、および tar 圧縮形式 をサポートし、それぞれに固有の圧縮方法を使用します。

ピン留めされたアプリ

最も使用されているアプリのピン留めは、[**スタート**] メニューから利用できるようになり、ニーズに合わせてカスタマイズできるようになりました。 現在、既定のピン留めされたアプリは次のとおりです。

- Azure Arc のセットアップ
- フィードバックハブ
- エクスプローラー
- Microsoft Edge
- サーバー マネージャ
- Settings
- Terminal
- Windows PowerShell

タスク マネージャ

Windows Server 2025 は、Windows 11 のスタイルに準拠 Mica 素材 を備えた最新のタスク マネージャー アプリを使用します。

Wi-Fi

ワイヤレス LAN サービス機能が既定でインストールされるようになったため、ワイヤレス機能を有効にする方が簡単になりました。 ワイヤレス スタートアップ サービスは手動に設定されています。 有効にするには、コマンド プロンプト、Windows ターミナル、または PowerShell で `net start wlansvc` を実行します。

Windows ターミナル

コマンド ライン ユーザー向けの強力で効率的なマルチシェル アプリケーションである Windows ターミナル は、Windows Server 2025 で使用できます。 検索バーで **ターミナル** を検索します。

WinGet

WinGet は既定でインストールされます。これは、Windows デバイスにアプリケーションをインストールするための包括的なパッケージ マネージャー ソリューションを提供するコマンド ライン Windows パッケージ マネージャー ツールです。 詳細については、「WinGet ツールを使用してアプリケーションをインストールおよび管理する」を参照してください。

高度な多層セキュリティ

Windows 2025 のセキュリティについて説明します。

ホットパッチ (プレビュー)

ホットパッチは、Azure Arc ポータルでホットパッチが有効になった後、Azure Arc に接続されている Windows Server 2025 マシンで使用できるようになりました。 Hotpatch を使用すると、コンピューターを再起動せずに OS セキュリティ更新プログラムを適用できます。 詳細については、ホットパッチに関するページを参照してください。

> **重要**
>
> Azure Arc 対応ホットパッチは現在プレビュー段階です。 ベータ版、プレビュー版、または一般提供としてまだリリースされていない Azure の機能に適用される法律条項については、「**Microsoft Azure プレビューの追加使用条件**」を参照してください。

クレデンシャルガード

Windows Server 2025 以降、要件を満たすデバイスでは Credential Guard が既定で有効になります。 Credential Guard の詳細については、「Credential Guard の構成」を参照してください。

Active Directory Domain Services

Active Directory Domain Services (AD DS) と Active Directory Lightweight Domain Services (AD LDS) に行われた最新の機能強化では、ドメイン管理エクスペリエンスの最適化を目的とするさまざまな新機能が導入されています。

- **32k データベース ページ サイズのオプション機能**: Active Directory では、8k データベース のページ サイズを使用する Windows 2000 の導入以降、拡張可能記憶域エンジン (ESE) データベースを使用します。 8k アーキテクチャ設計の決定により、Active Directory 全体で制限が生じ、Active Directory の最大制限であるスケーラビリティに関する記事に記載されています。 この制限の例として、Active Directory オブジェクトが 8k バイト以下の単一レコードである場合があります。 32,000 個のデータベース ページ形式に移行すると、従来の制限の影響を受ける領域が大幅に改善されます。 複数値の属性が最大で約 3,200 の値を保持できるようになりました。これは、2.6 倍の増加です。

  64 ビットの長い値 ID (LID) を使用する 32k ページ データベースを使用して新しいドメイン コントローラー (DC) をインストールし、以前のバージョンとの互換性のために 8k ページ モードで実行できます。 アップグレードされた DC は、現在のデータベース形式と 8,000 ページを引き続き使用します。 32k ページデータベースへの移行はフォレスト全体で行われ、フォレスト内のすべての DC に 32k ページ対応データベースが必要です。

- **Active Directory スキーマの更新**: Active Directory スキーマを拡張する 3 つの新しいログ データベース ファイル (`sch89.ldf`、 `sch90.ldf`、 `sch91.ldf`) が導入されました。 AD LDS と同等のスキーマの更新が `MS-ADAM-Upgrade3.ldf` に含まれています。 以前のスキーマ更新プログラムの詳細については、Windows Server Active Directory スキーマの更新に関するページを参照してください。

- **Active Directory オブジェクト修復**: エンタープライズ管理者は、 `SamAccountType` および `ObjectCategory` 不足しているコア属性を持つオブジェクトを修復できるようになりました。 エンタープライズ管理者は、オブジェクトの `LastLogonTimeStamp` 属性を現在の時刻にリセットできます。 これらの操作は、と呼ばれる影響を受けるオブジェクトの新しい `fixupObjectState` 変更操作機能によって実現されます。

- **チャネル バインド監査のサポート**: Lightweight Directory Access Protocol (LDAP) チャネル バインドに対してイベント 3074 と 3075 を有効にできるようになりました。 チャネル バインド ポリシーをより安全な設定に変更すると、管理者は、チャネル バインドを

サポートしていない、または失敗する環境内のデバイスを識別できます。 これらの監査イベントは、Windows Server 2022 以降でも KB4520412 を介して使用できます。

- **DC ロケーション アルゴリズムの機能強化**: DC 検出アルゴリズムは、短い NetBIOS スタイルのドメイン名を DNS スタイルのドメイン名にマッピングする機能が強化された新機能を提供します。 詳細については、「Windows および Windows Serverでのドメイン コントローラーの検索」を参照してください。

  > ⓘ Note
  >
  > Windows では DC 検出操作中に mailslots を使用しません。マイクロソフトは、これらのレガシ テクノロジの WINS と mailslots の 廃止を発表したためです。

- **フォレストとドメインの機能レベル**: 新しい機能レベルは、一般的なサポートのために使用され、新しい 32k データベース ページ サイズ機能に必要です。 新しい機能レベルは、自動実行インストールの値 `DomainLevel 10` と、自動実行インストールの値 `ForestLevel 10` にマップされます。 Microsoft には、Windows Server 2019 と Windows Server 2022 の機能レベルを新しく入れ替える予定はありません。 DC の無人昇格と降格を実行するには、ドメイン コントローラーの無人昇格と降格 DCPROMO 応答ファイル構文を参照してください。

  DsGetDcName API では、Windows Server 2025 を実行している DC の場所を有効にする新しいフラグ `DS_DIRECTORY_SERVICE_13_REQUIRED` もサポートされています。 機能レベルの詳細については、次の記事を参照してください。
  - AD DS の機能レベル
  - ドメインの機能レベルを上げる
  - フォレストの機能レベルを上げる

  > ⓘ Note
  >
  > 新しい Active Directory フォレストまたは AD LDS 構成セットは、Windows Server 2016 以降の機能レベルを持っている必要があります。 Active Directory または AD LDS レプリカを昇格するには、既存のドメインまたは構成セットが Windows Server 2016 以降の機能レベルで既に実行されている必要があります。
  >
  > Microsoft では、次のリリースに備えて、すべてのお客様が Active Directory および AD LDS サーバーを Windows Server 2022 にアップグレードする計画を開始することをお勧めします。

- **名前/SID 参照**のアルゴリズムが改善されました:ローカル セキュリティ機関 (LSA) 名とマシン アカウント間の SID 参照転送では、従来の Netlogon セキュリティで保護されたチ

ャネルが使用されなくなりました。 代わりに、Kerberos 認証と DC ロケーター アルゴリズムが使用されます。 従来のオペレーティング システムとの互換性を維持するために、フォールバック オプションとして Netlogon セキュア チャネルを使用することも可能です。

- **機密属性**セキュリティが強化されました。DC と AD LDS インスタンスでは、LDAP が接続の暗号化時に機密属性を含む操作の追加、検索、変更のみを行うことができます。

- **既定のコンピューター アカウント パスワードのセキュリティが強化**: Active Directory では、ランダムに生成される既定のコンピューター アカウント パスワードが使用されるようになりました。 Windows 2025 DC では、コンピューター アカウントのパスワードをコンピューター アカウント名の既定のパスワードに設定することがブロックされます。

  この動作を制御するには、ドメイン コントローラー グループ ポリシー オブジェクト *(GPO)* 設定を有効にします。コンピューターの構成*Windows* 設定\セキュリティ設定\ローカル ポリシー\セキュリティ オプション にある既定のコンピューター アカウント のパスワード の設定を拒否します。

  Active Directory 管理センター (ADAC)、Active Directory ユーザーとコンピューター (ADUC)、`net computer`、`dsmod` などのユーティリティでも、この新しい動作が優先されます。 ADAC と ADUC の両方で、Windows 2000 より前のアカウントの作成が許可されなくなりました。

- 暗号化の機敏性に対する Kerberos PKINIT のサポート : Kerberos (PKINIT) プロトコル実装での初期認証のための Kerberos 公開キー暗号化が更新され、より多くのアルゴリズムをサポートし、ハードコーディングされたアルゴリズムを削除することで、暗号化の機敏性が実現されます。

- **チケット発行チケットに使用されるアルゴリズムの変更**: Kerberos 配布センターは、RC4-HMAC(NT) などのRC4暗号化を使用して、チケット発行チケットを発行しなくなります。

- **サポートされている暗号化の種類の構成に対する Kerberos の変更**: Kerberos では、パス `SupportedEncryptionTypes` で見つかった従来のレジストリ キー REG_DWORD `HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Kerberos\Parameters` を受け入れなくなりました。代わりにグループ ポリシーを使用することをお勧めします。 グループ ポリシー設定の詳細については、「ネットワーク セキュリティ: Kerberos で許可される暗号化の種類を構成する」を参照してください。

- **LAN Manager GPO 設定**: GPO 設定 **ネットワーク セキュリティ: 次回のパスワード変更時に LAN Manager ハッシュ値を格納しないでください** は存在せず、新しいバージョンの Windows には適用されません。

- **既定では、LDAP 暗号化**: すべての新しい Active Directory 展開では、簡易認証およびセキュリティ層 (SASL) バインド後のすべての LDAP クライアント通信に対して、既定で LDAP 署名 (シール) が必要です。 署名動作の詳細については、「 Active Directory Domain Services の LDAP 署名」を参照してください。

- **LDAP によるトランスポート層セキュリティ (TLS) 1.3**のサポート: LDAP は最新の SCHANNEL 実装を使用し、TLS 接続を介した LDAP に対して TLS 1.3 をサポートします。 TLS 1.3 を使用すると、古い暗号化アルゴリズムが不要になり、古いバージョンよりもセキュリティが強化されます。 TLS 1.3 は、できるだけ多くのハンドシェイクを暗号化することを目的としています。 詳細については、 Windows Server 2022 の TLS/SSL (Schannel SSP) および TLS 暗号スイートのプロトコルに関するページを参照してください。

- **レガシ セキュリティ アカウント マネージャー (SAM) リモート プロシージャ コール (RPC) のパスワード変更動作**: Kerberos などのセキュリティで保護されたプロトコルは、ドメイン ユーザー パスワードを変更する推奨される方法です。 DC では、リモートで呼び出されたときに、SamrUnicodeChangePasswordUser4 Advanced Encryption Standard (AES) を使用して 最新の SAM RPC パスワード変更方法が既定で受け入れられます。 次の従来の SAM RPC メソッドは、リモートで呼び出されると既定でブロックされます。
  - SamrChangePasswordUser
  - SamrOemChangePasswordUser2
  - SamrUnicodeChangePasswordUser2

  Protected Users グループのメンバーであるドメイン ユーザーと、ドメイン メンバー コンピューター上のローカル アカウントの場合、従来の SAM RPC インターフェイスを介したリモート パスワードの変更はすべて既定でブロックされます (`SamrUnicodeChangePasswordUser4`を含む)。

  この動作を制御するには、次の GPO 設定を使用します。

  コンピューターの構成>管理用テンプレート>システム>セキュリティ アカウント マネージャー>SAM 変更パスワード RPC メソッド ポリシーの構成

- **一様でないメモリ アクセス (NUMA) のサポート**: AD DS では、すべてのプロセッサ グループで CPU を使用して NUMA 対応ハードウェアを利用できるようになりました。 以前は、Active Directory はグループ 0 の CPU のみを使用していました。 Active Directory は 64 コアを超えて拡張できます。

- **パフォーマンス カウンター**: 次のカウンターのパフォーマンスの監視とトラブルシューティングを利用できるようになりました。
  - **DC ロケーター**: クライアントおよび DC に固有のカウンターを使用できます。
  - **LSA 検索**: `LsaLookupNames`、 `LsaLookupSids`、および同等の API を使用した名前と SID の検索。 これらのカウンターは、クライアントとサーバーの両方のバージョンで使用

できます。
    - **LDAP クライアント**: KB 5029250 更新プログラムを介して Windows Server 2022 以降で使用できます。

- **レプリケーションの優先順位**: 管理者は、特定の名前付けコンテキストに対して、特定のレプリケーション パートナーを使用して、システム計算レプリケーションの優先順位を上げることができます。 この機能により、特定のシナリオに対処するため、レプリケーション順位を今までより柔軟に構成できます。

委任された管理サービス アカウント

この新しい種類のアカウントにより、サービス アカウントから委任された管理サービス アカウント (dMSA) への移行が可能になります。 このアカウントの種類には、元のサービス アカウント パスワードが無効になっている間にアプリケーションの変更を最小限に抑えるために、マネージド キーと完全ランダム化キーが付属しています。 詳細については、 委任された管理サービスアカウントの概要を参照してください。

Windows ローカル管理者パスワード ソリューション

Windows ローカル管理者パスワード ソリューション (LAPS) は、組織がドメインに参加しているコンピューターでローカル管理者パスワードを管理するのに役立ちます。 各コンピューターのローカル管理者アカウントに対して一意のパスワードが自動的に生成されます。 その後、Active Directory に安全に格納され、定期的に更新されます。 自動的に生成されたパスワードは、セキュリティの向上に役立ちます。 攻撃者が侵害されたパスワードや推測しやすいパスワードを使用して機密性の高いシステムにアクセスするリスクを軽減します。

Microsoft LAPS の新機能には、次の機能強化が導入されています。

- **新しい自動アカウント管理**: IT 管理者は、マネージド ローカル アカウントを簡単に作成できるようになりました。 この機能を使用すると、アカウント名をカスタマイズし、アカウントを有効または無効にすることができます。 セキュリティを強化するためにアカウント名をランダム化することもできます。 この更新プログラムには、Microsoft の既存のローカル アカウント管理ポリシーとの統合も強化されています。 この機能の詳細については、 Windows LAPS アカウント管理モードに関するページを参照してください。

- **新しいイメージ ロールバック検出**: Windows LAPS は、イメージのロールバックが発生したときに検出されるようになりました。 ロールバックが行われると、Active Directory に格納されているパスワードが、デバイスにローカルに格納されているパスワードと一致しなくなる可能性があります。 ロールバックにより、破損状態になることがあります。 この場合、IT 管理者は、永続化された Windows LAPS パスワードを使用してデバイスにサインインできません。

この問題に対処するために、`msLAPS-CurrentPasswordVersion`と呼ばれる Active Directory 属性を含む新しい機能が追加されました。 この属性には、新しいパスワードが Active Directory に永続化され、ローカルに保存されるたびに、Windows LAPS によって書き込まれるランダム・グローバル一意識別子 (GUID) が含まれます。 すべての処理サイクル中に、`msLAPS-CurrentPasswordVersion` に格納されている GUID が照会され、ローカルに永続化されたコピーと比較されます。 それらが異なる場合、パスワードはすぐにローテーションされます。

この機能を有効にするには、`Update-LapsADSchema` コマンドレットの最新バージョンを実行します。 その後、Windows LAPS は新しい属性を認識し、使用を開始します。 更新されたバージョンの `Update-LapsADSchema` コマンドレットを実行しない場合、Windows LAPS はイベント ログに 10108 警告イベントを記録しますが、他のすべての点で正常に機能し続けます。

この機能を有効化または構成するためにポリシー設定は使用されません。 この機能は、新しいスキーマ属性が追加された後に常に有効になります。

- **新しいパスフレーズ**: IT 管理者は、複雑でないパスフレーズを生成できる Windows LAPS の新機能を使用できるようになりました。 例として、EatYummyCaramelCandyなどのパスフレーズがあります。 この語句は、**V3r_b4tim#963 のような従来のパスワードと比較して、読みやすく、覚えやすく、入力しやすいですか**?.

  この新機能を使用すると、`PasswordComplexity` ポリシー設定を構成して、パスフレーズに 3 つの異なる単語リストのいずれかを選択できます。 すべてのリストは Windows に含まれており、個別のダウンロードは必要ありません。 `PassphraseLength` と呼ばれる新しいポリシー設定は、パスフレーズで使用される単語の数を制御します。

  パスフレーズを作成すると、選択した単語リストから指定した単語数がランダムに選択され、連結されます。 各単語の最初の文字は、読みやすくするために大文字になります。 この機能では、Active Directory または Microsoft Entra ID へのパスワードのバックアップも完全にサポートされています。

  3 つの新しい `PasswordComplexity` パスフレーズ設定で使用されるパスフレーズ ワードリストは、Electronic Frontier Foundation の記事「Deep Dive: EFF'S New Wordlists for Random Passphrases」から引用したものです。 Windows LAPS パスフレーズ ワードリスト は CC-BY-3.0 表示ライセンスに基づいてライセンスされており、ダウンロードできます。

  > **Note**
  >
  > Windows LAPS では、組み込みの単語リストのカスタマイズや、顧客が構成した単語リストの使用は許可されません。

- **読みやすさのパスワード ディクショナリの**が改善されました。Windows LAPS では、IT 管理者が複雑でないパスワードを作成できる新しい `PasswordComplexity` 設定が導入されています。 この機能を使用すると、LAPS をカスタマイズして、`4`の既存の複雑さの設定のような 4 つの文字カテゴリ (大文字、小文字、数字、特殊文字) をすべて使用できます。 `5`の新しい設定では、パスワードの読みやすさを高め、混乱を最小限に抑えるために、より複雑な文字が除外されます。 たとえば、1 数字と、l 文字は、新しい設定では使用されません。

  `PasswordComplexity`するように `5` を構成すると、既定のパスワード ディクショナリ文字セットに次の変更が加えられます。
  - **使用しないでください**: 文字 I、O、Q、l、o
  - **使用しないでください**: 数字 0、1
  - **使用しないでください**: 特殊文字 ,, ., &, {, }, [,], (,), ;
  - **使用**: 特殊文字 :、=、、、*

  ADUC スナップイン (Microsoft 管理コンソール経由) で、Windows LAPS タブが強化されました。Windows LAPS パスワードが新しいフォントに表示され、プレーン テキストで表示される際の読みやすさが向上します。

- **個々のプロセス**を終了するための認証後アクションのサポート: **認証後アクション** (PAA) グループ ポリシー設定 (`Reset the password, sign out the managed account, and terminate any remaining processes`) に新しいオプションが追加されます。これは、**コンピューター構成**>**管理用テンプレート**>**システム**>LAPS>**認証後アクション**にあります。

  この新しいオプションは、前のオプション `Reset the password and log off the managed account`の拡張機能です。 構成後、PAA は対話型サインイン セッションを通知して終了します。 Windows LAPS によって管理されているローカル アカウント ID でまだ実行されている残りのプロセスを列挙して終了します。 この終了の前に通知はありません。

  PAA の実行中にログ イベントを拡張すると、操作に関するより深い分析情報が得られます。

Windows LAPS の詳細については、「Windows LAPS とは」を参照してください。

OpenSSH

以前のバージョンの Windows Server では、OpenSSH 接続ツールを使用する前に手動インストールが必要でした。 OpenSSH サーバー側コンポーネントは、Windows Server 2025 に既定でインストールされます。 **リモート SSH アクセス** の下にあるサーバー マネージャー UI には、`sshd.exe` サービスを有効または無効にするためのワンステップ オプションも含まれています。 また、 **OpenSSH Users** グループにユーザーを追加して、デバイスへのアクセスを許可

または制限することもできます。 詳細については、「OpenSSH for Windows の概要」を参照してください。

セキュリティ ベースライン

カスタマイズされたセキュリティ ベースラインを実装することで、推奨されるセキュリティ態勢に基づいて、デバイスまたは VM ロールのセキュリティ対策を最初から確立できます。 このベースラインには、350 を超える構成済みの Windows セキュリティ設定が用意されています。 この設定を使用して、Microsoft と業界標準で推奨されるベスト プラクティスに沿った特定のセキュリティ設定を適用および適用できます。 詳細については、「OSConfig の概要」を参照してください。

仮想化ベースのセキュリティ エンクレーブ

仮想化ベースのセキュリティ (VBS) エンクレーブは、ホスト アプリケーションのアドレス空間内のソフトウェア ベースの信頼された実行環境です。 VBS エンクレーブでは、ベースとなる VBS テクノロジ を使用してアプリケーションの機密性の高い部分をメモリのセキュリティで保護されたパーティションに分離します。 VBS エンクレーブを使用すると、機密性の高いワークロードをホスト アプリケーションとシステムの残りの部分の両方から分離できます。

VBS エンクレーブでは、管理者を信頼する必要性を排除し、悪意のある攻撃者に対する防御を強化することで、アプリケーションでシークレットを保護できます。 詳細については、 VBS エンクレーブ Win32 リファレンスを参照してください。

仮想化ベースのセキュリティ キー保護

VBS キー保護を使用すると、Windows 開発者は VBS を使用して暗号化キーをセキュリティで保護できます。 VBS では、CPU の仮想化拡張機能を使用して、通常の OS の外部に分離されたランタイムを作成します。

使用中は、VBS キーはセキュリティで保護されたプロセスで分離されます。 キー操作は、この領域の外部で秘密キー マテリアルを公開することなく発生する可能性があります。 待機状態では、TPMキーが秘密鍵のマテリアルを暗号化し、VBSキーをデバイスに紐づけます。 この方法で保護されたキーは、プロセス メモリからダンプしたり、ユーザーのコンピューターからプレーン テキストでエクスポートしたりすることはできません。

VBS キー保護は、管理者レベルの攻撃者による流出攻撃を防ぐのに役立ちます。 キー保護を使用するには、VBS を有効にする必要があります。 VBS を有効にする方法については、「メモリ整合性を有効にする」を参照してください。

セキュリティで保護された接続

次のセクションでは、接続のセキュリティについて説明します。

セキュリティで保護された証明書管理

Windows での証明書の検索または取得では、CertFindCertificateInStore および CertGetCertificateContextProperty関数で説明されているように、SHA-256 ハッシュがサポートされるようになりました。 TLS サーバー認証は Windows 全体でより安全であり、RSA キーの最小長は 2,048 ビットである必要があります。 詳細については、TLS サーバー認証における弱い RSA 証明書の廃止 に関するブログを参照してください。

SMB over QUIC (ネットワークプロトコル)

SMB over QUIC サーバー機能が、Windows Server Standard バージョンと Windows Server Datacenter バージョンの両方で使用できるようになりました。 SMB over QUIC には、低遅延の暗号化された接続を提供するという QUIC のメリットが追加されています。

SMB over QUIC 有効化ポリシー

管理者は、グループ ポリシーと PowerShell を使用して、QUIC 経由の SMB クライアントを無効にすることができます。 グループ ポリシーを使用して SMB over QUIC を無効にするには、次のパスの [**SMB over QUIC ポリシーを有効にする**] を [**無効**] に設定します。

- コンピューターの構成\管理用テンプレート*Network**Lanman Workstation*
- コンピューターの構成\管理用テンプレート*Network**Lanman Server*

PowerShell を使用して SMB over QUIC を無効にするには、管理者特権の PowerShell プロンプトで次のコマンドを実行します。

PowerShell

```
Set-SmbClientConfiguration -EnableSMBQUIC $false
```

SMB署名と暗号化の監査

管理者は、SMB サーバーとクライアントの監査を有効にして、SMB 署名と暗号化をサポートできます。 Microsoft 以外のクライアントまたはサーバーが SMB 暗号化または署名をサポートしていない場合は、検出できます。 Microsoft 以外のデバイスまたはソフトウェアで SMB 3.1.1 がサポートされていると示されているが、SMB 署名のサポートに失敗した場合、 SMB 3.1.1 認証前の整合性 プロトコル要件に違反します。

グループ ポリシーまたは PowerShell を使用して、SMB 署名と暗号化の監査設定を構成できます。 これらのポリシーは、次のグループ ポリシー パスで変更できます。

- コンピューターの構成\管理用テンプレート\ネットワーク*Lanman Server*\監査クライアントは暗号化をサポートしていません
- *Computer Configuration*\管理テンプレート*Network**Lanman Server*\監査クライアントは署名をサポートしていません
- *Computer Configuration**Administrative Templates**Network**Lanman Workstation**Audit* サーバーは暗号化をサポートしていません
- *Computer Configuration**Administrative Templates**Network**Lanman Workstation**Audit* サーバーは署名をサポートしていません

PowerShell を使用してこれらの変更を実行するには、管理者特権のプロンプトで次のコマンドを実行します。ここで、`$true` はこれらの設定を有効にし、`$false` は無効にします。

PowerShell

```
Set-SmbServerConfiguration -AuditClientDoesNotSupportEncryption $true
Set-SmbServerConfiguration -AuditClientDoesNotSupportSigning $true

Set-SmbClientConfiguration -AuditServerDoesNotSupportEncryption $true
Set-SmbClientConfiguration -AuditServerDoesNotSupportSigning $true
```

これらの変更のイベント ログは、特定のイベント ID を持つ次のイベント ビューアー パスに格納されます。

テーブルを展開する

Path	イベント ID
アプリケーションとサービス ログ\Microsoft\Windows\SMBClient\Audit	31998 31999
アプリケーションとサービス ログ\Microsoft\Windows\SMBServer\Audit	3021 3022

SMB over QUIC 監査

SMB over QUIC クライアント接続監査では、QUIC トランスポートをイベント ビューアーに含めるためにイベント ログに書き込まれたイベントがキャプチャされます。 これらのログは、特定のイベント ID を持つ次のパスに格納されます。

テーブルを展開する

Path	イベント ID
アプリケーションとサービス ログ\Microsoft\Windows\SMBClient\Connectivity	30832
Applications and Services Logs\Microsoft\Windows\SMBServer\Connectivity （アプリケーションとサービスログ\マイクロソフト\ウィンドウズ\SMBサーバー\接続）	1913

SMB over QUIC のクライアントアクセス制御

Windows Server 2025 には、SMB over QUIC のクライアント アクセス制御が含まれています。 SMB over QUIC は、信頼されていないネットワーク経由でエッジ ファイル サーバーにセキュリティで保護された接続を提供する TCP および RDMA の代替手段です。 クライアント アクセス制御では、証明書を使用してデータへのアクセスを制限するためのより多くの制御が導入されています。 詳細については、 「クライアント アクセス制御のしくみ」を参照してください。

SMB 代替ポート

SMB クライアントを使用して、IANA/IETF の既定値である 445、5445、443 ではなく、代替 TCP、QUIC、RDMA ポートに接続できます。 グループ ポリシーまたは PowerShell を使用して、代替ポートを構成できます。 以前は、Windows の SMB サーバーは、IANA に登録されたポート TCP/445 を使用する受信接続を要求し、SMB TCP クライアントは同じ TCP ポートへの送信接続のみを許可しました。 現在、SMB over QUIC では、QUIC で義務付けられている UDP/443 ポートをサーバー デバイスとクライアント デバイスの両方で使用できる、 SMB 代替ポート を使用できます。 詳細については、 「代替 SMB ポートの構成」を参照してください。

SMB ファイアウォール規則のセキュリティ強化

以前は、共有が作成されたときに、関連するファイアウォール プロファイルの **ファイルとプリンター共有** グループを有効にするように SMB ファイアウォール規則が自動的に構成されていました。 Windows で SMB 共有を作成すると、新しい **ファイルおよびプリンター共有 (制限付き)** グループが自動的に構成され、受信 NetBIOS ポート 137 から 139 が許可されなくなります。 詳細については、 「更新したファイアウォール規則」を参照してください。

SMB 暗号化

SMB 暗号化を適用 は、すべての送信 SMB クライアント接続に対して有効になります。 この更新により、管理者は、すべての接続先サーバーが SMB 3.x と暗号化をサポートすることを

義務付けることができます。 サーバーにこれらの機能がない場合、クライアントは接続を確立できません。

SMB 認証制限装置

SMB 認証レートリミッターは、特定の期間内の認証試行回数を制限します。 SMB 認証レートリミッターは、ブルート フォース認証攻撃に対処するのに役立ちます。 SMB サーバーのサービスは、認証レートリミッターを使用して、失敗した NTLM または PKU2U ベースの認証試行間の遅延を実装します。 サービスは既定で有効になっています。 詳細については、「 SMB 認証レートリミッターのしくみを参照してください。

SMB NTLM を無効にする

Windows Server 2025 以降、SMB クライアントはリモート送信接続の NTLM ブロックをサポートしています。 以前は、Windows Simple and Protected GSSAPI ネゴシエーション メカニズム (SPNEGO) は、Kerberos、NTLM、およびその他のメカニズムを移行先サーバーとネゴシエートして、サポートされているセキュリティ パッケージを決定しました。 詳細については、「SMB での NTLM 接続のブロックを参照してください。

SMB 言語制御

Windows で SMB ダイアレクトを管理できるようになりました。 構成すると、SMB サーバーは、従来の動作と比較して交渉する SMB 2 および SMB 3 のプロトコルを決定し、最も高いプロトコルのみ対応します。

SMB 署名

すべての SMB 送信接続に対して、SMB 署名が既定で必要になりました。 以前は、Active Directory DC 上の SYSVOL と NETLOGON 名前の共有に接続している場合にのみ必要でした。 詳しくは、「署名のしくみ」を参照してください。

リモートメールスロット

リモート Mailslot プロトコルは、SMB と ACTIVE Directory で DC ロケーター プロトコルを使用する場合、既定で無効になっています。 リモート Mailslot は、後のリリースで削除される可能性があります。 詳細については、「機能の削除または Windows Serverで開発されなくなった機能」を参照してください。

ルーティングとリモート アクセス サービスのセキュリティ強化

既定では、新しいルーティングおよびリモート アクセス サービス (RRAS) のインストールでは、PPTP と L2TP に基づく VPN 接続は受け入れられません。 必要に応じて、これらのプロトコルを有効にすることもできます。 SSTP と IKEv2 に基づく VPN 接続は、変更なしで引き続き受け入れられます。

既存の構成はそのまま動作します。 たとえば、Windows Server 2019 を実行して PPTP 接続と L2TP 接続を受け入れ、インプレース アップグレードを使用して Windows Server 2025 にアップグレードする場合、L2TP と PPTP に基づく接続は引き続き受け入れられます。 この変更は、Windows クライアント オペレーティング システムには影響しません。 PPTP と L2TP を再び使用可能にする方法の詳細については、「VPN プロトコルを構成する」を参照してください。

IPsec の既定のキー設定プロトコルの変更

マシン証明書で認証された IPsec 接続では、既定のキー モジュールが IKEv1 および IKEv2 に変更されました。 その他の認証方法では、既定の AuthIP と IKEv1 が残ります。 これは、Windows Server 2025 クライアントと Windows 11 24H2 クライアントの両方に適用されます。 レジストリ パス `HKLM:\SYSTEM\CurrentControlSet\Services\MpsSvc\Parameters` では、値が **0 の** `IpsecRestoreLegacyKeyMod` **エントリ** は、新しいシーケンス IKEv2 と IKEv1 を利用します。 値 **1** は、前のシーケンスである AuthIP と IKEv1 を利用します。 以前の動作に戻すには、新しい既定のキー設定プロトコル シーケンスを使用して、システムに次のレジストリ キーを追加します。 変更を有効にするには、再起動が必要です。

PowerShell

```powershell
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\MpsSvc\Parameters"
-Name "IpsecRestoreLegacyKeyMod" -PropertyType "DWORD" -Value 1
```

Hyper-V、AI、およびパフォーマンス

以降のセクションでは、Hyper-V、AI、およびパフォーマンスについて説明します。

高速ネットワーク (プレビュー)

高速ネットワーク (AccelNet) を使用すると、Windows Server 2025 クラスターでホストされている仮想マシン (VM) の単一ルート I/O 仮想化 (SR-IOV) の管理が簡略化されます。 この機能では、高パフォーマンスの SR-IOV データ パスを使用して、待機時間、ジッター、および CPU 使用率を削減します。 AccelNet には、前提条件のチェック、ホスト構成、および VM のパフォーマンス設定を処理する管理レイヤーも含まれています。 詳細については、「高速ネットワーク (プレビュー) を参照してください。

動的プロセッサの互換性

動的プロセッサ互換性モードが更新され、クラスター化された環境で新しいプロセッサ機能が利用されます。 動的プロセッサの互換性では、クラスター内のすべてのサーバーで使用可能なプロセッサ機能の最大数が使用されます。 このモードでは、以前のバージョンのプロセッサ互換性と比較してパフォーマンスが向上します。

動的プロセッサの互換性を使用して、さまざまな世代のプロセッサを使用する仮想化ホスト間でその状態を保存することもできます。 プロセッサ互換モードでは、第 2 レベルのアドレス変換が可能なプロセッサで強化された動的機能が提供されるようになりました。 更新された互換モードの詳細については、「 Hyper-V 仮想マシンのプロセッサの互換性」を参照してください。

Hyper-V マネージャー

Hyper-V Manager を使用して新しい VM を作成すると、**第 2 世代** が、**仮想マシンの新規作成ウィザード**の既定のオプションとして設定されるようになりました。

ハイパーバイザーによって強制されるページング変換

ハイパーバイザーによって適用されるページング変換 (HVPT) は、線形アドレス変換の整合性を適用するためのセキュリティ強化です。 HVPT は、重要なシステム データを書き込み先攻撃から保護します。攻撃者は、バッファー オーバーフローの結果として、任意の場所に任意の値を書き込みます。 HVPT は、重要なシステム データ構造を構成するページ テーブルを保護します。 HVPT には、ハイパーバイザーで保護されたコード整合性 (HVCI) で既に保護されているすべてが含まれています。 HVPT は既定で有効になっており、ハードウェア サポートを利用できます。 WINDOWS Server が VM でゲストとして実行されている場合、HVPT は有効になりません。

GPU パーティション分割

GPU パーティション分割を使用して、物理 GPU デバイスを複数の VM と共有できます。 GPU 全体を 1 つの VM に割り当てる代わりに、GPU パーティション分割 (GPU-P) によって各 VM に GPU の専用の一部が割り当てられます。 Hyper-V GPU-P の高可用性により、計画外のダウンタイムが発生した場合、GPU-P VM が別のクラスター ノードで自動的に有効化されます。

GPU-P ライブ マイグレーションは、GPU-P を使用して VM を (計画されたダウンタイムまたは負荷分散のために) スタンドアロンまたはクラスター化された別のノードに移動するソリューションを提供します。 GPU パーティション分割の詳細については、GPU パーティション分割を参照してください。

ネットワーク ATC

ネットワーク ATC は、Windows Server 2025 クラスターのネットワーク構成の展開と管理を効率化します。 ネットワーク ATC では、意図ベースのアプローチを使用します。ユーザーは、ネットワーク アダプターの管理、コンピューティング、ストレージなど、目的の意図を指定します。 デプロイは、目的の構成に基づいて自動化されます。

この方法により、ホスト ネットワークの展開に関連する時間、複雑さ、およびエラーが軽減されます。 これにより、クラスター全体の構成の一貫性が確保され、構成のずれも排除されます。 詳細については、「 ネットワーク ATC を使用したホスト ネットワークのデプロイを参照してください。

Scalability

Windows Server 2025 では、Hyper-V はホストあたり最大 4 ペタバイトのメモリと 2,048 個の論理プロセッサをサポートするようになりました。 この増加により、仮想化されたワークロードのスケーラビリティとパフォーマンスが向上します。

Windows Server 2025 では、第 2 世代 VM に対して最大 240 TB のメモリと 2,048 個の仮想プロセッサもサポートされており、大規模なワークロードを実行するための柔軟性が向上しています。 詳細については、「 Plan for Hyper-V scalability in Windows Server」を参照してください。

ワークグループ クラスター

Hyper-V ワークグループ クラスターは、Hyper-V クラスター ノードがワークグループ クラスター内の VM をライブ マイグレーションする機能を持つ Active Directory ドメインのメンバーではない特殊な種類の Windows Server フェールオーバー クラスターです。

Storage

次のセクションでは、ストレージの更新について説明します。

ブロッククローンのサポート

開発ドライブでは、Windows 11 24H2 および Windows Server 2025 以降のブロック複製がサポートされるようになりました。 開発ドライブでは Resilient File System (ReFS) 形式が使用されるため、ブロック複製のサポートにより、ファイルをコピーするときにパフォーマンス上の大きな利点が得られます。 ブロック複製を使用すると、ファイル システムは、基になる物理データに対して負荷の高い読み取りと書き込みの操作を実行するのではなく、低コストのメタデータ操作としてアプリケーションのファイル バイトの範囲をコピーできます。

その結果、複数のファイルが同じ論理クラスターを共有できるようにすることで、ファイルのコピーの完了が高速化され、基になるストレージへの I/O が削減され、ストレージ容量が向上します。 詳細については、「ReFS でのブロッククローン作成」を参照してください。

開発用ドライブ

Dev Drive は、重要な開発者ワークロードのパフォーマンスを向上させることを目的としたストレージ ボリュームです。 Dev Drive は ReFS テクノロジを使用し、特定のファイル システムの最適化を組み込んで、ストレージ ボリュームの設定とセキュリティをより細かく制御します。 管理者は、信頼を指定し、ウイルス対策設定を構成し、アタッチされたフィルターに対する管理制御を実行できるようになりました。 詳細については、「Windows 11 で Dev Drive をセットアップする」を参照してください。

NVMe

NVMe は、高速ソリッドステート ドライブの新しい標準です。 NVMe ストレージのパフォーマンスは、Windows Server 2025 で最適化されています。 その結果、IOPS が増加し、CPU 使用率が低下してパフォーマンスが向上します。

記憶域レプリカの圧縮

記憶域レプリカの圧縮により、レプリケーション中にネットワーク経由で転送されるデータの量が減ります。 記憶域レプリカでの圧縮の詳細については、「記憶域レプリカの概要参照してください。

記憶域レプリカ拡張ログ

記憶域レプリカ拡張ログは、ログの実装に役立ち、ファイル システムの抽象化に関連するパフォーマンス コストを排除します。 ブロック レプリケーションのパフォーマンスが向上しました。 詳細については、「記憶域レプリカ拡張ログ」を参照してください。

ReFS ネイティブ ストレージの重複除去と圧縮

ReFS ネイティブ ストレージ重複除去と圧縮は、ファイル サーバーや仮想デスクトップなどの静的ワークロードとアクティブ ワークロードの両方のストレージ効率を最適化するために使用される手法です。 ReFS 重複除去と圧縮の詳細については、「Azure Localでの ReFS 重複除去と圧縮によるストレージの最適化」を参照してください。

シン プロビジョニング ボリューム

記憶域スペース ダイレクトでプロビジョニングされたシン ボリュームは、クラスターで必要な場合にのみプールから割り当てることで、記憶域リソースをより効率的に割り当て、コストの高い割り当てを回避する方法です。 固定ボリュームからシン プロビジョニング ボリュームに変換することもできます。 固定ボリュームからシン プロビジョニング ボリュームに変換すると、未使用の記憶域がプールに戻され、他のボリュームで使用できるようになります。 シン プロビジョニング ボリュームの詳細については、「ストレージのシン プロビジョニング」を参照してください。

サーバー メッセージ ブロック

サーバー メッセージ ブロック (SMB) は、ネットワークで最も広く使用されているプロトコルの 1 つです。 SMB は、ネットワーク上のデバイス間でファイルやその他のリソースを共有する信頼性の高い方法を提供します。 Windows Server 2025 には、業界標準の LZ4 圧縮アルゴリズムの SMB 圧縮サポートが含まれています。 LZ4 は、SMB の XPRESS (LZ77)、XPRESS Huffman (LZ77+Huffman)、LZNT1、およびPATTERN_V1の既存のサポートに加えて提供されています。

Azure Arc とハイブリッド

以降のセクションでは、Azure Arc とハイブリッドの構成について説明します。

簡略化された Azure Arc セットアップ

Azure Arc セットアップはオンデマンド機能であるため、既定でインストールされます。 ユーザー フレンドリなウィザード インターフェイスとタスク バーのシステム トレイ アイコンは、Azure Arc にサーバーを追加するプロセスを容易にするのに役立ちます。Azure Arc は、さまざまな環境で動作できるアプリケーションとサービスを作成できるように、Azure プラットフォームの機能を拡張します。 これらの環境には、データセンター、エッジ、マルチクラウド環境が含まれており、柔軟性が向上します。 詳細については、「Azure Arc セットアップを使用して Windows Server マシンを Azure に接続する」を参照してください。

従量課金制ライセンス

Azure Arc 従量課金制サブスクリプション ライセンス オプションは、Windows Server 2025 の従来の永続的ライセンスの代替手段です。 従量課金制オプションを使用すると、Windows Server デバイスを展開し、ライセンスを取得し、使用した分だけ支払うことができます。 この機能は Azure Arc を通じて容易になり、Azure サブスクリプション経由で課金されます。 詳細については、Azure Arc の従量課金制ライセンスを参照してください。

Azure Arc で有効化される Windows Server 管理

Azure Arc で有効になっている Windows Server Management は、アクティブなソフトウェア アシュアランスを持つ Windows Server ライセンスまたはアクティブなサブスクリプション ライセンスである Windows Server ライセンスを持つお客様に新しい利点を提供します。 Windows Server 2025 には、次の主な利点があります。

- **Azure Arcの** Windows Admin Center: Azure Arc と Windows Admin Center を統合して、Azure Arc ポータルから Windows Server インスタンスを管理できるようにします。 この統合により、Windows Server インスタンスがオンプレミス、クラウド、エッジのいずれで実行されているかに関係なく、統合された管理エクスペリエンスが提供されます。
- **リモート サポート**: プロフェッショナル サポートをお持ちのお客様に、詳細な実行トランスクリプトと失効権限を持つ Just-In-Time アクセスを許可する機能を提供します。
- **ベスト プラクティス評価**: サーバー データの収集と分析により、問題が発生し、修復ガイダンスとパフォーマンスが向上します。
- **Azure Site Recovery 構成**: Azure Site Recovery の構成により、ビジネス継続性が確保され、重要なワークロードのレプリケーションとデータの回復性が提供されます。

Azure Arc で有効になっている Windows Server Management と利用可能な利点の詳細については、「 Windows Server Management enabled by Azure Arc」を参照してください。

ソフトウェアによるネットワーク制御

Software-Defined ネットワーク (SDN) は、ネットワーク管理者が下位レベルの機能を抽象化してネットワーク サービスを管理するために使用できるネットワークへのアプローチです。 SDN を使用すると、ネットワークを管理するネットワーク コントロール プレーンを、トラフィックを処理するデータ プレーンから分離できます。 この分離により、ネットワーク管理における柔軟性とプログラミング性が向上します。 SDN には、Windows Server 2025 で次の利点があります。

- **ネットワーク コントローラーの**: SDN のこのコントロール プレーンは、物理ホスト マシン上のフェールオーバー クラスター サービスとして直接ホストされるようになりました。 クラスター ロールを使用すると、VM をデプロイする必要がなくなります。これにより、デプロイと管理が簡素化され、リソースが節約されます。
- **タグベースのセグメント化**: 管理者は、カスタム サービス タグを使用して、アクセス制御のためにネットワーク セキュリティ グループ (NSG) と VM を関連付けることができます。 管理者は、IP 範囲を指定する代わりに、シンプルでわかりやすいラベルを使用してワークロード VM にタグを付け、これらのタグに基づいてセキュリティ ポリシーを適用できるようになりました。 タグを使用すると、ネットワーク セキュリティを管理するプロセスが簡素化され、IP 範囲を記憶して再入力する必要がなくなります。 詳細については、「 Windows Admin Center でタグを使用してネットワーク セキュリティ グループを構成するを参照してください。

- **Windows Server 2025**の既定のネットワーク ポリシー: これらのポリシーは、Windows Admin Center を介してデプロイされたワークロードの NSG に Azure に似た保護オプションをもたらします。 既定のポリシーでは、すべての受信アクセスが拒否され、ワークロード VM からの完全な送信アクセスを許可しながら、既知の受信ポートを選択的に開きます。 既定のネットワーク ポリシーにより、ワークロード VM が作成時点からセキュリティで保護されます。 詳細については、「Azure Local 上の仮想マシンで既定のネットワーク アクセス ポリシーを使用する」を参照してください。
- **SDN マルチサイト**: この機能により、2 つの場所にまたがるアプリケーション間のネイティブ レイヤー 2 とレイヤー 3 の接続が、追加のコンポーネントなしで提供されます。 SDN マルチサイトを使用すると、アプリケーションまたはネットワークを再構成しなくても、アプリケーションをシームレスに移動できます。 また、ワークロード VM が別の場所に移動したときにポリシーを更新する必要がないように、ワークロードの統合されたネットワーク ポリシー管理も提供されます。 詳細については、「SDN マルチサイトとは」を参照してください。
- **SDN レイヤー 3 ゲートウェイのパフォーマンスが向上**: レイヤー 3 ゲートウェイは、より高いスループットと CPU サイクルの削減を実現します。 これらの機能強化は、既定で有効になっています。 ユーザーは、PowerShell または Windows Admin Center を使用して SDN ゲートウェイ レイヤー 3 接続を構成すると、パフォーマンスが自動的に向上します。

Windows コンテナーの移植性

移植性はコンテナー管理の重要な側面であり、Windows でコンテナーの柔軟性と互換性を強化することでアップグレードを簡略化する機能を備えます。

移植性は、ユーザーがコンテナー イメージとそれに関連するデータを、変更を必要とせずに異なるホストまたは環境間で移動するために使用できる Windows Server 機能です。 ユーザーは、互換性の問題を気にすることなく、1 つのホストにコンテナー イメージを作成し、別のホストにデプロイできます。 詳細については、「コンテナーの移植性」を参照してください。

Windows Server Insider Program

Windows Server Insider Program は、愛好家のコミュニティ向けに最新の Windows OS リリースへの早期アクセスを提供します。 メンバーとして、Microsoft が開発している新しいアイデアや概念を最初に試すことができます。 メンバーとして登録すると、さまざまなリリース チャネルに参加できます。 **スタート**>**設定**>**Windows Update**>**Windows Insider Program**に移動します。

関連コンテンツ

Windows Server Insider Community のディスカッション

Last updated on 2026/01/15

Windows Server 2022 の新機能

2025/07/21適用対象: ✅ Windows Server 2022

この記事では、Windows Server 2022 の新機能の一部について説明します。 Windows Server 2022 は、Windows Server 2019 の強力な基盤上に構築されており、セキュリティ、Azure ハイブリッド統合と管理、アプリケーション プラットフォームという 3 つの重要なテーマに多くのイノベーションをもたらします。

Azure Edition

Windows Server 2022 Datacenter: Azure Edition は、ダウンタイムを最小限に抑えながら、クラウドの利点を使用して VM を最新の状態に保つのに役立ちます。 このセクションでは、Windows Server 2022 Datacenter: Azure Edition の新機能についていくつか説明します。 Windows Server 用 Azure Automanage がこれらの新機能を Windows Server Azure Edition に提供する方法の詳細については、「Windows Server 用 Azure Automanage」の記事を参照してください。

Windows Server 2022 Datacenter: Azure Edition は Datacenter Edition 上に構築されており、クラウドの利点を利用するのに役立つ VM 専用オペレーティング システムを提供します。このオペレーティング システムは、SMB over QUIC、Hotpatch、Azure Extended Networking などの高度な機能を備えています。 このセクションでは、これらの新機能についていくつか説明します。

Windows Server 2022 のエディションの違いを比較します。 Windows Server 用 Azure Automanage がこれらの新機能を Windows Server Azure Edition に提供する方法の詳細については、「Windows Server 用 Azure Automanage」の記事でも確認できます。

2023 年 4 月

ホットパッチ

Windows Server 2022 Datacenter: Azure Edition Hotpatch は、Azure と Azure Local バージョン 22H2 でサポートされているゲスト VM の両方で、デスクトップ エクスペリエンスのパブリック プレビューになりました。

2022 年 9 月 9 日

このセクションでは、x64 ベースのシステム (KB5017381) 用の Microsoft サーバー オペレーティング システム バージョン 21H2 の 2022-09 の累積的な更新プログラム以降、Windows Server Datacenter: Azure Edition で利用できるようになった機能と機能強化について説明しま

す。 累積的な更新プログラムをインストールすると、OS ビルド番号は 20348.1070 以上になります。

データ転送用の記憶域レプリカ圧縮

この更新には、転送元サーバーと転送先サーバー間で転送されるデータの記憶域レプリカ圧縮機能が含まれています。 この新しい機能により、転送元システムでレプリケーション データが圧縮され、ネットワーク経由で送信され、転送先で圧縮が解除されて保存されます。 圧縮の結果、同じ量のデータを転送するネットワーク パケットが少なくなり、スループットが向上し、ネットワーク使用率が低下します。 また、データスループットを高くすると、ディザスター リカバリー シナリオなど、最も必要な同期時間が短縮されます。

新しい記憶域レプリカ PowerShell パラメーターは、既存のコマンドで使用できます。 詳細については、 StorageReplica PowerShell リファレンスを確認してください。 記憶域レプリカの詳細については、「記憶域レプリカの概要」を参照してください。

Azure Local のサポート

このリリースでは、サポートされているゲスト VM として Windows Server 2022 Datacenter: Azure Edition を Azure Local バージョン 22H2 で実行できます。 Azure Local で Azure Edition を実行すると、データセンターとエッジの場所で、Server Core 用 ホットパッチ や QUIC 経由の SMB など、既存のすべての機能を使用できるようになります。

Arc 対応 Azure Local (プレビュー) 上の Azure Marketplace からのデプロイを使用するか、ISO を使用して、Windows Server 2022 Datacenter: Azure Edition のデプロイを開始します。 ISO は、こちらからダウンロードできます。

- Windows Server 2022 Datacenter: Azure Edition (EN-US) ISO
- Windows Server 2022 Datacenter: Azure Edition (ZH-CN) ISO

お使いの Azure サブスクリプションから、Azure Local で動作する任意の仮想マシン インスタンス上の Windows Server Datacenter: Azure エディションを使用できます。 詳細については、 製品の使用条件 を参照してください。

Azure Local バージョン 22H2 の新機能に関するページで、最新の Azure Local 機能について説明します。

Arc 対応 Azure Local (プレビュー) の Azure Marketplace からデプロイする

Windows Server 2022 Datacenter: Azure Edition イメージは、Arc 対応 Azure Local の Azure Marketplace で利用できるようになり、容易に Azure 認定イメージを使用した試用、購入、デ

プロイを実行できます。

Azure Arc 対応 Azure Local 機能の Azure Marketplace 統合の詳細については、 Azure Local の新機能に 関する記事を参照してください。

Azure Edition (初期リリース)

このセクションには、Windows Server Datacenter: Azure Edition の 2021 年 9 月のリリースで利用できる機能と機能強化の一覧を示します。

Azure Automanage - ホットパッチ

Azure Automanage の一部であるホットパッチは、インストール後に再起動を必要としない新しい Windows Server Azure Edition 仮想マシン (VM) に更新プログラムをインストールする新しい方法です。 詳細については、「 Windows Server のホットパッチ」を参照してください。

SMB over QUIC (ネットワークプロトコル)

SMB over QUIC は、WINDOWS Server 2022 Datacenter の TCP ではなく、SMB 3.1.1 プロトコル (Azure Edition、Windows 11 以降、およびサポートされている場合はサード パーティ クライアント) を使用するように SMB 3.1.1 プロトコルを更新します。 TLS 1.3 と共に SMB over QUIC を使用することで、ユーザーとアプリケーションが Azure で実行されているエッジ ファイル サーバーからデータに安全かつ確実にアクセスできます。 在宅勤務者とモバイルのユーザーは、Windows を使用している場合に、SMB 経由でファイル サーバーにアクセスするために VPN が不要となりました。 詳細については、「AUTOmanage マシンのベスト プラクティスを使用した QUIC 経由の SMB および SMB over QUIC 管理」を参照してください。

QUIC の詳細については、 RFC 9000 を参照してください。

Azure の拡張ネットワーク

Azure 拡張ネットワークを使用すると、オンプレミスのサブネットを Azure に拡張して、Azure に移行するときに、オンプレミスの仮想マシンが元のオンプレミスのプライベート IP アドレスを保持できるようにします。 詳細については、Azure 拡張ネットワークに関するページを参照してください。

全エディション

このセクションでは、すべてのエディションの Windows Server 2022 の新機能についていくつか説明します。 さまざまなエディションの詳細については、「 Windows Server エディションの比較」を参照してください。

セキュリティ

Windows Server 2022 の新しいセキュリティ機能は、Windows Server の他のセキュリティ機能を複数の領域にまたがって統合して、高度な脅威に対する多層防御を実現します。 Windows Server 2022 の高度な多層セキュリティにより、サーバーに現在必要な包括的な保護が提供されます。

セキュア コア サーバー

OEM パートナーが提供する認定セキュアコア サーバー ハードウェアには、高度な攻撃に対して役に立つセキュリティ保護機能がその他にもあります。 認定済みのセキュリティで保護されたコア サーバー ハードウェアは、最も機密性の高い一部の業界でミッション クリティカルなデータを処理する際に、より高い保証を提供できます。 高度な Windows Server セキュリティ機能を実現するために、セキュアコア サーバーにはハードウェア、ファームウェア、ドライバーの機能が使用されています。 これらの機能の多くは Windows セキュアコア PC に搭載されていますが、セキュアコア サーバー ハードウェアと Windows Server 2022 でも使用できるようになりました。 詳細については、「 セキュリティで保護されたコア サーバー」を参照してください。

ハードウェアの信頼のルート

BitLocker ドライブ暗号化などの機能から使われるトラステッド プラットフォーム モジュール 2.0 (TPM 2.0) セキュア暗号化プロセッサ チップには、システム整合性の測定を含め、機密性の高い暗号化キーとデータに対応するセキュリティで保護されたハードウェアベースのストアが用意されています。 TPM 2.0 を使用すると、サーバーが正当なコードで起動され、後続のコード実行 (ハードウェアの信頼のルートとも呼ばれる) によって信頼できることを確認できます。

ファームウェアの保護

ファームウェアは高い特権で実行され、多くの場合、従来のウイルス対策ソリューションからは見えません。 これにより、ファームウェアベースの攻撃の数が増加しています。 セキュアコア サーバーで Dynamic Root of Trust for Measurement (DRTM) テクノロジを使って起動プロセスを測定および確認することができます。 セキュリティで保護されたコア サーバーは、 ダイレクト メモリ アクセス (DMA) 保護を使用して、メモリへのドライバー アクセスを分離することもできます。

UEFI セキュア ブート

UEFI セキュア ブート は、悪意のあるルートキットからサーバーを守るセキュリティ標準です。 セキュア ブートにより、ハードウェアの製造元によって信頼されているファームウェア

とソフトウェアのみがサーバーで起動されます。 サーバーが起動すると、ファームウェアはファームウェア ドライバーや OS を含む各ブート コンポーネントの署名を確認します。 署名が有効な場合、サーバーが起動し、ファームウェアによって OS に制御が渡されます。

仮想化ベースのセキュリティ (VBS)

セキュアコア サーバーは、仮想化ベースのセキュリティ (VBS) とハイパーバイザーベースのコード整合性 (HVCI) をサポートしています。 メモリのセキュリティで保護された領域を作成し、通常のオペレーティング システムから隔離するために、VBS にはハードウェア仮想化機能が使用されています。これにより、暗号通貨マイニング攻撃に使用される全クラスの脆弱性から保護されます。 また、VBS に Credential Guard を使用して、オペレーティング システムから直接アクセスできない仮想コンテナーにユーザーの資格情報とシークレット情報を格納することもできます。

HVCI では VBS を使って、コードの整合性ポリシーの適用を大幅に強化することができます。カーネル モードの整合性により、署名されていないカーネル モード ドライバーまたはシステム ファイルがシステム メモリに読み込まれるのを防ぐことができます。

カーネル データ保護 (KDP) には、メモリ ページがハイパーバイザーによって保護される実行不可能なデータを含むカーネル メモリの読み取り専用メモリ保護が備わっています。 KDP は、Windows Defender System Guard ランタイムのキー構造が改ざんされないように保護します。

セキュリティで保護された接続

トランスポート: Windows Serer 2022 で既定で有効になっている HTTPS と TLS 1.3

セキュリティで保護された接続は、現在の相互接続システムの中核です。 トランスポート層セキュリティ (TLS) 1.3 は、最も採用されているインターネットのセキュリティ プロトコルの最新バージョンです。これは、データを暗号化して、2 つのエンドポイント間にセキュリティで保護された通信チャネルを提供します。 HTTPS と TLS 1.3 は Windows Server 2022 では既定で有効になり、サーバーに接続するクライアントのデータを保護します。 これにより、廃止された暗号アルゴリズムが排除され、以前のバージョンよりもセキュリティが強化され、できるだけ多くのハンドシェイクの暗号化が目標とされています。 サポートされている TLS のバージョンとサポートされている暗号スイートについて詳細を確認してください。

プロトコル レイヤーの TLS 1.3 は既定で有効になりましたが、アプリケーションとサービスでもそれをアクティブにサポートする必要があります。 Microsoft Security ブログの投稿「TLS 1.3 を使用してトランスポート層セキュリティ (TLS) を次のレベルへ」 にも、詳細が記載されています。

セキュリティで保護された DNS: DNS-over-HTTPS で暗号化された DNS 名前解決要求

Windows Server 2022 の DNS クライアントでは、HTTPS プロトコルを使用して DNS クエリを暗号化する DNS over-HTTPS (DoH) がサポートされるようになりました。 DoH は、傍受や DNS データの操作を防ぐことで、トラフィックを可能な限りプライベートに保つのに役立ちます。 DoH を使用するように DNS クライアントを構成する方法について詳細を確認してください。

サーバー メッセージ ブロック (SMB): セキュリティを最も重視する場合の SMB AES-256 暗号化

Windows Server は、SMB の暗号化に AES-256-GCM と AES-256-CCM の暗号化スイートをサポートするようになりました。 Windows では、サポートされている別のコンピューターに接続するときに、より高度な暗号方法が自動的にネゴシエートされます。また、グループ ポリシーを使用して要求することもできます。 Windows Server は、下位互換性のために AES-128 を引き続きサポートしています。 また、AES-128-GMAC の署名により、署名のパフォーマンスが向上しました。

SMB: クラスター内通信のための東西間 SMB 暗号化制御

Windows Server フェールオーバー クラスターでは、クラスターの共有ボリューム (CSV) と記憶域バス層 (SBL) のノード内記憶域通信の暗号化と署名のきめ細かい制御がサポートされるようになりました。 記憶域スペース ダイレクトを使用する場合、より高いセキュリティのために、クラスター自体の中で東西の通信を暗号化または署名することを決定できるようになりました。

SMB ダイレクトと RDMA の暗号化

SMB ダイレクトと RDMA は、記憶域スペース ダイレクト、記憶域レプリカ、Hyper-V、Scale-Out ファイル サーバー、SQL Server などのワークロードに対して、高帯域幅で待機時間の短いネットワーク ファブリックを提供します。 Windows Server 2022 の SMB ダイレクトでは、暗号化がサポートされています。 以前は、SMB 暗号化を有効にすると、直接データの配置が無効になりました。 これは意図的なものでしたが、パフォーマンスに深刻な影響を与えました。 現在は、データはデータ配置前に暗号化されるため、パフォーマンスの低下ははるかに少なくなり、さらに AES-128 と AES-256 で保護されたパケットのプライバシーが追加されました。

SMB 暗号化、署名高速化、セキュリティで保護された RDMA、クラスターのサポートの詳細については、「 SMB セキュリティの強化」を参照してください。

Azure ハイブリッドの機能

Windows Server 2022 の組み込みのハイブリッド機能を使用すると、これまで以上に簡単にデータセンターを Azure に拡張できるため、効率と機敏性を向上させることができます。

Azure Arc 対応 Windows サーバー

Windows Server 2022 を使用する Azure Arc 対応サーバーは、Azure Arc を使用してオンプレミスおよびマルチクラウドの Windows Server を Azure に導入します。この管理エクスペリエンスは、ネイティブ Azure 仮想マシンの管理方法と一致するように設計されています。 ハイブリッド マシンは、Azure に接続されると接続済みマシンになり、Azure 内のリソースとして扱われます。 詳細については、 Azure Arc 対応サーバーのドキュメントを参照してください。

Windows Server マシンを追加する

KB5031364 更新プログラムの時点で、簡単なプロセスで Windows Server マシンを追加できます。

新しい Windows Server マシンを追加するには、タスク バーの右下隅にある Azure Arc アイコンに移動し、Azure Arc セットアップ プログラムを起動して、Azure 接続マシン エージェントをインストールして構成します。 インストール後、Azure アカウントに対して追加料金なしで Azure 接続マシン エージェントを使用できます。 サーバーで Azure Arc を有効にすると、タスク バー アイコンに状態情報が表示されます。

詳細については、「Azure Arc セットアップを使用して Windows Server マシンを Azure に接続する」を参照してください。

Windows Admin Center

Windows Server 2022 を管理するための Windows Admin Center の機能強化には、前述のセキュリティで保護されたコア機能の現在の状態を報告する機能や、該当する場合は機能を有効にするための機能が含まれます。 これらの詳細と Windows Admin Center のその他の機能強化については、 Windows Admin Center のドキュメントを参照してください。

アプリケーション プラットフォーム

アプリケーションの互換性や Kubernetes での Windows コンテナー エクスペリエンスなど、Windows コンテナーのプラットフォームの改善がいくつかあります。

新機能の一部を次に示します。

- Windows コンテナー イメージのサイズが最大 40%削減され、起動時間が 30% 短縮され、パフォーマンスが向上します。
- アプリケーションは、 コンテナー ホストにドメイン参加せずに、グループ管理サービス アカウント (gMSA) で Microsoft Entra ID を使用できるようになりました。 Windows コンテナーでは、Microsoft 分散トランザクション コーディネーター (DTC) と Microsoft メッセージ キュー (MSMQ) もサポートされるようになりました。
- プロセス分離された Windows Server のコンテナーに単純なバスを割り当てることができるようになりました。 SPI、I2C、GPIO、および UART/COM 経由で通信する必要があるコンテナーで実行されているアプリケーションで、これを実行できるようになりました。
- ローカル グラフィカル処理装置 (GPU) ハードウェアを使用した機械学習推論などのシナリオをサポートするために、Windows コンテナーでの DirectX API のハードウェア アクセラレーションのサポートを有効にしました。 詳細については、Windows コンテナーへの GPU アクセラレータの導入 に関するブログ記事を参照してください。
- Kubernetes での Windows コンテナー エクスペリエンスを簡略化するその他のいくつかの機能強化があります。 これらの機能強化には、ノード構成のホストプロセス コンテナー、IPv6、Calico による一貫したネットワーク ポリシーの実装の各サポートが含まれます。
- Windows Admin Center が更新され、.NET アプリケーションを容易にコンテナー化できるようになります。 アプリケーションがコンテナー内に配置されたら、それを Azure Container Registry でホストし、Azure Kubernetes Service などの他の Azure サービスにデプロイできます。
- Intel Ice Lake プロセッサのサポートを備えた Windows Server 2022 では、ビジネスに不可欠で大規模なアプリケーションがサポートされます。これには、64 個の物理ソケットで実行される最大 48 TB のメモリと 2,048 論理コアが必要です。 Intel Ice Lake 上の Intel Secured Guard Extension (SGX) を使用した機密性の高いコンピューティングは、保護されたメモリを使用してアプリケーションを相互に分離することによって、アプリケーションのセキュリティを強化します。

その他の主な機能

リモート デスクトップ IP 仮想化

KB5030216 更新プログラムの時点で、リモート デスクトップ IP 仮想化を使用できます。

リモート デスクトップ IP 仮想化は、Winsock アプリケーションのセッションごとおよびプログラムごとのリモート デスクトップ IP 仮想化をサポートすることで、シングル ユーザー デ

スクトップをシミュレートします。 詳細については、「Windows Server でのリモート デスクトップ IP 仮想化」を参照してください。

Server Core インストールのためのタスク スケジューラと Hyper-V マネージャー

このバージョンのアプリ互換性機能オンデマンド機能パッケージに、タスク スケジューラ (taskschd.msc) と Hyper-V Manager (virtmgmt.msc) の 2 つの管理ツールを追加しました。 詳細については、「Server Core アプリ互換性オンデマンド機能 (FOD)」を参照してください。

AMD プロセッサの入れ子になった仮想化

入れ子になった仮想化は、Hyper-V 仮想マシン (VM) 内での Hyper-V の実行を可能にする機能です。 Windows Server 2022 は、AMD プロセッサを使用した入れ子になった仮想化のサポートを提供し、ご利用の環境により多くのハードウェアの選択肢を提供します。 詳細については、ネストされた仮想化のドキュメントを参照してください。

Microsoft Edge ブラウザー

Internet Explorer に代わって、Microsoft Edge が Windows Server 2022 に付属しています。 これは、Chromium オープン ソース上に構築され、Microsoft のセキュリティとイノベーションによってサポートされています。 これは、デスクトップ エクスペリエンス搭載サーバーのインストール オプションと共に使用できます。 詳細については、 Microsoft Edge Enterprise のドキュメントを参照してください。 Microsoft Edge は、Windows Server の他のものとは異なり、そのサポート ライフサイクルに関してモダン ライフサイクルに従っています。 詳細については、Microsoft Edge ライフサイクルに関するドキュメントを参照してください。

ネットワーク パフォーマンス

UDP パフォーマンスの向上

UDP は、RTP とカスタム (UDP) ストリーミングおよびゲーミング プロトコルの普及により、伝達されるネットワーク トラフィックが増え、人気の高いプロトコルになっています。 UDP をベースに構築された QUIC プロトコルでは、UDP のパフォーマンスは TCP と同等のレベルになっています。 重要なこととして、Windows Server 2022 には UDP セグメント化オフロード (USO) が含まれています。 USO によって、UDP パケットの送信に求められるほとんどの処理が、CPU からネットワーク アダプターの専用ハードウェアに移されます。 USO は UDP Receive Side Coalescing (UDP RSC) によって補完され、これによりパケットがまとめられ、UDP の処理にかかる CPU の使用率が低下します。 さらに、送信と受信の両方で UDP データ

パスについて、数百もの機能改善が実施されました。 この新しい機能は、Windows Server 2022 と Windows 11 の両方に備わっています。

TCP パフォーマンスの向上

Windows Server 2022 では、TCP HyStart++ を使用して (特に高速ネットワークにおいて) 接続の起動中のパケット損失を減らし、RACK を使用して再転送タイムアウト (RTO) を減らしています。 これらの機能はトランスポート スタックで既定で有効になっており、高速時によりパフォーマンスを高める、より滑らかなネットワーク データ フローを実現します。 この新しい機能は、Windows Server 2022 と Windows 11 の両方に備わっています。

Hyper-V 仮想スイッチの改善

更新された Receive Segment Coalescing (RSC) により、Hyper-V の仮想スイッチが強化されます。 RSC により、ハイパーバイザー ネットワークでパケットがまとめられ、1 つの大きなセグメントとして処理できます。 CPU のサイクル数が減り、セグメントは目的のアプリケーションによって処理されるまで、データ パス全体にわたって結合されたままになります。 RSC により、仮想 NIC で受信された外部ホストからのネットワーク トラフィックと、仮想 NIC から同じホスト上の別の仮想 NIC へのネットワーク トラフィックの両方のパフォーマンスが改善されました。

vSwitch では、RSC は vSwitch を通過するデータの前に、複数の TCP セグメントを大きなセグメントに結合することもできます。 この変更により、仮想ワークロードのネットワーク パフォーマンスも向上します。 RSC は、既定で外部仮想スイッチで有効になっています。

システム インサイトでのディスク異常の検出

System Insights には、Windows Admin Center を使用したディスクの異常検出という別の機能があります。

ディスク異常の検出は、ディスクが通常とは異なる動作をしたとき、それを浮き彫りにする新機能です。 異なるのは必ずしも悪いことではありませんが、これらの異常な瞬間を見ることは、システムの問題のトラブルシューティングを行うときに役立ちます。 この機能は、Windows Server 2019 を実行するサーバーでも利用できます。

Windows Update のロールバックの機能強化

最新ドライバーや品質の Windows Update をインストールしたため起動に失敗するようになった場合、更新プログラムを削除することにより、起動の障害からサーバーを自動的に復旧できるようになりました。 最近の品質のドライバー更新プログラムのインストール後にデバイ

スが正常に起動できない場合、Windows は更新プログラムを自動的にアンインストールして、デバイスを正常にバックアップして実行するようになりました。

この機能を使用するには、サーバーが Windows 回復環境パーティションで Server Core インストール オプションを使用する必要があります。

Storage

Windows Server 2022 には、次の記憶域の更新プログラムが含まれています。 記憶域は、システム インサイトでのディスク異常の検出と Windows Admin Center の更新によっても影響を受けます。

記憶域移行サービス

Windows Server 2022 の Storage Migration Service の機能強化により、記憶域をより多くのソースの場所から Windows Server または Azure に簡単に移行できます。 Windows Server 2022 で記憶域移行サーバー オーケストレーターを実行するときに使用できる機能を次に示します。

- 新しいサーバーにローカル ユーザーとグループを移行する。
- フェールオーバー クラスターからの記憶域の移行、フェールオーバー クラスターへの移行、スタンドアロン サーバーとフェールオーバークラスター間での移行を行う。
- Samba を使用する Linux サーバーから記憶域を移行する。
- Azure File Sync を使用して、Azure に移行された共有をより簡単に同期する。
- Azure などの新しいネットワークに移行する。
- NetApp CIFS サーバーを NetApp FAS 配列から Windows サーバーとクラスターに移行する。

調整可能なストレージの修復速度

ユーザーが調整可能な記憶域の修復速度 は、データの再同期プロセスをより詳細に制御できる記憶域スペース ダイレクトの新機能です。 調整可能なストレージの修復速度により、データ コピーの修復 (回復性) またはアクティブなワークロードの実行 (パフォーマンス) のいずれかにリソースを割り当てることができます。 修復速度を制御することにより、可用性が向上し、クラスターをより柔軟かつ効率的に利用できるようになります。

修復と再同期の高速化

ノードの再起動やディスク障害などのイベント後のストレージの修復と再同期が 2 倍早くなりました。 修復の経過時間の差異が少ないため、修復にかかる時間をより確実に確認できます。 この改善は、データ追跡に細分性を追加することで実現されます。 修復では、移動する

必要があるデータのみが移動され、使用されるシステム リソースと修復にかかる時間が短縮されます。

スタンドアロン サーバーでの記憶域スペースによる記憶域バス キャッシュ

記憶域バス キャッシュは、スタンドアロン サーバーで使用できるようになりました。 ストレージの効率を維持し、運用コストを低く保ちながら、読み取りと書き込みのパフォーマンスを大幅に向上させることができます。 記憶域スペース ダイレクトの実装と同様に、この機能は高速なメディア (NVMe や SSD など) と低速なメディア (HDD など) を組み合わせて、階層を作成します。 高速なメディアの層の一部は、キャッシュ用に予約されています。 詳細については、「スタンドアロン サーバーでの記憶域スペースによる記憶域バス キャッシュの有効化」を参照してください。

ReFS ファイルレベルのスナップショット

Microsoft Resilient File System (ReFS) には、クイック メタデータ操作を使用してファイルのスナップショットを作成する機能が含まれるようになりました。 スナップショットは、複製が書き込み可能であるという点で ReFS ブロックの複製 とは異なりますが、スナップショットは読み取り専用です。 この機能は、VHD/VHDX ファイルを使用した仮想マシン バックアップのシナリオで特に便利です。 ReFS スナップショットは、ファイル サイズに関係なく一定の時間がかかるという意味でユニークです。 スナップショットのサポートは、ReFSUtil で、または API として利用できます。

SMB の圧縮

Windows Server 2022 と Windows 11 の SMB の機能強化により、ユーザーまたはアプリケーションはネットワーク経由で転送するときにファイルを圧縮できます。 低速またはより混雑したネットワークで高速に転送するために、ファイルを手動で zip 圧縮する必要がなくなりました。 詳細については、 SMB 圧縮に関するページを参照してください。

Containers

Windows Server 2022 には、Windows コンテナーに対する次の変更が含まれています。

Server Core イメージ サイズの縮小

Server Core イメージのサイズを縮小しました。 イメージ サイズを小さくすると、コンテナー化されたアプリケーションをより迅速にデプロイできます。 Windows Server 2022 では、GA 時の Server Core コンテナー イメージの Release to Manufacturing (RTM) 層は、ディスク上で

2.76 GB (非圧縮) でクロック インします。 ディスク上で 3.47 GB (非圧縮) でクロック インする、GA 時の Windows Server 2019 RTM 層と比較すると、これは、その層のディスク上のフットプリントでの 33% の削減になります。 イメージの合計サイズを 33%減らす必要はありませんが、RTM レイヤー のサイズを小さくすると、一般にイメージ全体のサイズが小さくなります。

> ⓘ **注意**
>
> Windows コンテナーの基本イメージは、RTM レイヤーと、RTM レイヤーにオーバーレイされた OS ライブラリとバイナリの最新のセキュリティ修正プログラムを含むパッチ レイヤーの 2 つのレイヤーとして出荷されます。 パッチ レイヤーのサイズは、バイナリ内の変更の数に応じて、コンテナー イメージのサポート サイクルの有効期間中に変化します。 コンテナーの基本イメージを新しいホストにプルする場合は、両方の層をプルする必要があります。

すべての Windows コンテナー イメージのサポート サイクルの延長

Windows Server 2022 イメージには、Server Core、Nano Server、Server が含まれており、メインストリーム サポートが 5 年間、延長サポートが 5 年間あります。 このサポート サイクルが長いほど、組織に適した場合に実装、使用、アップグレード、または移行する時間が確保されます。 詳細については、Windows コンテナーの基本イメージのライフサイクルに関する記事と Windows Server 2022 のライフサイクルに関する記事を参照してください。

仮想化されたタイム ゾーン

Windows Server 2022 では、Windows コンテナーはホストとは別に仮想化されたタイム ゾーン構成を維持できます。 ホスト タイム ゾーンで通常使用されるすべての構成が仮想化され、コンテナーごとにインスタンス化されるようになりました。 コンテナーのタイム ゾーンを構成するには、tzutil コマンド ユーティリティまたは Set-TimeZone Powershell コマンドレットを使用します。 詳細については、 仮想化されたタイム ゾーンに関するページを参照してください。

オーバーレイ ネットワーク サポートのスケーラビリティの向上

Windows Server 2022 では、Windows Server の以前の 4 つの半期チャネル (SAC) リリースですでに行われていたが、Windows Server 2019 にはバックポートされていなかったいくつかのパフォーマンスとスケールの改善を集約しています。

- 同じノード上で数百の Kubernetes サービスとポッドを使用する場合のポート不足の問題を解決。

- Hyper-V 仮想スイッチ (vSwitch) でのパケット転送のパフォーマンスの向上。
- Kubernetes でのコンテナー ネットワーク インターフェイス (CNI) 再起動の信頼性が向上しました。
- Windows Server コンテナーと Kubernetes ネットワークで使用される、ホスト ネットワーク サービス (HNS) コントロール プレーンとデータ プレーンの機能強化。

オーバーレイ ネットワーク サポートのパフォーマンスとスケーラビリティの向上の詳細については、「Windows 用 Kubernetes オーバーレイ ネットワーク」を参照してください。

オーバーレイおよび l2bridge ネットワークの Direct Server Return ルーティング

Direct Server Return (DSR) は、負荷分散されたシステム内の非対称ネットワーク負荷分散です。これにより、要求と応答のトラフィックで異なるネットワーク パスが使用できます。 異なるネットワーク パスを使用すると、余分なホップを避け、待機時間を短縮することができます。これにより、クライアントとサービスの間の応答時間が短縮され、ロード バランサーから余分な負荷が取り除かれます。 DSR を使用すると、インフラストラクチャの変更をほとんどまたはまったく行わずに、アプリケーションのネットワーク パフォーマンスの向上が透過的に実現されます。

詳細については、Kubernetes への Windows サポートの導入における DSR に関するページを参照してください。

gMSA の機能強化

Active Directory 認証を容易にするために、Windows コンテナーでグループ管理サービス アカウント (gMSA) を使用できます。 gMSA が Windows Server 2019 で導入されたときは、Active Directory から資格情報を取得するためにコンテナー ホストをドメインに参加させる必要がありました。 Windows Server 2022 では、ドメインに参加していないホストを持つコンテナーの gMSA は、ホスト ID ではなくポータブル ユーザー ID を使用して gMSA 資格情報を取得します。 そのため、Windows ワーカー ノードをドメインに手動で参加させる必要はなくなりました。 認証後、Kubernetes はユーザー ID をシークレットとして保存します。 ドメインに参加していないホストを使用するコンテナーの gMSA は、ホスト ノードをドメインに参加させることなく gMSA でコンテナーを作成するという柔軟性を提供します。

gMSA の機能強化の詳細については、「Windows コンテナー用に gMSA を作成する」を参照してください。

IPv6 サポート

Windows の Kubernetes では、Windows Server の L2bridge ベースのネットワークで IPv6 デュアル スタックがサポートされるようになりました。 IPv6 は Kubernetes で使用する CNI に依存しており、エンドツーエンドの IPv6 サポートを有効にするためには Kubernetes バージョン 1.20 以降も必要になります。 詳細については、Kubernetes への Windows のサポートの導入における IPv4/IPv6 に関するページを参照してください。

Windows 用の Calico を使用した Windows ワーカー ノードのマルチサブネット サポート

ホスト ネットワーク サービス (HNS) で、より制限の厳しいサブネット (プレフィックス長が長いサブネットなど) と、Windows ワーカー ノードごとに複数のサブネットも使用できるようになりました。 以前は、HNS では、Kubernetes コンテナー エンドポイント構成が、基になるサブネットのプレフィックス長のみを使用するように制限されていました。 この機能を使用する最初の CNI は、Windows 用の Calico です。 詳細については、「ホスト ネットワーク サービスでの複数のサブネットのサポート」を参照してください。

ノード管理用の HostProcess コンテナー

HostProcess コンテナーは、ホスト上で直接実行される新しいコンテナーの種類であり、Windows コンテナー モデルを拡張して、より広範な Kubernetes クラスター管理シナリオを実現します。 HostProcess コンテナーを使用すると、コンテナーによって提供されるバージョン管理とデプロイ方法を保持しながら、ホスト アクセスを必要とする管理操作をパッケージ化および配布できます。 Kubernetes のさまざまなデバイス プラグイン、ストレージ、ネットワーク管理のシナリオに Windows コンテナーを使用できます。

HostProcess コンテナーには、次のような利点があります。

- クラスター ユーザーは、Windows サービスの管理タスクと管理のために各 Windows ノードにサインインして個別に構成する必要がなくなりました。
- コンテナー モデルを使用して、必要な数のクラスターに管理ロジックをデプロイできます。
- HostProcess コンテナーは、既存の Windows Server 2019 以降の基本イメージの上に構築し、Windows コンテナー ランタイムを使用して管理し、ホスト コンピューターのドメインで使用可能な任意のユーザーとして実行できます。
- HostProcess コンテナーでは、Kubernetes 内の Windows ノードを管理するための最適な方法が提供されます。

詳細については、Windows HostProcess コンテナー に関するページを参照してください。

Windows Admin Center の機能強化

Windows Server 2022 は、Windows Admin Center に追加されたコンテナーの拡張機能を拡張し、.NET Framework の ASP.NET に基づいて既存の Web アプリケーションをコンテナー化します。 開発者の静的なフォルダーまたは Visual Studio ソリューションを使用できます。

Windows Admin Center には、次の機能強化が含まれています。

- コンテナー拡張機能で新たに Web 配置ファイルがサポートされます。これにより、実行中のサーバーからアプリとその構成を抽出し、アプリケーションをコンテナー化できます。
- イメージをローカルで検証し、そのイメージを Azure Container Registry にプッシュすることができます。
- Azure Container Registry と Azure Container Instances に基本的な管理機能が追加されました。 Windows Admin Center UI を使用して、レジストリの作成と削除、イメージの管理、新しいコンテナー インスタンスの開始と停止を行えるようになりました。

Azure Migrate: アプリ コンテナー化ツール

Azure Migrate アプリ: コンテナー化は、既存の Web アプリケーションをコンテナー化して Azure Kubernetes Service に移動するエンドツーエンドのソリューションです。 既存の Web サーバーの評価、コンテナー イメージの作成、Azure Container Registry へのイメージのプッシュ、Kubernetes デプロイの作成、そして Azure Kubernetes Service へのデプロイを行うことができます。

Azure Migrate App: Containerization ツールの詳細については、「 ASP.NET アプリのコンテナー化と Azure Kubernetes Service と Java Web アプリへのコンテナー化と Azure Kubernetes Service への移行」を参照してください。

Windows Server 2019 の新機能

2025/07/25適用対象: ✅ Windows Server 2019

この記事では、Windows Server 2019 の新機能の一部について説明します。 Windows Server 2019 は Windows Server 2016 の強力な基盤の上に構築されています。また、次の 4 つの主要テーマに沿って多数の技術革新が組み込まれています: ハイブリッド クラウド、セキュリティ、アプリケーション プラットフォーム、およびハイパー コンバージド インフラストラクチャ (HCI)。

General

Windows Admin Center

Windows Admin Center は、サーバー、クラスター、ハイパーコンバージド インフラストラクチャ、Windows 10 PC を管理するための、ローカルに展開されるブラウザー ベースのアプリです。 Windows 以外の追加費用は必要なく、運用環境で使用できます。

Windows Server 2019 および Windows 10 および 11 に Windows Admin Center をインストールし、それを使用して Windows Server 2012 以降を実行しているサーバーとクラスターを管理できます。

詳細については、Windows Admin Center に関するページを参照してください。

Desktop experience

Windows Server 2019 は長期サービス チャネル (LTSC) リリースであるため、**デスクトップ エクスペリエンス**が含まれています。 半期チャネル (SAC) リリースには、設計によるデスクトップ エクスペリエンスは含まれません。厳密には、Server Core と Nano Server コンテナー イメージのリリースです。 Windows Server 2016 の場合と同様、オペレーティング システムのセットアップ中には Server Core インストールまたはデスクトップ エクスペリエンス搭載サーバーのインストールを選択できます。

System Insights

システム インサイトは、ローカルの予測分析機能を Windows Server にネイティブに導入する、Windows Server 2019 で利用可能な新機能です。 これらの予測機能は、それぞれ機械学習モデルに支えられており、パフォーマンス カウンターやイベントなどの Windows Server システム データをローカルで分析するために使用できます。 システム インサイトを使うと、サーバーがどのように機能しているかを理解できます。また、Windows Server デプロイの問題を事後対応で管理することに関連する運用コストを削減できます。

Hybrid Cloud

サーバー コア アプリ互換性オンデマンド機能

Server Core アプリ互換性オンデマンド機能 (FOD) を使って、Windows Server のバイナリとコンポーネントのサブセットをデスクトップ エクスペリエンスに含めることで、アプリの互換性を大幅に高めることができます。 Server Core は、Windows Server デスクトップ エクスペリエンスのグラフィカル環境自体を追加しないことで、可能な限り無駄を省き、機能と互換性を高めています。

このオプションのオンデマンド機能は、独立した ISO で提供され、DISM を使用して Windows Server Core インストールとイメージのみに追加できます。

Server Core に追加された Windows 展開サービス (WDS) トランスポート サーバー ロール

トランスポート サーバーには、WDS のコア ネットワーク部分のみが含まれます。 Server Core とトランスポート サーバー ロールを使って、スタンドアロン サーバーからデータ (オペレーティング システム イメージを含む) を送信するマルチキャスト名前空間を作成できるようになりました。 また、クライアントが PXE ブートし、独自のカスタム セットアップ アプリケーションをダウンロードできるようにする PXE サーバーを用意する必要がある場合にも使用できます。

リモート デスクトップ サービスと Azure AD の統合

Azure AD と統合されたので、条件付きアクセス ポリシー、多要素認証、Azure AD を使用した他の SaaS アプリとの統合認証などを使用できます。 詳細については、RDS 展開と Azure AD Domain Services との統合に関するページをご覧ください。

ネットワーク

TCP Fast Open (TFO)、受信ウィンドウの自動調整、IPv6 など、コア ネットワーク スタックにいくつかの機能強化を加えました。 詳細については、コア ネットワーク スタック機能の機能強化 に関する投稿を参照してください。

動的な vRSS と VMMQ

これまで、仮想マシン キューと仮想マシン マルチキュー (VMMQ) では、ネットワーク スループットが最初に 10 GbE 以上に達するため、個々の VM に対してはるかに高いスループット

が実現されていました。 残念ながら、成功に必要な計画、基本計画、チューニング、監視は、IT 管理者が予想していたよりもはるかに大きな作業になりました。

Windows Server 2019 では、必要に応じてネットワーク ワークロードの処理を動的に分散および調整することで、これらの最適化が向上します。 Windows Server 2019 は、ピーク時の効率を保証し、IT 管理者の構成の負担を排除します。 詳細については、「Azure Local のホスト ネットワーク要件」を参照してください。

セキュリティ

Windows Defender Advanced Threat Protection (ATP)

ATP のディープ プラットフォーム センサーおよび対応アクションは、メモリとカーネル レベルの攻撃を検出したうえで、対応として悪意のあるファイルを抑制し、悪意のあるプロセスを終了します。

- Windows Defender ATP の詳細については、「Windows Defender ATP 機能の概要」を参照してください。
- サーバーのオンボーディングの詳細については、「Windows Defender ATP サービスへのサーバーのオンボーディング」を参照してください。

Windows Defender ATP Exploit Guard は、セキュリティ リスクと生産性の要件のバランスを取ることができる、新しい一連のホスト侵入防止機能です。 Windows Defender Exploit Guard は、さまざまな攻撃ベクトルに対してデバイスをロック ダウンし、マルウェアの攻撃でよく使われる動作をブロックするように設計されています。 コンポーネントは次のとおりです。

