ویندوز سرور 2019 ، با مجموعه‌ای کاربردی از قابلیت‌ها

## مراکز داده و زیرساخت‌های شبکه، هدف اصلی ویندوز سرور 2019


جدیدترین نسخه از خانواده سیستم‌عامل‌های سرور مایکروسافت به مراتب قدرتی بیشتر از اسلاف قبلی خود دارد. سیستم‌عاملی که سرعت نصب آن کمی بهبود یافته است؛ قابلیت‌های کاربردی و بهتری در ارتباط با کلاسترینگ ارائه کرده، به شیوه هوشمندانه‌ای پهنای باند شبکه را مدیریت کرده، از مکانیزم احراز هویت بهتری نسبت به گذشته استفاده کرده، عملکرد گیت‌وی‌ها در شبکه تحویل محتوا را بهبود داده، از مکانیزم‌های امنیتی به‌روزتری برای مقابله با تهدیدها و رفتارهای مخرب استفاده کرده و امنیت بیشتری را در ارتباط با شبکه‌های تحویل محتوا رقم زده، فرایند عیب‌یابی ماشین‌های مجازی محافظت شده را تسهیل کرده و در یک کلام به یک محصول ایده‌آل در خانواده سیستم‌عامل‌های سرور تبدیل شده است. اما پرسشی که ممکن است ذهن مدیران را به خود مشغول کرده باشد، این است که آیا نسخه جدید ارزش آن‌را دارد تا به سمت آن مهاجرت کرد یا بهتر است از همان نسخه 2016 استفاده کنیم؟ ما در این مقاله سعی خواهیم کرد به‌طور اجمالی برخی از قابلیت‌های کاربردی نسخه جدید را به شما معرفی کنیم.

### سازگاری برنامه‌های کاربردی با Server Core

ابتدا اجازه دهید با اصطلاح «ویژگی مبتنی بر تقاضا به منظور سازگاری برنامه‌های کاربردی با Server Core» که با عبارت App Compatibility Feature on Demand (FoD) for Server Core تعریف می‌شود آشنا شویم. بسته‌های نصبی «ویژگی مبتنی بر تقاضا» (FoD) به فایل‌های ایزو ویژه‌ای اشاره دارند که حاوی مولفه‌های اضافی هستند که شما می‌توانید آن‌ها را دانلود کرده و روی Windows Server Core نصب کنید. این مولفه‌های اضافی به شکل قابل توجهی سازگاری هر چه بیشتر برنامه‌ها با Windows Server Core را از طریق زیرمجموعه‌ای از کتابخانه‌های پویا، باینری‌ها و سایر مولفه‌ها به همراه می‌آورند. در به‌روزرسانی جدید ویژگی سازگاری مبتنی بر تقاضا FoD (سرنام Feature on Demand)، یک به‌روزرسانی کاربردی دریافت کرده و اکنون از اینترنت اکسپلورر 11 پشتیبانی می‌کند. بدون شک هنوز هم مدیرانی وجود دارند که ترجیح می‌دهند از مرورگر قدیمی و نه‌چندان مدرن اینترنت اکسپلورر استفاده کنند. مایکروسافت در توصیف به‌روزرسانی جدید FoD خاطر نشان کرده که به‌روزرسانی جدید قابلیت سازگاری Server Core را افزایش می‌دهد. به عبارت دیگر، زمانی که در نظر دارید از برنامه‌هایی برای نسخه دارای رابط گرافیکی ویندوز نوشته شده استفاده کنید و ویندوز به مولفه‌هایی نیاز دارد که به شکل پیش فرض در ویندوز نصب نشده، این ویژگی به یاری شما خواهد آمد. این ویژگی همچنین به سازمان‌ها کمک می‌کند تا فرایند بازنویسی برنامه‌های کاربردی سرور را به ساده‌ترین شکل برای Server Core مدیریت کنند. بسته FoD در قالب یک فایل ایزو جداگانه ارائه شده و تنها روی Windows Server Core قابل نصب است. مایکروسافت در مستندات سرور به این موضوع اشاره کرده که شما در حالت کلی پس از نصب بسته FoD بدون مشکل می‌توانید از ابزارها و برنامه‌های کاربردی که پیش از این استفاده می‌کردید، در نسخه جدید هم استفاده کنید. اگر در گذشته نمی‌توانستید در Server Core از برنامه‌های سروری که از سوی مایکروسافت یا شرکت‌های ثالث ارائه شده استفاده کنید، اکنون می‌توانید بدون مشکل از این ابزارها استفاده کنید. از مولفه‌های کاربردی سیستم‌عامل که از طریق به‌روزرسانی فوق

