سیستم‌عاملی برای کلاود، مرکزداده و سرور

نگاهی به ویژگی‌های جدید ویندوز سرور ۲۰۱۶ (بخش اول)

یکی از محصولات بسیار معروف و درآمدزای مایکروسافت، ویندوز سرور است. تعداد زیادی ویندوز سرور در فضای یک مرکز داده نصب می‌شوند و هر کدام از آن‌ها، بر اساس قابلیت‌ها و نسخه‌ها، هزینه متفاوتی دارند. از گذشته تا امروز، مایکروسافت سعی کرده است ویندوز سرور را به یک راه‌حل نرم‌افزاری همه‌فن‌حریف تبدیل کند که مهندسان شبکه بتوانند به جای استفاده از نرم‌افزارهای واسط، نیازهای خود را با کمک ویندوز سرور پاسخ دهند. در هر نسخه از ویندوز سرور، شاهد پیشرفت‌های چشمگیری در قابلیت‌های این سیستم‌عامل بوده‌ایم. طبق سنت مایکروسافت، در اول اکتبر 2014، اولین نسخه پیش‌نمایش از این سیستم‌عامل در دسترس عموم قرار گرفت. بعد از اولین پیش‌نمایش فنی، چهار پیش‌نمایش دیگر عرضه شد تا مهندسان شبکه با قابلیت‌های جدید این سیستم‌عامل آشنا شوند. حال پس از گذشت دو سال از انتشار اولین پیش‌نمایش فنی، در اول اکتبر 2016، نسخه نهایی این سیستم‌عامل عرضه شد.

در آوریل 2003، مایکروسافت نسخه‌ای از ویندوز را منتشر کرد که با ویندوزی که کاربران می‌شناختند، متفاوت بود. این ویندوز قابلیت‌های ویژه‌ای برای ایجاد شبکه‌های کامپیوتری داشت. مایکروسافت نام این ویندوز را به دلیل ساختار ارتباطی آن، «سرور» نهاد. ویندوز سرور به سایر کامپیوترها خدمات ارائه می‌کرد. از آن زمان تاکنون، همیشه آخرین تکنولوژی‌ها و دستاوردها در نسخه‌های ویندوز سرور گنجانده می‌شود تا همچنان در پیاده‌سازی زیرساخت‌های شبکه، گزینه‌ای بدون رقیب باشد. پس از گذشت 13 سال، مایکروسافت آخرین نسخه از این ویندوز را ارائه کرده است تا کاربران تجربه بهتری از ایجاد و مدیریت شبکه به دست آورند. در حال حاضر می‌توانید نسخه نهایی این سیستم‌عامل را از وب‌سایت‌های مختلف دانلود کنید و با نصب آن، با قابلیت‌های جدیدش آشنا شوید. برای آشنایی بیشتر با قابلیت‌های جدید این سیستم‌عامل، به بررسی برخی از ویژگی‌های آن پرداخته‌ایم. شایان ذکر است تغییراتی که مایکروسافت اعمال کرده است، بیش از موارد ذکرشده در این مقاله است.

مطلب پیشنهادی

عصری جدید در انتظار کاربران لینکدین
مایکروسافت چه برنامه‌هایی برای لینکدین دارد؟

امنیت

ویندوز سرور 2016 لایه‌های مختلفی از امنیت را ارائه می‌دهد که کمک می‌کند آن را عضو قابل اعتمادی برای تأمین امنیت شبکه خود بدانید. برخی از این قابلیت‌ها کاملاً مختص به ویندوز سرور 2016 هستند و برخی دیگر نیز در

نسخه‌های قبلی وجود داشتند و در این نسخه تکمیل شده‌اند.