- 攻撃表面の縮小 (ASR) は、悪意のある疑わしいファイルをブロックすることで、マルウェアがマシンに侵入することを防ぐために企業が活用できる一連のコントロールです。 たとえば、Office ファイル、スクリプト、横移動、ランサムウェアの動作、メールベースの脅威などです。
- ネットワーク保護では、Windows Defender SmartScreen によって、信頼されていないホスト/IP アドレスへの送信プロセスをデバイスでブロックすることにより、Web ベースの脅威からエンドポイントを保護します。
- フォルダー アクセスの制御 では、信頼されていないプロセスから保護されたフォルダーへのアクセスをブロックすることで、機密データをランサムウェアから保護します。
- Exploit Protection は、脆弱性の悪用に対する軽減策のセット (EMET を置き換える機能) で、システムおよびアプリケーションの保護のために簡単に構成できます。

- Windows Defender アプリケーション制御 はコード整合性 (CI) ポリシーとも呼ばれており、Windows Server 2016 でリリースされた機能です。 既定の CI ポリシーを含めることで、デプロイが容易になりました。 既定のポリシーでは、すべての Windows インボックス ファイルと Microsoft アプリケーション (SQL Server など) を許可し、CI をバイパスできる既知の実行可能ファイルをブロックしています。

ソフトウェア定義ネットワーク (SDN) によるセキュリティ

SDN のセキュリティでは、オンプレミスまたはクラウドのサービス プロバイダーとして、ワークロードの実行に対するお客様の信頼度を向上するための多数の機能が提供されています。

これらのセキュリティ強化機能は、Windows Server 2016 で導入された包括的な SDN プラットフォームに統合されています。

SDN の新機能の完全な一覧については、「Windows Server 2019 の SDN の新機能」を参照してください。

シールドされた仮想マシンの機能強化

シールドされた仮想マシンに次の機能強化を加えました。

ブランチ オフィスの機能強化

新しいフォールバック HGS 機能とオフライン モード機能を利用することにより、ホスト ガーディアン サービスへの接続が断続的なコンピューターで、シールドされた仮想マシンを実行できるようになりました。 フォールバック HGS を使用すると、プライマリ HGS サーバーにアクセスできない場合に試すことができるように、Hyper-V の URL のセカンダリ セットを構成できます。

HGS にアクセスできない場合でも、オフライン モードを使うと、シールドされた VM を引き続き起動できます。 VM が一度正常に起動し、ホストのセキュリティ構成が変更されていない限り、オフライン モードで VM を起動できます。

Troubleshooting improvements

VMConnect 拡張セッション モードと PowerShell ダイレクトのサポートが有効になり、シールドされた仮想マシンのトラブルシューティングも容易になりました。 これらのツールは、VM へのネットワーク接続が失われたため構成を更新してアクセスを復元する必要がある場合に役立ちます。 詳細については、「保護されたファブリックとシールドされた VM」を参照してください。

これらの機能は構成する必要がなく、Windows Server Version 1803 以降を実行している Hyper-V ホストにシールドされた VM が配置されると、自動的に利用可能になります。

Linux support

OS が混在する環境を使用している場合、Windows Server 2019 では、シールドされた仮想マシンでの Ubuntu、Red Hat Enterprise Linux、および SUSE Linux Enterprise Server の実行がサポートされるようになりました。

HTTP/2 による高速かつ安全な Web

- 接続の結合機能の強化により、正しく暗号化された中断のない閲覧エクスペリエンスを実現します。
- 接続エラーの自動軽減と展開の容易さを目的として、HTTP/2 サーバー側暗号スイートのネゴシエーションがアップグレードされました。
- 高いスループットを提供するために、既定の TCP 輻輳プロバイダーが Cubic に変更されました。

Encrypted networks

仮想ネットワークの暗号化では、**[暗号化有効]** のラベルが付いたサブネット内の仮想マシン間の仮想ネットワーク トラフィックが暗号化されます。 暗号化されたネットワークでは、仮想サブネット上のデータグラム トランスポート層セキュリティ (DTLS) も使用され、パケットが暗号化されます。 DTLS は、物理ネットワークにアクセスできるユーザーによる盗聴、改ざん、偽造からデータを保護します。

詳細については、「暗号化されたネットワーク」を参照してください。

Firewall auditing

ファイアウォールの監査は、SDN ファイアウォール規則によって処理されたすべてのフローと、ログ記録が有効になっているアクセス制御リスト (ACL) を記録する SDN ファイアウォールの新機能です。

仮想ネットワーク ピアリング

仮想ネットワーク ピアリングを使用すると、2 つの仮想ネットワークをシームレスに接続できます。 ピアリングされた仮想ネットワークは、監視で 1 つのネットワークとして表示されます。

Egress metering

エグレス測定 では、送信データ転送の使用状況メーターが提供されます。 ネットワーク コントローラーでは、この機能を使用して、仮想ネットワークごとに SDN 内で使用されるすべての IP 範囲の許可リストを保持します。 これらのリストでは、一覧に記載されている IP 範囲に含まれていない宛先へのパケット ヘッダーは、送信データ転送として課金されると見なされます。

Storage

Windows Server 2019 でストレージに行った変更の一部を次に示します。 ストレージは、データ重複除去の更新、特に重複除去されたボリュームへのイングレスまたはエグレスを最適化するための DataPort API の更新によっても影響を受けます。

ファイル サーバー リソース マネージャー

ファイル サーバー リソース マネージャー サービスの起動時に、すべてのボリュームで変更ジャーナル (USN ジャーナルとも呼ばれます) を作成しないようにできるようになりました。 変更体験の作成を防ぐことで、各ボリューム上の領域を節約できますが、リアルタイムのファイル分類は無効になります。 詳細については、「ファイル サーバー リソース マネージャーの概要」を参照してください。

SMB

- Windows Server では、既定で SMB1 クライアントとサーバーがインストールされなくなりました。 さらに、SMB2 以降のゲストとして認証する機能は、既定で無効になっています。 詳細については、「SMBv1 は、Windows 10 バージョン 1709、Windows Server バージョン 1709 以降のバージョンでは、既定でインストールされていません。」を参照してください。

- SMB2+ でレガシ アプリケーションの oplock を無効にできるようになりました。 クライアントからの接続ごとに署名または暗号化を必須にすることもできます。 詳細については、「SMBShare PowerShell モジュールのヘルプ」を参照してください。

記憶域移行サービス

記憶域移行サービスでは、Windows Server の新しいバージョンにサーバーを簡単に移行できます。 このグラフィカル ツールは、サーバー上のデータのインベントリを作成し、データと構成を新しいサーバーに転送します。 記憶域移行サービスでは、古いサーバーの ID を新しい

サーバーに移動することもできるため、ユーザーはプロファイルとアプリを再構成する必要がありません。 詳細については、「記憶域移行サービス」をご覧ください。

Windows Admin Center バージョン 1910 では、Azure 仮想マシンを展開する機能が追加されています。 この更新により、Azure VM の展開が記憶域移行サービスに統合されます。 詳細については、「Azure VM の移行」を参照してください。

また、KB5001384 がインストールされた Windows Server 2019 または Windows Server 2022 で記憶域移行サーバー オーケストレーターを実行すると、次の post-release-to-manufacturing (RTM) 機能にアクセスできます。

- 新しいサーバーにローカル ユーザーとグループを移行する。
- フェールオーバー クラスターからの記憶域の移行、フェールオーバー クラスターへの移行、スタンドアロン サーバーとフェールオーバークラスター間での移行を行う。
- Samba を使用する Linux サーバーから記憶域を移行する。
- Azure File Sync を使用して、移行された共有をより簡単に Azure に同期する。
- Azure などの新しいネットワークに移行する。
- NetApp 共通インターネット ファイル システム (CIFS) サーバーを NetApp Federated Authentication Service (FAS) 配列から Windows サーバーおよびクラスターに移行します。

記憶域スペース ダイレクト

記憶域スペース ダイレクトの新機能の一覧を次に示します。 検証済みの記憶域スペース ダイレクト システムを取得する方法の詳細については、「Azure Local ソリューションの概要」を参照してください。

- ReFS ボリュームの重複除去と圧縮。 オプションの圧縮機能を備えた可変サイズのチャンク ストアは節約率を最大化し、マルチスレッドの後処理アーキテクチャはパフォーマンスへの影響を最小限に抑えます。 この機能では、最大 64 TB のボリュームがサポートされ、各ファイルの最初の 4 TB が重複除去されます。

- 永続メモリのネイティブ サポートにより、PowerShell または Windows Admin Center で他のドライブと同様に永続メモリを管理できます。 この機能は、Intel Optane DC PM および NVDIMM-N 永続メモリ モジュールをサポートします。

- エッジの 2 ノード ハイパーコンバージド インフラストラクチャに対する入れ子の回復性。 RAID 5+1 に基づく新しいソフトウェア回復性オプションを使用すると、2 つのハードウェア障害が同時に発生しても耐えられるようになります。 2 ノードの記憶域スペース ダイレクト クラスターは、1 つのサーバー ノードがダウンし、別のサーバー ノードでドライブ障害が発生した場合でも、アプリと仮想マシンに継続的にアクセスできる記憶域を提供します。

- 2 つのサーバー クラスターで、USB フラッシュ ドライブを監視として使用できるようになりました。 サーバーがダウンしてからバックアップされると、USB ドライブ クラスターによって最新のデータがあるサーバーが認識されます。 詳細については、「記憶域スペース ダイレクトのお知らせブログ記事」およびフェールオーバー クラスタリング用のファイル共有監視の構成」を参照してください。

- Windows Admin Center は、記憶域スペース ダイレクトを管理および監視できるダッシュボードをサポートしています。 IOPS と IO 待機時間を、クラスター全体のレベルから個々の SSD または HDD まで、追加費用なしで監視できます。 詳細については、「Windows Admin Centerを使用したハイパーコンバージド インフラストラクチャの管理」を参照してください。

- パフォーマンス履歴は、リソースの使用状況と測定値を簡単に可視化できる新しい機能です。 詳細については、「記憶域スペース ダイレクトのパフォーマンス履歴」を参照してください。

- 最大 64 TB の最大 64 ボリュームの容量を使用して、クラスターあたり最大 4 PB まで拡張できます。 また、複数のクラスターをクラスター セットにまとめ、単一のストレージ名前空間内でさらに大規模なスケールを実現することもできます。

- ミラー高速パリティを利用すると、RAID-1 と RAID-5/6 の組み合わせと同様に、ミラーとパリティの両方の戦略を組み込んだ記憶域スペース ダイレクト ボリュームを構築できます。 ミラー加速パリティにより、Windows Server 2016 よりも 2 倍の速度を実現しました。

- ドライブの待機時間に関する外れ値の検出は、PowerShell および Windows Admin Center で「待機時間の異常」ステータスの低速ドライブを自動的に識別します。

- フォールト トレランスを高めるために、ボリュームの割り当てを手動で区切ります。 詳細については、「記憶域スペース ダイレクトでボリュームの割り当てを区切る」を参照してください。

Storage Replica

記憶域レプリカの新機能は次のとおりです。

- 記憶域レプリカは、Windows Server 2019 Standard Edition および Windows Server 2019 Datacenter Edition で利用できるようになりました。 ただし、Standard Edition では、レプリケートできるボリュームは 1 つだけであり、そのボリュームのサイズは最大 2 TB です。

- テスト フェールオーバーは、テストまたはバックアップの目的で、レプリケートされた記憶域のスナップショットを宛先サーバーに一時的にマウントできる新しい機能です。

詳細については、「記憶域レプリカについてよく寄せられる質問」を参照してください。

- 記憶域レプリカ ログのパフォーマンスが向上しました。これには、相互にレプリケートするオールフラッシュ記憶域および記憶域スペース ダイレクト クラスターでのレプリケーション スループットと待機時間の向上などが含まれます。

- Windows Admin Center のサポート。これには、サーバー間、クラスター間、ストレッチ クラスターのレプリケーションに対するサーバー マネージャーを使用したレプリケーションのグラフィカル管理が含まれます。

Data deduplication

Windows Server 2019 では、Resilient File System (ReFS) がサポートされるようになりました。 ReFS では、ReFS ファイルシステムの重複除去と圧縮により、同じボリュームに最大 10 倍のデータを格納できます。 可変サイズのチャンク ストアには、節約率を最大化できるオプションの圧縮機能が付属しており、マルチスレッドの後処理アーキテクチャはパフォーマンスへの影響を最小限に抑えます。 ReFS では、最大 64 TB のボリュームがサポートされ、各ファイルの最初の 4 TB が重複除去されます。 詳細については、「Windows Admin Center で重複除去と圧縮を有効にする方法」の簡単なビデオ デモを参照してください。

Failover Clustering

Windows Server 2019 のフェールオーバー クラスタリングに次の機能を追加しました。

- クラスター セットは、複数のクラスターをグループ化して、コンピューティング、ストレージ、ハイパーコンバージドの 3 種類の複数のフェールオーバー クラスターを疎結合でグループ化します。 このグループ化により、1 つのソフトウェア定義データセンター (SDDC) ソリューション内のサーバーの数が、クラスターの現在の制限を超えて増加します。 クラスター セットを使用すると、クラスター セット内のクラスター間でオンライン仮想マシンを移動できます。 詳細については、「クラスター セットのデプロイ」を参照してください。

- クラスターは既定で Azure 対応になりました。 Azure 対応クラスターは、Azure IaaS 仮想マシンで実行されているタイミングを自動的に検出し、その構成を最適化して最高レベルの可用性を実現します。 これらの最適化には、Azure の計画メンテナンス イベントのプロアクティブ フェールオーバーとログ記録が含まれます。 自動化された最適化により、クラスター名に分散ネットワーク名を使用してロード バランサーを構成する必要がなくなるため、デプロイが簡単になります。

- クロスドメイン クラスター移行を使用すると、フェールオーバー クラスターを Active Directory ドメイン間で動的に移動できるため、ドメインの統合が簡略化され、ハードウ

ェア パートナーはクラスターを作成して、後で顧客のドメインに参加できるようになります。

- USB 監視機能を使用すると、クラスターのクォーラムを決定する際に、ネットワーク スイッチに接続されている USB ドライブを監視として使用できます。 この機能には、SMB2 準拠デバイスの拡張ファイル共有監視サポートが含まれます。

- 仮想マシンのパフォーマンスを大幅に向上させるために、CSV キャッシュが既定で有効化されるようになりました。 MSDTC では、SQL Server など、記憶域スペース ダイレクトに MSDTC ワークロードをデプロイできるように、クラスター共有ボリュームがサポートされるようになりました。 ロジックが強化され、パーティション分割されたノードを検出して、自動修復でノードをクラスター メンバーシップに戻すことができるようになりました。 クラスター ネットワーク ルート検出と自動修復機能が強化されています。

- クラスター対応更新 (CAU) が記憶域スペース ダイレクトに対応して統合され、データ再同期の検証と確認が各ノードで完了するようになりました。 クラスター対応更新は、必要な場合にのみインテリジェントに再起動するように更新を検査します。 この機能を使用すると、計画メンテナンスのためにクラスター内のすべてのサーバーを再起動できます。

- 次のシナリオでファイル共有の監視を使用できるようになりました。

  - 離れた場所にあるためにインターネットにアクセスできない、またはインターネット アクセスが遅く、クラウド ミラーリング監視の使用が妨げられています。

  - ディスクのミラーリング監視用の共有ドライブが不足しています。 たとえば、共有ディスクを使用しない構成 (記憶域スペース ダイレクト ハイパーコンバージド構成、SQL Server Always On 可用性グループ (AG)、Exchange Database 可用性グループ (DAG) など)。

  - DMZ の背後にあるクラスターが原因でドメイン コントローラー接続が不足しています。

  - Active Directory クラスター名オブジェクト (CNO) がないワークグループまたはクロスドメイン クラスター。 Windows Server では、DFS 名前空間共有を場所として使用することもブロックされるようになりました。 ファイル共有監視を DFS 共有に追加すると、クラスターの安定性の問題が発生し、この構成がサポートされなくなることがあります。 共有が DFS 名前空間を使用しているかどうかを検出するロジックを追加しました。 DFS 名前空間が検出された場合、フェールオーバー クラスター マネージャーはミラーリング監視の作成をブロックし、サポートされていないことを通知するエラー メッセージを表示します。

- クラスター共有ボリュームと記憶域スペース ダイレクトのサーバー メッセージ ブロック (SMB) を介したクラスター内通信のセキュリティを強化するクラスター強化機能が実装されています。 この機能では、証明書を利用して、可能な限り最も安全なプラットフォームを提供します。 これにより、フェールオーバー クラスターを NTLM に依存せずに動作できるようになり、セキュリティ ベースラインを確立できるようになります。

- フェールオーバー クラスターでは、NTLM 認証が使用されなくなりました。 代わりに、Windows Server 2019 クラスターでは Kerberos と証明書ベースの認証のみが使用されるようになりました。 ユーザーは、このセキュリティ強化を利用するために変更を加えたり、何かをデプロイしたりする必要はありません。 この変更により、NTLM が無効になっている環境にフェールオーバー クラスターをデプロイすることもできます。

Application Platform

Windows 上の Linux コンテナー

同じコンテナー ホストで同じ Docker デーモンを使用して、Windows および Linux ベースのコンテナーを実行できるようになりました。 アプリケーション開発者に柔軟性を提供して、異種コンテナーのホスト環境を持つことができるようになりました。

Kubernetes の組み込みサポート

Windows Server 2019 では、Windows で Kubernetes をサポートするために必要な半期チャネル リリースから、計算、ネットワーク、および記憶域への機能強化が続行されます。 詳細は、今後の Kubernetes リリースで公開されます。

- Windows Server 2019 の Container Networking を使うと、Windows 上の Kubernetes の使いやすさが大幅に向上します。 プラットフォーム ネットワークの回復性とコンテナー ネットワーク プラグインのサポートを拡張しました。

- Kubernetes に展開されたワークロードでは、ネットワーク セキュリティを使用して、埋め込みツールにより Linux と Windows の両方のサービスを保護できます。

Container improvements

- **統合された ID 機能強化**

  Windows Server の以前のバージョンにあったいくつかの制限に対処し、コンテナー内の統合 Windows 認証の容易さと信頼性が向上しました。

- **アプリケーション互換性の向上**

Windows ベースのアプリケーションのコンテナー化が簡単になりました。既存の **windowsservercore** イメージに対するアプリの互換性が向上しました。 その他の API 依存関係があるアプリケーション用に、**windows** という 3 つ目の基本イメージが用意されました。

- **サイズの縮小とパフォーマンスの向上**

  基本コンテナー イメージのダウンロード サイズ、ディスク上のサイズ、起動時間が向上し、コンテナー ワークフローが高速化しました。

- **Windows Admin Center を使用した管理エクスペリエンス (プレビュー)**

  Windows Admin Center の新しい拡張機能により、これまでより簡単にコンピューターで実行しているコンテナーを表示し、個々のコンテナーを管理できるようになりました。 Windows Admin Center パブリック フィードで "Containers" 拡張機能を探してください。

Compute improvements

- **VM スタート順序指定**: VM スタート順序指定も、OS とアプリケーションの対応により機能が向上しており、次の VM を起動する前に VM が起動したと見なされるときのトリガーが強化されました。

- **VM の記憶域クラス メモリのサポート**により、NTFS フォーマットの直接アクセス ボリュームを、不揮発性 DIMM 上に作成し、Hyper-V VM に公開できるようになりました。Hyper-V VM が、ストレージクラス メモリ デバイスの低待機時間パフォーマンスの恩恵を受けられるようになりました。

- **Hyper-V VM の永続メモリ サポート**: 仮想マシンで永続メモリ (ストレージ クラス メモリとも呼ばれる) の高スループットと低待機時間を利用するために、VM に直接投影できるようになりました。 永続メモリにより、データベース トランザクションの待機時間を大幅に短縮し、低待機時間メモリ内データベースの障害時に復旧までの時間を短縮できます。

- **コンテナー記憶域 - 永続データ ボリューム**: アプリケーション コンテナーからボリュームに永続的にアクセスできるようになりました。 詳細については、クラスター共有ボリューム (CSV)、記憶域スペース ダイレクト (S2D)、SMB グローバル マッピングによるコンテナー記憶域のサポートに関するブログの記事をご覧ください。

- **仮想マシン構成ファイル形式 (更新)**: 構成バージョンが 8.2 以降の仮想マシン用に VM ゲスト状態ファイル (`.vmgs`) が追加されました。 VM ゲスト状態ファイルには、これまで VM ランタイム状態ファイルの一部であったデバイス状態情報が含まれています。

Encrypted Networks

暗号化されたネットワーク - 仮想ネットワークの暗号化を使用すると、"**暗号化有効**" とマークされているサブネット内で相互に通信する仮想マシン間で、仮想ネットワーク トラフィックの暗号化が有効になります。 また、この機能は、仮想サブネットのデータグラム トランスポート層セキュリティ (DTLS) を利用して、パケットを暗号化します。 DTLS は、物理ネットワークへのアクセスを持つユーザーによる盗聴、改ざん、偽造に対する保護を提供します。

仮想ワークロードに関するネットワーク パフォーマンスの向上

仮想ワークロードに関するネットワーク パフォーマンスの改善により、仮想マシンへのネットワーク スループットが最大限に向上します。ホストの継続的な調整や過度のプロビジョニングは必要ありません。 パフォーマンスが向上したことで、利用可能なホストの密度を高めながら、運用コストとメンテナンス コストを削減できます。 これらの新機能の名前は次のとおりです。

- 動的仮想マシン マルチキュー (d.VMMQ: Dynamic Virtual Machine Multi-Queue)
- vSwitch の Receive Segment Coalescing

低遅延遅延バックグラウンドトランスポート

Low Extra Delay Background Transport (LEDBAT) は、ユーザーとアプリケーションに帯域を自動的に割り当てるように設計された、待機時間を最適化するネットワーク輻輳制御プロバイダーです。 ネットワークが使われていない間、LEDBAT は使用できる帯域幅を使います。 このテクノロジは、お客様が直接使用するサービスや関連する帯域幅に影響を与えることなく、重要で大規模な更新プログラムを IT 環境全体に展開する場合に使用することを目的としています。

Windows タイム サービス

Windows タイム サービスには、UTC に厳密に準拠したうるう秒サポート、PTP (Precision Time Protocol) と呼ばれる新しい時刻プロトコル、エンド ツー エンドのトレーサビリティが含まれています。

ハイパフォーマンス SDN ゲートウェイ

Windows Server 2019 のハイ パフォーマンス SDN ゲートウェイにより、IPsec および GRE 接続のパフォーマンスが大幅に向上し、従来よりずっと低い CPU 使用率での超高性能スループットを提供しています。

SDN の新しい展開 UI と Windows Admin Center 拡張機能

Windows Server 2019 では、新しい展開 UI と Windows Admin Center 拡張機能により、だれもが SDN の機能を活用して、簡単に展開および管理できるようになりました。

Windows Subsystem for Linux (WSL)

WSL によって、サーバーの管理者は Windows Server の Linux から既存のツールとスクリプトを使用することができます。 コマンド ラインに関するブログ で紹介された、バックグラウンド タスク、DriveFS、WSLPath などの多くの機能強化は、Windows Server の一部として含まれるようになりました。

Active Directory フェデレーション サービス

Windows Server 2019 の Active Directory フェデレーション サービス (AD FS) には、次の変更が含まれています。

保護されたサインイン

AD FS での保護されたサインインに、次の更新プログラムが含まれるようになりました。

- ユーザーは、パスワードを公開することなく、第 1 の要素としてサード パーティの認証製品を使用できるようになりました。 外部認証プロバイダーが 2 つの要素を証明できる場合は、多要素認証 (MFA) を使用できます。
- パスワード以外のオプションを最初の要素として使用した後、ユーザーはパスワードを追加要素として使用できるようになりました。 このインボックス サポートにより、GitHub アダプターのダウンロードが必要な AD FS 2016 の全体的なエクスペリエンスが向上します。
- ユーザーは、事前認証段階で特定の種類の要求をブロックするために、独自のプラグイン リスク評価モジュールを構築できるようになりました。 この機能により、ID 保護などのクラウド インテリジェンスを使用して、危険なユーザーやトランザクションをブロックすることが容易になります。 詳細については、「AD FS 2019 のリスク評価モデルを使用してプラグインをビルドする」を参照してください。
- 次の機能を追加することで、エクストラネット スマート ロックアウト (ESL) クイック修正エンジニアリング (QFE) を改善します。
    - 従来のエクストラネット ロックアウト機能によって保護されている状態で監査モードを使用できるようになりました。

- ユーザーは、使い慣れた場所に独立したロックアウトしきい値を使用できるようになりました。 この機能を使用すると、共通のサービス アカウント内でアプリの複数のインスタンスを実行して、中断を最小限に抑えてパスワードをロールオーバーできます。

その他のセキュリティの強化

AD FS 2019 には、次のセキュリティ強化が含まれています。

- SmartCard サインインを使用したリモート PowerShell を使用すると、ユーザーは PowerShell コマンドを実行して SmartCard で AD FS にリモート接続できます。 ユーザーは、このメソッドを使用して、マルチノード コマンドレットを含むすべての PowerShell 関数を管理することもできます。

- HTTP ヘッダーのカスタマイズにより、ユーザーは AD FS 応答中に作成された HTTP ヘッダーをカスタマイズできます。 ヘッダーのカスタマイズには、次の種類のヘッダーが含まれます。

  - HSTS。準拠しているブラウザーの HTTPS エンドポイントでのみ AD FS エンドポイントを使用して適用できます。

  - X フレーム オプション。AD FS 管理者は、特定の証明書利用者が AD FS 対話型サインイン ページ用の iFrame を埋め込むことができます。 このヘッダーは HTTPS ホストでのみ使用してください。

  - Future header. 複数の将来のヘッダーを構成することもできます。

  詳細については、「AD FS 2019 で HTTP セキュリティ応答ヘッダーをカスタマイズする」を参照してください。

認証とポリシーの機能

AD FS 2019 には、次の認証とポリシーの機能が含まれています。

- ユーザーは、追加認証のためにデプロイによって呼び出される認証プロバイダーを指定する規則を作成できるようになりました。 この機能は、認証プロバイダー間の移行と、追加の認証プロバイダーに対する特別な要件を持つ特定のアプリのセキュリティ保護に役立ちます。

- トランスポート層セキュリティ (TLS) ベースのデバイス認証に対するオプションの制限により、TLS を必要とするアプリケーションのみがそのデバイス認証を使用できるようになります。 ユーザーは、クライアント TLS ベースのデバイス認証を制限でき、デバイス ベースの条件付きアクセスを実行しているアプリケーションのみがその認証を使用で

きるようになります。 この機能により、TLS ベースのデバイス認証を必要としないアプリケーションに対して、デバイス認証の不要なプロンプトが表示されないようにします。

- AD FS では、第 2 要素資格情報の鮮度に基づく第 2 要素資格情報の再実行がサポートされるようになりました。 この機能を使用すると、ユーザーは最初のトランザクションに対して TFA のみを要求し、その後、定期的に 2 番目の要素のみを必要とすることができます。 この機能は、AD FS で構成可能な設定ではないため、要求に追加のパラメーターを指定できるアプリケーションでのみ使用できます。 Microsoft Entra ID は、Microsoft Entra ID フェデレーション ドメイン信頼設定で **supportsMFA** を *True* に設定するように **Remember my MFA for X Days** 設定を構成した場合に、このパラメーターをサポートします。

シングル サインオンの機能強化

AD FS 2019 には、次のシングル サインオン (SSO) の機能強化も含まれています。

- AD FS では、ページ分割された UX フローと、ユーザーに、よりスムーズなサインイン エクスペリエンスを提供する中央に配置されたユーザー インターフェイス (UI) が使用されるようになりました。 この変更は、Azure AD で提供される機能を反映しています。 新しい UI に合わせて、組織のロゴと背景画像を更新することが必要な場合があります。

- Windows 10 デバイスでプライマリ更新トークン (PRT) 認証を使用するときに MFA 状態が保持されない問題を修正しました。 ユーザーは、第 2 要素資格情報の入力を求められる頻度が低くなります。 クライアント TLS と PRT 認証でデバイス認証が成功した場合、エクスペリエンスは一貫したものになります。

最新の基幹業務アプリを構築するためのサポート

AD FS 2019 には、最新の基幹業務 (LOB) アプリの構築をサポートするための次の機能が含まれています。

- AD FS には、豊富なサインイン エクスペリエンスをサポートするために、UI サーフェス領域のないデバイスを使用してサインインするための OAuth デバイス フロー プロファイルのサポートが含まれるようになりました。 この機能を使用すると、ユーザーは別のデバイスでのサインインを完了できます。 Azure Stack の Azure コマンド ライン インターフェイス (CLI) エクスペリエンスにはこの機能が必要であり、他のシナリオでも使用できます。

- 現在の OAUth 仕様に沿った AD FS を使用するために、*Resource* パラメーターは不要です。 クライアントは、要求されたアクセス許可を持つスコープ パラメーター long として証明書利用者信頼識別子のみを指定する必要があります。

- AD FS 応答では、クロスオリジン リソース共有 (CORS) ヘッダーを使用できます。 これらの新しい見出しを使用すると、ユーザーは、クライアント側の JavaScript ライブラリが AD FS の Open ID Connect (OIDC) 検出ドキュメントから署名キーのクエリを実行して、*id_token* 署名を検証できるシングルページ アプリケーションを構築できます。

- AD FS には、OAuth 内のセキュリティで保護された認証コード フロー用の Proof Key for Code Exchange (PKCE) サポートが含まれています。 この追加のセキュリティ層により、悪意のある行為者がコードをハイジャックして別のクライアントから再実行することを防ぐことができます。

- AD FS が x5t 要求のみを送信する原因となった軽微な問題を修正しました。 AD FS では、署名検証のキー ID ヒントを示す子要求も送信されるようになりました。

Supportability improvements

管理者は、ユーザーがエラー レポートを送信し、ログをトラブルシューティング用の ZIP ファイルとしてデバッグできるように AD FS を構成できるようになりました。 管理者は、簡易メール転送プロトコル (SMTP) 接続を構成して、ZIP ファイルをトリアージ メール アカウントに自動的に送信することもできます。 別の設定では、管理者は、そのメールに基づいてサポート システムのチケットを自動的に作成できます。

Deployment updates

AD FS 2019 には、次のデプロイの更新が追加されました。

- AD FS には、Windows Server 2016 バージョンと同様の機能があり、Windows Server 2016 サーバー ファームを Windows Server 2019 サーバー ファームに簡単にアップグレードできます。 Windows Server 2016 サーバー ファームに追加された Windows Server 2019 サーバーは、アップグレードの準備ができるまで Windows Server 2016 サーバーと同様に動作します。 詳細については、「Windows Server 2016 での AD FS へのアップグレード」に関する記事を参照してください。

SAML updates

AD FS 2019 には、次のセキュリティ アサーション マークアップ言語 (SAML) 更新プログラムが含まれています。

- 次の領域で、InCommon などの集計フェデレーション サポートの問題を修正しました。
    - 集計されたフェデレーション メタデータ ドキュメント内の多くのエンティティのスケーリングが改善されました。 以前は、これらのエンティティのスケーリングは失敗し、ADMIN0017 エラー メッセージが返されます。

- PowerShell コマンドレットを実行して、`Get-AdfsRelyingPartyTrustsGroup` パラメーターを使用してクエリを実行できるようになりました。
- 重複する *entityID* 値のエラー条件の処理が改善されました。

スコープ パラメーターの Azure AD スタイル リソース仕様

以前は、AD FS では、認証要求の別のパラメーターに目的のリソースとスコープが必要でした。 たとえば、次の OAuth 要求の例にはスコープ パラメーターが含まれています。

HTTP

```
https://fs.contoso.com/adfs/oauth2/authorize?
response_type=code&client_id=claimsxrayclient&resource=urn:microsoft:adfs:claimsxr
ay&scope=oauth&redirect_uri=https://adfshelp.microsoft.com/
ClaimsXray/TokenResponse&prompt=login
```

Windows Server 2019 の AD FS では、リソース値をスコープ パラメーターに埋め込んで渡すことができます。 この変更は、Microsoft Entra ID に対する認証と一致します。

スコープ パラメーターは、各エンティティをリソースまたはスコープとして構造化するスペース区切りのリストとして編成できるようになりました。

> **注意**
>
> 認証要求で指定できるリソースは 1 つだけです。 要求に複数のリソースを含める場合、AD FS はエラーを返し、認証は成功しません。

Windows Server 2016 の新機能

2025/04/08適用対象: ✅ Windows Server 2016

この記事では、Windows Server 2016 の新機能のうち、このリリースを使用する場合に大きな影響を与える可能性が最も高い機能について、いくつか説明します。

Compute

仮想化の領域には、Windows Server を設計、展開、および保守する IT プロフェッショナル向けの仮想化製品および機能が含まれます。

General

物理マシンと仮想マシンは、Win32 の時刻と Hyper-V の時刻同期サービスが向上したことによる時刻の精度の向上を享受できます。 Windows Server は、UTC に関して 1 ms の精度を必要とする今後の規制に準拠しているサービスをホストできるようになりました。

Hyper-V

Hyper-V ネットワーク仮想化 (HNV) は、マイクロソフトの更新されたソフトウェア定義ネットワーク (SDN) ソリューションの基本的な構成要素であり、SDN スタックに完全に統合されています。 Windows Server 2016 には、Hyper-V の次の変更が含まれています。

- Windows Server 2016 に、プログラム可能な Hyper-V スイッチが追加されました。 マイクロソフトのネットワーク コントローラーは、Open vSwitch Database Management Protocol (OVSDB) を SouthBound Interface (SBI) として使用し、各ホストで実行されているホスト エージェントに HNV ポリシーをプッシュします。 ホスト エージェントは、VTEP スキーマのカスタマイズを使用してこのポリシーを保存し、Hyper-V スイッチのパフォーマンスの高いフロー エンジンに複雑なフロー ルールをプログラムします。 Hyper-V スイッチのフロー エンジンは、Azure で使用されるフロー エンジンと同じです。 ネットワーク コントローラーとネットワーク リソース プロバイダーを介した SDN スタック全体も Azure と一貫性があり、そのパフォーマンスは Azure パブリック クラウドと同等になります。 マイクロソフトのフロー エンジン内では、Hyper-V スイッチは、スイッチ内でのパケットの処理方法を定義するシンプルな一致アクション メカニズムを通じてステートレス フロー ルールとステートフル フロー ルールの両方を処理する機能を備えています。

- HNV で、Virtual eXtensible Local Area Network (VXLAN) プロトコルのカプセル化がサポートされるようになりました。 HNV は、マイクロソフト ネットワーク コントローラーを通じて MAC 配布モードの VXLAN プロトコルを使用し、テナントのネットワーク IP

アドレスを物理的なアンダーレイ ネットワーク IP アドレスにマップします。 NVGRE および VXLAN タスク オフロードは、パフォーマンスを向上させるためにサードパーティ ドライバーをサポートします。

- Windows Server 2016 には、仮想ネットワーク トラフィックおよび HNV とのシームレスな対話機能を完全にサポートするソフトウェア ロード バランサー (SLB) が含まれています。 パフォーマンスの高いフロー エンジンがデータ プレーン v-スイッチで SLB を実装した後、ネットワーク コントローラーが仮想 IP (VIP) または動的 IP (DIP) マッピング用に制御します。

- HNV は、業界標準のプロトコルに依存するサードパーティの仮想および物理アプライアンスとの相互運用性を確保するために、正しい L2 イーサネット ヘッダーを実装します。 マイクロソフトは、相互運用性を確保するため、送信されるすべてのパケットのすべてのフィールドに準拠する値があることを保証しています。 NVGRE や VXLAN などのカプセル化プロトコルによって生じるパケット オーバーヘッドを考慮に入れるため、HNV では、物理 L2 ネットワークのジャンボ フレーム (MTU > 1780) のサポートが求められています。 ジャンボ フレームのサポートにより、HNV 仮想ネットワークに接続されているゲスト仮想マシンで 1514 MTU が維持されます。

- Windows コンテナーのサポートによって、Windows 10 でパフォーマンスの向上、ネットワーク管理の簡素化、および Windows コンテナーのサポートが実現しています。 詳細については、「Windows コンテナーのドキュメントおよびコンテナー: Docker、Windows、およびトレンド」をご覧ください。

- Hyper-V は、コネクト スタンバイと互換性を持つようになりました。 Always On/Always Connected (AOAC) 電源モデルを使用するコンピューターに Hyper-V ロールをインストールする場合、接続スタンバイ電源状態を使用するように構成できるようになりました。

- 個別のデバイス割り当てにより、仮想マシン (VM) に特定の PCIe ハードウェア デバイスへの直接かつ排他的なアクセス権を与えることができます。 この機能は Hyper-V 仮想化スタックをバイパスし、アクセスを高速化します。 詳細については、「個別のデバイスの割り当ておよび個別のデバイスの割り当て - 説明と背景」を参照してください。

- Hyper-V では、第 1 世代 VM のオペレーティング システム (OS) ディスクの BitLocker ドライブ暗号化がサポートされるようになりました。 この保護方法は、第 2 世代 VM でのみ使用可能な仮想トラステッド プラットフォーム モジュール (TPM) に代わるものです。 ディスクの暗号化を解除して VM を起動するには、Hyper-V ホストが、承認済みの保護されたファブリックの一部であるか、VM のいずれかのガーディアンからの秘密キーを持っている必要があります。 キー記憶域にはバージョン 8 の VM が必要です。 詳細については、「Hyper-V の仮想マシンのバージョンをアップグレードする (Windows または Windows Server)」を参照してください。

- ホスト リソース保護は、過度なレベルのアクティビティを追跡することで、VM がシステム リソースを過度に使用することを防ぎます。 監視によって VM のアクティビティ レベルが異常に高いことが検出されると、VM が消費するリソースの量が調整されます。 この機能を有効にするには、PowerShell で Set-VMProcessor コマンドレットを実行します。

- Linux または Windows OS を実行している第 2 世代 VM で VM の実行中に、ホット 追加または削除を使用してネットワーク アダプターを追加または削除できるようになりました。 また、Windows Server 2016 以降または Windows 10 以降を実行している第 1 世代と第 2 世代の VM の両方で動的メモリが有効になっていない場合でも、VM の実行中に割り当てられるメモリの量を調整することもできます。

- Hyper-V マネージャーでは、次の機能がサポートされるようになりました。

  - 代替資格情報。これにより、別の Windows Server 2016 または Windows 10 リモート ホストに接続するときに、Hyper-V マネージャーで別の資格情報セットを使用できます。 サインインを簡単にするために、これらの資格情報を保存することもできます。

  - Windows Server 2012 R2、Windows Server 2012、Windows 8.1、Windows 8 を実行しているマシンで Hyper-V を管理できるようになりました。

  - Hyper-V マネージャーは、CredSSP、Kerberos、および NTLM 認証を利用可能な WS-MAN プロトコルを使用してリモート Hyper-V ホストと通信するようになりました。 CredSSP を使用してリモート Hyper-V ホストに接続すると、Active Directory で制約付き委任を有効にせずにライブ マイグレーションを実行できます。 WS-MAN を使用すると、ホストをリモート管理することも簡単になります。 WS-MAN はポート 80 で接続します。このポートは既定で開かれています。

- Windows ゲストの統合サービスに対する更新は、Windows Update を通じて配布されるようになりました。 サービス プロバイダーとプライベート クラウド ホストは、VM を所有するテナントに更新プログラムの適用を制御する権限を与えることができます。 Windows テナントは、単一の方法で最新の更新プログラムをすべて適用して VM をアップグレードできるようになりました。 Linux テナントが統合サービスを使用する方法の詳細については、「Windows Server と Windows 上の Hyper-v がサポートされている Linux および FreeBSD 仮想マシン」を参照してください。

  > **ⓘ 重要**
  >
  > Windows Server 2016 の Hyper-V には、vmguest.iso イメージファイルは不要になったため、含まれなくなりました。

- 第 2 世代 VM で実行されている Linux OS は、セキュア ブート オプションを有効にして起動できるようになりました。 Windows Server 2016 ホストでセキュア ブートをサポー

トする OS には、Ubuntu 14.04 以降、SUSE Linux Enterprise Server 12 以降、Red Hat Enterprise Linux 7.0 以降、CentOS 7.0 以降が含まれます。 VM を初めて起動する前に、Hyper-V マネージャー、Virtual Machine Manager、または PowerShell で Set-VMFirmware コマンドレットを実行して、Microsoft UEFI 証明機関を使用するように VM を構成する必要があります。

- 第 2 世代 VM と Hyper-V ホストでは、より多くのメモリと仮想プロセッサを使用できるようになりました。 以前のバージョンよりも多くのメモリと仮想プロセッサを備えたホストを構成することもできます。 これらの変更は、オンライン トランザクション処理 (OLTP) 用の大規模なインメモリ データベースの実行や、e コマース用のデータ ウェアハウス (DW) などのシナリオをサポートします。 詳細については、「インメモリ トランザクション処理のための Windows Server 2016 Hyper-V 大規模 VM パフォーマンス」を参照してください。 バージョンの互換性とサポートされる最大構成の詳細については、「 Windows または Windows Server の Hyper-V での仮想マシンのバージョンのアップグレード」および「Windows Serverでの Hyper-V スケーラビリティの計画」を参照してください。

- 入れ子になった仮想化機能を使用すると、VM を Hyper-V ホストとして使用し、仮想化ホスト内に VM を作成できます。 この機能を使用すると、Intel VT-x 対応プロセッサを搭載した Windows Server 2016 または Windows 10 以降を実行する開発環境およびテスト環境を構築できます。 詳細については、「入れ子になった仮想化の概要」を参照してください。

- 運用ワークロードを実行している VM のサポート ポリシーに準拠するように運用チェックポイントを設定できるようになりました。 これらのチェックポイントは、保存された状態ではなく、ゲスト デバイス内のバックアップ技術に基づいて実行されます。 Windows VM はボリューム スナップショット サービス (VSS) を使用し、Linux VM はファイル システム バッファーをフラッシュしてファイル システムと一貫性のあるチェックポイントを作成します。 代わりに標準チェックポイントを使用することで、保存状態に基づくチェックポイントを引き続き使用できます。 詳細については、「Hyper-V で標準または運用チェックポイントを選択する」を参照してください。

  > **重要**
  >
  > 新しい VM は、既定で運用チェックポイントを使用します。

- ダウンタイムなしでゲスト クラスタリング用に共有仮想ハードディスク (`.vhdx` ファイル) のサイズを変更できるようになりました。 また、災害復旧用の Hyper-V レプリカを使用して、ゲスト クラスターで共有仮想ハードディスクを保護することもできます。 この機能は、Windows Management Instrumentation (WMI) を介してレプリケーションを有効にしたゲスト クラスター内のコレクションでのみ使用できます。 詳細については、

「Msvm_CollectionReplicationService クラス」および「仮想ハードディスク共有の概要」を参照してください。

> ⓘ **注意**
>
> PowerShell コマンドレットまたは WMI インターフェイスを使用してコレクションのレプリケーションを管理することはできません。

- 単一の仮想マシンをバックアップする場合、ホストがクラスター化されているかどうかに関係なく、VM グループまたはスナップショット コレクションを使用することはお勧めしません。 これらのオプションは、共有 vhdx を使用するゲスト クラスターをバックアップすることを目的としています。 代わりに、Hyper-V WMI プロバイダー (V2) を使用してスナップショットを作成することをお勧めします。

- ホストまたはマルウェアの Hyper-V 管理者がシールドされた VM の状態を検査または改ざんできないようにする機能を含むシールドされた Hyper-V VM を作成できるようになりました。 これらの機能は、シールドされた VM の状態からデータの盗難からも保護します。 データと状態は暗号化されるため、Hyper-V 管理者はビデオ出力や使用可能なディスクを確認できません。 また、ホスト ガーディアン サーバーが正常で信頼できると判断したホストでのみ実行するように VM を制限することもできます。 詳細については、保護されたファブリックとシールドされた VM の概要に関するページをご覧ください。

  > ⓘ **注意**
  >
  > シールドされた VM は Hyper-V レプリカと互換性があります。 シールドされた仮想マシンをレプリケートするには、レプリケートするホストがそのシールドされた VM を実行することを承認する必要があります。

- クラスター化された仮想マシンの起動順序の優先順位機能を使用すると、どのクラスター化された仮想マシンを最初に起動または再起動するかをより細かく制御できます。 起動順序の優先順位を決定すると、サービスを提供する VM を、それらのサービスを利用する VM を起動する前に起動できます。 New-ClusterGroupSet、Get-ClusterGroupSet、Add-ClusterGroupSetDependency などの PowerShell コマンドレットを使用して、セットを定義し、セットに VM を追加し、依存関係を指定できます。

- VM 構成ファイルでは、 `.vmcx` ファイル拡張子形式が使用され、ランタイム状態データ ファイルでは、 `.vmrs` ファイル拡張子形式が使用されます。 これらの新しいファイル形式は、より効率的な読み取りと書き込みを念頭に置いて設計されています。 更新された形式により、ストレージ障害が発生した場合でもデータが破損する可能性が低くなります。

> **ⓘ 重要**
>
> `.vmcx` ファイル名拡張子はバイナリー ファイルであることを示します。 Windows Server 2016 では、`.vmcx` または `.vmrs` ファイルの編集はサポートされていません。

- バージョン 5 VM とのバージョン互換性を更新しました。 これらの VM は、Windows Server 2012 R2 と Windows Server 2016 の両方と互換性があります。 ただし、Windows Server 2019 と互換性のあるバージョン 5 VM は、Windows Server 2012 R2 ではなく、Windows Server 2016 でのみ実行できます。 Windows Server 2012 R2 VM を、それ以降のバージョンの Windows Server を実行しているサーバーに移動またはインポートする場合は、それ以降のバージョンの Windows Server の機能を使用するために、VM 構成を手動で更新する必要があります。 バージョンの互換性と更新された機能の詳細については、「Hyper-V の仮想マシンのバージョンをアップグレードする (Windows または Windows Server)」を参照してください。

- Device Guard や Credential Guard などの第 2 世代 VM の仮想化ベースのセキュリティ機能を使用して、OS をマルウェアの攻撃から保護できるようになりました。 これらの機能は、バージョン 8 以降を実行している VM で利用できます。 詳細については、「Hyper-V の仮想マシンのバージョンをアップグレードする (Windows または Windows Server)」を参照してください。

- VMConnect またはリモート PowerShell の代わりに、Windows PowerShell Direct を使用してコマンドレットを実行し、ホストマシンから VM を構成できるようになりました。 使用を開始するために、ネットワークやファイアウォールの要件を満たす必要も、特別なリモート管理構成をする必要もありません。 詳細については、「PowerShell Direct で Windows 仮想マシンを管理する」を参照してください。

Nano Server

Nano Server には、Nano Server イメージをビルドするための更新されたモジュールが含まれるようになりました。 この更新プログラムは、物理ホストとゲスト仮想マシンの機能をより分離し、さまざまな Windows Server エディションのサポートを追加します。 詳細については、「Nano Server のインストール」を参照してください。

回復コンソールにも、受信と送信のファイアウォール ルールの分離、WinRM 構成を修復する機能などの機能強化があります。

シールドされた仮想マシン

Windows Server 2016 には、不正に使用されているファブリックから 第 2 世代仮想マシンを保護することを目的として、Hyper-V ベースのシールドされた仮想マシンが用意されています。 Windows Server 2016 で導入された主な機能には、次のようなものがあります。

- 新しい [**暗号化のサポート**] モード。これは、通常の仮想マシンよりも強化された (ただし、 [**シールド**] モードよりは弱い) 保護を提供する一方で、vTPM、ディスクの暗号化、ライブ マイグレーション トラフィックの暗号化、およびその他の機能 (仮想マシンのコンソール接続や PowerShell ダイレクトなどの便利な直接ファブリック管理機能を含む) を引き続きサポートします。

- 自動化されたディスクの暗号化を含め、既存のシールドされていない第 2 世代仮想マシンからシールドされた仮想マシンへの変換を完全にサポートします。

- Hyper-V Virtual Machine Manager では、シールドされた仮想マシンの実行が許可された時点でファブリックを表示できるようになりました。このため、ファブリック管理者はこの方法で、シールドされた仮想マシンのキーの保護機能 (KP) を開き、仮想マシンの実行を許可されているファブリックを表示することができます。

- 実行中のホスト ガーディアン サービスの構成証明モードを切り替えることができます。安全性が低い一方で単純な Active Directory ベースの構成証明と、TPM ベースの構成証明をその場で切り替えることができるようになりました。

- 保護された Hyper-V ホストとホスト ガーディアン サービスの両方の構成で誤りやエラーを検出できる Windows PowerShell ベースのエンド ツー エンドの診断ツール。

- シールドされた仮想マシン自体と同じレベルの保護機能を提供しながら、通常実行されるファブリック内のシールドされた仮想マシンを安全にトラブルシューティングし、修復をするための手段を提供する回復環境。

- ホスト ガーディアン サービスによる既存の安全な Active Directory のサポート。独自の Active Directory インスタンスを作成するのではなく、既存の Active Directory フォレストを Active Directory として使用するようにホスト ガーディアン サービスに対して指示できます。

シールドされた仮想マシンの操作の詳細および手順については、「保護されたファブリックとシールドされた VM」を参照してください。

ID およびアクセス

ID での新機能では、組織が Active Directory 環境をセキュリティで保護する機能が強化され、クラウドのみの展開およびハイブリッドの展開に移行するために役立ちます。ハイブリッドの展開では、一部のアプリケーションとサービスはクラウドでホストされ、それ以外はオンプレミスでホストされます。

Active Directory 証明書サービス

Windows Server 2016 の Active Directory 証明書サービス (AD CS) では、TPM キーの構成証明のサポートが強化されます。キーの構成証明にスマート カード KSP を使用でき、ドメインに参加していないデバイスで NDES の登録を使用して、TPM にあるキーを証明できる証明書を取得できるようになりました。

特権アクセス管理

特権アクセス管理 (PAM) は、Pass-the-Hash、スピア フィッシングなどの資格情報の盗難技術によって引き起こされる Active Directory 環境のセキュリティ上の懸念を軽減するのに役立ちます。 この新しい管理アクセス ソリューションは、Microsoft Identity Manager (MIM) を使用して構成することができ、次の機能が導入されています。

- MIM によってプロビジョニングされた bastion の Active Directory フォレストには、既存のフォレストとの特別な PAM 信頼があります。 Bastion フォレストは、既存のフォレストから分離され、特権アカウントへのアクセスのみを許可するため、悪意のあるアクティビティがない新しい種類の Active Directory 環境です。

- 要求を承認するための新しいワークフローなど、管理者特権を要求する MIM の新しいプロセス。

- 管理特権の要求に応じて MIM によって bastion フォレストにプロビジョニングされる、新しいシャドウ セキュリティのプリンシパル、またはグループ。 シャドウ セキュリティ グループには、既存フォレスト内の管理グループの SID を参照する属性があります。これにより、シャドウ グループは、アクセス制御リスト (ACL) を変更することなく、既存のフォレスト内にあるリソースにアクセスできます。

- ユーザーが指定した期間、シャドウ グループに一時的に参加し、管理タスクを実行できるようにする、期限切れのリンク機能。 メンバーシップ期間は、有効期限 (TTL) 値によって制御され、Kerberos チケットの有効期間も決定されます。

  > ⓘ **注意**
  >
  > リンクの期限切れは、リンクされたすべての属性で使用できます。 ただし、グループとユーザー間のリンクされた *member/memberOF* 属性リレーションシップのみが、有効期限付きリンク機能を使用するために PAM で事前設定されています。

- Kerberos ドメイン コントローラー (KDC) の組み込みの機能強化により、Active Directory ドメイン コントローラーは、ユーザーの管理者グループに期間限定のメンバーシップが複数設定されている場合に、Kerberos チケットの有効期間を可能な限り最小の Time to Live (TTL) 値に制限できます。 たとえば、ユーザーが期限付きグループ **A** のメンバーだ

とします。サインオンすると、Kerberos チケット保障チケット (TGT) の有効期間は、そのユーザーがグループ **A** に対して持っている残り時間と等しくなります。同じユーザーが、グループ **A** よりも TTL が短い別の期限付きグループ **B** にも参加している場合、TGT の有効期間は、そのユーザーがグループ **B** に対して持っている残り時間と等しくなります。

- アクセスを要求したユーザー、管理者に付与されたアクセス権、およびサインインしたユーザーや管理者によって実行されたアクティビティを識別できる新しい監視機能。

PAM の詳細については、「Active Directory ドメイン サービスの特権アクセス管理」を参照してください。

Microsoft Entra に参加

Microsoft Entra への参加は、会社のデバイスと個人のデバイスの機能を強化するだけでなく、企業、ビジネス、教育機関のお客様の ID エクスペリエンスも強化します。

- 最新の設定が、企業所有の Windows デバイスで利用できるようになりました。Windows のコア機能を使用するのに個人用の Microsoft アカウントは必要なくなり、既存の職場アカウントを使用して実行し、コンプライアンスを確保できるようになりました。 これらのサービスは、オンプレミスの Windows ドメインに参加している PC、および Microsoft Entra に参加している PC とデバイスで機能します。 設定は次のとおりです。
  - ローミングまたは個人用設定、アクセシビリティ設定、および資格情報
  - バックアップと復元
  - 職場アカウントを使用した Microsoft Store へのアクセス
  - ライブ タイルと通知
- 会社所有のデバイスか BYOD (Bring Your Own Device) かを問わず、電話やタブレットなど、Windows ドメインに参加できないモバイル デバイスで組織のリソースにアクセスできます。
- Office 365 およびその他の組織のアプリ、Web サイト、リソースにシングル サインオン (SSO) を使用できます。
- BYOD デバイスで、オンプレミス ドメインまたは Azure AD から個人所有のデバイスに職場アカウントを追加できます。 SSO を使用すると、条件付きアカウント制御やデバイス正常性構成証明などの新機能に準拠しながら、アプリを使用して、または Web 上で、職場のリソースにアクセスできます。

- モバイル デバイス管理 (MDM) 統合を使用すると、モバイル デバイス管理 (MDM) ツール (Microsoft Intune またはサード パーティ製) にデバイスを自動登録できます。
- 組織内の複数のユーザーに対してキオスク モードと共有デバイスを設定できます。
- 開発者エクスペリエンスでは、共有プログラミング スタックを使用して会社と個人の両方のコンテキストに対応するアプリをビルドできます。
- イメージング オプションを使用すると、イメージングか、ユーザーが最初の実行エクスペリエンスで会社所有デバイスを直接構成することを許可するかを選択できます。

Windows Hello for Business

Windows Hello for Business は、組織およびコンシューマー向けの、パスワードを超えるキーベースの認証方法です。 この形式の認証は、侵害、盗難、フィッシングに抵抗できる資格情報に依存します。

ユーザーは、証明書または非対称キー ペアにリンクされた生体認証または PIN を使用してデバイスにサインインします。 ID プロバイダー (IDP) は、ユーザーの公開キーを IDLocker にマッピングしてユーザーを検証し、One Time Password (OTP)、電話、または別の通知メカニズムを介してサインイン情報を提供します。

詳細については、「Windows Hello for Business」を参照してください。

ファイル レプリケーション サービス (FRS) と Windows Server 2003 の機能レベルの非推奨

ファイル レプリケーション サービス (FRS) と Windows Server 2003 の機能レベルは、以前のバージョンの Windows Server では非推奨でしたが、AD DS では Windows Server 2003 オペレーティング システムはサポートされなくなりました。 Windows Server 2003 を実行するすべてのドメイン コントローラーを、ドメインから削除する必要があります。 また、ドメインとフォレストの機能レベルを少なくとも Windows Server 2008 に上げる必要があります。

Windows Server 2008 以上のドメイン機能レベルでは、AD DS は分散ファイル サービス (DFS) レプリケーションを使用して、ドメイン コントローラー間で SYSVOL フォルダーの内容をレプリケートします。 Windows Server 2008 ドメイン機能レベル以上で新しいドメインを作成した場合、DFS レプリケーションは SYSVOL フォルダーを自動的にレプリケートします。 それより低い機能レベルでドメインを作成した場合は、SYSVOL フォルダーのレプリケーションを FRS から DFS に移行する必要があります。 移行手順の詳細については、「インストール、アップグレード、または Windows Server への移行」を参照してください。

詳細については、次のリソースを参照してください。

- Active Directory Domain Services (AD DS) の機能レベルとは
- Active Directory ドメインとフォレストの機能レベルを上げる方法

Active Directory フェデレーション サービス

Windows Server 2016 の Active Directory フェデレーション サービス (AD FS) には、ライトウェイト ディレクトリ アクセス プロトコル (LDAP) ディレクトリに格納されているユーザーを認証するよう AD FS を構成できる新機能が追加されています。

Web アプリケーション プロキシ

Web アプリケーション プロキシの最新バージョンでは、より多くのアプリケーションの発行と事前認証を可能にする新機能に力を入れており、ユーザー エクスペリエンスの向上が図られています。 SharePoint アプリの発行を容易にするために、Exchange ActiveSync やワイルドカード ドメインなどのリッチ クライアント アプリの事前認証を含む新機能の完全な一覧を確認してください。 詳細については、「Web Application Proxy in Windows Server 2016 (Windows Server 2016 の Web アプリケーション プロキシ)」を参照してください。

Administration

管理と自動化の領域では、Windows PowerShell など Windows Server 2016 を実行および管理する IT プロフェッショナル向けのツールとリファレンス情報に焦点を合わせています。

Windows PowerShell 5.1 に追加された重要な新機能には、クラスを使った開発のサポートや新しいセキュリティ機能があります。それらの機能により、用途が広がり、使いやすさが向上し、Windows ベースの環境をより簡単かつ包括的に制御して管理できます。 詳細については、「WMF 5.1 の新しいシナリオと機能」を参照してください。

Windows Server 2016 には、Nano Server で PowerShell.exe を実行する機能 (リモートのみではなくなりました)、GUI に代わる新しいローカル ユーザーとグループのコマンドレット、PowerShell デバッグのサポートの追加、セキュリティ ログとトランスクリプションおよび JEA に対するサポートの Nano Server への追加など、新しい追加機能があります。

次に、その他の新しい管理機能を示します。

Windows Management Framework (WMF) 5 の PowerShell Desired State Configuration (DSC)

Windows Management Framework 5 には、Windows PowerShell Desired State Configuration (DSC)、Windows リモート管理 (WinRM)、および Windows Management Instrumentation (WMI) に対する更新が含まれています。

Windows Management Framework 5 の DSC 機能のテストに関する詳細については、PowerShell DSC の機能の検証 に関する一連のブログ記事を参照してください。 ダウンロードするには、Windows Management Framework 5.1 に関するページを参照してください。

PackageManagement 統合パッケージ管理によるソフトウェアの検出、インストール、およびインベントリ

Windows Server 2016 および Windows 10 には、新しい PackageManagement 機能 (旧称 OneGet) が含まれています。この機能により、IT 技術者や DevOps は、インストーラーのテクノロジやソフトウェアの配置場所にかかわらず、ソフトウェアの検出、インストール、およびインベントリ (SDII) をローカルまたはリモートで自動化できます。

詳細については、「https://github.com/OneGet/oneget/wiki 」を参照してください。

デジタル法科学を支援し、セキュリティ侵害の減少に役立つ PowerShell の機能強化

セキュリティが侵害されたシステムの調査を担当するチーム ("ブルー チーム" とも呼ばれます) を支援するために、PowerShell にログおよびその他のデジタル法科学機能が追加されたほか、スクリプトの脆弱性を減らし (制約付きの PowerShell など)、CodeGeneration API をセキュリティで保護するのに役立つ機能が追加されました。

詳細については、ブログ記事「PowerShell ♥ the Blue Team 」を参照してください。

ネットワーク

ネットワークの領域では、IT プロフェッショナルが Windows Server 2016 を設計、展開、保守するためのネットワーク製品および機能を扱っています。

Software-Defined Networking

ソフトウェア定義ネットワーク (SDN) は、次の機能を含む新しいソフトウェア定義データセンター (SDDC) ソリューションです。

- ネットワーク コントローラー。これを使用すると、ネットワーク デバイスとサービスを手動で構成しなくても、ネットワーク インフラストラクチャの構成を自動化できます。ネットワーク コントローラーは、北向きインターフェースで Representational State Transfer (REST) を使用し、JavaScript Object Notation (JSON) ペイロードを処理します。ネットワーク コントローラーの southbound インターフェイスでは、Open vSwitch のデータベース管理プロトコル (OVSDB) が使用されます。

- Hyper-V の新機能:
  - Hyper-V 仮想スイッチ。これを使用すると、分散切り替えと分散ルーティング、および Microsoft Azure に合わせて配置され、互換性もあるポリシー適用レイヤーを作成できます。 詳細については、「Hyper-V 仮想スイッチ」を参照してください。
  - 仮想スイッチを作成するときのリモート ダイレクト メモリ アクセス (RDMA) とスイッチ埋め込みチーミング (SET)。 SET を既に使用しているかどうかに関係なく、Hyper-V 仮想スイッチにバインドされたネットワーク アダプターに RDMA を設定できます。 SET を使用すると、仮想スイッチに NIC チーミングと同様の機能を提供できます。 詳細については、「Azure ローカルのホスト ネットワーク要件 」を参照してください。
  - 仮想マシン マルチキュー (VMMQ) は、VM ごとに複数のハードウェアキューを割り当てることで VMQ スループットを向上させます。 既定のキューは VM のキューのセットとなり、キュー間でトラフィックを分散します。
  - ソフトウェア定義ネットワークのサービス品質 (QoS) は、既定クラスの帯域幅内の仮想スイッチを通過するトラフックの既定クラスを管理します。
- ネットワーク関数仮想化 (NFV)。これを使用すると、ハードウェア アプライアンスによって実行されるネットワーク機能を、ロード バランサー、ファイアウォール、ルーター、スイッチなどの仮想アプライアンスにミラーリングまたはルーティングできます。 System Center Virtual Machine Manager を使用して、SDN スタック全体をデプロイおよび管理することもできます。 Docker を使用して Windows Server コンテナー ネットワーキングを管理し、SDN ポリシーを仮想マシンとコンテナーの両方と関連付けることができます。
- きめ細かなアクセス制御リスト (ACL) を備えたデータセンター ファイアウォール。VM インターフェイス レベルまたはサブネット レベルでファイアウォール ポリシーを適用できます。 詳細については、「データセンターのファイアウォールとは」を参照してください。
- RAS ゲートウェイ。これを使用すると、クラウド データセンターからテナントのリモート サイトへのサイト間 VPN 接続など、仮想ネットワークと物理ネットワークの間でトラフィックをルーティングできます。 Border Gateway Protocol (BGP) を使用すると、インターネット キー交換バージョン 2 (IKEv2) のサイト間仮想プライベート ネットワーク (VPN)、レイヤー 3 (L3) VPN、汎用ルーティング カプセル化 (GRE) ゲートウェイなど、すべてのゲートウェイ シナリオでネットワーク間に動的ルーティングをデプロイおよび提供できます。 ゲートウェイでは、ゲートウェイ プールと M+N 冗長性もサポートされるようになりました。 詳細については、「ソフトウェア定義ネットワーク用のリモート アクセス サービス (RAS) ゲートウェイとは」を参照してください。

- ソフトウェア ロード バランサー (SLB) とネットワーク アドレス変換 (NAT)。Direct Server Return をサポートしてスループットを向上させます。 これにより、戻りのネットワーク トラフィックは負荷分散マルチプレクサーをバイパスでき、南北および東西のレイヤー 4 ロード バランサーと NAT を使用して実現できます。 詳細については、「SDN のソフトウェア ロード バランサー (SLB) とは」および「ネットワーク機能の仮想化」を参照してください。

- データ プレーンで動作し、Virtual Extensible LAN (VxLAN) と Network Virtualization Generic Routing Encapsulation (NVGRE) の両方をサポートする柔軟なカプセル化テクノロジ。

詳細については、「ソフトウェア定義ネットワーク インフラストラクチャを計画する」を参照してください。

クラウド スケールの基礎

Windows Server 2016 には、次のクラウド スケールの基礎が含まれています。

- コンバージド ネットワーク インターフェイス カード (NIC)。これを使用すると、1 つのネットワーク アダプターを使用して管理、リモート ダイレクト メモリ アクセス (RDMA) 対応ストレージ、およびテナント トラフィックに対応できます。 コンバージド NIC を使用すると、サーバーごとに異なる種類のトラフィックを管理するために必要なネットワーク アダプターの数が少なくなるため、データセンター内の各サーバーのコストが削減されます。

- パケット ダイレクトは、高いネットワーク トラフィックのスループットと待機時間の短いパケット処理インフラストラクチャを提供します。

- スイッチ埋め込みチーミング (SET) は、Hyper-V 仮想スイッチに統合されている NIC チーミング ソリューションです。 SET を使用すると、最大 8 つの物理 NIC を 1 つの SET チームにまとめることができるため、可用性が向上し、フェイルオーバーが可能になります。 Windows Server 2016 では、サーバー メッセージ ブロック (SMB) と RDMA の使用に制限されている SET チームを作成できます。 また、SET チームを使用して、Hyper-V ネットワーク仮想化のネットワーク トラフィックを分散することもできます。 詳細については、「Azure ローカルのホスト ネットワーク要件 」を参照してください。

TCP パフォーマンスの向上

既定の初期輻輳ウィンドウ (ICW) が 4 から 10 に増加し、TCP Fast Open (TFO) が実装されています。 TFO により TCP 接続の確立に必要な時間が短縮されるほか、ICW の増加により、初期バーストでさらに大きなオブジェクトを転送できるようになりました。 この組み合わせによ

り、クライアントとクラウドの間でインターネット オブジェクトを転送するのに必要な時間をさらに短くできます。

パケット損失からの復旧時の TCP 動作を改善するために、TCP Tail Loss Probe (TLP) と Recent Acknowledge (RACK) が実装されます。 TLP は、再転送タイムアウト (RTO) を高速回復に変換する際に役立ちます。また、RACK は高速回復の所要時間を短縮し、損失パケットを再転送します。

動的ホスト構成プロトコル (DHCP)

動的ホスト構成プロトコル (DHCP) には、Windows Server 2016 に次の変更が加えられています。

- Windows 10 バージョン 2004 以降では、Windows クライアントを実行中に、テザリングされた Android デバイスを使用してインターネットに接続すると、接続は従量制としてラベル付けされるようになりました。 特定の Windows デバイスで MSFT 5.0 と表示されていた従来のクライアント ベンダー名は、MSFT 5.0 XBOX になりました。

- Windows 10 バージョン 1803 以降、DHCP クライアントでは、システムが接続する DHCP サーバーからオプション 119 (ドメイン検索オプション) を読み取って適用できるようになりました。 ドメイン検索オプションでは、短い名前の DNS 検索用にドメイン ネーム サービス (DNS) のサフィックスも使用できます。 詳細については、RFC 3397 を参照してください。

- DHCP でオプション 82 (サブオプション 5) がサポートされるようになりました。 このオプションを使用すると、DHCP プロキシ クライアントとリレー エージェントが特定のサブネットの IP アドレスを要求できます。 DHCP オプション 82 (サブオプション 5) で構成された DHCP リレー エージェントを使用している場合、リレー エージェントは特定の IP アドレス範囲から DHCP クライアントの IP アドレス リースを要求できます。 詳細については、「DHCP サブネットの選択オプション」を参照してください。

- DNS サーバーで DNS レコードの登録が失敗するシナリオに対する新しいログ イベント。 詳細については、「DNS 登録の DHCP ログ イベント」を参照してください。

- DHCP サーバーのロールでは、ネットワーク アクセス保護 (NAP) がサポートされなくなりました。 DHCP サーバーでは NAP ポリシーが適用されず、DHCP スコープは NAP を有効できません。 NAP クライアントでもある DHCP クライアント コンピューターでは、正常性ステートメント (SoH) と DHCP 要求を送信します。 DHCP サーバーで Windows Server 2016 が実行されている場合、これらの要求は SoH が存在しない場合と同様に処理されます。 DHCP サーバーでは、通常の DHCP リースをクライアントに付与します。 Windows Server 2016 を実行しているサーバーが、NAP をサポートするネットワーク ポリシー サーバー (NPS) に認証要求を転送するリモート認証ダイヤルイン ユーザー サービス (RADIUS) プロキシである場合、NPS ではこれらのクライアントが NAP 非

対応と評価されるため、NAP 処理は失敗します。 NAP と NAP の非推奨の詳細については、「Windows Server 2012 R2 で削除された機能または非推奨にされた機能」を参照してください。

GRE tunneling

RAS ゲートウェイでは、サイト間接続用の高可用性 Generic Routing Encapsulation (GRE) トンネルと、ゲートウェイの M+N 冗長性がサポートされるようになりました。 GRE は軽量のトンネリング プロトコルで、インターネット プロトコル インターネットワークを介して Point-to-Point 仮想リンク内のさまざまなネットワーク レイヤー プロトコルをカプセル化します。 詳細については、「Windows Server 2016 の GRE トンネリング」を参照してください。

IP アドレス管理 (IPAM) に関するページ

IPAM には、次の更新プログラムがあります。

- 強化された IP アドレス管理。 IPv4 /32 および IPv6 /128 サブネットの処理や、IP アドレス ブロック内の空き IP アドレスのサブネットと範囲の検索などのシナリオで、IPAM 機能が改善されました。

- `Find-IpamFreeSubnet` コマンドレットを実行して、割り当てに使用できるサブネットを見つけることができるようになりました。 この関数はサブネットを割り当てず、可用性のみを報告します。 ただし、コマンドレットの出力を `Add-IpamSubnet` コマンドレットにパイプしてサブネットを作成することはできます。 詳細については、「Find-IpamFreeSubnet」を参照してください。

- `Find-IpamFreeRange` コマンドレットを実行して、IP ブロック内で使用可能な IP アドレス範囲、プレフィックスの長さ、および要求されたサブネットの数を検索できるようになりました。 このコマンドレットは IP アドレス範囲の割り当ては行わず、可用性を報告するだけです。 ただし、出力を `AddIpamRange` コマンドレットにパイプして範囲を作成することはできます。 詳細については、「Find-IpamFreeRange」を参照してください。

- 強化された DNS サービス管理:

  - DNSSEC 以外の DNS サーバーの DNS リソース レコード コレクション。

  - DNSSEC 以外のすべての種類のリソース レコードに対するプロパティと操作の構成。

  - ドメインに参加している Active Directory 統合 DNS サーバーとファイル格納 DNS サーバーの両方に対する DNS ゾーン管理。 プライマリ ゾーン、セカンダリ ゾーン、スタブ ゾーンなど、すべての種類の DNS ゾーンを管理できます。

    - 前方参照ゾーンと逆引き参照ゾーンのどちらであるかに関係なく、セカンダリ ゾーンとスタブ ゾーンでタスクをトリガーします。
    - レコードとゾーンでサポートされている DNS 構成に対するロールベースのアクセス制御。
    - Conditional forwarders

- 統合 DNS、DHCP、IP アドレス (DDI) の管理。 IP アドレス インベントリの IP アドレスに関連付けられている DNS リソース レコードをすべて表示できるようになりました。また、IP アドレスのポインター (PTR) レコードを自動的に保持し、DNS 操作と DHCP 操作の両方の IP アドレスライフサイクルを管理することもできます。
- 複数の Active Directory フォレストのサポート。 IPAM をインストールしたフォレストと各リモート フォレストとの間に双方向の信頼関係がある場合、IPAM を使用して複数の Active Directory フォレストの DNS サーバーと DHCP サーバーを管理できます。 詳細については、「複数の Active Directory フォレスト内のリソースを管理する」を参照してください。
- 使用率データ消去機能を使用すると、古い IP 使用率データを削除して IPAM データベースのサイズを削減できます。 日付を指定するだけで、IPAM は、ユーザーが入力した日付およびその日付以前のデータベース エントリをすべて削除します。 詳細については、「使用率データを消去する」を参照してください。
- ロールベースのアクセス制御 (RBAC) を使用して、PowerShell で IPAM オブジェクトのアクセス スコープを定義できるようになりました。 詳細については、「Windows PowerShell で役割ベースのアクセス制御を管理する」および「Windows PowerShell での IP アドレス管理 (IPAM) サーバー コマンドレット」を参照してください。

詳細については、次を参照してください。 IPAM の管理します。

セキュリティおよび保証

セキュリティおよび保証の領域には、IT プロフェッショナルがデータ センターとクラウド環境に展開するセキュリティ ソリューションおよび機能が含まれます。 Windows Server 2016 でのセキュリティについては、「セキュリティおよび保証」を参照してください。

Just Enough Administration (JEA)

Windows Server 2016 の JEA は、Windows PowerShell で管理できるあらゆるものに対して委任された管理を可能にするセキュリティ テクノロジです。 機能には、ネットワーク ID での実行、PowerShell ダイレクト経由での接続、JEA エンドポイントとの間での安全なファイル

コピー、既定で JEA コンテキストで起動する PowerShell コンソールの構成のサポートが含まれます。 GitHub の詳細については、「GitHub の JEA」を参照してください。

Credential Guard

Credential Guard は、特権を持つシステム ソフトウェアだけがシークレットにアクセスできるように、仮想化ベースのセキュリティを使用してシークレットを分離します。 詳細については、次を参照してください。 派生した資格情報 Guard でのドメイン資格情報を保護するです。

Windows Server 2016 用の Credential Guard には、サインイン済みユーザー セッションに関する次の更新プログラムが含まれています。

- Kerberos および New Technology LAN Manager (NTLM) は、仮想化ベースのセキュリティを使用し、サインイン済みユーザー セッションの Kerberos および NTLM シークレットを保護します。
- 資格情報マネージャーは、仮想化ベースのセキュリティを使用して保存されたドメイン資格情報を保護します。 サインイン済み資格情報と保存済みドメイン資格情報は、リモート デスクトップを使用してリモート ホストに渡されません。
- Unified Extensible Firmware Interface (UEFI) ロックを使用せずに Credential Guard を有効にすることができます。

リモート資格情報ガード

Credential Guard では RDP セッションがサポートされるため、ユーザーの資格情報はクライアント側に保持されたままで、サーバー側では公開されません。 また、リモート デスクトップにシングル サインオンも提供します。 詳しくは、「Windows Defender Credential Guard によるドメインの派生資格情報の保護」を参照してください。

Windows Server 2016 用の Remote Credential Guard には、サインイン済みユーザーに関する次の更新プログラムが含まれています。

- Remote Credential Guard は、サインイン済みユーザー資格情報の Kerberos および NTLM シークレットをクライアント デバイスに保持します。 ネットワーク リソースをユーザーとして評価するためのリモート ホストからの認証要求では、クライアント デバイスがシークレットを使用する必要があります。
- Remote Credential Guard は、リモート デスクトップの使用時に提供されたユーザー資格情報を保護します。

Domain protections

ドメイン保護には、Active Directory ドメインが必要になりました。

PKInit フレッシュネス拡張機能のサポート

Kerberos クライアントは、公開キー ベースのサインオンに対して PKInit フレッシュネス拡張機能を試みるようになりました。

KDC により PKInit Freshness Extension がサポートされるようになりました。 ただし、既定では PKInt フレッシュネス拡張機能は提供されません。

詳細については、「RFC 8070 PKInit フレッシュネス拡張機能の Kerberos クライアントと KDC のサポート」を参照してください。

公開キーのみのユーザーの NTLM シークレットをロールする

Windows Server 2016 ドメイン機能レベル (DFL) 以降、DC で、公開キーのみのユーザーの NTLM シークレットのローリングがサポートされるようになりました。 この機能は、下位ドメイン機能レベル (DFL) では使用できません。

> ⚠ **警告**
>
> NTLM シークレットのローリングをサポートしている、2016 年 11 月 8 日より前に有効になった DC をドメインに追加すると、DC がクラッシュする可能性があります。

新しいドメインの場合、この機能は既定で有効になっています。 既存のドメインの場合、Active Directory 管理センターで構成する必要があります。

Active Directory 管理センターで、左側のウィンドウでドメインを右クリックし、[**プロパティ**] を選択します。 [**対話型ログオンに Windows Hello for Business またはスマート カードを使用する必要があるユーザーに対して、サインオン時に期限切れの NTLM シークレットのローリングを有効にする**] チェック ボックスをオンにします。 その後、[OK] を選択してこの変更を適用します。

ユーザーが特定のドメイン参加済みデバイスに制限されている場合にネットワーク NTLM の許可する

DC では、Windows Server 2016 DFL 以降でユーザーが特定のドメイン参加デバイスに制限されている場合、ネットワーク NTLM の許可をサポートできるようになりました。 この機能は、Windows Server 2016 より前の OS を実行している DFL では使用できません。

この設定を構成するには、認証ポリシーで [**ユーザーが選択したデバイスに制限されている場合に、NTLM ネットワーク認証を許可する**] をオンにします。

詳細については、「認証ポリシーと認証ポリシー サイロ」を参照してください。

Device Guard (コードの整合性)

Device Guard は、サーバーで実行できるコードを指定するポリシーを作成することで、カーネル モードのコードの整合性 (KMCI) とユーザー モードのコードの整合性 (UMCI) を提供します。 「Windows Defender Device Guard の概要: 仮想化ベースのセキュリティとコードの整合性ポリシー」を参照してください。

Windows Defender

Windows Server 2016 用 Windows Defender の概要。 Windows Server マルウェア対策は、Windows Server 2016 では既定でインストールされ、有効になっていますが、Windows Server マルウェア対策のユーザー インターフェイスはインストールされていません。 ただし、Windows Server マルウェア対策はマルウェア対策の定義を更新し、ユーザー インターフェイスなしでコンピューターを保護します。 Windows Server マルウェア対策のユーザー インターフェイスが必要な場合は、役割と機能の追加ウィザードを使用して、OS のインストール後にインストールできます。

制御フロー ガード

制御フロー ガード (CFG) は、メモリ破損の脆弱性に対処するために作成されたプラットフォームのセキュリティ機能です。 詳細については、「Control Flow Guard (制御フロー ガード)」を参照してください。

Storage

Windows Server 2016 の記憶域には、ソフトウェア定義ストレージと従来のファイル サーバーのための新機能と拡張機能が含まれています。

記憶域スペース ダイレクト

記憶域スペース ダイレクトでは、ローカル記憶域を持つサーバーを使用して高可用性を備えた拡張性の高い記憶域を作成できます。 ソフトウェア定義ストレージ システムの展開と管理を簡素化し、SATA SSD や NVMe ディスク デバイスなどの新しいクラスのディスク デバイスを使用できるようにします。これは、以前の共有ディスクを使用したクラスター化された記憶域スペースでは利用できませんでした。

詳細については、「 記憶域スペース ダイレクト」を参照してください。

Storage Replica

記憶域レプリカは、障害復旧のためのサーバーやクラスタ間で、ストレージにとらわれないブロックレベルの同期レプリケーションを可能にし、サイト間のフェイルオーバー クラスターのストレッチを可能にします。 同期レプリケーションは、クラッシュ前後の整合性が維持されるボリュームを使用した物理サイト内のデータのミラーリングを実現して、ファイル システム レベルでデータがまったく失われないようにします。 非同期レプリケーションでは、データが失われる可能性はありますが、大都市圏の範囲を超えてサイトを拡張できます。

詳細については、記憶域レプリカに関する記事を参照してください。

記憶域のサービスの品質 (QoS)

記憶域のサービスの品質 (QoS) を使用して、Windows Server 2016 でエンド ツー エンドの記憶域のパフォーマンスを一元的に監視すると共に、Hyper-V クラスターと CSV クラスターを使用してポリシーを作成できるようになりました。

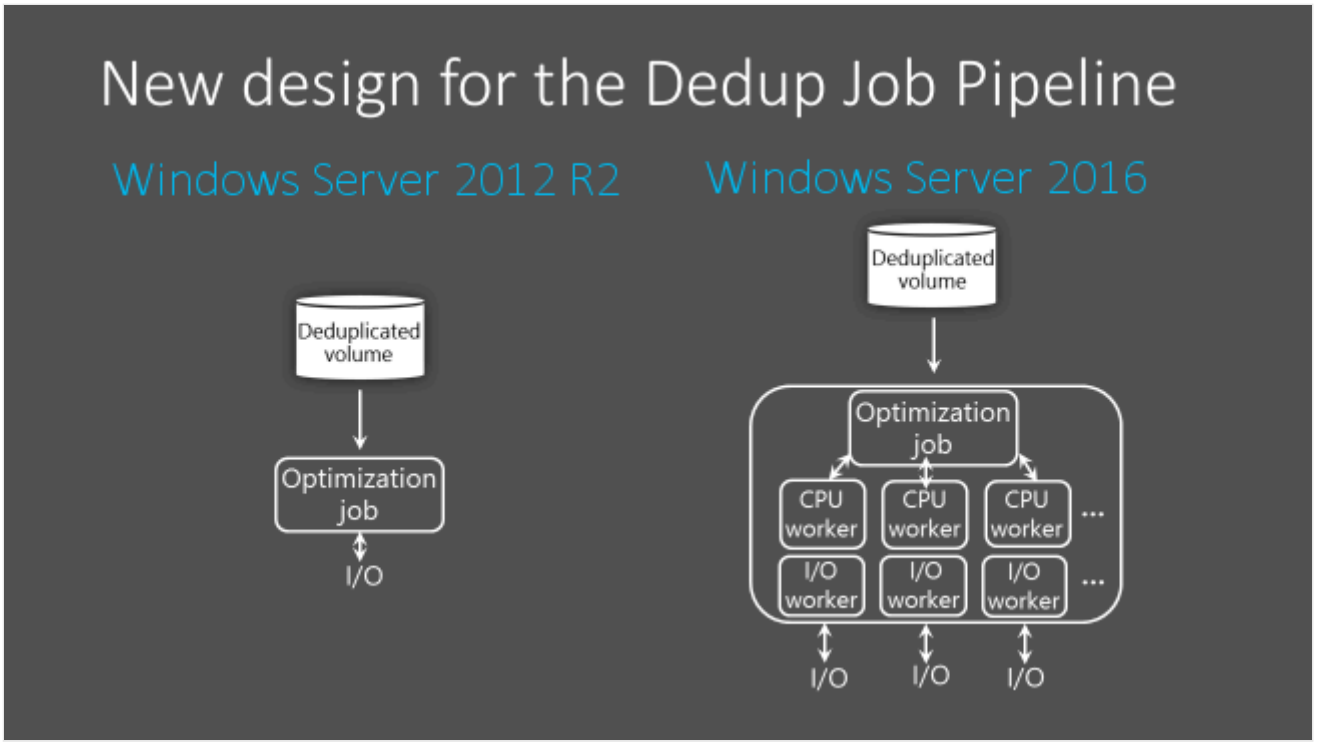
詳細については、「記憶域のサービスの品質」を参照してください。

Data deduplication

Windows Server 2016 には、データ重複除去のための次の新機能が含まれています。

大量ボリュームのサポート

Windows Server 2016 以降、データ重複除去ジョブのパイプラインでは、ボリュームごとに多数の I/O キューを使用して複数のスレッドを並列実行するようになりました。 この変更により、以前はデータを複数の小さなボリュームに分割することでのみ可能だったレベルにまで、パフォーマンスを向上させることができます。 これらの最適化は、最適化ジョブだけでなく、すべてのデータ重複除去ジョブに適用されます。 次の図は、Windows Server のバージョン間でパイプラインがどのように変化したかを示しています。



これらのパフォーマンスの向上により、Windows Server 2016 では、データ重複除去は最大 64 TB のボリュームでハイ パフォーマンスを発揮します。

大容量ファイルのサポート

Windows Server 2016 以降、データ重複除去では、新しいストリーム マップ構造とその他の改良を活用して、最適化のスループットとアクセス パフォーマンスを向上させています。 重複除去処理パイプラインでは、最初からやり直すのではなく、フェールオーバー シナリオの後に最適化を再開することもできます。 この変更により、最大 1 TB のファイルのパフォーマンスが向上し、管理者は、さまざまなワークロード (バックアップ ワークロードに関連付けられている大きなファイルなど) に重複除去による削減分を適用できますす。

Nano Server のサポート

Nano Server は、Windows Server 2016 のヘッドレス展開オプションであり、必要なシステム リソースのフットプリントがはるかに小さく、起動速度が速く、Windows Server Core の展開オプションよりも少ない更新プログラムと再起動が必要です。 Nano Server ではデータ重複除去も完全にサポートされています。 Nano Server の詳細については、「コンテナーの基本イメージ」を参照してください。

仮想化バックアップ アプリケーションの構成の簡略化

Windows Server 2016 以降では、仮想化されたバックアップ アプリケーションのシナリオのデータ重複除去が大幅に簡略化されています。 このシナリオは、定義済みの [使用法の種類] オプションになりました。 重複除去設定を手動で調整する必要はなくなり、General Purpose

ファイル サーバーや仮想デスクトップ インフラストラクチャ (VDI) と同様に、ボリュームの重複除去を有効にするだけです。

クラスター OS ローリング アップグレードのサポート

データ重複除去を実行している Windows Server フェールオーバー クラスターでは、Windows Server 2012 R2 バージョンと Windows 2016 バージョンの重複除去を実行しているノードを混在させることができます。 この混合モード クラスター機能により、クラスターのローリング アップグレード中に重複除去されたすべてのボリュームに完全なデータ アクセスが提供されます。 以降のバージョンのデータ重複除去を、以前のバージョンの Windows Server を実行しているクラスターにダウンタイムなしで段階的にロールアウトできるようになりました。

Hyper-V でローリング アップグレードも使用できるようになりました。 Hyper-V クラスターのローリング アップグレードを使用すると、Windows Server 2012 R2 を実行しているノードを含む Hyper-V クラスターに、Windows Server 2019 または Windows Server 2016 を実行しているノードを追加できるようになりました。 新しいバージョンの Windows Server を実行しているノードを追加した後、ダウンタイムなしでクラスターの残りの部分をアップグレードできます。 クラスター内のすべてのノードをアップグレードし、PowerShell で Update-ClusterFunctionalLevel を実行してクラスターの機能レベルを更新するまで、クラスターは Windows Server 2012 R2 の機能レベルで実行されます。 ローリング アップグレード プロセスの動作方法の詳細な手順については、「クラスター オペレーティング システムのローリング アップグレード」を参照してください。