در دسترس قرار دارند، به موارد زیر می‌توان اشاره کرد:
(Event Viewer (Eventvwr.msc
(Performance Monitor (PerfMon.exe
(Resource Monitor (Resmon.exe
(Device Manager (Devmgmt.msc
(Microsoft Management Console (mmc.exe
(File Explorer (Explorer.exe
(Windows PowerShell ISE (Powershell_ISE.exe
(Failover Cluster Manager (CluAdmin.msc
(Internet Explorer (IExplore.exe یک مولفه انتخابی

این مولفه‌ها از ابزار مدیریت پایگاه‌های داده مایکروسافت SSMS (سرنام SQL Server Management Studio) نسخه 16 و 17 که باید به شکل جداگانه از طریق SQL Server و از طریق خط فرمان نصب شود، پشتیبانی می‌کنند. برای نصب مدیر بهینه‌سازی کلاستر (Failover Cluster Manager) ابتدا باید پاورشل را اجرا کرده و در ادامه فرمان زیر را در محیط پاورشل اجرا کنید.

```
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
```

برای اجرای ابزار مدیر بهینه‌سازی کلاستر (Failover Cluster Manager) باید فرمان cluadmin را در پنجره خط فرمان اجرا کنید. توجه داشته باشید که برای اجرای فرمان فوق نیازی نیست پنجره خط فرمان را با مجوز مدیریتی اجرا کنید. برای آن‌که بتوانید باینری‌های FoD را روی Server Core نصب کنید باید از ابزار خط فرمان DISM.exe (سرنام Deployment Image Servicing and Management) استفاده کنید. برای اطلاعات بیشتر در ارتباط با این ابزار به آدرس DISM Capabilities Package Servicing Command-Line Options مراجعه کنید و برای نصب بسته‌های باینری روی Server Core مراحل زیر را انجام دهید:

1. ابتدا فایل ایزو FoD را دانلود کرده و فایل دانلود شده را در یک پوشه به‌اشتراک گذاشته شده روی شبکه محلی کپی کنید.
2. با مجوز سطح مدیریتی به کامپیوتری که Server Core روی آن نصب شده و به شبکه محلی متصل است، وارد شوید.
3. از net use یا راهکار دیگری که سراغ دارید برای اتصال به مکان فایل ایزو کپی شده استفاده کنید.
4. فایل ایزو را در پوشه محلی که انتخاب کرده‌اید، کپی کنید.
5. پاورشل را از طریق اجرای فرمان powershell.exe در محیط خط فرمان اجرا کنید.
6. برای Mount کردن (ساخت درایو مجازی) فایل ایزو از فرمان زیر استفاده کنید:

```
Mount-DiskImage -ImagePath drive_letter:\folder_where_ISO_is_saved
```

7. فرمان exit را در پاورشل تایپ کنید.
8. اکنون فرمان زیر را وارد کنید:

```
DISM/Online/Add-Capability/CapabilityName:ServerCore.Appcompatibility~~~~0.0.1.0/Source:drive_letter_of_mounted_ISO: /LimitAccess
```

