ایمن‌سازی و کاهش زمان تاخیر در برقراری ارتباطات

# دسترسی سریع‌تر و ایمن‌تر به اینترنت با ویندوز سرور 2019

اینترنت تبدیل به بخشی از زندگی حرفه‌ای و شخصی ما شده است. کاربران خانگی و سازمان‌های بزرگ تجاری برای انجام کارهای خود به اینترنت نیاز مبرمی دارند. به همین دلیل، شرکت‌های ارائه‌دهنده خدمات اینترنتی (ثابت و سایر) تلاش می‌کنند به مشتریان خود سریع‌ترین و ایمن‌ترین مکانیزم ارتباطی را ارائه دهند، اما یک ارتباط اینترنتی تنها زمانی به بهترین شکل در اختیار مصرف‌کننده نهایی قرار خواهد گرفت که کاربر از زیرساخت مطلوبی استفاده کرده باشد.

سیستم‌عامل‌ها در هر دو حوزه دسکتاپ و سرور مجبور هستند به بهترین شکل از کاربران خود در برابر مخاطرات امنیتی محافظت کرده و از پروتکل‌های ارتباطی به شکل صحیحی استفاده کنند. اگر این‌گونه نباشد، رخنه‌های امنیتی و مصرف غیر اصولی پهنای باند، نارضایتی کاربران را به همراه داشته و اطلاعات کاربران به راحتی در اختیار هکرها قرار می‌دهند. مایکروسافت برای بهبود سطح ایمنی ویندوز سرور 2019 و ارائه راهکارهای قدرتمندی برای اتصال به اینترنت تغییراتی در نسخه جدید ویندوز سرور اعمال کرده است. اما تغییرات در حوزه بهبود سطح ایمنی و ارتقا کیفی سطح دسترسی به اینترنت چه هستند؟ چگونه قابلیت‌های جدید ویندوز سرور 2019 می‌توانند اینترنت سریع و امن در اختیار مدیران شبکه قرار دهند؟ برای انجام چنین کاری مایکروسافت در ویندوز سرور 2019 سه تغییر مهم به شرح زیر اعمال کرده است:

- بهبود فرآیند مرتبط کردن اتصالات به یکدیگر و رمزگذاری درست ارتباطات با هدف ارائه یک تجربه وب‌گردی بدون تاخیر
- به‌روزرسانی مجموعه مکانیزم‌های رمزنگاری سمت سرور پروتکل HTTP/2 با هدف کاهش خودکار خرابی‌های ارتباطی و پیاده‌سازی راحت‌تر الگوهای رمزنگاری.
- در ویندوز سرور 2019 به‌طور پیش‌فرض، Cubic به جای کنترل‌کننده ازدحام TCP استفاده شده تا توان عملیاتی برای شبکه‌های باندپهن با کارایی بالا بهبود پیدا کند.

## HTTP/2 برای یک وب سریع‌تر و امن‌تر

مایکروسافت چند سال پیش، پشتیبانی از HTTP/2 را به ویندوز سرور 2016 و ویندوز 10 به شکل سرور HTTP (به‌طور خاص http.sys که جزیی از کرنل برای سرور HTTP و IIS است) اضافه کرد. ویندوز سرور 2019 با اتکا بر HTTP/2 در زمان استقرار وب‌سایت‌ها دو مزیت مهم عملکرد بالا و امنیت مطلوب را به ارمغان آورده است. برای درک بهتر عملکرد HTTP/2 نسبت به HTTP/1.1 در ویندوز سرور 2019، پیشنهاد می‌کنم آدرس https://http2.akamai.com/demo که دموی جالب توجهی در ارتباط با دو قابلیت فوق است را مشاهده کنید.