> ⓘ **注意**
>
> Windows 10上のHyper-Vはフェールオーバー クラスタリングをサポートしていません。

SYSVOL と NETLOGON 接続に関する SMB セキュリティ強化の向上

Windows 10 および Windows Server 2016 では、Active Directory ドメイン サービスへのクライアント接続では、既定でドメイン コントローラー上の SYSVOL および NETLOGON 共有が使用されていました。 現在、これらの接続には、Kerberos などのサービスを使用した SMB 署名と相互認証が必要です。 SMB 署名と相互認証が使用できない場合、Windows 10 または Windows Server 2016 コンピューターはドメイン ベースのグループ ポリシーとスクリプトを処理しません。 この変更により、デバイスは中間者攻撃から保護されます。

> ⓘ **注意**

これらの設定のレジストリ値は既定では存在しませんが、セキュリティ強化の規則は、グループ ポリシーまたはその他のレジストリ値でオーバーライドされるまで引き続き適用されます。

これらのセキュリティ強化の詳細については、「MS15-011: グループポリシーの脆弱性」および「MS15-011 & MS15-014: グループ ポリシーの強化」を参照してください。

Work Folders

Windows Server 2016 では、ワーク フォルダー サーバーが Windows Server 2016 を実行し、ワーク フォルダー クライアントが Windows 10 である場合の変更通知が改善されています。ファイルの変更がワーク フォルダー サーバーに同期されると、サーバーは直ちに Windows 10 クライアントに通知し、ファイルの変更を同期するようになりました。

ReFS

新しい ReFS では、データの信頼性、回復性、スケーラビリティを実現し、さまざまなワークロードに対応した大規模な記憶域の展開がサポートされます。

ReFS では、以下の点が強化されています。

- 新しいストレージ層機能により、パフォーマンスが向上し、次のようなストレージ容量が増加します。
  - パフォーマンス層でのミラーリングとキャパシティ層でのパリティを使用して、同じ仮想ディスク上で複数の回復性タイプを実現します。
  - 変動するワーキング セットに対する応答性を向上。
- `.vhdx` チェックポイントのマージ操作などの VM 操作のパフォーマンスを向上させるために、ブロックのクローン作成を導入しています。
- 損傷した記憶域を回復し、重大な破損からデータを救出するのに役立つ新しい ReFS スキャンツール。

Failover Clustering

Windows Server 2016には、フェールオーバークラスタリング機能を使用して、複数のサーバーを1つのフォールトトレラントクラスタにグループ化するための多くの新機能と機能強化が含まれています。

Cluster Operating System Rolling Upgrade (クラスター オペレーティング システムのローリング アップグレード)

クラスター オペレーティング システムのローリング アップグレードを使用すると、管理者はクラスター ノードの OS を Windows Server 2012 R2 から Windows Server 2016 にアップグレードでき、Hyper-V または Scale-Out ファイル サーバーのワークロードを停止する必要はありません。 この機能を使用すると、サービス レベル アグリーメント (SLA) のダウンタイムに対するペナルティを回避できます。

詳細については、「クラスター オペレーティング システムのローリング アップグレード」を参照してください。

Cloud witness

クラウド監視は、Microsoft Azure を仲裁ポイントとして活用する Windows Server 2016 の新しい種類のフェールオーバー クラスター クォーラム監視です。 クラウド監視は、他のクォーラム監視と同様に投票を取得し、クォーラム計算に参加できます。 クラスター クォーラムの構成ウィザードを使用して、クラウド監視をクォーラム監視として構成できます。

詳細については、「クォーラム監視をデプロイする」を参照してください。

仮想マシンの回復性

Windows Server 2016 には、コンピューティング クラスターのクラスター内通信の問題を削減できるように仮想マシン (VM) コンピューティングの回復性向上が含まれています。 この回復性の向上には、次の更新プログラムが含まれます。

- 次のオプションを構成して、一時的な障害時の VM の動作を定義できるようになりました。
    - **回復性レベル**は、デプロイで一時的な障害を処理する方法を定義します。
    - **回復性期間**は、すべての VM を分離して実行できる期間を定義します。
- 異常なノードは隔離され、クラスタに参加できなくなります。 この機能により、異常なノードが他のノードやクラスター全体に悪影響を及ぼすのを防ぎます。

コンピューティングの回復性機能の詳細については、「Windows Server 2016 の仮想マシンのコンピューティングの回復性」を参照してください。

Windows Server 2016 の VM には、一時的なストレージ障害を処理するための新しいストレージ回復性機能も含まれています。 回復性の向上は、ストレージの中断が発生した場合にテナント VM セッションの状態を維持するのに役立ちます。 VM は、基になるストレージから切

断されると一時停止し、ストレージが回復するのを待ちます。 一時停止中、VM はストレージ障害発生時に実行されていたアプリケーションのコンテキストを保持します。 VM とストレージの間の接続が復元されると、VM は実行中の状態に戻ります。 その結果、テナント コンピューターのセッション状態は回復時の状態に保持されます。

新しいストレージ回復性機能は、ゲスト クラスターにも適用されます。

Diagnostic improvements

フェールオーバー クラスターに関する問題を診断するために、Windows Server 2016 には次のものが含まれています。

- タイム ゾーン情報や DiagnosticVerbose ログなどのクラスター ログ ファイルに対するいくつかの機能強化により、フェールオーバー クラスタリングの問題のトラブルシューティングが容易になります。 詳細については、「Windows Server 2016 のフェールオーバー クラスターでのトラブルシューティングの機能強化 - クラスター ログ」を参照してください。

- 新しい種類のアクティブ メモリ ダンプでは、VM に割り当てられているほとんどのメモリ ページが除外されるため、memory.dmp ファイルのサイズが小さくなり、保存やコピーが簡単になります。 詳細については、「Windows Server 2016 のフェールオーバー クラスターでのトラブルシューティングの機能強化 - アクティブ ダンプ」を参照してください。

サイト認識フェールオーバー クラスター

Windows Server 2016 には、物理的な場所 (サイト) に基づいてストレッチ クラスター内のグループ ノードを有効にするサイト認識フェールオーバー クラスターが含まれています。 クラスターがサイトを認識することによって、フェールオーバーの動作、配置ポリシー、ノード間のハートビート、クォーラムの動作といった、クラスター ライフサイクルでの主な操作が拡張されます。 詳細については、「Windows Server 2016 のサイト認識フェールオーバー クラスター」を参照してください。

ワークグループ クラスターとマルチドメイン クラスター

Windows Server 2012 R2 以前では、同じドメインに参加しているメンバー ノード間でのみクラスターを作成できます。 Windows Server 2016 では、この障壁が取り除かれて、Active Directory の依存関係のないフェールオーバー クラスターを作成する機能が導入されています。 次の構成でフェールオーバー クラスターを作成できるようになりました。

- すべてのノードが同じドメインに参加している、単一ドメイン クラスター。

- 異なるドメインのメンバーであるノードを持つ、マルチドメイン クラスター。
- ドメインに参加していないメンバー サーバーまたはワークグループであるノードを持つ、ワークグループ クラスター。

詳細については、「Windows Server 2016 のワークグループ クラスターとマルチドメイン クラスター」を参照してください。

仮想マシンの負荷分散

仮想マシンの負荷分散は、フェールオーバー クラスタリングの新機能で、クラスター内のノード間で VM の負荷をシームレスに分散します。 この機能は、ノード上の VM メモリと CPU 使用率に基づいて、オーバーコミットしているノードを識別します。 次に、オーバーコミットしているノードから、使用可能な帯域幅を持つノードに VM をライブ移行します。 最適なクラスターのパフォーマンスと使用率を確保するために、この機能でノードのバランスを積極的に取るよう調整できます。 Windows Server 2016 テクニカル プレビューでは、負荷分散は既定で有効になっています。 ただし、SCVMM 動的最適化が有効になっている場合、負荷分散は無効になります。

仮想マシンの開始順序

仮想マシンの開始順序はフェールオーバー クラスタリングの新機能で、クラスター内の VM とその他のグループの開始順序に関するオーケストレーション機能になります。 VM を層にグループ化し、異なる層間で開始順序の依存関係を作成できるようになりました。 これらの依存関係に基づき、ドメイン コントローラーやユーティリティ VM など、最も重要な VM が最初に起動します。 優先順位が低い層のVMは、依存しているVMが起動してからでないと開始されません。

簡略化された SMB マルチチャネルと複数 NIC のクラスター ネットワーク

フェールオーバー クラスター ネットワークでは、サブネットごとまたはネットワークごとに 1 つのネットワーク インターフェイス カード (NIC) という制限がなくなりました。 簡素化されたサーバー メッセージ ブロック (SMB) のマルチチャネルおよびマルチ NIC のクラスター ネットワークを使用すると、ネットワーク構成が自動的に行われ、サブネット上のすべての NIC をクラスターとワークロードのトラフィックに使用できます。 この機能強化により、ユーザーは、Hyper-V、SQL Server フェールオーバー クラスター インスタンス、およびその他の SMB ワークロードのネットワーク スループットを最大化することができます。

詳細については、「簡略化された SMB マルチチャネルと複数 NIC のクラスター ネットワーク」を参照してください。

Application development

インターネット インフォメーション サービス (IIS) 10.0

Windows Server 2016 の IIS 10.0 Web サーバーにより提供される新機能は以下のとおりです。

- ネットワーク スタックでの HTTP/2 プロトコルのサポート。IIS 10.0 と統合されたため、IIS 10.0 Web サイトはサポートされる構成の HTTP/2 要求を自動的に処理できるようになりました。 これにより、接続の効率的な再利用、待機時間の短縮など、多くの機能強化が HTTP/1.1 に加えられ、Web ページの読み込み時間が短縮されます。
- Nano Server での IIS 10.0 の実行および管理機能。 「Nano Server の IIS」を参照してください。
- ワイルドカード ホスト ヘッダーのサポート。管理者は、ドメイン向けに Web サーバーをセットアップし、Web サーバーが任意のサブドメインの要求を処理するように設定できます。
- IIS を管理するための新しい PowerShell モジュール (IISAdministration)。

詳細については、 IIS を参照してください。

分散トランザクション コーディネーター (MSDTC)

Microsoft Windows 10 と Windows Server 2016 に 3 つの新機能が追加されました。

- Resource Manager Rejoin の新しいインターフェイスは、データベースがエラーのために再起動された後に未確定トランザクションの結果を調べるために、リソース マネージャーによって使されます。 詳細については、「IResourceManagerRejoinable::Rejoin」を参照してください。

- DSN 名の制限が 256 バイトから 3072 バイトに拡張されました。 詳細については、「IDtcToXaHelperFactory::Create」、「IDtcToXaHelperSinglePipe::XARMCreate」、または「IDtcToXaMapper::RequestNewResourceManager」を参照してください。

- Tracelogファイル名にイメージファイルのパスを含めるようにレジストリキーを設定することで、どのTracelogファイルをチェックするのかがわかるようになりました。 MSDTC のトレースの構成に関する詳細については、「Windows ベースのコンピューター上の MS DTC の診断トレースを有効にする方法 」を参照してください。

DNS Server

Windows Server 2016には、ドメイン・ネーム・システム（DNS）サーバーに関する以下の更新が含まれています。

DNS policies

DNS ポリシーを構成して、DNS サーバーが DNS クエリにどのように応答するかを指定できます。 クライアントのIPアドレス、時間帯、その他いくつかのパラメータに基づいてDNS応答を設定することができます。 DNSポリシーは、ロケーションアウェアDNS、トラフィック管理、ロードバランシング、スプリットブレインDNS、その他のシナリオを可能にします。 詳細については、DNS ポリシーのシナリオに関するガイドを参照してください。

RRL

DNSサーバーで応答速度制限（RRL）を有効にすると、悪意のあるシステムがDNSサーバーを使用してDNSクライアントに分散型サービス拒否（DDoS）攻撃を仕掛けるのを防ぐことができます。 RRLは、DNSサーバーが一度に多くのリクエストに応答するのを防ぎます。これは、ボットネットがサーバーの運用を妨害するために一度に複数のリクエストを送信するシナリオにおいて、DNSサーバーを保護します。

DANE support

DNS-based Authentication of Named Entities（DANE）サポート（>RFC6394 と RFC6698）を使用して、DNSサーバーでホストされているドメイン名に対して、DNSクライアントがどの認証局からの証明書を期待するかを指定できます。 これは、悪意のある行為者がDNSキャッシュを破壊し、DNS名を自分のIPアドレスに向けるという、一種の中間者攻撃を防ぐものである。

不明なレコードのサポート

DNSサーバーが明示的にサポートしていないレコードを追加するには、不明レコード機能を使用します。 レコードが不明なのは、DNSサーバーがそのRDATA形式を認識しない場合である。 Windows Server 2016は不明レコードタイプ（RFC 3597）をサポートしているため、バイナリー・オンワイヤー形式でWindows DNSサーバーゾーンに不明レコードを追加できます。 ウィンドウズ・キャッシュ・リゾルバはすでに不明レコードタイプを処理できます。 Windows DNSサーバーは不明レコードに対してレコード固有の処理を行わないが、受け取ったクエリに応答してレコードを送信することができます。

IPv6 ルート ヒント

Windows DNSサーバーは、インターネット割り当て番号機関（IANA）によって公開されたIPv6ルートヒントを含むようになりました。 IPv6ルートヒントのサポートにより、IPv6ルートサーバーを使用して名前解決を実行するインターネットクエリーを行うことができます。

Windows PowerShell のサポート

Windows Server 2016には、PowerShellでDNSを構成するために使用できる新しいコマンドが含まれています。 詳細については、Windows Server 2016 DnsServer モジュールおよびWindows Server 2016 DnsClient モジュールを参照してください。

ファイルベースの DNS に対する Nano Server でのサポート

Windows Server 2016 の DNS サーバーを Nano Server イメージにデプロイできます。 このデプロイ オプションは、ファイルベースの DNS を使用している場合に使用可能です。 Nano Server イメージで DNS サーバーを実行すると、フットプリントを削減し、起動を高速化し、パッチ適用を最小限に抑えて DNS サーバーを実行できます。

> ⓘ **注意**
>
> Nano Server では、Active Directory 統合 DNS はサポートされていません。

DNS client

DNS クライアント サービスでは、複数のネットワーク インターフェイスを持つコンピューターのサポートが強化されました。

マルチホーム コンピューターでは、DNS クライアント サービス バインドを使用してサーバーの解決を改善することもできます。

- 特定のインターフェイスで構成された DNS サーバーを使用して DNS クエリを解決するとき、DNS クライアントはクエリを送信する前にインターフェイスにバインドします。このバインドにより、DNS クライアントは名前解決を行う必要があるインターフェイスを指定し、ネットワーク インターフェイス経由でアプリケーションおよび DNS クライアント間の通信を最適化できます。

- 使用している DNS サーバーが、名前解決ポリシー テーブル (NRPT) のグループ ポリシー設定によって指定される場合、DNS クライアント サービスは指定されたインターフェイスにバインドされません。

> ⓘ **注意**
>
> Windows 10 の DNS クライアント サービスへの変更点は、Windows Server 2016 以降を実行しているコンピューターでも見られます。

リモート デスクトップ サービス

リモート デスクトップ サービス (RDS) は、Windows Server 2016 に対して次の変更を行いました。

App compatibility

RDS と Windows Server 2016 は、多くの Windows 10 アプリケーションと互換性があり、物理デスクトップとほぼ同じユーザー エクスペリエンスを作成します。

Azure SQL Database

リモート デスクトップ (RD) 接続ブローカーは、接続状態やユーザー ホスト マッピングなど、すべてのデプロイ情報を共有 Azure 構造化照会言語 (SQL) データベースに格納できるようになりました。 この機能を使用すると、SQL Server Always On 可用性グループを使用しなくても高可用性環境を使用できます。 詳細については、「高可用性環境のリモート デスクトップ接続ブローカーでの Azure SQL DB の使用」を参照してください。

Graphical improvements

Hyper-V の個別のデバイス割り当てを使用すると、ホスト マシン上のグラフィックス処理装置 (GPU) を仮想マシン (VM) に直接マップできます。 VM で提供できるよりも多くの GPU を必要とする VM 上のアプリケーションは、代わりにマップされた GPU を使用できます。 また、OpenGL 4.4、OpenCL 1.1、4K 解像度、Windows Server VM のサポートなど、RemoteFX vGPU も改善されました。 詳細については、「個別のデバイス割り当て」を参照してください。

RD 接続ブローカーの機能強化

ユーザーからの高サインイン要求の期間であるログオン ストーム中に RD 接続ブローカーが接続を処理する方法が改善されました。 RD 接続ブローカーは、10,000 を超える同時サインイン要求を処理できるようになりました。 また、メンテナンスの改善により、サーバーをオンラインに戻す準備ができたら、すぐに環境にサーバーを追加し直すことができるため、デプロイに対するメインテナントを簡単に実行できます。 詳細については、「リモート デスクトップ接続ブローカー パフォーマンスの強化」に関する記事を参照してください。

RDP 10 プロトコルの変更

リモート デスクトップ プロトコル (RDP) 10では、ビデオとテキストの両方で最適化される H.264/AVC 444 コーデックが使用されるようになりました。 このリリースには、ペンのリモ

ート処理のサポートも含まれています。 これらの機能を使用すると、リモート セッションの操作感がローカル セッションのようになります。 詳しくは、「Windows 10 および Windows Server 2016 における RDP 10 AVC/H.264 の機能強化」を参照してください。

個人セッション用デスクトップ

個人用セッション デスクトップは、お客様の個人用デスクトップをクラウドでホストする新しい機能です。 管理特権と専用セッション ホストにより、ユーザーがリモート デスクトップをローカル デスクトップと同様に管理するという複雑なホスティング環境が解消されます。 詳細については、「個人用セッション デスクトップ」を参照してください。

Kerberos authentication

Windows Server 2016 には、Kerberos 認証に関する次の更新プログラムが含まれています。

公開キー信頼ベースのクライアント認証に対する KDC のサポート

キー配布センター (KDC) で公開キー マッピングがサポートされるようになりました。 アカウントの公開キーをプロビジョニングする場合、KDC では、そのキーを明示的に使用する Kerberos PKInit がサポートされます。 証明書の検証が行われないため、Kerberos では自己署名証明書がサポートされていますが、認証メカニズムの保証はサポートされません。

キー信頼を使用するように構成したアカウントでは、UseSubjectAltName 設定の構成方法に関係なく、キー信頼のみが使用されます。

RFC 8070 PKInitフレッシュネス拡張機能に対するKerberosクライアントとKDCのサポート

Windows 10 バージョン 1607 および Windows Server 2016 以降では、Kerberos クライアントは、公開キーベースのサインオンに RFC 8070 PKInit フレッシュネス拡張機能 を使用できます。 KDC では PKInit フレッシュネス拡張機能が既定で無効になっているため、有効にするには、ドメイン内のすべての DC で PKInit フレッシュネス拡張機能の KDC 管理用テンプレート ポリシーに KDC サポートを構成する必要があります。

このポリシーには、ドメインが Windows Server 2016 ドメイン機能レベル (DFL) にある場合に使用できる次の設定があります。

- **無効**: KDC は PKInit Freshness 拡張機能を提供せず、鮮度を確認せずに有効な認証要求を受け入れる必要があります。 ユーザーには、新しい公開キー ID の SID は提供されません。

- **サポート対象**: Kerberos は、要求に応じて PKInit フレッシュネス拡張機能をサポートします。 Kerberos クライアントが PKInit Freshness 拡張機能で正常に認証されると、新しい公開キー ID SID を受け取ります。
- **必須**: 認証を成功させるには、PKInit Freshness 拡張機能が必要です。 PKInit フレッシュネス拡張機能がサポートされない Kerberos クライアントでは、公開キー資格情報を使用すると常に失敗します。

公開キーを使用した認証に対するドメイン参加デバイスのサポート

ドメイン参加デバイスが、バインドされた公開キーを Windows Server 2016 ドメイン コントローラー (DC) に登録できる場合、デバイスは Windows Server 2016 DC に対する Kerberos PKInit 認証を使用して公開キーで認証できます。

Windows Server 2016 ドメイン コントローラーに登録されたバインド済み公開キーを持つドメイン参加デバイスは、Kerberos Public Key Cryptography for Initial Authentication (PKInit) プロトコルを使用して Windows Server 2016 ドメイン コントローラーに対して認証できるようになりました。 詳細については、「ドメインに参加しているデバイスの公開キー認証」を参照してください。

キー配布センター (KDC) では、Kerberos キー信頼を使用した認証がサポートされるようになりました。

詳細については、「キー信頼アカウント マッピングの KDC サポート」を参照してください。

Kerberos クライアントでは、サービス プリンシパル名 (SPN) で IPv4 アドレスと IPv6 アドレスのホスト名が許可されます

Windows 10 バージョン 1507 および Windows Server 2016 以降では、SPN で IPv4 と IPv6 のホスト名をサポートするように Kerberos クライアントを構成できます。 詳細については、「IP アドレスの Kerberos の構成」を参照してください。

SPN で IP アドレスのホスト名のサポートを構成するには、TryIPSPN エントリを作成します。 既定では、このエントリはレジストリに存在しません。 このエントリは、次のパスに配置する必要があります。

```text
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters
```

エントリを作成したら、その DWORD 値を 1 に変更します。 この値が構成されていない場合、Kerberos は IP アドレスのホスト名を試行しません。

Kerberos 認証は、SPN が Active Directory に登録されている場合にのみ成功します。

キー信頼アカウント マッピングの KDC サポート

ドメイン コントローラーでは、SAN の動作で、キー信頼アカウント マッピングと、既存の AltSecID およびユーザー プリンシパル名 (UPN) へのフォールバックがサポートされるようになりました。 UseSubjectAltName 変数は、次の設定に構成できます。

- 変数を 0 に設定すると、明示的なマッピングが必要になります。 ユーザーは、キー信頼を使用するか、ExplicitAltSecID 変数を設定する必要があります。
- 変数を既定値の 1 に設定すると、暗黙的なマッピングが可能になります。
    - Windows Server 2016 以降でアカウントのキー信頼を構成すると、KDC ではマッピングに KeyTrust が使用されます。
    - SAN に UPN がない場合、KDC は AltSecID を使用してマッピングを試みます。
    - SAN に UPN がある場合、KDC はUPN を使用してマッピングを試みます。

Active Directory フェデレーション サービス (AD FS)

Windows Server 2016 用 AD FS には、次の更新プログラムが含まれています。

Microsoft Entra 多要素認証によるサインイン

AD FS 2016 は、Windows Server 2012 R2 の AD FS の多要素認証 (MFA) 機能に基づいて構築されています。 ユーザー名またはパスワードの代わりに、Microsoft Entra 多要素認証コードのみを要求するサインオンを許可できるようになりました。

- Microsoft Entra 多要素認証をプライマリ認証方法として構成している場合、AD FS はユーザー名と Azure Authenticator アプリからのワンタイム パスワード (OTP) コードの入力をユーザーに求めます。
- Microsoft Entra 多要素認証をセカンダリ認証または追加の認証方法として構成している場合、ユーザーはプライマリ認証の資格情報を提供します。 ユーザーは、Windows 統合認証を使用してサインインできます。この場合、ユーザー名とパスワード、スマート カード、またはユーザー証明書もしくはデバイス証明書が求められる可能性があります。 次に、テキスト、音声、OTP ベースの Microsoft Entra 多要素認証サインインなどのセカンダリ資格情報の入力を求めるプロンプトが表示されます。

- 新しい組み込みの Microsoft Entra 多要素認証アダプターでは、AD FS を使用した Microsoft Entra 多要素認証の簡単なセットアップと構成を利用できます。
- 組織は、オンプレミスの Microsoft Entra 多要素認証サーバーを必要とせずに、Microsoft Entra 多要素認証を使用できます。
- イントラネット用やエクストラネット用に、またはアクセス制御ポリシーの一部として、Microsoft Entra 多要素認証を構成できます。

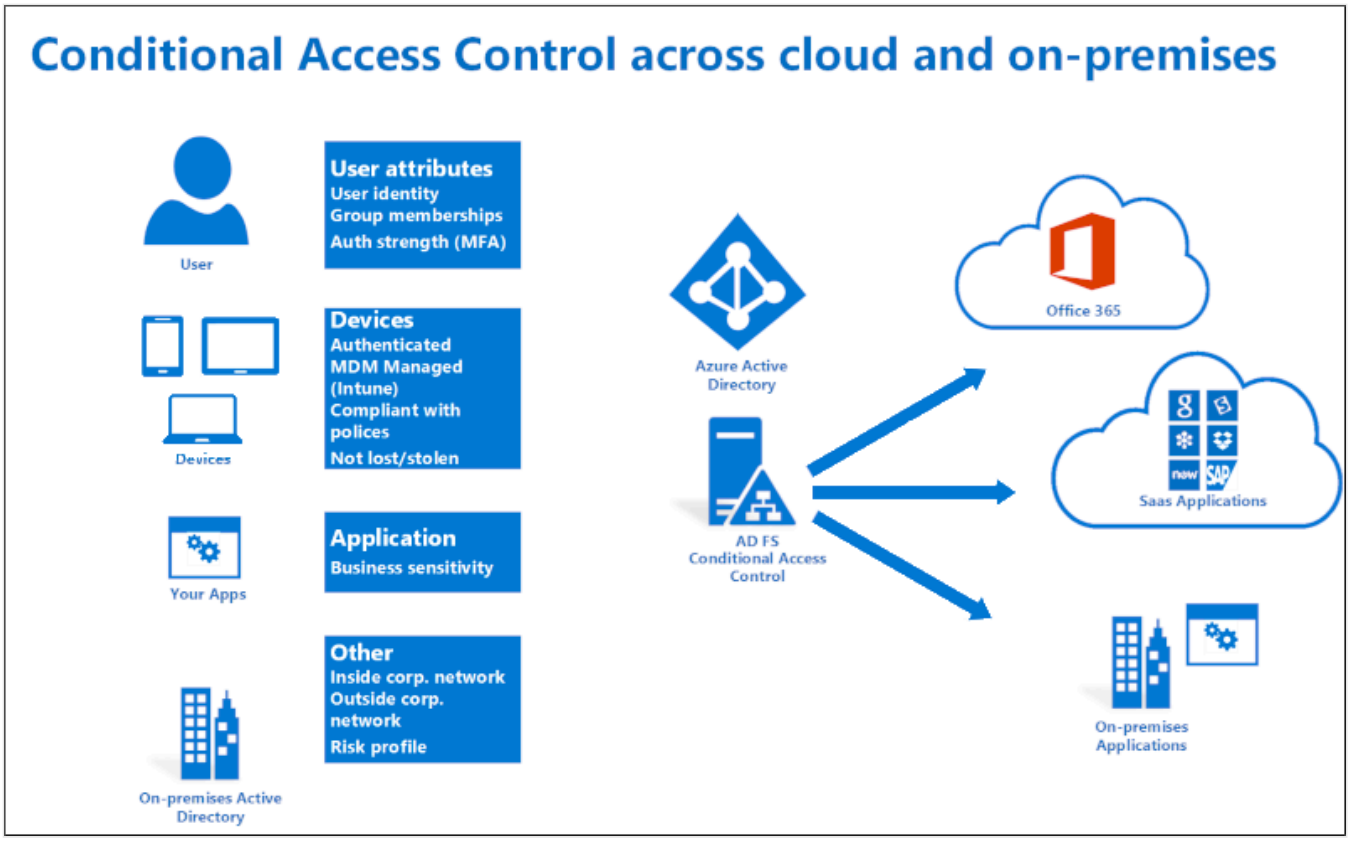
AD FS を使用した Microsoft Entra 多要素認証の詳細については、「AD FS 2016 と Microsoft Entra 多要素認証の構成」を参照してください。

準拠デバイスからのパスワードレス アクセス

AD FS 2016 は、デバイスのコンプライアンス状態に基づいてサインオンとアクセス制御を有効にする、以前のデバイス登録機能に基づいて構築されています。 ユーザーはデバイス資格情報を使用してサインオンできます。AD FS は、デバイスの属性が変更されるたびにコンプライアンスを再評価し、ポリシーが適用されていることを確認できます。 この機能により、次のポリシーが有効になります。

- マネージド デバイスまたは準拠しているデバイスからのアクセスのみを有効にします。
- マネージド デバイスまたは準拠しているデバイスからのエクストラネット アクセスのみを有効にします。
- 管理対象ではないコンピューターまたは準拠していないコンピューターに対して多要素認証を要求します。

AD FS は、ハイブリッド シナリオで条件付きアクセス ポリシーのオンプレミス コンポーネントを提供します。 クラウド リソースへの条件付きアクセス用に Azure AD にデバイスを登録すると、そのデバイス ID を AD FS ポリシーにも使用できます。



クラウドでのデバイス ベースの条件付きアクセスの使用の詳細については、「Azure Active Directory 条件付きアクセス」を参照してください。

AD FS によるデバイス ベースの条件付きアクセスの使用の詳細については、「AD FS を使用したデバイス ベースの条件付きアクセスの計画」および「AD FS のアクセス制御ポリシー」を参照してください。

Windows Hello for Business でサインインする

Windows 10 デバイスでは、Windows Hello および Windows Hello for Business が導入され、ユーザー パスワードは、ユーザーのジェスチャー (PIN の入力、指紋などの生体認証ジェスチャー、または顔認識など) で保護される強力なデバイスバインド ユーザー資格情報に置き換えられました。 Windows Hello を使用すると、ユーザーはパスワードを求められることなく、イントラネットまたはエクストラネットから AD FS アプリケーションにサインインできます。

組織で Windows Hello for Business を使用する方法の詳細については、「組織で Windows Hello for Business を有効にする」を参照してください。

Modern authentication

AD FS 2016 は、Windows 10 および最新の iOS および Android デバイスとアプリのユーザー エクスペリエンスを向上させる最新の先進プロトコルをサポートしています。

詳細については、「開発者向けの AD FS シナリオ」を参照してください。

要求規則言語の知識なしでアクセス制御ポリシーを構成する

以前は、AD FS 管理者は AD FS の要求規則言語を使用してポリシーを構成する必要があり、ポリシーの構成と保守が困難でした。 アクセス制御ポリシーを使用すると、管理者は組み込みテンプレートを使用して一般的なポリシーを適用できます。 たとえば、テンプレートを使用して次のようなポリシーを適用できます。

- イントラネット アクセスのみを許可します。
- すべてのユーザーを許可し、エクストラネットからの MFA を要求します。
- 特定グループのすべてのユーザーを許可し、MFA を要求します。

テンプレートは簡単にカスタマイズできます。 追加の例外またはポリシー規則を適用できます。また、これらの変更を 1 つ以上のアプリケーションに適用して、一貫性のあるポリシー適用を実現します。

詳細については、「AD FS でのアクセス制御ポリシー」を参照してください。

AD 以外の LDAP ディレクトリでのサインオンを有効にする

多くの組織は、Active Directory とサードパーティのディレクトリを組み合わせます。 ライトウェイト ディレクトリ アクセス プロトコル (LDAP) v3 準拠のディレクトリに格納されているユーザーの認証が AD FS でサポートされているため、AD FS を次のシナリオで使用できるようになりました。

- サード パーティの LDAP v3 準拠ディレクトリ内のユーザー。
- Active Directory の双方向の信頼が構成されていない Active Directory フォレスト内のユーザー。
- Active Directory ライトウェイト ディレクトリ サービス (AD LDS) のユーザー。

詳細については、「 Configure AD FS to authenticate users stored in LDAP directories」を参照してください。

AD FS アプリケーションのサインイン エクスペリエンスをカスタマイズする

以前の Windows Server 2012 R2 の AD FS では、すべての証明書利用者アプリケーションに共通のサインオン エクスペリエンスが提供されていて、アプリケーションごとにテキスト ベー

スのコンテンツのサブセットをカスタマイズする機能が用意されていました。 Windows Server 2016 では、メッセージだけでなく、アプリケーションごとに画像、ロゴ、および Web テーマをカスタマイズできます。 さらに、新しいカスタム Web テーマを作成し、証明書利用者ごとにそれらのテーマの適用ができます。

詳細については、「AD FS のユーザー サインインのカスタマイズ」を参照してください。

管理を容易にするための効率的な監査

以前のバージョンの AD FS では、1 つの要求で多数の監査イベントが生成される可能性がありました。 サインインまたはトークン発行アクティビティに関する関連情報が存在していなかったり、複数の監査イベントに分散されていたりすることがよくあり、問題の診断が困難でした。 そのため、監査イベントは既定でオフになっていました。 ただし、AD FS 2016 では、監査プロセスがより合理化され、関連情報が見つけやすくなっています。 詳細については、「Windows Server 2016 での AD FS の監査機能の強化」を参照してください。

コンフェデレーションに参加するための SAML 2.0 との相互運用性の改善

AD FS 2016 には、複数のエンティティを含むメタデータに基づいた信頼のインポートのサポートなど、追加の SAML プロトコルのサポートが含まれています。 この変更により、InCommon フェデレーションや、eGov 2.0 標準に準拠する他の実装など、コンフェデレーションに参加するように AD FS を構成できます。

詳細については、「SAML 2.0 との相互運用性の向上」を参照してください。

フェデレーション Microsoft 365 ユーザーのパスワード管理の簡素化

保護する証明書利用者の信頼またはアプリケーションにパスワードの有効期限の要求を送信するように、AD FS を構成できます。 これらの要求の表示方法は、アプリケーションによって異なります。 たとえば、証明書利用者として Office 365 を使用している場合、Exchange と Outlook に更新が実装され、フェデレーション ユーザーに対し、パスワードの期限切れが近づいていることが通知されます。

詳細については、「パスワードの有効期限クレームを送信するように AD FS を構成する」を参照してください。

Windows Server 2012 R2 の AD FS から Windows Server 2016 の AD FS への移行が簡単になりました

以前は、AD FS の新しいバージョンに移行するには、使用している Windows Server ファームから新しい並列サーバー ファームに構成設定をエクスポートする必要がありました。 Windows Server 2016 で AD FS を使用すると、並列サーバー ファームを使用する必要がなくなり、プロセスが簡単になります。 Windows Server 2016 サーバーを Windows Server 2012 R2 サーバー ファームに追加すると、新しいサーバーは Windows Server 2012 R2 サーバーのように動作します。 アップグレードの準備ができたら、古いサーバーを削除したら、操作レベルを Windows Server 2016 に変更できます。 詳細については、「Windows Server 2016 での AD FS へのアップグレード」を参照してください。

Windows Server Insiders Preview を開始する

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Server 向け Windows Insider Program に参加し、Windows Server Insider Preview とリモート サーバー管理ツールへの排他的アクセスを取得しましょう。 このコミュニティに参加することで、Windows Server の未来を形成する一助となり、イノベーションの最前線に立つ機会を得られます。

Windows Server Insiders Preview を入手できる場所

登録済みの Insider メンバーの方は、Windows Insider Preview のダウンロード ページに直接アクセスして、利用可能な Windows Server Preview ビルドを表示できます。 Insider のメンバーとして参加する場合は、「Windows Server 向け Windows Insider Program を開始する」を参照してください。

次のキーは、プレビュー ビルドでのみ有効です。

テーブルを展開する

Windows Server のバージョン	Key
Standard	MFY9F-XBN2F-TYFMP-CCV49-RMYVH
Datacenter	2KNJJ-33Y9H-2GXGX-KMQWH-G6H67
Azure Edition	キーは受け入れられません

> **注意**
>
> 特定の国/地域ではダウンロードが制限される場合があります。 詳細については、「**マイクロソフト、ロシアでの新規販売を一時停止**」を参照してください。

Insiders Preview の既知の問題

- OOBE のインストール作業中に、マウスを使って次のステップに進むと、ウィンドウが重なったり、グラフィックが乱れたりすることがあります。

- 最初のサインイン ユーザーのプライバシー設定は、すべての機能が必要に応じて使用できない場合や機能しない場合に制限されます。
- 任意の方法 **で WinPE-Powershell** オプション コンポーネントをインストールしても正しくインストールされず、関連するコマンドレットは失敗します。 WinPE で PowerShell に依存しているお客様は、このビルドを使用しないでください。
- このリリースでは、新しい **フィードバック ハブ** と **ターミナル** アプリが正しく機能していません。
- 断続的なアップグレードの失敗が確認されているため、このビルドを Windows Server 2019 または 2022 からのアップグレードの検証に使用しないことをお勧めします。
- `wevtutil al` コマンドを使用してイベント ログをアーカイブすると、Windows イベント ログ サービスがクラッシュし、アーカイブ操作が失敗します。 この問題を解決するには、昇格した PowerShell プロンプトで以下を実行して、サービスを再起動する必要があります。

  PowerShell

  ```
  Start-Service EventLog
  ```

- Secure Launch または Dynamic Root of Trust for Measurement (DRTM) コード パスが有効になっている場合は、このビルドのインストールを回避することをお勧めします。

Insiders Preview にフィードバックを送信する方法

皆さまからのフィードバックは、現在機能している点、バグの把握、改善点のご提案など、私たちにとって貴重です。 フィードバックを送信する方法については、「フィードバックの詳細」について参照してください。

登録済みの Windows 10 または Windows 11 デバイスを使用して、 フィードバック ハブ アプリを開きます。 フィードバック Hub アプリで、次の情報を提供します。

1. プレビュー ビルド番号の問題に関するタイトル。 たとえば、*Windows Server Standard 25997* のサーバー マネージャーの問題です。
2. 発生している内容の詳細な説明。
3. [**カテゴリ**] で、[**Windows Server**] を選択します。
4. 問題のスクリーンショットの添付は省略可能です。
5. フィードバックの送信を完了します。

こちらも参照ください

- Windows Server 2025 の新機能
- フィードバック Hub を確認する

Windows Server のエディションの比較

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

この記事を参照して、Windows Server の Standard、Datacenter、および Datacenter: Azure Edition を比較し、最適なものを確認してください。

> **ヒント**
>
> Windows Server のロックと制限の詳細については、「**Windows Server のロックと制限の比較**」を参照してください。

使用可能なロールと機能

テーブルを展開する

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
.NET Framework 3.5 の機能		✅	✅	✅
.NET Framework 4.8 の機能		✅	✅	✅
Activation		✅	✅	✅
	仮想マシンの自動ライセンス認証	⚠[1]	✅	✅[2]
	キー管理サービス (KMS)	✅	✅	❌[3]
Active Directory 証明書サービス		✅	✅	✅
	証明書の登録ポリシー Web サービス	✅	✅	✅
	証明書の登録 Web サービス	✅	✅	✅
	証明機関	✅	✅	✅
	証明機関 Web 登録	✅	✅	✅

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
	ネットワーク デバイス登録サービス	✅	✅	✅
	オンライン レスポンダー	✅	✅	✅
Active Directory Domain Services		✅	✅	✅
Active Directory フェデレーション サービス		✅	✅	✅
Active Directory Lightweight Directory サービス		✅	✅	✅
Active Directory Rights Management サービス		✅	✅	✅
Azure 拡張ネットワーク		❌	❌	✅
バックグラウンド インテリジェント転送サービス (BITS)		✅	✅	✅
BitLocker ドライブ暗号化		✅	✅	✅
BitLocker ネットワーク ロック解除		✅[4]	✅[4]	✅[4]
BranchCache		✅	✅	✅
NFS クライアント		✅	✅	✅
データ センター ブリッジング		✅	✅	✅
デバイス正常性構成証明		✅	✅	✅
DHCP サーバー		✅	✅	✅
ダイレクト プレイ		✅[3]	✅[4]	✅[4]
DLNA コーデックおよび Web メディア ストリーミング		✅[3]	✅[4]	✅[4]

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
DNS サーバー		✅	✅	✅
拡張記憶域		✅	✅	✅
フェールオーバー クラスタリング		✅	✅	✅
FAX サーバー		✅	✅	✅
ファイル サービスおよび記憶域サービス		✅	✅	✅
	ネットワーク ファイル用 BranchCache	✅	✅	✅
	データ重複除去	✅	✅	✅
	DFS 名前空間	✅	✅	✅
	DFS レプリケーション	✅	✅	✅
	ファイル サーバー	✅	✅	✅
	ファイル サーバー リソース マネージャー	✅	✅	✅
	ファイル サーバー VSS エージェント サービス	✅	✅	✅
	iSCSI ターゲット サーバー	✅	✅	✅
	iSCSI ターゲット記憶域プロバイダー (VDS および VSS ハードウェア プロバイダー)	✅	✅	✅
	NFS サーバー	✅	✅	✅
	SMB 1.0/CIFS ファイル共有のサポート	✅	✅	✅
	SMB 帯域幅の制限	✅	✅	✅
	SMB over QUIC (ネットワーク プロトコル)	✅	✅	✅
	作業フォルダー	✅	✅	✅
	ストレージ移行サービス	✅	✅	✅

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
	記憶域移行サービス プロキシ	✅	✅	✅
	記憶域スペース	✅	✅	✅
	記憶域スペース ダイレクト	❌	✅	✅
	記憶域レプリカ	✅	✅	✅
グループ ポリシー管理		✅	✅	✅
Host Guardian Hyper-V サポート		❌	✅	✅
ホスト ガーディアン サービス		✅	✅	✅
Hotpatching		✅[5]	✅[5]	✅
サービスの I/O 品質		✅	✅	✅
IIS ホスト可能な Web コア		✅	✅	✅
IP アドレス管理 (IPAM) サーバー		✅	✅	✅
Management OData IIS 拡張機能		✅	✅	✅
メディア ファンデーション		✅	✅	✅
メッセージ キュー		✅	✅	✅
	メッセージ キュー DCOM プロキシ	✅	✅	✅
	メッセージ キュー サービス	✅	✅	✅
Microsoft Defender ウイルス対策		✅	✅	✅
マルチパス I/O		✅	✅	✅
MultiPoint コネクタ		✅	✅	✅
ネットワーク ATC		✅	✅	✅

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
ネットワーク コントローラー		✗	✓	✓
ネットワーク負荷分散		✓	✓	✓
ネットワーク ポリシーおよびアクセス サービス		✓[4]	✓[4]	✓[4]
ネットワーク仮想化		✓	✓	✓
印刷とドキュメント サービス		✓	✓	✓
	インターネット印刷	✓[4]	✓[4]	✓[4]
	ライン プリンター デーモン (LPD) サービス	✓[4]	✓[4]	✓[4]
	プリント サーバー	✓[4]	✓[4]	✓[4]
高品質な Windows オーディオ ビデオ エクスペリエンス		✓	✓	✓
RAS 接続マネージャー管理キット (CMAK)		✓	✓	✓
リモート アクセス		✓	✓	✓
	DirectAccess および VPN (RAS)	✓	✓	✓
	Routing	✓	✓	✓
	Web アプリケーション プロキシ	✓	✓	✓
リモート アシスタンス		✓[4]	✓[4]	✓[4]
リモート デスクトップ サービス		✓[4]	✓[4]	✓[4]
リモート差分圧縮		✓	✓	✓
リモート サーバー管理ツール		✓	✓	✓

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
RPC over HTTP プロキシ		✅	✅	✅
セットアップおよびブート イベント収集		✅	✅	✅
簡易 TCP/IP サービス		✅[4]	✅[4]	✅[4]
SNMP サービス		✅	✅	✅
ソフトウェア ロード バランサー		✅	✅	✅
システム データ アーカイバー		✅	✅	✅
System Insights		✅	✅	✅
Telnet クライアント		✅	✅	✅
TFTP クライアント		✅[4]	✅[4]	✅[4]
Virtualization		✅	✅	✅
	Containers	✅	✅	❌
	Hyper-V	✅	✅	✅
	GPU パーティション分割	✅[6]	✅	✅[6]
	ファブリック管理用の VM シールド ツール	✅	✅	✅
ボリューム ライセンス認証サービス		✅	✅	✅
Web サーバー (IIS)		✅	✅	✅
	FTP サーバー	✅	✅	✅
	ウェブサーバー	✅	✅	✅
WebDAV リダイレクター		✅	✅	✅
Windows 生体認証フレームワーク		✅[4]	✅[4]	✅[4]

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
Windows 展開サービス (Deployment Services)		✅	✅	✅
Windows Identity Foundation 3.5		✅[4]	✅[4]	✅[4]
Windows 内部データベース		✅	✅	✅
Windows PowerShell		✅	✅	✅
	Windows PowerShell 2.0 エンジン	✅	✅	✅
	Windows PowerShell 5.1	✅	✅	✅
	Windows PowerShell Desired State Configuration サービス	✅	✅	✅
	Windows PowerShell Web アクセス	✅	✅	✅
Windows プロセス アクティブ化サービス		✅	✅	✅
Azure Arc で有効化される Windows Server 管理		✅[7]	✅[7]	✅[7]
	Azure Update Manager	✅[7]	✅[7]	✅[7]
	変更履歴とインベントリ	✅[7]	✅[7]	✅[7]
	Azure マシン構成	✅[7]	✅[7]	✅[7]
	Azure for Arc での Windows Admin Center	✅[7]	✅[7]	✅[7]
	リモート サポート	✅[7]	✅[7]	✅[7]
	ネットワーク HUD	✅[7]	✅[7]	✅[7]
	ベスト プラクティス アセスメント	✅[7]	✅[7]	✅[7]
	Azure Site Recovery 構成	✅[7]	✅[7]	✅[7]
Windows Search サー		✅[4]	✅[4]	✅[4]

Feature	Subfeature	Standard Edition	Datacenter エディション	データセンター: Azure のエディション
ビス				
Windows Server バックアップ		✅	✅	✅
Windows Server 移行ツール		✅	✅	✅
Windows Server Update Services		✅	✅	✅
Windows 標準ベースの記憶域の管理		✅	✅	✅
Linux 用 Windows サブシステム		✅	✅	✅
Windows TIFF IFilter		✅[4]	✅[4]	✅[4]
WinRM IIS 拡張機能		✅	✅	✅
WINS サーバー		✅	✅	✅
ワイヤレス LAN サービス		✅	✅	✅
WoW64 サポート		✅	✅	✅
XPS ビューアー		✅[4]	✅[4]	✅[4]

1. Datacenter エディションでアクティブ化された仮想化ホストでホストされている場合はゲストとして
2. Datacenter: Azure Edition は、入れ子になったホストまたはゲストとして使用可能
3. Azure によってアクティブ化され、KMS ホストとしては構成できない
4. デスクトップ エクスペリエンス搭載サーバーとしてインストールされた場合
5. Azure Arc 対応サービスとして使用可能 Azure Arc の価格の詳細については、「Azure 料金計算ツール」を参照してください
6. Windows Server 2025 Standard で使用でき、スタンドアロン サーバー用に設計されています。 計画的なダウンタイムのために、スタンドアロン ノード間で VM をライブ マイグレーションします。 計画外のダウンタイムにクラスタリングが必要な場合は、代わりに Windows Server 2025 Datacenter を使用する必要があります。

7. アクティブなソフトウェア アシュアランスを持つ Windows Server ライセンスまたはアクティブなサブスクリプション ライセンスを持つ Windows Server ライセンスを持つ Azure Arc によって有効になっている Windows Server Management に登録されているマシンで使用できます。 利用可能な Azure の利点、課金、要件の詳細については、 Azure Arc による Windows Server 管理の有効化に関するページを参照してください。

Azure Edition for Windows Server とは

2025/08/15適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022

Windows Server Datacenter: Azure Edition は、Azure での実行に最適化され、イノベーションと仮想化に重点を置いた Windows Server のエディションです。 Azure Edition には、長期サービス チャネル (LTSC) と年単位の製品更新プログラムが用意されており、最初の 3 年間で 2 回のメジャー製品更新プログラムが提供されます。 また Azure Edition では、Windows Server の Standard エディションや Datacenter エディションよりも早く、新しい機能が Windows Server ユーザーに提供されます。

Azure Edition の年次更新プログラムは、OS のフル アップグレードではなく、Windows Update を使用して配信されます。 この年次更新周期の一環として、Azure Edition Insider プレビュー プログラムでは早期ビルドにアクセスする機会が提供され、これが一般提供に生かされます。 Azure Edition Insider プレビューを始めるには、Azure Edition プレビュー Azure Marketplace オファーにアクセスしてください。 各プレビューに関する詳細は、Microsoft Tech Community の Windows Server Insider スペースに投稿されるリリースのお知らせで共有されます。

主要な相違点

次の表に主要な相違点を示します。

テーブルを展開する

説明	Windows Server Standard、Datacenter	Windows Server Datacenter: Azure Edition
新しいリリース	通常、2 - 3 年	通常、2 - 3 年
製品の更新	新しいリリース	毎年、最初の 3 年間に 2 回のメジャー更新プログラム
サポート	5 年間のメインストリーム サポートとそれに続く 5 年間の延長サポート	5 年間のメインストリーム サポートとそれに続く 5 年間の延長サポート
サービス チャネル	長期サービス チャネル	長期サービス チャネル
利用できるユーザー	すべてのチャネルのすべてのユーザー	ソフトウェア アシュアランス、 Windows Server サブスクリプション、クラウドのお客様のみ

説明	Windows Server Standard、Datacenter	Windows Server Datacenter: Azure Edition
インストール オプション	Server Core、デスクトップ エクスペリエンス搭載サーバー、Nano Server コンテナー イメージ	Server Core およびデスクトップ エクスペリエンス搭載サーバーのみ。 Windows Server コンテナーはサポートされていません。
オペレーティング システム環境 (OSE)	物理または仮想	仮想のみ
関連する仮想化権限	Standard 用の 2 つの仮想 OSE、Datacenter 用の無制限の仮想 OS	None

機能はイメージによって異なります。詳しくは、「Windows Server Datacenter: Azure Edition の概要」をご覧ください。

> **ヒント**
>
> 詳細については、**Microsoft ソフトウェアのライセンス条項** に関するページを参照してください。 ライセンス条項は、商用ライセンス プログラム、リテール、オリジナル 機器メーカー (OEM) など、配布チャネルによって異なる場合があります。

主な機能

ホットパッチ

Windows Server 2022 Datacenter: Azure Edition 以降、ホットパッチを使用すると、再起動しなくても VM にセキュリティ更新プログラムを適用できます。 Azure と共に Azure ゲスト パッチ適用サービスと Automanage for Window Server を使用した場合、ホットパッチのオンボード、構成、オーケストレーションが自動化されます。 詳しくは、「新しい仮想マシンのホットパッチ」をご覧ください。

サポートされているプラットフォーム

Azure および Azure Stack HCI で実行されている VM のホットパッチをサポートするオペレーティング システムの詳細については、「 サポートされているプラットフォーム」を参照してください。

> **注意**

ホットパッチは、Windows Server コンテナー基本イメージではサポートされていません。

SMB over QUIC

Windows Server 2022 Datacenter: Azure Edition 以降、SMB over QUIC では、在宅勤務者、モバイル デバイス ユーザー、ブランチ オフィス向けに "SMB VPN" が提供されています。 SMB over QUIC は、インターネットなどの信頼されていないネットワーク経由で、エッジ ファイル サーバーにセキュリティで保護された信頼性の高い接続を提供します。 QUIC は、HTTP/3 で使用される IETF 標準化プロトコルで、TLS 1.3 による最大限のデータ保護を目的に設計されており、無効にできない暗号化が必要とされます。 SMB は QUIC トンネル内で通常通り動作します。つまり、ユーザー エクスペリエンスは変わりません。 マルチチャネル、署名、圧縮、継続的な可用性、ディレクトリ リースなどの SMB 機能は通常通り動作します。

SMB over QUIC は、Windows Server 向けの Azure Automanage マシンのベスト プラクティスとも統合されており、SMB over QUIC の管理が容易になります。 QUIC は証明書を使用して暗号化を提供するため、組織は複雑な公開キー インフラストラクチャの維持に苦労することがよくあります。 Azure Automanage マシンのベスト プラクティスにより、証明書が警告なしに期限切れになることはありません。また、SMB over QUIC は有効な状態を維持し、サービス継続性を最大化します。

詳しくは、「SMB over QUIC」および「Automanage マシンのベスト プラクティスを使用した SMB over QUIC 管理」をご覧ください。

データ転送用の記憶域レプリカ圧縮

Windows Server 2022 Datacenter: Azure Edition の Update 1 以降では、ソース サーバーと同期先サーバー間で記憶域レプリカ データを圧縮できます。 圧縮により、同じ量のデータを転送するネットワーク パケットが少なくなり、スループットが向上し、ネットワーク使用率が低下します。 データ スループットが高いことで、ディザスター リカバリー シナリオなどの、同期が最も必要なときにかかる時間が短縮されます。

記憶域レプリカの機能について詳しくは、「記憶域レプリカの機能」をご覧ください

Azure 用拡張ネットワーク

Windows Server 2022 Datacenter: Azure Edition 以降では、Azure 拡張ネットワークを使用すると、オンプレミスのサブネットを Azure に拡張できます。これにより、オンプレミスの仮想マシンを Azure に移行する場合には、元のオンプレミス プライベート IP アドレスを保持できます。 詳しくは、
Azure 拡張ネットワークをご覧ください。

Windows Server Datacenter: Azure Edition の概要

Azure Edition の使用を開始するには、任意の方法で Azure または Azure ローカルの VM を作成し、使用したい *Windows Server Datacenter: Azure Edition* イメージを選択します。

> **ⓘ 重要**
>
> 一部の機能には、VM の作成時に実行する特定の構成手順があり、プレビュー段階の一部の機能には特定のオプトインとポータル表示の要件があります。 VM でのその機能の使用の詳細については、個々の機能に関する記事を参照してください。

> **⊗ 注意事項**
>
> Windows Server Datacenter: Azure Edition がインストールされると、OS を Azure Edition 以外の OS に切り替えることはできません。 Azure Edition をインストールするつもりがなかった場合は、切り替えるために以前の OS を再インストールする必要があります。

Azure または Azure Local を使用した仮想マシンの作成の詳細については、「Azure portal で Windows 仮想マシンを作成する」と「Azure Localで Windows Server Azure Edition VM をデプロイする 」を参照してください。

次のステップ

- Windows Server 2022 の Standard、Datacenter、Datacenter Azure Edition の各エディションの比較
- 新しい仮想マシンのホットパッチ
- ISO から構築された Azure Edition 仮想マシンのホットパッチを有効にする
- SMB over QUIC
- Azure 用拡張ネットワークを使用して、オンプレミスのサブネットを Azure に拡張する

Azure Arc を使用して Windows Server 従量課金制を構成する

2025/08/16適用対象: ✅ Windows Server 2025

Azure Arc の従量課金制サブスクリプション ライセンス オプションは、Windows Server 2025 の従来の永続的ライセンスの代替手段です。 従量課金制では、Windows Server デバイスを展開し、ライセンスを取得して、使用した分だけのお支払いが可能です。 この機能は Azure Arc を通じて提供されており、Azure サブスクリプション経由で課金されます。 従量課金制は、必要に応じて柔軟に無効にすることが可能です。 さらに、試用版として有効にした場合、最初の 7 日間は、従量課金制を無料で使用できます。 Windows Server 従量課金制は Azure サービスであり、その詳細な使用権限は「Microsoft 製品条項」に記載されています。

> **⊗ 注意事項**
>
> 従量課金制を無効にせずにデバイスをシャットダウンまたはプロビジョニング解除した場合、課金は続行されます。 予期しない料金を回避するには、Azure portal、PowerShell、API を使用するか、Azure Arc からデバイスを削除して、従量課金制を無効にします。

Windows Server 従量課金制は、Microsoft Azure 上の Windows Server ライセンスと同じ価格とモデルを共有しますが、Microsoft Azure の外部に展開されているデバイス向けに設計されています。 Azure Arc での Windows Server の従量課金制は、Microsoft Azure ではサポートされていません。Microsoft Azure のサービスで従量課金制で Windows Server にライセンスを付与する方法は他に用意されています。

従量課金制の規制は、従来の永続的ライセンスとは異なります。 たとえば、従量課金制では、コストは Standard Edition と Datacenter Edition のどちらでも同じであり、標準機能に必要なクライアント アクセス ライセンス (CAL) はありません。 ただし、リモート デスクトップ サービス (RDS) CAL は引き続き必要です。

従量課金制ライセンスは、Microsoft Azure で機能が有効になっているデバイスにのみ適用されます。 従来の永続的ライセンスとは異なり、同じサーバー上で実行されている仮想マシン (VM) に対する追加の権限は提供されません。 したがって、仮想マシンの自動ライセンス認証 (AVMA) 機能は使用できません。 各 VM には、ホスト サーバーに関係なく、それ自体のライセンスが別個に必要です。 ホストと VM は、異なるバージョンのオペレーティング システム (OS) を実行し、さまざまなライセンスの種類を混在させることができます。

Prerequisites

Windows Server 従量課金制を設定する前に、デバイスが次の前提条件を満たしていることを確認します。

- デバイスは Windows Server 2025 Standard または Datacenter Edition を実行している必要があります。 Windows Server を初めて使用する場合は、 機能更新プログラム、クリーン インストール、または Windows Server への移行について 詳しく理解してください。
- デバイスは Azure Arc 対応で、Microsoft Azure Connected Machine Agent バージョン 1.47 以降を実行している必要があります。 デバイスを Azure Arc にオンボードする方法の詳細については、「Azure Arc セットアップを使用して Windows Server マシンを Azure に接続する」を参照してください。
- デバイスは現在、OEM、リテール、ボリューム ライセンス (VL) などの別のライセンスの種類でライセンス付与 (アクティブ化) されていません。
- アクティブなインターネット接続が必要です。

Windows Server 従量課金制を設定する

Windows Server のインストール中またはインストールの完了後に、Windows Server の従量課金制を有効にすることができます。 次のセクションでは、両方のオプションについて順を追って説明します。

ライセンス方法を選択する

Windows Server のインストール中に、従量課金制のセットアップを選択できます。 このオプションは、通常はプロダクト キーを入力する **[ライセンス方法の選択]** 画面で使用できます。 従量課金制を選択すると、プロダクト キーを指定する必要はなくなります。

Windows Server が既にインストールされていてアクティブ化されていない場合は、「 Windows Server 従量課金制の管理 」セクションに進むことができます。 Windows Server のインストールを初めて使用する場合は、「 インストール メディアから Windows Server をインストール する」の手順に従い、[**ライセンス方法の選択**] 画面が表示されたら、次の手順に戻ります。

> **注意**
>
> 従量課金制の統合は、Windows Server メディアのリテール コピーから Windows セットアップを実行している場合にのみ、オペレーティング システムのインストール中に使用できます。 Windows Server の評価版またはボリューム ライセンス (VL) メディアを使用している場合、プロダクト キー ページはバイパスされるため、オペレーティング システムのインストール中に従量課金制にオプトインすることはできません。 ただし、

「Windows Server 従量課金制の管理」セクションの説明に従って、インストール後に従量課金制を 有効にすることができます。

従量課金制のセットアップには、グラフィカル ウィザードとコマンド ラインの 2 つの方法があります。 インストールする Windows のエディションに基づいて、次の手順に従います。

GUI

[**ライセンス方法の選択**] 画面が表示されたら、次の手順に従います。

1. [**従量課金制**] を選択し、[**次へ**] を選択します。
2. **デスクトップ エクスペリエンス**を備えた Windows のエディションを選択し、[**次へ**] を選択します。
3. 続行するには、[同意する] を選択してライセンス条項に **同意** します。
4. [**Windows Server をインストールする場所の選択**] で、必要に応じてディスクとパーティションを選択します。 次に、[**次へ**] を選択します。
5. [**インストール準備完了**] ページで、[**インストール**] を選択します。

インストール プロセスでは、必要に応じてデバイスが自動的に再起動されます。 インストールを続行するためにパスワードを作成するように求められます。 完了してサインインすると、[**Azure Arc のセットアップ**] ウィザードが表示されます。 従量課金制の設定を続行するには、次の手順に従います。

1. [**Azure Arc の使用を開始する**] 画面で、[**次へ**] を選択します。
2. [**Azure Arc のインストール**] 画面で、デバイスは複数のチェックを行って Azure Connected Machine (AzCM) Agent をインストールします。 次に、[構成] を選択 **します**。
3. [**Azure Arc の構成**] 画面で、[**次へ**] を選択します。
4. [**Azure にサインイン**] 画面で、[Azure Cloud] を選択し、サインインして、[**次へ**] を選択します。
5. [**リソースの詳細**] 画面で、必要な情報を入力し続けて、[**次へ**] を選択します。
6. [**Windows Server のライセンス方法を選択**] 画面で、[**Azure で従量課金制**] を選択し、[**次へ**] を選択します。
7. 構成プロセス中に最後の画面に到達したら、[**完了**] を選択します。

> ⓘ **注意**
>
> [**Windows Server のライセンス方法を選択**] 画面で [**プロダクト キーを使用する**] を選択し、インストール ウィザードを続行すると、OS のインストール中に以前にオプトインしていた場合でも、従量課金制はアクティブになりません。

従量課金制の使用をオプトアウトする場合は、サポートされている方法を使用してプロダクト キーを手動で入力する必要があります。 ただし、従量課金制を引き続き使用する場合は、Azure Arc 構成ウィザードで有効になっていない場合でも、Azure portal を使用してアクティブ化できます。

Windows Server の従量課金制を管理する

Windows Server の従量課金制の管理は、Azure Portal、PowerShell、または API を使用して行うことができます。 OS の初回インストール中に従量課金制を有効にすることを選択しなかった場合でも、必要な前提条件が満たされている限り、オプションとして使用することができます。

Windows Server 従量課金制を有効にするには、次の手順に従います。

Azure Portal

Azure portal を使用して Windows Server 従量課金制を有効にするには、次の手順に従います。

1. Azure portal に移動し、**マシン - Azure Arc** を検索して選択します。
2. Windows Server 従量課金制を有効にするマシンを選択します。
3. **従量課金制** タイルを選択します。
4. **[Azure の従量課金制]** の横にあるチェック ボックスをオンにし、**[確認]** を選択します。

または、左側のウィンドウ メニューで [**ライセンス**] を展開し、[**Windows Server**] を選択し、手順 4 に従います。

Windows Server 従量課金制を無効にするには、次の手順に従います。

Azure Portal

Azure portal を使用して Windows Server 従量課金制を無効にするには、次の手順に従います。

1. Azure portal に移動し、**マシン - Azure Arc** を検索して選択します。
2. Windows Server 従量課金制を無効にするマシンを選択します。
3. **従量課金制** のタイルを選択します。
4. **[Azure の従量課金制]** の横にあるチェック ボックスをオフにし、**[確認]** を選択します。

5. **[従量課金制の非アクティブ化]** 通知が表示され、非アクティブ化するかどうかを確認するメッセージが表示されます。 **[非アクティブ化] を選択します。**

または、左側のウィンドウ メニューで [**ライセンス**] を展開し、[**Windows Server**] を選択し、手順 4 に従います。

こちらも参照ください

- Azure Arc 対応サーバー
- Azure Arc セットアップを使用して Windows Server マシンを Azure に接続する

コンテナー用の Windows Server 年間チャネルとは

2025/08/14適用対象: ✅ Windows Server, version 23H2 and later

Windows Server Annual Channel for Containers は、Windows Server コンテナーをホストするためのオペレーティング システムです。 年間チャネルを利用すると、急速なイノベーションを行っているお客様は、オペレーティング システムの新機能を、特にコンテナー、マイクロサービス、移植性に集中して、より速いペースで利用できます。

コンテナー用の Windows Server 年間チャネルは、新機能が年単位でリリースされることを意味します。 年間チャネルのリリース頻度が高いほど、お客様は、コンテナーとマイクロサービスに重点を置きながら、より迅速なイノベーションを活用できます。 ライフサイクルの詳細については、Windows Server 半期チャネルのライフサイクルに関する記事を参照してください。 サービス チャネル間の違いの詳細については、Windows Server サービス チャネルを参照してください。

サポートされているプラットフォーム

Windows Server バージョン 23H2 コンテナー ホストでは、Windows Server 2022 長期サービス チャネル (LTSC) コンテナー イメージのみがサポートされます。

Portability

移植性は、コンテナー用の Windows Server 年間チャネルで導入された重要な機能です。これにより、ユーザーは異なるコンテナー イメージ バージョンでワークロードを実行できます。 移植性により、Windows Server 2022 ベースのコンテナー イメージは、新しいバージョンの Windows Server を実行するセッション ホストで実行できます。 このサポートの強化は、AKS などのコンテナー サービスで、コンテナー自体を更新しなくても、コンテナー ホスト上のオペレーティング システムをより頻繁に更新するのに役立ちます。 移植性は、アップグレード プロセスを効率化するだけでなく、コンテナーが提供する高められた柔軟性と互換性を、開発者が最大限に活用するのにも役立ちます。 移植性の詳細については、コンテナー用の Windows Server 年間チャネルの移植性 を参照してください。

コンテナー用の Windows Server 年間チャネルの概要

コンテナー用の年間チャネルの使用を開始するには、お好みの方法を使用してコンテナー ホストに Windows Server をインストールします。 年間チャネルは、ソフトウェア アシュアラ

ンスとロイヤルティ プログラム (Visual Studio サブスクリプションなど) をお持ちのボリューム ライセンスのお客様が利用できます。 年間チャネル リリースは、次の場所から入手できます。

- ボリューム ライセンス サービス センター (VLSC): ソフトウェア アシュアランス をお持ちの、ボリューム ライセンスのお客様がこのリリースを入手するには、ボリューム ライセンス サービス センター に移動して、[**サインイン**] を選択します。 最後に、[**ダウンロードとキー**] を選択し、「年間チャネル」を検索して、メディアをダウンロードします。

- Visual Studio サブスクリプション: Visual Studio サブスクライバーが年間チャネルのリリースを入手するには、Visual Studio サブスクライバー ダウンロード ページ からダウンロードします。 まだサブスクライバーではない場合は、Visual Studio サブスクリプション にサインアップしてから、Visual Studio サブスクライバーのダウンロード ページ にアクセスします。 Visual Studio サブスクリプション経由で入手したリリースは、開発とテストにのみ利用できます。

> ⚠ **警告**
>
> 年間チャネルは、Server Core インストール オプションでのみインストールできます。 LTSC から年間チャネル リリースに移行するか、既存の年間チャネル インストールをアップグレードするには、クリーン インストールを実行する必要があります。

関連コンテンツ

- コンテナー用の Windows Server 年間チャネルの移植性

Windows Server のハードウェア要件

2025/07/02

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Serverを正しくインストールするには、この記事で説明されている最小ハードウェア要件をコンピューターが満たしている必要があります。 お使いのコンピュータがこれらの要件を満たしていない場合、製品が正しくインストールされない可能性があります。 実際の要件は、システム構成、アプリケーション、およびインストールされている機能によって異なります。

特に指定がない限り、これらの最小ハードウェア要件は、Windows Server Standardエディションと Windows Server Datacenterエディションの両方のすべてのインストールオプション (Server Coreおよびデスクトップエクスペリエンス搭載サーバー) に適用されます。

> **ⓘ 重要**
>
> 潜在的な展開の範囲が非常に多様であるため、適用可能な推奨ハードウェア要件を示すのが現実的ではありません。 特定のサーバー ロールのリソース ニーズの詳細については、デプロイする各サーバー ロールのドキュメントを参照してください。 良い結果を得るために、展開のテストを実施して特定の展開シナリオに合ったハードウェア要件を決定してください。

コンポーネント

CPU

プロセッサのパフォーマンスは、プロセッサのクロック周波数だけでなく、プロセッサ コアの数やプロセッサ キャッシュのサイズの影響も受けます。 プロセッサーの動作環境は以下の通りです。

最小:

- 1.4 GHz 64 ビット プロセッサ
- x64 命令セット対応
- NX と DEP のサポート
- CMPXCHG16b、LAHF/SAHF、および PrefetchW 命令のサポート

- 第 2 レベルのアドレス変換 (EPT または NPT) のサポート
- SSE4.2 (ストリーミング SIMD Extensions 4.2) 命令セットのサポート
- POPCNT 命令のサポート

Windows Sysinternalsに含まれるツールである Coreinfo を活用して、CPU の機能を確認できます。

セキュリティで保護されたコア サーバーの要件

セキュリティで保護されたコアは、高度な脅威に対する強化された保護を提供する一連の統合されたハードウェア、ファームウェア、ドライバー、オペレーティング システム (OS) のセキュリティ機能です。 セキュリティで保護されたコア システムは、OS が起動する前に開始され、システム操作全体を通じて続行されるセキュリティを提供します。 セキュリティで保護されたコア サーバー機能は、Windows Server 2022 以降で使用できます。 セキュリティで保護されたコア サーバーを展開するには、デバイスが次の追加要件を満たしている必要があります。

- **DMA 再マッピング (IOMMU)**: *Intel VT-d* または *AMD-Vi* のサポートは、デバイスによるダイレクト メモリ アクセス (DMA) を安全かつ効率的に管理し、承認されていないメモリ アクセスから保護するために必要です。
- **カーネル DMA 保護**: システムにはカーネル DMA 保護のオプトイン機能が必要です。これにより、外部周辺機器を悪用して不正アクセスを受ける攻撃を防ぐことができます。
- **DRTM (測定のための信頼の動的ルート)**: この機能は、システムのスタートアップ環境の整合性を検証し、ファームウェアベースの攻撃から保護することで、セキュリティで保護されたブート プロセスを確保するために必要です。

> ⓘ **注意**
>
> セキュリティで保護されたコア サーバーに関して概説されている特定の要件に加えて、ハードウェアで次の機能を有効にする必要があります。
>
> - TPM 2.0
> - セキュア ブート
> - ハードウェア仮想化拡張機能を含む仮想化ベースのセキュリティ (VBS) のサポート
>
> 詳細については、「**セキュリティで保護されたコア サーバーとは**」を参照してください。

その他の要件

シナリオに応じて、考慮すべきその他のハードウェア要件があります。

- DVD ドライブ (DVD メディアから OS をインストールする場合)

次の項目は、特定の機能にのみ必要です。

- セキュア ブートをサポートする UEFI 2.3.1c ベースのシステムとファームウェア。
- トラステッド プラットフォーム モジュール (TPM)。
- スーパーVGA(1024 x 768)以上の解像度が可能な統合または専用のグラフィックスおよびモニター。
- キーボードとマウス (またはその他の互換性のあるポインティング デバイス)。
- インターネット アクセス。 (料金が適用される場合があります)。

> ⓘ **注意**
>
> **BitLocker ドライブ暗号化**などの特定の機能を使用するには、TPM チップが必要です。コンピューターにTPMが搭載されている場合は、次の要件を満たす必要があります。
>
> - ハードウェアベースの TPM では、TPM 仕様のバージョン 2.0 を実装する必要があります。
> - バージョン 2.0 を実装する TPM には、ハードウェア ベンダーによって TPM に事前プロビジョニングされているか、最初の起動時にデバイスによって取得できる EK 証明書が必要です。
> - バージョン 2.0 を実装する TPM は、SHA-256 PCR バンクを搭載し、SHA-256 の PCR 0 - 23 を実装している必要があります。 SHA-1 と SHA-256 の両方の測定に使用できる単一の切り替え可能な PCR バンクを備えた TPM を出荷することは許容されます。

Windows Server のロックと制限の比較

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

組織の技術要件とビジネス要件を満たすために、Windows Server の適切なエディションを選択することが不可欠です。 この記事では、サポートされている Windows Server エディション間の主要なオペレーティング システムのロックと制限を並べて比較します。 次の表を使用して、次のような Windows Server エディション間の主な機能を比較します。

- 最大ユーザー数
- 接続の制限
- 仮想化の権限
- ハードウェアのサポート

この情報は、ニーズに最も適したバージョンを選択するのに役立ちます。

Windows Server リリースを選択して、そのロックと制限を表示します。

ロックと制限

Windows Server 2025 のロックと制限を表示するには、完全な比較タブまたはバージョン間の違いタブを選択します。

完全な比較

テーブルを展開する

ロックと制限	Windows Server 2025 Standard	Windows Server 2025 Datacenter	Windows Server 2025 Datacenter: Azure Edition
最大ユーザー数	CAL に基づく	CAL に基づく	CAL に基づく
最大 SMB 接続数	16,777,216	16,777,216	16,777,216
最大 RRAS 接続数	Unlimited	Unlimited	Unlimited
最大 IAS 接続数	2,147,483,647	2,147,483,647	2,147,483,647
最大 RDS 接続	65,535	65,535	65,535

ロックと制限	Windows Server 2025 Standard	Windows Server 2025 Datacenter	Windows Server 2025 Datacenter: Azure Edition
数			
64 ビット ソケットの最大数	64	64	64
コアの最大数	Unlimited	Unlimited	2,048 個の論理プロセッサ
最大 RAM	• 5 レベルのページングをサポートするホストの場合、4 PB • 4 レベルのページングをサポートするホストの場合、256 TB	• 5 レベルのページングをサポートするホストの場合、4 PB • 4 レベルのページングをサポートするホストの場合、256 TB	• 第 2 世代仮想マシンの場合、240 TB • 第 1 世代仮想マシンの場合、1 TB
仮想化ゲストとしての使用	○ (2 台の仮想マシン、およびライセンスごとに 1 台の Hyper-V ホスト)	はい; **無制限の仮想マシン**と、ライセンスごとに 1 つの Hyper-V ホスト	はい; **無制限の仮想マシン**と、ライセンスごとに 1 つの Hyper-V ホスト
Windows Server コンテナー	Unlimited	Unlimited	Unlimited
仮想 OSE/Hyper-V の分離コンテナー	2	Unlimited	Unlimited
Windows Server コンテナー	無制限の Windows コンテナーおよび最大 2 台の Hyper-V コンテナー	無制限の Windows コンテナーと Hyper-V コンテナー	無制限の Windows コンテナーと Hyper-V コンテナー
記憶域レプリカ	2 TB の単一ボリュームを持つ 1 つのパートナーシップと 1 つのリソース グループ	**Unlimited**	**Unlimited**

Windows Server で削除または開発されなくなった機能

2025/09/24

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Server の各リリースには、新機能と機能強化が導入されています。 古い機能は、より良い代替手段を得るために削除される場合があります。 この記事では、Windows Server で削除または非推奨になった機能について詳しく説明します。

> **ヒント**
>
> Windows Insider Program for Business に参加することで、Windows Server ビルドに早期にアクセスできます。これは、機能の変更をテストする優れた方法です。

> **注意**
>
> Windows Server 長期サービス チャネル (LTSC) リリースには、5 年間のメインストリーム サポートと 5 年間の延長サポートを含む固定ライフサイクル ポリシーがあり、合計ライフサイクルは 10 年間です。 詳細については、以下をご覧ください。
>
> - 固定ライフサイクル ポリシー
> - ライフサイクル用語と定義

この一覧は変更される可能性があり、影響を受けるすべての機能が含まれているわけではありません。

開発が中止された機能

これらの機能は現在積極的に開発されておらず、今後の更新プログラムから削除される可能性があります。 一部の機能は、他の機能に置き換えられました。 その他はさまざまなソースから利用できるようになりました。 非推奨 とは、機能、またはサービスがアクティブな開発でなくなったことを意味します。 非推奨の機能は、今後のリリースで削除される可能性があります。 非推奨のコンポーネントは引き続き Windows Server に付属しており、運用環境の展開でサポートされており、製品ライフサイクルごとにセキュリティと品質の更新プログラムを引き続き受け取ります。

Windows Server 2025

テーブルを展開する

Feature	Explanation
コンピューター ブラウザー	コンピューター ブラウザー のドライバーとサービスは非推奨です。 ブラウザー (ブラウザー プロトコルとサービス) は、古くて安全でないデバイスの場所プロトコルです。 Windows 10 では、このプロトコル、サービス、ドライバーが既定で無効になり、SMB1 サービスが削除されました。 コンピューター ブラウザー ドライブとサービスで使用される CIFS ブラウザー プロトコルの詳細については、「 MS-BRWS Common Internet File System」を参照してください。
フェールオーバー クラスタリングのクラスター セット	フェールオーバー クラスタリング クラスター セット機能は、アクティブな機能開発ではなくなり、非推奨となります。
ネットワーク負荷分散 (NLB)	NLB はアクティブな機能開発ではなくなり、非推奨になりました。 代わりにソフトウェア ロード バランサー (SLB) を使用することを検討してください。 SLB の詳細については、「SDN のソフトウェア ロード バランサー (SLB) とは」を参照してください。
NTLM	NTLMv1 が削除されました。 LANMAN と NTLMv2 は、アクティブな機能開発の対象ではなくなり、非推奨となります。 NTLMv2 は引き続き動作しますが、今後のリリースでは Windows Server から削除される予定です。 NTLM の呼び出しを ネゴシエートの呼び出しに置き換えます。ネゴシエートは Kerberos で認証を試み、必要な場合にのみ NTLM にフォールバックします。 詳細については、「 Windows 認証の進化 」を参照してください。
リモート Mailslots	リモート Mailslot は非推奨です。 MS DOS で最初に導入されたリモート Mailslot プロトコルは、信頼性が低く安全でない、日付が付いたシンプルな IPC メソッドです。 このプロトコルは 、Windows 11 Insider Preview Build で既定で最初に無効になりました。 リモート メールスロットの詳細については、「 Mailslots について 」および 「[MS-MAIL]: Remote Mailslot Protocol」を参照してください。
TLS 1.0 TLS 1.1	TLS バージョン 1.0 および 1.1 は、 RFC 8996 に記載されているセキュリティ上の問題により、インターネット標準および規制機関ごとに非推奨とされます。 これらのバージョンは、Windows Server 2025 では既定で無効になっています。 TLS の非推奨の詳細については、Windows での TLS 1.0 および TLS 1.1 の非推奨を参照してください。
WebDAV リダイレクター サービス	WebDAV リダイレクター サービスは非推奨です。 サービスは、Windows Server に既定ではインストールされません。 WebDAV リダイレクター サービスの詳細については、「 WebDAV - Win32 アプリ」を参照してください。

Feature	Explanation
Windows 内部データベース (WID)	WID は、AD FS、AD RMS、IPAM、RD 接続ブローカー、WSUS など、いくつかの役割で使用されます。 これらのロールには、無料版または完全版の SQL Server を使用することを検討してください。 WID は、今後のリリースで Windows から削除される予定です。 詳細については、 SQL Server のエディションに関するページを参照してください。
Windows Management Instrumentation コマンド ライン (WMIC)	Windows Server 2025 以降、WMIC はオンデマンド機能 (FOD) として使用できます。 `DISM /Add-Capability` コマンドを使用して追加できます。 今後のリリースで Windows から削除される予定です。 WMI 用の PowerShell によって WMIC ツールが置き換えられます。 PowerShell を使用するか、WMIC の代わりにプログラムで WMI にクエリを実行します。 WMIC の減価償却の詳細については、「WMI コマンド ライン (WMIC) ユーティリティの廃止: 次の手順」を参照してください。
VB スクリプト	VBScript は FOD として使用でき、Windows Server 2025 にプレインストールされてから、後のリリースでオペレーティング システムから削除されます。 VBScript の代わりに、タスク、カスタム アクション、またはスクリプトを自動化するために PowerShell を使用します。 PowerShell への移行の詳細については、 VBScript から Windows への PowerShell 変換ガイドを参照してください。 Web ページ内で VBScript を使用している場合、機能は現在、Internet Explorer 11 より前のブラウザーに制限されています。 Web ページを JavaScript に移行することをお勧めします。JavaScript では、ブラウザー間の互換性と最新のブラウザーのサポートが提供されます。
Windows Server Update Services (WSUS)	WSUS はアクティブに開発されなくなりました。 既存のすべての機能とコンテンツは、引き続きデプロイで使用できます。

削除された機能

Windows Server にインストールされている製品イメージから、次の機能を削除します。 これらの機能に依存するアプリケーションまたはコードは、別の方法を使用しない限り、今後のリリースでは機能しません。 削除は、機能が使用できなくなり、製品またはサービスから削除された場合に発生します。 機能と機能の削除は、Windows Server の任意のリリースで行うことができます。 一部の機能は非推奨ですが、現在のバージョンの Windows Server には引き続き付属しています。 コンポーネントは、製品ライフサイクル内にある一般公開されているサポートされているバージョンから削除されません。

Windows Server 2025

テーブルを展開する

Feature	Explanation
データ暗号化標準 (DES)	対称キー ブロック暗号化暗号である DES は、最新の暗号化攻撃に対するセキュリティ保護とは見なされません。 これは、より堅牢な暗号化アルゴリズムに置き換えられます。 DES は Windows Server 2008 R2 以降では無効になっており、Windows Server 2025 以降のリリースから削除されています。
IIS 6 管理コンソール (Web-Lgcy-Mgmt-Console)	Windows Server 2019 での開発が中止されたため、コンソールは削除されます。また、IIS 6.0 以前のバージョンから最新バージョンの IIS への移行も開始する必要があります。これは、Windows Server の最新リリースで常に利用可能です。
NTLMv1	NTLM の呼び出しを ネゴシエートの呼び出しに置き換えます。ネゴシエートは Kerberos で認証を試み、必要な場合にのみ NTLM にフォールバックします。 詳細については、「 Windows 認証の進化 」を参照してください。
Windows PowerShell 2.0 の場合	2025 年 9 月の更新プログラム 以降、Windows Server 2025 には Windows PowerShell 2.0 は含めなくなりました。 9 月の更新プログラムの前に Windows PowerShell 2.0 がインストールされている場合は、使用できなくなります。 Windows PowerShell 2.0 のアプリケーションとコンポーネントは、PowerShell 5.0 以降に移行する必要があります。 非推奨の詳細については、 Windows PowerShell 2.0 の非推奨に関する ページを参照してください。
SMTP サーバー	SMTP サーバーの機能は Windows Server 2025 から削除されたため、オペレーティング システム内に置き換えはありません。 代わりに、Exchange Server または Microsoft 以外の SMTP サーバーを使用することを検討してください。 Exchange Server で SMTP 接続を有効にする方法の詳細については、「Exchange Server の受信コネクタ」を参照してください。
Wordpad	`.doc` や `.rtf` などのリッチ テキスト ドキュメントには Microsoft Word、`.txt` などのプレーンテキスト ドキュメントには Windows メモ帳をお勧めします。

関連コンテンツ

- 非推奨: Windows ライフサイクルにおける意味

Windows Server のリリース情報

Windows Server には、長期サービス チャネルと年次チャネルの 2 つのプライマリ リリース チャネル があります。LTSC は、セキュリティと品質の更新プログラムの従来のライフサイクルに重点を置いた、より長期的なオプションを提供します。AC では、コンテナーとマイクロサービスに焦点を当てたより頻繁なリリースが提供されるため、イノベーションをより迅速に活用できます。

Windows Server 2025 は、現在の LTSC リリースです。Windows Server バージョン 23H2 は、最新の AC リリースです。仮想化、コンテナー、マイクロサービスのイノベーションに重点が置かれているのは、 Azure Stack HCI、 Windows コンテナー、 AKS on Azure Stack HCI です。

IT 管理者であり、プログラムでこのページから情報を取得する場合は、Microsoft Graph の Windows 更新プログラム API を使用します。

サービス オプションによる Windows Server のメジャー バージョン

(すべての日付は ISO 8601 形式: YYYY-MM-DD で表示されています)

テーブルを展開する

Windows Server バージョン	サービス オプション	エディション	公開日	メインストリーム サポートの終了日	延長サポートの終了日	ESU の最新の更新プログラム	最新のリビジョン日付	最新のビルド
Windows Server 2025	長期間のサービス チャネル (LTSC)	Datacenter, Standard	2024-11-01	2029-11-13	2034-11-14	2026-01 OOB	2026-01-17	26100.32234
Windows Server 2022	長期間のサービス チャネル (LTSC)	Datacenter, Standard	2021-08-18	2026-10-13	2031-10-14	2026-01 OOB	2026-01-17	20348.4650
Windows Server 2019 (version 1809)	長期間のサービス チャネル (LTSC)	Datacenter, Standard	2018-11-13	更新の終了	2029-01-09	2026-01 OOB	2026-01-17	17763.8280
Windows Server 2016 (version 1607)	Long-Term Servicing Branch (LTSB)	Datacenter, Essentials, Standard	2016-08-02	更新の終了	2027-01-12	2026-01 B	2026-01-13	14393.8783

Note

Windows Server は、**固定ライフサイクル ポリシー**によって管理されます。 サービス要件とその他の重要な情報の詳細については、**Windows ライフサイクルに**関する FAQ とサービス**チャネル**の比較に関するページを参照してください。 Windows Server のライフサイクル ポリシーの詳細については、「**Windows Server のリリース**」を参照してください。

Windows Server のリリース履歴

次の表は、長期サービス チャネルで Windows Server のサポート対象バージョン向けにリリースされたすべての月次セキュリティおよびセキュリティ以外のプレビュー更新プログラムの履歴を示します。

「更新プログラムの種類」列は、年ごとの各月次更新プログラムとそのリリースの月を参照し、後には月の週を示す文字が続きます (B は月の第 2 週、D は月の第 4 週です)。定例外の更新プログラムは OOB として参照されます。この短縮形表記は、Microsoft Intune に表示される表記と一致します。詳細については、更新プログラムのリリースの種類に関する記事を参照してください。

Windows Server のリリース ノートは、「Windows Server 2025 の更新プログラムの履歴」、「Windows Server 2022 更新履歴」、Windows Server 2019 の更新履歴に関する記事、Windows Server 2016 の更新履歴 に関する記事に記載されています。

Windows Server 2025 (OS build 26100)

テーブルを展開する

サービス オプション	更新プログラムの種類	公開日	構築	サポート技術情報の記事
LTSC	2026-01 OOB	2026-01-17	26100.32234	KB5077793
LTSC	2026-01 B	2026-01-13	26100.32230	KB5073379
LTSC	2025-12 B	2025-12-09	26100.7462	KB5072033
LTSC	2025-11 OOB	2025-11-18	26100.7178	KB5072359
LTSC	2025-11 B	2025-11-11	26100.7171	KB5068861
LTSC	2025-10 OOB	2025-10-23	26100.6905	KB5070881
LTSC	2025-10 OOB	2025-10-20	26100.6901	KB5070773
LTSC	2025-10 B	2025-10-14	26100.6899	KB5066835
LTSC	2025-09 OOB	2025-09-22	26100.6588	KB5068221
LTSC	2025-09 B	2025-09-09	26100.6584	KB5065426
LTSC	2025-08 B	2025-08-12	26100.4946	KB5063878
LTSC	2025-07 OOB	2025-07-13	26100.4656	KB5064489
LTSC	2025-07 B	2025-07-08	26100.4652	KB5062553
LTSC	2025-06 B	2025-06-10	26100.4349	KB5060842