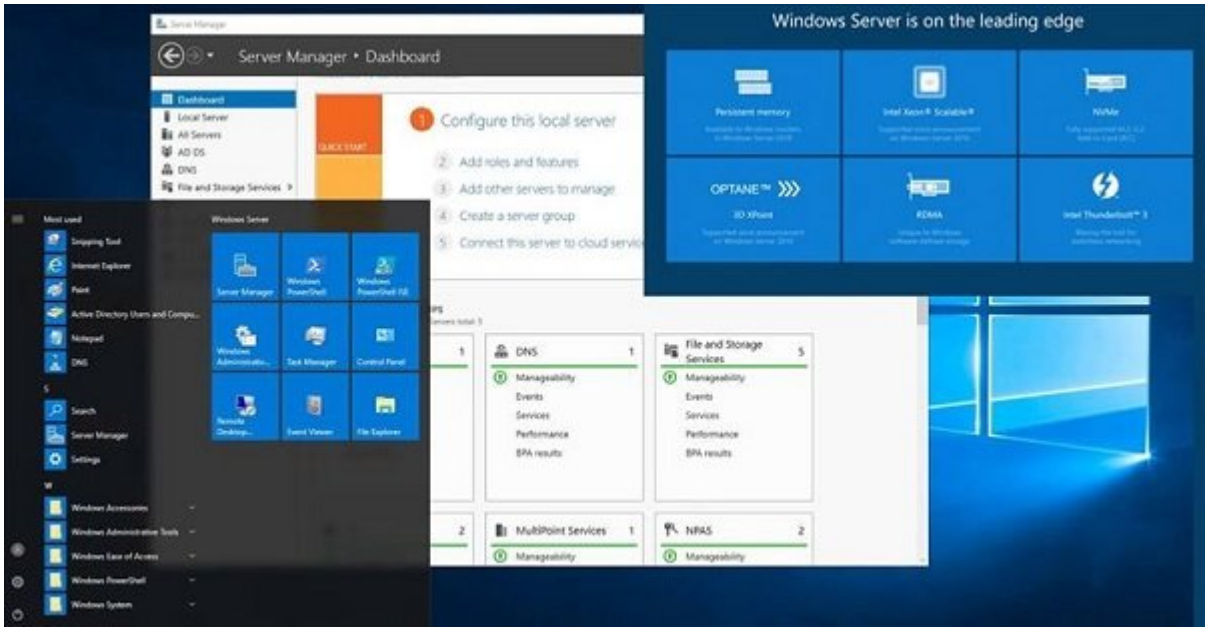
9. پس از کامل شدن نوار پیشرفت کارها، سیستم‌عامل را دوباره راه‌اندازی کنید. توجه داشته باشید که اگر در نظر دارید از اینترنت اکسپلورر 11 استفاده کنید، ضروری است که ابتدا بسته Fod را که به آن اشاره شد روی سیستم‌عامل خود نصب کنید. هرچند نصب اینترنت اکسپلورر 11 انتخابی بوده و ضرورتی ندارد آن‌را نصب کنید.