## HTTP/2 Refresher

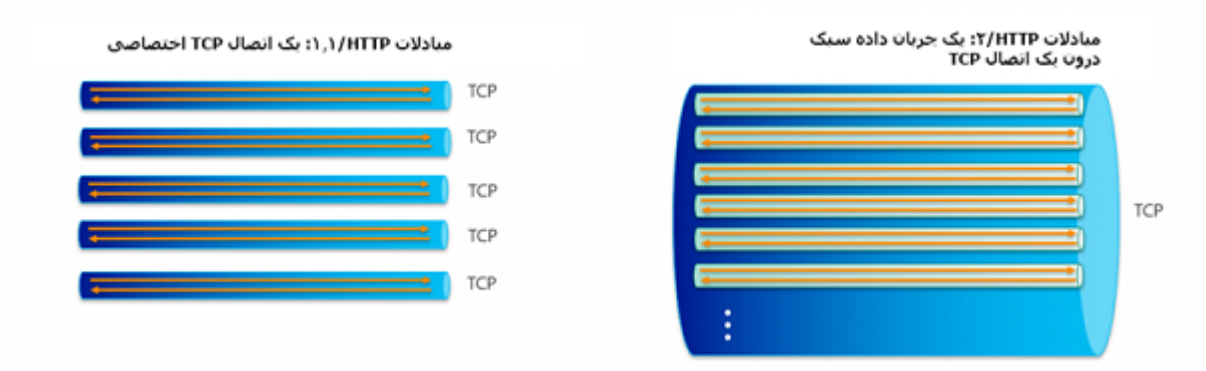
HTTP/2 بزرگ‌ترین ارتقا پروتکل محبوب انتقال ابرمتن، پس از گذشت 20 سال موفق شد، تاثیر مهمی روی شبکه‌های کامپیوتری گذاشته و اثرگذاری زمان تاخیر را به میزان قابل توجهی کم کند. این تغییر نسخه از 1.1 به 2 (نه 1.1 به 1.2) نشان‌دهنده یک تحول بزرگ در این پروتکل است. HTTP/2 برای آن‌که عملکرد وب‌سایت‌ها را بهبود بخشد، تغییرات اساسی در برخی از قابلیت‌های بنیادین به وجود آورد که باعث شد قابلیت‌های قدرتمندی در اختیار ما قرار گیرد. از قابلیت‌های مهم و تاثیرگذار به موارد زیر می‌توان اشاره کرد:

### انتقال چندگانه پیام (Muliplexing)

پروتکل انتقال ابرمتن، شناخته شده‌ترین و پرکاربردترین پروتکل اینترنت است که شالوده وب را شکل داده است. با این وجود، به خودی خود قادر نیست هیچ کاری انجام دهد. برای تبادل داده‌ها، پروتکل فوق به لایه انتقال وابسته است. دقت کنید که نگارش 2 و نگارش 1.1 این پروتکل به شکل‌های متفاوتی از لایه انتقال استفاده می‌کنند.

- HTTP/1.1: در نگارش 1.1 پروتکل انتقال ابرمتن، هر درخواست نیاز به یک اتصال TCP (و TLS در هنگام استفاده از HTTP) اختصاصی دارد که به‌طور بالقوه چند فرآیند رفت و برگشت را برای برقراری ارتباط تکرار می‌کند.
- HTTP/2: نگارش دوم به درخواست‌های هم‌زمان اجازه می‌دهد از ارتباط TCP استفاده کنند. این همان انتقال چندگانه پیام یا Multiplexing است.

با قابلیت مالتی‌پلکسینگ HTTP/2 تنها در اولین درخواست فرآیند رفت و برگشت برای برقراری اتصال انجام می‌شود. درخواست‌های مرتبط بعدی نیازی به برقراری ارتباط ندارند و بلافاصله داده‌های HTTP را ارسال می‌کنند. شکل1، تمایز بین HTTP/1.1 و HTTP/2 در نحوه استفاده از لایه انتقال را نشان می‌دهد.




### فشرده‌سازی سرآیند

تبادلات HTTP معمولا سرآیندهای HTTP بسیاری را تولید کرده و استفاده می‌کنند. برخی اوقات این سرآیندها داده‌های به مراتب بیشتری از بارداده اصلی را با خود به همراه دارند. برای رفع این مشکل، HTTP از یک ساختار فشرده‌سازی به‌نام HPACK برای فشرده کردن سرآیند HTTP استفاده می‌کند. این تکنیک به میزان قابل توجهی مقدار داده‌هایی که باید بین کلاینت و سرور مبادله شوند را کاهش داده و باعث صرفه‌جویی در زمان رفت و برگشت درخواست‌ها می‌شود.