LTSC	2025-05 OOB	2025-05-27	26100.4066	KB5061977
LTSC	2025-05 B	2025-05-13	26100.4061	KB5058411
LTSC	2025-04 OOB	2025-04-16	26100.3781	KB5059087
LTSC	2025-04 B	2025-04-08	26100.3775	KB5055523
LTSC	2025-03 B	2025-03-11	26100.3476	KB5053598
LTSC	2025-02 B	2025-02-11	26100.3194	KB5051987
LTSC	2025-01 B	2025-01-14	26100.2894	KB5050009
LTSC	2024-12 B	2024-12-10	26100.2605	KB5048667
LTSC	2024-11 B	2024-11-12	26100.2314	KB5046617
LTSC	2024-10 A	2024-11-01	26100.1742	

▼ Windows Server 2022 (OS build 20348)

テーブルを展開する

サービス オプション	更新プログラムの種類	公開日	構築	サポート技術情報の記事
LTSC	2026-01 OOB	2026-01-17	20348.4650	KB5077800
LTSC	2026-01 B	2026-01-13	20348.4648	KB5073457
LTSC	2025-12 B	2025-12-09	20348.4529	KB5071547
LTSC	2025-11 B	2025-11-11	20348.4405	KB5068787
LTSC	2025-10 OOB	2025-10-23	20348.4297	KB5070884
LTSC	2025-10 B	2025-10-14	20348.4294	KB5066782
LTSC	2025-09 B	2025-09-09	20348.4171	KB5065432
LTSC	2025-08 B	2025-08-12	20348.4052	KB5063880
LTSC	2025-07 B	2025-07-08	20348.3932	KB5062572
LTSC	2025-06 B	2025-06-10	20348.3807	KB5060526
LTSC	2025-05 OOB	2025-05-23	20348.3695	KB5061906
LTSC	2025-05 B	2025-05-13	20348.3692	KB5058385
LTSC	2025-04 OOB	2025-04-16	20348.3566	KB5059092
LTSC	2025-04 OOB	2025-04-11	20348.3561	KB5058920
LTSC	2025-04 B	2025-04-08	20348.3453	KB5055526
LTSC	2025-03 B	2025-03-11	20348.3328	KB5053603
LTSC	2025-02 B	2025-02-11	20348.3207	KB5051979

LTSC	2025-01 OOB	2025-01-18	20348.3095	KB5052819
LTSC	2025-01 B	2025-01-14	20348.3091	KB5049983
LTSC	2024-12 B	2024-12-10	20348.2966	KB5048654
LTSC	2024-11 B	2024-11-12	20348.2849	KB5046616
LTSC	2024-10 B	2024-10-08	20348.2762	KB5044281
LTSC	2024-09 B	2024-09-10	20348.2700	KB5042881
LTSC	2024-08 B	2024-08-13	20348.2655	KB5041160
LTSC	2024-07 B	2024-07-09	20348.2582	KB5040437
LTSC	2024-06 OOB	2024-06-20	20348.2529	KB5041054
LTSC	2024-06 B	2024-06-11	20348.2527	KB5039227
LTSC	2024-05 B	2024-05-14	20348.2461	KB5037782
LTSC	2024-04 B	2024-04-09	20348.2402	KB5036909
LTSC	2024-03 OOB	2024-03-22	20348.2342	KB5037422
LTSC	2024-03 B	2024-03-12	20348.2340	KB5035857
LTSC	2024-02 B	2024-02-13	20348.2322	KB5034770
LTSC	2024-01 B	2024-01-09	20348.2227	KB5034129
LTSC	2023-12 B	2023-12-12	20348.2159	KB5033118
LTSC	2023-11 B	2023-11-14	20348.2113	KB5032198
LTSC	2023-10 B	2023-10-10	20348.2031	KB5031364
LTSC	2023-09 B	2023-09-12	20348.1970	KB5030216
LTSC	2023-08 B	2023-08-08	20348.1906	KB5029250
LTSC	2023-07 B	2023-07-11	20348.1850	KB5028171
LTSC	2023-06 B	2023-06-13	20348.1787	KB5027225
LTSC	2023-05 B	2023-05-09	20348.1726	KB5026370
LTSC	2023-04 B	2023-04-11	20348.1668	KB5025230
LTSC	2023-03 B	2023-03-14	20348.1607	KB5023705
LTSC	2023-02 B	2023-02-14	20348.1547	KB5022842
LTSC	2023-01 B	2023-01-10	20348.1487	KB5022291
LTSC	2022-12 OOB	2022-12-20	20348.1368	KB5022553
LTSC	2022-12 B	2022-12-13	20348.1366	KB5021249
LTSC	2022-11 C	2022-11-22	20348.1311	KB5020032

LTSC	2022-11 OOB	2022-11-17	20348.1251	KB5021656
LTSC	2022-11 B	2022-11-08	20348.1249	KB5019081
LTSC	2022-10 C	2022-10-25	20348.1194	KB5018485
LTSC	2022-10 OOB	2022-10-17	20348.1131	KB5020436
LTSC	2022-10 B	2022-10-11	20348.1129	KB5018421
LTSC	2022-09 C	2022-09-20	20348.1070	KB5017381
LTSC	2022-09 B	2022-09-13	20348.1006	KB5017316
LTSC	2022-08 C	2022-08-16	20348.946	KB5016693
LTSC	2022-08 B	2022-08-09	20348.887	KB5016627
LTSC	2022-07 C	2022-07-19	20348.859	KB5015879
LTSC	2022-07 B	2022-07-12	20348.825	KB5015827
LTSC	2022-06 C	2022-06-23	20348.803	KB5014665
LTSC	2022-06 B	2022-06-14	20348.768	KB5014678
LTSC	2022-05 C	2022-05-24	20348.740	KB5014021
LTSC	2022-05 OOB	2022-05-19	20348.709	KB5015013
LTSC	2022-05 B	2022-05-10	20348.707	KB5013944
LTSC	2022-04 C	2022-04-25	20348.681	KB5012637
LTSC	2022-04 B	2022-04-12	20348.643	KB5012604
LTSC	2022-03 C	2022-03-22	20348.617	KB5011558
LTSC	2022-03 B	2022-03-08	20348.587	KB5011497
LTSC	2022-02 C	2022-02-15	20348.558	KB5010421
LTSC	2022-02 B	2022-02-08	20348.524	KB5010354
LTSC	2022-01 C	2022-01-25	20348.502	KB5009608
LTSC	2022-01 OOB	2022-01-17	20348.473	KB5010796
LTSC	2022-01 B	2022-01-11	20348.469	KB5009555
LTSC	2022-01 OOB	2022-01-05	20348.407	KB5010197
LTSC	2021-12 B	2021-12-14	20348.405	KB5008223
LTSC	2021-11 C	2021-11-22	20348.380	KB5007254
LTSC	2021-11 B	2021-11-09	20348.350	KB5007205
LTSC	2021-10 C	2021-10-26	20348.320	KB5006745
LTSC	2021-10 B	2021-10-12	20348.288	KB5006699

LTSC	2021-09 C	2021-09-27	20348.261	KB5005619
LTSC	2021-09 B	2021-09-14	20348.230	KB5005575
LTSC	2021-08 C	2021-08-26	20348.202	KB5005104

▼ Windows Server 2019 (OS build 17763)

テーブルを展開する

サービス オプション	更新プログラムの種類	公開日	構築	サポート技術情報の記事
LTSC	2026-01 OOB	2026-01-17	17763.8280	KB5077795
LTSC	2026-01 B	2026-01-13	17763.8276	KB5073723
LTSC	2025-12 OOB	2025-12-18	17763.8148	KB5074975
LTSC	2025-12 B	2025-12-09	17763.8146	KB5071544
LTSC	2025-11 B	2025-11-11	17763.8027	KB5068791
LTSC	2025-10 OOB	2025-10-23	17763.7922	KB5070883
LTSC	2025-10 B	2025-10-14	17763.7919	KB5066586
LTSC	2025-09 B	2025-09-09	17763.7792	KB5065428
LTSC	2025-08 OOB	2025-08-19	17763.7683	KB5066187
LTSC	2025-08 B	2025-08-12	17763.7678	KB5063877
LTSC	2025-07 B	2025-07-08	17763.7558	KB5062557
LTSC	2025-06 B	2025-06-10	17763.7434	KB5060531
LTSC	2025-05 OOB	2025-05-27	17763.7322	KB5061978
LTSC	2025-05 B	2025-05-13	17763.7314	KB5058392
LTSC	2025-04 OOB	2025-04-16	17763.7249	KB5059091
LTSC	2025-04 OOB	2025-04-11	17763.7240	KB5058922
LTSC	2025-04 B	2025-04-08	17763.7136	KB5055519
LTSC	2025-03 B	2025-03-11	17763.7009	KB5053596
LTSC	2025-02 B	2025-02-11	17763.6893	KB5052000
LTSC	2025-01 B	2025-01-14	17763.6775	KB5050008
LTSC	2024-12 B	2024-12-10	17763.6659	KB5048661
LTSC	2024-11 B	2024-11-12	17763.6532	KB5046615
LTSC	2024-10 B	2024-10-08	17763.6414	KB5044277
LTSC	2024-09 B	2024-09-10	17763.6293	KB5043050

LTSC	2024-08 B	2024-08-13	17763.6189	KB5041578
LTSC	2024-07 B	2024-07-09	17763.6054	KB5040430
LTSC	2024-06 B	2024-06-11	17763.5936	KB5039217
LTSC	2024-05 OOB	2024-05-23	17763.5830	KB5039705
LTSC	2024-05 B	2024-05-14	17763.5820	KB5037765
LTSC	2024-04 B	2024-04-09	17763.5696	KB5036896
LTSC	2024-03 OOB	2024-03-25	17763.5579	KB5037425
LTSC	2024-03 B	2024-03-12	17763.5576	KB5035849
LTSC	2024-02 B	2024-02-13	17763.5458	KB5034768
LTSC	2024-01 B	2024-01-09	17763.5329	KB5034127
LTSC	2023-12 B	2023-12-12	17763.5206	KB5033371
LTSC	2023-11 B	2023-11-14	17763.5122	KB5032196
LTSC	2023-10 B	2023-10-10	17763.4974	KB5031361
LTSC	2023-09 B	2023-09-12	17763.4851	KB5030214
LTSC	2023-08 B	2023-08-08	17763.4737	KB5029247
LTSC	2023-07 B	2023-07-11	17763.4645	KB5028168
LTSC	2023-06 B	2023-06-13	17763.4499	KB5027222
LTSC	2023-05 B	2023-05-09	17763.4377	KB5026362
LTSC	2023-04 B	2023-04-11	17763.4252	KB5025229
LTSC	2023-03 B	2023-03-14	17763.4131	KB5023702
LTSC	2023-02 B	2023-02-14	17763.4010	KB5022840
LTSC	2023-01 B	2023-01-10	17763.3887	KB5022286
LTSC	2022-12 OOB	2022-12-20	17763.3772	KB5022554
LTSC	2022-12 B	2022-12-13	17763.3770	KB5021237
LTSC	2022-11 OOB	2022-11-17	17763.3653	KB5021655
LTSC	2022-11 B	2022-11-08	17763.3650	KB5019966
LTSC	2022-10 OOB	2022-10-17	17763.3534	KB5020438
LTSC	2022-10 B	2022-10-11	17763.3532	KB5018419
LTSC	2022-09 C	2022-09-20	17763.3469	KB5017379
LTSC	2022-09 B	2022-09-13	17763.3406	KB5017315
LTSC	2022-08 C	2022-08-23	17763.3346	KB5016690

LTSC	2022-08 B	2022-08-09	17763.3287	KB5016623
LTSC	2022-07 C	2022-07-21	17763.3232	KB5015880
LTSC	2022-07 B	2022-07-12	17763.3165	KB5015811
LTSC	2022-06 C	2022-06-23	17763.3113	KB5014669
LTSC	2022-06 B	2022-06-14	17763.3046	KB5014692
LTSC	2022-05 C	2022-05-24	17763.2989	KB5014022
LTSC	2022-05 OOB	2022-05-19	17763.2931	KB5015018
LTSC	2022-05 B	2022-05-10	17763.2928	KB5013941
LTSC	2022-04 C	2022-04-21	17763.2867	KB5012636
LTSC	2022-04 B	2022-04-12	17763.2803	KB5012647
LTSC	2022-03 C	2022-03-22	17763.2746	KB5011551
LTSC	2022-03 B	2022-03-08	17763.2686	KB5011503
LTSC	2022-02 C	2022-02-15	17763.2628	KB5010427
LTSC	2022-02 B	2022-02-08	17763.2565	KB5010351
LTSC	2022-01 C	2022-01-25	17763.2510	KB5009616
LTSC	2022-01 OOB	2022-01-18	17763.2458	KB5010791
LTSC	2022-01 B	2022-01-11	17763.2452	KB5009557
LTSC	2022-01 OOB	2022-01-04	17763.2369	KB5010196
LTSC	2021-12 B	2021-12-14	17763.2366	KB5008218
LTSC	2021-11 C	2021-11-22	17763.2330	KB5007266
LTSC	2021-11 OOB	2021-11-14	17763.2305	KB5008602
LTSC	2021-11 B	2021-11-09	17763.2300	KB5007206
LTSC	2021-10 C	2021-10-19	17763.2268	KB5006744
LTSC	2021-10 B	2021-10-12	17763.2237	KB5006672
LTSC	2021-09 C	2021-09-21	17763.2213	KB5005625
LTSC	2021-09 B	2021-09-14	17763.2183	KB5005568
LTSC	2021-08 C	2021-08-26	17763.2145	KB5005102
LTSC	2021-08 B	2021-08-10	17763.2114	KB5005030
LTSC	2021-07 OOB	2021-07-27	17763.2091	KB5005394
LTSC	2021-07 C	2021-07-20	17763.2090	KB5004308
LTSC	2021-07 B	2021-07-13	17763.2061	KB5004244

LTSC	2021-07 OOB	2021-07-06	17763.2029	KB5004947
LTSC	2021-06 C	2021-06-15	17763.2028	KB5003703
LTSC	2021-06 B	2021-06-08	17763.1999	KB5003646
LTSC	2021-05 C	2021-05-20	17763.1971	KB5003217
LTSC	2021-05 B	2021-05-11	17763.1935	KB5003171
LTSC	2021-04 C	2021-04-22	17763.1911	KB5001384
LTSC	2021-04 B	2021-04-13	17763.1879	KB5001342
LTSC	2021-03 C	2021-03-25	17763.1852	KB5000854
LTSC	2021-03 OOB	2021-03-18	17763.1823	KB5001638
LTSC	2021-03 OOB	2021-03-15	17763.1821	KB5001568
LTSC	2021-03 B	2021-03-09	17763.1817	KB5000822
LTSC	2021-02 C	2021-02-16	17763.1790	KB4601383
LTSC	2021-02 B	2021-02-09	17763.1757	KB4601345
LTSC	2021-01 C	2021-01-21	17763.1728	KB4598296
LTSC	2021-01 B	2021-01-12	17763.1697	KB4598230
LTSC	2020-12 B	2020-12-08	17763.1637	KB4592440
LTSC	2020-11 C	2020-11-19	17763.1613	KB4586839
LTSC	2020-11 OOB	2020-11-17	17763.1579	KB4594442
LTSC	2020-11 B	2020-11-10	17763.1577	KB4586793
LTSC	2020-10 C	2020-10-20	17763.1554	KB4580390
LTSC	2020-10 B	2020-10-13	17763.1518	KB4577668
LTSC	2020-09 C	2020-09-16	17763.1490	KB4577069
LTSC	2020-09 B	2020-09-08	17763.1457	KB4570333
LTSC	2020-08 C	2020-08-20	17763.1432	KB4571748
LTSC	2020-08 B	2020-08-11	17763.1397	KB4565349
LTSC	2020-07 C	2020-07-21	17763.1369	KB4559003
LTSC	2020-07 B	2020-07-14	17763.1339	KB4558998
LTSC	2020-06 OOB	2020-06-16	17763.1294	KB4567513
LTSC	2020-06 B	2020-06-09	17763.1282	KB4561608
LTSC	2020-05 B	2020-05-12	17763.1217	KB4551853
LTSC	2020-04 C	2020-04-21	17763.1192	KB4550969

LTSC	2020-04 B	2020-04-14	17763.1158	KB4549949
LTSC	2020-03 OOB	2020-03-30	17763.1132	KB4554354
LTSC	2020-03 C	2020-03-17	17763.1131	KB4541331
LTSC	2020-03 B	2020-03-10	17763.1098	KB4538461
LTSC	2020-02 C	2020-02-25	17763.1075	KB4537818
LTSC	2020-02 B	2020-02-11	17763.1039	KB4532691
LTSC	2020-01 C	2020-01-23	17763.1012	KB4534321
LTSC	2020-01 B	2020-01-14	17763.973	KB4534273
LTSC	2019-12 B	2019-12-10	17763.914	KB4530715
LTSC	2019-11 B	2019-11-12	17763.864	KB4523205
LTSC	2019-10 C	2019-10-15	17763.832	KB4520062
LTSC	2019-10 B	2019-10-08	17763.805	KB4519338
LTSC	2019-09 OOB	2019-10-03	17763.775	KB4524148
LTSC	2019-09 C	2019-09-24	17763.774	KB4516077
LTSC	2019-09 OOB	2019-09-23	17763.740	KB4522015
LTSC	2019-09 B	2019-09-10	17763.737	KB4512578
LTSC	2019-08 C	2019-08-17	17763.720	KB4512534
LTSC	2019-08 B	2019-08-13	17763.678	KB4511553
LTSC	2019-07 C	2019-07-22	17763.652	KB4505658
LTSC	2019-07 B	2019-07-09	17763.615	KB4507469
LTSC	2019-06 OOB	2019-06-26	17763.593	KB4509479
LTSC	2019-06 C	2019-06-18	17763.592	KB4501371
LTSC	2019-06 B	2019-06-11	17763.557	KB4503327
LTSC	2019-05 C	2019-05-21	17763.529	KB4497934
LTSC	2019-05 OOB	2019-05-19	17763.504	KB4505056
LTSC	2019-05 B	2019-05-14	17763.503	KB4494441
LTSC	2019-04 C	2019-05-03	17763.475	KB4495667
LTSC	2019-04 OOB	2019-05-01	17763.439	KB4501835
LTSC	2019-04 B	2019-04-09	17763.437	KB4493509
LTSC	2019-03 D	2019-04-02	17763.404	KB4490481
LTSC	2019-03 B	2019-03-12	17763.379	KB4489899

LTSC	2019-02 D	2019-03-01	17763.348	KB4482887
LTSC	2019-02 B	2019-02-12	17763.316	KB4487044
LTSC	2019-01 D	2019-01-22	17763.292	KB4476976
LTSC	2019-01 B	2019-01-08	17763.253	KB4480116
LTSC	2018-12 OOB	2018-12-19	17763.195	KB4483235
LTSC	2018-12 B	2018-12-11	17763.194	KB4471332
LTSC	2018-11 D	2018-12-05	17763.168	KB4469342
LTSC	2018-11 B	2018-11-13	17763.134	KB4467708
LTSC	2018-10 D	2018-11-13	17763.107	KB4464455
LTSC	2018-10 B	2018-10-09	17763.55	KB4464330
LTSC	2018-10 A	2018-10-02	17763.1	

▼ Windows Server 2016 (OS build 14393)

テーブルを展開する

サービス オプション	更新プログラムの種類	公開日	構築	サポート技術情報の記事
LTSB	2026-01 B	2026-01-13	14393.8783	KB5073722
LTSB	2025-12 OOB	2025-12-18	14393.8692	KB5074974
LTSB	2025-12 B	2025-12-09	14393.8688	KB5071543
LTSB	2025-11 B	2025-11-11	14393.8594	KB5068864
LTSB	2025-10 OOB	2025-10-23	14393.8524	KB5070882
LTSB	2025-10 B	2025-10-14	14393.8519	KB5066836
LTSB	2025-09 B	2025-09-09	14393.8422	KB5065427
LTSB	2025-08 B	2025-08-12	14393.8330	KB5063871
LTSB	2025-07 B	2025-07-08	14393.8246	KB5062560
LTSB	2025-06 B	2025-06-10	14393.8148	KB5061010
LTSB	2025-05 B	2025-05-13	14393.8066	KB5058383
LTSB	2025-04 OOB	2025-04-11	14393.7973	KB5058921
LTSB	2025-04 B	2025-04-08	14393.7969	KB5055521
LTSB	2025-03 B	2025-03-11	14393.7876	KB5053594
LTSB	2025-02 B	2025-02-11	14393.7785	KB5052006
LTSB	2025-01 B	2025-01-14	14393.7699	KB5049993

LTSB	2024-12 B	2024-12-10	14393.7606	KB5048671
LTSB	2024-11 B	2024-11-12	14393.7515	KB5046612
LTSB	2024-10 B	2024-10-08	14393.7428	KB5044293
LTSB	2024-09 B	2024-09-10	14393.7336	KB5043051
LTSB	2024-08 B	2024-08-13	14393.7259	KB5041773
LTSB	2024-07 B	2024-07-09	14393.7159	KB5040434
LTSB	2024-06 B	2024-06-11	14393.7070	KB5039214
LTSB	2024-05 B	2024-05-14	14393.6981	KB5037763
LTSB	2024-04 B	2024-04-09	14393.6897	KB5036899
LTSB	2024-03 OOB	2024-03-22	14393.6800	KB5037423
LTSB	2024-03 B	2024-03-12	14393.6796	KB5035855
LTSB	2024-02 B	2024-02-13	14393.6709	KB5034767
LTSB	2024-01 B	2024-01-09	14393.6614	KB5034119
LTSB	2023-12 B	2023-12-12	14393.6529	KB5033373
LTSB	2023-11 B	2023-11-14	14393.6452	KB5032197
LTSB	2023-10 B	2023-10-10	14393.6351	KB5031362
LTSB	2023-09 B	2023-09-12	14393.6252	KB5030213
LTSB	2023-08 B	2023-08-08	14393.6167	KB5029242
LTSB	2023-07 B	2023-07-11	14393.6085	KB5028169
LTSB	2023-06 OOB	2023-06-23	14393.5996	KB5028623
LTSB	2023-06 B	2023-06-13	14393.5989	KB5027219
LTSB	2023-05 B	2023-05-09	14393.5921	KB5026363
LTSB	2023-04 B	2023-04-11	14393.5850	KB5025228
LTSB	2023-03 B	2023-03-14	14393.5786	KB5023697
LTSB	2023-02 B	2023-02-14	14393.5717	KB5022838
LTSB	2023-01 B	2023-01-10	14393.5648	KB5022289
LTSB	2022-12 B	2022-12-13	14393.5582	KB5021235
LTSB	2022-11 OOB	2022-11-17	14393.5502	KB5021654
LTSB	2022-11 B	2022-11-08	14393.5501	KB5019964
LTSB	2022-10 OOB	2022-10-18	14393.5429	KB5020439
LTSB	2022-10 B	2022-10-11	14393.5427	KB5018411

LTSB	2022-09 B	2022-09-13	14393.5356	KB5017305
LTSB	2022-08 B	2022-08-09	14393.5291	KB5016622
LTSB	2022-07 B	2022-07-12	14393.5246	KB5015808
LTSB	2022-06 B	2022-06-14	14393.5192	KB5014702
LTSB	2022-05 OOB	2022-05-19	14393.5127	KB5015019
LTSB	2022-05 B	2022-05-10	14393.5125	KB5013952
LTSB	2022-04 B	2022-04-12	14393.5066	KB5012596
LTSB	2022-03 B	2022-03-08	14393.5006	KB5011495
LTSB	2022-02 B	2022-02-08	14393.4946	KB5010359
LTSB	2022-01 OOB	2022-01-17	14393.4889	KB5010790
LTSB	2022-01 B	2022-01-11	14393.4886	KB5009546
LTSB	2022-01 OOB	2022-01-05	14393.4827	KB5010195
LTSB	2021-12 B	2021-12-14	14393.4825	KB5008207
LTSB	2021-11 OOB	2021-11-14	14393.4771	KB5008601
LTSB	2021-11 B	2021-11-09	14393.4770	KB5007192
LTSB	2021-10 B	2021-10-12	14393.4704	KB5006669
LTSB	2021-09 B	2021-09-14	14393.4651	KB5005573
LTSB	2021-08 B	2021-08-10	14393.4583	KB5005043
LTSB	2021-07 OOB	2021-07-29	14393.4532	KB5005393
LTSB	2021-07 B	2021-07-13	14393.4530	KB5004238
LTSB	2021-07 OOB	2021-07-07	14393.4470	KB5004948
LTSB	2021-06 B	2021-06-08	14393.4467	KB5003638
LTSB	2021-05 B	2021-05-11	14393.4402	KB5003197
LTSB	2021-04 B	2021-04-13	14393.4350	KB5001347
LTSB	2021-03 OOB	2021-03-18	14393.4288	KB5001633
LTSB	2021-03 B	2021-03-09	14393.4283	KB5000803
LTSB	2021-02 B	2021-02-09	14393.4225	KB4601318
LTSB	2021-01 B	2021-01-12	14393.4169	KB4598243
LTSB	2020-12 B	2020-12-08	14393.4104	KB4593226
LTSB	2020-11 OOB	2020-11-19	14393.4048	KB4594441
LTSB	2020-11 B	2020-11-10	14393.4046	KB4586830

LTSB	2020-10 B	2020-10-13	14393.3986	KB4580346
LTSB	2020-09 B	2020-09-08	14393.3930	KB4577015
LTSB	2020-08 B	2020-08-11	14393.3866	KB4571694
LTSB	2020-07 B	2020-07-14	14393.3808	KB4565511
LTSB	2020-06 OOB	2020-06-18	14393.3755	KB4567517
LTSB	2020-06 B	2020-06-09	14393.3750	KB4561616
LTSB	2020-05 B	2020-05-12	14393.3686	KB4556813
LTSB	2020-04 C	2020-04-21	14393.3659	KB4550947
LTSB	2020-04 B	2020-04-14	14393.3630	KB4550929
LTSB	2020-03 C	2020-03-17	14393.3595	KB4541329
LTSB	2020-03 B	2020-03-10	14393.3564	KB4540670
LTSB	2020-02 C	2020-02-25	14393.3542	KB4537806
LTSB	2020-02 B	2020-02-11	14393.3504	KB4537764
LTSB	2020-01 C	2020-01-23	14393.3474	KB4534307
LTSB	2020-01 B	2020-01-14	14393.3443	KB4534271
LTSB	2019-12 B	2019-12-10	14393.3384	KB4530689
LTSB	2019-11 B	2019-11-12	14393.3326	KB4525236
LTSB	2019-10 C	2019-10-15	14393.3300	KB4519979
LTSB	2019-10 B	2019-10-08	14393.3274	KB4519998
LTSB	2019-09 OOB	2019-10-03	14393.3243	KB4524152
LTSB	2019-09 C	2019-09-24	14393.3242	KB4516061
LTSB	2019-09 OOB	2019-09-23	14393.3206	KB4522010
LTSB	2019-09 B	2019-09-10	14393.3204	KB4516044
LTSB	2019-08 C	2019-08-17	14393.3181	KB4512495
LTSB	2019-08 B	2019-08-13	14393.3144	KB4512517
LTSB	2019-07 C	2019-07-16	14393.3115	KB4507459
LTSB	2019-07 B	2019-07-09	14393.3085	KB4507460
LTSB	2019-06 OOB	2019-06-27	14393.3056	KB4509475
LTSB	2019-06 C	2019-06-18	14393.3053	KB4503294
LTSB	2019-06 B	2019-06-11	14393.3025	KB4503267
LTSB	2019-05 C	2019-05-23	14393.2999	KB4499177

LTSB	2019-05 OOB	2019-05-19	14393.2972	KB4505052
LTSB	2019-05 B	2019-05-14	14393.2969	KB4494440
LTSB	2019-04 C	2019-04-25	14393.2941	KB4493473
LTSB	2019-04 OOB	2019-04-25	14393.2908	KB4499418
LTSB	2019-04 B	2019-04-09	14393.2906	KB4493470
LTSB	2019-03 C	2019-03-19	14393.2879	KB4489889
LTSB	2019-03 B	2019-03-12	14393.2848	KB4489882
LTSB	2019-02 C	2019-02-19	14393.2828	KB4487006
LTSB	2019-02 B	2019-02-12	14393.2791	KB4487026
LTSB	2019-01 C	2019-01-17	14393.2759	KB4480977
LTSB	2019-01 B	2019-01-08	14393.2724	KB4480961
LTSB	2018-12 OOB	2018-12-19	14393.2670	KB4483229
LTSB	2018-12 B	2018-12-11	14393.2665	KB4471321
LTSB	2018-11 OOB	2018-12-03	14393.2641	KB4478877
LTSB	2018-11 C	2018-11-27	14393.2639	KB4467684
LTSB	2018-11 B	2018-11-13	14393.2608	KB4467691
LTSB	2018-10 C	2018-10-18	14393.2580	KB4462928
LTSB	2018-10 B	2018-10-09	14393.2551	KB4462917
LTSB	2018-09 C	2018-09-20	14393.2515	KB4457127
LTSB	2018-09 B	2018-09-11	14393.2485	KB4457131
LTSB	2018-08 C	2018-08-30	14393.2457	KB4343884
LTSB	2018-08 B	2018-08-14	14393.2430	KB4343887
LTSB	2018-07 OOB	2018-07-30	14393.2396	KB4346877
LTSB	2018-07 C	2018-07-24	14393.2395	KB4338822
LTSB	2018-07 OOB	2018-07-16	14393.2368	KB4345418
LTSB	2018-07 B	2018-07-10	14393.2363	KB4338814
LTSB	2018-06 C	2018-06-21	14393.2339	KB4284833
LTSB	2018-06 B	2018-06-12	14393.2312	KB4284880
LTSB	2018-05 C	2018-05-17	14393.2273	KB4103720
LTSB	2018-05 B	2018-05-08	14393.2248	KB4103723
LTSB	2018-04 C	2018-04-17	14393.2214	KB4093120

LTSB	2018-04 B	2018-04-10	14393.2189	KB4093119
LTSB	2018-03 OOB	2018-03-29	14393.2156	KB4096309
LTSB	2018-03 C	2018-03-22	14393.2155	KB4088889
LTSB	2018-03 B	2018-03-13	14393.2125	KB4088787
LTSB	2018-02 C	2018-02-22	14393.2097	KB4077525
LTSB	2018-02 B	2018-02-13	14393.2068	KB4074590
LTSB	2018-01 C	2018-01-17	14393.2035	KB4057142
LTSB	2018-01 B	2018-01-03	14393.2007	KB4056890
LTSB	2017-12 B	2017-12-12	14393.1944	KB4053579
LTSB	2017-11 C	2017-11-27	14393.1914	KB4051033
LTSB	2017-11 B	2017-11-14	14393.1884	KB4048953
LTSB	2017-10 OOB	2017-11-02	14393.1797	KB4052231
LTSB	2017-10 C	2017-10-17	14393.1794	KB4041688
LTSB	2017-10 B	2017-10-10	14393.1770	KB4041691
LTSB	2017-09 C	2017-09-28	14393.1737	KB4038801
LTSB	2017-09 B	2017-09-12	14393.1715	KB4038782
LTSB	2017-08 OOB	2017-08-28	14393.1670	KB4039396
LTSB	2017-08 C	2017-08-16	14393.1613	KB4034661
LTSB	2017-08 B	2017-08-08	14393.1593	KB4034658
LTSB	2017-08 OOB	2017-08-07	14393.1537	KB4038220
LTSB	2017-07 C	2017-07-18	14393.1532	KB4025334
LTSB	2017-07 B	2017-07-11	14393.1480	KB4025339
LTSB	2017-06 C	2017-06-27	14393.1378	KB4022723
LTSB	2017-06 B	2017-06-13	14393.1358	KB4022715
LTSB	2017-05 B	2017-05-09	14393.1198	KB4019472
LTSB	2017-04 B	2017-04-11	14393.1066	KB4015217
LTSB	2017-03 OOB	2017-03-20	14393.969	KB4015438
LTSB	2017-03 B	2017-03-14	14393.953	KB4013429
LTSB	2017-01 B	2017-01-10	14393.693	KB3213986
LTSB	2016-12 B	2016-12-13	14393.576	KB3206632
LTSB	2016-11 C	2016-12-09	14393.479	KB3201845

LTSB	2016-11 B	2016-11-08	14393.447	KB3200970
LTSB	2016-10 D	2016-10-27	14393.351	KB3197954
LTSB	2016-10 B	2016-10-11	14393.321	KB3194798
LTSB	2016-09 D	2016-09-29	14393.222	KB3194496
LTSB	2016-09 B	2016-09-20	14393.187	KB3193494
LTSB	2016-09 B	2016-09-13	14393.187	KB3189866
LTSB	2016-08 E	2016-08-31	14393.105	KB3176938
LTSB	2016-08 D	2016-08-23	14393.82	KB3176934
LTSB	2016-08 B	2016-08-09	14393.51	KB3176495
LTSB	2016-08 A	2016-08-02	14393.10	KB3176929

Windows Server のホットパッチ カレンダー

Windows Server 2025 と Windows Server 2022 のホットパッチ更新プログラムのカレンダーを表示します。ホットパッチの適用を行うと、デバイスはカレンダーの年の各四半期の最初の月にベースラインの累積的な更新プログラムを受信します。ベースラインの更新プログラムをインストールするには、再起動が必要です。次の 2 か月間に、デバイスはホットパッチ更新プログラムを受信します。これには、セキュリティ更新プログラムのみが含まれ、再起動なしでインストールされます。

Windows Server 2025 (OS build 26100)

各更新プログラムの内容の詳細については、「Windows Server 2025 Datacenter Azure Edition に対するホットパッチのリリース ノート」を参照してください。

カレンダーの年 2026

テーブルを展開する

月	更新プログラムの種類	タイプ	公開日	構築	サポート技術情報の記事
1月	2026.01 B	ベースライン (再起動)	2026-01-13	26100.32230	KB5073379
2月	2026.02 B	ホットパッチ			
3月	2026.03 B	ホットパッチ			
4月	2026.04 B	ベースライン (再起動)			
5月	2026.05 B	ホットパッチ			
6月	2026.06 B	ホットパッチ			
7月	2026.07 B	ベースライン (再起動)			
8月	2026.08 B	ホットパッチ			

9月	2026.09 B	ホットパッチ
10月	2026.10 B	ベースライン (再起動)
11月	2026.11 B	ホットパッチ
12月	2026.12 B	ホットパッチ

▼ カレンダーの年 2025

テーブルを展開する

月	更新プログラムの種類	タイプ	公開日	構築	サポート技術情報の記事
1月	2025.01 B	ベースライン (再起動)	2025-01-14	26100.2894	KB5050009
2月	2025.02 B	ホットパッチ	2025-02-11	26100.3107	KB5052105
3月	2025.03 B	ホットパッチ	2025-03-11	26100.3403	KB5053636
4月	2025.04 B	ベースライン (再起動)	2025-04-08	26100.3775	KB5055523
5月	2025.05 B	ホットパッチ	2025-05-13	26100.3981	KB5058497
6月	2025.06 B	ホットパッチ	2025-06-10	26100.4270	KB5060841
7月	2025.07 B	ベースライン (再起動)	2025-07-08	26100.4652	KB5062553
8月	2025.08 B	ホットパッチ	2025-08-12	26100.4851	KB5064010
9月	2025.09 B	ホットパッチ	2025-09-09	26100.6508	KB5065474
10月	2025.10 B	ベースライン (再起動)	2025-10-14	26100.6899	KB5066835
11月	2025.11 B	ホットパッチ	2025-11-11	26100.7092	KB5068966
12月	2025.12 B	ホットパッチ	2025-12-09	26100.7392	KB5072014

▼ カレンダーの年 2024

テーブルを展開する

月	更新プログラムの種類	タイプ	公開日	構築	サポート技術情報の記事
11月	2024.11 B	ホットパッチ	2024-11-12	26100.2240	KB5046696
12月	2024.12 B	ホットパッチ	2024-12-10	26100.2528	KB5048794

▼ Windows Server 2022 (OS build 20348)

各更新プログラムの内容の詳細については、「Azure Automanage for Windows Server 2022 に対するホットパッチのリリース ノート」を参照してください。

カレンダーの年 2026

テーブルを展開する

月	更新プログラムの種類	タイプ	公開日	構築	サポート技術情報の記事
1月	2026.01 B	ベースライン (再起動)	2026-01-13	20348.4648	KB5073457
2月	2026.02 B	ホットパッチ			
3月	2026.03 B	ホットパッチ			
4月	2026.04 B	ベースライン (再起動)			
5月	2026.05 B	ホットパッチ			
6月	2026.06 B	ホットパッチ			
7月	2026.07 B	ベースライン (再起動)			
8月	2026.08 B	ホットパッチ			
9月	2026.09 B	ホットパッチ			
10月	2026.10 B	ベースライン (再起動)			
11月	2026.11 B	ホットパッチ			
12月	2026.12 B	ホットパッチ			

▼ カレンダーの年 2025

テーブルを展開する

月	更新プログラムの種類	タイプ	公開日	構築	サポート技術情報の記事
1月	2025.01 B	ベースライン (再起動)	2025-01-14	20348.3091	KB5049983
2月	2025.02 B	ホットパッチ	2025-02-11	20348.3148	KB5052106
3月	2025.03 B	ホットパッチ	2025-03-11	20348.3270	KB5053638
4月	2025.04 B	ベースライン (再起動)	2025-04-08	20348.3453	KB5055526
5月	2025.05 B	ホットパッチ	2025-05-13	20348.3630	KB5058500
6月	2025.06 B	ホットパッチ	2025-06-10	20348.3745	KB5060525
7月	2025.07 B	ベースライン (再起動)	2025-07-08	20348.3932	KB5062572
8月	2025.08 B	ホットパッチ	2025-08-12	20348.3989	KB5063812
9月	2025.09 B	ホットパッチ	2025-09-09	20348.4106	KB5065306
10月	2025.10 B	ベースライン (再起動)	2025-10-14	20348.4294	KB5066782
11月	2025.11 B	ホットパッチ	2025-11-11	20348.4346	KB5068840
12月	2025.12 B	ホットパッチ	2025-12-09	20348.4467	KB5071413

▼ カレンダーの年 2024

テーブルを展開する

月	更新プログラムの種類	タイプ	公開日	構築	サポート技術情報の記事
1月	2024.01 B	ベースライン (再起動)	2024-01-09	20348.2227	KB5034129
2月	2024.02 B	ホットパッチ	2024-02-13	20348.2277	KB5034860
3月	2024.03 B	ホットパッチ	2024-03-12	20348.2333	KB5035959
4月	2024.04 B	ベースライン (再起動)	2024-04-09	20348.2402	KB5036909
5月	2024.05 B	ホットパッチ	2024-05-14	20348.2458	KB5037848
6月	2024.06 B	ホットパッチ	2024-06-11	20348.2522	KB5039330
7月	2024.07 B	ベースライン (再起動)	2024-07-09	20348.2582	KB5040437
8月	2024.08 B*	ベースライン (再起動)	2024-08-13	20348.2655	KB5041160
9月	2024.09 B	ホットパッチ	2024-09-10	20348.2695	KB5042880
10月	2024.10 B	ベースライン (再起動)	2024-10-08	20348.2762	KB5044281
11月	2024.11 B	ホットパッチ	2024-11-12	20348.2819	KB5046698
12月	2024.12 B	ホットパッチ	2024-12-10	20348.2908	KB5048800

* のマークが付いたリリースは当初はホットパッチ更新プログラムとして計画されたものです。

Last updated on 2026/01/16

Windows Server 2025 の既知の問題と通知

Windows Server 2025 の既知の問題とサービスの状態に関する情報を確認します。 Windows 更新プログラムの問題に関する即時のヘルプについては、Windows デバイスを使用してヘルプアプリを開くか、support.microsoft.com に移動する場合は、ここをクリックしてください。 X for Windows リリースの正常性更新プログラムの @WindowsUpdate に従います。 IT 管理者で、プログラムによってこのページから情報を取得する場合は、Microsoft Graph の Windows Updates API を使用します。

2024 年 11 月 6 日時点の現在の状態

Windows Server 2025 が一般公開されました。 高パフォーマンスの AI 対応プラットフォームで、セキュリティの進歩と新しいハイブリッド クラウド機能を提供します。 Windows Server 2025 は、Windows Server. 用の Microsoft の最新の Long-Term サービス チャネル (LTSC) リリースです無料の 180 日間の評価をダウンロードするには、Microsoft 評価センター にアクセスしてください。

Windows Server 2025 は、組織がインプレース アップグレードを実行する場合、Windows Server 2022 および Window Server 2019 デバイスの**オプション**更新プログラムとして提供されます。 2025 が自動的にインストールされないWindows Server、これらの方法を使用して、Windows Server機能更新プログラムを展開することをお勧めします。

Windows Serverのライフサイクル ポリシーの詳細については、Windows Server 2025 lifecycle の記事を参照してください。

Windows Server 2025 の新機能

高度な機能とイノベーションを確認する

Graph API Windows Server既知の問題を取得する

サポートされているWindows Serverバージョンでデータを使用できます

すべてのメッセージを表示 >

既知の問題

未解決の問題、過去 30 日間に更新されたコンテンツ、 セーフガードホールド に関する情報を参照してください。 特定の問題を見つけるには、ブラウザーで検索機能を使用します (Microsoft Edge の場合は Ctrl + F)。

テーブルを展開する

要約	発生元の更新プログラム	状態	最終更新日時
共有フォルダーからインストールした場合、WUSA 経由でインストールされたUpdatesが失敗する可能性があります この問題は、複数の .msu ファイルを含むネットワーク フォルダーから更新プログラムをインストールするときに発生する可能性があります。	OS ビルド 26100.4349 KB5060842 2025-06-10	軽減	2025-09-30 10:04 PT
Windows Server 2022 と Server 2019 が予期せず Windows Server 2025 にアップグレードされました この問題は軽減されました。 これは、一部のサード パーティ製アプリケーションを介して更新プログラムが管理されたときに観察されました。	該当なし	軽減	2024-11-13 17:15 PT

問題の詳細

2025 年 8 月

共有フォルダーからインストールした場合、WUSA 経由でインストールされたUpdatesが失敗する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
軽減	OS ビルド 26100.4349 KB5060842 2025-06-10	最終更新日: 2025-09-30、 10:04 PT オープン: 2025-08-15、 11:56 PT

Windows Update スタンドアロン インストーラー (WUSA) を使用してインストールされた Windows 更新プログラム 、WUSA を使用して更新プログラムがインストールされている場合、または複数の .msu ファイルを含むネットワーク共有から .msu ファイルをダブルクリックすると、エラー ERROR_BAD_PATHNAMEで失敗します。 これらの問題は、2025 年 5 月 28 日 (KB5060842) 以降にリリースされた更新プログラムをインストールしたデバイスで発生する可能性があります。

WUSA は、Windows Update エージェント API を使用して更新プログラムをインストールする方法であり、通常はエンタープライズ環境でのみ使用されます。 個人や家庭の設定では一般的ではありません。

この問題は、ネットワーク共有に .msu ファイルが 1 つしかない場合や、.msu ファイルがデバイスにローカルに保存されている場合には発生しません。 さらに、WUSA をダブルクリックまたは使用して .msu ファイルをインストールし、Windows を再起動すると、[設定] の [更新履歴] ページに、更新プログラムを完了するために再起動が必要であることが示され続ける場合があります。 これは一時的なものであり、それ自体で解決する必要があります。

回避 策： この問題を回避するには、.msu ファイルをデバイスにローカルに保存し、この場所から更新プログラムをインストールします。 また、WUSA 経由で .msu ファイルをインストールした後に Windows を再起動した場合は、[設定] の [更新履歴] ページを確認する前に 15 分以上待ってください。 この短い遅延の後、設定アプリは更新プログラムが正常にインストールされたかどうかを正しく示す必要があります。

軽減策: この問題は 既知のイシュー ロールバック (KIR) を使用して解決され、ほとんどのホーム ユーザーと管理されていないビジネス デバイスに対して自動的に解決されます。 Windows デバイスを再起動すると、解決策がデバイスに適用される時間を短縮できる可能性があります。

IT 管理者は、影響を受ける更新プログラムをインストールし、この問題が発生したマネージド デバイスのこの問題を解決できます。 これは、以下に示すグループ ポリシーをインストールして構成することで修正できます。 これらの特別なグループ ポリシーのデプロイと構成については グループ ポリシー[を使用して既知の問題のロールバックをデプロイする方法](#)に関するページを参照してください。 特別なグループ ポリシーは **Computer Configuration** > **Administrative Templates** > [**グループ ポリシー name]にあります。**

グループ ポリシーをグループ ポリシー名でダウンロードします。

- [Windows 11、バージョン 24H2、Windows Server、バージョン 2025](#) - Windows 11 24H2、Windows Server 2025 KB5062660 250806_17201 既知の問題のダウンロード Rollback.msi

次の手順: 今後の Windows 更新プログラムで、この問題の解決策のリリースに取り組んでいます。 詳細が利用可能な場合は、更新プログラムを提供します。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2
- サーバー: Windows Server 2025

ページのトップへ

2024 年 11 月

Windows Server 2022 と Server 2019 が予期せず Windows Server 2025 にアップグレードされました

テーブルを展開する

状態	発生元の更新プログラム	履歴
軽減	該当なし	最終更新日: 2024-11-13、 17:15 PT オープン: 2024-11-09、12:16 PT

Windows Server 2025 は、Windows Server 2019 および **Windows Server** 2022 を実行しているデバイスの Windows Update設定で**オプション**のアップグレードとして提供されることを目的としています。 特定の環境では、次の 2 つのシナリオが観察されました。

- 一部のデバイスは、Windows Server 2025 (KB5044284) に自動的にアップグレードされます。 これは、サードパーティ製品を使用してクライアントとサーバーの更新を管理する環境で観察されました。 環境内のサード パーティの更新プログラム ソフトウェアが機能更新プログラムを展開しないように構成されているかどうかを確認してください。 このシナリオは軽減されました。

- Windows Server 2025 へのアップグレードは、デバイスの **[Windows Update]** ページの **[設定]** に表示されるバナーにメッセージを介して提供されました。 このメッセージは、インプレース アップグレードを実行する組織を対象としています。 このシナリオは既に解決されています。

Windows Server 2025 機能更新プログラムは、アップグレード分類の "DeploymentAction=OptionalInstallation" の**下のオプション**更新プログラムとしてリリースされました。 機能更新プログラムのメタデータは、パッチ管理ツールで**推奨**されるのではなく、**省略可能**と解釈する必要があります。

Microsoft が推奨する方法を使用して、Windows Server機能更新プログラムを展開することをお勧めします。

次の手順: Microsoft は、ベスト プラクティスと推奨される手順を合理化するために、サード パーティのプロバイダーと協力しています。 Microsoft は、暫定的な手段として、**Windows Update**設定パネルを使用してアップグレード オファーを一時的に一時停止しました。 2025 年前半に提供される予定です。 Windows Server 2025 をインストールするための他のすべてのアップグレード方法は、通常のチャネルを通じて引き続き使用できます。

Windows Update経由のオファーが再開されると、IT 管理者は、[ターゲットの機能更新プログラムのバージョンを選択する] のグループ ポリシーでターゲット バージョンを "保留" に設定することで、機能更新プログラムオファー バナーを制御できるようになります このグループ ポリシーを使用して機能の更新プログラムを管理する方法については、「Windows Serverでのグループ ポリシーを使用した機能Updatesの管理」を参照してください。

注: Windows Server 2025 機能更新プログラムは、Windows 11 バージョン 24H2 で使用されたのと同じ KB 番号であったKB5044284 として、2024 年 11 月 1 日に利用可能になりました。 これは、クライアントとサーバーの両方の Windows 更新プログラムの KB 番号です。 Windows Server 2025 および Windows 11 バージョン 24H2 用にリリースされた今後の更新プログラムは、同じ KB 番号を共有しますが、リリース ノート サイトとリンクは異なります。

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2025;Windows Server 2022;Windows Server 2019

ページのトップへ

Windows 更新プログラムに関する問題を報告する

いつでも Microsoft に問題を報告するには、 フィードバック ハブ アプリを使用します。 詳細については、「 フィードバック ハブ アプリを使用して Microsoft にフィードバックを送信する 」を参照してください。

Windows の更新についてのヘルプが必要ですか?

Microsoft サポート コミュニティ を検索、参照、または質問します。 organizationをサポートしている IT 担当者の場合は、Microsoft 365 管理センターの Windows リリース正常性に関するページで詳細を確認してください。

自宅の PC を直接サポートするには、Windows のヘルプアプリを使用するか、Microsoft サポート にお問い合わせください。 組織は、 ビジネスのサポート を通じて即時サポートを要求できます。

お使いの言語でこのサイトを表示する

このサイトは、英語、繁体字中国語、簡体字中国語、フランス語 (フランス)、ドイツ語、イタリア語、日本語、韓国語、ポルトガル語 (ブラジル)、ロシア語、スペイン語 (スペイン) の 11 の言語 で利用できます。 ブラウザーの既定の言語が 11 のサポートされている言語の 1 つでない場合、すべてのテキストが英語で表示されます。 表示言語を手動で変更するには、このページの下部まで下にスクロールし、ページの左下に表示されている現在の言語をクリックし、サポートされている 11 の言語のいずれかを一覧から選択します。

Last updated on 2026/04/10

Windows Server 2025 で解決された問題

Windows Server 2025 の最近解決された問題に関する情報を確認します。 特定の問題を見つけるには、ブラウザーで検索機能を使用します (Microsoft Edge の場合は Ctrl + F)。 Windows 更新プログラムの問題に関する即時のヘルプについては、Windows デバイスを使用してヘルプアプリを開くか、support.microsoft.com に移動する場合は、ここをクリックしてください。 X for Windows リリースの正常性更新プログラムの @WindowsUpdate に従います。 IT 管理者で、プログラムによってこのページから情報を取得する場合は、Microsoft Graph の Windows Updates API を使用します。

解決済みの問題

テーブルを展開する

要約	発生元の更新プログラム	状態	解決日
Kerberos でのパスワードローテーションの失敗による認証の問題 この問題は、PKINIT プロトコルを使用する場合のニッチなシナリオで観察され、2025 年 4 月のセキュリティ更新プログラムで解決されます。	該当せず	解決済み KB5055523	2025-04-08 10:00 PT
クラウドでバックアップされたストレージにファイルを保存すると、アプリが応答しなくなる可能性があります 影響を受けるアプリには Outlook が含まれます。これは、Microsoft OneDrive に保存されている PST ファイルにアクセスするときに応答しなくなる可能性があります。	OS ビルド 26100.32230 KB5073379 2026-01-13	解決済み KB5078135	2026-01-23 14:00 PT
Azure Virtual Desktop と Windows 365 での接続と認証の失敗 2026 年 1 月の Windows 更新プログラムにより、Azure Virtual Desktop と Windows 365 で資格情報プロンプトのWindows アプリエラーが発生する	OS ビルド 26100.32230 KB5073379 2026-01-13	解決済み KB5077793	2026-01-17 14:00 PT
管理者以外は、MSI 修復操作を実行するときに予期しない UAC プロンプトを受け取る可能性があります	OS ビルド 26100.4946 KB5063878 2025-08-12	解決済み KB5065426	2025-09-09 10:00 PT

要約	発生元の更新プログラム	状態	解決日
この問題は、Autodesk AutoCAD や Office Professional Plus 2010 など、Windows インストーラー (MSI) を使用するアプリに影響する可能性があります。			
IIS Web サイトの読み込みに失敗する可能性がある HTTP.sys に依存するサーバー側アプリケーションでは、受信接続に問題が発生する可能性があります。	OS ビルド 26100.6899 KB5066835 2025-10-14	解決済み KB5068861	2025-11-11 10:00 PT
10,000 人を超える AD グループのディレクトリ同期が失敗する Microsoft Entra Connect Sync など、Active Directory Domain Services (AD DS) 同期に影響する問題	OS ビルド 26100.6584 KB5065426 2025-09-09	解決済み KB5068861	2025-11-11 10:00 PT
スマートカード認証の問題は、2025 年 10 月の Windows 更新プログラムで発生する可能性があります この問題は、Windows 暗号化サービスを強化するために導入されたセキュリティの変更に関連しています。	OS ビルド 26100.6899 KB5066835 2025-10-14	解決済み	2025-10-22 17:31 PT
Windows Recovery Environment (WinRE) で USB マウスとキーボードが動作しない この問題は、2025 年 10 月 14 日にリリースされた Windows 更新プログラムをインストールした後にのみ、WinRE 内の USB デバイスに影響します。	OS ビルド 26100.6899 KB5066835 2025-10-14	解決済み KB5070773	2025-10-20 14:00 PT
Microsoft Changjie Input メソッドを使用する場合に発生する問題 影響を受けるのは繁体字中国語を使用するデバイスのみです。 以前の IME バージョンに戻した場合、問題は回避されます。	OS ビルド 26100.4652 KB5062553 2025-07-08	解決済み KB5062660	2025-07-22 10:00 PT
信頼された起動が無効になっている一部のAzure仮想マシンは、起動に失敗する可能性があります これは、7 月のセキュリティ更新プログラムのインストール後に VBS が有効になっている特定の SKU に対する Gen 2 VM の小さなサブセットに影響します。	OS ビルド 26100.4652 KB5062553 2025-07-08	解決済み KB5064489	2025-07-13 14:00 PT
キー信頼モードでWindows Helloでログオンが失敗し、Kerberos イベントがログに記録される場合があります	OS ビルド 26100.3775 KB5055523 2025-04-08	解決済み KB5060842	2025-06-10 10:00 PT

要約	発生元の更新プログラム	状態	解決日
2025 年 4 月の更新プログラムは、Kerberos イベント ID 45 と 21 をログに記録するドメイン コントローラーでの動作をトリガーする可能性があります			
再起動後にドメイン コントローラーがネットワーク トラフィックを誤って管理する ドメイン ファイアウォール プロファイルが使用されていないため、アプリケーションまたはサービスが失敗する	該当せず	解決済み KB5060842	2025-06-10 10:00 PT
2025 年 2 月の更新プログラムをインストールした後、リモート デスクトップがフリーズする可能性がある この問題は現在、Windows Server 2025 デバイスに影響します。 解像度は、バージョン 24H2 Windows 11で使用できます。	OS ビルド 26100.3194 KB5051987 2025-02-11	解決済み KB5055523	2025-04-08 10:00 PT
一部のテキストは、インストール プロセス中に英語で表示される場合があります これは、CD や USB などの特定のメディアを使用して 2025 Windows Serverインストールする場合にのみ発生します	該当せず	解決済み KB5055523	2025-04-08 10:00 PT

問題の詳細

2026 年 1 月

クラウドでバックアップされたストレージにファイルを保存すると、アプリが応答しなくなる可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5078135	OS ビルド 26100.32230 KB5073379 2026-01-13	解決済み: 2026-01-23、14:00 PT オープン: 2026-01-20、 22:10 PT

2026 年 1 月 13 日以降にリリースされた Windows 更新プログラム (KB5073379) をインストールすると、OneDrive や Dropbox などのクラウドでバックアップされたストレージにファイルを開いたり保存したりするときに、一部のアプリケーションが応答しなくなるか、予期しないエラーが発生する可能性があります。

たとえば、 in OneDrive に PST ファイルを格納する Outlook の一部の構成では 応答が停止し reopen プロセス が終了 タスク マネージャー システムが再起動されます さらに、 ent emails が [送信済みアイテム] フォルダーに表示されず 以前にダウンロードされたメールがダウンロードされる場合があります again. 影響を受ける Outlook の構成には、主に従来の Outlook が含まれます。これは一般的にエンタープライズ ライセンスに関連付けられており、Windows のほとんどのホーム インストールには含まれていません。 Outlook の構成をチェックするには、「新しい Outlook と従来の Outlook の機能の比較」を参照してください。

解決策:

この問題は、2026 年 1 月 24 日にリリースされた帯域外 (OOB) 更新プログラム KB5078135 で解決され、Microsoft Update Catalog および この日以降にリリースされた更新プログラムから入手できます。 デバイスの最新の更新プログラムは、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

注: Microsoft Update Catalog から更新プログラムをダウンロードするには この記事で説明されている手順に従います。

OOB 更新プログラムをまだインストールしていないデバイスの場合は、Outlook 固有のシナリオに対するオプションの回避策があります。 Outlook PST ファイルを OneDrive から移動すると、この問題が解決されます。 ガイダンスについては OneDrive. から Outlook .pst データ ファイルを削除する方法 に関するドキュメントを参照してください。さらに、 email アカウントは、メール プロバイダーによってサポートされている場合は webmail 経由で引き続きアクセスできます。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 10バージョン 22H2;WINDOWS 10 ENTERPRISE LTSC 2021;Windows 10 Enterprise LTSC 2019
- サーバー: Windows Server 2025;Windows Serverバージョン 23H2;Windows Server 2022;Windows Server 2019

ページのトップへ

Azure Virtual Desktop と Windows 365 での接続と認証の失敗

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5077793	OS ビルド 26100.32230 KB5073379 2026-01-13	解決済み: 2026-01-17、14:00 PT オープン: 2026-01-14, 00:52 PT

2026 年 1 月の Windows セキュリティ更新プログラム (KB5073379) をインストールすると、一部のリモート接続アプリケーションで資格情報プロンプトエラーが発生する可能性があります。 これには、Windows クライアント デバイス、Azure Virtual Desktop、Windows 365上のWindows アプリを使用したリモート デスクトップ接続が含まれます。 Windows アプリは、特定の Windows ビルドでのこの問題の影響を受け、サインイン エラーが発生する可能性があります。

その他のリモート接続と関連するアプリケーションも同様に影響を受ける可能性があります。

解像 度： この問題に対処するために、 an out-of-band (OOB) 更新プログラムは Microsoft Update Catalog で 2026 年 1 月 17 日にリリースされました。 これは、KB5077793 として見つけることができます。

2026 年 1 月の Windows セキュリティ更新プログラムをまだ展開しておらず、IT 環境に影響を受けるアプリケーションと機能が含まれている場合は、代わりにこの OOB 更新プログラムを適用することをお勧めします。 その他のガイダンスについては、「 Microsoft Update カタログから更新プログラムをダウンロードする方法」を参照してください。 常に、デバイスの最新の更新プログラムをインストールすることをお勧めします。これには、この更新プログラムを含む重要な機能強化と問題解決が含まれています。

OOB がインストールされていない場合は、次のいずれかの接続オプションを一時的な回避策として使用できます。

- Windows 用リモート デスクトップ クライアントを使用して、ここで Azure Virtual Desktop に接続します (/previous-versions/remote-desktop-client/whats-new-windows?tabs=windows-msrdc-msi)
- windows.cloud.microsoft の Windows アプリ Web クライアントを使用して接続する

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 10バージョン 22H2;Windows 10、バージョン 21H2、Windows 10 Enterprise LTSC 2019
- サーバー: Windows Server 2025;Windows Server 2022;Windows Server 2019

ページのトップへ

2025 年 10 月

IIS Web サイトの読み込みに失敗する可能性がある

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5068861	OS ビルド 26100.6899 KB5066835	解決済み: 2025-11-11、10:00 PT オープン: 2025-10-16、16:06 PT

	2025-10-14

さらに調査した結果、この問題は 2025 年Windows Server適用されないと結論付けました。これは、バージョン 25H2 と 24H2 のWindows 11にのみ影響します。

この問題は、ユーザー Windows Server無視できます。

この問題がWindows 11に与える影響について学習するには、次のリンクから選択します。

- Windows 11、バージョン 25H2
- Windows 11 バージョン 24H2

以下で説明する問題は、この結果と 2025 年 11 月 14 日の編集の前に公開されました。

9 月 29 日以降に Windows 更新プログラムのリリースをインストールした後、HTTP.sys に依存するサーバー側アプリケーションで受信接続に問題が発生する可能性があります その結果、IIS Web サイトの読み込みに失敗し、"接続のリセット - エラー (ERR_CONNECTION_RESET)" などのメッセージが表示されたり、同様のエラーが表示されたりすることがあります。 これには、 http://localhost/でホストされている Web サイト、およびその他の IIS 接続が含まれます。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2

ページのトップへ

10,000 人を超える AD グループのディレクトリ同期が失敗する

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5068861	OS ビルド 26100.6584 KB5065426 2025-09-09	解決済み: 2025-11-11、10:00 PT オープン: 2025-10-14、17:49 PT

オンプレミスの Active Directory Domain Services (AD DS) に Active Directory ディレクトリ同期 (DirSync) コントロールを使用するアプリケーション (Connect Sync を使用 Microsoft Entraする場合など) は、10,000 を超える大規模な AD グループの同期が不完全になることがあります。 この問題は、2025 年 9 月の Windows セキュリティ更新プログラム (KB5065426) 以降の更新プログラムをインストールした後、Windows Server 2025 でのみ発生します。

解像 度： この問題は、2025 年 11 月 11 日にリリースされた Windows 更新プログラム、 KB5068861 、およびその日以降にリリースされた更新プログラムによって解決されました。 デバイスの最新の更新プロ

グラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

2025 年 11 月 11 日以降にリリースされた更新プログラム (KB5068861) をインストールした場合、この問題を解決するために、 Known Issue Rollback (KIR) または特別なグループ ポリシーを使用する必要はありません。

2025 年 11 月 11 日より前にリリースされた更新プログラムを使用していて、この問題が発生している場合、IT 管理者は、次に示す特別なグループ ポリシーをインストールして構成することで解決できます。

グループ ポリシー名を使用してダウンロードをグループ ポリシーします。

- Windows 11、バージョン 24H2、25H2、Windows Server 2025 のダウンロード -- Windows 11 24H2、Windows 11 25H2、Windows Server 2025 KB5066835 251016_21401 既知の問題ロールバック

特別なグループ ポリシーは **Computer Configuration -> 管理用テンプレート -> Windows 11 24H2、Windows 11 25H2、および Windows Server 2025 KB5066835 251016_21401 Known Issue Rollback**. グループ ポリシーをインストールした後、**KB5066835 251016_21401 既知の問題のロールバック**の値を **[無効]** に構成し、2025 Windows Server再起動してグループ ポリシー設定を適用します。 (Windows 11は、この通知とガイダンスの範囲外です)。この特別なグループ ポリシーのデプロイと構成については、「グループ ポリシーを使用して既知のイシュー ロールバックをデプロイする方法」を参照してください。

または、影響を受けるお客様は、機能の変更を無効にする回避策として、次のレジストリ キーを適用できます。

警告: レジストリ エディターを使用するか、別の方法を使用してレジストリを誤って変更すると、重大な問題が発生する可能性があります。 このような問題では、オペレーティング システムの再インストールが必要になることもあります。 Microsoft では、このような問題の解決に関しては保証できません。 レジストリを自分の責任で変更してください。 詳細については、「 高度なユーザー向けの Windows レジストリ」を参照してください。

パス:
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\Microsoft\FeatureManagement\Overrides

名前: 2362988687

型： Reg_dword

値: 0

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2025

ページのトップへ

スマートカード認証の問題は、2025 年 10 月の Windows 更新プログラムで発生する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済み	OS ビルド 26100.6899 KB5066835 2025-10-14	解決済み: 2025-10-22、17:31 PT オープン: 2025-10-17、20:06 PT

2025 年 10 月 14 日以降にリリースされた Windows Updates (KB5066835) をインストールした後、セキュリティの脆弱性 セキュリティの脆弱性 CVE-2024-30098 をインストールすると、スマート カード認証やその他の証明書操作が意図的に失敗する可能性があります。 この暗号化の強化の一環として、CSP (暗号化サービス プロバイダー) ではなく KSP (キー ストレージ プロバイダー) を使用するには、RSA ベースのスマート カード証明書が必要です。

CSP を使用する証明書の一般的な症状は次のとおりです。

- 32 ビット アプリケーションでスマート カードが CSP プロバイダー (暗号化サービス プロバイダー) として認識されない
- ドキュメントに署名できない
- 証明書ベースの認証に依存するアプリケーションのエラー
- "無効なプロバイダーの種類が指定されました" や "CryptAcquireCertificatePrivateKey エラー" などのエラー メッセージが表示される場合があります。

2025 年 10 月の Windows セキュリティ更新プログラム (KB5066835) をインストールする前に、システム ログに Smart Card Service または Microsoft-Windows-Smartcard-Server **Event ID: 624** メッセージ テキストが含まれている場合、スマート カードがこのセキュリティ適用の影響を受けるかどうかを検出できます。 詳細については、次のリンクを参照してください: https://go.microsoft.com/fwlink/?linkid=2300823 。

解像 度：

永続的な解決のために、 developers は、Key Storage API を使用してキー ストレージ取得を実行するように認証アプリ Key Storage and Retrieval を更新する必要があります。 開発者は、2026 年 4 月にリリースされた Windows 更新プログラムの前にこの変更を完了する必要があります。この時点で、以下に示す **DisableCapiOverrideForRSA** 回避策が削除される予定です。

回避策:

この問題が発生した場合は、 **DisableCapiOverrideForRSA** registry キーの値を 0 に設定することで、一時的に解決できます。 これは CVE-2024-30098 に記載されています。 レジストリ キーを変更するための詳細な手順を次に示します。 **注**: このオプションは、2026 年 4 月にリリース予定の Windows 更新プログラムで削除されます。

レジストリを変更する手順

⚠ <**重要**: レジストリを誤って編集すると、システムの問題が発生する可能性があります。 変更を行う前に、常にレジストリをバックアップしてください。

1. レジストリ エディターを開きます。

- Win + R キーを押し、「regedit」と入力し、Enter キーを押します。
- ユーザー アカウント制御のプロンプトが表示されたら、[はい] をクリックします。

2. サブキーに移動します。

- [移動]: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais

3. キーを編集し、値を設定します。

- カレー内で、キー DisableCapiOverrideForRSA が存在するかどうかをチェックします
- DisableCapiOverrideForRSA をダブルクリックします。
- [値の日付] に「0」と入力します。

注: DisableCapiOverrideForRSA レジストリ設定は、既定の OS インストールまたは Windows Updatesのインストールでは追加されず、各デバイスに手動で追加する必要があります。

4. 閉じて再起動します。

- レジストリ エディターを閉じます。
- 変更を有効にするには、コンピューターを再起動します。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 10バージョン 22H2
- サーバー: Windows Server 2025;Windows Server 23H2;Windows Server 2022;Windows Server 2019;Windows Server 2016。Windows Server 2012 R2

ページのトップへ

Windows Recovery Environment (WinRE) で USB マウスとキーボードが動作しない

⛶ **テーブルを展開する**

状態	発生元の更新プログラム	履歴
解決済みの KB5070773	OS ビルド 26100.6899 KB5066835	解決済み: 2025-10-20、14:00 PT オープン: 2025-10-17、22:18 PT

	2025-10-14

2025 年 10 月 14 日 (KB5066835) にリリースされた Windows セキュリティ更新プログラムをインストールした後、キーボードやマウスなどの USB デバイスは Windows Recovery Environment (WinRE) では機能しません。 この問題により、WinRE 内の回復オプションのナビゲーションが回避されます。 USB デバイスは引き続き Windows オペレーティング システム内で正常に動作します。

解像 度： この問題は、2025 年 10 月 20 日 (KB5070773) にリリースされた Windows 帯域外更新プログラムによって解決されました。これは、Microsoft Update Catalog Microsoft Update Catalog 、 、その日以降にリリースされた更新プログラムから入手できます。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

回避策: デバイスがこの問題の影響を受け、Windows で起動して最新の Windows 更新プログラムをインストールできない場合は、次のいずれかの方法でこの問題を回避できます。

- PC にタッチスクリーンがある場合は、タッチスクリーンのタッチ キーボードを使用して WinRE 内を移動できます。
- PC に PS/2 ポートがある場合は、PS/2 キーボードまたはマウスを使用して WinRE 内を移動できます。
- 以前に USB 回復ドライブ を作成していた場合は、回復ドライブからコンピューターを起動できます。 これにより、復元された USB 機能を使用して WinRE に直接移動します。
- OEM および企業は、Configuration Managerでプレブート実行環境 (PXE) を使用することも、Windows Assessment and Deployment Kit (Windows ADK) アドオンと Windows プレインストール環境 (WinPE) アドオンを使用してプッシュ ボタン リセット機能を展開して 影響を受けるデバイスを回復することもできます。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2
- サーバー: Windows Server 2025

ページのトップへ

2025 年 9 月

管理者以外は、MSI 修復操作を実行するときに予期しない UAC プロンプトを受け取る可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5065426	OS ビルド 26100.4946 KB5063878	解決済み: 2025-09-09、10:00 PT オープン: 2025-09-03、14:28 PT

	2025-08-12

(11/26/25 更新: [解決策] セクションに追加の機能強化が追加されました。

2025 年 8 月の Windows セキュリティ更新プログラム (KB5063878) 以降の更新プログラムには、Windows インストーラー (MSI) の修復および関連する操作を実行するときに、ユーザー アカウント制御 (UAC) が管理者の資格情報を求めるという要件が適用されます。 この改善により、セキュリティの脆弱性 CVE-2025-50173 が 解決されました。

その結果、2025 年 8 月の Windows セキュリティ更新プログラム以降の更新プログラムをインストールした後、次のシナリオでは、標準ユーザーに対して管理者権限の入力を求める UAC プロンプトが表示される可能性があります。

- MSI 修復コマンドの実行 (msiexec /fu など)。
- 一部のバージョンのAutoCAD、Civil 3D、Inventor CAM を含むオートデスク アプリケーションを起動するか、ユーザーが初めてアプリにサインインした後に MSI ファイルをインストールする場合。
- ユーザーごとに自身を構成するアプリケーションのインストール。
- アクティブセットアップ中の Windows インストーラーの実行。
- ユーザー固有の "アドバタイズ" 構成に依存する Manager Configuration Manager (ConfigMgr) を使用してパッケージを展開する。
- Secure Desktop の有効化。

標準ユーザーが UI を表示せずに MSI 修復操作を開始するアプリを実行すると、エラー メッセージで失敗します。 たとえば、Office Professional Plus 2010 を標準ユーザーとしてインストールして実行すると、構成プロセス中にエラー 1730 で失敗します。

解決策:

2025 年 9 月の Windows セキュリティ更新プログラム (KB5065426) 以降の更新プログラムをインストールした後、ターゲット MSI ファイルに追加されたカスタム アクションが含まれている場合にのみ、MSI 修復操作中に UAC プロンプトが必要になります この要件は、2025 年 11 月 11 日以降にリリースされた Windows 更新プログラムをインストールした後にさらに調整されるため、UAC プロンプトが必要になるのは 修復フロー中に昇格されたカスタム アクションが実行された場合のみです。

最新の Windows 更新プログラムをインストールすると、このような昇格されたカスタム アクション (Autodesk AutoCADなど) を実行しないアプリのこの問題が解決されます。

カスタム アクションを実行するアプリには UAC プロンプトが引き続き必要になるため、2025 年 9 月の更新プログラムをインストールした後、IT 管理者は、MSI ファイルを許可リストに追加することで、特定のアプリの UAC プロンプトを無効にする回避策にアクセスできます。 詳細については、「 2025 年 8 月の Windows セキュリティ更新プログラムをインストールした後に MSI 修復操作を実行するときに予期しない UAC プロンプトが表示 される」を参照してください。

この問題を回避するために、以前に Microsoft のビジネスサポート から Known Issue Rollback (KIR) からグループ ポリシーが提供されていました 組織では、この問題に対処するために、このグループ ポリシーをインストールして構成する必要がなくなりました。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 10バージョン 22H2;Windows 10バージョン 21H2;Windows 10 Version 1809。WINDOWS 10 ENTERPRISE LTSC 2019;WINDOWS 10 ENTERPRISE LTSC 2016;Windows 10バージョン 1607;Windows 10 Enterprise 2015 LTSB
- サーバー: Windows Server 2025;Windows Server 2022;Windows Serverバージョン 1809;Windows Server 2019;Windows Server 2016。Windows Server 2012 R2;Windows Server 2012。Windows Server 2008 R2;Windows Server 2008 SP2

ページのトップへ

2025 年 7 月

Microsoft Changjie Input メソッドを使用する場合に発生する問題

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5062660	OS ビルド 26100.4652 KB5062553 2025-07-08	解決済み: 2025-07-22、10:00 PT オープン: 2025-07-11, 08:52 PT

2025 年 7 月の Windows セキュリティ更新プログラム (KB5062553) のインストール後に、繁体字中国語の Microsoft Changjie IME (入力方法エディター) を使用するときに問題が発生する可能性があります。

この問題は、繁体字中国語が優先または共通の言語または入力方法であり、特に Changjie IME が使用されているデバイスにのみ影響します。 報告される症状は次のとおりです。

- 完全なコンポジションを入力した後に単語を形成または選択できない (フレーズ ウィンドウを関連付ける)
- spacebar または空白キーが応答しない
- 正しくない、または歪んだ単語の出力
- 変換候補ウィンドウが正しく表示されない

Microsoft Changjie は、Windows に含まれ、現在サポートされているバージョン 利用可能な IME です。

解決策: この問題は、2025 年 7 月の Windows 非セキュリティ更新プログラム (KB5062660) 以降の更新プログラムで解決されます。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

2025 年 7 月より前にリリースされた Windows 更新プログラムをインストールしている場合は、次の回避策を使用できます。 Windows IME では、代わりに以前のバージョンの IME を使用できる互換性設定がサポ

ートされています。 このオプションを使用すると、この問題を解決するのに役立ちます。

Microsoft Changjie IME の古いバージョンに戻すには、次の手順に従います。

1. **[言語&リージョン]** 設定を開きます。 これを行うには、 **設定** アプリを開き、[**時間 & 言語**]、[**言語 & リージョン]** の順に選択します。 スタート メニューを開き、「言語」と入力し、上位の結果を選択することもできます。
2. このデバイスで繁体字中国語が使用されている場合は、上部の近くに中国語 (繁体字) オプションが表示されます。 **[中国語 (繁体字)]** の横にある 3 つのドットを選択してメニューを開き、[**言語オプション**] を選択します。
3. [**キーボード**] で、 **Microsoft Changjie** の横にある 3 つのドットを選択し、メニューから [**キーボード オプション**] を選択します。
4. [**互換性**] で、[**以前のバージョンの Microsoft Changjie を使用**する] オプションを **[オン] に設定します**。 次に、[**OK] を選択します**。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 10バージョン 22H2;Windows 10 Version 1809。WINDOWS 10 ENTERPRISE LTSC 2016;バージョン 1607 Windows 10
- サーバー: Windows Server 2025;Windows Server 2022;Windows Serverバージョン 1809;Windows Server 2016

ページのトップへ

信頼された起動が無効になっている一部のAzure 仮想マシンは、起動に失敗する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5064489	OS ビルド 26100.4652 KB5062553 2025-07-08	解決済み: 2025-07-13、14:00 PT オープン: 2025-07-11, 00:18 PT

202 Windows 11 5 年またはバージョン 24H2 Windows Server実行されているAzure 仮想マシン (VM) のごく一部 (信頼された起動が無効になっているバージョン 24H2)、レジストリ キーを介して適用された Virtualization-Based セキュリティ (VBS) が、7 月の Windows セキュリティ更新プログラム (KB5062553) をインストールした後に起動できない可能性があります。

仮想マシンが影響を受ける可能性があるかどうかをチェックするには:

1. VM が "Standard" として作成されているかどうかを確認します。

2. VBS が有効になっているかどうかを確認します。 システム情報 (msinfo32.exe) を開き、仮想化ベースのセキュリティが実行されていることと Hyper-V ロールが VM にインストールされていないことを確認します。

解像 度： この問題は、アウトオブバンド (OOB) 更新プログラム KB5064489 で解決されました。これは、Microsoft Update Catalog . から入手できます。仮想マシンの構成がこの問題の影響を受けた場合は、KB5062553 ではなく、この帯域外の更新プログラムをインストールすることをお勧めします。

管理者は、ホットパッチ エディションを含む、Windows Server 2025 のすべてのエディションの更新された VM イメージを受け取ることができます。 新しいメディアは、2025 年 7 月の画像Windows Server 記事に記載されています。

注: 信頼された起動を有効にすることで、この問題を回避することもできます。 Windows 11を実行する Virtual Machinesには、トラステッド起動が必要です。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 24H2
- サーバー: Windows Server 2025

ページのトップへ

2025 年 5 月

キー信頼モードでWindows Helloでログオンが失敗し、Kerberos イベントがログに記録される場合があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5060842	OS ビルド 26100.3775 KB5055523 2025-04-08	解決済み: 2025-06-10、10:00 PT オープン: 2025-05-06、13:25 PT

2025 年 4 月 8 日 (KB5055523) 以降にリリースされた 4 月の Windows 月次セキュリティ更新プログラムをインストールすると、Active Directory **msds-KeyCredentialLink** フィールドを介してキー信頼に依存する証明書ベースの資格情報を使用して Kerberos ログオンまたは委任を処理するときに、Active Directory ドメイン コントローラー (DC) で認証の中断が発生する可能性があります。

これらの更新の後、DC が Kerberos 認証に使用する証明書を検証する方法が変更され、証明書が NTAuth ストアの発行元証明機関 (CA) にチェーンされている必要があります。 これは、「 KB5057784 - CVE-2025-26647 (Kerberos 認証の保護)」 で説明されているセキュリティ対策に関連しています。 その結果、デバイス公開キー認証 (Machine PKINIT とも呼ばれます) を展開した Windows Hello for Business (WHfB) キー信

頼環境または環境で認証エラーが発生する可能性があります。 この機能に依存する他の製品も影響を受ける可能性があります。

この検証メソッドの有効化は、. の Windows レジストリ値 **AllowNtAuthPolicyBypass** によって制御 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc**できます。DC の認証に 2025 年 4 月の Windows 月次セキュリティ更新プログラムをインストールした後、2 つのシナリオを確認できます。

- レジストリ値 **AllowNtAuthPolicyBypass** が構成解除されているか、"1" に設定されている場合、Kerberos-Key-Distribution-Center **イベント ID 45** は DC システム イベント ログに繰り返し記録されます。"キー配布センター (KDC) で、有効であったが NTAuth ストアの発行元 CA にチェーンされていないクライアント証明書が検出されました。 これは、安全でない証明書を使用して認証要求を処理する DC によって意図的にログに記録される新しいイベントです。 このイベントは過度にログに記録される可能性がありますが、関連するログオン操作は成功し、これらのイベント ログ レコードの外部で他の変更は行われません。

- レジストリ値 **AllowNtAuthPolicyBypass** が "2" に設定されている場合、自己署名証明書ベースの認証は失敗します。 Kerberos-Key-Distribution-Center **イベント ID 21** は、DC システム イベント ログに記録されます。 これは、証明書ベースの認証が失敗したときにログに記録されるレガシ イベントであり、DC が安全でない証明書を使用して認証要求をサービスするときに意図的にログに記録されます。 このイベントのイベント説明テキストは異なる場合があります。

AllowNtAuthPolicyBypass レジストリ キーが存在しない場合、DC は値が "1" に構成されているかのように動作します。 キーが存在しない場合は、手動で作成し、上記のように構成できます。

2025 年 4 月 8 日以降にリリースされた Windows Updates、NTAuth ストア内の CA にチェーンされない自己署名証明書を使用して認証要求を処理するときに、イベント ID 45 と 21 が誤ってログに記録されます。 自己署名証明書は、次のシナリオで AD PKINIT キー信頼機能によって使用される場合があります。

- Windows Hello for Business (WHfB) キー信頼デプロイ
- デバイス公開キー認証 (マシン PKINIT とも呼ばれます)。
- スマート カード製品、サード パーティ製シングル サインオン (SSO) ソリューション、ID 管理システムなど、**msds-KeyCredentialLink** フィールドに依存するその他のシナリオ。

解決策: この問題は、2025 年 6 月 10 日 (KB5060842) 以降にリリースされた Windows 更新プログラムによって解決されました。 デバイスの最新のセキュリティ更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

2025 年 6 月 10 日以降にリリースされた更新プログラムをインストールする場合は、この問題の回避策を使用する必要はありません。 この日付より前にリリースされた更新プログラムを使用していて、この問題が発生した場合は、自己署名証明書ベースの認証を処理する更新された DC で、レジストリ キー **AllowNtAuthPolicyBypass** に値 '2' を設定するのを一時的に遅らせる必要があります。 詳細については、「KB5057784 のレジストリ設定」セクションを参照してください。

影響を受けるプラットフォーム:

- クライアント: なし

- サーバー: Windows Server 2025;Windows Server 2022;Windows Server 2019;Windows Server 2016

ページのトップへ

2025 年 4 月

Kerberos でのパスワードローテーションの失敗による認証の問題

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5055523	該当せず	解決済み: 2025-04-08、10:00 PT オープン: 2025-04-07、16:30 PT

Windows Server 2025 をインストールした後、Identity Update Manager 証明書/公開キー暗号化 (PKNIT) を使用しているデバイスで、パスワードが正しく回転せず、認証エラーが発生する可能性があります。 この問題は、特に Kerberos 認証 が使用され、 Credential Guard 機能が有効になっている場合に発生します。 PKINIT パスを使用したマシン認定はニッチなユース ケースであり、この問題はエンタープライズ環境の少数のデバイスに影響します。

この問題により、デバイスは既定の間隔として 30 日ごとにパスワードを変更できません。 このエラーが発生したため、デバイスは古い、無効、または削除されたと認識され、ユーザー認証の問題が発生します。

Kerberos 認証は通常エンタープライズ環境で使用され、個人設定やホーム設定では一般的ではないため、Windows Home エディションを実行しているデバイスはこの問題の影響を受ける可能性は低いです。

解像 度：

この問題は、2025 年 4 月の Windows セキュリティ更新プログラム (KB5055523) 以降の更新プログラムで解決されます。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

メモ： Kerberos 経由のマシン パスワードローテーションに依存する **Credential Guard の機能 Machine Accounts** は、永続的な修正が利用可能になるまで無効になっています。 この機能の可用性の詳細については、「 Credential Guard で保護されたマシン アカウント」を参照してください。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 24H2
- サーバー: Windows Server 2025

ページのトップへ

再起動後にドメイン コントローラーがネットワーク トラフィックを誤って管理する

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5060842	該当せず	解決済み: 2025-06-10、10:00 PT オープン: 2025-04-11、13:20 PT

Windows Server 2025 ドメイン コントローラー (Active Directory ドメイン コントローラー ロールをホストしているサーバーなど) は、再起動後にネットワーク トラフィックを正しく管理できない可能性があります。 その結果、Windows Server 2025 ドメイン コントローラーにドメイン ネットワークでアクセスできない場合や、ドメイン ファイアウォール プロファイルで防止する必要があるポートとプロトコルを介して正しくアクセスできない場合があります。

この問題は、ドメイン コントローラーが再起動されるたびにドメイン ファイアウォール プロファイルの使用に失敗した結果です。 代わりに、標準のファイアウォール プロファイルが使用されます。 その結果、ドメイン コントローラーまたはリモート デバイスで実行されているアプリケーションまたはサービスが失敗したり、ドメイン ネットワークで到達できない状態のままになる可能性があります。

回避 策： ネットワーク アダプターを再起動すると、予期される動作を復元できます。 これは、PowerShell を使用して次のコマンドを使用するなど、さまざまな方法で手動で実行できます。

```
Restart-NetAdapter *
```

この問題はドメイン コントローラーが再起動されるたびにトリガーされるため、ドメイン コントローラーが再起動されるたびにこの回避策を繰り返す必要があることに注意してください。 ドメイン コントローラーが再起動されるたびにネットワーク アダプターを再起動するスケジュールされたタスクを作成すると便利な場合があります。

解決策: この問題は、2025 年 6 月の Windows セキュリティ更新プログラム (KB5060842) 以降の更新プログラムで解決されます。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2025

ページのトップへ

2025 年 3 月

2025 年 2 月の更新プログラムをインストールした後、リモート デスクトップがフリーズする可能性がある

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5055523	OS ビルド 26100.3194 KB5051987 2025-02-11	解決済み: 2025-04-08、10:00 PT オープン: 2025-03-25、10:26 PT

2025 年 2 月 11 日以降にリリースされた 2025 年 2 月のセキュリティ更新プログラム (KB5051987) を Windows Server 2025 デバイスにインストールした後、接続直後にリモート デスクトップ セッションがフリーズする可能性があります。 この問題が発生すると、マウスとキーボードの入力がセッション内で応答しなくなり、ユーザーは切断して再接続する必要があります。

解像 度 :

この問題は、 KB5055523 で解決されています。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 24H2
- サーバー: Windows Server 2025

ページのトップへ

2024 年 10 月

一部のテキストは、インストール プロセス中に英語で表示される場合があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5055523	該当せず	解決済み: 2025-04-08、10:00 PT オープン: 2024-10-31、13:12 PT

Windows Server 2025 をインストールすると、インストールに選択されている言語に関係なく、インストール プロセス中に英語で一部のテキストが表示されることがあります。 これは、インストールに英語以外の言語が選択されている場合に顕著になります。

これは、CD や USB フラッシュ ドライブなどのメディアを使用して、Windows Server 2025 をインストールする場合にのみ発生します。 この問題は、多言語ユーザー インターフェイス (MUI) を使用Windows Server メディア 25100.1742 以降でのみ発生します。

解決策: この問題は、2025 年 4 月 8 日 (KB5055523) 以降にリリースされた Windows 更新プログラムによって解決されました。 デバイスの最新のセキュリティ更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2025

ページのトップへ

Windows 更新プログラムに関する問題を報告する

いつでも Microsoft に問題を報告するには、 フィードバック ハブ アプリを使用します。 詳細については、「 フィードバック ハブ アプリを使用して Microsoft にフィードバックを送信する」を参照してください。

Windows の更新についてのヘルプが必要ですか?