ماشین‌های مجازی حفاظت‌شده (Shielded Virtual Machines):

ماشین‌های مجازی حفاظت‌شده قابلیت جدیدی است که تنها در آخرین نسخه ویندوز سرور وجود دارد. هر کدام از این ماشین‌های مجازی، جداگانه در برابر تهدیدات احتمالی شبکه محافظت می‌شوند. این روش احتمال نفوذ به سایر ماشین‌های مجازی مهم در شبکه شما، برای مثال دامین کنترلر یا SQL سرورتان را به صفر می‌رساند. با این روش، اختلالات یک ماشین مجازی، باعث تأثیر روی سایر ماشین‌ها نمی‌شود و ماشین‌های مجازی سرویس‌های زیرساختی شبکه شما همیشه در حال اجرا خواهند بود.

ماشین‌های مجازی محافظت‌شده از نوع دومین نسل ماشین‌های مجازی (Generation 2 VM) هستند که TPM مجازی دارند و توسط BitLocker رمزگذاری می‌شوند. این نوع ماشین‌ها تنها بر روی هاست‌های سالم قابل اجرا هستند. سالم بودن یک هاست از طریق سایر سرویس‌های مایکروسافتی تشخیص داده می‌شود.

اعتبارنامه‌های محافظت‌شده (Credential Guard):

این قابلیت تنها در ویندوز سرور 2016 وجود دارد. با استفاده از این قابلیت، از حملات Hash جلوگیری می‌شود. با استفاده از اعتبارنامه‌های محافظت‌شده، اعتبارنامه‌های شما از خطر بدافزارها در امان خواهند ماند. این قابلیت روی Remote Desktop Services و Virtual Desktop Infrastructure نیز قابل اعمال است و همچنین از اعتبارنامه‌های کاربرانی که قصد اتصال به این سرویس‌ها را دارند، محافظت می‌کند.

محافظ دستگاه (Device Guard):

این قابلیت تنها در ویندوز سرور 2016 وجود دارد. با استفاده از آن، تنها باینری‌هایی که تأیید شده‌اند، اجازه اجرا شدن روی سیستم را دارند. اگر برنامه یا درایور قابل اعتماد نباشد یا تأیید نشده باشد، اجازه اجرا روی سیستم را ندارد. از این قابلیت برای محافظت از Remote Desktop Services نیز می‌توان استفاده کرد. در این روش، از سیستم در برابر اجرای برنامه‌های تأیید نشده و خطرناک، محافظت می‌شود.

Control Flow Guard:

این ویژگی از سیستم‌عامل در برابر حملاتی که قصد دارند با تغییر آدرس، فرایند یک پروسه را تغییر دهند، محافظت می‌کند. شرکت‌های برنامه‌نویس واسط نیز می‌توانند با استفاده از ویژوال استودیو 2015، برای برنامه‌های خود Control Flow ایجاد کنند تا از کاربرانشان محافظت کنند.

Windows Defender Antimalware:

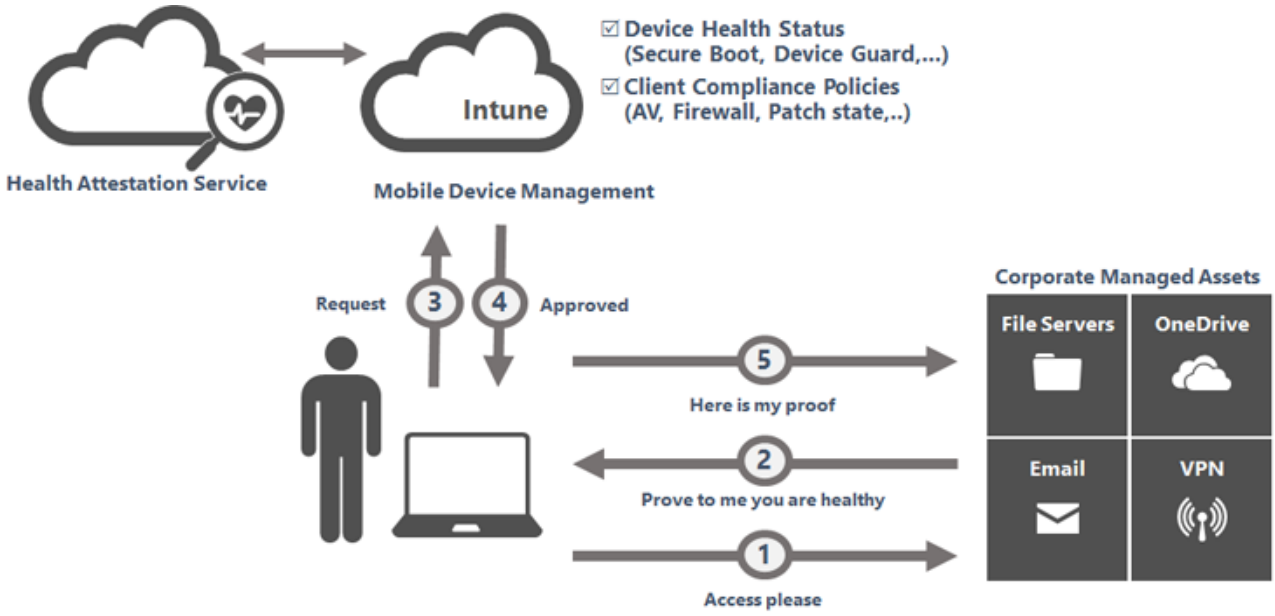
در این نسخه از ویندوز سرور، Windows Defender به طور شایسته‌ای از سیستم در برابر بدافزارها محافظت می‌کند. دیتابیس این ویژگی، توسط به‌روزرسانی‌هایی که ویندوز دانلود می‌کند، به‌روزرسانی می‌شود. این قابلیت جدید و مخصوص آخرین نسخه است. یکپارچگی آن با Powershell، اجرای دستوراتی برای محاظت سیستم از طریق Powershell را امکان‌پذیر کرده است.

دیواره آتش توزیع‌شده:

با پیاده‌سازی دیواره آتش توزیع‌شده، مهندسان شبکه می‌توانند سیاست‌های مختلف دیواره آتش را در بخش‌های مختلف پیاده‌سازی کنند و از کاربران خود در برابر ترافیک‌های ناخواسته که از طریق اینترنت و حتی اینترانت ایجاد می‌شود، محافظت کنند. با تقسیم این بخش‌ها به بخش‌های کوچک‌تر، برای هر کدام سیاست‌های متفاوتی اتخاذ می‌شود. در ویندوز سرور 2016 به این پروسه، Microsegmentation گفته می‌شود.

سرویس تأیید سلامت دستگاه:

Device Health Attestation، سرویس جدیدی است که مایکروسافت برای دستگاه‌های بر پایه ویندوز 10 ارائه کرده است. با استفاده از این سرویس، مایکروسافت سلامت دستگاه سیار، مانند موبایل یا تبلت‌های مبتنی بر ویندوز 10 را تأیید یا رد می‌کند. تنها دستگاه‌هایی می‌توانند به شبکه، برنامه‌ها و سرویس‌ها دسترسی پیدا کنند که سلامت آن‌ها تأیید شده باشد. نحوه عملکرد این سیستم در شکل 1 نشان داده شده است.



DHA

Virtual TPM: Trusted Platform Module

این قابلیت تنها مختص ویندوز سرور 2016 است. در این نسخه از ویندوز سرور، ماشین‌های مجازی نسل دو می‌توانند از Virtual TPM به عنوان چیپ پردازشگر رمز استفاده کنند. این چیپ کاملاً مجازی و امن بوده، نیاز به سخت‌افزار ویژه ندارد و مختص رمزنگاری است. همراه با جابه‌جایی ماشین مجازی، جابه‌جا می‌شود و از ماشین مجازی محافظت می‌کند.