**مطلب پیشنهادی**



کلاسترها- توسعه دادن (بزرگ کردن) کلاسترها با استفاده از Cluster Sets

کلاسترینگ یا همان خوشه‌بندی به فرایندی اشاره دارد که در آن چند سامانه در قالب یک سامانه واحد کار می‌کنند تا راندمان یک سامانه چند برابر افزایش پیدا کند. Cluster Sets، یک فناوری جدید ابرمحور است که تعداد گره‌های خوشه را در یک مرکز داده نرم‌افزار محور (SDDC) ابری بر مبنای مرتبه توسعه آن‌ها افزایش می‌دهد. قابلیتی که اولین بار مایکروسافت در کنفرانس Ignite 2017 و همراه با معرفی ویندوز سرور 2019 از آن رونمایی کرد. یک Cluster Set را مجموعه‌ای متشکل از چند خوشه جداگانه از کلاسترهای بهینه شده (Failover Clusters) پدید می‌آورند که شامل مولفه‌های محاسباتی، مخزن یا فراهمگرا هستند.
Failover Clusters به گروهی از سرورها اشاره دارد که به شکلی پیکربندی شده‌اند که قادر هستند اثرات منفی از کار افتادگی سرورها را کم رنگ کنند. فناوری فوق باعث می‌شود زمانی‌که مشکل از کار افتادگی در سروری به وجود آمد، کلاینت‌ها باز هم بتوانند از سرویس‌ها استفاده کنند. برنامه‌های کاربردی یا سرویس‌هایی که در قالب کلاسترهای بهینه شده کار می‌کنند با نام‌هایی همچون نقش‌های خدماتی در دسترس، برنامه‌های خوشه‌بندی شده، سرویس‌های خوشه‌بندی شده، نقش‌های خوشه‌بندی شده و.... شناخته می‌شود.
همچنین به هر یک از سرورهایی که در یک کلاستر بهینه‌سازی شده خدمات‌رسانی می‌کنند یک گره (Node) می‌گویند. در یک کلاستر بهینه‌سازی شده هر زمان یک گره دچار خرابی شود، گره دیگر جایگزین گره خراب شده و نقش آن‌را بر عهده می‌گیرد که به این کار FailOver می‌گویند. ویندوز سرور 2019 گزینه‌های جدیدی در ارتباط با زیرساخت فراهمگرا و مدیریت خوشه‌ها ارائه کرده که به خوبی با جریان فعلی مدیریت حاکم بر مراکز داده‌ها همخوانی دارد. زیرساخت فراهمگرا (Cluster Set یک ویژگی کاربردی بوده که همراه با ویندوز سرور 2019 ارائه شده و به شما اجازه می‌دهد تا خوشه‌ای از خوشه‌ها را ایجاد کنید.
ماحصل این کار پدید آمدن خوشه‌های بزرگ فراهمگرا است.) در ارتباط با فاکتورهایی همچون گسترش‌پذیری، افزایش پایداری در برابر خرابی‌های سخت‌افزاری، نظارت مستمر بر صحت عملکرد، مدیریت، پشتیبانی مداوم از حافظه و.... پیشرفت‌های قابل ملاحظه‌ای داشته است. Cluster Sets ماشین‌های مجازی منعطف و یک مخزن واحد در اختیار کلاسترهای عضو یک Cluster Set قرار می‌دهد.
Cluster Set Instance ویژگی‌های شاخص و کلیدی را که به منظور مدیریت چرخه عمر یک مجموعه کلاستری به آن‌ها نیاز دارید، در اختیارتان قرار می‌دهد.




## ویژگی‌های جدید (Failover clustering: file share witness)

یکی از گزینه‌های witness که همراه با خوشه‌بندی بهینه شده ارائه شده و دو ارتقای جالب توجه را دریافت کرده File Share Witness است. اولین ارتقا در ارتباط با عدم به‌کارگیری سیستم توزیع فایل DFS (سرنام Distributed File System) به عنوان یک مکان به‌اشتراک گذاشته شده است. اضافه کردن یک FSW (سرنام File Share Witness) به یک سیستم توزیع فایل اشتراکی می‌تواند برای یک کلاستر مشکلاتی در ارتباط با عدم پایداری به وجود آورد. در نتیجه، در به‌روزرسانی جدید راهکاری برای تشخیص این مسئله که یک فرایند به‌اشتراک‌گذاری از یک سیستم توزیع فایل استفاده کرده ارائه شده است. در نتیجه اگر چنین موضوعی شناسایی شود، مدیر بهینه‌سازی خوشه‌ها (FCM) فرایند ساخت witness را مسدود کرده و پیغام خطایی را مبنی بر عدم پشتیبانی نشان می‌دهد.