### مطلب پیشنهادی

آموزش رایگان ویندوز سرور منطبق با سرفصل‌های بین المللی – 18
**گواهی‌نامه‌ها چه نقشی در ویندوز سرور 2019 دارند؟**

## بهینه‌سازی‌های HTTP/2 در ویندوز سرور 2019
## تلفیق اتصال

ویندوز سرور 2019 برای آن‌که بتواند مزایای پروتکل انتقال ابرمتن نسخه2 را به دامنه‌هایی که بر مبنای نگارش 1.1 طراحی شده‌اند، توسعه‌دهد از راهکار تلفیق اتصال (connection coalescing) برای کاهش sharding استفاده می‌کند. در پروتکل HTTP/1.1 شاردینگ زمانی رخ می‌دهد که یک دامنه طراحی شده به‌عنوان دامنه‌های متفاوتی ظاهر شود تا اتصالات TCP مستقل‌تری را بتوان ایجاد کرد. رویکرد فوق، یک شیوه مصنوعی برای ایجاد توازن است که HTTP/2 نیازی به آن ندارد، اما تکنیک شاردینگ و وبسایت‌های طراحی شده برای HTTP/1.1 تا مدت‌های طولانی در دنیای وب حضور خواهند داشت. برای کم کردن اثر شاردینگ، ویندوز سرور 2019 امکان تلفیق اتصال در دو سمت لبه و سرور HTTP را فراهم کرده است. در این روش دامنه‌هایی مثل a.bing.com و b.bing.com در صورتی که گواهینامه‌های آن‌ها هماهنگ باشد به یک اتصال TCP واحد ختم می‌شوند. بدون تلفیق سایت‌هایی مثل a.bing.com و b.bing.com به اتصالات TCP جداگانه نیاز دارند.

## اصلاحات امنیتی

ویندوز سرور 2019 با کمک گرفتن از HTTP/2 به‌طور خودکار خطاهای احتمالی یک اتصال را برطرف می‌کند. برای درک بهتر این‌که چرا خطاهای اتصال ممکن است بوجود آیند، اجازه دهید این نکته را متذکر شویم که HTTP/2 حداقل به نگارش 1.2 پروتکل TLS به همراه مجموعه الگوریتم‌های امنیتی نیاز دارد. متاسفانه این نیاز امنیتی می‌تواند منجر به برقراری ارتباطات HTTP/2 شکننده شود. اگر چنین مشکلی به وجود آید، کاربران وبسایت شما ممکن است تا زمانی‌که مدیر وب‌سرور مشکل مربوط به سایفر SSL را برطرف کند موفق نشوند به وب‌سایت متصل شوند. با ویندوز سرور 2019 این مشکل بدون هیچ دخالتی از سوی مدیر حل می‌شود و در نتیجه کاربران با مشکل اتصال روبرو نخواهند شد. اجازه دهید، به‌طور اجمالی جزییات این فرآیند مهم که ویندوز سرور 2019 عهده‌دار انجام آن است را تشریح کنیم.

- این خطای ارتباطی می‌تواند زمانی پدیدار شود که مجموعه الگوریتم‌های امنیتی SSL پیش‌فرض ویندوز سرور 2016 به شکل نادرستی تغییر کرده باشند. فرآیند تغییر نادرست زمانی رخ می‌دهد که هر یک از مجموعه الگوریتم‌های امنیتی گنجانده شده در فهرست سیاه توسط HTTP/2 قبل از نمونه‌هایی که HTTP/2 آن‌ها را مجاز در نظر گرفته، ظاهر شوند، در چنین حالتی مرورگرهای فایرفاکس و کروم مانع برقرار اتصال می‌شوند. مرورگر کروم پیغام خطای ERR_SPDY_INADEQUATE_TRANSPORT_SECURITY و مرورگر فایرفاکس پیغام خطای NS_ERROR_NET_INADEQUATE_SECURITY را نشان می‌دهند.
- حتا اگر مرتب‌سازی صحیح مجموعه الگوریتم‌های امنیتی SSL از بروز این مشکل جلوگیری کند، مایکروسافت در ویندوز سرور 2019 مکانیزم تبادل این مجموعه الگوریتم‌های امنیتی را بهینه‌سازی کرده تا مرتب‌سازی مجموعه الگوریتم‌های امنیتی SSL غیرقابل نفوذ شود. مسلما این فهرست هنوز هم باید شامل مجموعه الگوریتم‌های امنیتی مورد پذیرش HTTP/2 باشد، اما دیگر لازم نیست در ابتدای این فهرست و قبل از اسامی مسدود شده قرار بگیرند.