SMB 3.1.1:

پروتکل SMB برای دسترسی از راه دور به فایل‌ها در یک شبکه استفاده می‌شود و نقش مهمی در شبکه‌ها ایفا می‌کند. در این نسخه از SMB، امنیت به طرز چشمگیری افزایش یافته است. مایکروسافت در این نسخه قابلیت Pre-authentication را قرار داده است. این قابلیت باعث جلوگیری از حمله Man-in-the-middle می‌شود. Pre-Authentication تمام مراحل «مذاکره» و «برقراری اتصال» را توسط الگوریتم قوی رمزنگاری SHA-512 رمزنگاری کرده و از سیستم محافظت می‌کند. به گفته مایکروسافت اگر کاربران شما ارتباطی با یک سرور مجهز به این SMB برقرار کنند، احتمال اینکه اطلاعات و ارتباط شما برای حمله‌کننده افشا شود، صفر است. علاوه بر SHA-512 امکان استفاده از AES-128-CCM و AES-128-GCM نیز وجود دارد.

PowerShell 5.1:

در این نسخه از PowerShell، امکانات امنیتی جدیدی همچون Log گرفتن از اسکریپت‌ها و یکپارچگی با سیستم‌های ضد بدافزار گنجانده شده است. این نسخه از PowerShell روی ویندوز سرورهای 2008 R2 به بالا قابل نصب است.

قابلیت‌های جدید ADDS:

Active Directory Domain Services، اطلاعات مربوط به دایرکتوری‌ها و ارتباطات بین کاربران و دامین‌ها را کنترل و مدیریت می‌کند. پروسه لاگین کاربر، احراز هویت و جست‌وجوی دایرکتوری، از جمله مسائل مرتبط به این سرویس‌ها است. در ویندوز سرور 2016 سه قابلیت جدید به این سرویس اضافه شده است:

- **Privileged Access Management:** این قابلیت به سازمان‌ها اجازه می‌دهد تا مدیر شبکه‌های سطوح پایین‌تر، زمان محدودی برای دسترسی به حساب‌های کاربری مدیریتی داشته باشند.
- **Azure Active Directory Join:** با استفاده از این قابلیت، کاربران با حساب کاربری دامین خود می‌توانند به Windows Store دسترسی پیدا کنند و notification roaming داشته باشند. با notification roaming، از هر سیستمی که لاگین کنند، notificationهای مربوط به سیستم‌های آنلاین مایکروسافت به آن‌ها نشان داده می‌شود.
- **Microsoft Passport:** با استفاده از Microsoft Passport و ADDS می‌توانید از سیستمی که ویندوز 10 دارد و به یک دامین join شده است، به دسکتاپ لاگین کنید. Microsoft Passport روش جدیدی برای ذخیره رمز عبور و

احراز هویت کاربر است.

به‌روزرسانی آسان AD FS:

در نسخه‌های قبلی Active Directory Federation Services برای مهاجرت به نسخه بالاتر، باید تنظیمات از نسخه قبلی به نسخه جدید منتقل می‌شد. در ویندوز سرور 2016، مهاجرت از AD FS ویندوز R2 2012 به‌راحتی صورت می‌پذیرد. کلیات این مراحل بدین شرح است:

1. به سرور فارم خود یک ویندوز سرور 2016 اضافه کنید. این ویندوز، سطح عملکرد خود را بر روی R2 2012 تنظیم کرده و درست مانند یک ویندوز سرور R2 2012 عمل می‌کند.

2. ویندوز سرورهای قبلی را به 2016 ارتقا دهید و مطمئن شوید که همه آن‌ها به‌درستی کار می‌کنند.

3. زمانی‌که تمام ویندوز سرورهای شما به 2016 ارتقا پیدا کرد، سطح عملیاتی AD FS را به 2016 ارتقا دهید و از قابلیت‌های جدید آن بهره ببرید.

به دلیل استفاده از Wizard برای اعمال سیاست‌ها در AD FS ویندوز سرور 2016، اعمال تنظیمات بسیار آسان است. برای ساده‌تر شدن، این تمهیدات صورت گرفته است:

- استفاده از قالب‌های آماده و ساده برای اعمال سیاست‌ها به برنامه‌های مختلف
- پارامتری کردن سیاست‌ها برای پشتیبانی از مقادیر مختلف به‌منظور کنترل دسترسی (مانند گروه‌های امنیتی)
- ظاهر کاربرپسند به همراه پشتیبانی از شروط جدید

AD FS در ویندوز سرور 2016 قابلیت جداسازی مدیریت سرور و مدیریت سرویس‌های AD FS را دارد. این بدان معنا است که برای مدیریت AD FS دیگر نیاز نیست با حساب کاربری مدیر سرور کار کنید و این بخش‌ها از یکدیگر تفکیک شده‌اند.