دومین ارتقا به شما اجازه می‌دهد از FSW در ارتباط با سناریوهای چندگانه‌ای استفاده کنید که در گذشته پشتیبانی از آن‌ها به عمل نیامده بود. از جمله این سناریوها می‌توان به موارد زیر اشاره کرد:
• سناریو اول به عدم دسترسی به اینترنت یا دسترسی به اینترنت ضعیف در مناطق دورافتاده‌ای اشاره دارد که ضعیف بودن ارتباط اینترنتی مانع از آن می‌شود تا مصرف‌کننده بتواند از Cloud witness استفاده کند.
• سناریو دوم به عدم وجود درایوهای مشترک برای یک disk witness اشاره دارد که در عمل به فناوری‌های پیکربندی فراهمگرای (AG SQL Server Always On Availability Groups ، Storage Spaces Direct) و (DAG Exchange Database Availability Group) اجازه نمی‌دهد از دیسک‌های مشترک استفاده کنند.
• سناریو سوم به وجود کلاستر در پشت یک DMZ (سرنام De-Militarized Zone) اشاره دارد که دسترسی به یک اتصال کنترل‌کننده دامنه را غیر ممکن می‌کند. De-Militarized Zone ناحیه‌ای است که سرورها در آن قسمت به شکل محافظت شده قرار دارند. حفاظتی که از جانب دیوارهای آتش سخت‌افزاری و نرم‌افزاری ارائه می‌شود.
• سناریو چهارم به یک گروه کاری یا خوشه چند دامنه‌ای اشاره دارد که هیچ‌گونه CNO (سرنام Active Directory Cluster Name Object) برای آن‌ها وجود ندارد.

**مطلب پیشنهادی**

**به این 5 دلیل زمان به‌روزرسانی سرور شما فرارسیده است!**

## بهینه‌سازی خوشه‌ها- جابه‌جایی خوشه‌ها میان دامنه‌ها

جابه‌جایی یک خوشه از یک دامنه به دامنه دیگر یک فرایند سخت و دشوار است، به دلیل این‌که شما همواره باید برای جابه‌جایی کلاستر آن‌ها را از میان ببرید. با توجه به نقش‌هایی که در یک کلاستر وجود دارد، آن نقش‌ها نیز باید حذف شده و دومرتبه ساخته شوند. در به‌روزرسانی جدید دو فرمان جدید پاورشل موسوم به Comanndet اضافه شده‌اند که اجازه می‌دهند یک خوشه را بدون نیاز به از میان بردن آن به مکان دیگری انتقال دهید.

## بهینه‌سازی خوشه - حذف به‌کارگیری مکانیزم احراز هویت NTLM

از این پس Failover Clusters به جای آن‌که از مکانیزم احراز هویت NTLM استفاده کند، از احراز هویت مبتنی بر گواهی‌نامه‌ها و Kerberos استفاده می‌کند. برای آن‌که بتوانید از این قابلیت استفاده کنید، نیازی نیست هیچ تغییری اعمال کرده یا ابزار خاصی را روی سامانه مستقر کنید. مکانیزم جدید به Failover Cluster اجازه می‌دهد در محیط‌هایی که NTLM در آن‌ها غیرفعال شده مستقر شده و عملیاتی شود.

## کانتینرها

## حساب‌های خدماتی مدیریت شده گروهی (Group Managed Service Accounts)

گسترش‌پذیری و قابلیت اطمینان کانتینرهایی که از حساب‌های خدماتی مدیریت شده گروهی موسوم به gMSA برای دسترسی به منابع شبکه استفاده می‌کنند، بهبود پیدا کرده است. از این پس در زمان به‌کارگیری یک gSMA واحد با چند نمونه از کانتینرها باید خطاهای احراز هویت کمتری را مشاهده کنید. همچنین، دیگر نیازی نیست نام میزبان کانیتنر را یکسان با gMSA تعیین کنید. همچنین مشکل مربوط به ممانعت از عدم به‌کارگیری gMSA همراه با کانتیرهای ایزوله شده Hyper-V هم برطرف شده است.