این نوع بهینه‌سازی پیچیدگی‌های عملیاتی استقرار HTTP/2 را کاهش می‌دهد و مشتریان را قادر می‌سازد با آسودگی بیشتری از مزایای مجموعه الگوریتم‌های امنیتی سطح بالایی که HTTP/2 به آن‌ها نیاز دارد، استفاده کنند.

## مطلب پیشنهادی

سازمان‌دهی منحصر به فرد کانتینرها توسط ویندوز سرور 2019
**یکپارچگی کوبرنتس با ویندوز سرور 2019**

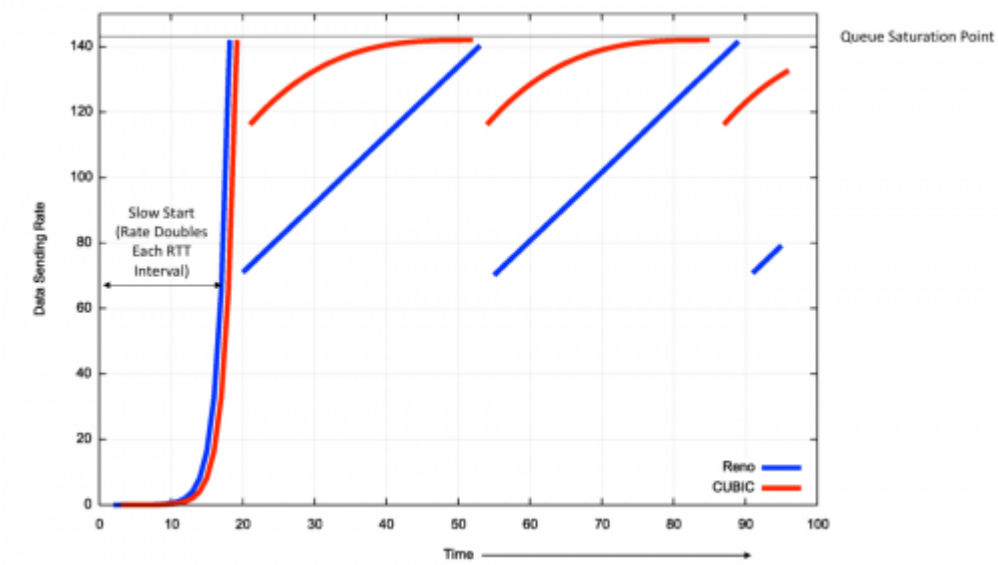
## Windows TCP به سمت Cubic می‌رود!

ویندوز سرور 2019 به لطف کنترل‌کننده ازدحام جدید خود به ویژگی‌هایی همچون کاهش زمان تاخیر و توان عملیاتی انتقال بالاتر تجهیز شده است. دو فاکتور فوق درخواست‌های TCP را به گونه‌ای تنظیم می‌کنند که توازنی میان

کلاینت و سرور برقرار شود. کنترل‌های ازدحام ویندوز سرور 2019 شامل Cubic، Compound TCP، New-Reno و LEDBAT هستند. اکنون، Cubic به کنترل‌کننده ازدحام پیش‌فرض تبدیل شده است. برای شناسایی کنترل‌کننده باید پاورشل را باز کرده و فرمان زیر را درون آن اجرا کنید.