مایکروسافت علاوه بر موارد مذکور، قابلیت‌های امنیتی دیگری به ویندوز سرور 2016 اضافه کرده است که فهرست تمام این قابلیت و مقایسه آن‌ها با ویندوز سرورهای نسخه‌های قبل در جدول 1 آمده است.

جدول 1: مقایسه ویژگی‌های ویندوز سرور 2016 با نسخه‌های قبلی

پشتیبانی کامل ● پشتیبانی ناقص ◑ عدم پشتیبانی ○

ویژگی	ویندوز سرور 2008 R2	ویندوز سرور 2012 R2	ویندوز سرور ۲۰۱۶
ماشین مجازی محافظت‌شده: با استفاده از Bitlocker وضعیت ماشین مجازی و دیسک آن را رمزنگاری می‌کند.	○	○	●
Host Guardian Service: کمک می‌کند تا از سلامت Hyper-V و ماشین‌های مجازی آن اطمینان پیدا کنید.	○	○	●
Just Enough Administration (JEA): با این قابلیت دسترسی‌های کارمندان شبکه که نیازمند استفاده از حساب‌های کاربری Administrative هستند، کاسته می‌شود.	●	●	●
Just-in-Time Administration (JIT): دسترسی تحت نظارت و با زمان محدود به کاربران	◑	●	●
Credential Guard: با استفاده از مجازی‌سازی، از اطلاعات گواهی‌نامه‌ها حفاظت می‌کند.	○	○	●
Remote Credential Guard: با کمک Credential Guard، امکان استفاده از Single Sign-On (SSO) برای ارتباطاتی که با Remote Desktop Protocol (RDP) ایجاد می‌شوند، میسر می‌شود.	○	○	●
Device Guard: تنها به برنامه‌هایی اجازه اجرا می‌دهد که تأیید شده‌اند.	○	○	●
AppLocker: ابزاری برای سیاست‌گذاری، کنترل و مدیریت دسترسی به برنامه‌ها بوده و در این نسخه بهبود یافته است.	◑	●	●
Windows Defender: به صورت خودکار از دستگاه در برابر اجرای بدافزارها محافظت می‌کند.	◑	◑	●
Control Flow Guard: از سیستم‌عامل در برابر حملاتی که کلاس‌های حافظه را تخریب می‌کنند، محافظت می‌کند.	○	○	●
نسل دوم ماشین مجازی: برای افزایش امنیت، به ماشین‌های مجازی امکان استفاده از تمهیدات سخت‌افزاری را می‌دهد.	○	◑	●
Enhanced auditing for threat detection: سیستم ثبت وقایع ویندوز سرور، بهبودهای بسیاری داشته است و به‌راحتی وقایع مدنظر خود را پیدا خواهید کرد.	○	◑	●
DAC: به مدیران شبکه اجازه می‌دهد بر اساس قوانین تعریف‌شده، دسترسی‌های مختلفی بدهند و این دسترسی‌ها را کنترل کنند.	○	●	●
ویندوز فایروال به همراه تنظیمات تخصصی: در این نسخه تنظیماتی به ویندوز فایروال اضافه شده است تا مدیریت بهتری بر امنیت سرور خود داشته باشید.	○	●	●
BitLocker: با استفاده از یک سخت‌افزار یا TPM، اطلاعات را رمزنگاری و از آن‌ها محافظت می‌کند.	◑	●	●
مجازی‌سازی با حداقل امکانات: استفاده از نانو سرور باعث شده است احتمال حملات موفق به سیستم کمتر شود.	◑	◑	●

تاریخ انتشار:
11 دی 1395

نشانی منبع: https://www.shabakeh-mag.com/networking-technology/6029