Microsoft サポート コミュニティ を検索、参照、または質問します。 organizationをサポートしている IT 担当者の場合は、Microsoft 365 管理センターの Windows リリース正常性に関するページで詳細を確認してください。

自宅の PC を直接サポートするには、Windows のヘルプアプリを使用するか、Microsoft サポート にお問い合わせください。 組織は、 ビジネスのサポート を通じて即時サポートを要求できます。

お使いの言語でこのサイトを表示する

このサイトは、英語、繁体字中国語、簡体字中国語、フランス語 (フランス)、ドイツ語、イタリア語、日本語、韓国語、ポルトガル語 (ブラジル)、ロシア語、スペイン語 (スペイン) の 11 の言語 で利用できます。 ブラウザーの既定の言語が 11 のサポートされている言語の 1 つでない場合、すべてのテキストが英語で表示されます。 表示言語を手動で変更するには、このページの下部まで下にスクロールし、ページの左下に表示されている現在の言語をクリックし、サポートされている 11 の言語のいずれかを一覧から選択します。

Last updated on 2026/04/10

Windows Server 2022

既知の問題と通知

Windows Server 2022 の既知の問題とサービスの状態に関する情報を確認します。 Windows 更新プログラムの問題に関する即時のヘルプについては、Windows デバイスを使用してヘルプアプリを開くか、support.microsoft.com に移動する場合は、ここをクリックしてください。 Windows リリースの正常性更新プログラムについては、X (旧称 Twitter) の @WindowsUpdate に従ってください。 IT 管理者で、プログラムによってこのページから情報を取得する場合は、Microsoft Graph の Windows Updates API を使用します。

2025 年 5 月 2 日時点の現在の状態

Windows Server 2022 一般公開されています。 サービス要件とその他の重要な情報の詳細については **サービス チャネルの Comparison** を参照してください。

詳細については、「 the Windows Server 2022 lifecycle」ページを参照してください。

注: Windows Server 2025 は、Windows Serverの最新の Long-Term サービス チャネル (LTSC) リリースになりました。 無料の 180 日評価版をダウンロードするには Microsoft Evaluation Center にアクセスしてください。

Windows Server 2025 の新機能

高度な機能とイノベーションを確認する

Graph API Windows Server既知の問題を取得する

サポートされているWindows Serverバージョンでデータを使用できます

すべてのメッセージを表示 >

既知の問題

未解決の問題、過去 30 日間に更新されたコンテンツ、 セーフガードホールド に関する情報を参照してください。 特定の問題を見つけるには、ブラウザーで検索機能を使用します (Microsoft Edge の場合は Ctrl + F)。

テーブルを展開する

要約	発生元の更新プログラム	状態	最終更新日時
Windows Server 2022 と Server 2019 が予期せず Windows Server 2025 にアップグレードされました この問題は軽減されました。 これは、一部のサード パーティ製アプリケーションを介して更新プログラムが管理されたときに観察されました。	該当なし	軽減	2024-11-13 17:15 PT

問題の詳細

2024 年 11 月

Windows Server 2022 と Server 2019 が予期せず Windows Server 2025 にアップグレードされました

テーブルを展開する

状態	発生元の更新プログラム	履歴
軽減	該当なし	最終更新日: 2024-11-13、 17:15 PT オープン: 2024-11-09、12:16 PT

Windows Server 2025 は、Windows Server 2019 および **Windows Server** 2022 を実行しているデバイスの Windows Update設定で**オプション**のアップグレードとして提供されることを目的としています。 特定の環境では、次の 2 つのシナリオが観察されました。

- 一部のデバイスは、Windows Server 2025 (KB5044284) に自動的にアップグレードされます。 これは、サードパーティ製品を使用してクライアントとサーバーの更新を管理する環境で観察されました。 環境内のサード パーティの更新プログラム ソフトウェアが機能更新プログラムを展開しないように構成されているかどうかを確認してください。 このシナリオは軽減されました。

- Windows Server 2025 へのアップグレードは、デバイスの **[Windows Update]** ページの **[設定]** に表示されるバナーにメッセージを介して提供されました。 このメッセージは、インプレース アップグレードを実行する組織を対象としています。 このシナリオは既に解決されています。

Windows Server 2025 機能更新プログラムは、アップグレード分類の "DeploymentAction=OptionalInstallation" の**下のオプション**更新プログラムとしてリリースされました。 機能更新プログラムのメタデータは、パッチ管理ツールで**推奨**されるのではなく、**省略可能**と解釈する必要があります。

Microsoft が推奨する方法を使用して、Windows Server機能更新プログラムを展開することをお勧めします。

次の手順: Microsoft は、ベスト プラクティスと推奨される手順を合理化するために、サード パーティのプロバイダーと協力しています。 Microsoft は、暫定的な手段として、**Windows Update**設定パネルを使用してアップグレード オファーを一時的に一時停止しました。 2025 年前半に提供される予定です。 Windows Server 2025 をインストールするための他のすべてのアップグレード方法は、通常のチャネルを通じて引き続き使用できます。

Windows Update経由のオファーが再開されると、IT 管理者は、[ターゲットの機能更新プログラムのバージョンを選択する] のグループ ポリシーでターゲット バージョンを "保留" に設定することで、機能更新プログラムオファー バナーを制御できるようになります このグループ ポリシーを使用して機能の更新プログラムを管理する方法については、「Windows Serverでのグループ ポリシーを使用した機能Updatesの管理」を参照してください。

注: Windows Server 2025 機能更新プログラムは、Windows 11 バージョン 24H2 で使用されたのと同じ KB 番号であったKB5044284 として、2024 年 11 月 1 日に利用可能になりました。 これは、クライアントとサーバーの両方の Windows 更新プログラムの KB 番号です。 Windows Server 2025 および Windows 11 バージョン 24H2 用にリリースされた今後の更新プログラムは、同じ KB 番号を共有しますが、リリース ノート サイトとリンクは異なります。

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2025;Windows Server 2022;Windows Server 2019

ページのトップへ

Windows 更新プログラムに関する問題を報告する

いつでも Microsoft に問題を報告するには、 フィードバック ハブ アプリを使用します。 詳細については、「 フィードバック ハブ アプリを使用して Microsoft にフィードバックを送信する 」を参照してください。

Windows の更新についてのヘルプが必要ですか?

Microsoft サポート コミュニティ を検索、参照、または質問します。 organizationをサポートしている IT 担当者の場合は、Microsoft 365 管理センターの Windows リリース正常性に関するページで詳細を確認してください。

自宅の PC を直接サポートするには、Windows のヘルプアプリを使用するか、Microsoft サポート にお問い合わせください。 組織は、 ビジネスのサポート を通じて即時サポートを要

求できます。

お使いの言語でこのサイトを表示する

このサイトは、英語、繁体字中国語、簡体字中国語、フランス語 (フランス)、ドイツ語、イタリア語、日本語、韓国語、ポルトガル語 (ブラジル)、ロシア語、スペイン語 (スペイン) の 11 の言語 で利用できます。 ブラウザーの既定の言語が 11 のサポートされている言語の 1 つでない場合、すべてのテキストが英語で表示されます。 表示言語を手動で変更するには、このページの下部まで下にスクロールし、ページの左下に表示されている現在の言語をクリックし、サポートされている 11 の言語のいずれかを一覧から選択します。

Last updated on 2026/04/10

Windows Server 2022 で解決された問題

Windows Server 2022 の最近解決された問題に関する情報をご覧ください。 特定の問題を見つけるには、ブラウザーで検索機能を使用します (Microsoft Edge の場合は Ctrl + F)。 Windows 更新プログラムの問題に関する即時のヘルプについては、Windows デバイスを使用してヘルプアプリを開くか、support.microsoft.com に移動する場合は、ここをクリックしてください。 Windows リリースの正常性更新プログラムについては、X (旧称 Twitter) の @WindowsUpdate に従ってください。 IT 管理者で、プログラムによってこのページから情報を取得する場合は、Microsoft Graph の Windows Updates API を使用します。

解決済みの問題

テーブルを展開する

要約	発生元の更新プログラム	状態	解決日
一部のデバイスはシャットダウンまたは休止状態に失敗する可能性があります この問題は、1 月の '26 年 1 月の更新プログラムをインストールした後、仮想セキュア モードが有効になっているセキュア起動対応 PC の一部に影響します。	OS ビルド 20348.4648 KB5073457 2026-01-13	解決済み KB5075906	2026-02-10 10:00 PT
クラウドでバックアップされたストレージにファイルを保存すると、アプリが応答しなくなる可能性があります 影響を受けるアプリには Outlook が含まれます。 これは、Microsoft OneDrive に保存されている PST ファイルにアクセスするときに応答しなくなる可能性があります。	OS ビルド 20348.4648 KB5073457 2026-01-13	解決済み KB5078136	2026-01-23 14:00 PT
Azure Virtual Desktop と Windows 365 での接続と認証の失敗 2026 年 1 月の Windows 更新プログラムにより、Azure Virtual Desktop と Windows 365 で資格情報プロンプトのWindows アプリエラーが発生する	OS ビルド 20348.4648 KB5073457 2026-01-13	解決済み KB5077800	2026-01-17 14:00 PT
管理者以外は、MSI 修復操作を実行するときに予期しない UAC プロンプトを受け取る可能性があ	OS ビルド 20348.4052 KB5063880	解決済み KB5065432	2025-09-09 10:00 PT

要約	発生元の更新プログラム	状態	解決日
ります この問題は、Autodesk AutoCAD や Office Professional Plus 2010 など、Windows インストーラー (MSI) を使用するアプリに影響する可能性があります。	2025-08-12		
スマートカード認証の問題は、2025 年 10 月の Windows 更新プログラムで発生する可能性があります この問題は、Windows 暗号化サービスを強化するために導入されたセキュリティの変更に関連しています。	OS ビルド 20348.4294 KB5066782 2025-10-14	解決済み	2025-10-22 17:31 PT
Active Directory フォレストの信頼情報を使用するアプリで問題が発生する可能性があります Microsoft .NET を使用してフォレストの信頼情報を取得または設定するアプリが失敗するか、閉じるか、エラーが発生する可能性があります。	OS ビルド 20348.469 KB5009555 2022-01-11	解決済み	2025-08-29 14:19 PT
一部のバージョンの Windows へのアップグレードがエラー 0x8007007Fで失敗する可能性があります Windows サーバーとクライアントの特定のアップグレード パスが影響を受けた。この問題は解決されました。	該当せず	解決済み	2025-08-18 18:59 PT
Microsoft Changjie Input メソッドを使用する場合に発生する問題 影響を受けるのは繁体字中国語を使用するデバイスのみです。 以前の IME バージョンに戻した場合、問題は回避されます。	OS ビルド 20348.3932 KB5062572 2025-07-08	解決済み KB5063880	2025-08-12 10:00 PT
2025 年 4 月のWindows RE更新プログラムは、Windows Updateで失敗と表示される場合があります ユーザーは、デバイスの再起動後に解決される WinRE 更新プログラムのインストール中にインストールエラーが発生する可能性があります。	該当せず KB5057588 2025-04-08	解決済み KB5063522	2025-07-08 10:00 PT
キー信頼モードでWindows Helloでログオンが失敗し、Kerberos イベントがログに記録される場合があります 2025 年 4 月の更新プログラムは、Kerberos イベント ID 45 と 21 をログに記録するドメイン コントローラーでの動作をトリガーする可能性があります	OS ビルド 20348.3453 KB5055526 2025-04-08	解決済み KB5060526	2025-06-10 10:00 PT

要約	発生元の更新プログラム	状態	解決日
2024 年 8 月のセキュリティ更新プログラムは、デュアルブート セットアップ デバイスLinuxブートに影響する可能性があります この問題は、Windows と SBAT 設定が適用されている場合にLinuxのデュアル ブートセットアップを持つデバイスに影響を与える可能性があります	OS ビルド 20348.2655 KB5041160 2024-08-13	解決済み KB5058385	2025-05-13 10:00 PT

問題の詳細

2026 年 1 月

一部のデバイスはシャットダウンまたは休止状態に失敗する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5075906	OS ビルド 20348.4648 KB5073457 2026-01-13	解決済み: 2026-02-10、10:00 PT オープン: 2026-01-15、18:33 PT

2026 年 1 月 13 日以降にリリースされた Windows 更新プログラム (KB5073457) をインストールした後、仮想セキュア モード (VSM) が有効になっているセキュア起動対応 PC の一部をシャットダウンまたは休止状態に入ることができません。 代わりに、デバイスが再起動します。 この問題は、AMD または ARM64 プロセッサを搭載したデバイスには影響せず、以下に示す影響を受けるプラットフォームに限定されます。

解像 度： この問題は、2026 年 2 月 10 日 (KB5075906) にリリースされた Windows 更新プログラムと、その日以降にリリースされた更新プログラムによって解決されました。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 23H2;Windows 10バージョン 22H2;WINDOWS 10 ENTERPRISE LTSC 2021;Windows 10 Enterprise LTSC 2019
- サーバー: Windows Server 2022; Windows Server 2019

ページのトップへ

クラウドでバックアップされたストレージにファイルを保存すると、アプリが応答しなくなる可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5078136	OS ビルド 20348.4648 KB5073457 2026-01-13	解決済み: 2026-01-23、 14:00 PT オープン: 2026-01-20、 22:10 PT

2026 年 1 月 13 日以降にリリースされた Windows 更新プログラム (KB5073457) をインストールした後、OneDrive や Dropbox などのクラウドでバックアップされたストレージにファイルを開いたり保存したりするときに、一部のアプリケーションが応答しなくなったり、予期しないエラーが発生したりする可能性があります。

たとえば、 in OneDrive に PST ファイルを格納する Outlook の一部の構成では 応答が停止し reopen プロセス が終了 タスク マネージャー システムが再起動されます さらに、 ent emails が [送信済みアイテム] フォルダーに表示されず 以前にダウンロードされたメールがダウンロードされる場合があります again. 影響を受ける Outlook の構成には、主に従来の Outlook が含まれます。これは一般的にエンタープライズ ライセンスに関連付けられており、Windows のほとんどのホーム インストールには含まれていません。Outlook の構成をチェックするには、「新しい Outlook と従来の Outlook の機能の比較」を参照してください。

解決策:

この問題は、2026 年 1 月 24 日にリリースされた帯域外 (OOB) 更新プログラム KB5078136 で解決され、Microsoft Update Catalog およびこの日以降にリリースされた更新プログラムから入手できます。 デバイスの最新の更新プログラムは、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

注: Microsoft Update Catalog から更新プログラムをダウンロードするには この記事で説明されている手順に従います。

OOB 更新プログラムをまだインストールしていないデバイスの場合は、Outlook 固有のシナリオに対するオプションの回避策があります。 Outlook PST ファイルを OneDrive から移動すると、この問題が解決されます。 ガイダンスについては OneDrive. から Outlook .pst データ ファイルを削除する方法 に関するドキュメントを参照してください。さらに、 email アカウントは、メール プロバイダーによってサポートされている場合は webmail 経由で引き続きアクセスできます。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 10バージョン 22H2;WINDOWS 10 ENTERPRISE LTSC 2021;Windows 10 Enterprise LTSC 2019

- サーバー: Windows Server 2025;Windows Serverバージョン 23H2;Windows Server 2022;Windows Server 2019

ページのトップへ

Azure Virtual Desktop と Windows 365 での接続と認証の失敗

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5077800	OS ビルド 20348.4648 KB5073457 2026-01-13	解決済み: 2026-01-17、14:00 PT オープン: 2026-01-14, 00:52 PT

2026 年 1 月の Windows セキュリティ更新プログラム (KB5073457) をインストールすると、一部のリモート接続アプリケーションで資格情報プロンプトエラーが発生する可能性があります。 これには、Windows クライアント デバイス、Azure Virtual Desktop、Windows 365上のWindows アプリを使用したリモート デスクトップ接続が含まれます。 Windows アプリは、特定の Windows ビルドでのこの問題の影響を受け、サインイン エラーが発生する可能性があります。

その他のリモート接続と関連するアプリケーションも同様に影響を受ける可能性があります。

解像 度： この問題に対処するために、 an out-of-band (OOB) 更新プログラムは Microsoft Update Catalog で 2026 年 1 月 17 日にリリースされました。 これは、KB5077800 として見つけることができます。

2026 年 1 月の Windows セキュリティ更新プログラムをまだ展開しておらず、IT 環境に影響を受けるアプリケーションと機能が含まれている場合は、代わりにこの OOB 更新プログラムを適用することをお勧めします。 その他のガイダンスについては、「 Microsoft Update カタログから更新プログラムをダウンロードする方法」を参照してください。 常に、デバイスの最新の更新プログラムをインストールすることをお勧めします。これには、この更新プログラムを含む重要な機能強化と問題解決が含まれています。

OOB がインストールされていない場合は、次のいずれかの接続オプションを一時的な回避策として使用できます。

- Windows 用リモート デスクトップ クライアントを使用して、ここで Azure Virtual Desktop に接続します (/previous-versions/remote-desktop-client/whats-new-windows?tabs=windows-msrdc-msi)
- windows.cloud.microsoft の Windows アプリ Web クライアントを使用して接続する

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 10バージョン 22H2;Windows 10、バージョン 21H2、Windows 10 Enterprise LTSC 2019

- サーバー: Windows Server 2025;Windows Server 2022;Windows Server 2019

ページのトップへ

2025 年 10 月

スマートカード認証の問題は、2025 年 10 月の Windows 更新プログラムで発生する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済み	OS ビルド 20348.4294 KB5066782 2025-10-14	解決済み: 2025-10-22、17:31 PT オープン: 2025-10-17、20:06 PT

2025 年 10 月 14 日以降にリリースされた Windows Updates (KB5066782) をインストールした後、セキュリティの脆弱性に対する保護 CVE-2024-30098 をインストールした後、スマート カード認証やその他の証明書操作が意図的に失敗する可能性があります。 この暗号化の強化の一環として、CSP (暗号化サービス プロバイダー) ではなく KSP (キー ストレージ プロバイダー) を使用するには、RSA ベースのスマート カード証明書が必要です。

CSP を使用する証明書の一般的な症状は次のとおりです。

- 32 ビット アプリケーションでスマート カードが CSP プロバイダー (暗号化サービス プロバイダー) として認識されない
- ドキュメントに署名できない
- 証明書ベースの認証に依存するアプリケーションのエラー
- "無効なプロバイダーの種類が指定されました" や "CryptAcquireCertificatePrivateKey エラー" などのエラー メッセージが表示される場合があります。

2025 年 10 月の Windows セキュリティ更新プログラム (KB5066782) をインストールする前に、システム ログに Smart Card Service または Microsoft-Windows-Smartcard-Server **Event ID: 624** メッセージ テキストが含まれている場合に、スマート カードがこのセキュリティ適用の影響を受けるかどうかを検出できます。このシステムは、RSA 暗号化操作に CAPI を使用しています。 詳細については、次のリンクを参照してください: https://go.microsoft.com/fwlink/?linkid=2300823 。

解像 度 :

永続的な解決のために、 developers は、Key Storage API を使用してキー ストレージ取得を実行するように認証アプリ Key Storage and Retrieval を更新する必要があります。 開発者は、2026 年 4 月にリリースされた Windows 更新プログラムの前にこの変更を完了する必要があります。この時点で、以下に示す **DisableCapiOverrideForRSA** 回避策が削除される予定です。

回避策:

この問題が発生した場合は、 **DisableCapiOverrideForRSA** registry キーの値を 0 に設定することで、一時的に解決できます。 これは CVE-2024-30098 に記載されています。 レジストリ キーを変更するための詳細な手順を次に示します。 **注**: このオプションは、2026 年 4 月にリリース予定の Windows 更新プログラムで削除されます。

レジストリを変更する手順

⚠ <**重要**: レジストリを誤って編集すると、システムの問題が発生する可能性があります。 変更を行う前に、常にレジストリをバックアップしてください。

1. レジストリ エディターを開きます。

- Win + R キーを押し、「regedit」と入力し、Enter キーを押します。
- ユーザー アカウント制御のプロンプトが表示されたら、[はい] をクリックします。

2. サブキーに移動します。

- [移動]: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais

3. キーを編集し、値を設定します。

- カレー内で、キー DisableCapiOverrideForRSA が存在するかどうかをチェックします
- DisableCapiOverrideForRSA をダブルクリックします。
- [値の日付] に「0」と入力します。

注: DisableCapiOverrideForRSA レジストリ設定は、既定の OS インストールまたは Windows Updatesのインストールでは追加されず、各デバイスに手動で追加する必要があります。

4. 閉じて再起動します。

- レジストリ エディターを閉じます。
- 変更を有効にするには、コンピューターを再起動します。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 10バージョン 22H2
- サーバー: Windows Server 2025;Windows Server 23H2;Windows Server 2022;Windows Server 2019;Windows Server 2016。Windows Server 2012 R2

ページのトップへ

2025 年 9 月

管理者以外は、MSI 修復操作を実行するときに予期しない UAC プロンプトを受け取る可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5065432	OS ビルド 20348.4052 KB5063880 2025-08-12	解決済み: 2025-09-09、10:00 PT オープン: 2025-09-03、14:28 PT

(11/26/25 更新: [解決策] セクションに追加の機能強化が追加されました。

2025 年 8 月の Windows セキュリティ更新プログラム (KB5063880) 以降の更新プログラムには、Windows インストーラー (MSI) の修復および関連する操作を実行するときに、ユーザー アカウント制御 (UAC) が管理者の資格情報を求めるという要件が適用されます。 この改善により、セキュリティの脆弱性 CVE-2025-50173 が 解決されました。

その結果、2025 年 8 月の Windows セキュリティ更新プログラム以降の更新プログラムをインストールした後、次のシナリオでは、標準ユーザーに対して管理者権限の入力を求める UAC プロンプトが表示される可能性があります。

- MSI 修復コマンドの実行 (msiexec /fu など)。
- 一部のバージョンのAutoCAD、Civil 3D、Inventor CAM を含むオートデスク アプリケーションを起動するか、ユーザーが初めてアプリにサインインした後に MSI ファイルをインストールする場合。
- ユーザーごとに自身を構成するアプリケーションのインストール。
- アクティブセットアップ中の Windows インストーラーの実行。
- ユーザー固有の "アドバタイズ" 構成に依存する Manager Configuration Manager (ConfigMgr) を使用してパッケージを展開する。
- Secure Desktop の有効化。

標準ユーザーが UI を表示せずに MSI 修復操作を開始するアプリを実行すると、エラー メッセージで失敗します。 たとえば、Office Professional Plus 2010 を標準ユーザーとしてインストールして実行すると、構成プロセス中にエラー 1730 で失敗します。

解決策:

2025 年 9 月の Windows セキュリティ更新プログラム (KB5065432) 以降の更新プログラムをインストールした後、ターゲット MSI ファイルに追加されたカスタム アクションが含まれている場合にのみ、MSI 修復操作中に UAC プロンプトが必要になります この要件は、2025 年 11 月 11 日以降にリリースされた Windows 更新プログラムをインストールした後にさらに調整されるため、UAC プロンプトが必要になるのは 修復フロー中に昇格されたカスタム アクションが実行された場合のみです。

最新の Windows 更新プログラムをインストールすると、このような昇格されたカスタム アクション (Autodesk AutoCADなど) を実行しないアプリのこの問題が解決されます。

カスタム アクションを実行するアプリには UAC プロンプトが引き続き必要になるため、2025 年 9 月の更新プログラムをインストールした後、IT 管理者は、MSI ファイルを許可リストに追加することで、特定のアプリの UAC プロンプトを無効にする回避策にアクセスできます。 詳細については、「2025 年 8 月の Windows セキュリティ更新プログラムをインストールした後に MSI 修復操作を実行するときに予期しない UAC プロンプトが表示 される」を参照してください。

この問題を回避するために、以前に Microsoft のビジネスサポート から Known Issue Rollback (KIR) からグループ ポリシーが提供されていました 組織では、この問題に対処するために、このグループ ポリシーをインストールして構成する必要がなくなりました。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 25H2;Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 10バージョン 22H2;Windows 10バージョン 21H2;Windows 10 Version 1809。WINDOWS 10 ENTERPRISE LTSC 2019;WINDOWS 10 ENTERPRISE LTSC 2016;Windows 10バージョン 1607;Windows 10 Enterprise 2015 LTSB
- サーバー: Windows Server 2025;Windows Server 2022;Windows Serverバージョン 1809;Windows Server 2019;Windows Server 2016。Windows Server 2012 R2;Windows Server 2012。Windows Server 2008 R2;Windows Server 2008 SP2

ページのトップへ

2025 年 8 月

一部のバージョンの Windows へのアップグレードがエラー 0x8007007F で失敗する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済み	該当せず	解決済み: 2025-08-18、18:59 PT オープン: 2025-08-18、18:06 PT

2025 年 8 月 12 日から、一部の Windows アップグレードは、"Windows セットアップ > アップグレード" インストールを使用して実行すると、エラー コード '0x8007007F' で失敗する可能性があります。 この問題は、特定のアップグレード パスの下のクライアント プラットフォームとサーバー プラットフォームの両方に影響します。

影響を受けるクライアント アップグレード パス:

- **Windows 10 Version 1809、**Windows 10、バージョン 21H2、Windows 10、バージョン 22H2 から Windows 11、バージョン 23H2 および 22H2 **へのアップグレード**

影響を受けるサーバー アップグレード パス:

- Windows Server 2016 **から** Windows Server 2019 または Windows Server 2022 **へのアップグレード**
- **Windows Server** 2019 から Windows Server 2022 **へのアップグレード**

注: Windows 11、24H2、Windows Server 2025 へのアップグレードは、この問題の影響を受けません

解像 度： この問題は、2025 年 8 月 15 日に解決されました。 この日付より後にアップグレードされたデバイスでは、このエラーが発生しなくなります。 エラー '0x8007007F' が発生した場合、通常、アップグレード プロセスを再試行すると問題が解決されます。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 23H2;Windows 11バージョン 22H2
- サーバー: Windows Server 2022; Windows Server 2019

ページのトップへ

2025 年 7 月

Microsoft Changjie Input メソッドを使用する場合に発生する問題

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5063880	OS ビルド 20348.3932 KB5062572 2025-07-08	解決済み: 2025-08-12、10:00 PT オープン: 2025-07-11, 08:52 PT

2025 年 7 月の Windows セキュリティ更新プログラム (KB5062572) のインストール後に、繁体字中国語の Microsoft Changjie IME (入力方法エディター) を使用するときに問題が発生する可能性があります。

この問題は、繁体字中国語が優先または共通の言語または入力方法であり、特に Changjie IME が使用されているデバイスにのみ影響します。 報告される症状は次のとおりです。

- 完全なコンポジションを入力した後に単語を形成または選択できない (フレーズ ウィンドウを関連付ける)
- spacebar または空白キーが応答しない
- 正しくない、または歪んだ単語の出力
- 変換候補ウィンドウが正しく表示されない

Microsoft Changjie は、Windows に含まれ、現在サポートされているバージョン 利用可能な IME です。

解決策: この問題は、2025 年 8 月の Windows セキュリティ更新プログラム (KB5063880) 以降の更新プログラムで解決されます。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

2025 年 8 月より前にリリースされた Windows 更新プログラムをインストールしている場合は、次の回避策を使用できます。 Windows IME では、代わりに以前のバージョンの IME を使用できる互換性設定がサポートされています。 このオプションを使用すると、この問題を解決するのに役立ちます。

Microsoft Changjie IME の古いバージョンに戻すには、次の手順に従います。

1. **[言語&リージョン]** 設定を開きます。 これを行うには、 **設定** アプリを開き、[**時間 & 言語**]、[**言語 & リージョン]** の順に選択します。 スタート メニューを開き、「言語」と入力し、上位の結果を選択することもできます。
2. このデバイスで繁体字中国語が使用されている場合は、上部の近くに中国語 (繁体字) オプションが表示されます。 **[中国語 (繁体字)]** の横にある 3 つのドットを選択してメニューを開き、[**言語オプション**] を選択します。
3. [**キーボード**] で、 **Microsoft Changjie** の横にある 3 つのドットを選択し、メニューから [**キーボード オプション]** を選択します。
4. [**互換性]** で、[**以前のバージョンの Microsoft Changjie を使用**する] オプションを **[オン] に設定します**。 次に、[**OK] を選択します**。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 24H2;Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 10バージョン 22H2;Windows 10 Version 1809。WINDOWS 10 ENTERPRISE LTSC 2016;バージョン 1607 Windows 10
- サーバー: Windows Server 2025;Windows Server 2022;Windows Serverバージョン 1809;Windows Server 2016

ページのトップへ

2025 年 5 月

キー信頼モードでWindows Helloでログオンが失敗し、Kerberos イベントがログに記録される場合があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5060526	OS ビルド 20348.3453 KB5055526 2025-04-08	解決済み: 2025-06-10、10:00 PT オープン: 2025-05-06、13:25 PT

2025 年 4 月 8 日 (KB5055523) 以降にリリースされた 4 月の Windows 月次セキュリティ更新プログラムをインストールすると、Active Directory **msds-KeyCredentialLink** フィールドを介してキー信頼に依存する証明書ベースの資格情報を使用して Kerberos ログオンまたは委任を処理するときに、Active Directory ドメイン コントローラー (DC) で認証の中断が発生する可能性があります。

これらの更新の後、DC が Kerberos 認証に使用する証明書を検証する方法が変更され、証明書が NTAuth ストアの発行元証明機関 (CA) にチェーンされている必要があります。 これは、「KB5057784 - CVE-2025-26647 (Kerberos 認証の保護)」で説明されているセキュリティ対策に関連しています。 その結果、デバイス公開キー認証 (Machine PKINIT とも呼ばれます) を展開した Windows Hello for Business (WHfB) キー信頼環境または環境で認証エラーが発生する可能性があります。 この機能に依存する他の製品も影響を受ける可能性があります。

この検証メソッドの有効化は、. の Windows レジストリ値 **AllowNtAuthPolicyBypass** によって制御 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc**できます。DC の認証に 2025 年 4 月の Windows 月次セキュリティ更新プログラムをインストールした後、2 つのシナリオを確認できます。

- レジストリ値 **AllowNtAuthPolicyBypass** が構成解除されているか、"1" に設定されている場合、Kerberos-Key-Distribution-Center **イベント ID 45** は DC システム イベント ログに繰り返し記録されます。"キー配布センター (KDC) で、有効であったが NTAuth ストアの発行元 CA にチェーンされていないクライアント証明書が検出されました。 これは、安全でない証明書を使用して認証要求を処理する DC によって意図的にログに記録される新しいイベントです。 このイベントは過度にログに記録される可能性がありますが、関連するログオン操作は成功し、これらのイベント ログ レコードの外部で他の変更は行われません。

- レジストリ値 **AllowNtAuthPolicyBypass** が "2" に設定されている場合、自己署名証明書ベースの認証は失敗します。 Kerberos-Key-Distribution-Center **イベント ID 21** は、DC システム イベント ログに記録されます。 これは、証明書ベースの認証が失敗したときにログに記録されるレガシ イベントであり、DC が安全でない証明書を使用して認証要求をサービスするときに意図的にログに記録されます。 このイベントのイベント説明テキストは異なる場合があります。

AllowNtAuthPolicyBypass レジストリ キーが存在しない場合、DC は値が "1" に構成されているかのように動作します。 キーが存在しない場合は、手動で作成し、上記のように構成できます。

2025 年 4 月 8 日以降にリリースされた Windows Updates、NTAuth ストア内の CA にチェーンされない自己署名証明書を使用して認証要求を処理するときに、イベント ID 45 と 21 が誤ってログに記録されます。 自己署名証明書は、次のシナリオで AD PKINIT キー信頼機能によって使用される場合があります。

- Windows Hello for Business (WHfB) キー信頼デプロイ
- デバイス公開キー認証 (マシン PKINIT とも呼ばれます)。
- スマート カード製品、サード パーティ製シングル サインオン (SSO) ソリューション、ID 管理システムなど、**msds-KeyCredentialLink** フィールドに依存するその他のシナリオ。

解決策: この問題は、2025 年 6 月 10 日 (KB5060526) 以降にリリースされた Windows 更新プログラムによって解決されました。 デバイスの最新のセキュリティ更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

2025 年 6 月 10 日以降にリリースされた更新プログラムをインストールする場合は、この問題の回避策を使用する必要はありません。 この日付より前にリリースされた更新プログラムを使用していて、この問題が発生した場合は、自己署名証明書ベースの認証を処理する更新された DC で、レジストリ キー **AllowNtAuthPolicyBypass** に値 '2' を設定するのを一時的に遅らせる必要があります。 詳細については、「KB5057784 のレジストリ設定」セクションを参照してください。

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2025;Windows Server 2022;Windows Server 2019;Windows Server 2016

ページのトップへ

2025 年 4 月

2025 年 4 月のWindows RE更新プログラムは、Windows Updateで失敗と表示される場合があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済みの KB5063522	該当せず KB5057588 2025-04-08	解決済み: 2025-07-08、 10:00 PT オープン: 2025-04-11、 17:03 PT

2025 年 4 月の Windows Recovery Environment 更新プログラム [KB5057588] をインストールすると、Windows Update設定ページ: 0x80070643 - ERROR_INSTALL_FAILURE. に次のエラー メッセージが表示される場合があります。このエラー メッセージは正確ではなく、更新プログラムやデバイスの機能には影響しません Windows Recovery Environment (WinRE) は、起動できないオペレーティング システムの一般的な原因を修復できる回復環境です。

このエラーは、別の更新がある場合にデバイスが WinRE 更新プログラムをインストールしたときに 保留中の再起動状態で発生します 更新が完了しなかったことを示すエラー メッセージが表示されますが、WinRE 更新プログラムは通常、デバイスの再起動後に正常に適用されます。 Windows Updateは、次の毎日のスキャンまで更新プログラムを失敗として表示し続ける可能性があります。この時点で更新プログラムは提供されなくなり、エラー メッセージは自動的にクリアされます。

解像 度 :

2025 年 4 月 21 日午後 2 時より前にインストールされた KB5057588 で以前に確認された ERROR_INSTALL_FAILURE エラー メッセージは、2025 年 7 月 8 日 (KB5063522) にリリースされた Windows 更新プログラムで解決されました。 デバイスの最新の更新プログラムには、重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

ご注意ください: この更新プログラムでは、Windows Update履歴ページに表示される可能性がある誤ったエラー メッセージは削除されません。

2025 年 4 月 21 日午後 2 時以降に KB5057588 をインストールしたユーザーは、インストール エラーに関する誤ったエラー メッセージを確認しないでください 更新プログラムが既にインストールされている場合は、再び提供されず、 Dism /Online /Get-Packages command を使用してこの更新プログラムの状態を確認できます。

影響を受けるプラットフォーム:

- クライアント: Windows 10バージョン 22H2;Windows 10バージョン 21H2
- サーバー: Windows Server 2022

ページのトップへ

2024 年 8 月

2024 年 8 月のセキュリティ更新プログラムは、デュアルブート セットアップ デバイスLinuxブートに影響する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決された KB5058385	OS ビルド 20348.2655 KB5041160 2024-08-13	解決済み: 2025-05-13、10:00 PT オープン: 2024-08-21、18:33 PT

2024 年 8 月の Windows セキュリティ更新プログラム (KB5041160) または 2024 年 8 月のプレビュー更新プログラムをインストールした後、デバイスで Windows とLinuxのデュアルブートセットアップを有効にしている場合、Linuxの起動に関する問題が発生する可能性があります。 この問題の結果、デバイスがLinux起動に失敗し、「shim SBAT データの確認に失敗しました: セキュリティ ポリシー違反」というエラー メッセージが表示されることがあります。 SBAT の自己チェックが失敗しました: セキュリティ ポリシー違反。

2024 年 8 月の Windows セキュリティおよびプレビュー更新プログラムは、古い脆弱なブート マネージャーをブロックするために Windows を実行するデバイスにセキュア ブート Advanced Targeting (SBAT) 設定を適用します。 この SBAT 更新プログラムは、デュアル ブートが検出されたデバイスには適用されません。 一部のデバイスでは、デュアルブート検出では、デュアルブートのいくつかのカスタマイズされた方法が検出されず、SBAT 値が適用されていない場合に適用されました。

大事な： この既知の問題は、2024 年 8 月のセキュリティ更新プログラムとプレビュー更新プログラムのインストールでのみ発生します。 2024 年 9 月のセキュリティ更新プログラム以降の更新プログラムには、この問題の原因となった設定は含まれていません。

解像 度： この問題は、2025 年 5 月 13 日 (KB5058385) 以降にリリースされた Windows 更新プログラムによって解決されました。 デバイスの最新の更新プログラムには、この更新プログラムを含む重要な機能強化と問題解決が含まれているので、インストールすることをお勧めします。

注: Windows 専用システムでは、2024 年 9 月以降の更新プログラムをインストールした後、SBAT セキュリティ更新プログラムが適用されていることを確認するために CVE-2022-2601 and CVE-2023-40547 に記載されているレジストリ キーを設定できます。 デュアルブートLinuxおよび Windows のシステムでは、2024 年 9 月以降の更新プログラムをインストールした後に追加の手順は必要ありません。

影響を受けるプラットフォーム:

- クライアント: Windows 11バージョン 23H2;Windows 11バージョン 22H2;Windows 11バージョン 21H2;Windows 10バージョン 22H2;Windows 10バージョン 21H2;Windows 10 Enterprise 2015 LTSB
- サーバー: Windows Server 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2; Windows Server 2012

ページのトップへ

2022 年 2 月

Active Directory フォレストの信頼情報を使用するアプリで問題が発生する可能性があります

テーブルを展開する

状態	発生元の更新プログラム	履歴
解決済み	OS ビルド 20348.469 KB5009555 2022-01-11	解決済み: 2025-08-29、14:19 PT オープン: 2022-02-04、16:57 PT

2022 年 1 月 11 日以降にリリースされた更新プログラムをインストールした後、Microsoft .NET Framework を使用して Active Directory フォレストの信頼情報を取得または設定するアプリが失敗するか、閉じるか、アプリまたは Windows からエラーが発生する可能性があります。 アクセス違反 (0xc0000005) エラーが表示される場合もあります。 **開発者向けの注意**: 影響を受けるアプリでは、 System.DirectoryServices API を使用します。

解像 度：この問題は、アプリで使用される.NET Frameworkのバージョンの帯域外更新プログラムで解決されました。 **メモ：**これらの帯域外の更新プログラムは、Windows Updateからは利用できません。また、自動的にはインストールされません。 スタンドアロン パッケージを取得するには、Microsoft Update カタログ で、お使いのバージョンの Windows と .NET Framework の KB 番号を検索します。 これらの更新プログラムは、Windows Server Update Services (WSUS) と Microsoft Endpoint Configuration Manager に手動でインポートできます。 WSUS の手順については、「WSUS とカタログ サイト」を参照してください。 構成

マネージャーの手順については、「Microsoft Update カタログから更新プログラムをインポートする」を参照してください。

オペレーティング システム用にこの更新プログラムをインストールする方法については、以下のサポート情報記事を参照してください。

- Windows Server 2022:
  - .NET Framework 4.8 KB5011258
- Windows Server 2019:
  - .NET Framework 4.8 KB5011257
  - .NET Framework 4.7.2 KB5011259
- Windows Server 2016:
  - .NET Framework 4.8 KB5011264
  - .NET Framework 4.6.2、4.7、4.7.1、または 4.7.2 KB5011329
- Windows Server 2012 R2:
  - .NET Framework 4.8 KB5011266
  - .NET Framework 4.6、4.6.1、4.6.2、4.7、4.7.1、または 4.7.2 KB5011263
  - .NET Framework 4.5.2 KB5011261
- Windows Server 2012:
  - .NET Framework 4.8 KB5011265
  - .NET Framework 4.6、4.6.1、4.6.2、4.7、4.7.1、または 4.7.2 KB5011262
  - .NET Framework 4.5.2 KB5011260

影響を受けるプラットフォーム:

- クライアント: なし
- サーバー: Windows Server 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2; Windows Server 2012

ページのトップへ

Windows 更新プログラムに関する問題を報告する

いつでも Microsoft に問題を報告するには、 フィードバック ハブ アプリを使用します。 詳細については、「 フィードバック ハブ アプリを使用して Microsoft にフィードバックを送信する 」を参照してください。

Windows の更新についてのヘルプが必要ですか?

Microsoft サポート コミュニティ を検索、参照、または質問します。 organizationをサポートしている IT 担当者の場合は、Microsoft 365 管理センターの Windows リリース正常性に関するページで詳細を確認してください。

自宅の PC を直接サポートするには、Windows のヘルプアプリを使用するか、Microsoft サポート にお問い合わせください。 組織は、 ビジネスのサポート を通じて即時サポートを要求できます。

お使いの言語でこのサイトを表示する

このサイトは、英語、繁体字中国語、簡体字中国語、フランス語 (フランス)、ドイツ語、イタリア語、日本語、韓国語、ポルトガル語 (ブラジル)、ロシア語、スペイン語 (スペイン) の 11 の言語 で利用できます。 ブラウザーの既定の言語が 11 のサポートされている言語の 1 つでない場合、すべてのテキストが英語で表示されます。 表示言語を手動で変更するには、このページの下部まで下にスクロールし、ページの左下に表示されている現在の言語をクリックし、サポートされている 11 の言語のいずれかを一覧から選択します。

Last updated on 2026/04/10

Windows Server のアップグレードを計画する

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Server では、インプレース アップグレード、クリーン インストール、移行、クラスターローリング アップグレード、エディション変換など、新しいバージョンに移行するためのいくつかの方法がサポートされています。 各方法には、ダウンタイム、複雑さ、ハードウェア要件に関して異なるトレードオフがあります。 アップグレードにより、サーバーはセキュリティで保護され、サポートされ、最新の機能とパフォーマンスの向上を使用できます。

この記事では、使用可能なアップグレード方法、サポートされているインプレース アップグレード パス (バージョン別)、および適用される制限について説明します。

アップグレード方法を選択するための要因

最適な方法は、環境と要件によって異なります。 アップグレードを計画するときは、次の要因を考慮してください。

- **ダウンタイム許容度** — インプレース アップグレードには再起動が必要ですが、同じハードウェア上に保持されます。 クラスターのローリング アップグレードでは、プロセス全体でワークロードの可用性が維持されます。 クリーン インストールまたは移行には、より多くのダウンタイムが必要になる場合がありますが、新しい環境が提供されます。
- **ハードウェアの制約** - 同じハードウェア上に留まっている場合は、インプレース アップグレードまたはクリーン インストールが適しています。 新しいハードウェアに移行する場合は、移行することをお勧めします。
- **ロールと機能** - すべてのロールがインプレース アップグレードをサポートしているわけではありません。 ロールと機能の移行マトリックスを確認して、構成のサポートを確認します。
- **バージョンギャップ** - Windows Server 2025 以降では、非クラスター化システムは一度に最大 4 つのバージョンをアップグレードできます。 Windows Server 2022 以前の場合、非クラスター化システムでは、一度に最大 2 つのバージョンをアップグレードできます。 クラスターのローリング アップグレードでは、一度に 1 つのバージョンのみを進めることができます。 詳細については、 サポートされているパスの表 を参照してください。

- **ライセンス** - アップグレードする前に、ターゲット バージョンの有効なプロダクト キーとアクティブ化方法があることを確認します。 Windows クライアントとは異なり、Windows Server のアップグレードごとに個別のライセンスが必要です。

Windows Server のアップグレード方法

次の表を使用して、シナリオに適した方法を決定します。

> **ⓘ 重要**
>
> インプレース アップグレード、クリーン インストール、または新しいバージョンの Windows Server への移行を実行する前に、システムと重要なファイルを常にバックアップしてください。

テーブルを展開する

メソッド	動作内容	いつ使用するか	詳細情報
既存環境でのアップグレード	新しいバージョンの Windows Server を既存のバージョンにインストールし、設定、サーバーの役割、機能、データを保持します。 インプレース アップグレードは、インストール メディアを使用して実行することも、Windows Update を通じて機能更新プログラムとして受け取ることもできます。	同じハードウェア上の新しいバージョンへの最速のパスが必要であり、ロールと機能 はインプレース アップグレードをサポートします。	インプレース アップグレードを実行する
クリーン インストール	Windows Server を新しいサーバーにインストールするか、既存の OS を上書きします。	新しいスタートが必要な場合、ハードウェアが新しい場合、またはインプレース アップグレードが現在の構成でサポートされていません。	Windows Server のインストール
移行	役割または機能を移行元サーバーから Windows Server を実行している別の移行先サーバーに移動します。	新しいハードウェアに移行するか、OS をインプレースアップグレードせずに一度に 1 つのロールまたは機能を移行する必要があります。	ロールと機能のアップグレードと移行
クラスタ	Hyper-V やスケールアウト ファイルサーバーのワークロードを停止せずに、クラスター ノードのオペレーテ	フェールオーバー クラスターを実行し	クラスター OS のローリ

メソッド	動作内容	いつ使用するか	詳細情報
ー OS のローリング アップグレード	ィング システムを一度に 1 つずつアップグレードします。 クラスターは、一度に 1 つのバージョンのみをアップグレードできます。 ローリング アップグレードは、インストール メディアを使用して実行することも、Windows Update を通じて機能更新プログラムとして受け取ることもできます。 Azure Local で実行されているフェールオーバー クラスターの場合は、代わりにライフサイクル マネージャー (LCM) を使用します。	ており、アップグレード中に可用性を維持する必要があります。	ング アップグレード
ライセンスの変換	コマンドとプロダクト キー (Standard から Datacenter など) を使用して、Windows Server の 1 つのエディションを同じリリースの別のエディションに変換します。	Windows Server エディションを変更するか、リテール、ボリューム ライセンス、OEM ライセンスを切り替える必要があります。	Windows Server のエディションとライセンスの種類を変換する

バージョン別にサポートされているインプレース アップグレード パス

最新バージョンの Windows Server にアップグレードして、最新の機能、セキュリティ更新プログラム、および最高のパフォーマンスを取得します。

Windows Server 2025 以降、非クラスター化システムでは、一度に最大 4 つのバージョンをアップグレードできます。 Windows Server 2012 R2 以降から Windows Server 2025 に直接アップグレードできます。 Windows Server 2022 以前の場合、非クラスター化システムでは、一度に最大 2 つのバージョンをアップグレードできます。 クラスター OS のローリング アップグレードを使用している場合は、一度にアップグレードできるバージョンは 1 つだけです。

次の表に、現在のバージョンに基づいてサポートされているインプレース アップグレード パスを示します。

テーブルを展開する

アップグレード元/先	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025
Windows Server 2012	はい	はい	いいえ	いいえ	いいえ
Windows Server 2012 R2	いいえ	はい	はい	いいえ	はい

アップグレード元/先	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2022	Windows Server 2025
Windows Server 2016	いいえ	いいえ	はい	はい	はい
Windows Server 2019	いいえ	いいえ	いいえ	はい	はい
Windows Server 2022	いいえ	いいえ	いいえ	いいえ	はい
Windows Server 2025	いいえ	いいえ	いいえ	いいえ	はい

Windows Server のライセンスバージョンのアップグレード制限

Windows Server が既にライセンスされているインプレース アップグレード (評価版ではない) には、次の制限が適用されます。

- 32 ビット アーキテクチャから 64 ビット アーキテクチャへのアップグレードはサポートされていません。 Windows Server 2008 R2 以降のすべてのリリースは、64 ビット版のみです。
- 特定の言語から別の言語へのアップグレードはサポートされていません。
- サーバーが Active Directory ドメイン コントローラーの場合は、製品版に変換することはできません。 重要な情報については、「 Windows Server へのドメイン コントローラーのアップグレード 」を参照してください。
- Windows Server のプレリリース バージョン (プレビュー) からのアップグレードはサポートされていません。 代わりにクリーン インストールを実行してください。
- インプレース アップグレード中に Server Core のインストールからデスクトップ エクスペリエンスインストールを使用したサーバーへの切り替え (またはその逆) はサポートされていません。
- 以前の Windows Server インストールから評価版へのアップグレードはサポートされていません。 クリーン インストールとして評価版をインストールします。
- 既定では、アップグレードでは既存のエディションが保持されます。 たとえば、Standard から Standard、Datacenter から Datacenter へのアップグレードです。
- アップグレード中に、Standard から Datacenter または Datacenter: Azure Edition に、または Datacenter から Datacenter: Azure Edition に変更できます。 Datacenter から Standard に、または Datacenter: Azure Edition から Standard または Datacenter にダウングレードすることはできません。

- サーバーで NIC チーミングを使用している場合は、インプレース アップグレードの前に NIC チーミングを無効にします。 インプレース アップグレードが完了したら、再度有効にすることができます。 詳細については、「 NIC チーミングの概要」を参照してください。
- VHD から起動するように構成された Windows Server でのインプレース アップグレードはサポートされていません。
- Windows Storage Server エディションからのインプレース アップグレードはサポートされていません。
- 一部のパブリック およびプライベート クラウド プロバイダーでは、インプレース アップグレードがサポートされています。 詳細については、クラウド プロバイダーに問い合わせてください。

サポート終了バージョンの Windows Server

Windows Server 2012 および Windows Server 2012 R2 のサポートは、2023 年 10 月 10 日に終了しました。 使用できる拡張セキュリティ更新プログラム (ESU) には、オンプレミス のサーバーを Azure に移行するオプションが 1 つあり、仮想マシンで引き続き実行できます。 詳細については、「 拡張セキュリティ更新プログラムの概要」を参照してください。

関連コンテンツ

- Windows Server のインプレース アップグレードを実行する
- Windows Server のエディションとライセンスの種類を変換する
- Windows Server の役割と機能のアップグレードと移行
- クラスター OS のローリング アップグレード
- クラスター対応更新の概要

Last updated on 2026/04/03

Server Core とデスクトップ エクスペリエンスを備えたサーバーのインストール オプション

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

セットアップ ウィザードを使用して Windows Server をインストールする場合は、Server Core またはデスクトップ エクスペリエンス搭載サーバーのインストール オプションを選択できます。 Server Core では、標準のグラフィカル ユーザー インターフェイス (デスクトップ エクスペリエンス) はインストールされません。PowerShell、サーバー 構成ツール (SConfig)、またはリモート メソッドを使用して、コマンド ラインからサーバーを管理します。 デスクトップ エクスペリエンスを備えたサーバーは、標準のグラフィカル ユーザー インターフェイスと、クライアント エクスペリエンス機能を含むすべてのツールをインストールします。

デスクトップ エクスペリエンスのサーバー インストール オプションに含まれる追加のユーザー インターフェイス要素とグラフィカル管理ツールが特に必要な場合を除き、Server Core インストール オプションを選択することをお勧めします。

セットアップ ウィザードにインストール オプションが一覧表示されます。 この一覧では、**デスクトップ エクスペリエンス** のないエディションは、Server Core のインストール オプションです。

- Windows Server Standard
- Windows Server Standard とデスクトップ エクスペリエンス
- Windows Server Datacenter
- デスクトップ エクスペリエンスを備えた Windows Server データセンター

> ⓘ **注意**
>
> 一部の以前のリリースの Windows Server とは異なり、インストール後に Server Core とデスクトップ エクスペリエンスを備えたサーバーの間で変換することはできません。 後でインストールして別のオプションを使用する場合は、 **クリーン インストール** を行う必要があります。

Differences

Server Core とデスクトップ エクスペリエンスを備えたサーバーには、いくつかの主な違いがあります。

テーブルを展開する

Component	サーバー コア	デスクトップ エクスペリエンス搭載サーバー
ユーザーインターフェース	最小限のコマンド ライン ドリブン (PowerShell、 SConfig、cmd)	標準の Windows グラフィカル ユーザー インターフェイス
ディスク領域	要件が小さい	より大きな要件
サーバーロールをローカルにインストール、構成、アンインストールする	PowerShell	サーバー マネージャーまたは PowerShell
役割と機能	一部のロールと機能は使用できません。詳細については、「 Windows Server - Server Core 以外の役割、役割サービス、および機能」を参照してください。 アプリケーションの互換性のためのデスクトップ エクスペリエンスを備えたサーバーの機能の一部は、 アプリ互換性機能オンデマンド (FOD) を使用してインストールできます。	アプリケーションの互換性を確保するために、すべてのロールと機能を使用できます。
リモート管理	はい。Windows Admin Center、リモート サーバー管理ツール (RSAT)、サーバー マネージャー、PowerShell などの GUI ツールを使用してリモートで管理できます。	はい。Windows Admin Center、リモート サーバー管理ツール (RSAT)、サーバー マネージャー、PowerShell などの GUI ツールを使用してリモートで管理できます。
潜在的な攻撃対象領域	攻撃面が大幅に減少	削減なし
Microsoft 管理コンソール	インストールされていません - アプリ互換性機能オンデマンド (FOD) と共にインストールできます。	Installed

注意

RSAT の場合は、Windows 10 以降に含まれているバージョンを使用する必要があります。

Windows Server サービス チャネル

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

2023 年 9 月以降、Windows Server では、長期サービス チャネルと年間チャネルの 2 つをプライマリ リリース チャネルとして提供しています。 長期サービス チャネル (LTSC) は、従来のライフサイクルの品質とセキュリティ更新プログラムの提供に重点を置いた長期的なオプションを提供します。一方、年間チャネル (AC) はより頻繁なリリースを提供します。 AC のリリースが頻繁に行われるほど、コンテナーとマイクロサービスに重点を置いて、より迅速なイノベーションが実現されます。

Long-Term サービス チャネル (LTSC)

長期サービス チャネルでは通常、Windows Server の新しいメジャー バージョンが、2 年から 3 年ごとにリリースされます。 ユーザーは、5 年間のメインストリーム サポートとそれに続く 5 年間の延長サポートを受けることができます。 このチャネルでは、長期サービス オプションと一貫性が提供され、Server Core インストール オプションまたはデスクトップ エクスペリエンス インストール オプションでインストールすることができます。

年間チャネル (AC)

Windows Server Annual Channel for Containers は、Windows Server コンテナーをホストするためのオペレーティング システムです。 年間チャネルを利用すると、コンテナーとマイクロサービスに重点を置き、急速なイノベーションを行っているお客様が、新しいオペレーティング システム機能をより速いペースで活用できるようになります。 Windows Server Annual Channel for Containers の詳細については、TechCommunity からのお知らせ を参照してください。

このチャネルの各リリースは、最初のリリースから 24 か月間サポートされます。 このチャネルは、Server Core インストール オプションでのみインストールできます。 年間チャネルは、ソフトウェア アシュアランス とロイヤルティ プログラム (Visual Studio サブスクリプションなど) をお持ちのボリューム ライセンスのお客様が利用できます。

年間チャネルのリリースは更新プログラムではなく、年間チャネルにおける Windows Server の次のリリースです。 年間チャネル リリースに移行するには、クリーン インストールを実行する必要があります。

年間チャネルでの Windows Server のリリースは、通常 12 か月ごとに行われます。 各リリースの 24 か月のサポート ライフサイクルは、18 か月のメインストリーム サポートと 6 か月の

延長サポートです。 ライフサイクルの詳細については、「Windows Server 2022 のライフサイクル」を参照してください。 各リリースの名前は、リリース サイクルに基づいています。 たとえば、**バージョン 23H2** は 2023 年後半のリリースです。

主な違い

次の表は、チャネル間の主な違いをまとめたものです。

テーブルを展開する

説明	長期サービス チャネル	年間チャネル
推奨されるシナリオ	汎用ファイル サーバー、Microsoft と Microsoft 以外のワークロード、従来のアプリ、インフラストラクチャの役割、ソフトウェア定義データセンター、ハイパーコンバージド インフラストラクチャ	コンテナホスト上で実行されるコンテナ化されたアプリケーションは、より迅速なイノベーションの恩恵を受けます
新しいリリース	通常、2 ～ 3 年	通常 12 か月
支援	5 年間のメインストリーム サポートとそれに続く 5 年間の延長サポート	18 か月のメインストリーム サポートと 6 か月の延長サポート
アクティブ化	すべての Windows Server アクティブ化キー	Windows Server Datacenter アクティブ化キー
ライセンス	すべてのライセンス プログラム	ソフトウェア アシュアランスのお客様のみ
メディアの取得	すべての配布チャネル	ボリューム ライセンス サービス センター (VLSC) と Visual Studio Subscription のみ
インストール オプション	Server Core とデスクトップ エクスペリエンス搭載サーバー	Server Core (コンテナー ホストのみ)

デバイスの互換性

年間チャネルのリリースを実行するための最小ハードウェア要件は、Windows Server の最新の長期サービス チャネルのリリースと同じです。 ほとんどのハードウェア ドライバーは、これらのリリースでも引き続き機能します。

サービス

Microsoft ライフサイクルに関するページに記載されている期日になるまで、長期サービス チャネルと年間チャネルのどちらのリリースも、セキュリティ更新プログラムとセキュリティ以外の更新プログラムでサポートされます。 違いは、この記事の「年間チャネル (AC)」セクションで説明されているように、リリースがサポートされる期間の長さです。

サービス ツール

Windows Server を操作するためのツールは数多く存在します。 機能や制御からシンプルさや管理要件の低さまで、各オプションにはそれぞれ長所と短所があります。 更新プログラムの管理に使用できるサービス ツールの例を次に示します。

- **Windows Update (スタンドアロン)** : このオプションは、インターネットに接続されていて、Windows Update が有効にされているサーバーでのみ利用できます。
- **Windows Server Update Services (WSUS)** は、Windows Server と Windows クライアントの更新プログラムを詳細に管理することができ、Windows Server オペレーティング システムでネイティブに利用できます。 更新プログラムの適用延期や、承認レイヤーの追加のほか、準備完了後に特定コンピューターまたはコンピューター グループに展開することも可能です。
- **Microsoft Endpoint Configuration Manager** では、サービスを最も制御できます。 更新プログラムを延期、承認することができ、展開のターゲットを設定し、帯域幅の使用と展開回数を管理するための複数のオプションを選択できます。

年間チャネルのリリースでも、同じプロセスを引き続き使用できます。たとえば、既に更新プログラムの管理に Configuration Manager を使用している場合は、使用を継続できます。 同様に、WSUS を使用している場合は、使用を継続できます。

年間チャネルを入手できる場所

年間チャネル リリースは、次の場所から入手できます。

- ボリューム ライセンス サービス センター (VLSC): ソフトウェア アシュアランス をお持ちの、ボリューム ライセンスのお客様がこのリリースを入手するには、ボリューム ライセンス サービス センター に移動して、[**サインイン**] を選択します。 最後に、[**ダウンロードとキー**] を選択し、「年間チャネル」を検索して、メディアをダウンロードします。

- Visual Studio Subscription: Visual Studio サブスクライバーが年間チャネルのリリースを入手するには、Visual Studio サブスクライバー ダウンロード ページ からダウンロードします。 まだサブスクライバーではない場合は、Visual Studio Subscription にサインアップしてから、Visual Studio サブスクライバーのダウンロード ページ にアクセスし

ます。 Visual Studio サブスクリプション経由で入手したリリースは、開発とテストにのみ利用できます。

年間チャネル リリースのライセンス認証

VLSC から取得したアクティブ化キーを使用して、インストールをアクティブ化する必要があります。 KMS を使用している場合、年間チャネル リリースでは、リリース前の最後の LTSC リリースと同じ CSVLK が使用されます。 たとえば、Windows Server 2022 以降にリリースされる年間チャネルでは、Windows Server 2022 CSVLK が使用されます。 詳細については、「KMS クライアント セットアップ キー」を参照してください。

LTSC または AC のいずれのリリースがサーバーで実行されているかを確認する方法

長期サービス チャネルのリリースは、年間チャネルの新しいバージョンと同時にリリースされる可能性があります。 サーバーが年間チャネル リリースを実行しているかどうかを判断するには、オペレーティング システムのバージョンを確認する必要があります。 製品名には、サービス チャネルが反映されていません。 サーバーが LTSC リリースと AC リリースのどちらを実行しているかを判断するには、PowerShell コマンド Get-ComputerInfo を実行します。 以下は、Windows Server 2022 Datacenter Edition (LTSC) を実行しているコンピューターの例です。

オペレーティング システムのバージョンを確認するには、次のコマンドを実行します。

PowerShell

```
Get-ComputerInfo  | fl WindowsProductName,OSDisplayVersion
```

Windows Server LTSC を実行しているコンピューターからの出力例を次に示します。

出力

```
WindowsProductName : Windows Server 2022 Datacenter
OSDisplayVersion   : 21H2
```

Windows Server Annual Channel for Containers を実行しているコンピューターからの出力例を次に示します。

出力

```
WindowsProductName : Windows Server 2022 Datacenter
```

```
OSDisplayVersion    : 23H2
```

> **ヒント**
>
> `OSDisplayVersion` は、Windows Server 2022 以降にのみ適用されます。 年間チャネル リリースは、Windows Server 2019 以前には適用されません。 Windows Server 2019 以前を実行している場合は、LTSC リリースが実行されています。

次の表に、Windows Server LTSC および AC リリースと、それに対応するオペレーティング システムのバージョンを示します。

テーブルを展開する

チャネル	オペレーティング システムの表示バージョン
LTSC	21H2
年間チャネル	23H2

このガイダンスは、ライフサイクルおよび一般的なインベントリの目的において、LTSC と AC の識別および区別にお役立ていただくことを目的としています。 アプリケーションの互換性や特定の API サーフェスを保証する意図ではありません。 アプリ開発者は、互換性を確保するために他のガイダンスを参照する必要があります。 コンポーネント、API、および機能は、システムのライフサイクル中に追加されるか、まだ使用できない可能性があります。 プログラムによるバージョンを確認する方法の使用の詳細については、「オペレーティング システムのバージョン」を参照してください。

Windows Server の Microsoft サーバー アプリケーションの互換性

2025/08/15

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

アプリケーションの互換性は、お客様が Windows Server を選択する主な理由の 1 つであることを理解しています。 Windows Server 開発サイクルを通じて、Microsoft は Microsoft および Microsoft 以外のアプリケーションの大規模なスイートを定期的にテストして、製品ができるだけ多くのアプリケーションと互換性があることを確認します。 これらのテストは、開発ツール、グラフィックス ツール、セキュリティ ツール、ビジネス オフィス スイート、ストレージ管理、ウイルス対策、バックアップまたは回復、ユーティリティなど、Microsoft 以外の幅広いエンタープライズ アプリケーションを対象とします。

次の表に、Window Server でのインストールと機能をサポートする Microsoft サーバー アプリケーションの一覧を示します。 この情報はクイック リファレンス用であり、個々のサーバー アプリケーションの個々の製品仕様、要件、お知らせ、または一般的な通信を置き換えるものではありません。 互換性とオプションを完全に理解するには、各製品の公式ドキュメントを参照してください。

> **ヒント**
>
> Microsoft 以外のアプリケーションとの Windows Server の互換性に関する詳細を探しているソフトウェア ベンダー パートナーの場合は、**商用アプリ認定ポータルの** にアクセスしてください。

テーブルを展開する

Product	Server Core でサポートされます	デスクトップ エクスペリエンスを備えたサーバーでサポートされます	製品 Web リンク
Configuration Manager (バージョン 2409)	✅[2]	✅	Windows Server 2025 のサポート
Exchange Server（エクスチェンジ サーバー）	✅	✅	Exchange Server のサポート行列
Microsoft 365 アプリ	❌	✅	Windows と Office の構成サポート マトリックス

Product	Server Core でサポートされます	デスクトップ エクスペリエンスを備えたサーバーでサポートされます	製品 Web リンク
プロジェクトサーバー サブスクリプションエディション	✅	✅	Project Server サブスクリプション エディションのソフトウェア要件
SharePoint Server サブスクリプション エディション	✅	✅	SharePoint Server サブスクリプション エディションのシステム要件
SQL Server 2019	✅ [1]	✅	SQL Server 2019 をインストールするためのハードウェアとソフトウェアの要件
SQL Server 2022	✅ [1]	✅	SQL Server 2022 をインストールするためのハードウェアとソフトウェアの要件
システムセンター データ保護マネージャー	✅ [1]	✅	System Center Data Protection Manager の環境の準備
System Center Operations Manager	✅ [1]	✅	System Center Operations Manager のシステム要件
System Center Virtual Machine Manager	✅ [1]	✅	System Center Virtual Machine Manager のシステム要件

1. 制限がある場合や、Server Core アプリ互換性機能オンデマンド (FOD)が必要な場合があります。 詳細については、特定の製品またはオンデマンド機能のドキュメントを参照してください。

2. はい。管理されたクライアントと配布ポイントですが、サイト サーバーとしてではありません。

Windows Server 向け Azure ハイブリッド特典

2025/09/05

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Azure ハイブリッド特典を受けることで、商用利用のお客様は対象となるオンプレミス ライセンスを使用して、Azure 上で Windows 仮想マシン (VM) を割引価格で利用できます。 この記事では、対象となる Windows Server ライセンスを使用して、Azure、Azure Local、Azure Kubernetes Service (AKS) ハイブリッド デプロイの Windows Server VM のコスト削減を実現する利点について説明します。

その他の Azure ハイブリッド特典 (Microsoft SQL Server など) については、「Azure ハイブリッド特典」を参照してください。

Azure ハイブリッド特典に必要な資格は何ですか?

Windows Server 向け Azure ハイブリッド特典を利用するには、有効なソフトウェア アシュアランスまたは対象となるサブスクリプション ライセンスが適用されたプログラムの Windows Server 向けオンプレミス コア ライセンスが必要です。 ソフトウェア アシュアランスおよび対象となるサブスクリプション ライセンスは、特定の商用ライセンス契約の一部としてのみ利用できます。 商用ライセンスの詳細については、Microsoft ライセンスに関するリソースを参照してください。 Windows Server コア ライセンスの詳細については、Windows Server 製品ライセンスに関するページを参照してください。

> ⓘ **重要**
>
> - Azure ハイブリッド特典を利用したワークロードは、ソフトウェア アシュアランスまたはサブスクリプション ライセンスの期間中のみ実行できます。 ソフトウェア アシュアランスまたはサブスクリプション ライセンスの有効期限が近づいた場合、契約のソフトウェア アシュアランスまたはサブスクリプション ライセンスを更新するか、ハイブリッド特典機能を無効にするか、Azure ハイブリッド特典を使用しているそれらのワークロードをプロビジョニング解除する必要があります。
> - ご客様のプログラムの Microsoft 製品利用規約がこの記事よりも優先されます。 詳細については、**Microsoft Azure 製品利用規約** で、ご利用のプログラムを選択して、規約を確認してください。

Azure ハイブリッド特典には何が含まれていますか?

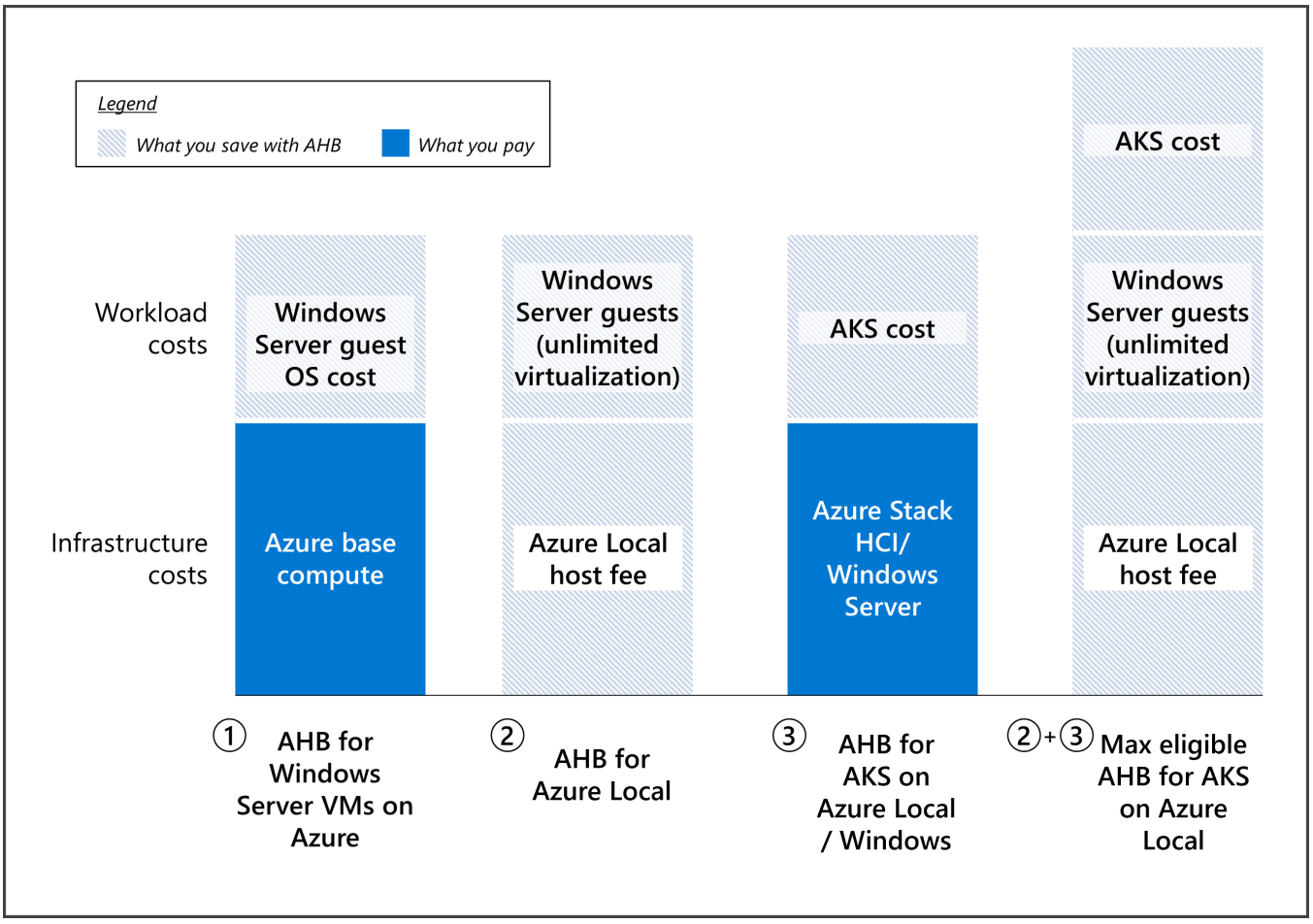
有効なソフトウェア アシュアランスまたは対象となるサブスクリプション ライセンスが適用されたプログラムによってライセンスされた Windows Server をお持ちのお客様は、Azure ハイブリッド特典を利用して、クラウド、データ センター、エッジ ロケーションのコストをさらに削減できます。

Azure ハイブリッド特典によって得られるコスト削減効果の例を次に示します。

- **Azure 上の Windows Server VM**: Windows Server のライセンスは Azure ハイブリッド特典によってカバーされるので、VM のベース コンピューティング レートのみの支払いで済みます。 ベース コンピューティング レートは、VM の Linux レートと等価です。

- **Azure Local**: Azure ハイブリッド特典では、Azure ローカル ホスト料金と Windows Server サブスクリプション料金が免除されます。 つまり、無制限の仮想化権限が追加料金なしで提供されます。 引き続き、Azure Local に関連付けられているその他のコスト (カスタマー マネージド ハードウェア、Azure サービス、ワークロードなど) を支払います。

- **AKS**: 追加料金なしで Windows Server と Azure Local で AKS を実行します。 Azure Local 向けの Azure ハイブリッド特典の対象でもある場合を除き、基になるホスト インフラストラクチャと Windows コンテナーのライセンスの料金は引き続き課金されます。 Azure Local の Azure ハイブリッド特典を使用すると、Azure ローカル ホストと Windows Server サブスクリプションの料金を免除できます。



Azure ハイブリッド特典の価格

コスト削減の可能性を評価するには、次のリソースを使用してください。

- **Azure 上の Windows VM:**Windows Virtual Machines の料金。 Azure 料金計算ツールを使用してコスト削減を見積もるか、Azure ハイブリッド特典の有無にかかわらず Windows VM の価格を比較します。
- **Azure Local:**Azure Local の価格。
- **Azure Kubernetes Service (AKS):**AKS on Azure Local の価格。

Azure ハイブリッド特典の利用

お客様のシナリオに対応するタブを選択します。

Azure

Azure の Windows VM 向け Azure ハイブリッド特典を入手して管理するには、このセクションのガイダンスに従ってください。

ライセンスの前提条件

Azure の Windows VM 向け Azure ハイブリッド特典の資格を得るためには、次のライセンス前提条件を満たしている必要があります。

ライセンスの種類

- アクティブなソフトウェア アシュアランスまたはサブスクリプション付きの Windows Server Standard。
- アクティブなソフトウェア アシュアランスまたはサブスクリプション付きの Windows Server Datacenter。

ライセンス数

VM ごとに少なくとも 8 つのコア ライセンス (Datacenter または Standard エディション) が必要です。 たとえば、4 コア インスタンスを実行する場合は、8 つのコア ライセンスが必要です。 また、インスタンスのコア サイズと同じライセンスを割り当てることで、8 コアを超えるインスタンスを実行することもできます。 たとえば、12 コア インスタンスには 12 個のコア ライセンスが必要です。 プロセッサ ライセンスをお持ちのお客様の場合、各プロセッサ ライセンスは 16 コアのライセンスに相当します。

Azure 移行許容量

- **Windows Server Standard Edition:** ライセンスは、オンプレミスと Azure のどちらかで使用する必要があり、同時に使用することはできません。 唯一の例外は、最大 180 日間に 1 回だけ、同じワークロードを Azure に移行できるようにすることです。

- **Windows Server Datacenter エディション**: VM ライセンスの場合、ワークロードを Azure に移行する場合、ライセンスではオンプレミスと Azure での同時使用が無期限に許可されます。 専用ホスト ライセンスの場合、ワークロードを Azure に移行する場合、ライセンスは、ライセンスが Azure に割り当てられた時点から 180 日間、オンプレミスと Azure で同時に使用できます。

無制限の仮想化

無制限の仮想化権限とは、ホスト上の任意の数の Windows Server VM を使用する権利を指します。

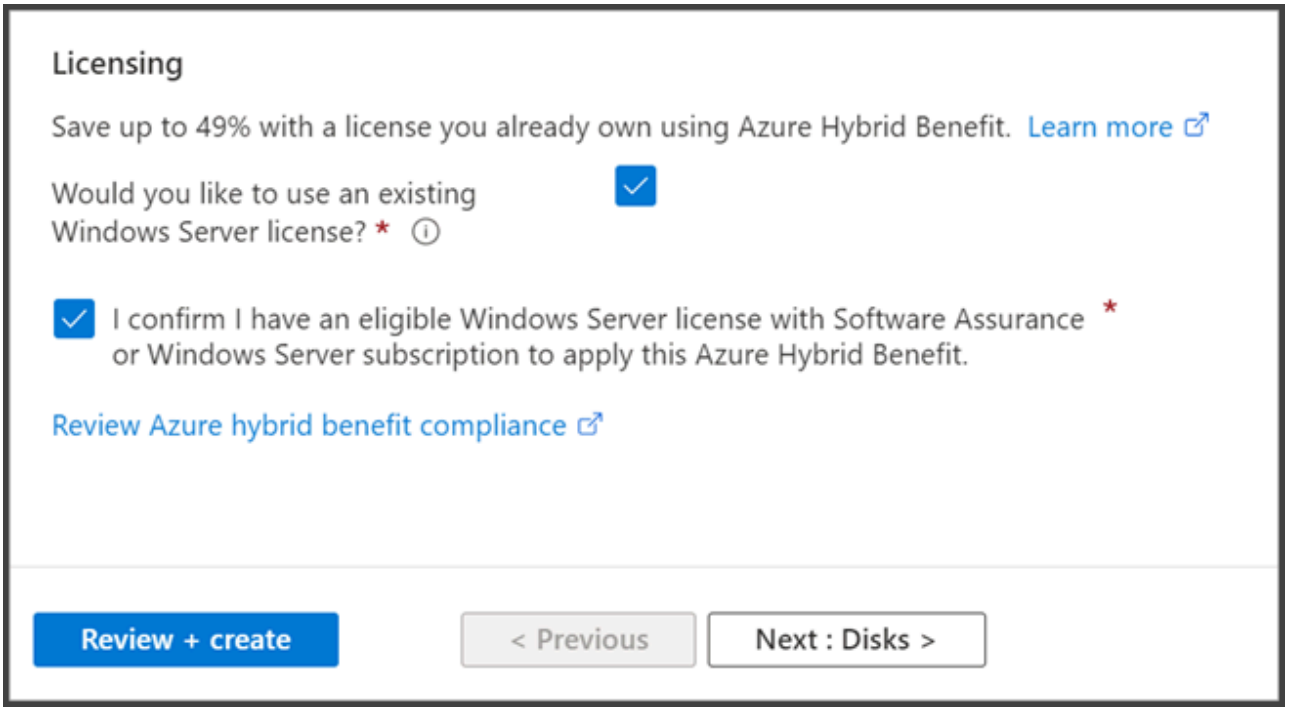
- **Windows Server Datacenter エディション**: アクティブなソフトウェア アシュアランスまたはサブスクリプションを持つ Windows Server Datacenter ライセンスを、

その Azure サーバー上で使用可能なすべての物理コアに割り当てる場合は、Azure 専用ホスト上の任意の数の Windows Server VM を使用できます。

- **Windows Server Standard Edition:** 無制限の仮想化権限は使用できません。

Azure の Windows VM 向け Azure ハイブリッド特典を適用する方法

Azure ハイブリッド特典を使用して Azure に Windows Server VM をデプロイする方法については、Windows VM 向け Azure ハイブリッド特典の調査に関する記事の手順に従ってください。 Windows Server VM の Azure ハイブリッド特典をアクティブ化する 1 つの方法は、次のスクリーンショットに示すように、VM の作成時に [**ライセンス**] の下にあるチェック ボックスをオンにすることです。



ライセンス要件への準拠を維持する方法

Windows Server VM に Azure ハイブリッド特典を適用する場合は、この特典をアクティブにする前に、対象となるライセンスの数とソフトウェア アシュアランス (またはサブスクリプション) のカバレッジ期間を確認してください。 上記のガイドラインに従い、この特典を使用して適切な数の Windows Server VM をデプロイしてください。

既に Azure ハイブリッド特典を使用して Windows Server VM を実行している場合は、インベントリを実行して稼働ユニット数を確認し、保有するソフトウェア アシュアランスまたはサブスクリプション ライセンスに照らしてその数をチェックします。 ご使用中のソフトウェア アシュアランス ライセンス位置については、Microsoft のライセンス専門家にお問い合わせください。

Azure サブスクリプションで Azure ハイブリッド特典を使用してデプロイされたすべての VM を表示およびカウントするには、 すべての VM と仮想マシン スケール セットを一覧表示します。

また、Microsoft Azure の請求書で、Windows Server 向け Azure ハイブリッド特典を利用して実行している VM の数を確認できます。 特典があるインスタンスの数に関する情報は、[**追加情報**] で確認できます。

JSON


```
"
{"ImageType":"WindowsServerBYOL","ServiceType":"Standard_A1","VMName":"","Usag
eType":"ComputeHR"}"
```


課金はリアルタイムでは適用されません。 Azure ハイブリッド特典で Windows Server VM をアクティブにしてから VM が請求書に表示されるまでに、数時間の時間差を見込んでください。

ライセンスの状況を包括的に確認するには、各 Azure サブスクリプションでインベントリを実行します。 Azure ハイブリッド特典で実行されている Windows Server VM のライセンスが完全に付与されていることを確認してください。 それ以上の操作を行う必要はありません。

インベントリを定期的に実行して、ご自身に付与されているライセンス特典をすべて使用していることを確認してください。 定期的なインベントリによってコストを削減でき、また、Azure ハイブリッド特典でデプロイした Windows Server VM をカバーできるだけのライセンスがあることを常に確認できます。

デプロイした VM に適用できる Windows Server ライセンスが不足している場合は、次の 3 つの選択肢があります。

- ソフトウェア アシュアランスまたはサブスクリプションの対象となる Windows Server ライセンスを、商用ライセンス契約を通じて追加購入します。
- 一部の VM の Azure ハイブリッド特典を無効にし、Azure の通常の時間単位料金でそれらを購入します。
- いくつかの VM の割り当てを解除します。

> ⓘ **注意**
>
> Microsoft は、Azure ハイブリッド特典の利用資格を確認するために、随時、お客様を監査する権利を留保します。

FAQ: Azure ハイブリッド特典

Azure ハイブリッド特典の対象となるリージョンはどこですか?

Azure ハイブリッド特典は、すべての Azure リージョンとソブリン クラウドで利用できます。

ソフトウェア アシュアランスまたはサブスクリプションの有効期限が切れた場合、特典はどうなりますか?

これらの特典を使用するには、ソフトウェア アシュアランスまたは対象となるサブスクリプションがアクティブである必要があります。 ソフトウェア アシュアランスまたはサブスクリプションの有効期限が切れたときに、更新しないことを選択をした場合は、Azure portal 内のリソースから特典を削除する必要があります。

ソフトウェア アシュアランスとは何ですか?

ソフトウェア アシュアランスは、包括的なボリューム ライセンス プログラムです。 ソフトウェア アシュアランスはボリューム ライセンスを通じてのみ利用でき、ユーザーがボリューム ライセンス契約を購入または更新するときに購入します。 一部の契約には含まれていますが、契約によってはオプションで購入する必要があります。 ソフトウェア アシュアランスの特典には、IT 投資を最大化するための新しい製品バージョンの権利、サポート、ライセンス モビリティ権、他にはないテクノロジとサービスのセットが含まれます。

ボリューム ライセンスの詳細については、「Microsoft ライセンス」を参照してください。 ソフトウェア アシュアランスの特典について、また、それぞれの特典がビジネス ニーズをどのように満たすかについて詳しくは、ソフトウェア アシュアランスの特典に関するページを参照してください。

サブスクリプションとは

サブスクリプション ライセンスとは、サブスクリプション期間中のみソフトウェアを実行するためのライセンスです。 サブスクリプション ライセンスには、ソフトウェアを実行するための永続的な権利は含まれません。

ソフトウェア アシュアランスはどのようにして入手できますか?

ソフトウェア アシュアランスはボリューム ライセンスを通じてご購入いただけます。 ソフトウェア アシュアランスの特典は、ボリューム ライセンス サービス センター (VLSC) でアク

ティブ化されます。 組織に Microsoft 製品およびサービス契約 (MPSA) がある場合、 ビジネス センター はソフトウェア アシュアランスの特典を簡単に管理するための目的地です。

こちらも参照ください

- Azure ハイブリッド特典の製品ページ
- Windows VMs 向け Azure ハイブリッド特典の検索について
- Azure Stack HCI の Azure ハイブリッド特典

Windows Server の拡張セキュリティ更新プログラムの概要

2025/08/16適用対象: ✅ Windows Server 2012, ✅ Windows Server 2012 R2

拡張セキュリティ更新プログラム (ESU) は、サポート終了後に特定のレガシ Microsoft 製品を実行する必要があるお客様のための最終手段です。 Windows Server Long Term Servicing Channel (LTSC) には、少なくとも 10 年間のサポートがあります。メインストリーム サポートの場合は 5 年、延長サポートの場合は 5 年間です。これには、定期的なセキュリティ更新プログラムが含まれます。

ただし、製品がサポート終了になると、セキュリティ更新プログラムとセキュリティ情報の終了も意味します。 このシナリオでは、セキュリティまたはコンプライアンスの問題が発生し、ビジネス アプリケーションが危険にさらされる可能性があります。 Microsoft では、最新 バージョンの Windows Server にアップグレードして 、最も高度なセキュリティ、パフォーマンス、イノベーションを実現することをお勧めします。

Windows Server 2012 および Windows Server 2012 R2 の延長サポートは、2023 年 10 月 10 日に終了しました。

> **ヒント**
>
> Microsoft ライフサイクルのサポート日に関する情報を確認できます。

拡張セキュリティ更新プログラムとは?