**مطلب پیشنهادی**

سفری به اعماق کانتینرها
**کانتینرها چه هستند و چرا به آن‌ها نیاز داریم؟**

## ارائه ایمیج کانتینر جدید ویندوز

مایکروسافت همچنین یک ایمیج پایه جدید را به مجموعه کانتینرهای ویندوز سرور اضافه کرده است. علاوه بر ایمیج کانتینرهای نانوسرور و Windows server core، ویندوز ایمیج جدید نیز در دسترس است. این ایمیج در مقایسه با دو ایمیج قبلی مولفه‌های بیشتری داشته و قادر است از برنامه‌های کاربردی که به واسطه‌های برنامه‌نویسی بیشتری

نیاز دارند، پشتیبانی کند.

## استقرار کوبرتینیز روی ویندوز سرور

کوبرتینیز ابزاری محبوب برای پیکربندی کانتینرها است که فرایند پیاده‌سازی، مدیریت شهودی و گسترش‌پذیری موثر را به بهترین شکل در دسترس مدیران شبکه قرار می‌دهد. از ویژگی‌های از پیش ساخته شده این فناوری به مواردی همچون برنامه‌ریزی به منظور پیدا کردن یک ماشین ایده‌آل برای اجرای کانتینر همراه با اختصاص یک ایمیج کانتینر، نظارت بر عملکرد درست فرایندها با زیرنظر گرفتن خرابی‌های کانتینرها و زمان‌بندی دوباره آن‌ها به شکل خودکار، شناسایی سرویس‌ها که به کانتینرها این امکان را می‌دهد که در زمان تغییر هاست یا آدرس آی‌پی یکدیگر را به شکل خودکار پیدا کنند، گسترش‌پذیری که امکان اضافه یا حذف دستی یا خودکار Container Instances را امکان‌پذیر ساخته که ماحصل آن پاسخ‌گویی دقیق و موثر به درخواست‌ها است و در نهایت شبکه‌سازی اشاره کرد.

## کنترل ازدحام از طریق به‌کارگیری LEDBEAT

متخصصان فناوری اطلاعات به خوبی می‌دانند که بدون وقفه باید بر امنیت شبکه نظارت داشته باشند. نظارت مستمر بر به‌روزرسانی‌های ارائه شده و نصب وصله‌ها برای محافظت از سامانه‌ها در برابر انواع مختلفی از بردارهای حمله از جمله وظایف اصلی کارشناسان شبکه است. اما متاسفانه این نظارت مستمر نارضایتی‌هایی را به همراه خواهد آورد. نظارت مستمر به معنای آن است که پهنای باند شبکه برای دریافت به‌روزرسانی‌ها مصرف شده و در نتیجه کاربران نهایی برای انجام فعالیت‌های خود که بیشتر رویکرد تعاملی دارند با محدودیت روبه‌رو می‌شوند. در ویندوز سرور 2019 یک ابزار کنترل ازدحام شبکه موسوم به «بهینه‌سازی زمان تاخیر» (LEDBAT) ارائه شده که قادر است پهنای باند باقی مانده روی شبکه را جمع‌آوری کرده و از آن استفاده کند.

## Microsoft Hyper-V 2019

مایکروسافت هایپر وی سرور 2019 یک محصول ایستا بوده که تنها شامل ویندوز هایپرویزور بوده و به منظور ساخت و مدیریت سرورها و شبکه‌های مجازی در مقیاس بزرگ و کوچک به کار گرفته می‌شود. Microsoft Hyper-V راهکاری ساده و قابل اعتماد برای مجازی‌سازی ارائه کرده و به شما کمک می‌کند تا بهره‌وری سرور را بهبود بخشیده و هزینه‌ها را کاهش دهید. فناوری هایپرویزور ویندوز که در مایکروسافت هایپر-وی سرور به کار گرفته شده درست مشابه با Hyper-V role است که در خود ویندوز سرور قرار دارد. در نتیجه بیشتر قابلیت‌های Hyper-V که روی ویندوز سرور 2016 موجود هستند در مایکروسافت Hyper-V Server نیز وجود دارند. از قابلیت‌های کلیدی هایپر وی سرور می‌توان به قابلیت ترکیب خوشه‌ها به شکل همگرا یا هایپر وی، امکان اجرای کانتینرهای لینوکسی، سیستم جامع مدیریت، سامانه حفاظتی ATP در سطح حافظه و هسته، مجهز بودن به فناوری ASR و تعیین خط‌مشی‌هایی به منظور اجرای نرم‌افزارها، پشتیبانی از Storage Replica به منظور برقراری ارتباط هم‌زمان سرورها و خوشه‌ها و.... اشاره کرد.