Windows Server の拡張セキュリティ更新プログラムには、バージョンに応じて、延長サポートの終了から最大期間にわたって重要と評価されるセキュリティ更新プログラムとセキュリティ情報が含まれます。 Azure でホストされているサーバーでは無料で利用でき、Azure でホストされていないサーバーでは購入できます。 拡張セキュリティ更新プログラムには、新機能、顧客が要求したセキュリティ以外の修正プログラム、設計変更要求は含まれません。 詳細については、「 ライフサイクルに関する FAQ - 拡張セキュリティ更新プログラム」を参照してください。

拡張セキュリティ更新プログラムでは、これらのバージョンの Windows Server のさまざまなフェーズを次に示します。

サーバーをまだアップグレードしていない場合は、移行中にアプリケーションとデータを保護するために次のことを行うことができます。

- 影響を受ける既存の Windows Server ワークロード as-is Azure Virtual Machines (VM) に移行します。 Azure に移行すると、定義された期間の拡張セキュリティ更新プログラムが自動的に提供されます。 Azure VM のコストに基づいて拡張セキュリティ更新プログラムに追加料金はかかりません。また、他の構成を行う必要はありません。
- サーバーの拡張セキュリティ更新プログラム サブスクリプションを購入し、新しい Windows Server バージョンにアップグレードする準備ができるまで保護されたままになります。 拡張セキュリティ更新プログラムサブスクリプションをお持ちの場合、Microsoft は定義された期間の更新プログラムを提供します。 サブスクリプションを購入したら、プロダクト キーを取得し、該当する各サーバーにインストールする必要があります。 詳細については、「 拡張セキュリティ更新プログラムを取得する方法」を参照してください。

次の表に、Windows Server の各バージョンの拡張セキュリティ更新プログラムの期間を示します。

テーブルを展開する

製品バージョン	ホストされている	ESU 期間	ESU の終了日
Windows Server 2012 Windows Server 2012 R2	紺碧*	3年間	2026 年 10 月 13 日
Windows Server 2012 Windows Server 2012 R2	Azure にありません	3年間	2026 年 10 月 13 日

* Azure サービスと機能を選択した環境に拡張する製品の Azure Stack ポートフォリオ が含まれています。

> ⚠ **警告**
>
> 拡張セキュリティ更新プログラムの期間が終了すると、更新プログラムの提供は停止されます。 できるだけ早く、Windows Server のバージョンをより新しいバージョンに更新することをお勧めします。

Azure への移行

オンプレミス のサーバーが、延長サポートに達したか、または延長サポートの終了に近づくバージョンの Windows Server を実行している場合は、それらを Azure に移動できます。 Azure では、これらのサーバーを仮想マシンとして引き続き実行できます。 Azure に移行する場合、セキュリティ更新プログラムに準拠し続けるだけでなく、クラウド イノベーションを作業に追加することもできます。 Azure に移行する利点は次のとおりです。

- Azure のセキュリティ更新プログラム。
- Windows Server の重要で重要なセキュリティ更新プログラムを一定期間取得します(追加料金なしで含まれます)。
- Azure でのアップグレードは無料です。
- 準備ができたらいつでも、より多くのクラウド サービスを導入します。
- SQL Server を Azure VM に移行すると、さらに 3 年間の Windows Server の重要なセキュリティ更新プログラムが追加料金なしで含まれます。 SQL Server を Azure SQL Managed Instance に最新化することもできます。
- Azure ハイブリッド特典 を利用すると、Azure 固有のクラウド節約のために既存の Windows Server ライセンスと SQL Server ライセンスを使用できます。

移行を開始するには、 一般化された VHD をアップロードし、それを使用して Azure に新しい VM を作成する方法、または Azure で共有イメージ ギャラリーを使用する方法について説明します。

Windows Server の移行ガイド を読んで、次のことに関するヘルプを参照することもできます。

- 既存の IT リソースを分析します。
- デプロイの現在の状態を評価します。
- 特定のサービスとアプリケーションをクラウドに移動するかどうかを決定します。 または、オンプレミスのままにして、最新バージョンの Windows Server にアップグレードします。 組織に最適なオプションを選択します。

オンプレミスのアップグレード

Azure とクラウドに移行するのではなく、サーバーをオンプレミスに保持する必要がある場合は、次の 2 つの方法を選択できます。

- サポートされているバージョンの Windows Server で新しいサーバーを構築し、アプリケーションとデータを移行します。
- サポートされているバージョンの Windows Server にインプレースでアップグレードします。

インプレース アップグレードでは、通常、少なくとも 1 つのバージョン (場合によっては 2 つのバージョン) を使用して Windows Server をアップグレードできます。 たとえば、Windows Server 2012 R2 は、インプレースで Windows Server 2025 にアップグレードできます。 アップグレードすると、いつでも Azure に移行できます。 オンプレミスのアップグレード オプションの詳細については、 Windows Server でサポートされているアップグレード パスを参照してください。

Windows Server と並行して SQL Server をアップグレードする

延長サポートに達したか、延長サポートが終了するバージョンの SQL Server を実行している場合は、SQL Server の拡張セキュリティ更新プログラムの恩恵を受けることもできます。 詳細については、「 SQL Server と Windows Server の拡張セキュリティ更新プログラム」を参照してください。

関連コンテンツ

- Windows Server の拡張セキュリティ更新プログラム (ESU) を取得する方法について説明します。
- Windows Server のアップグレードの概要

セキュア コア サーバーとは

2023/04/11

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Azure Local 2311.2 and later

セキュア コアとは、組み込みのハードウェア、ファームウェア、ドライバー、オペレーティング システムのセキュリティ機能を提供する機能のコレクションです。 セキュア コア システムによって提供される保護は、オペレーティング システムを起動する前に開始され、実行中は継続されます。 セキュア コア サーバーは、重要なデータとアプリケーション向けにセキュリティで保護されたプラットフォームを提供するように設計されています。

セキュア コア サーバーは 3 つのセキュリティの柱に基づいて構築されています。

- ハードウェアによる信頼のルートを作成する。
- ファームウェア レベルの攻撃から防御する。
- 検証されていないコードの実行から OS を保護する。

セキュア コア サーバーの概要

セキュア コア イニシアチブは、これまでで最も高度な Windows セキュリティを提供するために、Microsoft と PC 製造パートナー間の深いコラボレーションを通じて Windows PC から始まりました。 Microsoft は、Windows Server で安全なオペレーティング システム環境を提供できるように、サーバー製造パートナーとのパートナーシップをさらに拡大しました。

Windows Server はハードウェアと密接に統合され、強化されたセキュリティ レベルを実現します。

- 推奨されるベースライン: ハードウェアの信頼のルートとセキュア ブートのために TPM 2.0 を使用して基本的なシステム整合性を提供するために、すべてのシステムに推奨される最小値。 Windows Server ハードウェア認定では、TPM 2.0 とセキュア ブートは必須です。 詳細については、「Microsoft が次の主要な Windows Server リリースのセキュリティ標準を引き上げる」を参照してください。
- セキュア コア サーバー: より高いレベルの保証を必要とするシステムや業界に推奨されます。 セキュア コア サーバーは、以前の機能を基に構築され、高度なプロセッサ機能を活用してファームウェア攻撃から保護します。

次の表は、各セキュリティの概念と機能を使用して、セキュア コア サーバーを作成する方法を示しています。

テーブルを展開する

概念	機能	要件	推奨されるベースライン	セキュア コア サーバー
ハードウェアによる Root of Trust を作成する				
	セキュア ブート	セキュア ブートは、Unified Extensible Firmware Interface (UEFI) BIOS で既定で有効になっています。	✓	✓
	トラステッド プラットフォーム モジュール (TPM) 2.0	Trusted Computing Group (TCG) 仕様に関する最新の Microsoft 要件を満たします。	✓	✓
	Windows Server 認定	サーバー システムがセキュリティ、信頼性、管理容易性において Microsoft の最高の技術水準を満たしていることを示します。	✓	✓
	ブート DMA 保護	入出力メモリー管理ユニット (IOMMU) を持つデバイスでのサポート。 たとえば、Intel VT-D や AMD-Vi などです。		✓
ファームウェア レベルの攻撃から防御する				
	System Guard セキュア起動	測定のための動的な信頼のルート (DRTM) 互換の Intel および AMD を搭載したオペレーティング システムで有効です。		✓
検証されていないコードの実行から OS を保護する				
	仮想化ベースのセキュリティ (VBS)	Windows ハイパーバイザーが必要です。このハイパーバイザーは、Intel VT-X や AMD-v などの仮想化拡張機能を備えた 64 ビットの IA プロセッサでのみサポートされています。	✓	✓
	ハイパーバイザーで強化されたコード整合性 (HVCI)	ハイパーバイザー コード整合性 (HVCI) 互換ドライバーと VBS 要件。	✓	✓

ハードウェアによる Root of Trust を作成する

UEFI セキュア ブートは、システムのブート コンポーネントを検証して、悪意のあるルートキットからサーバーを保護するセキュリティ標準です。 セキュア ブートは、信頼された作成者が UEFI ファームウェア ドライバーとアプリケーションにデジタル署名したことを確認します。 サーバーが起動されると、ファームウェアは、ファームウェア ドライバーや OS を含む各ブート コンポーネントの署名をチェックします。 署名が有効な場合、サーバーが起動し、ファームウェアによって OS に制御が渡されます。

ブート プロセスの詳細については、「Windows ブート プロセスをセキュリティで保護する」を参照してください。

TPM 2.0 は、機密性の高いキーとデータに対して、安全でハードウェアを使用したストレージを提供します。 ブート プロセス中に読み込まれるすべてのコンポーネントが測定され、測定値が TPM に格納されます。 ハードウェアの信頼のルートを検証すると、TPM 2.0 を使用する BitLocker などの機能によって提供される保護が強化され、構成証明ベースのワークフローの作成が容易になります。 これらの構成証明ベースのワークフローは、ゼロ トラスト セキュリティ戦略に組み込むことができます。

トラステッド プラットフォーム モジュールと Windows による TPM の使用方法についての詳細を確認してください。

セキュア ブートと TPM 2.0 と共に、Windows Server セキュア コアでは、入出力メモリ管理ユニット (IOMMU) を備えた互換性のあるプロセッサでブート DMA 保護が使用されます。 たとえば、Intel VT-D や AMD-Vi などです。 ブート DMA 保護を使用すると、システムはブート中およびオペレーティング システムの実行中にダイレクト メモリ アクセス (DMA) 攻撃から保護されます。

ファームウェア レベルの攻撃から防御する

エンドポイント保護と検出ソリューションでは、通常、オペレーティング システムの下でファームウェアが実行されることを考えると、ファームウェアの可視性が制限されます。 ファームウェアは、オペレーティング システムとハイパーバイザー カーネルよりも高いレベルのアクセス権と特権を持つため、攻撃者にとって魅力的なターゲットになります。 ファームウェアを対象とする攻撃により、オペレーティング システムによって実装される他のセキュリティ対策が損なわれるため、システムまたはユーザーがいつ侵害されたかを特定することが困難になります。

Windows Server 2022 以降では、System Guard Secure Launch は、AMD と Intel のハードウェア機能を使用して、ファームウェア攻撃からブート プロセスを保護します。 測定のための動的な信頼のルート (DRTM) テクノロジのプロセッサ サポートを使用して、セキュア コア サーバーではハードウェアを使用するサンドボックスにファームウェアを配置します。これは、高

い権限を持つファームウェア コードの脆弱性の影響を制限するのに役立ちます。 System Guard は、互換性のあるプロセッサに組み込まれている DRTM 機能を使用してオペレーティング システムを起動し、検証済みコードを使用して、システムが信頼された状態で起動されるようにします。

検証されていないコードの実行から OS を保護する

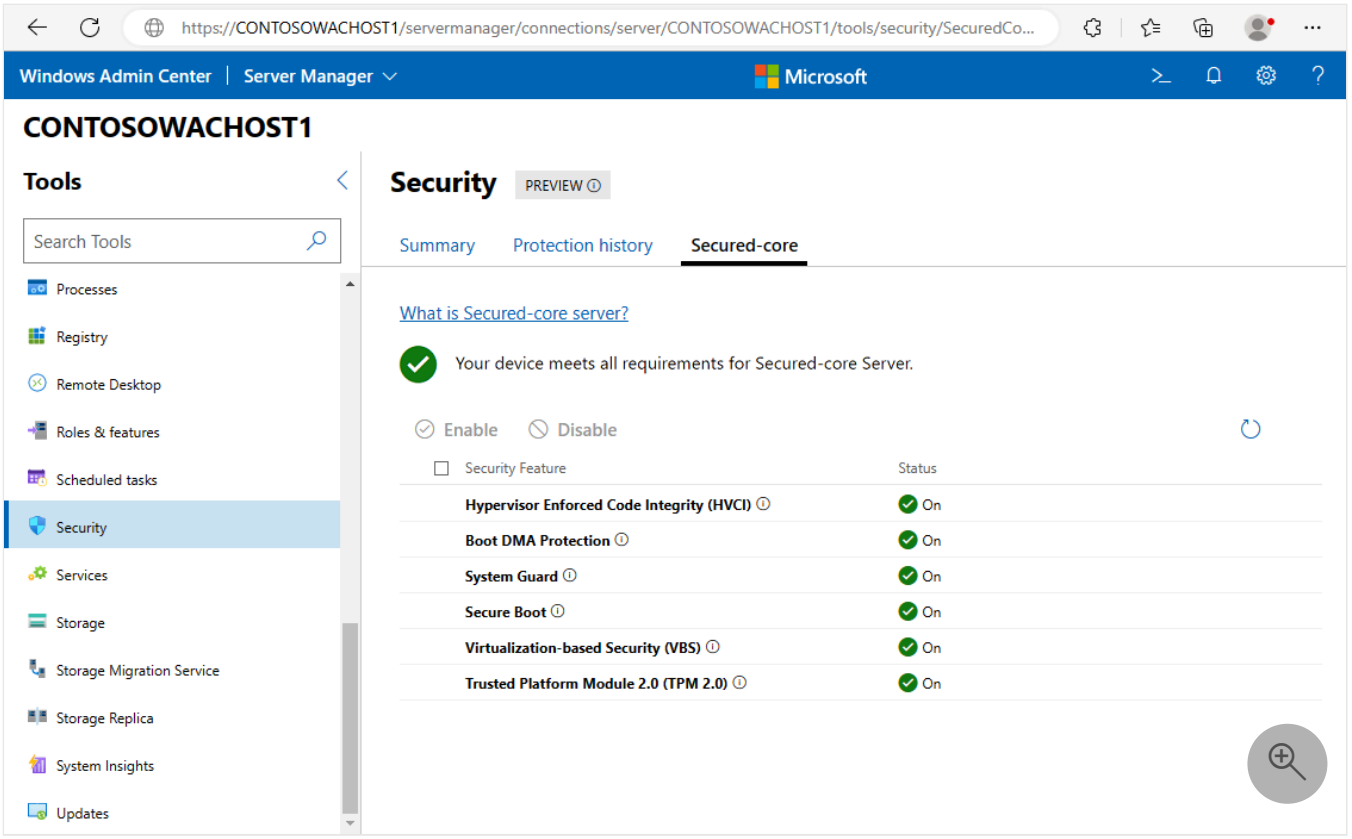
セキュア コア サーバーは、仮想化ベースのセキュリティ (VBS) とハイパーバイザーで保護されたコード整合性 (HVCI) を使用して、メモリのセキュリティで保護された領域を作成し、通常のオペレーティング システムから分離します。 VBS では、Windows ハイパーバイザーを使用して仮想保護モード (VSM) を作成し、オペレーティング システム内でセキュリティ境界を提供します。これは、他のセキュリティ ソリューションで使用できます。

HVCI は、一般にメモリ整合性保護と呼ばれ、署名済みで信頼されたコードのみがカーネルでの実行を許可されるようにするのに役立つセキュリティ ソリューションです。 署名済みの信頼されたコードのみを使用すると、カーネル モード コードの変更を試みる攻撃を防ぐことができます。 たとえば、ドライバーを変更する攻撃や、悪意のあるコードをカーネルに挿入しようとする WannaCry などの悪用。

VBS とハードウェアの要件の詳細については、仮想化ベースのセキュリティに関する記事を参照してください。

簡素化された管理

Windows PowerShell または Windows Admin Center のセキュリティ拡張機能を使用して、セキュア コア システムの OS セキュリティ機能を表示および構成できます。 Azure Local 統合システムを使用すると、製造パートナーは、Microsoft の最高のサーバー セキュリティをすぐに利用できるように、お客様の構成エクスペリエンスをさらに簡素化しました。



Windows Admin Center の詳細を確認してください。

予防的防御

セキュア コア機能を有効にすることで、攻撃者がシステムを悪用するために使用するさまざまな経路を積極的に防御し、妨害することができます。 セキュア コア サーバーは、テクノロジ スタックの最下位層で高度なセキュリティ機能を有効にし、多くのセキュリティ ツールが悪用を認識する前に、最も高いレベルの特権が必要なシステム領域を保護します。 また、IT および SecOps チームによる追加のタスクや監視を必要とせずに実行されます。

セキュア コアの使用を開始する

セキュリティで保護されたコア サーバーの認定を受けたハードウェアは、Windows Server カタログ から、Azure ローカル サーバーは Azure ローカル カタログ にあります。 これらの認定サーバーには、ハードウェア、ファームウェア、オペレーティング システムに組み込まれた業界をリードするセキュリティ軽減策が完全に装備されており、一部の最も高度な攻撃ベクトルを阻止するのに役立ちます。

次のステップ

セキュア コア サーバーの概要を理解したので、ここでは、使用を開始するためのリソースをいくつか紹介します。 次の方法について説明します。

- セキュア コア サーバーの構成。
- Microsoft セキュリティ ブログの「Microsoft がセキュア コアを使用して、高度なハードウェア セキュリティをサーバーとエッジに提供」。
- Microsoft セキュリティ ブログの「インフラストラクチャをセキュリティで保護するために、Microsoft エコシステムから新しいセキュア コア サーバーを利用可能」。
- 「Windows ハードウェア互換性プログラムの仕様とポリシー」のすべての Windows プラットフォームでの Windows 互換デバイス、システム、フィルター ドライバーの構築。

セキュリティで保護されたコア サーバーを構成する

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

セキュリティで保護されたコアは、組み込みのハードウェア、ファームウェア、ドライバー、オペレーティング システムのセキュリティ機能を提供する機能のコレクションです。 この記事では、Windows Admin Center、Windows Server デスクトップ エクスペリエンス、およびグループ ポリシーを使用して、セキュリティで保護されたコア サーバーを構成する方法について説明します。

セキュリティで保護されたコア サーバーは、重要なデータとアプリケーション用のセキュリティで保護されたプラットフォームを提供するように設計されています。 詳細については、「セキュリティで保護されたコア サーバー 」を参照してください。

Prerequisites

セキュリティで保護されたコア サーバーを構成する前に、次のセキュリティ コンポーネントが BIOS にインストールされ、有効になっている必要があります。

- セキュア ブート。
- トラステッド プラットフォーム モジュール (TPM) 2.0。
- システム ファームウェアは、プリブート DMA 保護要件を満たし、カーネル DMA 保護をオプトインして有効にするには、ACPI テーブルに適切なフラグを設定する必要があります。 カーネル DMA 保護の詳細については、oemのカーネル DMA 保護 (メモリ アクセス保護) を参照してください。
- BIOS で次のサポートが有効になっているプロセッサ。
  - 仮想化拡張機能。
  - 入出力メモリ管理ユニット (IOMMU)。
  - Dynamic Root of Trust for Measurement (DRTM)。
  - 透過的なセキュリティで保護されたメモリ暗号化は、AMD ベースのシステムにも必要です。

> **ⓘ 重要**
>
> BIOS で各セキュリティ機能を有効にすることは、ハードウェア ベンダーによって異なる場合があります。 ハードウェアの製造元のセキュリティで保護されたコア サーバーの有効化ガイドを確認してください。

セキュリティで保護されたコア サーバーの認定を受けたハードウェアは、Windows Server カタログ から、Azure ローカル サーバーは Azure ローカル カタログ にあります。

セキュリティ機能を有効にする

セキュリティで保護されたコア サーバーを構成するには、特定の Windows Server セキュリティ機能を有効にする必要があります。関連する方法を選択し、手順に従います。

GUI

ユーザー インターフェイスを使用して、セキュリティで保護されたコア サーバーを有効にする方法を次に示します。

1. Windows デスクトップから [**スタート**] メニューを開き、[**Windows 管理ツール**] を選択し、[**コンピューターの管理**] **を開きます**。
2. [コンピューターの管理] で、[**デバイス マネージャー**] を選択し、必要に応じてデバイス エラーを解決します。
   a. AMD ベースのシステムの場合は、続行する前に DRTM ブート ドライバー デバイスが存在することを確認します
3. Windows デスクトップから [**スタート**] メニューを開き、[**Windows セキュリティ**] を選択します。
4. デバイス セキュリティ コア分離の詳細を選択し、メモリ整合性 とファームウェア保護有効にします。 ファームウェア保護を最初に有効にしてサーバーを再起動するまで、メモリの整合性を有効にできない場合があります。
5. メッセージが表示されたら、サーバーを再起動します。

サーバーが再起動されると、サーバーはセキュリティで保護されたコア サーバーに対して有効になります。

セキュリティで保護されたコア サーバーの構成を確認する

セキュリティで保護されたコア サーバーを構成したので、関連する方法を選択して構成を確認します。

GUI

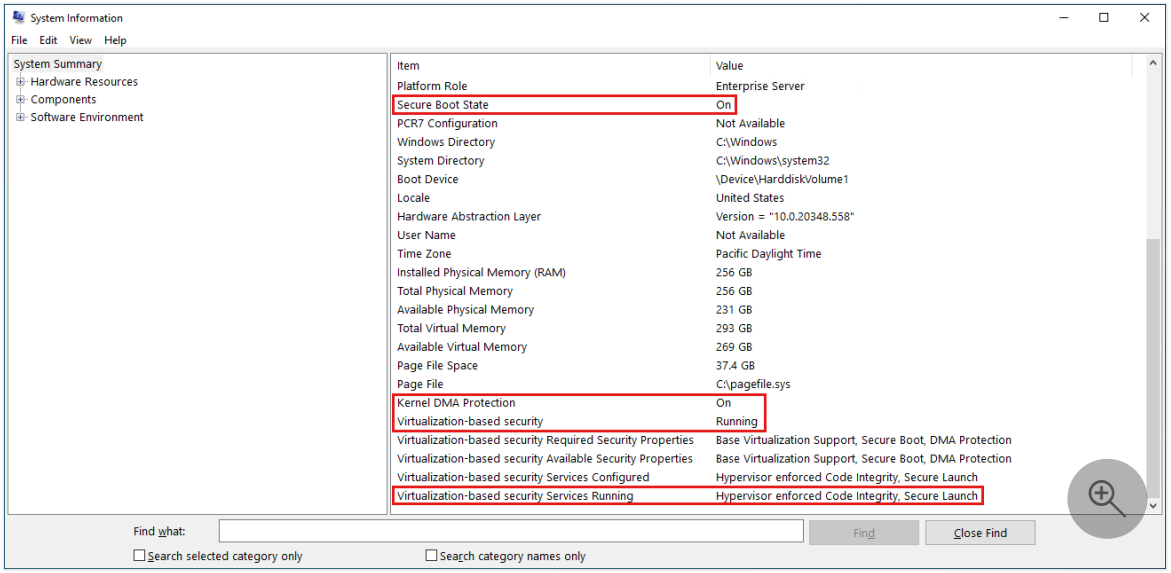
セキュリティで保護されたコア サーバーがユーザー インターフェイスを使用して構成されていることを確認する方法を次に示します。

1. Windows デスクトップから[**スタート**] メニューを開き、「 `msinfo32.exe` 」と入力してシステム情報を開きます。 [システムの概要] ページで、次の内容を確認します。

   a. [**セキュア ブートの状態**] と [**カーネル DMA 保護**] がオンになっていること。

   b. **仮想化ベースのセキュリティ** は実行中です。

   c. **仮想化ベースのセキュリティサービスは、** 実行中に、**ハイパーバイザーによって強制されるコード整合性** と **セキュアローンチ**を示します。



次のステップ

セキュリティで保護されたコア サーバーを構成したので、詳細については、次のリソースを参照してください。

- 仮想化ベースのセキュリティ (VBS)
- メモリ整合性と VBS 有効化
- システムガード セキュア起動

Windows Server 用ホットパッチ

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022

ホットパッチは、コンピューターを再起動しなくても Windows Server に OS セキュリティ更新プログラムをインストールする方法です。 ホットパッチを適用すると、プロセスを再起動する必要なく、実行中のプロセスのメモリ内コードにパッチが適用されます。 ホットパッチには、次の利点もあります。

- バイナリの数が少ないほど、更新プログラムのインストール速度が速くなり、ディスクと CPU リソースの消費が少なくなります。
- マシンを再起動する必要が少なく、ワークロードへの影響が少なくなります。
- ホットパッチ更新プログラム パッケージは、コンピューターの再起動を必要とせずに高速にインストールされる Windows セキュリティ更新プログラムを対象とするため、保護が強化されます。
- セキュリティ リスクや変更ウィンドウに晒される時間を短縮し、Azure Update Manager を使用したパッチ オーケストレーションが容易になります。

サポートされているプラットフォーム

Azure と Azure ローカル仮想マシン

次の表に、Azure 上の Windows Server 2022 と Windows Server 2025 のホットパッチをサポートする発行元、OS オファー、SKU の正確な組み合わせを示します。 これらの組み合わせを使用して Azure Local で作成した仮想マシン (VM) でもホットパッチがサポートされます。

> **Note**
>
> Windows Server コンテナーの基本イメージ、カスタム イメージ、または発行元、オファー、SKU のその他の組み合わせはサポートされていません。

テーブルを展開する

出版社	OS 製品	SKU
MicrosoftWindowsServer	ウィンドウズサーバー	2022-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	ウィンドウズサーバー	2022-Datacenter-Azure-Edition-Core-smalldisk
MicrosoftWindowsServer	ウィンドウズサーバー	2022-Datacenter-Azure-Edition-Hotpatch

出版社	OS 製品	SKU
MicrosoftWindowsServer	ウィンドウズサーバー	2022-Datacenter-Azure-Edition-Hotpatch-smalldisk
MicrosoftWindowsServer	ウィンドウズサーバー	2025-Datacenter-Azure-Edition
MicrosoftWindowsServer	ウィンドウズサーバー	2025-Datacenter-Azure-Edition-smalldisk
MicrosoftWindowsServer	ウィンドウズサーバー	2025-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	ウィンドウズサーバー	2025-Datacenter-Azure-Edition-Core-smalldisk

使用可能なイメージの詳細については、Azure Marketplace 上の Windows Server に関するページを参照してください。

Azure Arc に接続されたマシン

> **重要**
>
> Windows Server 2025 用 Azure Arc 対応ホットパッチは、月額サブスクリプション料金で利用できるようになりました。 価格の詳細については、「**すべての再起動の疲れ」を参照してください。Windows Server のホットパッチを取得します**。

Azure Arc に接続された Windows Server 2025 マシンは、Azure Arc Portal で機能を有効にした場合、ホットパッチを受け取ることができます。 Azure Arc 対応ホットパッチの使用を開始するには、次のいずれかのエディションを使用して Azure Arc をマシンに接続します。

- Windows Server 2025 Datacenter Edition)
- Windows Server 2025 Standard Edition

ホットパッチのしくみ

ホットパッチは、まず、Windows Server 用の現在の累積的な更新プログラムを使用してベースラインを確立します。 3 か月ごとに、ベースラインは最新の累積的な更新プログラムで定期的に更新されます。 その後、累積的な更新プログラムの後の 2 か月間のホットパッチ リリースを受け取ります。 たとえば、1 月が累積的な更新プログラムの場合、2 月と 3 月にはホットパッチリリースが適用されます。 ホットパッチリリーススケジュールの詳細については、Windows Server ホットパッチカレンダーを参照してください。

ベースラインには、計画ベースラインと**計画外ベースラインの** 2 種類があります。

- **計画されたベースライン** は定期的にリリースされ、その間にホットパッチのリリースが行われています。 計画されたベースラインには、その月の同等の最新累積更新がすべて含まれており、コンピューターを再起動する必要があります。
  - たとえば、計画された 1 年間のリリース期間には、カレンダー年に 4 つの計画されたベースライン リリースと 8 つのホットパッチ リリースが含まれる場合があります。

- **計画外のベースライン** は、その特定の更新プログラムをホットパッチとしてリリースできない場合、計画外の重要な更新 (ゼロデイ修正など) 中にリリースされます。 計画外のベースラインがリリースされると、ホットパッチ リリースはその月の計画外のベースラインに置き換えられます。 計画外ベースラインには、その月の最新の累積的な更新プログラムに相当するすべての更新プログラムも含まれているため、コンピューターの再起動が必要になります。
  - これらのイベントは計画外であるため、開発者は計画外のベースラインを事前に予測できません。

ホットパッチの更新プログラムでは、コンピューターを再起動する必要はありません。 Hotpatches は実行中のプロセスのメモリ内コードにパッチを適用するため、再起動する必要がないため、アプリケーションは影響を受けません。 この再起動の欠如は、パッチ自体のパフォーマンスや機能への影響には影響しません。

サポートされている更新プログラム

ホットパッチは、Windows セキュリティ更新プログラムを対象とし、通常の非ホットパッチ Windows 更新プログラム チャネルで発行されるセキュリティ更新プログラムの内容と同等の状態を維持します。

サポートされているバージョンの Windows Server でホットパッチを有効にする際に考慮する必要がある重要な点がいくつかあります。 ホットパッチ プログラムに含まれていない更新プログラムをインストールするには、コンピューターを再起動する必要があります。 また、新しいベースラインをインストールした後、定期的に再起動する必要もあります。 再起動すると、最新の累積的な更新プログラムに含まれるセキュリティ以外のパッチと VM の同期が維持されます。

現在、次のパッチはホットパッチ プログラムに含まれていないので、ホットパッチのリリース月中にマシンを更新する必要があります。

- Windows のセキュリティ以外の更新プログラム
- .NET の更新
- Windows 以外の更新プログラム (ドライバー、ファームウェアの更新プログラムなど)。

パッチ オーケストレーション プロセス

ホットパッチは、Windows Update と一般的な管理プロセスの拡張機能です。 ただし、パッチ管理用のツールは、使用しているプラットフォームによって異なります。

紺碧

- サポートされている Windows Server イメージを使用して Azure で作成した VM では、VM ゲストの自動修正が 既定で有効になっています。
- ホットパッチは自動的にダウンロードされ、重大またはセキュリティとして分類されたパッチが VM に適用されます。
- ホットパッチは、VM タイム ゾーンのピーク外の時間帯にパッチを適用します。
- Azure はパッチを自動的に管理し、 可用性優先の原則に従ってパッチを適用します。
- Azure は、プラットフォームの正常性シグナルを通じて VM の正常性を監視して、修正プログラムの適用エラーを検出します。

> **Note**
>
> ホットパッチを使用する Azure Edition イメージで、均一オーケストレーションを使用して Azure Virtual Machine Scale Sets を作成することはできません。 スケール セットの Uniform オーケストレーションでサポートされる機能の詳細については、「**フレキシブル セット、Uniform セット、可用性セットの比較**」を参照してください。

Azure Local

Azure Local では、次のツールを使用して、VM のホットパッチ更新プログラムを調整できます。

- グループ ポリシーは、Windows Update クライアント設定を構成します。
- SCONFIG は、Server Core の Windows Update クライアント設定を構成します。
- Microsoft 以外のパッチ管理ソリューション。

Azure Arc に接続されたマシン

Azure Arc に接続されたマシンでは、次のツールを使用してホットパッチ更新プログラムをインストールおよび管理できます。

- Azure Update Manager
- グループ ポリシーは、Windows Update クライアント設定を構成します。
- SCONFIG は、Server Core の Windows Update クライアント設定を構成します。
- Microsoft 以外のパッチ管理ソリューション。

ホットパッチが使用するツールの詳細については、 Azure Update Manager のドキュメントを参照してください。

Azure の VM のパッチの状態について

VM のパッチの状態を表示するには、Azure portal で VM の [概要] ページを開きます。 そこから、[**操作**] で [**更新プログラム**] を選択します。 [**推奨される更新**プログラム] の下に、パッチの状態と最近インストールされたパッチが表示されます。

[**推奨される更新プログラム**] ページでは、VM のホットパッチの状態と、VM に使用可能なパッチがあるかどうかを確認できます。 「ホットパッチのしくみ」で説明したように、VM ゲストパッチの自動適用では、すべての重大パッチとセキュリティパッチが VM に自動的にインストールされます。

これら 2 つのカテゴリ以外のパッチは自動的にインストールされず、[Update compliance]\(**更新プログラムのコンプライアンス** \) タブに使用可能なパッチの一覧として表示されます。 また、[**更新履歴**] タブを確認して、過去 30 日間の VM での更新プログラムのデプロイに関するパッチ インストールの詳細を表示することもできます。

VM ゲストパッチの自動適用では、利用可能なパッチの評価が定期的に実行され、[**更新**] タブに表示されます。[**今すぐ評価**] ボタンを選択して、評価を手動で開始できます。 [更新プログラムを **今すぐ** インストール] ボタンを選択して、オンデマンドでパッチをインストールすることもできます。 このオプションを使用すると、特定のパッチ分類の下ですべての更新プログラムをインストールするかどうかを選択できます。 ナレッジ ベースの記事の一覧を指定して、含めるまたは除外する個々の更新プログラムを選択することもできます。 ただし、手動でインストールするパッチは可用性優先の原則に従っていないので、VM の再起動が必要になる場合があることに注意してください。

インストールされているパッチは、PowerShell で Get-HotFix コマンドレットを実行するか、デスクトップ エクスペリエンスの [**設定**] メニューを表示して表示することもできます。

ホットパッチのロールバックのサポート

ホットパッチ更新プログラムでは、自動ロールバックはサポートされていません。 更新中または更新後に問題が発生した場合は、最新の更新プログラムをアンインストールし、最後の機

能ベースライン更新プログラムをインストールする必要があります。 このプロセスでは、VM を再起動する必要があります。

次のステップ

- Azure Arc 対応サーバーのホットパッチを有効にする
- VM ゲストの自動パッチ
- ISO から構築された Azure Edition 仮想マシンのホットパッチを有効にする
- Azure Update Management

Last updated on 2025/07/23

インストール メディアから Windows Server をインストールする

2025/10/13

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Server をデバイスにインストールするために使用できる起動可能な USB ドライブまたは DVD を作成する方法について説明します。 Windows Server インストール メディアを作成することは、新しいサーバーを設定したり、既存のサーバーからアップグレードしたりする際に重要な手順です。 この記事では、インストール メディアを作成し、Server Core またはデスクトップ エクスペリエンスのインストール オプションを使用して Windows Server をインストールする方法について説明します。

前提 条件

Windows Server のターゲット バージョンのセットアップ メディアは、OEM (Original Equipment Manufacturer)、Retail、Visual Studio サブスクリプション、ボリューム ライセンス サービス センター (VLSC) チャネルから取得できます。 また、デバイスが Azure で実行されていない必要もあります。 Azure に Windows Server をインストールする場合は、「クイック スタート: Azure portalで Windows 仮想マシンを作成する」を参照してください。 Windows Server をインストールする前に、次のものが必要です。

- **ハードウェア**
  - デバイスは、ハードウェアの最小要件を満たすか、超える必要があります。 詳細については、「Windows Serverのハードウェア要件」を参照してください。
  - 8 GB 以上の USB フラッシュ ドライブ。
  - DVD+/-RW デュアルレイヤー ディスクを書き込み可能な光学ドライブ。
  - デュアルレイヤーの 8.5 GB DVD。
- **ソフトウェア**
  - 環境に適した Windows Server のバージョンを決定します。 詳細については、「Windows Server エディションの比較」を参照してください。
  - 製品の有効なプロダクト キーまたはサブスクリプション ライセンスがあることを確認します。 プロダクト キーとライセンス認証方法は、商用ライセンス プログラム、リテール、OEM など、Windows Server メディアを受信した配布チャネルによって異なる場合があります。

> ⓘ **注意**

Windows Hyper-V 経由で仮想環境に Windows Server をインストールするユーザーの場合、最小 RAM 要件は異なります。 詳細については、「Windows Server コンポーネントのハードウェア要件」タブを参照してください。

起動可能な USB フラッシュ ドライブを作成する

一般に、起動可能な USB ドライブの作成は、diskpart.exe ユーティリティを使用して実行できます。 USB ドライブを手動で準備する代わりに、ユーザーは次の PowerShell スクリプトを実行して USB ドライブを起動できるようにします。 このスクリプトを実行する前に、Windows Server のインストール ISO ファイルをマウントする必要があります。 ISO ファイルをマウントするには、次の手順を実行します。

1. Windows Server のインストール ISO ファイルを見つけます。
2. ISOファイルを右クリックし、**マウント**を選択します。

ISO ファイルをマウントすると、独自のドライブ文字を持つ仮想光学式ドライブが作成され、ユーザーは ISO コンテンツを USB ドライブに移行できます。

USB ドライブを接続すると、ドライブ文字が割り当てられます。 USB ドライブとマウントされた ISO の両方のドライブ文字がわかったら、次のいずれかのスクリプトを実行します。 各スクリプトは、次の一連のファイルにスキップする前に、3 回の再試行を行います。

NTFSとしてフォーマットする

します。

このスクリプトにより、USB ドライブが NTFS 形式で起動できるようになります。

PowerShell

```
# Select USB drive letter
$usbDriveLetter = Read-Host "Enter USB drive letter (Ex: E)"

# Format USB drive
Format-Volume -DriveLetter $usbDriveLetter -FileSystem NTFS -
NewFileSystemLabel "WinServerUSB" -Confirm:$false | Out-Null

# Select ISO file mount point
$isoMountPointDriveLetter = Read-Host "Enter ISO mount point drive letter (Ex:
F)"

# Copy ISO files to USB drive
$source = "$($isoMountPointDriveLetter):\"
$destination = "$($usbDriveLetter):\"
robocopy $source $destination /COPYALL /Z /E /SEC /R:3 /W:3

# Make USB drive bootable
```

```
$usbDriveNumber = (Get-WmiObject -Class Win32_DiskDrive | Where-Object
{$_.InterfaceType -eq "USB" -and $_.DeviceID -like "*$usbDriveLetter"}).Index
bootsect /nt60 $usbDriveLetter`:

# Task completion notification
Write-Host "USB Creation Complete!"
Start-Sleep -Seconds 2
```

起動可能な DVD を作成する

1. デュアルレイヤーの 8.5 GB DVD を光学ドライブに挿入します。
2. Windows Server のインストール ISO ファイルを見つけます。
3. ISO ファイルを右クリックし、**[ディスク イメージの書き込み]** を選択します。
4. **Windows ディスク イメージ バーナー** ウィザードでは、使用する **ディスク バーナー** ドライブを選択するように求められます。
5. 適切なドライブを選択した後、**[書き込み]** ボタンを選択します。
6. この手順は省略可能ですが、書き込まれたディスクと元の ISO イメージの間のエラーや不一致に対してデータ整合性が検証されるようにすることをお勧めします。 **[書き込み後のディスクの確認]** チェックボックスをオンにして、書き込まれたデータと元の ISO ファイルの内容の違いを検出できるようにします。

BIOS 設定を構成する

USB または DVD 経由で Windows Server をインストールする前に、システムが USB または DVD から起動するように、BIOS のコンピューターのブート順序を変更する必要があります。 BIOS へのアクセスは、ハードウェアによって異なる場合があります。 ほとんどの場合、デバイスの起動時に特定のキーを押して BIOS にアクセスできます。 通常、キーは、**F2**、**F10**、**F12**、または **削除**です。 デバイスのユーザー マニュアルを参照してください。 特定のハードウェアでは、POST が完了すると、BIOS にアクセスするための短いウィンドウが許可されます。 POST が完了したらすぐに、いずれかのキーを繰り返し押す必要がある場合があります。

BIOS の設定に入ったら、メニューを移動し、**ブート順序** または **ブート シーケンス** オプションを探します。 この設定を見つけるには、デバイスのユーザー マニュアルを参照してください。 ブート順序の設定を選択すると、トップダウン順に基づいてブート順序の優先順位を編集できます。 使用しているメディアのインストール方法に応じて、USB または光学式ドライブから一覧の先頭にブートを移動します。 適切な変更を加えたら、その変更を保存して BIOS を終了します。 これらの変更を適用すると、デバイスが自動的に再起動します。

> ⓘ **注意**

システムに 2 つのディスクがあり、2 つ目のディスクに Windows Server 2025 をインストールしようとすると、インストールが失敗する可能性があります。 これは、レガシ BIOS システムでは、BIOS によって列挙されたプライマリ ディスク (通常は BIOS ディスク 0) に OS をインストールする必要があるためです。 BIOS でプライマリ BIOS 列挙ディスクの明示的な構成が許可されている場合は、インストール時に指定されたディスクを選択してください。 diskpart で `SELECT DISK=SYSTEM` を実行して、最初の BIOS 列挙ディスクを識別できます。

Windows Server のインストール

ブート順序に変更を加え、USB または DVD ドライブから起動するように選択したら、次の手順に従って Windows Server をインストールします。

デスクトップ エクスペリエンス

1. USB ドライブまたは DVD を光学ドライブに接続し、デバイスを再起動します。
2. デバイスが起動すると、任意のキーを押してインストール メディアから起動するように求められます。
3. **言語設定**を選択し、言語、時刻、通貨の形式を選択し、次 を選択します。
4. **キーボード設定**を選択し、キーボードの言語を選択し、次 を選択します。
5. 「**セットアップオプション**を選択し、**Windows Server**のインストールを選択し、**ファイル、アプリ、設定を含め、すべてが削除されることに同意する**を選択して、**次へ**を選択します。」
6. **ライセンス方法の選択**で、環境に最適なオプションを選択し、**次の**を選択します。
   a. **プロダクト キー** を使用する - このオプションは、OEM、Retail、または Volume License (VL) キーを持つユーザーを対象とします。 このライセンスの種類が選択されている場合は、次の手順に進みます。
   b. **従量課金制** - このオプションは、Azure サブスクリプション ライセンスを使用するユーザーを対象とします。 このオプションは Windows Server 2025 でのみ使用でき、独自のセットである 前提条件があります。 このライセンスの種類が選択されている場合は、「Windows Server 従量課金制のセットアップ」 を参照して、インストール プロセスを続行します。
7. **[イメージの選択]** で、Windows Server のバージョンを選択した後、**[次へ]** を選択します。

8. **適用される通知とライセンス条項**を確認し、ソフトウェア条項をレビューした後、**同意**を選択します。
9. [**Windows Server をインストールする場所の選択**] で、Windows Server をインストールするディスクを選択し、[**次へ**] を選択します。
10. **[インストールの準備完了]** で、**[インストール]** を選択します。
11. デバイスが数回再起動すると、**ライセンス条項** 表示されます。 「**を選択し、** 同意して続行します。」
12. [**設定**のカスタマイズ] で、管理者アカウントの複雑なパスワードを入力し、[完了] [] を選択します。
13. 管理者アカウントにログインしたら、「診断データを Microsoft **に送信する」** の情報を確認し、**「受け入れる」**を選択します。

> ⓘ **注意**
>
> Windows Server Core 環境を管理および構成するには、サーバー構成ツール (**SConfig**) を使用できます。 詳細については、「Server Core **サーバー** の管理」および「Server Configuration Tool (SConfig)を使用して Windows Server と Azure Local の Server Core インストールを構成する」を参照してください。

関連項目

- Windows Server の使い方を始める
- Windows Server 2025 の新機能
- 役割、役割サービス、機能のインストールまたはアンインストール
- Hyper-V テクノロジの概要
- Windows Server の SMB 3 プロトコルを使用したファイル共有の概要

Server Core にアプリケーション互換性機能をオンデマンドでインストールする

2025/07/18適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019

アプリケーション互換性機能オンデマンド (FOD) は、Windows Server での Server Core インストールの互換性を強化するために設計されたオプションの機能パッケージです。 Windows Server 2019 以降では、この機能をいつでもインストールして、Windows Server の Server Core インストールとのアプリケーションの互換性を向上させ、毎日のタスク用の追加ツールを提供できます。 この記事では、アプリケーション互換性機能オンデマンドの利点について説明し、そのインストール プロセスの概要と、サーバーまたはカスタム Windows イメージに追加する手順について説明します。

その他のオンデマンド機能の詳細については、「オンデマンド 機能」を参照してください。

アプリケーション互換性機能をオンデマンドでインストールする理由

Server Core のオンデマンドアプリケーション互換性機能には、デスクトップ エクスペリエンスインストールオプションを備えたサーバーのバイナリとパッケージのサブセットが含まれています。 この省略可能なパッケージは、Windows Update または別の ISO で使用できますが、Server Core のインストールとイメージにのみ追加できます。

アプリケーション互換性機能オンデマンドで提供される主な利点は次の 2 つあります。

- サーバー アプリケーションの Server Core の互換性が向上しました。
- 通常は Server Core に含まれていない OS コンポーネントを追加します。これは、急性のトラブルシューティングとデバッグのシナリオで使用される管理タスクとソフトウェア ツールの互換性に役立ちます。

アプリケーション互換性機能オンデマンドの一部として使用できるオペレーティング システム コンポーネントは次のとおりです。

テーブルを展開する

コンポーネント	ファイル名	以降で使用可能
Device Manager	`devmgmt.msc`	Windows Server 2019
ディスクの管理	`diskmgmt.msc`	Windows Server 2019

コンポーネント	ファイル名	以降で使用可能
イベント ビューアー	`eventvwr.msc`	Windows Server 2019
フェールオーバー クラスター マネージャー	`cluadmin.msc`	Windows Server 2019
エクスプローラー	`explorer.exe`	Windows Server 2019
Hyper-V マネージャー	`virtmgmt.msc`	Windows Server 2022
Microsoft 管理コンソール	`mmc.exe`	Windows Server 2019
パフォーマンス モニター	`perfmon.exe`	Windows Server 2019
リソース モニター	`resmon.exe`	Windows Server 2019
タスク スケジューラ	`taskschd.msc`	Windows Server 2022
Windows PowerShell Integrated Scripting Environment (ISE)	`powershell_ise.exe`	Windows Server 2019

[前提条件]

開始する前に、次の前提条件を満たしていることを確認してください。

- アプリケーション互換性機能オンデマンドは、Windows Server の Server Core インストールにのみインストールできます。 デスクトップ エクスペリエンスのインストール オプションを使用して、オンデマンドでアプリケーション互換性機能をサーバーに追加しないでください。
- 必要に応じてアプリケーション互換性機能を追加する Server Core コンピューターの管理者アカウントでサインインする必要があります。
- 次の Windows Server の機能には、追加の構成が必要です。
  - フェールオーバー クラスター マネージャー (`cluadmin.msc`) では、最初にフェールオーバー クラスタリング Windows Server 機能をインストールする必要があります。
  - IIS 管理コンソール (`Web-Mgmt-Console`) は、Microsoft 管理コンソール (`mmc.exe`) を実行する必要があるため、オンデマンドでアプリケーション互換性機能をインストールする必要があります。

- カスタム Windows イメージ (WIM) にオンデマンドでアプリケーション互換性機能を追加する場合は、カスタム イメージを作成する Windows Server のバージョン用の ISO イメージ ファイルが必要です。

アプリケーション互換性機能をオンデマンドでインストールする

アプリケーション互換性機能をオンデマンドでインストールするには、特別なパッケージを Server Core インストールに追加する必要があります。このパッケージを使用すると、デスクトップ エクスペリエンスを備えたサーバーで通常見つかった追加のツールと互換性機能が提供されます。

インストール プロセスは、Windows Update からオンデマンドでアプリケーション互換性機能をインストールするか、ISO イメージをインストールするかによって異なります。 PowerShell コマンドを実行すると、Windows Update から直接この機能をインストールできます。 ISO イメージの場合は、関連する Windows Server 言語とオプション機能 ISO をダウンロードし、ローカルにマウントし、そのソースから機能をインストールする必要があります。

アプリケーション互換性機能をオンデマンドでインストールし、サーバーを再起動すると、コマンド コンソール ウィンドウのフレームの色が別の青色の網掛けに変わります。

お好みのインストール方法に関連するタブを選択します。

Windows Update

Windows Update から Windows Server の Server Core インストールにアプリケーション互換性機能をオンデマンドでインストールするには:

1. 管理者アカウントを使用してサーバーにサインインします。
2. `SConfig` では、オプション **15** を使用して PowerShell への `SConfig` を終了します。
3. 次のコマンドを実行して、アプリケーション互換性機能をオンデマンドでインストールします。 コマンドの完了には数分かかります。

   PowerShell

   ```
   Add-WindowsCapability -Online -Name
   "ServerCore.AppCompatibility~~~~0.0.1.0"
   ```

   出力は次の例のようになります。

   出力

```
Path          :
Online        : True
RestartNeeded : True
```

4. コマンドが完了したら、サーバーを再起動して変更を適用し、最新のオペレーティング システムの更新プログラムをインストールします。

> **重要**
>
> Windows Server を新しいバージョンにインプレース アップグレードする場合、アプリケーション互換性機能オンデマンドは適用されません。 アップグレード後にもう一度インストールする必要があります。 または、Windows Server のインストールに使用するカスタム Windows イメージ (WIM) に、オンデマンドでアプリケーション互換性機能を追加することもできます。 カスタム イメージにオンデマンドでアプリケーション互換性機能を追加すると、アップグレードが完了した後にアプリケーション互換性機能が存在することが保証されます。 詳細については、「**カスタム WIM イメージにオンデマンドでアプリケーション互換性機能を追加する**」セクションを参照してください。

カスタム WIM イメージにオンデマンドでアプリケーション互換性機能を追加する

カスタム Windows イメージ (WIM) にオンデマンドでアプリケーション互換性機能を追加し、そのイメージを使用して Windows Server をインストールすると、インストール プロセス中に自動的にインストールされます。 これは、Windows Server を新しいバージョンに一括アップグレードした後もそのまま残ります。

カスタム WIM イメージにアプリケーション互換性機能オンデマンドを追加するには、次の手順に従います。 必ず自分で `<values>` を変更してください。

1. カスタム イメージを作成する Windows Server のバージョンのオンデマンド機能を含む ISO イメージ ファイルをダウンロードします。 ISO イメージを、Windows Server ISO イメージ ファイルがあるのと同じフォルダーに保存します。 ISO イメージは、次のバージョンの Windows Server で使用できます。

   - Windows Server 2025
   - Windows Server 2022
   - Windows Server 2019

2. 管理者特権の PowerShell セッションで次のコマンドを実行して、言語とオプション機能の ISO と Windows Server ISO の両方をマウントします。

```PowerShell
$isoFolder = "<ISO folder path>"
$fodIsoFilename = "<FOD_ISO_filename.iso>"
$wsIsoFilename = "<Windows_Server_ISO_filename.iso>"

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
$wsIso = Mount-DiskImage -ImagePath "$isoFolder\$wsIsoFilename"
```

3. 次のコマンドを実行して、FOD ISO と Windows Server ISO がマウントされているドライブ文字を取得します。

```PowerShell
$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
$wsDriveLetter = ($wsIso | Get-Volume).DriveLetter
```

4. 次のコマンドを実行して、Windows Server ISO イメージの内容をローカル フォルダー (**C:\SetupFiles\WindowsServer\Files** など) にコピーします。 コピー操作には時間がかかる場合があります。

```PowerShell
$wsFiles = "<Windows Server files path>"
New-Item -ItemType Directory -Path $wsFiles

Copy-Item -Path ${wsDriveLetter}:\* -Destination $wsFiles -Recurse
```

5. 次のコマンドを実行して、 `install.wim` ファイル内で変更するイメージ名を取得します。 `install.wim` ファイルは、Windows Server ISO イメージの**ソース** フォルダー内にあります。 この `install.wim` ファイルで使用できるイメージの名前が出力に含まれています。

```PowerShell
$installWimPath = "<Windows Server Files Path>\sources\install.wim"

Get-WindowsImage -ImagePath $installWimPath
```

6. 次のコマンドを実行して、 `install.wim` ファイルを新しいフォルダーにマウントします。

- `$wimImageName` - 前のコマンドの出力からマウントするイメージの名前を入力します。 この例では 、**Windows Server 2022 Datacenter を使用しています**。
- `$wimMountFolder` - install.wim ファイルの内容にアクセスするときに使用する空のフォルダーを指定します。

```PowerShell
$wimImageName = "<Image name, for example Windows Server 2022 Datacenter>"
$wimMountFolder = "<WIM folder path>"

New-Item -ItemType Directory -Path $wimMountFolder
Set-ItemProperty -Path $installWimPath -Name IsReadOnly -Value $false
Mount-WindowsImage -ImagePath $installWimPath -Name $wimImageName -Path
$wimMountFolder
```

7. (バージョンに応じて) 次のコマンドを実行して、マウントされた `install.wim` イメージに必要な機能とパッケージを追加し、サンプル変数の値を独自の値に置き換えます。

   - Windows Server 2022 以降の場合:

     ```PowerShell
     $capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"

     Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
     Source "${fodDriveLetter}:\LanguagesAndOptionalFeatures" -LimitAccess
     ```

   - 以前のバージョンの Windows Server の場合:

     ```PowerShell
     $capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"

     Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
     Source "${fodDriveLetter}:\" -LimitAccess
     ```

8. 次のコマンドを実行して、 `install.wim` ファイルの変更をマウント解除してコミットします。

   ```PowerShell
   Dismount-WindowsImage -Path $wimMountFolder -Save
   ```

Windows Server をインストールするには、アプリケーション互換性機能がオンデマンドで含まれているカスタム WIM イメージを使用できます。Windows Server を新しいバージョンに

一括アップグレードしてもそのまま残ります。

Server Core に Internet Explorer 11 をインストールする

Internet Explorer 11 は、Windows Server 2022 以前のバージョンの Server Core インストールにインストールできます。 Internet Explorer では、アプリケーション互換性機能オンデマンドを最初にインストールする必要があります。 インストールする必要がある場合は、「アプリケーション互換性機能をオンデマンドでインストールする」セクションを参照してください。 オンデマンドでアプリケーション互換性機能を追加するために Internet Explorer をインストールする必要はありません。

> **ヒント**
>
> Windows Server 2022 では、Windows Server の Server Core インストールに Internet Explorer 11 を追加できますが、代わりに **Microsoft Edge** を使用する必要があります。 Microsoft Edge には **Internet Explorer モード** (IE モード) が組み込まれているため、従来の Internet Explorer ベースの Web サイトやアプリケーションに Microsoft Edge から直接アクセスできます。 Internet Explorer の製品ライフサイクルの詳細については、「ライフサイクルに関する **FAQ - Internet Explorer と Microsoft Edge**」を参照してください。

お好みのインストール方法に関連するタブを選択します。

Windows Update

Windows Update から Windows Server の Server Core インストールに Internet Explorer 11 をインストールするには:

1. Windows Server の Server Core インストールにオンデマンドでアプリケーション互換性機能がインストールされていることを確認します。
2. もう一度、必要に応じて アプリケーション互換性機能をインストールするセクションの手順に従いますが、手順 3 では、代わりに次のコマンドを実行します。

   PowerShell

   ```
   Add-WindowsCapability -Online -Name
   "Browser.InternetExplorer~~~~0.0.11.0"
   ```

   出力は次の例のようになります。

出力

```
Path           :
Online         : True
RestartNeeded : True
```

3. コマンドが完了したら、サーバーを再起動して変更を適用し、最新のオペレーティング システムの更新プログラムをインストールします。

4. サーバーの再起動後、 `SConfig` から PowerShell プロンプトに戻り、次のコマンドを実行することで、Internet Explorer 11 にアクセスできます。

PowerShell

```
& "$env:ProgramFiles\Internet Explorer\iexplore.exe"
```

> ⓘ **重要**
>
> ダブルクリックしてローカルに保存された `.htm` ファイルを開く機能はサポートされていません。 ただし、**右クリックして [Internet Explorer で開く]** を選択するか、[ファイル] を選択して Internet Explorer から直接開き、**ファイル**を**開いて**参照することができます。

ⓘ **注:** 作成者は AI の支援の下、この記事を作成しました。 詳細情報

Windows Serverのインプレース アップグレードを実行する

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

インプレース アップグレードでは、設定、サーバーの役割、およびデータをそのまま維持したまま、サーバーを古いバージョンのWindows Serverから新しいバージョンに移動します。 たとえば、Windows Server 2012 R2 から Windows Server 2025 にアップグレードできます。 その場でアップグレードしても、最新のセキュリティ機能とパフォーマンス機能を備えたサポートされているバージョンで環境が実行され続け、すべて再構築されません。

この記事では、インストール メディアからの Windows Server セットアップまたは Windows Update の機能更新プログラムを使用してアップグレードする方法について説明します。

前提条件

- Windows Serverバージョンとサポートされているアップグレード パスを確認するには、バージョン別のサポートされているインプレース アップグレード パスを参照してください。
- ターゲット サーバーに対する管理者権限。
- オペレーティング システム、アプリ、データ、VM など、サーバーの完全バックアップ。 復元テストを実行して、バックアップが有効で回復可能であることを確認します。 Windows Server Backup またはパートナー バックアップ ソリューションを使用できます。
- アップグレード中にダウンタイムが必要であるため、スケジュールされたメンテナンス期間。
- 以下の知識:
  - インプレース アップグレードをサポートするロールと機能。 Windows Server の役割と機能のアップグレードと移行を参照してください。
  - Windows Serverでサポートされているサーバー アプリケーション。 Microsoft サーバー アプリケーションの互換性については、Windows Serverの説明を参照してください。
  - Microsoft以外のアプリケーション ベンダーのサポート要件。

- あるサーバーは次のように特化されています:
  - Windows Server の ハードウェア要件を満たすか、それを超えています。
  - クラスター化されていません。 クラスターを実行している場合は、 Cluster-Aware 更新 機能または クラスター オペレーティング システムのローリング アップグレード を代わりに使用します。
- 有効なプロダクト キーとライセンス認証方法。 キーと方法は、商用ライセンス プログラム、小売チャネル、OEM など、Windows Server メディアを受信した配布チャネルによって異なる場合があります。
- USB フラッシュ ドライブやネットワークの場所など、サーバーから離れた場所にファイルを格納する場所。
- Windows Server 2012 または Windows Server 2012 R2 サーバーに Configuration Manager がインストールされている場合は、Configuration Manager をサポートするオンプレミス インフラストラクチャをアップグレードする 前と後の手順に従ってください。

> **ⓘ 重要**
>
> ほとんどのWindows Serverロールはインプレース アップグレードをサポートしていますが、Active Directory ドメイン Controllers は例外です。 インプレース アップグレードは機能する可能性がありますが、Active Directory Domain Servicesロールを実行するサーバーはアップグレードしないでください。 詳細については、「**ドメイン コントローラーを新しいバージョンの Windows Server** にアップグレードする」を参照してください。

インストール メディアを使用してアップグレードするか、Windows Updateを使用してアップグレードするかに応じて、追加の前提条件を満たす必要があります。 アップグレード方法のタブを選択します。

インストール メディア

インストール メディアのアップグレード方法は、Azure以外のサーバーにのみ適用されます。 Azure 仮想マシン (VM) 上の Windows Server をアップグレードするには、Azure 上で Windows Server を実行する VM のインプレース アップグレードを参照するか、Windows Update メソッドを使用してください。

- アップグレードするWindows Serverのバージョンのインストール メディア (ISO イメージ、USB ドライブ、または DVD)。

- ターゲット バージョンのWindows Serverのインストール メディアは、OEM (oem)、小売販売チャネル、Visual Studio サブスクリプション、またはMicrosoft 365 管理センターから入手できます。

アップグレード前の診断情報を収集する

アップグレードに失敗した場合に備え、アップグレードする前にサーバーから診断情報を収集します。 サーバーがダウンした場合にアクセスできる診断ファイルを格納します。

情報を収集するには:

1. 管理者特権の PowerShell プロンプトを開き、現在のディレクトリを書き留め、次のコマンドを実行します。

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsBuildLabEx,WindowsEditionID | Out-File -
   FilePath .\computerinfo.txt
   systeminfo.exe | Out-File -FilePath systeminfo.txt
   ipconfig /all | Out-File -FilePath ipconfig.txt
   ```

   The `Get-ComputerInfo` コマンドには PowerShell 5.1 以降が必要です。 Windows Server バージョンに PowerShell 5.1 が含まれていない場合は、レジストリ エディターを開き、`BuildLabEx` と `EditionID` の値を `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion` で見つけます。

2. エクスプローラーを開き、書き込んだディレクトリに移動し、コンピューターの USB フラッシュ ドライブまたはネットワーク上の場所にファイルをコピーします。

システム情報を収集した後、サーバー オペレーティング システム、アプリ、VM をバックアップします。 サーバーで現在実行されている VM をシャットダウンまたは移行します。 アップグレード中に VM が実行されていないことを確認します。

インプレース アップグレードを実行する

インプレース アップグレードは、インストール メディアまたはWindows Updateを使用して実行できます。 アップグレード方法のタブを選択します。

インストール メディア

> **ヒント**
>
> インストール メディアなしでアップグレードする方法をお探しですか? インストール メディアを必要とせずにアップグレードするには、[Windows Update] タブを使用します。

インストール メディアから Windows Server セットアップを実行して、インプレース アップグレードを実行します。 この手順は、Windows Server 2012 R2以降を実行している非 Azure、非クラスター化サーバーに適用されます。 アップグレード中に、サーバーが数回再起動します。

インストール メディアを使用してインプレース アップグレードを実行するには:

1. インストール メディアをマウントまたは挿入します。 エクスプローラーを開き、インストール メディアのルートに移動し、 `setup.exe` 開きます。 たとえば、ISO イメージをマウントした場合や、ドライブ D として DVD を挿入した場合、ファイル パスは `D:\setup.exe`。 **ユーザー アカウント制御**で、セットアップによる変更の許可を求められた場合は、[**はい**] を選択します。

2. 既定では、セットアップによってインストールの更新プログラムが自動的にダウンロードされます。 既定の設定で問題ない場合は、[**次へ**] を選択して続行します。

   セットアップで更新プログラムを自動的にダウンロードしない場合は、[セットアップの更新 **プログラムのダウンロード方法を変更する**] を選択し、環境に適したオプションを選択して、[**次へ**] を選択します。

3. メッセージが表示されたら、プロダクト キーを入力し、[**次へ**] を選択します。

4. インストールするWindows Serverのエディションを選択し、**Next** を選択します。

5. 該当する通知とライセンス条項を確認します。 使用条件に同意する場合は、[**同意する**] を選択します。

6. [**ファイル、設定、アプリを保持** してインプレース アップグレードを実行する] を選択し、[**次へ**] を選択します。

7. セットアップがデバイスの分析を完了すると、[**インストールの準備完了**] 画面が表示されます。 インプレース アップグレードを開始するには、[インストール] を選択**します**。

インプレース アップグレードが開始され、進行状況が画面に表示されます。 インプレース アップグレードが完了すると、サーバーが再起動します。

その場でのアップグレードを確認する

サーバーの再起動後、Windows Serverバージョンを確認し、アプリケーションをテストすることで、アップグレードが成功したことを確認します。

1. 管理者特権の PowerShell プロンプトを開きます。 次のコマンドを実行して、バージョンとエディションが予期したバージョンと一致することを確認します。

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsProductName
   ```

2. すべてのアプリケーションが実行され、クライアント接続が成功していることを確認します。

インプレース アップグレード後にサーバーが想定どおりに動作しない場合は、`C:\Windows\Panther` ディレクトリ内のセットアップ ログ ファイルを分析します。 また、SetupDiag ツールをダウンロードしてセットアップ ログ ファイルを分析します。

テクニカル サポートが必要な場合は、Microsoft サポート にお問い合わせください。

関連するコンテンツ

- Windows Server アップグレードを計画します
- ロールと機能を追加または削除する
- Windows Server管理の概要
- Windows Admin Center
- キー管理サービス (KMS) のアクティブ化計画

Last updated on 2026/04/15

Windows Server の役割と機能のアップグレードと移行

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Server の役割と機能のアップグレードまたは移行は、セキュリティ、パフォーマンス、およびサポート可能性を維持するために不可欠です。 この記事では、インプレースアップグレードまたは新しいサーバーへの移行が可能なロールと機能の概要について説明します。また、各役割と機能の詳細な移行ガイドへのリンクのほか、Windows Server 移行ツールと記憶域移行サービスに関する情報も提供します。 この情報を使用して、新しいバージョンの Windows Server へのスムーズな移行を計画し、ダウンタイムを最小限に抑え、ワークロードの継続的な信頼性を確保します。

役割と機能を Windows Server の新しいバージョンに更新するには、次の 2 つの方法があります。

- **移動：** 新しいバージョンの Windows Server を実行している新しいサーバーに役割と機能を移動します。
- **インプレース アップグレード**: 既存の Windows Server に新しいバージョンの Windows Server をインストールし、役割と機能を維持します。

ロールと機能の中には両方の方法をサポートするものもあれば、移行のみをサポートするものもあります。

Windows Server 移行ツールを使用して、多くの役割と機能を移行できます。 この機能は Windows Server に組み込まれており、役割と機能を新しいサーバーに移動するのに役立ちます。 ファイル サーバーとストレージの場合は、 Storage Migration Service を使用します。

移行ガイドでは、指定された役割と機能を 1 台のサーバーから別のサーバーに移行できます (インプレース アップグレードではありません)。 ガイドに特に記載がない限り、物理コンピューターと仮想コンピューターの間で移行できます。 デスクトップ エクスペリエンス搭載サーバーまたは Server Core を使用する Windows Server インストール間で移行することもできます。

> **ⓘ 重要**
>
> 役割と機能の移行を開始する前に、移行元サーバーと移行先サーバーの両方で、オペレーティング システムで使用可能な最新の更新プログラムが実行されていることを確認します。

新しいバージョンの Windows Server に移行またはアップグレードする前に、そのバージョンの サポート ライフサイクル ポリシー を確認してください。 サポートされている期間を理解していることを確認します。 使用する予定の特定の Windows Server リリースの ライフサイクル情報を検索 できます。

Windows Server 移行ツール

Windows Server 移行ツールを使用すると、サーバーの役割、機能、オペレーティング システムの設定、およびその他のデータと共有を、以降のバージョンの Windows Server を含むサーバーに移行できます。 これは Windows Server の機能であるため、役割と機能の追加ウィザードまたは PowerShell を使用して簡単にインストールできます。 Windows Server 移行ツールをインストール、使用、および削除する方法について説明します。

> **注意**
>
> Windows Server 移行ツールを使用したクロスサブネット移行は、Windows Server 2012 以降のリリースで利用できます。 以前のバージョンの Windows Server 移行ツールでは、同じサブネット内の移行のみがサポートされています。

アップグレードと移行のマトリックス

テーブルを展開する

サーバーの役割	インプレースでアップグレード可能?	移行はサポートされていますか?	ダウンタイムなしで移行を完了できますか?
Active Directory 証明書サービス	イエス	はい	いいえ
Active Directory Domain Services	はい	はい	イエス
Active Directory フェデレーション サービス	いいえ	イエス	いいえ (新しいノードをファームに追加する必要があります)
Active Directory ライトウェイト ディレクトリ サービス	イエス	イエス	イエス
Active Directory Rights	イエス	はい	いいえ

サーバーの役割	インプレースでアップグレード可能?	移行はサポートされていますか?	ダウンタイムなしで移行を完了できますか?
Management サービス			
DHCP サーバー	イエス	はい	イエス
DNS サーバー	イエス	イエス	いいえ
フェールオーバー クラスタリング	はい 。クラスター OS ローリング アップグレードの場合、またはアップグレードのためにクラスターによってサーバーが削除され、別のクラスターに追加された場合。	イエス	はい(Hyper-V VM を使用するフェールオーバー クラスター、またはスケールアウト ファイル サーバー ロールを実行しているフェールオーバー クラスターの場合)。 クラスター OS のローリング アップグレードを参照してください。
ファイル サービスおよび記憶域サービス	イエス	サブ構造によって異なります	いいえ
Hyper-V	はい (クラスター OS のローリング アップグレード プロセスを使用)	イエス	はい(Hyper-V VM を使用するフェールオーバー クラスター、またはスケールアウト ファイル サーバー ロールを実行しているフェールオーバー クラスターの場合)。 クラスター OS のローリング アップグレードを参照してください。
印刷および FAX サービス	いいえ	はい (`Printbrm.exe` を使用)	いいえ
リモート デスクトップ サービス	はい。すべてのサブロールに対して、混合モードのファームはサポートされていません	はい	いいえ
Web サーバー (IIS)	イエス	イエス	いいえ
Windows Server Essentials エクスペリエンス	イエス	イエス	いいえ
Windows Server Update Services	イエス	はい	いいえ
作業フォルダー	イエス	イエス	はい 。 クラスター OS のローリング アップグレード プロセスを使用しま

サーバーの役割	インプレースでアップグレード可能?	移行はサポートされていますか?	ダウンタイムなしで移行を完了できますか?
			す。

移行ガイド

以下には、特定の Windows の役割と機能に関する移行ガイドへのリンクがあります。

Active Directory

- 証明機関を移行する
- Active Directory フェデレーション サービスの役割サービスの移行
- AD RMS を Windows Server 2016 にアップグレードする
- ドメイン コントローラーを新しいバージョンの Windows Server にアップグレードする
- Active Directory Domain Services とドメイン ネーム システム (DNS) サーバー移行ガイド

BranchCache（ブランチキャッシュ）

- BranchCache 移行ガイド

DHCP

- DHCP サーバーの移行
- 既存の DHCP フェールオーバーの展開を移行する

フェールオーバー クラスタリング

- クラスター OS のローリング アップグレードを使用して Windows Server フェールオーバー クラスターをアップグレードする
- 同じハードウェア上のフェールオーバー クラスターのアップグレード
- クラスター ロールの移行
- クラスター化されたサービスとアプリケーションを Windows Server 2012 に移行する

ファイル サービスおよび記憶域サービス

- ストレージ移行サービス
- ファイル サービスとストレージ サービスの移行
- 記憶域スペース ダイレクト クラスターをアップグレードする

Hyper-V

- Hyper-V の移行
- Windows または Windows Server の Hyper-V での仮想マシンのバージョンのアップグレード

ネットワーク ポリシー サーバー

- ネットワーク ポリシー サーバーの移行
- 正常性登録機関の移行

印刷とドキュメント サービス

- 印刷サービスとドキュメント サービスを移行する

リモート デスクトップ サービス

- リモート デスクトップ サービスの移行
- リモート デスクトップ サービス クライアント アクセス ライセンス (RDS CAL) を移行する

ルーティングとリモート アクセス

- DirectAccess から Always On VPN への移行の概要
- RRAS 移行ガイド

Web サーバー (IIS)

- Web サーバー (IIS)

Windows Server Update Services

- Windows Server Update Services を Windows Server 2012 R2 に移行する

その他の Windows 移行ガイド

- ローカル ユーザーとグループの移行ガイド
- IP 構成移行ガイド

Windows Server のエディションとライセンスの種類を変換する

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows Server をインストールした後は、エディション間 (評価版からリテール版、Standard 版からデータセンター版など) を変換し、ライセンスの種類 (リテール、ボリューム ライセンス、OEM) を切り替えることができます。 この記事では、各変換シナリオの手順について説明します。

サポートされているインプレース アップグレードのパスと制限については、「 Windows Server のアップグレードを計画する」を参照してください。

前提条件

Windows Server のエディションまたはライセンスの種類を変換する前に、次の内容を確認してください。

- ターゲット エディションまたはライセンスの種類のプロダクト キー。
- 変換対象のサーバーで管理者特権のコマンド プロンプトまたは PowerShell セッション。
- サーバーへの管理アクセス。

評価版から製品版への変換

Windows Server の評価版およびエディションを製品版およびエディションに変換できます。 たとえば、Standard (デスクトップ エクスペリエンス) エディションの評価版をインストールする場合は、Standard (Desktop Experience) エディションまたは Datacenter (Desktop Experience) エディションの製品版に変換できます。

ただし、Windows Server のどの評価版およびエディションも、すべての製品版またはエディションに変換できるわけではありません。 たとえば、評価版 Datacenter エディションをインストールする場合は、Retail Standard エディションではなく、Retail Datacenter エディションにのみ変換できます。

Windows Server 2016 以降、デスクトップ エクスペリエンスの評価版をコア リテール バージョンに変換することはできません。 Standard Core の評価版をインストールしている場合、製

品版の Datacenter Core にのみ変換でき、製品版の Standard Core に変換することはできません。

次の手順の指示に従って、 `DISM /online /Get-TargetEditions` コマンドを実行して、どの製品版に変換できるかを判断することが重要です。 必要な製品版がターゲットのバージョンとして一覧表示されていない場合は、必要な製品版を新たにインストールする必要があります。

> ⓘ **Note**
>
> サーバーで評価版が実行されていることを確認するには、管理者特権でのコマンド プロンプトで次のいずれかのコマンドを実行します。
>
> - `DISM /online /Get-CurrentEdition` を実行し、現在のエディション名が `Eval` に含まれていることを確認します。
> - `slmgr.vbs /dlv` を実行し、出力に `EVAL` が含まれていることを確認します。

Windows がアクティブ化されていない場合、デスクトップの右下隅に評価期間の残り時間が表示されます。

Windows Server Standard または Datacenter

サーバーで Windows Server の Standard または Datacenter エディションが実行されている場合、利用可能な製品版に変換できます。 管理者特権でのコマンド プロンプトまたは PowerShell セッションで次のコマンドを実行します。

1. 以下のコマンドを実行して、現在のエディション名を確認します。 出力は、エディション名の省略形です。 たとえば、Windows Server Datacenter (デスクトップ エクスペリエンス) の評価版の場合、 `ServerDatacenterEval` になります。

   Windows コマンド プロンプト

   ```
   DISM /online /Get-CurrentEdition
   ```

2. 以下のコマンドを実行して、現在のインストールをどのエディションに変換できるかを確認します。 出力から、変換するエディション名を書き留めます。

   Windows コマンド プロンプト

   ```
   DISM /online /Get-TargetEditions
   ```

3. 次のコマンドを実行して、Windows Server の Microsoft ソフトウェアライセンス条項を保存します。これにより、内容を確認できるようになります。 `<target edition>` プレースホルダーを、前の手順でメモしたエディション名に置き換えます。

   Windows コマンド プロンプト

   ```
   DISM /online /Set-Edition:<target edition> /GetEula:C:\license.rtf
   ```

4. 次のコマンドで、その新しいエディション名と、対応する製品版のプロダクト キーを入力します。 set edition プロセスでは、前に保存した Windows Server の Microsoft ソフトウェアライセンス条項に同意する必要があります。

   Windows コマンド プロンプト

   ```
   DISM /online /Set-Edition:<target edition> /ProductKey:<product key>
   /AcceptEula
   ```

   例えば次が挙げられます。

   Windows コマンド プロンプト

   ```
   DISM /online /Set-Edition:ServerDatacenter /ProductKey:ABCDE-12345-ABCDE-
   12345-ABCDE /AcceptEula
   ```

> **ヒント**
>
> Dism.exe について詳しくは、「**DISM コマンド ライン オプション**」をご覧ください。

> **重要**
>
> Active Directory ドメイン コントローラーを評価版から製品版に変換することはできません。 この場合は、製品版を実行するサーバーに別のドメイン コントローラーをインストールします。 次に、評価ドメイン コントローラーによって保持されている FSMO ロールを移行します。 最後に、評価版で実行されるドメイン コントローラーから Active Directory Domain Services (AD DS) を削除します。 詳細については、「**ドメイン コントローラーから Windows Server へのアップグレード**」を参照してください。

Windows Server Essentials

サーバーで Windows Server Essentials が実行されている場合は、管理者特権でのコマンド プロンプトを起動し、次のコマンドに製品版、ボリューム ライセンス、または OEM のキーを入力することで、完全な製品版に変換できます。

Windows コマンド プロンプト

```
slmgr.vbs /ipk <license key>
```

Windows Server Standard Edition から Datacenter Edition への変換

Windows Server をインストールした後は、いつでも Windows Server Standard Edition を Datacenter Edition に変換できます。 インストール メディアから `setup.exe` を実行して、インストールをアップグレードまたは修復できます。インプレース修復と呼ばれることもあります。 `setup.exe` を実行して、任意のエディションの Windows Server でインプレース アップグレードまたはインプレース修復を行うと、結果は開始時と同じエディションになります。

Windows Server Standard Edition は、次のように Datacenter Edition に変換できます。

1. 以下のコマンドを実行して、現在のエディション名が Windows Server Standard であることを確認します。 出力はエディション名の省略形です。たとえば、Windows Server Standard (デスクトップ エクスペリエンス) Edition の場合は、`ServerStandard` になります。

   Windows コマンド プロンプト

   ```
   DISM /online /Get-CurrentEdition
   ```

2. 次のコマンドを実行して、Windows Server Datacenter が変換先として有効なオプションであることを確認します。

   Windows コマンド プロンプト

   ```
   DISM /online /Get-TargetEditions
   ```

3. 次のコマンドで、`ServerDatacenter` と製品版のプロダクト キーを入力します。

   Windows コマンド プロンプト

   ```
   DISM /online /Set-Edition:ServerDatacenter /ProductKey:<product key>
   /AcceptEula
   ```

製品版、ボリューム ライセンス、OEM ライセンス間の変換

Windows Server をインストールした後は、いつでも製品ライセンス、ボリューム ライセンス、OEM ライセンスの間で自由に変換できます。 エディション (Standard または Datacenter) は、この変換中も変わりません。 評価版から始めた場合、まず、製品版に変換し、その後、管理者特権でのコマンド プロンプトから次のコマンドを実行して、バージョン間での変換を行います。 ボリューム ライセンス、製品版、または OEM のプロダクト キーを指定します。

Windows コマンド プロンプト

```
slmgr.vbs /ipk <product key>
```

関連するコンテンツ

- Windows Server のアップグレードを計画する
- Windows Server のインプレース アップグレードを実行する
- Server Core インストール オプションとデスクトップ エクスペリエンス搭載サーバー インストール オプション
- Azure で Windows Server を実行している VM のインプレース アップグレード

Last updated on 2026/04/03

Windows Server での仮想マシンの自動ライセンス認証

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

仮想マシンの自動ライセンス認証 (AVMA) は、購入証明メカニズムとして機能し、Windows 製品が製品使用権利およびマイクロソフト ソフトウェア ライセンス条項に従って使用されていることを保証します。 AVMA を使用すると、切断された環境であっても、適切にライセンス認証された Windows Server Hyper-V ホスト上の Windows Server 仮想マシン (VM) をライセンス認証できます。 AVMA は、VM アクティブ化をライセンス認証された仮想化ホストにバインドし、起動時に VM をアクティブ化します。 AVMA を使うと、VM のライセンス状態の使用状況と履歴データに関するリアルタイム レポートを取得できます。 レポートの作成やデータの追跡は、仮想化ホストで行うことができます。

実際の適用例

仮想化ホストでは、AVMA によりいくつかのベネフィットが提供されます。 サーバー データセンター管理者は、AVMA を使って次のタスクを実行できます。

- リモートの場所で VM をアクティブ化する。
- インターネット接続の有無に関係なく VM をアクティブ化する。
- 仮想化されたシステムにアクセスする権限をまったく必要とせずに、VM の使用状況とライセンス状態を仮想化ホストから追跡する。

Service Provider License Agreement (SPLA) パートナーやその他のホスティング プロバイダーは、テナントとプロダクト キーを共有したり、テナントの VM にアクティブ化のためにアクセスしたりする必要はありません。 AVMA を使っているとき、VM のアクティブ化はテナントに対して透過的に行われます。 ホスティング プロバイダーはサーバーのログを使用して、ライセンスの準拠を確認し、クライアントの使用履歴を追跡できます。

システム要件

仮想化サーバー ホストでゲスト VM を実行するには、ホストをアクティブにする必要があります。 ホストライセンス認証キーは、 Microsoft 365 管理センター または OEM プロバイダーから取得できます。

> **注意**

フェールオーバー クラスターでは、実行されるサーバーに関係なく、ゲスト VM がアクティブ化されたままになるためには、クラスター内の各仮想化サーバー ホストがアクティブ化されている必要があります。

AVMA には、Hyper-V サーバー ホストの役割がインストールされた Windows Server Datacenter エディションが必要です。 ホストの Windows Server バージョンによって、ゲスト VM でアクティブ化できるバージョンが決まります。 次の表に、各ホスト バージョンでアクティブ化できるゲスト VM のバージョンを示します。 ホスト バージョンは、対象となるゲスト VM バージョンのすべてのエディション (Datacenter、Standard、または Essentials) にアクセスできます。

テーブルを展開する

サーバー ホストのバージョン	Windows Server 2025 ゲスト VM	Windows Server 2022 ゲスト VM	Windows Server 2019 ゲスト VM	Windows Server 2016 ゲスト VM	Windows Server 2012 R2 ゲスト VM
Windows Server 2025	X	X	X	X	X
Windows Server 2022		X	X	X	X
Windows Server 2019			X	X	X
Windows Server 2016				X	X
Windows Server 2012 R2					X

注意

AVMA は、他のサーバー仮想化テクノロジでは機能しません。

AVMA を実装する方法

AVMA を使用して VM をアクティブ化するには、アクティブ化する Windows Server のバージョンに対応する汎用 AVMA キー (AVMA キーで詳しく説明) を使用します。 VM を作成し、AVMA キーを使ってアクティブ化するには、以下の手順を実行します。

1. VM をホストするサーバーで、Microsoft Hyper-V サーバーの役割をインストールして構成します。 サーバーが正常にライセンス認証されたことを確認します。 詳細については、Hyper-V Server のインストールに関するページを参照してください。

2. 仮想マシンを作成し、サポートされている Windows Server オペレーティング システムをインストールします。

   > **ⓘ 重要**
   >
   > AVMA が機能するには、VM の設定で**データ交換統合サービス** (キーと値のペア交換とも呼ばれます) が有効になっている必要があります。 これは、新しい VM に対して既定で有効になっています。

3. Windows Server を VM にインストールしたら、VM に AVMA キーをインストールします。 PowerShell または管理者特権でのコマンド プロンプトから、次のコマンドを実行します。

   ```
   slmgr /ipk <AVMA_key>
   ```

仮想化ホスト自体がライセンス認証されていれば、VM が自動的にライセンス認証されます。

> **ヒント**
>
> 任意の**無人セットアップ ファイル**に AVMA キーを追加することもできます。

AVMA キー

Windows Server 2025

テーブルを展開する

Edition	Key
Datacenter	YQB4H-NKHHJ-Q6K4R-4VMY6-VCH67
Datacenter: Azure Edition	6NMQ9-T38WF-6MFGM-QYGYM-88J4F

Edition	Key
Standard	WWVGQ-PNHV9-B89P4-8GGM9-9HPQ4

レポートと追跡

仮想化ホストと VM の間でのキーと値のペア (KVP) 交換により、ライセンス認証情報を含む、ゲスト オペレーティング システムのリアルタイム追跡データが提供されます。 このアクティブ化情報は、VM の Windows レジストリに格納されます。 AVMA の要求に関する履歴データは、仮想化ホスト上のイベント ビューアーに記録されます。

KVP の詳細については、「データ交換: キーと値のペアを使用して Hyper-V 上のホストとゲストの間で情報を共有する」を参照してください。

> **重要**
>
> KVP データはセキュリティで保護されていません。 変更可能であり、変更の監視は行われません。 AVMA キーが別のプロダクト キー (リテール、OEM、またはボリューム ライセンス キー) に置き換えられた場合、KVP のデータは削除してください。

AVMA のアクティブ化は透過的であるため、エラー メッセージは表示されません。 ただし、AVMA 要求は、イベント ID **12310** のアプリケーション ログのイベント ビューアーの仮想化ホストと、イベント ID **が 12309** の VM にも記録されます。 次のイベントは、仮想マシンで取り込まれます。

テーブルを展開する

Notification	Description
AVMA の成功	VM がアクティブ化されました。
無効なホスト	仮想化ホストが応答していません。 このイベントは、サーバーがサポートされているバージョンの Windows を実行していない場合に生じることがあります。
無効なデータ	通常、これのイベントは、破損、暗号化、またはデータの不一致によって、仮想化ホストと VM との通信にエラーが発生したことが原因です。
アクティブ化が拒否されました	AVMA ID が一致しないため、仮想化ホストはゲスト オペレーティング システムのライセンス認証を行うことができませんでした。

キー管理サービス (KMS) 有効化の計画

2025/07/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

ここでは、キー管理サービス (KMS) のライセンス認証について、初期計画の際に検討が必要な考慮事項を説明します。

KMS はクライアントとサーバーのモデルを用いてクライアントをアクティブ化し、ボリュームライセンス認証に使用されます。 KMS クライアントは、ライセンス認証を行うために、KMS ホストと呼ばれる KMS サーバーに接続します。 KMS ホストは、ローカル ネットワーク上に存在する必要があります。

KMS ホストは、専用サーバーである必要はありません。KMS は、他のサービスと共同ホストにすることができます。 サポートされている Windows Server または Windows クライアント オペレーティング システムを実行している任意の物理または仮想システム上で KMS ホストを実行できます。 Windows Server オペレーティング システムで実行されている KMS ホストは、サーバーとクライアントの両方のオペレーティング システムを実行しているコンピューターをアクティブ化できます。 ただし、Windows クライアント オペレーティング システムで実行されている KMS ホストは、同様にクライアント オペレーティング システム実行しているコンピューターのみをアクティブ化できます。

KMS を使用するため、KMS ホストには、Microsoft で KMS ホストのライセンス認証 (つまり、認証) を実行するキーが必要です。 このキーは KMS ホスト キーと呼ばれることもありますが、正式には Microsoft 顧客固有のボリューム ライセンス キー (CSVLK) と呼ばれます。 Open、Open Value、Select、Enterprise、および Services Provider License の契約の場合は、ボリューム ライセンス サービス センター の [プロダクト キー] セクションでこのキーを取得できます。 最寄りの Microsoft ライセンス認証専用窓口 に連絡してサポートを受けることもできます。

運用上の要件

KMS は、物理コンピューターと仮想コンピューターをライセンス認証できます。しかし、KMS ライセンス認証を行うには、ネットワークに最小限の数 ("ライセンス認証のしきい値" といいます) のコンピューターが存在している必要があります。 このしきい値が満たされたうえで、KMS クライアントのライセンス認証を行うことができます。 ライセンス認証のしきい値が満たされていることを確認するために、KMS ホストは、ネットワーク上でライセンス認証を要求しているコンピューターの数を数えます。

KMS ホストは、最新の接続をカウントします。 クライアントまたはサーバーが KMS ホストにコンタクトすると、ホストはマシン ID をカウントに追加し、応答時に現在のカウント値を

返します。 カウント数が十分であれば、クライアントまたはサーバーがアクティブ化されます。 クライアントは、カウントが 25 以上の場合に有効化されます。 Microsoft Office 製品のサーバーおよびボリューム エディションは、カウントが 5 以上の場合にライセンス認証されます。 KMS は、過去 30 日間の一意の接続のみをカウントし、直近 50 件のコンタクトだけを保存します。

KMS ライセンス認証の有効期間は 180 日間です。これはライセンス認証の一般的な有効期間です。 KMS クライアントは、認証状態を維持するために、少なくとも 180 日ごとに 1 回 KMS ホストに接続してライセンス認証を更新する必要があります。 KMS クライアント コンピューターは、既定で 7 日ごとにライセンス認証を更新します。 クライアントのライセンス認証が更新された後、再びライセンス認証の有効期間が開始されます。

1 つの KMS ホストで無制限の数の KMS クライアントをサポートできます。 50 台を超えるクライアントがある場合は、KMS ホストが使用できなくなった場合に備えて 2 台以上の KMS ホストを用意することをお勧めします。 ほとんどの組織では、2 つの KMS ホストでインフラストラクチャ全体をサポートできます。

最初の KMS ホストがライセンス認証された後、最初のホスト上で使用されている CSVLK を使用して、ネットワーク上の KMS ホストをさらに 5 つまで (合計で 6 つ) ライセンス認証できます。 KMS ホストがライセンス認証された後、管理者は、同じキーを使用して、同じホストに対してライセンスの再認証を 9 回まで行うことができます。

組織で 6 つ以上の KMS ホストが必要な場合は、組織の CSVLK に対してさらにアクティブ化を要求できます。 たとえば、1 つのボリューム ライセンス認証契約に 10 か所の物理位置が含まれ、それぞれの位置にローカル KMS ホストを配置する場合などがこれに該当します。 この例外を要求するには、最寄りの Microsoft ライセンス認証専用窓口 に問い合わせます。

Windows Server および Windows クライアントのボリューム ライセンス エディションが実行されているコンピューターは、既定では、追加の構成が必要ない KMS クライアントです。

コンピューターを KMS ホスト、MAK、または製品版の Windows から KMS クライアントに変換する場合は、該当する KMS クライアント セットアップ キーをインストールすることが必要です。 詳細については、「KMS クライアント セットアップ キー」を参照してください。

ネットワークの要件

KMS ライセンス認証では、TCP/IP 接続が必要になります。 KMS ホストおよびクライアントは、既定でドメイン ネーム システム (DNS) を使用するように構成されます。 KMS ホストは、KMS クライアントがそれらを見つけ出し、接続するために必要な情報を、DNS 動的更新を使用して自動的に公開します。 これらの既定の設定をそのまま使用することもできますが、特殊なネットワークおよびセキュリティ構成要件がある場合は KMS ホストおよびクライアントを手動で構成することもできます。

KMS ホストの既定では、ポート 1688 で TCP を使用するように構成されています。

ライセンス認証のバージョン

次の表は、Windows Server および Windows のクライアント デバイスを含んだネットワークの、KMS ホストおよびクライアントのバージョンをまとめたものです。

> **ⓘ 重要**
>
> 比較的新しいクライアントでは、ライセンス認証をサポートするために KMS サーバーで Windows の更新プログラムが必要になることがあります。 ライセンス認証のエラーが発生したときは、この表の下に示した適切な更新プログラムを適用してあるかどうかを確認してください。

Windows Server 2025

テーブルを展開する

CSVLK グループ	CSVLK は KMS で有効化される	Windows エディション この KMS ホストによってアクティブ化されます
Windows Server 2025 のボリューム ライセンス	• Windows Server 2025[1] • Windows Server 2022[1] • Windows Server 2019	• Windows Server 2025 (すべてのエディション) • Windows Server 2022 (すべてのエディション) • Windows Server 半期チャネル • Windows Server 2019 (すべてのエディション) • Windows Server 2016 (すべてのエディション) • Windows Server 2012 R2 (すべてのエディション) • Windows Server 2012 (すべてのエディション) • Windows Server 2008 R2 (すべてのエディション) • Windows Server 2008 (すべてのエディション) • Windows 11 Enterprise LTSC 2024 • Windows 11 Enterprise/Enterprise N • Windows 11 Professional/Professional N • ワークステーション用 Windows 11 Professional/ワークステーション用 Professional N • 教育機関向けの Windows 11 / 教育機関向け N • Windows 10 Enterprise LTSC/LTSC N/LTSB • Windows 10 Enterprise/Enterprise N • Windows 10 Professional/Professional N

CSVLK グループ	CSVLK は KMS で有効化される	Windows エディション この KMS ホストによってアクティブ化されます
		• ワークステーション用Windows 10プロフェッショナル/ワークステーション用プロフェッショナルN • Windows 10 教育向け/Education N • Windows 8.1 Enterprise • Windows 8.1 Professional • Windows 7 Enterprise • Windows 7 Professional

1. Azure で Windows Server Datacenter: Azure Edition がアクティブ化されます。つまり、KMS ホストとして構成することはできません

KMS ホストに必要な更新プログラム

KMS ホストが実行されているオペレーティング システムとアクティブ化するオペレーティング システムによっては、次の更新プログラムの 1 つ以上をインストールする必要があります。 更新プログラムは、KMS ホストが実行されているバージョンよりも新しいバージョンの Windows をアクティブ化する場合に必要です。

> **注意**
>
> 表示される更新プログラムは最低限必要です。 以降の累積的な更新プログラムまたは月単位のロールアップがオプションとして表示される場合は、セキュリティやその他の修正プログラムの恩恵を受けるために、オペレーティング システムで利用可能な最新バージョンをインストールします。

テーブルを展開する

KMS ホストの OS バージョン	ライセンス認証する KMS クライアントの OS バージョン	必須の更新
Windows Server 2022	- Windows Server 2025	2024 年 2 月 13 日 - KB5034765 以降の累積的な更新プログラム
Windows Server 2019	- Windows Server 2025 - Windows Server 2022	2024 年 2 月 13 日 - KB5034768 以降の累積的な更新プログラム 2021 年 6 月 8 日 - KB5003646 以降の累積的な更新プログラム

KMS ホストの OS バージョン	ライセンス認証する KMS クライアントの OS バージョン	必須の更新
Windows Server 2016	- Windows Server 2022 - Windows Server 2019	2021 年 6 月 8 日 - KB5003638 以降の累積的な更新プログラム
Windows Server 2016	- Windows Server 2019	2018 年 12 月 3 日 - KB4478877 以降の累積的な更新プログラム
Windows Server 2012 R2	- Windows Server 2019 - Windows Server 2016 - Windows 10	2018 年 11 月 27 日 - KB4467695 (マンスリー ロールアップのプレビュー) 以降のマンスリー ロールアップ
Windows Server 2012 R2	- Windows Server 2016 - Windows 10	Windows 8.1 および Windows Server 2012 R2 の 2016 年 7 月更新プログラムのロールアップ またはそれ以降のマンスリー ロールアップ
Windows Server 2012	- Windows Server 2016 - Windows Server 2012 R2 - Windows 10	Windows Server 2012 の 2016 年 7 月更新プログラムのロールアップ またはそれ以降のマンスリー ロールアップ
Windows Server 2008 R2	- Windows Server 2012 R2 - Windows Server 2012 - Windows 10	Windows 7 と Windows Server 2008 R2 KMS のホストで Windows 10 のライセンス認証を可能にするための更新プログラム
Windows 8.1	- Windows 10	Windows 8.1 および Windows Server 2012 R2 の 2016 年 7 月更新プログラムのロールアップ またはそれ以降のマンスリー ロールアップ
Windows 7	- Windows 10	Windows 7 と Windows Server 2008 R2 KMS のホストで Windows 10 のライセンス認証を可能にするための更新プログラム

キー管理サービス (KMS) ライセンス認証ホストを作成する

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

キー管理サービス (KMS) は、クライアント/サーバー モデルを使用して Windows クライアントをアクティブ化します。 KMS は、ローカル ネットワークでのボリュームライセンス認証に使用されます。 KMS クライアントは、ライセンス認証を行うために、KMS ホストと呼ばれる KMS サーバーに接続します。 KMS ホストからライセンス認証できる KMS クライアントは、KMS ホストのライセンス認証に使用されたホスト キーによって変わります。

この記事では、KMS ホストを作成するために必要な手順について説明します。 KMS と初期計画に関する考慮事項の詳細については、「 キー管理サービス (KMS) ライセンス認証計画」を参照してください。

Prerequisites

1 つの KMS ホストで無制限の数の KMS クライアントをサポートできます。 50 台を超えるクライアントがある場合は、KMS ホストが使用できなくなった場合に備えて 2 台以上の KMS ホストを用意することをお勧めします。 ほとんどの組織では、2 つの KMS ホストでインフラストラクチャ全体をサポートできます。

KMS ホストは専用サーバーである必要はありません。 KMS ホストで他のサービスをホストできます。 サポートされている Windows Server または Windows クライアント オペレーティング システムを実行する任意の物理システムまたは仮想システムで KMS ホストを実行できます。

KMS ホストに使用する Windows のバージョンによって、KMS クライアントに対してライセンス認証できる Windows のバージョンが決まります。 環境に適したバージョンの決定については、 ライセンス認証バージョンの表を参照してください。

既定では、KMS ホストはドメイン ネーム システム (DNS) でサービス (SRV) リソース レコードを発行します。 その結果、KMS クライアントは KMS ホストを自動的に検出し、KMS クライアントで構成を行わなくてもアクティブ化できます。 自動発行を無効にし、レコードを手動で作成できます。 DNS サービスが動的更新をサポートしていない場合は、自動アクティブ化にこれらの手順が必要です。

KMS ホストを作成するには、次の前提条件が必要です。

- Windows Server または Windows を実行しているコンピューター。 Windows Server で実行されている KMS ホストは、サーバーとクライアントの両方のオペレーティング システムを実行しているコンピューターをアクティブ化できます。 ただし、Windows クライアント オペレーティング システムで実行されている KMS ホストは、クライアント オペレーティング システムを実行しているコンピューターのみをアクティブ化できます。
- KMS ホストの Administrators グループのメンバーであるユーザー アカウント。
- 相互に互換性のある KMS とクライアントのバージョン、および KMS をホストできる Windows バージョン。 詳細については、「 キー管理サービス (KMS) ライセンス認証計画」を参照してください。
- 組織の KMS ホスト キー。 このキーは、Microsoft 365 管理センターから取得できます。 詳細については、「 ボリューム ライセンスのプロダクト キーを検索して使用する」を参照してください。
- KMS ホストをアクティブ化したり、電話によるライセンス認証を実行したりするためのインターネットへのアクセス。

KMS ホストのインストールと構成

KMS ホストをインストールして構成するには、次のセクションの手順を実行します。

ボリューム ライセンス認証サービスの役割をインストールする

ボリューム ライセンス認証サービスの役割をインストールするには、管理者特権の PowerShell セッションで次のコマンドを実行します。

PowerShell

```
Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
```

Windows ファイアウォールの構成

KMS がネットワーク トラフィックを受信できるように Windows ファイアウォールを構成します。 このトラフィックは、既定の設定である任意のネットワーク プロファイル、またはドメイン、プライベート、パブリックのネットワーク プロファイルの任意の組み合わせに対して許可できます。 既定では、KMS ホストは、ポート 1688 で伝送制御プロトコル (TCP) を使用するように構成されています。

ドメインとプライベートのネットワーク プロファイルに対してのみネットワーク トラフィックを許可するようにファイアウォール規則を構成するには、次のコマンドを実行します。

PowerShell

```
Set-NetFirewallRule -Name SPPSVC-In-TCP -Profile Domain,Private -Enabled True
```

ボリューム ライセンス認証ツール ウィザードを使用してホストを構成する

1. 次のコマンドを実行して、ボリューム ライセンス認証ツール ウィザードを開きます。

   ```
   PowerShell

   vmw.exe
   ```

2. 概要ページで、[**次へ**] を選択します。

3. アクティブ化の種類として、 **キー管理サービス** (KMS) を選択します。 サーバーの場合は、「 **localhost」と** 入力してローカル サーバーを構成します。 別のサーバーを構成する場合は、そのホスト名を入力します。 [**次へ**] を選択します。

4. [KMS **ホスト キーのインストール**] を選択し、組織のプロダクト キーを入力して、[コミット] を選択 **します**。

5. プロダクト キーがインストールされたら、[**次へ**] を選択して製品をアクティブ化します。

6. [**製品の選択**] で、アクティブ化する製品を選択し、アクティブ化方法を選択します。 キーをオンラインでアクティブ化するには、[**オンラインでアクティブ化**] を選択し、[コミット] を選択 **します**。 KMS ホストのアクティブ化を確認するメッセージが表示されたら、[**はい**] を選択します。

構成を完了する

ライセンス認証が正常に完了すると、KMS ホスト構成が表示されます。

- 構成設定が要件を満たしている場合:

  1. [**閉じる**] を選択してウィザードを終了します。 システムによって DNS レコードが作成され、 KMS クライアントのアクティブ化を開始できます。
  2. KMS ホストを発行するために SRV レコードを手動で作成する必要がある場合は、この記事で後述する 「DNS レコードを手動で作成 する」を参照してください。

- 構成設定を変更する場合:

  1. [**次へ**] を選択します。

2. 要件に基づいて構成値を変更し、[**コミット**] を選択します。

> ⓘ **注意**
>
> **これで、KMS クライアントのアクティブ化を**開始できます。 ただし、ネットワークには、最初にコンピューターの最小数 (ライセンス認証のしきい値と呼ばれます) が必要です。 KMS ホストは、最近の接続の数を追跡します。 クライアントまたはサーバーが KMS ホストに接続すると、ホストはマシン ID をメモし、連絡先の数をインクリメントしてから、応答で現在の数を返します。 クライアントまたはサーバーは、数が十分に多い場合にアクティブ化されます。
>
> - 数が 25 以上の場合、Windows クライアントがアクティブになります。
> - 数が 5 つ以上の場合、Microsoft Office 製品の Windows Server エディションとボリューム エディションがアクティブになります。
>
> このカウントでは、KMS には過去 30 日間の一意の接続のみが含まれており、最新の 50 件の連絡先のみが格納されます。

DNS レコードを手動で作成する

DNS サービスで動的更新がサポートされていない場合は、KMS ホストを発行するためにリソース レコードを手動で作成する必要があります。 次の情報を使用して、DNS サービスで KMS の DNS リソース レコードを手動で作成します。 KMS ホスト構成で既定のポート番号を変更する場合は、リソース レコードに使用するポート番号も調整します。

テーブルを展開する

Property	Value
タイプ	SRV
Service/Name	_vlmcs
Protocol	_tcp
Priority	0
Weight	0
ポート番号	1688
Hostname	<FQDN-of-KMS-host>

また、DNS サービスが動的更新をサポートしていない場合は、すべての KMS ホストでの発行を無効にする必要があります。 手順については、この記事 で後述する「DNS レコードの発行を無効にする 」を参照してください。 発行を無効にすると、失敗した DNS 発行イベントをイベント ログで収集できなくなります。

> **ヒント**
>
> 手動で作成したリソース レコードは、すべてのレコードが競合を防ぐように保守されている限り、他のドメイン内で KMS ホストから自動的に発行されるリソース レコードと共存することができます。

DNS レコードの発行を無効にする

KMS ホストによる DNS レコードの発行を無効にするには:

1. 次のコマンドを実行して、ボリューム ライセンス認証ツール ウィザードを開きます。

   PowerShell

   ```
   vmw.exe
   ```

2. 概要ページで、[**次へ**] を選択します。

3. アクティブ化の種類として、 **キー管理サービス (KMS)** を選択します。 サーバーの場合は、「 **localhost」と** 入力してローカル サーバーを構成します。 別のサーバーを構成する場合は、そのホスト名を入力します。 [**次へ**] を選択します。

4. [**構成にスキップ**] を選択し、[**次へ**] を選択します。

5. [**DNS レコード**] の横にある [**発行**] チェック ボックスをオフにして、[**コミット**] を選択します。

KMS ホストを置き換える

2025/07/30

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

この記事では、キー管理サービス (KMS) ホスト ロールを新しいサーバーに移行するための手順とベスト プラクティスについて説明します。 多くの場合、KMS ホストの移行は、既存のホストのオペレーティング システム (OS) がサポート終了に近づいているときに必要になります。 また、役割を別のサーバーに移動することを義務付ける運用または組織の変更が原因で必要になる場合もあります。 このガイドの手順では、Microsoft Windows および Microsoft Office クライアントのアクティブ化サービスを中断せずに維持しながら、シームレスな移行プロセスを提供します。 KMS ホストはデータベースやバックアップに依存しないため、このプロセス中にデータを移行する必要はありません。

インストールとライセンスのタスクに進む前に、新しい KMS ホストに関する次の詳細を確認してください。

- 新しい顧客固有ボリューム ライセンス キー (CSVLK) にアクセスできることを確認します。 CSVLK は、Microsoft 365 管理センターを通じて取得される Microsoft Windows OS および Microsoft Office の **KMS ホスト キー** とも呼ばれます。 CSVLK には、事前に定義されたアクティブ化制限があります。 ライセンス認証の制限を超えたことを示すエラーが発生した場合は、要求ごとにキーをリセットできます。 詳細については、「 ボリューム ライセンスのプロダクト キーを検索して使用する」を参照してください。
- CSVLK が見つからない場合は、ライセンス サポートにお問い合わせください 。

Prerequisites

- **ボリューム ライセンス認証サービス**の役割は、新しい KMS ホストとして機能するデバイスにインストールする必要があります。 詳細については、「役割、役割サービス、または機能 をインストールまたはアンインストールするを参照してください。

  または、次の PowerShell コマンドを実行できます。

  ```
  PowerShell
  Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
  ```

- 次のグループのメンバーである必要があります。
  - Administrators
  - ドメイン管理者

    - エンタープライズ管理者

- CSVLK は有効であり、組織のライセンス ポータルまたは Microsoft 365 管理センターからアクセスできる必要があります。 次のように、アクティブ化する製品に適切な CSVLK があることを確認します。
    - Microsoft Windows OS CSVLK
    - Microsoft Office CSVLK

- デバイスを KMS ホストとして構成する前に、OS に最新の Windows 更新プログラムがインストールされている必要があります。 詳細については、 KMS ホストに必要な更新プログラムに関するページを参照してください。

既存の KMS ホストを確認する

新しい KMS ホストに移行する前に、既存のすべての KMS ホストを識別するように環境のインベントリを作成することをお勧めします。 これにより、承認されていない、または不要な KMS ホストが存在しないことを確認できます。 CSVLK を使用して KMS ホストとして機能しないデバイスをアクティブ化した場合、未承認の KMS ホストが表示されることがあります。 承認されたサーバーのみを CSVLK でアクティブ化し、KMS ホストとして構成する必要があります。 これらのアクションの実行は、管理者特権のコマンド プロンプトまたは PowerShell ウィンドウで実行できます。

KMS ホストを取得する

コマンド プロンプト

ドメイン ネーム システム (DNS) によって KMS ホストを取得するには、次のコマンドを実行します。

Windows コマンド プロンプト

```
nslookup -type=srv _vlmcs._tcp
```

完全修飾ドメイン名 (FQDN) によって KMS ホストを取得するには、次のコマンドを実行します。

Windows コマンド プロンプト

```
nslookup -type=SRV _vlmcs._tcp.mydomain.com
```

特定の DNS サーバー (8.8.8.8 など) によって KMS ホストを取得するには、次のコマンドを実行します。

Windows コマンド プロンプト

```
nslookup -type=SRV _vlmcs._tcp.mydomain.com 8.8.8.8
```

承認されていない KMS ホストを検出した場合は、管理者特権のウィンドウで次のコマンドを実行して KMS クライアントに戻し、デバイスを再起動できます。 汎用ボリューム ライセンス キー (GVLK) を自分のGVLKに置き換えます。

```
slmgr.vbs /ipk <GVLK>
```

KMS ホスト製品のライセンス認証を確認する

現在の KMS ホストがアクティブ化している製品を確認し、新しい KMS ホストが同じ Windows OS と Microsoft Office クライアントをアクティブ化していることを確認するには、次のコマンドを実行します。

Windows コマンド プロンプト

```
cscript %windir%\system32\slmgr.vbs /dlv All
```

PowerShell

```
cscript $env:windir\system32\slmgr.vbs /dlv All
```

出力を確認して、KMS ホストが Windows OS、Microsoft Office、またはその両方のライセンス認証要求を処理しているかどうかを確認します。 表示される部分的なプロダクト キーは、これらの KMS ホスト キー (CSVLK) をレコードと照合するのに役立ちます。 さらに、 KMS ホスト イベント ログ を確認して、この KMS ホストにアクティブ化要求を送信しているクライアントを特定します。

KMS ホストを準備する

KMS ホストとして環境を構成する前に、新しいサーバーにターゲット OS をクリーン インストールします。 Windows Server OS をインストールする方法については、「 インストール メディアから Windows Server をインストールする」を参照してください。 使用可能なすべての

OS 更新プログラムとセキュリティ パッチが適用されていることを確認し、必要に応じて再起動します。 KMS ホストを設定するには、2 つのオプションがあります。

Windows OS KMS ホスト

ホスト OS を準備した後、次の手順では、KMS ホストとして機能するように構成します。 「キー管理サービス (KMS) ライセンス認証ホストの作成」を参照してください。

ファイアウォール設定を確認する

KMS ホストを管理する方法に進む前に、KMS クライアントからのアクティブ化要求を受け入れるようにファイアウォール例外がポート **1688** 用に構成されていることを確認します。 さらに、ポート **135** (匿名 RPC) も構成する必要があります。

GUI

1. **[スタート] を**選択し、「wf.msc」と入力して選択し、**セキュリティが強化された Windows Defender ファイアウォールを開きます**。
2. 左側のウィンドウで、[**受信規則**] を選択します。
3. 右側のウィンドウで、[**新しい規則**] を選択して、 **新しい受信規則ウィザード**を開きます。
4. [**ルールの種類] で** [**ポート**] を選択し、[**次へ**] を選択します。
5. [**プロトコルとポート**] で [TCP] を選択し、[**特定のローカル ポート**] フィールドに「**1688**」と入力し、[**次へ**] を選択します。
6. [**アクション**] で、[**接続を許可する**] が選択されていることを確認し、[**次へ**] を選択します。
7. [**プロファイル**]、[**ドメイン**]、[**プライベート**]、[**パブリック**] が既定で選択されています。 [**次へ**] を選択します。
8. [**名前**] で、ルールに必要な名前 ("KMS ホスト" など) を指定し、[**完了**] を選択します。

ポート **135** を構成するには、次の手順を繰り返します。

ポート **1688** または **135** を介してトラフィックが許可されていることを確認するには、**ComputerName** の値がデバイス名または IP アドレスである次のコマンドを実行します。

PowerShell

```
Test-NetConnection -ComputerName "MyDevice" -Port 1688
```

接続が成功すると、 **TcpTestSucceededed** エントリは **True** になりますが、ポート 1688 への接続を確立できない場合 (たとえば、サービスがリッスンしていない場合、またはファイアウォールやネットワークの問題が原因である場合) は 、**TcpTestSucceeded はFalse** になります。

KMS ホストを登録する

Windows OS および Microsoft Office 用に KMS ホストを構成した後、ドメインのアクセス許可が許可されている場合は、自動的に DNS に登録される場合があります。 手動登録が必要な場合は、「 DNS レコードを手動で作成する」の手順に従います。

新しい KMS ホストを DNS に登録した後、古い KMS ホストを DNS から削除できます。 クライアント デバイスは、新しい KMS ホストへのアクティブ化要求の送信を開始しますが、アクティブ化数が必要な最小しきい値に達するまでに時間がかかる場合があります。

> ⚠ **注意**
>
> - **KMS Count クライアント ライセンス認証しきい値**: KMS では、クライアント OS のアクティブ化を開始するために、クライアントまたはサーバー OS からの少なくとも **25** 個の一意のライセンス認証要求が必要です。
> - **KMS カウント サーバーのライセンス認証しきい値**: KMS では、サーバー OS のアクティブ化を開始するために、サーバーまたはクライアント OS から少なくとも **5** つの一意のライセンス認証要求が必要です。

移行が成功したことを確認するには、新しい KMS ホスト (イベント ビューアー>>) の**イベント** ログを確認します。 次のコマンドを実行し、出力を確認することもできます。

```
slmgr.vbs /dlv
```

クライアント デバイスがアクティブ化要求を新しいホストに送信すると、古い KMS ホストを DNS から安全に削除できます。

> ⚠ **注意**
>
> - KMS ホスト機能を古い KMS ホストから削除するには、GVLK をインストールしてデバイスを再起動します。
> - ベスト プラクティスは、クライアント デバイスが新しい KMS ホストに確実に移行されるように、古い KMS ホストを完全にシャットダウンすることです。

- `slmgr.vbs /skms` を使用してデバイスが特定の KMS ホスト用に構成されている場合、 `slmgr.vbs /ckms` を実行すると、その構成がクリアされ、デバイスは新しい KMS ホストを自動的に検出できます。

KMS ライセンス認証のトラブルシューティング

これらのアクションの実行は、管理者特権のコマンド プロンプトまたは PowerShell ウィンドウで行う必要があります。 その他の問題をさらにトラブルシューティングするには、 キー管理サービス (KMS) のトラブルシューティングに関するガイドラインを参照してください。

こちらも参照ください

- キー管理サービス (KMS) のアクティブ化計画
- ボリューム ライセンス認証情報を取得するための Slmgr.vbs オプション

KMS クライアントのアクティブ化とプロダクト キー

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

キー管理サービス (KMS) を使用するには、ローカル ネットワークで使用可能な KMS ホストが必要です。 KMS ホストでライセンス認証されるコンピューターには、特定のプロダクト キーが必要です。 このキーは、KMS クライアント キーと呼ばれる場合がありますが、正式には Microsoft Generic Volume License Key (GVLK) と呼ばれます。 Windows Server および Windows クライアントのボリューム ライセンス エディションが実行されているコンピューターは、既定では、追加の構成が必要ない (関連する GVLK が既に存在するため) KMS クライアントです。

KMS ホストに対してアクティブ化するコンピューターに GVLK を追加する必要があるシナリオがいくつかあります。次に例を示します。

- コンピューターをマルチ ライセンス認証キー (MAK) の使用から変換する
- Windows の製品版ライセンスを KMS クライアントに変換する
- コンピューターが以前に KMS ホストであった場合

一覧表示されている GVLK を使用するには、ローカル ネットワーク上に KMS ホストが必要です。 ない場合は、 KMS ホストを作成する方法を学習できます。

KMS ホストでは、Microsoft でライセンス認証または認証を行うために、KMS ホスト キーと呼ばれる独自のキーが必要です。 このキーは、 Microsoft 365 管理センター で、Open、Open Value、Select、Enterprise、Services Provider License 契約で使用できます。 ローカルの Microsoft ライセンス認証センター からヘルプを受けることができます。

> **⊗ 注意事項**
>
> KMS ホストを使用して Windows または Windows Server をアクティブ化する場合、ここで提供されるキーはボリューム ライセンス シナリオを対象としており、リテール エディションでは **使用できません** 。 KMS クライアント キー **は、ライセンス認証も** 、リテール ライセンス キーとしても機能しません。 Windows のリテール 版のコピーをインストールした場合は、MAK などの別のライセンス認証方法を使用するか、正規のリテール ライセンスを購入する必要があります。 詳細については、以下をご覧ください。
>
> - **Windows を有効化する** 。
> - **Windows Server の価格とライセンス** 。

プロダクト キーのインストール

コンピューターを KMS ホスト、MAK、または製品版の Windows から KMS クライアントに変換する場合は、この記事の一覧から該当するプロダクト キー (GVLK) をインストールしてください。 クライアントプロダクト キーをインストールするには、クライアントで管理コマンド プロンプトを開き、次のコマンドを実行して **Enter キー**を押します。

Windows コマンド プロンプト

```
slmgr /ipk <product key>
```

たとえば、Windows Server 2022 Datacenter Edition のプロダクト キーをインストールするには、次のコマンドを実行して **Enter キー**を押します。

Windows コマンド プロンプト

```
slmgr /ipk WX4NM-KYWYW-QJJR4-XV3QB-6VM33
```

汎用ボリューム ライセンス キー

次の一覧に、Windows の各バージョンおよびエディションの GVLK を示します。 LTSC は "長期サービス チャネル"、LTSB は *Long-Term Servicing Branch* を意味します。

Windows 11 と Windows 10 半期チャネル

サポートされているバージョンとサービス終了日の情報については、「Windows ライフサイクルのファクト シート」をご覧ください。

テーブルを展開する

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows 11 Pro Windows 10 Pro	W269N-WFGWX-YVC9B-4J6C9-T83GX
Windows 11 Pro N Windows 10 Pro N	MH37W-N47XK-V7XM9-C7227-GCQG9
Windows 11 Pro ワークステーション向け Windows 10 Pro for Workstations (ワークステーション用)	NRG8B-VKK3Q-CXVCJ-9G2XF-6Q84J
Windows 11 Pro for Workstations N Windows 10 Pro for Workstations N	9FNHH-K3HBT-3W4TD-6383H-6XYWF

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows 11 Pro Education Windows 10 Pro Education	6TP4R-GNPTD-KYYHQ-7B7DP-J447Y
Windows 11 Pro Education N Windows 10 Pro Education N	YVWGF-BXNMC-HTQYQ-CPQ99-66QFC
Windows 11 Education Windows 10 Education	NW6C2-QMPVW-D7KKK-3GKT6-VCFB2
Windows 11 Education N Windows 10 Education N	2WH4N-8QGBV-H22JP-CT43Q-MDWWJ
Windows 11 Enterprise Windows 10 Enterprise	NPPR9-FWDCX-D2C8J-H872K-2YT43
Windows 11 Enterprise N Windows 10 Enterprise N	DPH2V-TTNVB-4X9Q3-TJR4H-KHJW4
Windows 11 Enterprise G Windows 10 Enterprise G	YYVX9-NTFWV-6MDM3-9PT4T-4M68B
Windows 11 Enterprise G N Windows 10 Enterprise G N	44RPN-FTY23-9VTTB-MP9BX-T84FV

Windows Enterprise LTSC および LTSB

Windows 11 LTSC 2024
Windows 10 LTSC 2021、2019

テーブルを展開する

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows 11 Enterprise LTSC 2024 Windows 10 Enterprise LTSC 2021 Windows 10 Enterprise LTSC 2019	M7XTQ-FN8P6-TTKYV-9D4CC-J462D
Windows 11 Enterprise N LTSC 2024 Windows 10 Enterprise N LTSC 2021 Windows 10 Enterprise N LTSC 2019	92NFX-8DJQP-P6BBQ-THF9C-7CG2H

以前のバージョンの Windows クライアント

Windows 8.1

テーブルを展開する

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows 8.1 Pro	GCRJD-8NW9H-F2CDX-CCM8D-9D6T9
Windows 8.1 Pro N	HMCNV-VVBFX-7HMBH-CTY9B-B4FXY
Windows 8.1 Enterprise	MHF9N-XY6XB-WVXMC-BTDCT-MKKG7
Windows 8.1 Enterprise N	TT4HM-HN7YT-62K67-RGRQJ-JFFXW

Windows Server LTSC

Windows Server 2025

テーブルを展開する

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows Server 2025 Standard	TVRH6-WHNXV-R9WG3-9XRFY-MY832
Windows Server 2025 Datacenter	D764K-2NDRG-47T6Q-P8T8W-YP6DF
Windows Server 2025 Datacenter: Azure Edition	XGN3F-F394H-FD2MY-PP6FD-8MCRC

Windows Server 半期チャネル

Windows Server バージョン 20H2、2004、1909、1903、1809

テーブルを展開する

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows Server Standard	N2KJX-J94YW-TQVFB-DG9YT-724CC
Windows Server Datacenter	6NMRW-2C8FM-D24W7-TQWMY-CWH2D

> **ⓘ 重要**
>
> Windows Server バージョン 20H2 は、2022 年 8 月 9 日にサービスが終了し、セキュリティ更新プログラムを受信しなくなりました。 これには、今後のリリースがない Windows Server 半期チャネル (SAC) の廃止が含まれます。
>
> Windows Server SAC を使用しているお客様は Azure Stack HCI に移行する必要があります。 または、お客様は Windows Server の Long-Term サービス チャネルを使用できます。

旧バージョンの Windows Server

Windows Server、バージョン 1803

テーブルを展開する

オペレーティング システムのエディション	KMS クライアント プロダクト キー
Windows Server Standard	PTXN8-JFHJM-4WC78-MPCBR-9W4KR
Windows Server Datacenter	2HXDN-KRXHB-GPYC7-YCKFJ-7FVDG

Windows ボリュームアクティベーションのトラブルシューティング

2025/05/07

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

製品のライセンス認証は、特定のコンピューターにインストールされたソフトウェアを検証するプロセスです。 ライセンス認証は、製品が正規のもの (不正なコピーではない) であること、およびプロダクト キーまたはシリアル番号が有効であり、侵害または取り消されていないことを確認します。 アクティベーションにより、プロダクトキーとインストールの間にリンクまたは関係が確立されます。

ボリューム ライセンス認証は、ボリューム ライセンス製品をアクティブ化するプロセスです。 ボリューム ライセンスのお客様になるには、組織が Microsoft とのボリューム ライセンス契約を設定する必要があります。 Microsoft では、組織のサイズと購入の好みに合わせてカスタマイズされたボリューム ライセンス プログラムを提供しています。 詳細については、Microsoft ボリューム ライセンス サービス センターを参照してください。

Windows Server 2016 ライセンス認証ガイドでは、キー管理サービス (KMS) ライセンス認証テクノロジに重点を置いています。 このセクションでは、一般的な問題に対処し、KMS とその他のいくつかのボリューム ライセンス認証テクノロジのトラブルシューティング ガイドラインを示します。

ボリューム ライセンス認証のベスト プラクティス

次の記事では、Microsoft のボリューム ライセンス認証テクノロジの技術情報とベスト プラクティスについて説明します。

キー管理サービス (KMS)

- ボリューム ライセンス認証の計画
- KMS について
- KMS ライセンス認証の展開
- KMS ホストの構成
- DNS の構成
- キー管理サービスを使用してアクティブ化する

Active Directory ベースのアクティブ化 (ADBA)

- Active Directory に基づくライセンス認証の展開
- Active Directory によるアクティブ化を使用したアクティブ化
- Active Directory-Based の有効化概要

マルチ ライセンス認証キー (MAK) ライセンス認証

- MAK ライセンス認証の使用
- MAK ライセンス認証について
- MAK クライアントのアクティブ化

サブスクリプションの有効化

- Windows 10 サブスクリプションのアクティブ化
- Windows 10 Enterprise ライセンスを展開する
- CSP での Windows 10 Enterprise E3

アクティブ化に関する問題のトラブルシューティングに関するリソース

次の記事では、ボリューム ライセンス認証の問題をトラブルシューティングするためのガイドラインとツールに関する情報を提供します。

- キー管理サービス (KMS) のトラブルシューティングに関するガイドライン
- ボリューム ライセンス認証情報を取得するための Slmgr.vbs オプション
- 例: アクティブ化されない ADBA クライアントのトラブルシューティング

次の記事では、より具体的なアクティブ化の問題に対処するためのガイダンスを提供します。

- 一般的なアクティブ化エラー コードの解決
- KMS ライセンス認証: 既知の問題
- MAK ライセンス認証: 既知の問題
- DNS に関連するライセンス認証の問題のトラブルシューティングに関するガイドライン
- Tokens.dat ファイルを再構築する方法

キー管理サービス (KMS) のトラブルシューティングに関するガイドライン

2025/09/15

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

エンタープライズのお客様は、デプロイ プロセスの一部として Key Management Service (KMS) を設定します。これは、単純で簡単なプロセスを使用して、環境で Windows をアクティブ化できるためです。 通常、KMS ホストを設定すると、KMS クライアントは自動的にホストに接続し、独自にアクティブ化します。 ただし、プロセスが期待どおりに動作しない場合があります。 この記事では、発生する可能性がある問題をトラブルシューティングする方法について説明します。

イベント ログ エントリと `slmgr.vbs` スクリプトの詳細については、「ボリューム ライセンス認証テクニカル リファレンス」を参照してください。

KMS のトラブルシューティングを開始する場所

KMS ライセンス認証のしくみを簡単におさらいしてみましょう。 KMS は、動的ホスト構成プロトコル (DHCP) といくつかの類似点を持つクライアント サーバー モデルです。 ただし、KMS では、要求に応じてクライアントに IP アドレスを渡す代わりに、製品のライセンス認証を有効にします。 KMS は更新モデルでもあり、クライアントは定期的に再アクティブ化を試みます。 *KMS* ホストと *KMS* クライアントの 2 つのロールがあります。

- KMS ホストはアクティブ化サービスを実行し、環境内でアクティブ化を有効にします。 KMS ホストを構成するには、ボリューム ライセンス サービス センター (VLSC) から KMS キーをインストールし、サービスをアクティブ化する必要があります。
- KMS クライアントは、環境に展開し、アクティブ化する必要がある Windows オペレーティング システム (OS) です。 KMS クライアントは、ボリューム ライセンス認証を使用する任意のエディションの Windows を実行できます。 KMS クライアントには、 汎用ボリューム ライセンス キー *(GVLK)* または *KMS* クライアント セットアップ キーと呼ばれるプレインストールキーが付属しています。 GVLK の存在は、システムを KMS クライアントにします。 KMS クライアントは、ドメイン ネーム システム (DNS) SRV レコード (`_vlmcs._tcp`) を使用して KMS ホストを識別します。 次に、クライアントは自動的にこのサービスを検出して使用してアクティブ化しようとします。 既定では 30 日間の猶予期間中は、2 時間ごとにライセンス認証が試行されます。 KMS クライアントをアクティブ化した後、7 日ごとにライセンス認証を更新しようとします。

トラブルシューティングの観点から、問題が発生している理由を把握するために、ホスト側とクライアント側の両方を確認する必要がある場合があります。

KMS ホストでのトラブルシューティング

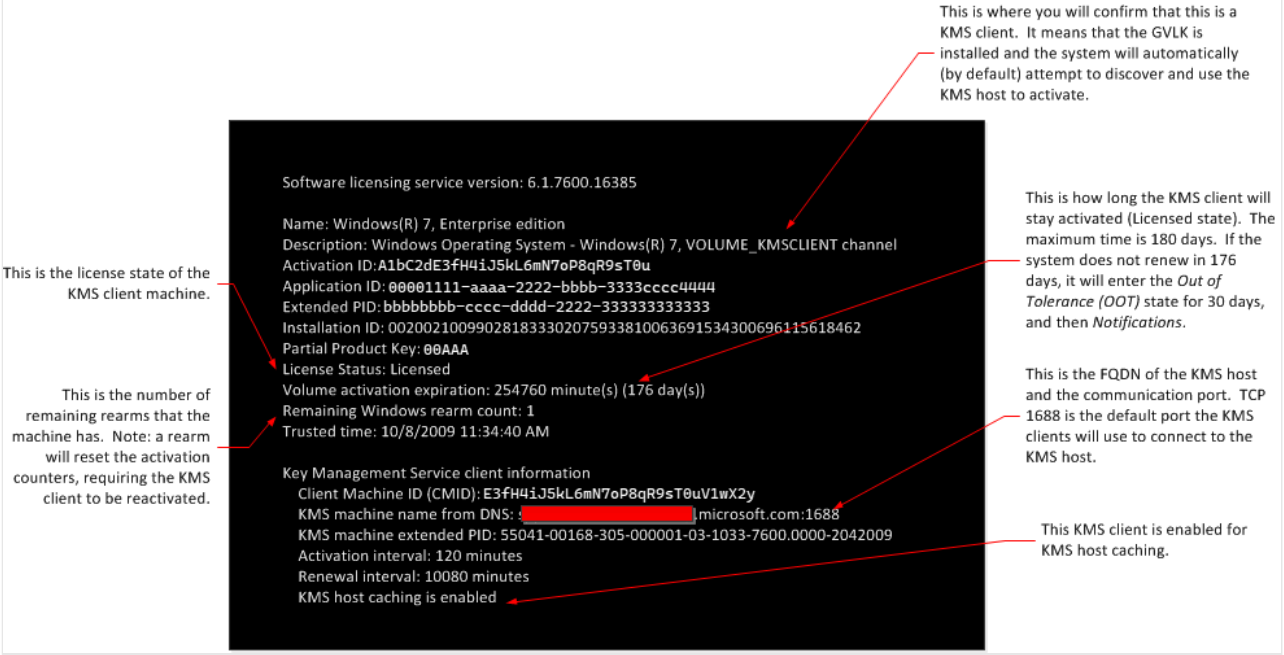
トラブルシューティング中に KMS ホストを調べるときは、次の 2 つの領域を確認する必要があります。

- コマンド ライン プロンプトで `slmgr.vbs` コマンドを使用して、ホスト ソフトウェア ライセンス サービスの状態を確認します。
- イベント ビューアーで、ライセンスまたはライセンス認証に関連するイベントを確認します。

Slmgr.vbs とソフトウェア ライセンス サービス

`slmgr.vbs` コマンド ライン ツールとイベント ビューアーを使用して、KMS クライアントでのアクティブ化の問題のトラブルシューティングを行うことができます。 ソフトウェア ライセンス サービスからの詳細な出力を表示するには、管理者特権のコマンド プロンプト ウィンドウまたは PowerShell ウィンドウを開き、 `slmgr.vbs /dlv`実行します。 次のスクリーンショットは、KMS クライアントと KMS ホストに対するこのコマンドの結果をそれぞれ示しています。

KMS クライアント



トラブルシューティング中に出力で注意する必要がある変数を次に示します。

- バージョン情報は、`slmgr.vbs /dlv`出力の先頭にあります。 バージョン情報は、サービスが -date up-toかどうかを判断するのに役立ちます。 KMS サービスではさまざまな KMS ホスト キーがサポートされるため、すべてが最新であることを確認することが重要です。 このデータを使用して、現在使用しているバージョンがインス

トールしようとしている KMS ホスト キーをサポートしているかどうかを評価できます。 更新プログラムの詳細については、「 Windows Vista および Windows Server 2008 で Windows 7 および Windows Server 2008 R2 の KMS ライセンス認証のサポートを拡張するための更新プログラムを使用できる」を参照してください。

- 名前は、KMS ホスト システムで実行されている Windows のエディションを示 します 。 この情報を使用して、KMS ホスト キーの追加または変更に関する問題のトラブルシューティングを行うことができます。 たとえば、この情報を使用して、使用しようとしているキーが OS エディションでサポートされているかどうかを確認できます。

- *[説明]* には、現在インストールされているキーが表示されます。 このフィールドを使用して、最初にサービスをアクティブ化したキーが、デプロイした KMS クライアントの正しいキーであるかどうかを確認します。

- ライセンスの状態には、KMS ホスト システムの状態が表示されます。 値は **Licensed** である必要があります。 その他の値は、ホストを再アクティブ化する必要があることを意味します。

- 現在のカウントには、**0 から 50** までの数が表示されます。 この数は OS 間の累積であり、 **30 日以内** にアクティブ化を試みた有効なシステムの数を示します。

  カウントが **0** の場合、サービスが最近アクティブ化されたか、有効なクライアントが KMS ホストに接続されていません。

  この数は、環境内に有効なシステムの数に関係なく、 **50** を超えて増加することはありません。 カウントは、KMS クライアントによって返される最大ライセンス ポリシーの 2 倍のみをキャッシュするように設定されます。 Windows クライアント OS によって設定される最大ポリシーでは、それ自体をアクティブ化するために KMS ホストから **25** 以上の数が必要です。 そのため、KMS ホストで使用できる最大カウントは **、50** または 2 x 25 です。 Windows Server KMS クライアントのみを含む環境では、KMS ホストの最大数は **10 です**。 この制限は、Windows Server エディションのしきい値が **5** (2 x 5 または 10) であるためです。

  この数に関連する一般的な問題は、環境にアクティブ化された KMS ホストと十分なクライアントがあるが、カウントが 1 を超えて増加しない場合に発生します。 この問題が発生した場合は、デプロイされたクライアント イメージが正しく構成されていないため、システムに一意のクライアント マシン ID (CMID) が設定されていないことを意味します。 詳細については、次の記事を参照してください。

  - 新しい Windows Vista または Windows 7 ベースのクライアント コンピューターをネットワークに追加しても、KMS の現在の数は増加しません。

- KMS ホスト クライアントの数は、CMID が重複しているために増加しません。

  カウントが増加しないもう 1 つの理由は、環境内に KMS ホストが多すぎて、その数がそれらのすべてに分散されることです。

- **ポートでリッスンしています**。 KMS との通信では、匿名 RPC が使用されます。 既定では、クライアントは 1688 TCP ポートを使用して KMS ホストに接続します。 このポートが KMS クライアントと KMS ホストの間で開いていることを確認します。 KMS ホストでポートを変更または構成できます。 KMS ホストは、通信中に、KMS クライアントにポートの指定を送信します。 KMS クライアントでポートを変更すると、そのクライアントがホストに接続したときにポートの指定が上書きされます。

多くの場合、出力の`slmgr.vbs /dlv`セクションについて質問されます。 一般に、このデータはトラブルシューティングには役立ちません。 KMS ホストは、アクティブ化または再アクティブ化を試みる各 KMS クライアントの状態の継続的な記録を保持します。 失敗した要求は、KMS ホストが特定の KMS クライアントをサポートしていないことを示します。 たとえば、Windows 7 KMS クライアントが Windows Vista KMS キーを使用してアクティブ化された KMS ホストに対してアクティブ化しようとすると、ライセンス認証は失敗します。

[ライセンスステータスの要求] 行には、過去と現在の両方の使用可能なすべてのライセンス状態が記載されています。 トラブルシューティングの観点からは、このデータは、カウントが予想どおりに増加していない場合にのみ関連します。 その場合、失敗した要求の数が増加していることがわかります。 この問題を解決するには、最初に KMS ホスト システムをアクティブ化するために使用されたプロダクト キーを確認する必要があります。 また、累積要求値は、KMS ホスト システムを再インストールした場合にのみリセットされることに注意してください。

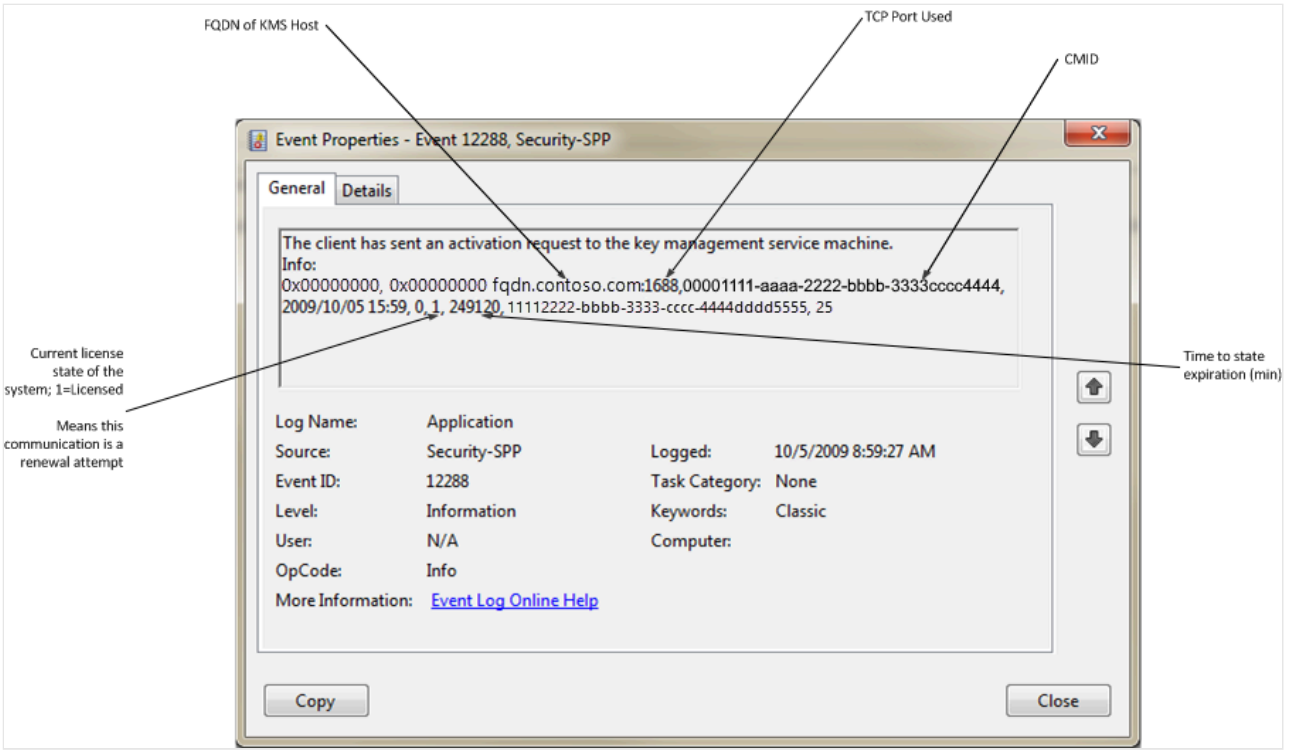
KMS イベント ID

以下のセクションでは、潜在的な問題をより効率的にトラブルシューティングするために理解しておく必要があるクライアント イベントについて説明します。 KMS クライアントが正常にアクティブ化または再アクティブ化されると、クライアントはイベント ID 12288 とイベント ID 12289 をログに記録します。

KMS クライアント

イベント ID 12288:

KMS イベント ログからのイベント ID 12288 エントリのセグメントを示す次のスクリーンショット。



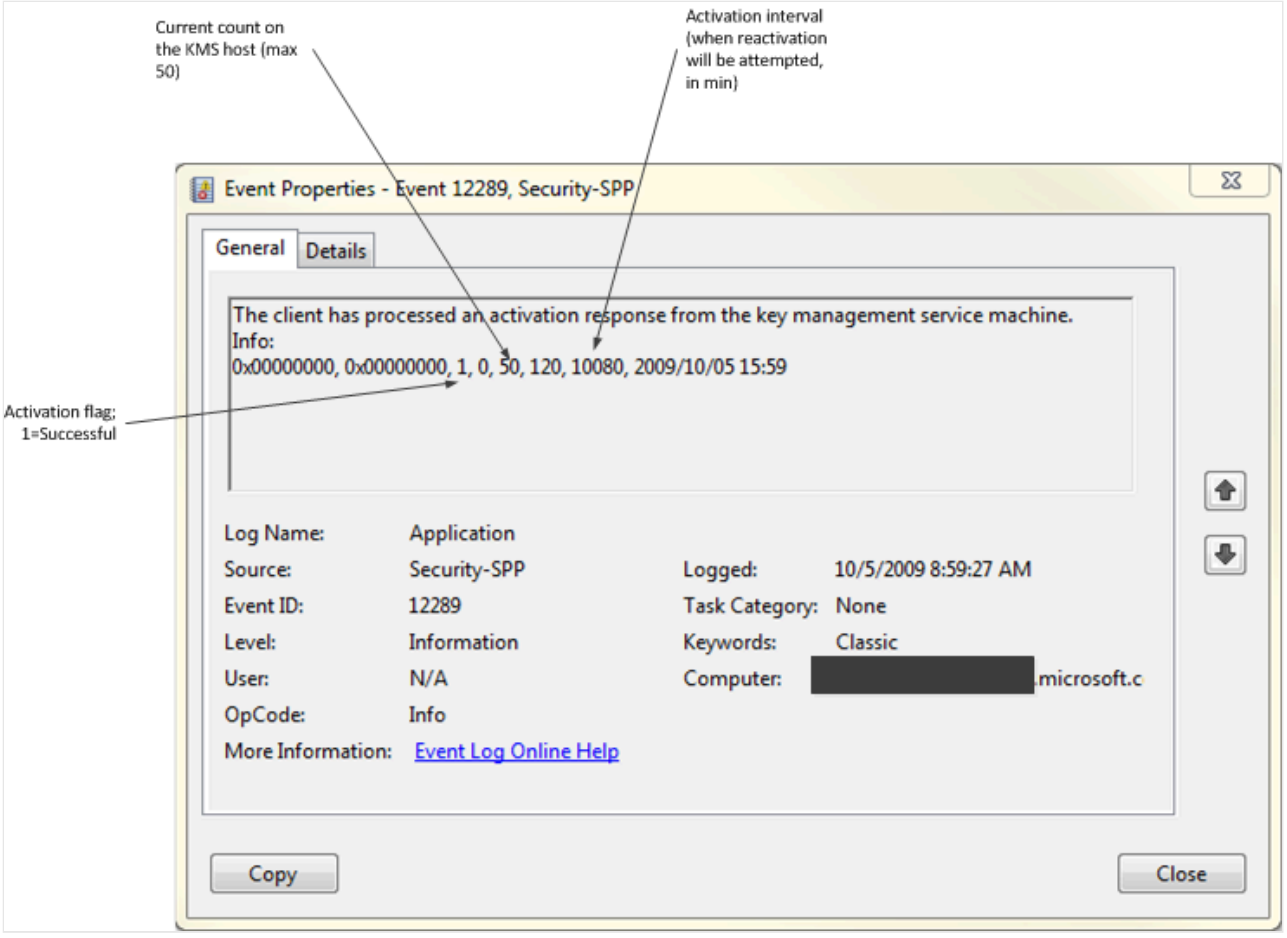
対応するイベント ID 12289 がないイベント ID 12288 のみが表示される場合、KMS クライアントが KMS ホストに到達できなかったか、KMS ホストが応答しなかったか、クライアントがホストの応答を受信しませんでした。 このような場合は、KMS ホストが検出可能であること、および KMS クライアントが KMS ホストに接続できることを確認する必要があります。

イベント ID 12288 の最も関連性の高い情報は、 情報 フィールドのデータです。 たとえば、[情報] フィールドには、クライアントの現在の状態と、アクティブ化を試みたときにクライアントが使用した FQDN と TCP ポートが表示されます。 FQDN を使用して、KMS ホストの数が増えないシナリオのトラブルシューティングを行うことができます。 たとえば、クライアントで使用できる KMS ホストが多すぎる (正当なシステムまたはサポートされていないシステム) 場合、その数はそれらのすべてに分散される可能性があります。

アクティブ化に失敗した場合、クライアントのイベント ID が 12288 であり、12289 ではないというわけではありません。 アクティブ化または再アクティブ化に失敗した場合も、両方のイベントが発生する可能性があります。 この場合は、2 番目のイベントを調べて、エラーの理由を確認する必要があります。

イベント ID 12289:

KMS イベント ログからのイベント ID 12289 エントリのセグメントを示す次のスクリーンショット。



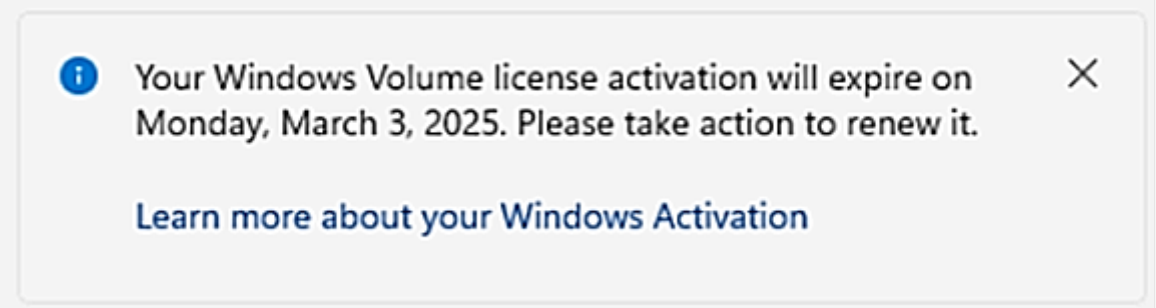
イベント ID 12289 の *Info* セクションには、次の情報が表示されます。

- アクティブ化フラグ。アクティブ化が成功した (**1**) か失敗 (**0**) かを示します。
- *KMS* ホストの現在の数。クライアントがアクティブ化を試みたときに KMS ホストのカウント値が表示されます。 アクティブ化に失敗した場合は、このクライアント OS のカウントが不十分であるか、環境内にカウントをビルドするのに十分なシステムがない可能性があります。

KMS クライアントの更新要件

KMS ライセンス認証は更新モデルで動作します。ライセンス認証を維持するには、各クライアント デバイスが少なくとも 180 日に 1 回 KMS ホスト サーバーに接続する必要があります。 既定では、KMS クライアントは 7 日ごとにライセンス認証の更新を試みます。 更新が成功すると、アクティブ化の有効期間はさらに 180 日間リセットされます。

何らかの理由で、更新要件が満たされていない場合は、更新の 180 日前の 30 日前にトースト通知が表示されます。 更新トースト通知は、アクティベーションパネルにも表示されます。



KMS クライアントの更新要件のトラブルシューティング

- この通知は、企業所有またはマネージド デバイスを使用している場合 にのみ 受け取ります。 これが正しくない場合は、 Microsoft Store からリテール キーを取得します。
- 企業所有またはマネージド デバイスを使用している場合は、IT 管理者に問い合わせてください。 このメッセージを受け取る理由として、次のことが考えられます。
  - **KMS ホストは使用停止です**。IT 管理者は KMS サーバーを使用して KMS クライアント バージョンを構成する必要があります。 「キー管理サービスを使用したアクティブ化」を参照してください。
  - **別のポートでリッスンする**: KMS との通信では匿名 RPC が使用されます。 既定では、クライアントは TCP ポート 1688 を使用して KMS ホストに接続します。 このポートが KMS クライアントと KMS ホストの間で開かれていることを確認します。 セキュリティが強化された Windows ファイアウォールを使用して、KMS ホスト上のポートを構成できます。
  - **DNS 構成の確認**: 既定では、KMS クライアントは自動検出プロセスを使用して、サーバーの一覧の DNS を照会します。 詳細については、 DNS 関連のアクティブ化に関する問題のトラブルシューティングに関するガイドラインを参照してください。

サポートは何を求めるのですか?

トラブルシューティング後にアクティブ化が期待どおりに動作しない場合は、 Microsoft サポート に問い合わせてテクニカル サポートにお問い合わせください。 通常、サポート エンジニアは次の情報を求めます。

- `slmgr.vbs /dlv` KMS ホストおよび KMS クライアント システムからの出力。
- KMS ホスト (キー管理サービス ログ) と KMS クライアント システム (アプリケーション ログ) の両方からのイベント ログ。

ボリューム ライセンス認証情報を取得するための Slmgr.vbs オプション

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Slmgr.vbs は、オペレーティング システムのライセンスとライセンス認証を管理するためのコマンド ライン ツールとして機能する、Windows に含まれる Visual Basic スクリプトです。 プロダクト キーのインストールと変更、Windows のライセンス認証、現在のライセンス認証またはライセンスの状態の確認を行えます。 また、ライセンス認証の猶予期間の延長 (再調整) や、アクティブ化に関連する問題のトラブルシューティングなどのタスクもサポートします。

この記事の Slmgr.vbs スクリプトとテーブルの構文では、各コマンド ライン オプションについて説明します。

Windows コマンド プロンプト

```
slmgr.vbs [<ComputerName> [<User> <Password>]] [<Options>]
```

> ⓘ **注意**
>
> この記事では、角かっこ ([ ]) で省略可能な引数を囲み、山かっこ (<>) でプレースホルダーを囲みます。 これらのステートメントを入力するときは、かっこを省略し、対応する値でプレースホルダーを置き換えてください。
>
> ボリューム アクティベーションを使用する他のソフトウェア製品については、それらのアプリケーション用に記述されたドキュメントを参照してください。

リモート コンピューターでの Slmgr の使用

リモート クライアントを管理するには、ボリューム ライセンス認証管理ツール (VAMT) バージョン 1.2 以降を使用するか、プラットフォームの違いに合わせた WMI スクリプトを独自に作成してください。 詳細については、ボリューム認証のWMIプロパティとメソッドを参照してください。

> ⓘ **重要**
>
> Windows 7 および Windows Server 2008 R2 での WMI の変更により、Slmgr.vbs スクリプトはプラットフォーム間で動作することを意図していません。 Slmgr.vbs を使用して

Windows Vista オペレーティング システムから Windows 7 または Windows Server 2008 R2 システムを管理することはできません。 Windows 7 または Windows Server 2008 R2 から古いシステムを管理しようとすると、特定のバージョンの不一致エラーが発生します。 たとえば、**cscript slmgr.vbs <vista_machine_name> /dlv** を実行すると、出力は次のようになります。

```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

The remote machine does not support this version of SLMgr.vbs
```

一般的な Slmgr.vbs のオプション

テーブルを展開する

選択肢	説明
[<ComputerName>]	リモート コンピューターの名前。 (既定値はローカル コンピューターです)。
[<User>]	リモート コンピューターで必要な特権を持つアカウント。
[<パスワード>]	リモート コンピューターで必要な特権を持つアカウントのパスワード。

グローバルなオプション

テーブルを展開する

選択肢	説明
/ipk <プロダクトキー>	5×5 プロダクト キーのインストールを試行します。 このパラメーターで指定されるプロダクト キーは、有効であることが確認済みであり、インストールされているオペレーティング システムに適用可能なものであることが必要です。 そうでない場合は、エラーが返されます。 キーが有効で適用可能な場合は、キーがインストールされます。 キーが既にインストールされている場合は、自動的に置き換えられます。 ライセンス サービスが不安定になるのを防止するために、システムを再起動するか、ソフトウェア保護サービスを再起動してください。 この操作は、管理者特権でのコマンド プロンプト ウィンドウから実行する必要があり

選択肢	説明
	ます。または、特権なしのユーザーが特別にソフトウェア保護サービスにアクセスできるように Standard User Operations レジストリ値が設定されている必要があります。
/ato [<Activation ID>]	リテール エディションやボリューム システムに KMS ホスト キーまたはマルチ ライセンス認証キー (MAK) がインストールされている場合は、 **/ato** を指定するとオンライン ライセンス認証が試行されます。 汎用ボリューム ライセンス キー (GVLK) がインストールされているシステムの場合、 **/ato** は KMS ライセンス認証の試行を求めます。 自動 KMS ライセンス認証試行 (**/stao**) を中断するように設定されているシステムは、 **/ato** の実行時に KMS ライセンス認証を試みます。 **注**: Windows 8 以降 (および Windows Server 2012) では、 **/stao** オプションが非推奨となっています。 **/act-type** オプションを代わりに使用してください。 パラメーター <**Activation ID**> は、コンピューター上にインストールされている Windows のエディションを **/ato** で指定できるようにするためのものです。 < **Activation ID**> パラメーターを指定すると、このオプションの効果が及ぶのは、その Activation ID に関連付けられたエディションに限定されます。 **slmgr.vbs /dlv all** を実行して、インストールされているバージョンの Windows のライセンス認証 ID を取得します。 他のアプリケーションをサポートする必要がある場合は、アプリケーションによって提供されるガイダンスで詳細な手順を参照してください。 KMS ライセンス認証では、昇格された特権は必要ありません。 ただし、オンライン ライセンス認証を行うには昇格が必要です。昇格しない場合は、特権なしのユーザーが特別にソフトウェア保護サービスにアクセスできるように Standard User Operations レジストリ値が設定されている必要があります。
/dli [<Activation ID> | すべて]	ライセンス情報を表示します。 **/dli** だけを指定すると、インストール済みのアクティブな Windows エディションのライセンス情報が表示されます。 < **Activation ID**> パラメーターを指定すると、そのライセンス認証 ID に関連付けられている指定されたエディションのライセンス情報が表示されます。 **All** をパラメーターとして指定すると、該当するすべてのインストール済み製品のライセンス情報が表示されます。 この操作では、昇格された特権は必要ありません。
/dlv [<Activation ID> | All]	詳細なライセンス情報を表示します。 **/dlv** だけを指定すると、インストール済みのオペレーティング システムのライセンス情報が表示されます。 < **Activation ID**> パラメーターを指定すると、そのライセンス認証 ID に関連付けられている指定されたエディションのライセンス情報が表示されます。 **All** パラメーターを指定すると、該当するすべてのインストール済み製品のライセンス情報が表示されます。 この操作では、昇格された特権は必要ありません。

選択肢	説明
/xpr [<Activation ID>]	製品のライセンス認証有効期限を表示します。 既定では、日付は現在の Windows エディションを参照し、MAK とリテールライセンス認証は永続的であるため、主に KMS クライアントに役立ちます。 < **Activation ID**> パラメーターを指定すると、そのアクティブ化 ID に関連付けられている指定されたエディションのアクティブ化の有効期限が表示されます。 この操作では、昇格された特権は必要ありません。

詳細オプション

テーブルを展開する

選択肢	説明
/cpky	一部のサービス操作では、Out of Box Experience (OOBE) 操作中にレジストリでプロダクト キーを使用できるようにする必要があります。 **/cpky** オプションを指定すると、プロダクト キーがレジストリから削除されるので、悪意のあるコードによってこのキーが盗まれるのを防止できます。 キーを展開するリテール インストールの場合は、このオプションを実行することをお勧めします。 MAK および KMS ホスト キーでは、このオプションは必要ありません。これは、これらのキーの既定の動作であるためです。 このオプションは、レジストリからキーをクリアしない既定の動作を持つ他の種類のキーにのみ必要です。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/ilc <license_file>	必須パラメーターで指定したライセンス ファイルがインストールされます。 これらのライセンスは、トラブルシューティングの手段として、トークン ベースのアクティブ化をサポートするため、またはオンボード アプリケーションの手動インストールの一部としてインストールされる場合があります。 このプロセス中にライセンスは検証されません。ライセンスの検証は Slmgr.vbs の範囲外です。 代わりに、検証は実行時にソフトウェア保護サービスによって処理されます。 この操作は、管理者特権でのコマンド プロンプト ウィンドウから実行する必要があります。または、特権なしのユーザーが特別にソフトウェア保護サービスにアクセスできるように Standard User Operations レジストリ値が設定されている必要があります。
/rilc	%SystemRoot%\system32\oem と %SystemRoot%\System32\spp\tokens に格納されているすべてのライセンスを再インストールします。 これらは、インストール時に格納された "既知の正常な" コピーです。 信頼されたストアにある、一致するライセンスはすべて置き換えられます。 信頼され

選択肢	説明
	た機関 (TA) 発行ライセンス (ILs)、アプリケーションのライセンスなど、追加のライセンスは影響を受けません。 この操作は、管理者特権のコマンド プロンプト ウィンドウで実行する必要があります。または、特権のないユーザーがソフトウェア保護サービスに追加アクセスできるように Standard User Operations レジストリ値を設定する必要があります。
/rearm	ライセンス認証タイマーをリセットします。 **/rearm** プロセスは、**sysprep /generalize** からも呼び出されます。 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm** レジストリ エントリが **1** に設定されている場合は、この操作を行っても何も変化しません。 このレジストリ エントリの詳細については、「ボリューム ライセンス認証のためのレジストリ設定」を参照してください。 この操作は、管理者特権のコマンド プロンプト ウィンドウで実行する必要があります。または、特権のないユーザーがソフトウェア保護サービスに追加アクセスできるように Standard User Operations レジストリ値を設定する必要があります。
/rearm-app <アプリケーション ID>	指定されたアプリのライセンス ステータスをリセットします。
/rearm-sku <アプリケーション ID>	指定された SKU のライセンス ステータスをリセットします。
/upk [<アプリケーション ID>]	現在の Windows エディションのプロダクト キーをアンインストールします。 再起動後に、システムは "ライセンスなし" 状態になります。これを解除するには、新しいプロダクト キーをインストールする必要があります。 < **Activation ID**> パラメーターを使用して別のインストール済み製品を指定することもできます。 この操作は、管理者特権でのコマンド プロンプト ウィンドウから実行する必要があります。
/dti [<Activation ID>]	オフラインでのライセンス認証のためのインストール ID を表示します。
/atp <確認ID>	指定された確認 ID を使用して製品のライセンス認証を行います。

KMS クライアントのオプション

テーブルを展開する

選択肢	説明
/skms <Name[:Port] | :Port> [<Activation ID>]	問い合わせ先となる KMS ホスト コンピューターの名前を指定します。ポートを指定することもできます。 この値を設定すると、KMS ホストの自動検出は行われなくなります。 KMS ホストで IPv6 (Internet Protocol version 6) のみが使用されている場合は、アドレスを <hostname>:<port> の形式で指定する必要があります。 IPv6 アドレスにはコロン (:)が含まれています。これは、Slmgr.vbs スクリプトが正しく解析しません。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/skms-domain <FQDN> [<Activation ID>]	すべての KMS SRV レコードが存在する、特定の DNS ドメインを設定します。 この設定は、 **/skms** オプションで特定の KMS ホストが 1 つだけ設定されている場合は効果を持たなくなります。 このオプションを使用すると、特に不整合名前空間環境において、DNS サフィックス検索リストが無視されて、代わりに指定の DNS ドメインの中で KMS ホスト レコードが検索されます。
/ckms [<Activation ID>]	このオプションは、指定した KMS ホスト名、アドレス、ポート情報をレジストリから削除し、KMS 自動検出の動作を復元します。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/skhc	このオプションにより、KMS ホスト キャッシュが有効になります (既定)。 クライアントが動作している KMS ホストを検出すると、この設定によって、ドメイン ネーム システム (DNS) の優先順位と重みがホストとのそれ以降の通信に影響を与えなくなります。 動作している KMS ホストにシステムからアクセスできなくなった場合は、クライアントが新しいホストを検出しようとします。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/ckhc	KMS ホスト キャッシュを無効にします。 この設定は、KMS のアクティブ化を試みるたびに DNS 自動検出を使用するようにクライアントに指示します (優先度と重みを使用する場合に推奨)。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。

KMS ホストの構成オプション

テーブルを展開する

選択肢	説明
/sai <インターバル>	このオプションは、非アクティブ化されたクライアントが KMS への接続を試みる間隔を分単位で設定します。 ライセンス認証間隔は 15 分以上 30 日以下で指定する必要がありますが、既定値 (2 時間) をお勧めします。 KMS クライアントは、最初にレジストリからこの間隔を取得しますが、最初の KMS 応答を受け入れた後、KMS 設定に切り替えます。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/sri <間隔>	このオプションでは、ライセンス認証されたクライアントが KMS への接続を試みる更新間隔を分単位で設定します。 更新の間隔は 15 分以上 30 日以下で指定する必要があります。 このオプションは、最初に KMS サーバー側とクライアント側の両方で設定されます。 既定値は 10,080 分 (7 日) です。 KMS クライアントは、最初にレジストリからこの間隔を取得しますが、最初の KMS 応答を受け入れた後、KMS 設定に切り替えます。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/sprt <Port>	KMS ホストのどのポートでクライアント ライセンス認証要求をリッスンするかを設定します。 既定の TCP ポートは 1688 です。 この操作は、管理者特権でのコマンド プロンプト ウィンドウから実行する必要があります。
/sdns	KMS ホストによる DNS 発行を行うように設定します (既定の動作)。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/cdns	KMS ホストによる DNS 発行を行わないように設定します。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/spri	KMS 優先度を "通常" (既定値) に設定します。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/cpri	KMS 優先度を "低" に設定します。 このオプションを使用すると、共同ホスト環境での KMS からの競合を最小限に抑えることができます。これにより、他のアプリケーションまたはサーバー ロールがアクティブかどうかに応じて KMS の不足が発生する可能性があります。 慎重にこのオプションを使用してください。

選択肢	説明
	この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。
/act-type [<Activation-Type>] [<Activation ID>]	ボリューム ライセンス認証のタイプを 1 つに限定するようにレジストリ値を設定します。 アクティブ化の種類 **1** では、アクティブ化は Active Directory のみに制限されます。 **2** により KMS ライセンス認証に限定されます。 **3** では、トークンベースのアクティブ化に制限されます。 **0** を指定すると、どのライセンス認証タイプも使用できるようになります。これが既定値です。

トークンベース ライセンス認証の構成オプション

テーブルを展開する

選択肢	説明
/lil	インストール済みのトークンベース ライセンス認証発行ライセンスのリストを返します。
/ril <ILID> <ILvID>	インストール済みのトークンベース ライセンス認証発行ライセンスを削除します。 この操作は、管理者特権でのコマンド プロンプト ウィンドウから実行する必要があります。
/stao	**Token-based Activation Only** フラグを設定します。自動 KMS ライセンス認証が行われなくなります。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。 このオプションは、Windows Server 2012 R2 および Windows 8.1 で削除されました。 **/act–type** オプションを代わりに使用してください。
/ctao	**Token-based Activation Only** フラグを解除します (既定の動作)。自動 KMS ライセンス認証が行われるようになります。 この操作は、管理者特権でのコマンド プロンプト ウィンドウで実行する必要があります。 このオプションは、Windows Server 2012 R2 および Windows 8.1 で削除されました。 **/act–type** オプションを代わりに使用してください。
/ltc	インストール済みソフトウェアのライセンス認証に使用できる、有効なトークンベース ライセンス認証証明書のリストを返します。
/fta <証明書のサムプリント>	指定した証明書を使用してトークンベース ライセンス認証を強制します。 必要に応じて、暗証番号 (PIN) を指定できます。指定しておくと、ハードウェア (たとえばスマー

選択肢	説明
[<PIN>]	ト カード) で保護されている証明書を使用するときに画面から PIN を入力しなくても秘密キーのロックを解除できるようになります。

Active Directory によるライセンス認証の構成オプション

テーブルを展開する

選択肢	説明
/ad-activation-online <Product Key> [<認証 オブジェクト名>]	Active Directory データを収集して Active Directory フォレスト ライセンス認証を実行します。コマンド プロンプトの実行に使用されている資格情報が使用されます。 ローカル管理者アクセスは必要ありません。 ただし、フォレストのルート ドメインにあるライセンス認証オブジェクト コンテナーに対する読み取り/書き込みアクセス権が必要です。
/ad-activation-get-IID <プロダクトキー>	Active Directory フォレスト ライセンス認証を電話モードで開始します。 インターネット接続が利用できない場合は、電話でフォレストをアクティブ化するために使用できるインストール ID (IID) が出力されます。 アクティブ化電話呼び出しで IID が提供されると、アクティブ化を完了するために使用される CID が返されます。
/ad-activation-apply-cid <Product Key><Confirmation ID> [<アクティベーションオブジェクト名>]	このオプションを使用する場合は、ライセンス認証窓口に電話をかけて受け取った CID を入力してライセンス認証を完了してください
[/name: <AO_Name>]	上記のどのコマンドも、必要に応じて末尾に **/name** オプションを付加することができます。このオプションでは、Active Directory に格納されているライセンス認証オブジェクトの名前を指定します。 名前は Unicode で 40 文字を超えないようにする必要があります。 名前の文字列を明示的に定義するには、二重引用符を使用します。 Windows Server 2012 R2 と Windows 8.1 では、**/ad-activation-online <Product Key>** と **/ad-activation-apply-cid** の後に、**/name** オプションを使用せず名前を直接追加できます。
/ao-list	このローカル コンピューターで使用できるライセンス認証オブジェクトをすべて表示します。
/del-ao <AO_DN> /del-ao <AO_RDN>	指定したライセンス認証オブジェクトをフォレストから削除します。

関連コンテンツ

- ボリューム ライセンス認証テクニカル リファレンス
- ボリューム ライセンス認証の概要

KMS ライセンス認証: 既知の問題

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

仮想エージェントを試す - KMS と MAK のライセンス認証に関連する一般的な問題をすばやく特定して修正するのに役立ちます

この記事では、キー管理サービス (KMS) のアクティブ化中に確認できる一般的な質問と問題について説明し、問題に対処するためのガイダンスを提供します。

> ⓘ **注意**
>
> 問題が DNS に関連していると思われる場合は、 **KMS と DNS の問題に関する一般的なトラブルシューティング手順を**参照してください。

KMS ホスト情報をバックアップする必要がありますか?

KMS ホストのバックアップは必要ありません。 ただし、ツールを使用してイベント ログを定期的にクリーンアップすると、ログに格納されているアクティブ化履歴が失われる可能性があります。 イベント ログを使用して KMS のアクティブ化を追跡または文書化する場合は、イベント ビューアーの [アプリケーションとサービス ログ] フォルダーからキー管理サービスのイベント ログを定期的にエクスポートします。

System Center Operations Manager を使用する場合、System Center Data Warehouse データベースにはレポート用のイベント ログ データが格納されるため、イベント ログを個別にバックアップする必要はありません。

KMS クライアント コンピューターはアクティブ化されていますか?

KMS クライアント コンピューターで、[**システム**] コントロール パネルを開き、 **Windows がアクティブ化された** メッセージを探します。 または、Slmgr.vbs を実行し、 **/dli** コマンド ライン オプションを使用します。

KMS クライアント コンピューターがアクティブ化されない

KMS ライセンス認証のしきい値が満たされていることを確認します。 KMS ホスト コンピューターで、Slmgr.vbs を実行し、 **/dli** コマンド ライン オプションを使用してホストの現在の数を確認します。 KMS ホストの数が 25 になるまで、Windows 7 クライアント コンピューターをアクティブ化することはできません。 Windows Server 2008 R2 KMS クライアントでは、ライセンス認証に KMS カウント 5 が必要です。 KMS の要件の詳細については、「ボリューム ライセンス認証の計画ガイド」を参照してください。

KMS クライアント コンピューターで、アプリケーション イベント ログでイベント ID 12289 を確認します。 このイベントで次の情報を確認します。

- 結果コード **は 0** ですか? それ以外はエラーです。
- イベント内の KMS ホスト名は正しいですか?
- KMS ポートは正しいですか?
- KMS ホストにアクセスできますか?
- クライアントが Microsoft 以外のファイアウォールを実行している場合、送信ポートを構成する必要がありますか?

KMS ホスト コンピューターで、KMS イベント ログでイベント ID 12290 を確認します。 このイベントで次の情報を確認します。

- KMS ホストは、クライアント コンピューターからの要求をログに記録しましたか? KMS クライアント コンピューターの名前が一覧表示されていることを確認します。 クライアントと KMS ホストが通信できることを確認します。 クライアントは応答を受信しましたか?
- KMS クライアントからイベントがログに記録されない場合、要求が KMS ホストに到達しなかったか、KMS ホストで処理できませんでした。 ルーターが TCP ポート 1688 を使用してトラフィックをブロックしないこと (既定のポートが使用されている場合) と、KMS クライアントへのステートフル トラフィックが許可されていることを確認します。

このエラー コードの意味

イベント ID が 12290 の KMS イベントを除き、Windows は、すべてのアクティブ化イベントをイベント プロバイダー名 Microsoft-Windows-Security-SPP の下のアプリケーション イベント ログに記録します。 Windows は、KMS イベントをアプリケーションとサービス フォルダーのキー管理サービス ログに記録します。 IT 担当者は、Slui.exe を実行して、ほとんどのアクティブ化関連のエラー コードの説明を表示できます。 このコマンドの一般的な構文は次のとおりです。

Windows コマンド プロンプト

```
slui.exe 0x2a ErrorCode
```

たとえば、イベント ID 12293 にエラー コード 0x8007267Cが含まれている場合は、次のコマンドを実行してそのエラーの説明を表示できます。

Windows コマンド プロンプト

```
slui.exe 0x2a 0x8007267C
```

特定のエラー コードとその対処方法の詳細については、「 一般的なアクティブ化エラー コードの解決」を参照してください。

クライアントが KMS のカウントに追加されない

クライアント コンピューター ID (CMID) とその他の製品ライセンス認証情報をリセットするには、 **sysprep /generalize** または **slmgr /rearm** を実行します。 それ以外の場合、各クライアント コンピューターは同じように見え、KMS ホストでは個別の KMS クライアントとしてカウントされません。

KMS ホストで SRV レコードを作成できない

ドメイン ネーム システム (DNS) は、書き込みアクセスを制限したり、動的 DNS (DDNS) をサポートしていない場合があります。 この場合は、KMS ホストに DNS データベースへの書き込みアクセス権を付与するか、サービス (SRV) リソース レコード (RR) を手動で作成します。 KMS と DNS の問題の詳細については、 KMS と DNS の問題に関する一般的なトラブルシューティング手順を参照してください。

最初の KMS ホストのみが SRV レコードを作成できます

組織に複数の KMS ホストがある場合、SRV の既定のアクセス許可が変更されていない限り、他のホストは SRV RR を更新できないことがあります。 KMS と DNS の問題の詳細については、 KMS と DNS の問題に関する一般的なトラブルシューティング手順を参照してください。

KMS クライアントに KMS キーをインストールしました

KMS キーは、KMS クライアントではなく KMS ホストにのみインストールする必要があります。 **slmgr.vbs -ipk < SetupKey>** を実行します。 コンピューターを KMS クライアントとして構成するために使用できるキーのテーブルについては、 KMS クライアントセットアップ キーに関する説明を参照してください。 これらのキーは一般に知られており、エディション固有です。 不要な SRV R を DNS から削除してから、コンピューターを再起動してください。

KMS ホストが失敗しました

KMS ホストが失敗した場合は、新しいホストに KMS ホスト キーをインストールしてから、ホストをアクティブ化する必要があります。 新しい KMS ホストが DNS データベースに SRV RR を持っていることを確認します。 失敗した KMS ホストと同じコンピューター名と IP アドレスを使用して新しい KMS ホストをインストールした場合、新しい KMS ホストは、失敗したホストの DNS SRV レコードを使用できます。 新しいホストのコンピューター名が異なる場合は、失敗したホストの DNS SRV RR を手動で削除するか(DNS で清掃が有効になっている場合)、DNS で自動的に削除することができます。 ネットワークが DDNS を使用している場合、新しい KMS ホストによって DNS サーバーに新しい SRV RR が自動的に作成されます。 その後、新しい KMS ホストはクライアント更新要求の収集を開始し、KMS ライセンス認証のしきい値に達するとすぐにクライアントのアクティブ化を開始します。

KMS クライアントが自動検出を使用している場合、元の KMS ホストが更新要求に応答しない場合は、別の KMS ホストが自動的に選択されます。 クライアントが自動検出を使用しない場合は、 **slmgr.vbs /skms** を実行して、失敗した KMS ホストに割り当てられた KMS クライアント コンピューターを手動で更新する必要があります。 このシナリオを回避するには、自動検出を使用するように KMS クライアントを構成します。 詳細については、「ボリューム アクティベーションの展開ガイド」を参照してください。

MAK ライセンス認証: 既知の問題

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

仮想エージェントを試す - KMS と MAK のライセンス認証に関連する一般的な問題をすばやく特定して修正するのに役立ちます

この記事では、複数ライセンス認証キー (MAK) のアクティブ化中に発生する可能性がある一般的な問題について説明し、それらの問題に対処するためのガイダンスを提供します。

コンピューターがアクティブ化されているかどうかを確認するにはどうすればよいですか?