## Remote Desktop Session Host (RDSH)

RD Session Host سرویسی است که به کاربران اجازه می‌دهد برنامه‌های مبتنی بر ویندوز یا برنامه‌های کاملا دسکتاپی را به‌اشتراک قرار دهند. کاربران می‌توانند برای اجرای برنامه‌ها، ذخیره‌سازی فایل‌ها و به‌کارگیری منابع شبکه که روی سرور قرار دارد به یک سرور
RD Session Host متصل شوند. وجود یک باگ در نسخه‌های آزمایشی ویندوز سرور 2019 باعث شده بود تا قابلیت RDSH در دسترس کاربران قرار نگیرد، اما اکنون این قابلیت در اختیار کاربران قرار دارد.

## Windows Defender Advanced Threat Protection

در به‌روزرسانی جدید مایکروسافت از سیاست امنیتی جالبی استفاده کرده است. ویندوز سرور 2019 به ماژول‌های خاص سطح کرنل و پاسخ‌گویی سریع و موثر تجهیز شده است. این فاکتورهای جدید به ویندوز سرور اجازه می‌دهند هرگونه فعالیت تهاجمی در سطح حافظه و هسته را شناسایی کرده، از تدابیر دفاعی مناسبی روی ماشین‌های آلوده برای تعمیر و بازنویسی فایل‌های آلوده و از میان بردن پردازه‌های مخرب استفاده کرده و همچنین به سرعت داده‌های اضافی را که برای جرم‌شناسی به کار گرفته می‌شوند و مرتبط با حوادث بحرانی هستند، از راه دور جمع‌آوری کند.

## Windows Defender ATP Exploit Guard

Windows Defender ATP Exploit Guard به مجموعه‌ای جدید از قابلیت‌های دفاعی به منظور ممانعت از ورود تهدیدات به میزبان‌ها تجهیز شده‌اند. چهار مولفه، Attack Surface Reduction (ASR)، Network protection، Controlled folder access و Exploit protection که در ماژول امنیتی Windows Defender ATP Exploit Guard به کار گرفته شده‌اند، به گونه‌ای طراحی شده‌اند که از سامانه‌ها در برابر طیف گسترده‌ای از بردارهای حمله محافظت کرده و هرگونه رفتار مشکوکی را که نشانه‌ای از پیاده‌سازی یک حمله مخرب در آن‌ها وجود دارد، بلوکه می‌کنند. همچنین به سازمان‌ها اجازه می‌دهند میان مخاطرات امنیتی و نیازهای مرتبط با بهره‌وری خود توازنی به وجود آورند .

**منبع:**

docs.microsoft
docs.microsoft
datacenterknowledge
virtualizationhowto

**تاریخ انتشار:**
20 آذر 1397

---

**نشانی منبع:**
https://www.shabakeh-mag.com/networking-technology/14207/%D9%85%D8%B1%D8%A7%DA%A9%D8%B2-%D8%AF%D8%A7%D8%AF%D9%87-%D9%88-%D8%B2%DB%8C%D8%B1%D8%B3%D8%A7%D8%AE%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%B4%D8%A8%DA%A9%D9%87%D8%8C-%D9%87%D8%AF%D9%81-%D8%A7%D8%B5%D9%84%DB%8C-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019