コンピューターで、[**システム**] コントロール パネルを開き、 **Windows がアクティブになっていることを**確認します。 または、Slmgr.vbs を実行し、 **/dli** コマンド ライン オプションを使用します。

コンピューターがインターネット経由で起動しない

必要なポートがファイアウォールで開いていることを確認します。 ポートの一覧については、「ボリューム ライセンス認証の展開ガイド」を参照してください。

インターネットと電話のアクティベーションができない

ローカルの Microsoft ライセンス認証センターにお問い合わせください。 世界中の Microsoft ライセンス認証センターの電話番号については、 Microsoft ライセンス 認証センターの世界中の電話番号 にアクセスしてください。 呼び出すときは、ボリューム ライセンス契約の情報と購入証明を必ず入力してください。

Slmgr.vbs /ato はエラー コードを返します

Slmgr.vbs が 16 進数のエラー コードを返す場合は、次のスクリプトを実行して対応するエラー メッセージを確認します。

Windows コマンド プロンプト

```
slui.exe 0x2a 0x <ErrorCode>
```

特定のエラー コードとその対処方法の詳細については、「 一般的なアクティブ化エラー コードの解決」を参照してください。

DNS 関連のアクティブ化に関する問題のトラブルシューティングに関するガイドライン

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

次の条件の 1 つ以上が当てはまる場合は、これらのメソッドの一部を使用する必要があります。

- ボリューム ライセンス メディアとボリューム ライセンス汎用プロダクト キーを使用して、次のいずれかのオペレーティング システムをインストールします。
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows 10
  - Windows 8.1
  - Windows 8
- ライセンス認証ウィザードは KMS ホスト コンピューターに接続できません。

クライアント システムをアクティブ化しようとすると、ライセンス認証ウィザードは DNS を使用して、KMS ソフトウェアを実行している対応するコンピューターを見つけます。 ウィザードが DNS を照会し、KMS ホスト コンピューターの DNS エントリが見つからない場合、ウィザードはエラーを報告します。

次の一覧を確認して、状況に合ったアプローチを見つけてください。

- KMS ホストをインストールできない場合、または KMS ライセンス認証を使用できない場合は、「 プロダクト キーを MAK に変更する 」の手順を試してください。
- KMS ホストをインストールして構成する必要がある場合は、 クライアントの KMS ホストを構成してアクティブ化する手順を使用します 。
- クライアントで既存の KMS ホストが見つからない場合は、次の手順に従ってルーティング構成のトラブルシューティングを行います。 これらの手順は、最も単純なものから最も複雑なものまで構成されています。
  - DNS サーバーへの基本的な IP 接続を確認する
  - KMS ホストの構成を確認する
  - ルーティングの問題の種類を特定する

- DNS 構成を確認する
- KMS SRV レコードを手動で作成する
- KMS クライアントに KMS ホストを手動で割り当てる
- 複数の DNS ドメインで発行するように KMS ホストを構成する

プロダクト キーを MAK に変更する

KMS ホストをインストールできない場合、または何らかの理由で KMS ライセンス認証を使用できない場合は、プロダクト キーを MAK に変更します。 Microsoft Developer Network (MSDN) または TechNet から Windows イメージをダウンロードした場合、メディアの下に一覧表示されている在庫保持ユニット (SKU) は一般にボリューム ライセンス メディアであり、提供されるプロダクト キーは MAK キーです。

プロダクト キーを MAK に変更するには、次の手順に従います。

1. 管理者特権のコマンド プロンプト ウィンドウを開きます。 これを行うには、Windows ロゴ キーを押しながら X キーを押し、 **コマンド プロンプト**を右クリックし、[**管理者として実行**] を選択します。 管理者パスワードまたは確認入力を求められた場合は、パスワードを入力するか、確認入力を行います。
2. コマンド プロンプトで、次のコマンドを実行します。

   Windows コマンド プロンプト

   ```
   slmgr -ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
   ```

   > ⓘ **注意**
   >
   > **xxxxx-xxxxx-xxxxx-xxxxx-xxxxx** プレースホルダーは MAK プロダクト キーを表します。

プロシージャの一覧に戻ります。

ライセンス認証するクライアントに合わせて KMS ホストを構成する

KMS ライセンス認証では、クライアントがライセンス認証を行うために KMS ホストを構成する必要があります。 環境内に KMS ホストが構成されていない場合は、適切な KMS ホスト キーを使用して、KMS ホストをインストールしてアクティブ化します。 KMS ソフトウェアをホストするようにネットワーク上のコンピューターを構成した後、ドメイン ネーム システム (DNS) 設定を発行します。

KMS ホスト構成プロセスの詳細については、「 キー管理サービスを使用したアクティブ化 」および 「VAMT のインストールと構成」を参照してください。

プロシージャの一覧に戻ります。

DNS サーバーへの基本的な IP 接続を確認する

ping コマンドを使用して、DNS サーバーへの基本的な IP 接続を確認します。 これを行うには、エラーが発生している KMS クライアントと KMS ホスト コンピューターの両方で、次の手順に従います。

1. 管理者特権のコマンド プロンプト ウィンドウを開きます。
2. コマンド プロンプトで、次のコマンドを実行します。

Windows コマンド プロンプト

```
ping <DNS_Server_IP_address>
```

> **注意**
>
> このコマンドの出力に "Reply from" という語句が含まれていない場合は、この記事の他の手順を使用する前に解決する必要があるネットワークの問題または DNS の問題があります。 DNS サーバーに ping を実行できない場合に TCP/IP の問題をトラブルシューティングする方法の詳細については、 **TCP/IP の問題に関する高度なトラブルシューティングを**参照してください。

プロシージャの一覧に戻ります。

KMS ホストの構成を確認する

KMS ホスト サーバーのレジストリを調べて、DNS に登録しているかどうかを確認します。 既定では、KMS ホスト サーバーは DNS SRV レコードを 24 時間ごとに 1 回動的に登録します。

> **重要**
>
> 慎重にこのセクションの手順に従います。 レジストリを正しく変更しないと、重大な問題が発生する可能性があります。 変更する前に、問題が発生した場合に**復元するためにレジストリをバックアップ**します。

この設定を確認するには、次の手順に従います。

1. レジストリエディタを起動します。 これを行うには、[**スタート**] を右クリックし、[**実行**] を選択し、「 **regedit**」と入力して、Enter キーを押します。
2. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** サブキー (以前は Windows Server 2008 および Windows Vista の **SoftwareProtectionPlatform** ではなく **SL**) を見つけて、**DisableDnsPublishing** エントリの値を確認します。 このエントリには、次の可能な値があります。

   - **0** または未定義 (既定値): KMS ホスト サーバーは、24 時間に 1 回 SRV レコードを登録します。
   - **1**: KMS ホスト サーバーは SRV レコードを自動的に登録しません。 実装で動的更新がサポートされていない場合は、「 KMS SRV レコードを手動で作成する」を参照してください。

3. **DisableDnsPublishing** エントリがない場合は、作成します (型は DWORD)。 動的登録が許容される場合は、値を未定義のままにするか 、**0** に設定します。

プロシージャの一覧に戻ります。

ルーティングの問題の種類を特定する

次のコマンドを使用して、これが名前解決の問題か SRV レコードの問題かを判断できます。

1. KMS クライアントで、管理者特権のコマンド プロンプト ウィンドウを開きます。
2. コマンド プロンプトで次のコマンドを実行します。

   Windows コマンド プロンプト

   ```
   cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
   cscript \windows\system32\slmgr.vbs -ato
   ```

   > ⓘ **注意**
   >
   > このコマンドでは、 <KMS_FQDN> は KMS ホスト コンピューターの完全修飾ドメイン名 (FQDN) を表し、 <port> は KMS が使用する TCP ポートを表します。

   これらのコマンドで問題が解決された場合、これは SRV レコードの問題です。 KMS クライアントに KMS ホストを手動で割り当てる手順に記載されているコマンドのいずれかを使用して、トラブルシューティングを行うことができます。

3. 問題が解決しない場合は、次のコマンドを実行します。

```
Windows コマンド プロンプト

cscript \windows\system32\slmgr.vbs -skms <IP Address>:<port>
cscript \windows\system32\slmgr.vbs -ato
```

> ⓘ **注意**
>
> このコマンドでは、 <IP アドレス> は KMS ホスト コンピューターの IP アドレスを表し、 <port> は KMS が使用する TCP ポートを表します。

これらのコマンドで問題が解決された場合、これは名前解決の問題である可能性が最も高くなります。 その他のトラブルシューティング情報については、「 DNS 構成の確認」 の手順を参照してください。

4. これらのコマンドのいずれも問題を解決しない場合は、コンピューターのファイアウォール構成を確認してください。 KMS クライアントと KMS ホストの間で発生するアクティブ化通信では、1688 TCP ポートが使用されます。 KMS クライアントと KMS ホストの両方のファイアウォールで、ポート 1688 経由の通信を許可する必要があります。

プロシージャの一覧に戻ります。

DNS 構成を確認する

> ⓘ **注意**
>
> 特に明記されていない限り、該当するエラーが発生した KMS クライアントで次の手順に従います。

1. 管理者特権でのコマンド プロンプト ウィンドウを開く
2. コマンド プロンプトで、次のコマンドを実行します。

```
Windows コマンド プロンプト

IPCONFIG /all
```

3. コマンドの結果から、次の情報に注意してください。

   - KMS クライアント コンピューターの割り当てられた IP アドレス

- KMS クライアント コンピューターが使用するプライマリ DNS サーバーの IP アドレス
- KMS クライアント コンピューターが使用する既定のゲートウェイの IP アドレス
- KMS クライアント コンピューターが使用する DNS サフィックス検索リスト

4. KMS ホスト SRV レコードが DNS に登録されていることを確認します。 これを行うには、次の手順に従います。
   a. 管理者特権のコマンド プロンプト ウィンドウを開きます。
   b. コマンド プロンプトで、次のコマンドを実行します。

```
Windows コマンド プロンプト

nslookup -type=all _vlmcs._tcp>kms.txt
```

   c. コマンドによって生成される KMS.txt ファイルを開きます。 このファイルには、次のエントリのような 1 つ以上のエントリが含まれている必要があります。

```
_vlmcs._tcp.contoso.com SRV service location:
priority = 0
weight = 0
port = 1688 svr hostname = kms-server.contoso.com
```

> ⓘ **注意**
>
> このエントリでは、contoso.com KMS ホストのドメインを表します。

   i. KMS ホストの IP アドレス、ホスト名、ポート、およびドメインを確認します。
   ii. これらの **_vlmcs** エントリが存在し、予期される KMS ホスト名が含まれている場合は、「 KMS クライアントに KMS ホストを手動で割り当てる」に進みます。

> ⓘ **注意**
>
> nslookup コマンドが KMS ホストを見つけた場合、DNS クライアントが KMS ホストを見つけることができるという意味ではありません。 **nslookup** コマンドで KMS ホストが見つかるが、KMS ホストを使用してアクティブ化できない場合は、プライマリ DNS サフィックスや DNS サフィックスの検索リストなど、他の DNS 設定を確認します。

5. プライマリ DNS サフィックスの検索リストに、KMS ホストに関連付けられている DNS ドメイン サフィックスが含まれていることを確認します。 検索リストにこの情報が含まれていない場合は、「 複数の DNS ドメインで発行するように KMS ホストを構成する」の手順に進みます。

プロシージャの一覧に戻ります。

KMS SRV レコードを手動で作成する

Microsoft DNS サーバーを使用する KMS ホストの SRV レコードを手動で作成するには、次の手順に従います。

1. DNS サーバーで、DNS マネージャーを開きます。 DNS マネージャーを開くには、[**スタート**] を選択し、[**管理ツール**] を選択して、[DNS] を選択 **します**。
2. SRV リソース レコードを作成する必要がある DNS サーバーを選択します。
3. コンソール ツリーで、[**前方参照ゾーン**] を展開し、ドメインを右クリックし、[**その他の新しいレコード**] を選択します。
4. 一覧を下にスクロールし、[**サービスの場所 (SRV)**]、[**レコードの作成**] の順に選択します。
5. 次の情報を入力します。

    - サービス: **_VLMCS**
    - プロトコル: **_TCP**
    - ポート番号: **1688**
    - サービスを提供するホスト: ***KMS* ホストの <*FQDN*>**

6. 完了したら、[**OK**] **を**選択し、[**完了**] を選択します。

BIND 9.x 準拠 DNS サーバーを使用する KMS ホストの SRV レコードを手動で作成するには、その DNS サーバーの指示に従い、SRV レコードに関する次の情報を指定します。

- 名前: **_vlmcs._TCP**
- 型: **SRV**
- 優先度: **0**
- 重み: **0**
- ポート: **1688**
- ホスト名: ***KMS* ホストの <*FQDN* または *A-Name*>**

KMS 自動発行をサポートするように BIND 9.x 互換 DNS サーバーを構成するには、KMS ホストからのリソース レコードの更新を有効にするように DNS サーバーを構成します。 たとえば、Named.conf または Named.conf.local のゾーン定義に次の行を追加します。

Windows コマンド プロンプト

```
allow-update { any; };
```

KMS クライアントに KMS ホストを手動で割り当てる

既定では、KMS クライアントは自動検出プロセスを使用します。 このプロセスによると、KMS クライアントは、クライアントのメンバーシップ ゾーン内の SRV レコード `_vlmcs` 公開されているサーバーの一覧を DNS に照会します。 DNS は、KMS ホストの一覧をランダムな順序で返します。 クライアントは KMS ホストを選択し、その上でセッションを確立しようとします。 この試行が機能する場合、クライアントは KMS ホストの名前をキャッシュし、次回の更新の試行に使用しようとします。 セッションのセットアップが失敗した場合、クライアントは別の KMS ホストをランダムに選択します。 自動検出プロセスを使用することを強くお勧めします。

ただし、KMS ホストを特定の KMS クライアントに手動で割り当てることができます。 これを行うには、次の手順に従ってください。

1. KMS クライアントで、管理者特権のコマンド プロンプト ウィンドウを開きます。
2. 実装に応じて、次のいずれかの手順に従います。

    - ホストの FQDN を使用して KMS ホストを割り当てるには、次のコマンドを実行します。

        Windows コマンド プロンプト

        ```
        cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
        ```

    - ホストのバージョン 4 の IP アドレスを使用して KMS ホストを割り当てるには、次のコマンドを実行します。

        Windows コマンド プロンプト

        ```
        cscript \windows\system32\slmgr.vbs -skms <IPv4Address>:<port>
        ```

    - ホストのバージョン 6 の IP アドレスを使用して KMS ホストを割り当てるには、次のコマンドを実行します。

        Windows コマンド プロンプト

        ```
        cscript \windows\system32\slmgr.vbs -skms <IPv6Address>:<port>
        ```

    - ホストの NETBIOS 名を使用して KMS ホストを割り当てるには、次のコマンドを実行します。

        ```
        ```

Windows コマンド プロンプト

```
cscript \windows\system32\slmgr.vbs -skms <NETBIOSName>:<port>
```

- KMS クライアントで自動検出に戻すには、次のコマンドを実行します。

Windows コマンド プロンプト

```
cscript \windows\system32\slmgr.vbs -ckms
```

> ⓘ **注意**
>
> これらのコマンドでは、次のプレースホルダーを使用します。
> - **<KMS_FQDN>** は、KMS ホスト コンピューターの完全修飾ドメイン名 (FQDN) を表します
> - **<IPv4Address>** は、KMS ホスト コンピューターの IP バージョン 4 アドレスを表します
> - **<IPv6Address>** は、KMS ホスト コンピューターの IP バージョン 6 アドレスを表します
> - **<NETBIOSName>** は、KMS ホスト コンピューターの NETBIOS 名を表します。
> - **<port>** KMS が使用する TCP ポートを表します。

複数の DNS ドメインで発行するように KMS ホストを構成する

> ⓘ **重要**
>
> 慎重にこのセクションの手順に従います。 レジストリを正しく変更しないと、重大な問題が発生する可能性があります。 変更する前に、問題が発生した場合に**復元するためにレジストリをバックアップ**します。

KMS クライアントに KMS ホストを手動で割り当てる方法で説明されているように、KMS クライアントは通常、自動検出プロセスを使用して KMS ホストを識別します。 このプロセスでは、 SRV レコードが KMS クライアント コンピューターの DNS ゾーンで使用できる必要があります。 DNS ゾーンは、コンピューターのプライマリ DNS サフィックスまたは次のいずれかに対応します。

- ドメインに参加しているコンピューターの場合、DNS システムによって割り当てられたコンピューターのドメイン (Active Directory Domain Services (AD DS) DNS など)。
- ワークグループ コンピューターの場合、動的ホスト構成プロトコル (DHCP) によって割り当てられたコンピューターのドメイン。 このドメイン名は、コメント要求 (RFC) 2132 で定義されているコード値が 15 のオプションによって定義されます。

既定では、KMS ホストは、KMS ホスト コンピューターのドメインに対応する DNS ゾーンに SRV レコードを登録します。 たとえば、KMS ホストが contoso.com ドメインに参加しているとします。 このシナリオでは、KMS ホストは、contoso.com DNS ゾーンに `_vlmcs` SRV レコードを登録します。 そのため、レコードはサービスを `_VLMCS._TCP.CONTOSO.COM` として識別します。

KMS ホストと KMS クライアントが異なる DNS ゾーンを使用する場合は、複数の DNS ドメインでその SRV レコードを自動的に発行するように KMS ホストを構成する必要があります。 この手順を実行するには、以下のステップに従ってください。

1. KMS ホストで、レジストリ エディターを起動します。
2. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** サブキー (Windows Server 2008 および Windows Vista の **SoftwareProtectionPlatform** ではなく、以前**は SL**) を見つけて選択します。
3. **[詳細]** ウィンドウで、空白領域を右クリックし、[**新規**] を選択し、[**複数文字列値**] を選択します。
4. 新しいエントリの名前として、「 **DnsDomainPublishList」と入力します**。
5. 新しい **DnsDomainPublishList** エントリを右クリックし、[**変更**] を選択します。
6. [**複数文字列の編集**] ダイアログ ボックスで、KMS が発行する各 DNS ドメイン サフィックスを別の行に入力し、[**OK**] を選択します。

   > ⓘ **注意**
   >
   > Windows Server 2008 R2 の場合、 **DnsDomainPublishList** の形式は異なります。 詳細については、「ボリューム ライセンス認証テクニカル リファレンス ガイド」を参照してください。

7. サービス管理ツールを使用して、ソフトウェア保護サービス (以前は Windows Server 2008 および Windows Vista のソフトウェア ライセンス サービス) を再起動します。 この操作により、SRV レコードが作成されます。
8. 一般的な方法を使用して、KMS クライアントが構成した KMS ホストに接続できることを確認します。 KMS クライアントが名前と IP アドレスの両方で KMS ホストを正しく識別していることを確認します。 これらの検証のいずれかが失敗した場合は、この DNS クライアント リゾルバーの問題を調査します。

9. KMS クライアントで以前にキャッシュされた KMS ホスト名をクリアするには、KMS クライアントで管理者特権のコマンド プロンプト ウィンドウを開き、次のコマンドを実行します。

Windows コマンド プロンプト

```
cscript C:\Windows\System32\slmgr.vbs -ckms
```

Tokens.dat ファイルをリビルドする

2025/08/16

適用対象: ✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016

Windows のライセンス認証に関する問題のトラブルシューティングを行うときは、Tokens.dat ファイルの再構築が必要になる場合があります。 この記事では、これを行う方法について詳しく説明します。

Resolution

Tokens.dat ファイルをリビルドするには、次の手順に従います。

1. 管理者特権でのコマンド プロンプト ウィンドウを開く: **Windows 10 の場合**
   a. [**スタート**] メニューを開き、「cmd」と入力**します**。
   b. 検索結果で、[**コマンド プロンプト**] を右クリックし、[**管理者として実行**] を選択します。

   Windows 8.1 の場合
   a. 画面の右端からスワイプし、[**検索**] をタップします。 または、マウスを使用している場合は、画面の右下隅をポイントし、[**検索**] を選択します。
   b. 検索ボックスに「cmd」と入力 **します**。
   c. 表示された **コマンド プロンプト** アイコンをスワイプするか右クリックします。
   d. [**管理者として実行**] をタップまたはクリックします。

   Windows 7 の場合
   a. [**スタート**] メニューを開き、「cmd」と入力**します**。
   b. 検索結果で、 **cmd.exe**を右クリックし、[**管理者として実行**] を選択します。

2. オペレーティング システムに適したコマンドの一覧を入力します。

   Windows 10、Windows Server 2016 以降のバージョンの Windows の場合は、次のコマンドを順番に入力します。

   Windows コマンド プロンプト

```
net stop sppsvc
cd %Systemdrive%\Windows\System32\spp\store\2.0\
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

Windows 8.1、Windows Server 2012、Windows Server 2012 R2 の場合は、次のコマンドを順番に入力します。

Windows コマンド プロンプト

```
net stop sppsvc
cd %Systemdrive%\Windows\System32\spp\store\
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

Windows 7、Windows Server 2008、Windows Server 2008 R2 の場合は、次のコマンドを順番に入力します。

Windows コマンド プロンプト

```
net stop sppsvc
cd
%Systemdrive%\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwareProtectionPlatform
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

3. コンピューターを再起動します。

詳細情報

Tokens.dat ファイルをリビルドした後、次のいずれかの方法を使用してプロダクト キーを再インストールする必要があります。

- 同じ管理者特権のプロンプト コマンドで、次のコマンドを入力し、Enter キーを押します。

  Windows コマンド プロンプト

  ```
  cscript.exe %windir%\system32\slmgr.vbs /ipk <Product key>
  ```

  > **ⓘ 重要**
  >
  > **/upk** スイッチを使用してプロダクト キーをアンインストールしないでください。既存のプロダクト キーにプロダクト キーをインストールするには、 **/ipk** スイッチを使用します。

- [**マイ コンピューター**] を右クリックし、[**プロパティ**] を選択し、[**プロダクト キーの変更**] を選択します。

KMS クライアント セットアップ キーの詳細については、「 KMS クライアント セットアップ キー」を参照してください。

Azure Connected Machine エージェントのデプロイ オプション

要件と使用するツールに応じて、さまざまな方法を使用して、ハイブリッド環境のマシンを Azure に直接接続できます。

オンボード方法

次の表では、デプロイに最適な方法を決定できるように、各方法を示します。 詳細については、各メソッドの手順を表示するリンクに従ってください。

テーブルを展開する

サポートされている OS の種類	メソッド	説明
Linux と Windows	対話型	デプロイ スクリプトを使用してマシンを接続する単一または少数のマシンにエージェント を手動でインストールします。 Azure portal からスクリプトを生成し、マシン上で実行して、エージェントのインストールと構成の手順を自動化できます。
Linux と Windows	対話型または大規模	PowerShell を使用してマシンを接続します。
Linux と Windows	大規模	Ansible Core または Ansible Automation Platform の Azure Arc オンボード ロールを使用して、Ansible を使用して大規模なマシンを接続します。
Linux と Windows	大規模	サービス プリンシパルを使用してマシンを接続 し、エージェントを非対話型で大規模にインストールします。
Linux と Windows	大規模	Azure Arc 対応 VMware vSphere を使用して、大規模な VMware 仮想マシン (VM) に Azure Arc エージェントをインストールします。 Azure Arc 対応 VMware vSphere を使用すると、 VMware vCenter サーバーを Azure に接続し、VMware VM を自動的に検出して、Azure Arc エージェントをインストールできます。 VM 上の VMware ツールが必要です。
Linux と Windows	大規模	Azure Arc 対応 SCVMM を使用して、System Center Virtual Machine Manager (SCVMM) VM に大規模に Azure Arc エージェントをインストールします。 Azure Arc 対応 SCVMM を使用すると、 SCVMM 管理サーバーを Azure に接続し、SCVMM VM を自動的に検出して、Azure Arc エージェントをインストールできます。

サポートされている OS の種類	メソッド	説明
Linux と Windows	大規模	Azure Arc で有効になっているマルチクラウド コネクタを使用して AWS クラウドを接続し、Arc オンボードソリューションを有効にして、EC2 VM を自動検出してオンボードします。
ウィンドウズ	対話型	Windows Admin Center からマシンを接続します。
ウィンドウズ	対話型	Azure Arc セットアップを使用して Windows Server マシンを Azure に接続します。
ウィンドウズ	大規模	Configuration Manager で PowerShell スクリプトを実行してマシンを接続します。
ウィンドウズ	大規模	Configuration Manager カスタム タスク シーケンスを使用してマシンを接続します。
ウィンドウズ	大規模	グループ ポリシーを使用して Windows マシンを接続します。

> ⓘ **重要**
>
> 接続されたマシン エージェントを Azure VM にインストールすることはできません。 インストール スクリプトによって警告が表示され、サーバーが Azure で実行されていることが検出された場合はロールバックされます。

エージェントをデプロイする前に、基本的な 前提条件 と ネットワーク構成の要件 と、選択したオンボード方法の手順に記載されている特定の要件を確認してください。 エージェントがシステムに加える変更の詳細については、「 Azure Connected Machine エージェントの概要」を参照してください。

SQL Server の自動接続

Microsoft SQL Server がインストールされた Windows または Linux サーバーを Azure Arc に接続すると、SQL Server インスタンスも自動的に Azure Arc に登録されます。 Azure Arc によって有効化された SQL Server には、SQL Server インスタンスとデータベース用の詳細インベントリと追加の管理機能が備わっています。 接続プロセスの一環として、拡張機能が Azure Arc 対応サーバーにデプロイされ、SQL Server およびデータベースに新しいロールが自動的に適用されます。 SQL Server を Azure Arc に自動的に接続したくない場合は、Azure Arc への接続時に、名前が `ArcSQLServerExtensionDeployment`、値が `Disabled` のタグを Windows または Linux サーバーに追加することでオプトアウトできます。

詳細については、「Azure Arc によって有効化された SQL Server の自動接続を管理する」を参照してください。

関連コンテンツ

- Azure Connected Machine エージェントの前提条件とネットワーク要件について学習する。
- Azure Arc 対応サーバーの計画とデプロイ ガイドを確認します。
- Connected Machine エージェントの再構成、アップグレード、および削除について学習する。
- Azure Arc Jumpstart を使用して 、Azure Arc 対応サーバーを試してみてください。

Last updated on 2026/03/27

Azure Arc セットアップを使用して Windows Server マシンを Azure に接続する

Windows Server に含まれるグラフィカル ウィザードを使用して、Windows Server マシンを Azure Arc に直接オンボードできます。 ウィザードは、Azure Arc のオンボードを成功させるために必要な前提条件を確認し、最新バージョンの Azure Connected Machine (AzCM) エージェントをフェッチしてインストールすることで、オンボード プロセスを自動化します。 ウィザードプロセスが完了すると、Azure portal で Window Server マシンに移動します。このマシンは、他の Azure Arc 対応リソースと同様に表示および管理できます。

Windows Server マシンが既に Azure で実行されている場合は、Azure Arc にオンボードする必要はありません。

Windows Server 2022 の場合、Azure Arc Setup はオプションのコンポーネントであり、 **役割と機能の削除ウィザード**を使用して削除できます。 Windows Server 2025 以降の場合、Azure Arc セットアップは オンデマンド機能です。 削除と有効化の手順は、OS のバージョンによって異なります。

> **Note**
>
> Azure Arc セットアップ機能は、Windows Server 2022 以降にのみ適用されます。 これは、2023 年 10 月 10 日の**累積的な更新プログラム**でリリースされました。

SQL Server の自動接続

Microsoft SQL Server もインストールされている Azure Arc に Windows または Linux サーバーを接続すると、SQL Server インスタンスも Azure Arc に自動的に接続されます。 Azure Arc によって有効化された SQL Server には、SQL Server インスタンスとデータベース用の詳細なインベントリと追加の管理機能が備わっています。 接続プロセスの一環として、拡張機能が Azure Arc 対応サーバーにデプロイされ、 新しいロール が SQL Server とデータベースに適用されます。 SQL Server を Azure Arc に自動的に接続しない場合は、Azure Arc に接続するときに、 `ArcSQLServerExtensionDeployment` と値 `Disabled` という名前のタグを Windows または Linux サーバーに追加することでオプトアウトできます。

詳細については、「Azure Arc によって有効化された SQL Server の自動接続を管理する」を参照してください。

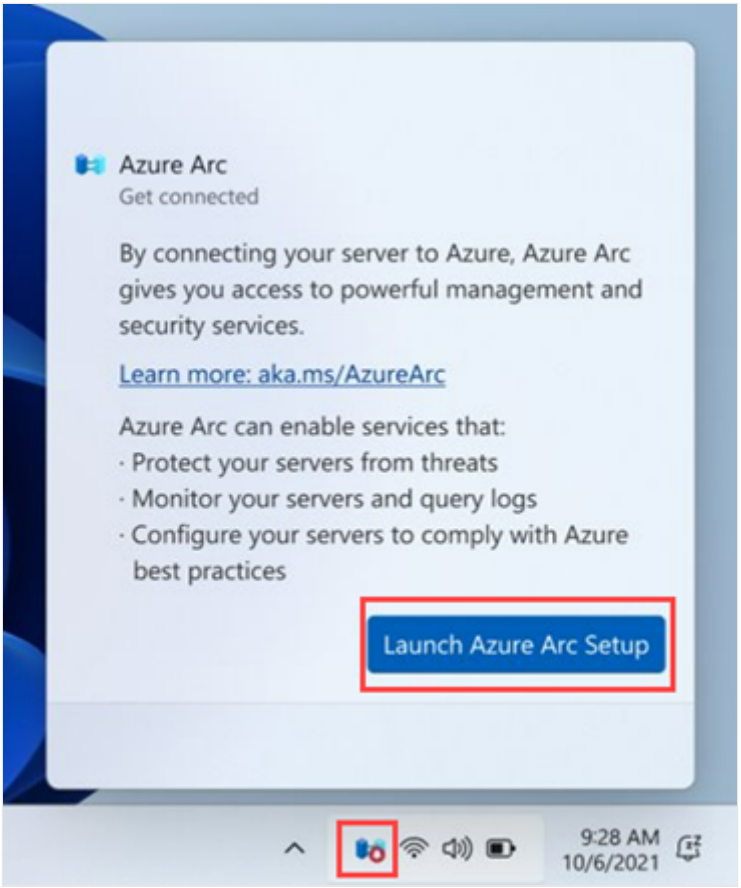
前提条件

- Azure Arc 対応サーバーの前提条件を確認し、サブスクリプション、Azure アカウント、リソースが要件を満たしていることを確認します。
- Azure サブスクリプション。 お持ちでない場合は、開始する前に無料アカウントを作成してください。
- Microsoft Azure への認証用の最新ブラウザー (Microsoft Edge)。 Azure 接続マシン エージェントを構成するには、最新のブラウザーでの対話型認証または別のデバイスでのデバイス コード認証 (コンピューターに最新のブラウザーがない場合) を使用した Azure アカウントへの認証が必要です。

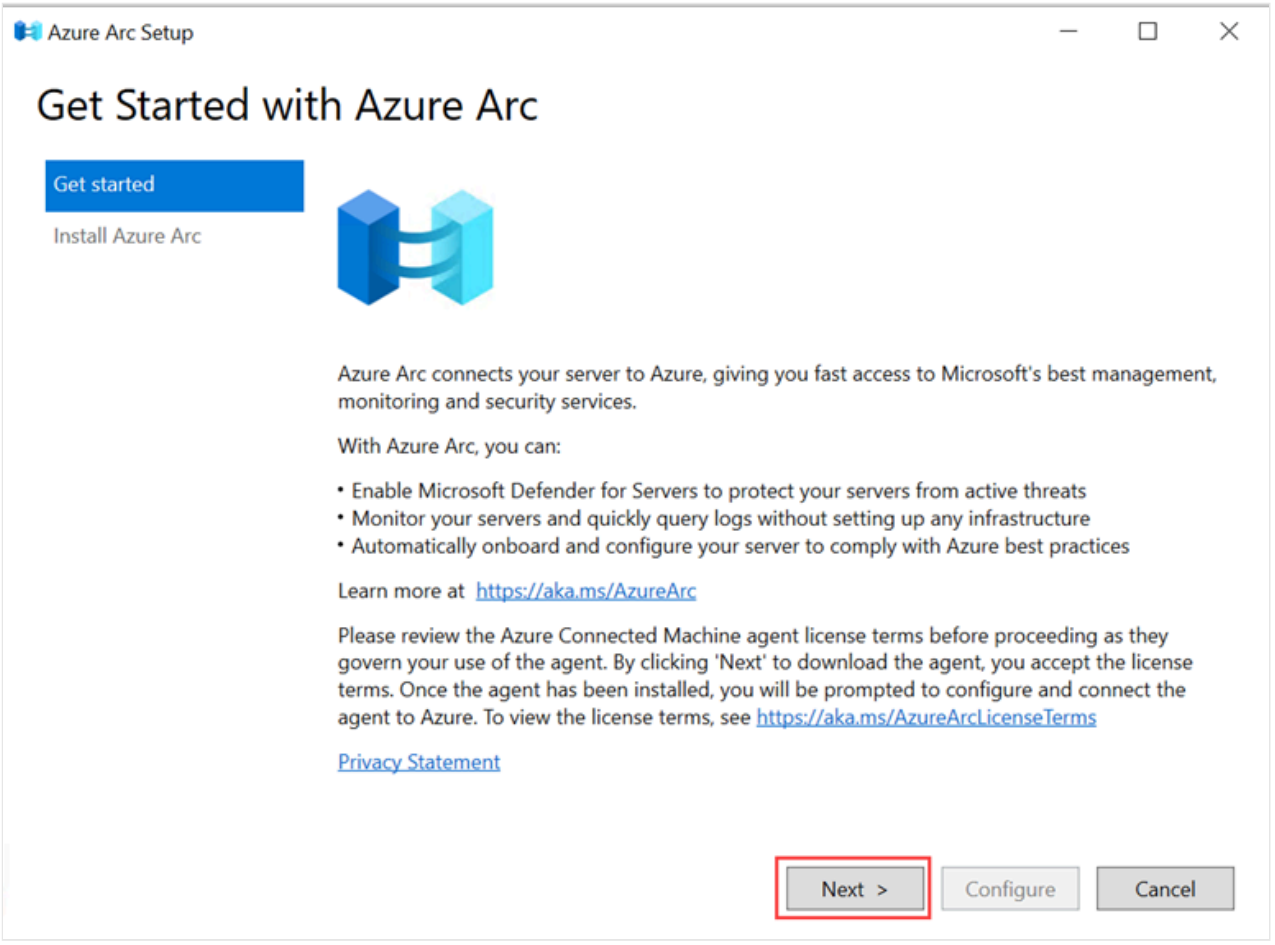
Azure Arc セットアップを起動し、Azure Arc に接続する

Azure Arc セットアップ機能が有効になっている場合、Windows Server マシンの下部にあるシステム トレイ アイコンから Azure Arc セットアップ ウィザードを起動できます。 この機能は、既定で有効になっています。 あるいは、サーバー マネージャーのポップアップ ウィンドウまたは Windows Server の [スタート] メニューから、ウィザードを起動することもできます。

1. Azure Arc システム トレイ アイコンを選択し、[**Launch Azure Arc Setup]\(Azure Arc セットアップの起動\)** を選択します。



2. Azure Arc セットアップ ウィザードの概要ウィンドウでは、マシンを Azure Arc にオンボードする利点について説明します。続行する準備ができたら、[**次へ**] を選択します。



3. ウィザードにより、Windows Server マシンに Azure Connected Machine Agent をインストールするために必要な前提条件が、自動的に確認されます。 このプロセスが完了し、エージェントがインストールされたら、[**構成**] を選択します。

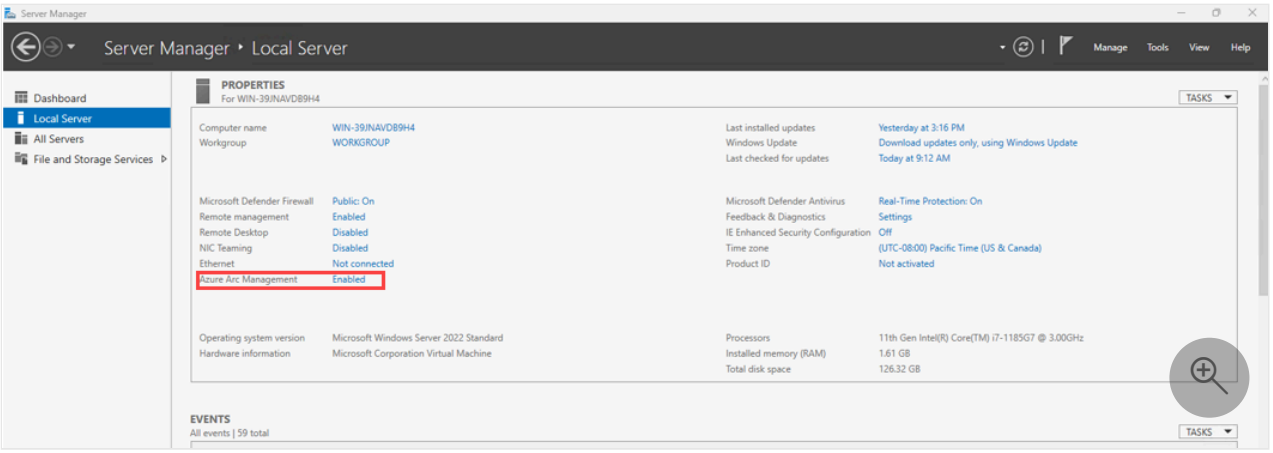
4. 構成ウィンドウでは、Azure Connected Machine エージェントを構成するために必要な手順について説明します。 構成を開始する準備ができたら、[**次へ**] 選択します。

5. 該当する Azure クラウドを選択し、[Azure にサインイン] を選択して **Azure にサインイン**します。 サインイン資格情報を指定します。

6. [**リソースの詳細**] で、テナント、サブスクリプション、リソース グループなど、Azure でのマシンの表示方法の詳細を指定します。 [**次へ**] を選択します。

7. 構成が完了し、マシンが Azure Arc にオンボードされたら、[**完了**] を選択します。

8. サーバー マネージャーに移動し、[**ローカル サーバー**] を選択して、[**Azure Arc による管理**] フィールドにマシンの状態を表示します。 正常にオンボードされたマシンの状態は、[**有効**] になっています。



サーバー マネージャー機能

サーバー マネージャーの **[Azure Arc による管理]** フィールドで **[有効/無効]** リンクを選択すると、マシンの状態に基づいてさまざまな機能を起動できます。

- Azure Arc セットアップがインストールされていない場合、**[有効/無効]** を選択すると、**[役割と機能の追加ウィザード]** が起動します。
- Azure Arc セットアップがインストールされていて、Azure Connected Machine エージェントがインストールされていない場合は、[**無効]** を選択すると、Azure Arc セットアップ ウィザードの実行可能ファイル `AzureArcSetup.exe` が起動します。
- Azure Arc セットアップがインストールされていて、Azure Connected Machine Agent も既にインストールされている場合は、**[有効/無効)** を選択すると、マシンと連携するように Azure Connected Machine Agent を構成するための実行可能ファイルである `AzureArcConfiguration.exe` が起動します。

接続されているマシンを表示する

Windows Server マシンの下部にある Azure Arc システム トレイ アイコンは、マシンが Azure Arc に接続されているかどうかを示します。赤い記号は、マシンに Azure Connected Machine エージェントがインストールされていないことを意味します。

Azure Arc で接続されているマシンを表示するには、アイコンを選択し、[**Azure でマシンを表示**] を選択します。 その後、他の Azure Arc 対応リソースと同様に、Azure portal でマシンを表示できます。

Azure Arc セットアップのアンインストール

> ⓘ Note

Azure Arc セットアップをアンインストールしても、マシンから Azure Connected Machine エージェントはアンインストールされません。 エージェントをアンインストールする手順については、「**Connected Machine Agent の管理と保守**」を参照してください。

Windows Server 2022 コンピューターから Azure Arc セットアップをアンインストールするには、以下の手順に従います。

1. サーバー マネージャーで、 **役割と機能の削除ウィザード**に移動します。
2. [**機能**] ページで、[**Azure Arc セットアップ**] のチェック ボックスをオフにします。
3. 確認ページで、必要に応じて [**移行先サーバーを自動的に再起動**する] を選択し、[削除] を選択 **します**。

PowerShell を使用して Azure Arc セットアップをアンインストールするには、次のコマンドを実行します。

PowerShell

```
Disable-WindowsOptionalFeature -Online -FeatureName AzureArcSetup
```

Windows Server 2025 コンピューターから Azure Arc セットアップをアンインストールするには、以下の手順に従います。

1. コンピューターで [設定] アプリを開き、[**システム**] を選択し、[**オプション機能**] を選択します。
2. **[AzureArcSetup]** 、 **[削除]** の順に選択します。

Windows Server 2025 コンピューターからコマンド ラインを使って Azure Arc Setup をアンインストールするには、次のコード行を実行します。

```
DISM /online /Remove-Capability /CapabilityName:AzureArcSetup~~~~
```

関連コンテンツ

- Azure Connected Machine エージェントのトラブルシューティングを行う方法について説明します。
- 計画と展開ガイドを参照して、任意の規模で Azure Arc 対応サーバーをデプロイし、一元的な管理と監視を実装する計画を立ててください。
- Arc 対応サーバーの従量課金制の Windows Server ライセンスの詳細については、「Windows Server 従量課金制」を参照してください。

Last updated on 2026/02/09

Windows Server の拡張セキュリティ更新プログラム (ESU) を取得する方法

2025/05/23適用対象: ✅ Windows Server 2012, ✅ Windows Server 2012 R2

Extended Security Updates (ESU) for Windows Server include security updates and bulletins rated *critical* and *important*. ESU を使用する前に、「Windows Server 用の拡張セキュリティ更新プログラムの概要 」を参照 して、ESU の概要、使用できる期間、オプションについて理解しておく必要があります。

ESU を取得する方法は、サーバーがホストされている場所によって異なります。 次のオプションを使用して、ESU にアクセスできます。

- **Azure 仮想マシン** - **Azure** でホストされている適用可能な仮想マシン (VM) は自動的に ESU に対して有効になり、これらの更新プログラムは無料で提供されます。MAK キーをデプロイしたり、他のアクションを実行したりする必要はありません。 詳細については、「 Azure の拡張セキュリティ更新プログラム」を参照してください。

- **Azure Arc 対応サーバー** - サーバーがオンプレミスまたはホストされている環境にある場合は、Azure portal から Azure Arc 経由で Windows Server 2012 および 2012 R2 または SQL Server 2012 のマシンを拡張セキュリティ更新プログラムに登録できます。登録すると、Azure サブスクリプション経由で毎月課金されます。 詳細については、「 Azure Arc で有効になっている拡張セキュリティ更新プログラム 」を参照してください。 [1]

- **Azure 以外の物理マシンと仮想マシン** - Azure Arc を使用して接続できない場合は、複数ライセンス認証キー (MAK) を使用して関連するサーバーに適用することで、Azure 以外の VM で拡張セキュリティ更新プログラムを使用します。 この MAK キーを使用すると、セキュリティ更新プログラムを引き続き受け取ることができることが Windows Update サーバーに認識されます。 詳細については、「 Microsoft 365 管理センターから複数のライセンス認証キーにアクセス する」を参照してください。 [1]

[1] When using Azure Arc-enabled servers and non-Azure machines you must purchase ESUs. ESU を購入するには、Enterprise Agreement (EA)、Enterprise Agreement Subscription (EAS)、Enrollment for Education Solutions (EES)、Server and Cloud Enrollment (SCE) などのボリューム ライセンス プログラムを通じてのソフトウェア アシュアランスが必要です。

> ⓘ **注意**
>
> オンプレミスの VM または物理サーバーの ESU を購入した後、複数のライセンス認証キーが使用可能になるまでに 3 ~ 5 営業日かかる場合があります。 組織では、新しいキー

の計画と展開に時間が必要になる場合もあります。 ESU を購入する前に、これらのタイムラインを念頭に置く必要があります。

Azure の拡張セキュリティ更新プログラム

Azure でホストされている適用可能な仮想マシン (VM) は ESU に対して自動的に有効になり、これらの更新プログラムは無料で提供されます。 何も構成する必要はありません。また、Azure VM で ESU を使用しても追加料金は発生しません。 ESU は、更新プログラムを受信するように構成されている場合、Azure VM に自動的に配信されます。

> ⓘ **注意**
>
> 一部の Azure 製品では、拡張セキュリティ更新プログラムも無料です。 これらの製品には、Azure Dedicated Host、Azure VMware Solution、Azure Nutanix Solution、Azure Local、Azure Stack Hub and Edge が含まれます。 これらの製品の一部では、追加の構成が必要になる場合があります。 Contact Microsoft Support for more help.
>
> また、Azure クラシック VM (Microsoft.ClassicCompute) では、ESU の適格性を決定する Azure Instance Metadata Service にアクセスできないため、拡張セキュリティ更新プログラムを受け取るために追加の構成が必要になります。

Azure Arc で有効な拡張セキュリティ・アップデート

Azure Arc 対応サーバーが接続され、Azure Arc を介して ESU に登録されている場合、ESU は Azure Arc 対応サーバーに自動的に配信されます。これは、Azure Arc に接続されている Azure 以外のサーバーにも適用できます。

Azure Policy または Azure portal を使用して大規模に ESU に登録できます。前払い料金はなく、Azure サブスクリプションを通じて毎月課金されます。 プロダクト キーをアクティブ化する必要はありません。

Azure Arc 対応サーバーを使用すると、次のような他の Azure サービスを使用することもできます。

- Azure Update Manager。
- Microsoft Defender for Cloud。
- Azure Policy (マシンの構成)。
- Azure Monitor (VM Insights)。

2023 年 9 月から、Azure Arc 経由で Windows Server 2012 および 2012 R2 ESU をアクティブ化できます。現在、Windows Server 2012 および 2012 R2 サーバーを Azure Arc に接続し、ハイブリッド マシンを Azure Arc 対応サーバーに接続できます。

Arc 対応サーバーで Windows Server 2012 および 2012R2 ESU をアクティブ化する準備をするには、次の手順に従います。

1. Sign in to the Azure portal.
2. 検索バーに「*Servers - Azure Arc*」と入力し、一致するサービス エントリを選択します。
3. 既存の Windows Server 2012 または 2012 R2 マシンを Azure Arc に追加します。Azure Arc 対応サーバーの概要については、ハイブリッド マシンと Azure Arc 対応サーバーの接続に関するページを参照してください。

Azure Arc での ESU の詳細については、「Windows Server 2012 の拡張セキュリティ更新プログラムを提供する準備」および「Windows 2012および 2012 R2 用の拡張セキュリティ更新プログラムを提供する」を参照してください。

Microsoft 365 管理センターから複数のライセンス認証キーにアクセスする

Azure Arc に接続して ESU を適用できないお客様は、Microsoft 365 管理センターで複数のライセンス認証キー (MAK) を使用できます。

1. Microsoft 365 管理センターにサイン インします。
2. [**ボリューム ライセンス**] > [**製品**] > [**契約の表示**] を選択する
3. ESU の購入に使用した契約番号を選択し、その横にある 3 つの点 ([その他の操作] アイコン) を選択し、[**プロダクト キーの表示**] を選択します。 このページに表示される契約で使用できるすべてのプロダクト キー。
4. MAK を取得したら、対象のサーバーに新しいキーをインストールします。 MAK のインストールとアクティブ化の詳細については、Tech Community のブログ投稿「対象となる Windows デバイスの拡張セキュリティ更新プログラムの入手」を参照してください。

拡張セキュリティ更新プログラムのダウンロードとインストール

Windows Server の ESU の配信、ダウンロード、およびアプリケーションは、他の Windows 更新プログラムと同じ違いはありません。 The updates provided through ESUs are only *Security* updates.

ESU をダウンロードしてインストールする前に、最新のサービス スタック更新プログラム (SSU) とライセンス準備パッケージをインストールしておく必要があります。 最新の SSU およびライセンス準備パッケージをインストールするために必要な手順の詳細については、「KB5031043: 延長サポートが 2023 年 10 月 10 日に終了した後もセキュリティ更新プログラムを受け取り続ける手順」を参照してください。

既にインストールされているツールとプロセスを使用して、更新プログラムをインストールできます。 唯一の違いは、前のセクションで生成されたキーにシステムを登録する必要があるということです。 システムが登録されると、更新プログラムがダウンロードされてインストールされます。

Azure でホストされている VM の場合、ESU に対してサーバーを有効にするプロセスは自動的に完了します。 更新プログラムは、追加の構成なしでダウンロードしてインストールする必要があります。

Windows Server 2012 用の拡張セキュリティ更新プログラムを配信する

2025/05/13

この記事では、Arc 対応サーバーにオンボードされている Windows Server 2012 マシンへの拡張セキュリティ更新プログラム (ESU) の配信を有効にする手順について説明します。 ESU はこれらのマシンに対して個別に、または大規模に有効化できます。

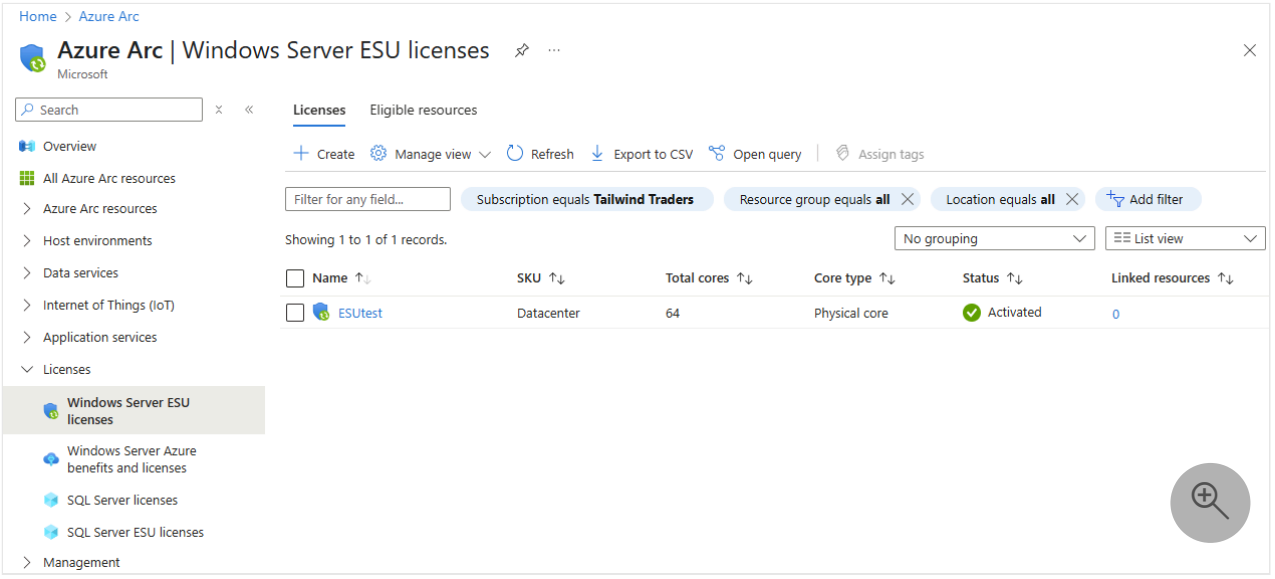
開始する前に

マシンを Azure Arc 対応サーバーにオンボードする計画と準備を行います。 詳細については、「Windows Server 2012 用の拡張セキュリティ更新プログラムの配信の準備」を参照してください。

Arc 対応サーバーに ESU を作成して割り当てるには、Azure RBAC の共同作成者ロールも必要です。

ESU ライセンスを管理する

1. ブラウザーから Azure portal にサインインします。
2. サービス メニューの [**ライセンス**] で、 **Windows Server ESU ライセンスを選択します**。



ここから、ESU **ライセンス**を表示して作成し、ESU の**対象リソース**を表示できます。

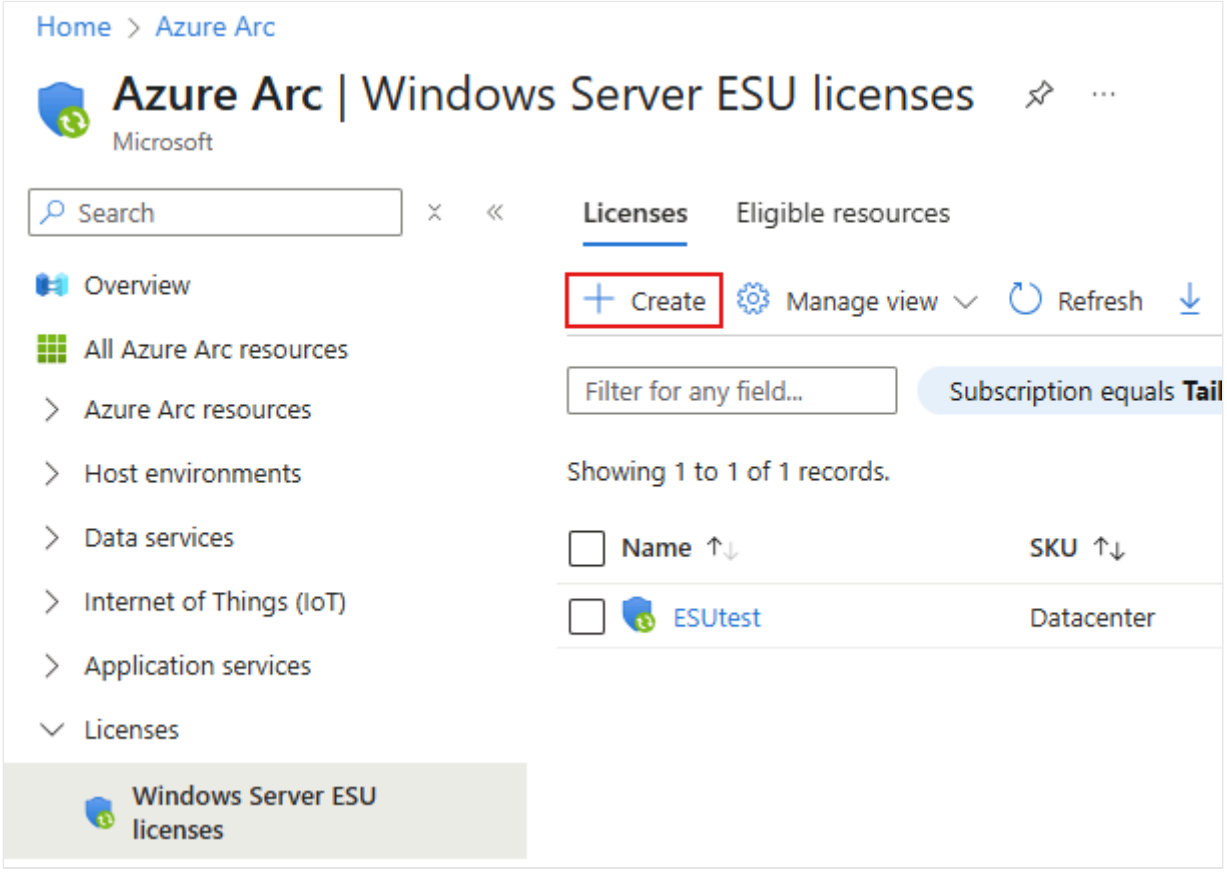
Azure Arc Windows Server 2012 ライセンスを作成する

最初の手順では、Azure Arc から Windows Server 2012 および 2012 R2 拡張セキュリティ更新プログラム ライセンスをプロビジョニングします。これらのライセンスは、次のセクションで選択する 1 つ以上の Arc 対応サーバーにリンクします。

ESU ライセンスをプロビジョニングしたら、ESU ライセンスのプロビジョニングのための SKU (Standard または Datacenter)、コアの種類 (物理または仮想コア)、および 16 コア パックと 2 コア パックの数を指定する必要があります。 また、拡張セキュリティ更新プログラムライセンスを非アクティブな状態でプロビジョニングして、課金が開始されたり、作成時に機能したりしないようにすることもできます。 また、ライセンスに関連付けられているコアは、プロビジョニング後に変更できます。

> **注意**
>
> ESU ライセンスのプロビジョニングには、SA または SPLA でカバーされていることを証明することが必要になります。

[ライセンス] タブには、使用可能な Azure Arc Windows Server 2012 ライセンスが表示されます。 ここから、適用する既存のライセンスを選択するか、新しいライセンスを作成できます。



1. 新しい Windows Server 2012 ライセンスを作成するには、**[作成]** を選択した後に、ページ上でライセンスを構成するために必要な情報を指定します。

   この手順を完了する方法の詳細については、「Windows Server 2012 用の拡張セキュリティ更新プログラムのライセンス プロビジョニング ガイドライン」を参照してください。

2. 指定した情報を確認してから、**[作成]** を選択します。

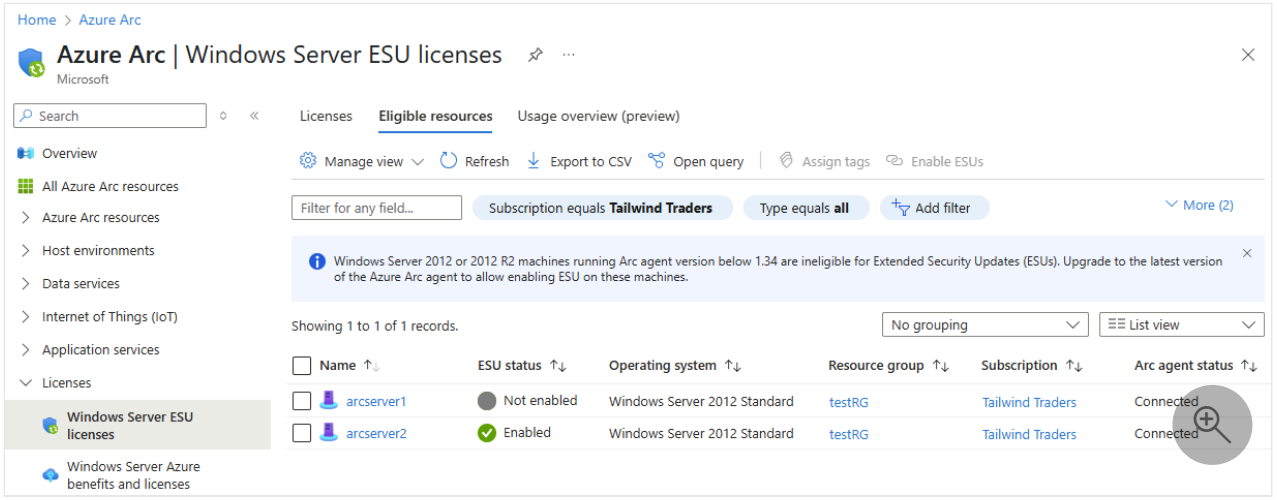
   作成したライセンスが一覧に表示されます。 次のセクションの手順に従って、1 つ以上の Arc 対応サーバーにリンクできます。

ESU ライセンスを Arc 対応サーバーにリンクする

拡張セキュリティ更新プログラム ライセンスにリンクする 1 つ以上の Arc 対応サーバーを選択できます。 アクティブ化された ESU ライセンスにサーバーをリンクすると、サーバーは Windows Server 2012 および 2012 R2 ESU を受け取る資格があります。

> **注意**
>
> これらの更新プログラムを受け取るための自分で選択したパッチ適用ソリューションを柔軟に構成できます。ソリューションは、**更新マネージャー**、Windows Server Update Services、Microsoft Updates、Microsoft Endpoint Configuration Manager、またはサードパーティのパッチ管理ソリューションのいずれでも構いません。

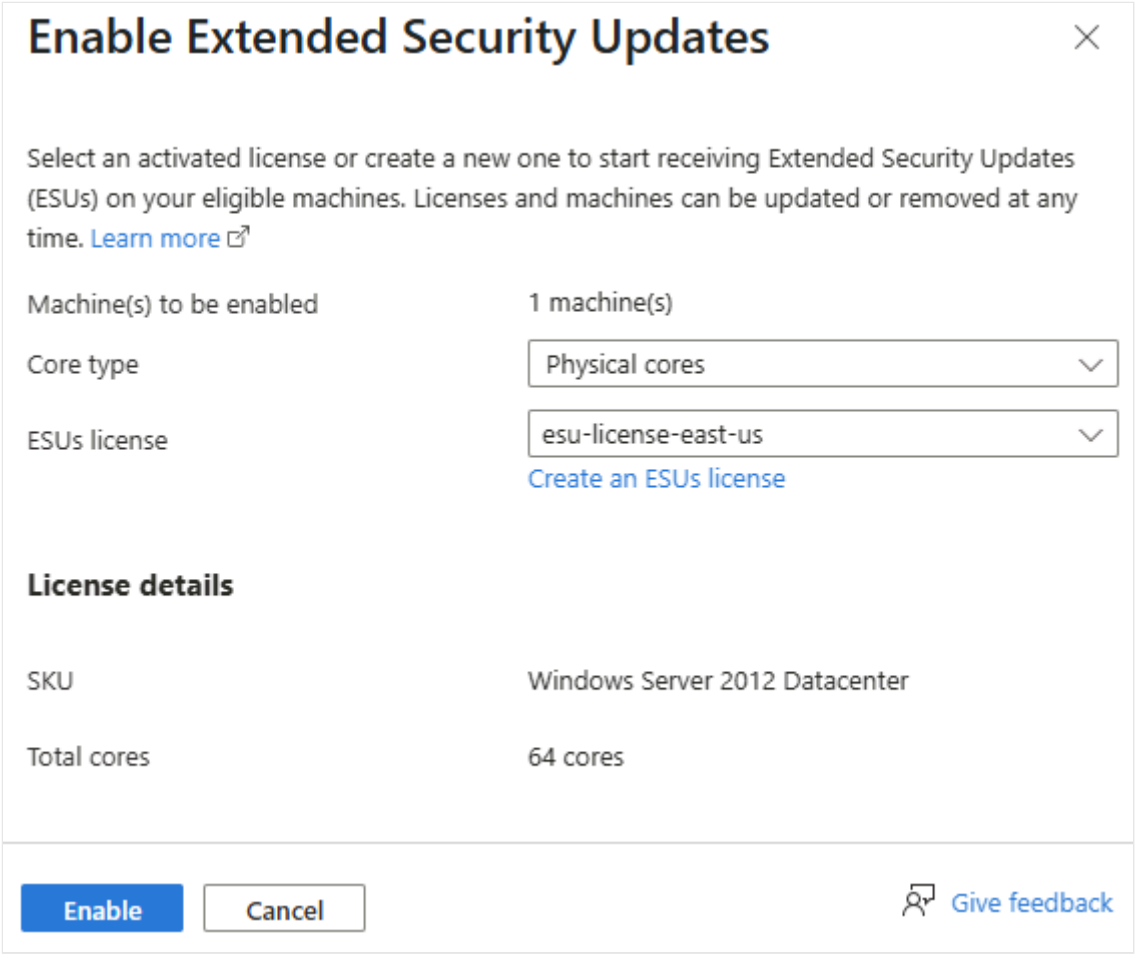
1. [**対象リソース**] タブを選択すると、Windows Server 2012 および 2012 R2 を実行しているすべての Arc 対応サーバーの一覧が表示されます。



ESU 状態列は、マシンが ESU に対して有効になっているかどうかを示します。

2. 1 つ以上のマシンに対して ESU を有効にするには、一覧からそれらを選択してから、**[ESU の有効化]** を選択します。

3. [**拡張セキュリティ更新プログラムの有効化**] ウィンドウには、ESU を有効にするために選択されたマシンの数と、適用できる Windows Server 2012 ライセンスが表示されます。 選択した (複数の) マシンにリンクするライセンスを選択してから、**[有効にする]** を選択します。



> ⓘ **注意**
>
> [ESU ライセンスの作成] を選択すると、既存のライセンスを選択するのではなく、このページから **ライセンスを作成**できます。

[**対象となるリソース**] タブに戻ると、選択したマシンの状態が **[有効] と**表示されます。

有効化プロセス中に問題が発生した場合は、「 Windows Server 2012 の拡張セキュリティ更新プログラムの配信のトラブルシューティング 」を参照してください。

Azure Policy を使用して大規模な ESU を有効にする

サーバーを Azure Arc Extended Security Update ライセンスに大規模にリンクし、ライセンスの変更または作成をロックダウンする場合は、次の組み込みの Azure ポリシーの使用を検討してください。

- 拡張セキュリティ更新プログラム (ESU) ライセンスを有効にして、サポート ライフサイクルが終了した後も Windows 2012 マシンが保護されるようにする (プレビュー)
- 拡張セキュリティ更新プログラム (ESU) ライセンスの作成または変更を拒否する (プレビュー)

Azure ポリシーは、監査と管理の両方のシナリオで、対象のサブスクリプションまたはリソース グループに対して指定できます。

その他のシナリオ

追加コストなしで拡張セキュリティ更新プログラムのパッチを受け取る対象となるシナリオがいくつかあります。 Azure Arc でサポートされているこれらのシナリオの 2 つに、 Dev/Test (Visual Studio) と ディザスター リカバリー (ソフトウェア アシュアランス または サブスクリプションからの DR インスタンスの特典のみ) があります。 どちらのシナリオでも、課金対象の実稼働マシンに対して Azure Arc によって有効になっている Windows Server 2012/R2 ESU を既に使用している必要があります。

> ⚠ **警告**
>
> Dev/Test ワークロードまたはディザスター リカバリー ワークロードのみのための Windows Server 2012/R2 ESU ライセンスを作成しないでください。 ESUライセンスは、非課金のワークロードに対してのみプロビジョニングするべきではありません。 さらに、ESU ライセンスでプロビジョニングされたすべてのコアに対して完全に課金されます。また、そのライセンスの Dev/Test コアは、次の条件に基づいてタグ付けされている限り課金されません。

これらのシナリオに該当するには、以下を持っている必要があります:

- **課金対象の ESU ライセンス。** 運用環境で実行されている通常の Azure Arc 対応サーバー (通常は課金される ESU シナリオなど) にリンクすることを目的とした WS2012 Arc ESU ライセンスを既にプロビジョニングしてアクティブ化している必要があります。 このライセンスは、たとえば Dev/Test コアなど、無料の拡張セキュリティ更新プログラムの対象となるコアではなく、課金対象のコアに対してのみプロビジョニングする必要があります。

- **Arc 対応サーバー。** Visual Studio サブスクリプションまたはディザスター リカバリーを使用した Dev/Test を目的として、Windows Server 2012 および Windows Server 2012 R2

マシンを Azure Arc 対応サーバーにオンボードされているもの。

追加コストなしで ESU の対象となる Azure Arc 対応サーバーを登録するには、以下の手順に従ってタグ付けとリンクを行います:

1. WS2012 Arc ESU ライセンス (運用環境用に作成され、運用環境サーバー専用のコアを持つ運用環境用に作成) と非運用環境の Azure Arc 対応サーバーの両方に、適切な例外に対応する次のいずれかの名前と値のペアにタグを付けます。

   a. 名前: "ESU Usage"; 値: "WS2012 VISUAL STUDIO DEV TEST"

   b. 名前: "ESU Usage"; 値: "WS2012 DISASTER RECOVERY"

   複数の例外シナリオで ESU ライセンスを使用している場合は、ライセンスに次のタグを付けてください。名前: "ESU 使用状況"; 値: "WS2012 多目的"

2. タグ付けされたライセンス (運用環境サーバー専用のコアを持つ運用環境用に作成) を、タグ付けされた非運用環境の Azure Arc 対応 Windows Server 2012 および Windows Server 2012 R2 マシンにリンクします。 **これらのサーバーのコアのライセンスを付与したり、これらのサーバー専用の新しい ESU ライセンスを作成したりしないでください。**

このリンクは、コンプライアンス違反や強制ブロックをトリガーせず、プロビジョニングされたコアを超えてライセンスの適用を拡張できます。 このライセンスには、実稼働サーバーと課金対象サーバーのコアのみが含まれていることが想定されています。 追加のコアはいずれも課金され、超過課金が発生します。

> ⓘ **重要**
>
> これらのタグをライセンスに追加しても、ライセンスは無料になりません。また、課金対象のライセンス コアの数も減らされません。 これらのタグを使用すると、新しいライセンスを作成したり、無料のマシンにコアを追加したりする必要なく、支払い対象コアが既に構成されている既存のライセンスに Azure マシンをリンクできます。

例:

- 8 つの Windows Server 2012 R2 Standard インスタンスがあり、それぞれに 8 つの物理コアがあります。 これらの Windows Server 2012 R2 Standard マシンのうち 6 台は運用環境用です。また、オペレーティング システムは Visual Studio Dev Test サブスクリプションを通じてライセンスが付与されているため、これらの Windows Server 2012 R2 Standard マシンのうち 2 台は無料 ESU の対象となります。
  - 最初に、6 台の運用マシンをカバーするために、Standard エディションで物理コアが 48 個ある Windows Server 2012/R2 の通常の ESU ライセンスをプロビジョニングして

アクティブ化する必要があります。 この通常の運用 ESU ライセンスは、6 台の運用サーバーにリンクする必要があります。
- 次に、この既存のライセンスを再利用し、コアを追加したり、別のライセンスをプロビジョニングしたりせず、このライセンスを 2 台の非運用環境の Windows Server 2012 R2 標準マシンにリンクする必要があります。 ESU ライセンスと2台の非運用 Windows Server 2012 R2 Standard マシンに、Name: "ESU Usage"、Value: "WS2012 VISUAL STUDIO DEV TEST" というタグを付けてください。
- これにより、48 コアの ESU ライセンスが取得され、それらの 48 コアに対して課金されます。 ESU ライセンスと開発テスト サーバー リソースが適切にタグ付けされている限り、このライセンスに追加した開発テスト サーバーの追加の 16 コアに対して課金されることはありません。

> **注意**
>
> まず、通常の運用ライセンスが必要です。実稼働コアに対してのみ課金されます。

Windows Server 2012/2012 R2 からのアップグレード

Windows Server 2012/2012R マシンを Windows Server 2016 以降にアップグレードする場合、そのマシンから Connected Machine エージェントを削除する必要はありません。 アップグレードが完了してから数分以内に、Azure にマシンの新しいオペレーティング システムが表示されます。 アップグレードされたマシンは ESU を必要としなくなり、それらの対象ではなくなります。 マシンに関連付けられている ESU ライセンスは、マシンから自動的にはリンク解除されません。 それを手動で行う手順については、「ライセンスのリンクを解除する」を参照してください。

WS2012 ESU パッチの状態を評価する

Azure Arc 対応サーバーに最新の Windows Server 2012/R2 拡張セキュリティ更新プログラムが適用されているかどうかを検出するには、Azure Policy 拡張セキュリティ更新プログラムを Windows Server 2012 Arc コンピューターにインストールする必要があります。 このポリシー定義は、マシン構成を利用して、サーバーが最新の ESU パッチを受信したかどうかを識別します。 これは、Azure portal に組み込まれているゲスト割り当てビューと Azure Policy コンプライアンス ビューから監視できます。

Azure Local で Azure Edition 仮想マシンのホットパッチを有効にする

2024/12/21適用対象: ✅ Windows Server 2022 Datacenter: Azure Edition hosted on Azure Local

Windows Server 2022 Datacenter のホットパッチ: Azure Local でホストされている Azure Edition 仮想マシン (VM) を使用すると、インストール後に再起動を必要とせずに、AZURE Local 上の ISO にデプロイされたマシンにセキュリティ更新プログラムをインストールできます。 ホットパッチは、デスクトップ エクスペリエンスと Server Core の両方で使用できます。 この記事では、ISO を使用してオペレーティング システムをインストールまたはアップグレードした後にホットパッチを構成する方法について説明します。

> ⓘ **注意**
>
> Azure Marketplace を使用する場合は、この記事の手順に従わないようにしてください。 代わりに、Azure Marketplace にあるホットパッチに対応した以下のイメージを使用してください。
>
> - Windows Server 2022 Datacenter: Azure Edition ホットパッチ - Gen2
> - Windows Server 2022 Datacenter: Azure Edition Core - Gen2

Azure Local で ISO でデプロイされたマシンにホットパッチを使用する場合、ホットパッチ エクスペリエンスと Azure VM 用 Azure Automanage の一部としてのホットパッチの使用に比べて、いくつかの重要な違いがあります。

次のような相違点があります。

- ホットパッチ構成は、Azure Update Manager 経由では使用できません。
- ホットパッチを無効にすることはできません。
- 自動修正プログラムのオーケストレーションは使用できません。
- オーケストレーションは手動で実行する必要があります (たとえば、SConfig 経由の Windows Updateを使用)。

前提条件

ホットパッチを有効にするには、開始する前に次の前提条件を準備しておく必要があります。

- Windows Server 2022 Datacenter: Azure の特典が有効になっている Azure や Azure Local など、サポートされているプラットフォームでホストされている Azure Edition。
  - Azure Local はバージョン 21H2 以降である必要があります。

- 新しい仮想マシンのホットパッチに関する記事の「ホットパッチのしくみ」セクションを確認してください。
- 送信ネットワーク アクセス、または次のエンドポイントへの HTTPS (TCP/443) トラフィックを許可する送信ポートの規則。
  - `go.microsoft.com`
  - `software-static.download.prss.microsoft.com`

コンピューターを準備する

VM のホットパッチを有効にする前に、次の手順を使用してコンピューターを準備する必要があります。

1. コンピューターにサインインします。 Server Core を使用している場合は、SConfig メニューからオプション **15** を入力し、`Enter` キーを押して PowerShell セッションを開きます。 デスクトップ エクスペリエンスを使用している場合は、VM にリモート デスクトップ接続し、PowerShell を起動します。

2. 次の PowerShell コマンドを実行して、適切なレジストリ設定を構成することで、仮想化ベースのセキュリティを有効にします。

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "EnableVirtualizationBasedSecurity"
       Value = "0x1"
       Force = $True
       PropertyType = "DWORD"
   }
   New-ItemProperty @parameters
   ```

3. コンピューターを再起動します。

4. 次の PowerShell コマンドを実行して、レジストリでホットパッチ テーブルのサイズを構成します。

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session
   Manager\Memory Management"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "HotPatchTableSize"
       Value = "0x1000"
       Force = $True
   ```

```
    PropertyType = "DWORD"
}
New-ItemProperty @parameters
```

5. 次の PowerShell コマンドを実行して、レジストリでホットパッチの Windows Update エンドポイントを構成します。

```PowerShell
$registryPath = "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Update\TargetingInfo\DynamicInstalled\Hotpatch.amd64"
$nameParameters = $parameters = @{
    Path = $registryPath
    Name = "Name"
    Value = "Hotpatch Enrollment Package"
    Force = $True
}
$versionParameters = $parameters = @{
    Path = $registryPath
    Name = "Version"
    Value = "10.0.20348.1129"
    Force = $True
}
New-Item $registryPath -Force
New-ItemProperty @nameParameters
New-ItemProperty @versionParameters
```

これでコンピューターの準備が完了したので、ホットパッチ サービス パッケージをインストールできます。

ホットパッチ サービス パッケージをインストールする

> ⚠ **注意**
>
> 現在、ホットパッチの前提条件 KB は Microsoft Update カタログに公開されていません。

ホットパッチ更新プログラムを受信できるようにするには、ホットパッチ サービス パッケージをダウンロードしてインストールする必要があります。 PowerShell セッションで、次の手順を実行します。

1. 次の PowerShell コマンドを使用して、Microsoft Update カタログから (KB5003508) Microsoft Update スタンドアロン パッケージをダウンロードし、コンピューターにコピ

ーします。

```PowerShell
$parameters = @{
      Source = "https://go.microsoft.com/fwlink/?linkid=2211714"
      Destination = ".\KB5003508.msu"
}
Start-BitsTransfer @parameters
```

2. スタンドアロン パッケージをインストールするために、次のコマンドを実行します。

```PowerShell
wusa.exe .\KB5003508.msu
```

3. 画面の指示に従います。 完了したら、[終了] を選択します。

4. インストールを確認するために、次のコマンドを実行します。

```PowerShell
Get-HotFix | Where-Object {$_.HotFixID -eq "KB5003508"}
```

> ⚠ **注意**
>
> Server Core を使用すると、更新プログラムは既定で手動でインストールされるように設定されます。 この設定は、SConfig ユーティリティを使用して変更できます。

次のステップ

これでコンピューターをホットパッチ用に設定しました。コンピューターの更新に役立つ記事をいくつか次に示します。

- Server Core インストールにパッチを適用する。
- 「Windows Server Update Services (WSUS)」の詳細を確認します。

Azure Arc 対応サーバーのホットパッチを有効にする

適用対象: ✅ Windows Server 2025

> **ⓘ 重要**
>
> Windows Server 2025 用 Azure Arc 対応ホットパッチは、月額サブスクリプション料金で利用できるようになりました。 価格について詳しく知るには、**再起動にうんざりですか？ Windows Server のホットパッチを取得**を参照してください。

ホットパッチを使用すると、インストール後にユーザーを再起動しなくても、Windows Server のインストールを更新できます。 この機能により、更新に費やされるダウンタイムを最小限に抑え、ユーザーがワークロードを中断なく実行し続けます。 ホットパッチのしくみの詳細については、「Windows Server用ホットパッチ」を参照してください。

Windows Server 2025 には、Azure Arc 対応サーバーに対してホットパッチを有効にする機能が用意されています。 Azure Arc 対応サーバーでホットパッチを使用するには、Connected Machine エージェントをデプロイし、Windows Server ホットパッチを有効にする必要があります。 この記事では、ホットパッチを有効にする方法について説明します。

Prerequisites

Windows Server 2025 の Arc 対応サーバーでホットパッチを有効にするには、次の要件を満たす必要があります。

- サーバーが Windows Server 2025 (ビルド 26100.1742 以降) を実行している必要があります。 プレビュー バージョンまたは Windows Server Insider ビルド はサポートされていません。これは、プレリリース オペレーティング システム用にホットパッチが作成されていないためです。

- コンピューターは、次のいずれかのエディションの Windows Server を実行している必要があります。
  - Windows Server 2025 Standard
  - Windows Server 2025 Datacenter
  - Windows Server 2025 Datacenter: Azure Edition。 このエディションは Azure Arc 対応である必要 **はありません** 。ホットパッチは既定で既に有効になっています。 残りの技術的な前提条件は引き続き適用されます。

- **Server with Desktop Experience** と **Server Core** インストール オプションの両方がサポートされています。

- ホットパッチを有効にする物理マシンまたは仮想マシンは、仮想セキュア モード (VSM) とも呼ばれる仮想化ベースのセキュリティ (VBS) の要件を満たす必要があります。 少なくとも、マシンはセキュア ブートが有効になっている Unified Extensible Firmware Interface (UEFI) を使用する必要があります。 そのため、Hyper-V 上の仮想マシン (VM) の場合は、第 2 世代仮想マシン である必要があります。

- Azure サブスクリプション。 まだお持ちでない場合は、開始する前に 無料アカウント を作成してください。

- サーバーとインフラストラクチャは、サーバーで Azure Arc を有効にするために 接続マシン エージェントの前提条件を満たしている必要があります。

- マシンは Azure Arc (Arc 対応) に接続されている必要があります。 マシンを Azure Arc にオンボードする方法の詳細については、Azure Connected Machine エージェントのデプロイ オプション に関するページを参照してください。

必要に応じて仮想セキュア モードを確認して有効にする

Azure ポータルを使用してホットパッチを有効にすると、マシン上で仮想セキュア モード (VSM) が実行されているかどうかの確認が行われます。 VSM が実行されていない場合、ホットパッチの有効化は失敗し、VSM を有効にする必要があります。

または、ホットパッチを有効にする前に、VSM の状態を手動で確認することもできます。 VSM に依存する他の機能 (ホットパッチなど) を以前に構成した場合、VSM は既に有効になっている可能性があります。 このような機能の一般的な例としては、 Credential Guard や 、コード整合性の仮想化ベースの保護 (ハイパーバイザーで保護されたコード整合性 (HVCI) とも呼ばれます) があります。

> **ヒント**
>
> グループ ポリシーまたは別の一元管理ツールを使用して、次の 1 つ以上の機能を有効にすることができます。
>
> - **クレデンシャル ガード**
> - **Credential Guard によるマシン アカウントの保護**
> - **仮想化ベースのコード整合性の保護**
> - **System Guard Secure Launch と SMM 保護**
> - **カーネルモードのハードウェアによるスタック保護**
> - **セキュリティで保護されたコア サーバー**

これらの機能のいずれかを構成すると、VSM も有効になります。

VSM が構成され、実行されていることを確認するには、任意の方法を選択し、出力を確認します。

PowerShell

PowerShell

```
Get-CimInstance -Namespace 'root/Microsoft/Windows/DeviceGuard' -ClassName
'win32_deviceGuard' | Select-Object -ExpandProperty
'VirtualizationBasedSecurityStatus'
```

コマンド出力が `2` されている場合は、VSM が構成され、実行されます。 この場合は、Windows Server 2025 でホットパッチを有効にするに直接進みます。

出力が `2` されていない場合は、VSM を有効にする必要があります。

▼ VSM を有効にするには、このセクションを展開します。

次のいずれかのコマンドを使用して VSM を有効にします。

PowerShell

PowerShell

```
New-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\DeviceGuard' -
Name 'EnableVirtualizationBasedSecurity' -PropertyType 'Dword' -Value 1 -Force
```

ヒント

VSM を有効にした後、サーバーを再起動する必要があります。

再起動した後、次のコマンドをもう一度実行して、出力が `2` されていることを確認して、VSM が実行されていることを確認します。

PowerShell

PowerShell

PowerShell

```
Get-CimInstance -Namespace 'root/Microsoft/Windows/DeviceGuard' -ClassName
'win32_deviceGuard' | Select-Object -ExpandProperty
'VirtualizationBasedSecurityStatus'
```

出力がまだ `2` でない場合は、コンピューターの VSM に問題がある可能性があるため、調査が必要です。 最も可能性の高い理由は、物理または仮想 ハードウェアの要件 が満たされていないことです。 ハードウェアまたは仮想化プラットフォームのベンダーのドキュメントを参照してください。 たとえば、VMware vSphere のドキュメントには、既存の仮想マシン に対する仮想化ベースのセキュリティを有効化する方法が記載されています。

VSM を正常に有効にし、それが実行されていることを確認したら、次のセクションに進みます。

Windows Server 2025 でホットパッチを有効にする

1. 以前に Arc が有効になっていない場合は、マシンを Azure Arc に接続します。
2. マシンを Azure Arc に接続したら、Azure Arc ポータルにサインインし、 **Azure Arc** → Machines に移動 **します**。
3. お使いのコンピュータの名前を選択します。
4. [**ホットパッチ**] を選択し、[確認] を選択**します**。
5. 変更が適用されるまで約 10 分待ちます。 更新プログラムが 保留中 の状態のままである場合は、 Azure Arc エージェントのトラブルシューティングに進みます。

Windows Server 2025 でのホットパッチの使用

Windows Update からホットパッチを入手できる場合は常に、インストールを求めるメッセージが表示されます。 これらの更新プログラムは毎月リリースされないため、次のホットパッチが公開されるまで待つ必要がある場合があります。

必要に応じて、Azure Update Manager (AUM) などの更新管理ツールを使用してホットパッチのインストールを自動化できます。

既知の問題

2025 年 10 月にリリースされた複数の更新プログラム

2025 年 10 月、Microsoft は一部の Windows Server ユーザーに提供された更新プログラムをいくつかリリースしました。 ホットパッチに登録した場合、または登録する予定で、2025 年 11 月と 12 月にホットパッチ更新プログラムをインストールする予定の場合は、Windows Server マシンが次のいずれかの更新 **レベルで実行** されていることを確認します。

- 2025 年 10 月 14 日 - **KB5066835** (OS ビルド 26100.6899)
- 2025 年 10 月 24 日 - Windows Server Update Services の **KB5070893** (OS ビルド 26100.6905) セキュリティ更新プログラム

他の 10 月の更新プログラムのいずれかがインストールされている場合は、現在 2026 年 1 月に予定されている次のベースライン月まで、および次の基準月を含む、定期的な非ホットパッチ更新プログラムが発生します。 これらの更新プログラムは、毎月再起動する必要があります。 特に、次の更新プログラムがインストールされている場合、マシンは今後のホットパッチと互換性がありません: 2025 年 10 月 23 日 - **KB5070881** (OS ビルド 26100.6905) 帯域外、およびその他の更新プログラムはこのセクションに明示的に記載されていません。

2025 年 10 月の更新プログラムでの機能ライセンスの問題

Windows Server 2025 の 2025 年 10 月のセキュリティ更新プログラムで問題が特定されました。 これは 、2025 年 10 月 14 日から KB5066835 (OS ビルド 26100.6899) 以降の更新プログラムを実行しているお客様に影響を与える可能性があります。 この問題により、次の予期しない動作が発生する可能性があります。

- 新しいマシンで Azure Arc 経由で Windows Server ホットパッチを有効にすると、正常に失敗するか、完了しない可能性があります。 代わりに、問題が解決されるまで、機能の有効化は "進行中" 状態のままになります。
- 以前に Windows Server ホットパッチが有効になっているマシンでは、機能ライセンスの有効期限が切れる可能性があり、これにより次のホットパッチがインストールされなくなります。 代わりに、アクションが実行されない場合、次の更新によって再起動が発生します。

Windows Server 2025 Datacenter: Azure Edition でのホットパッチは、この問題の影響を受けません。

この問題を解決するには、一連の手動手順をお勧めします。 いずれかの回避策を適用しないと、現在 2026 年 1 月に予定されている次のベースライン月まで、および次のベースライン月を含む、定期的な非ホットパッチ更新が発生します。 これらの更新プログラムは、毎月再起動する必要があります。

影響を受けるマシンに手動による回避策を適用するには、2 つの方法があります。 提供される各オプションは、完全なソリューションを提供します。 次の更新プログラムが提供される **前** に、影響を受ける各マシンに回避策を適用する必要があります。これは、 **2025 年 11 月 11**

日の次の "パッチ火曜日" 日に予定されています。 回避策を適用するには再起動が必要なので、それに応じて計画してください。

いずれかの回避策を適用すると、2025 年 11 月と 12 月にリリースされたホットパッチ更新プログラムは、再起動を必要とせずにインストールされます。

オプション 1: ローカル ポリシーまたはグループ ポリシーを使用して修復を有効にする

1. Windows 11 24H2、Windows 11 25H2、および Windows Server 2025 KB5062660 251028_18301 機能プレビュー パッケージをダウンロードしてインストールします。 これにより、この特定の修復用のローカル ポリシー テンプレートまたはグループ ポリシー テンプレート (`ADMX` ファイル) がインストールされます。

2. [**スタート**] **を**選択し、「 **gpedit**」と入力し、[**グループ ポリシーの編集**] を選択します。 **コンピューターの構成\管理用テンプレート\KB5062660 251028_18301 機能プレビュー\Windows 11 バージョン 24H2、25H2\KB5062660 251028_18301 機能プレビュー**に移動します。

   この特別なグループ ポリシーの展開と構成の詳細については、「 グループ ポリシーを使用して、既定で無効になっている更新プログラムを有効にする」を参照してください。

3. 右側のウィンドウ ウィンドウ **で、KB5062660 251028_18301 機能プレビューを**開き、[**有効**] を選択し、[**OK**] **を選択します**。

4. 影響を受けるコンピューターを再起動します。

5. 次のコマンドを実行して、 **レジストリから** DeviceLicensingServiceCommandMutex エントリを削除します。 このエントリが影響を受けるデバイスに存在しない場合、削除は無視されます。

   PowerShell

   ```
   try {
   Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
   NT\CurrentVersion\Subscriptions' -Name 'DeviceLicensingServiceCommandMutex' -
   ErrorAction Stop
   } catch {
   Write-Host "DeviceLicensingServiceCommandMutex entry not present, skipping
   removal."
   }
   ```

   または、好みのレジストリ編集ツールまたはオートメーション ソリューションを使用して、同じ値を削除します。 レジストリ キー全体を削除しないでください。

オプション 2: スクリプトを使用して修復を有効にする

影響を受ける各マシンで管理者特権の PowerShell ウィンドウを開き、次のコマンドを実行します。 最後のコマンドでは、デバイスを再起動するように求められます。 この軽減策は、マシンが再起動されるまで完了せず、このスクリプトを実行した直後に再起動することをお勧めします。

PowerShell

```
Stop-Service -Name 'HIMDS'
New-Item -Path
'HKLM:\SYSTEM\CurrentControlSet\Policies\Microsoft\FeatureManagement\Overrides' -
Force
New-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Policies\Microsoft\FeatureManagement\Overrides' -
PropertyType 'dword' -Name '4264695439' -Value 1 -Force
try {
  Remove-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Subscriptions' -Name 'DeviceLicensingServiceCommandMutex' -
ErrorAction Stop
} catch {
  Write-Host "DeviceLicensingServiceCommandMutex entry not present, skipping
removal."
}
Restart-Computer -Confirm
```

次のステップ

ホットパッチが有効になったので、コンピューターの更新に役立つ記事をいくつか紹介します。

- Windows Server のホットパッチ
- Server Core のインストールにパッチを適用する
- VM ゲストの自動パッチ適用
- Azure Update Manager

Last updated on 2025/10/31

Windows のリリースの正常性

Windows 更新プログラムとサービス マイルストーンに関する公式の情報をすばやく見つけます。 次の更新プログラムの計画に役立つ、既知の問題とセーフガードに関するリソース、ツール、ニュースにアクセスします。 最新の Windows のリリース正常性更新プログラムが必要ですか? X の @WindowsUpdate に従います。

GET STARTED
バージョン 25H2 Windows 11を取得する...

WHAT'S NEW
Windows 11バージョン 25H2 の IT 担当者...

DEPLOY
2026 年に期限切れになる証明書のセキュア...

GET STARTED
新しい Windows 11回復オプション...

REFERENCE
Windows 11ロードマップ: 新機能と今後の...

OVERVIEW
Windows の月次更新プログラムについて

メッセージ センター

- Windows 展開サービス (WDS): ハンズフリー展開の強化 (フェーズ 2)
- 管理アクションの強化: Windows イメージング、複製、認証ワークフロー
- Windows 営業時間: 2026 年 4 月 16 日

その他を表示 >

Windows 11バージョン 26H1

- 既知の問題
- 解決した問題
- リリース ノート
- Windows 11 リリース情報
- バージョン 26H1 Windows 11について知っておくべきこと

Windows 11、バージョン 25H2

- 既知の問題
- 解決した問題
- リリース ノート
- Windows 11 リリース情報

Windows 11 バージョン 24H2

- 既知の問題
- 解決した問題
- リリース ノート
- Windows 11 リリース情報

バージョン 25H2 Windows 11を取得する方法

バージョン 24H2 Windows 11を取得する方法

Windows 10 バージョン 22H2

- 既知の問題
- 解決した問題
- リリース ノート
- Windows 10 リリース情報
- バージョン 22H2 Windows 10を取得する方法

Windows Server 2025

- 既知の問題
- 解決した問題
- リリース ノート
- Windows Server のリリース情報
- Windows Server 2025 の新機能

Windows Server 2022

- 既知の問題
- 解決した問題
- リリース ノート
- Windows Server のリリース情報
- Windows Server 2022 の新機能

追加バージョン

サポートされている他のバージョンの Windows および Windows Server の既知の問題と解決した問題の詳細を参照してください。

- 既知の問題: 以前のバージョン

質問がありますか? 営業時間に参加する

カスタマイズされたガイダンス、ヒントとテクニック、および質問への回答を入手してください。

フィードバックの送信

既存の機能についての考えや、フィードバック Hub を介した新しい機能のアイデアを共有してください。

ヘルプを参照する

Windows デバイスで Get Help アプリを開き、一般的な問題のトラブルシューティングを行うリソースを見つけます。

Windows Server - ライセンス条項

2025/07/14

Windows Server 関連のライセンス条項を確認します。

- Windows Server 2016 用の追加ソフトウェア
- Windows Server Technical Preview の有効期限
- Windows Server 2016 Technical Preview ライセンス条項
- Microsoft ソフトウェア ライセンス条項 - MICROSOFT。WINDOWSSERVER。SYSTEMINSIGHTS
- Microsoft ソフトウェア ライセンス条項 - MICROSOFT。WINDOWSSERVER。SYSTEMINSIGHTS。資格
- Windows Admin Center - ライセンス条項