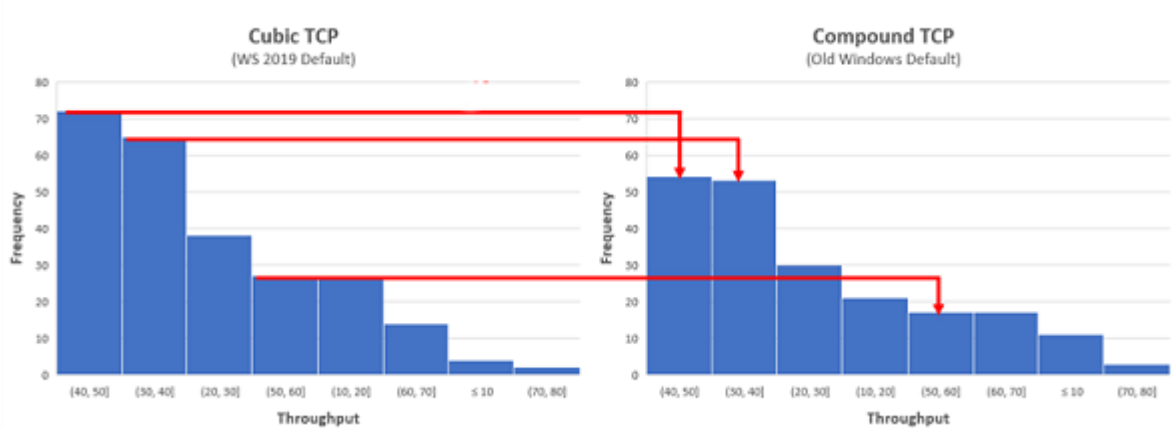
```
PS C:\WINDOWS\system32> Get-NetTCPSetting | Select SettingName, CongestionProvider
SettingName       CongestionProvider
-----------       ------------------
Automatic
InternetCustom    CUBIC
DatacenterCustom  CUBIC
Compat            NewReno
Datacenter        CUBIC
Internet          CUBIC
```

همان‌گونه که مشاهده می‌کنید Cubic همه جا حضور دارد. چرا این موضوع که Cubic به عنوان کنترل‌کننده ازدحام پیش‌فرض انتخاب شده، حائز اهمیت است؟ زیرا Cubic سریع‌تر از TCP است. Cubic به ویژه برای پهنای باند بالا، لینک‌های با زمان تاخیر بالا و در مکان‌هایی که TCP استاندارد با اجرای ضعیف همراه است مناسب‌تر است. اگر مدیر یک شبکه هستید و در نظر دارید حجم قابل توجهی از داده‌ها را با پهنای باند و زمان تاخیر بالا (فاصله طولانی) ارسال کنید، قطعا از مزایای Cubic برخوردار خواهید شد. چرا Cubic در لینک‌های شبکه پرسرعت و مسافت طولانی سریع‌تر از سایرین عمل می‌کند؟ شکل دو این مسئله را به خوبی تشریح می‌کند. شکل دو چگونگی تغییرات نرخ ارسال داده (توان عملیاتی) در طی زمان را نشان داده است. خط آبی TCP استاندارد (New Reno) و خط قرمز Cubic است.




سمت چپ این نمودار مرحله شروع اتصال را نمایش می‌دهد. الگوریتم‌های کنترل ازدحام روی شروع TCP تاثیر ندارند، به همین دلیل این بخش از منحنی‌ها یکسان هستند. بعد از این‌که مرحله شروع کامل شد اتصالات به مرحله اجتناب از ازدحام وارد می‌شوند. توجه داشته باشید که منحنی Cubic به نسبت TCP استاندارد زمان بیشتری از وقت خود را نزدیک نقطه اشباع شبکه می‌گذراند. به همین دلیل است که Cubic سریع‌تر عمل می‌کند، زیرا منحنی ازدحام در آن به جای حالت خطی TCP استاندارد به صورت منحنی نمایی است.

حالا اجازه دهید کمی از مباحث نظری جدا شده و به داده‌ها بپردازیم. شکل سه فرآیند ارسال داده‌ها در سراسر ایالات متحده در عرض یک شب در قطعه‌های 250 مگابیتی را نشان می‌دهد. ما داده‌ها را به یک نمودار پارتو (بدون نمودار خطی برای وضوح) تقسیم کردیم. در سمت چپ Cubic و در سمت راست Compound (فراهم‌کننده ازدحام قبل از ویندوز سرور 2019) را مشاهده می‌کنید. Cubic همواره به توان عملیاتی بالاتری نسبت به Compound دست پیدا می‌کند.




تیم عملیاتی Windows Core Networking در تلاش بوده تا ابتدا پیاده‌سازی سرور HTTP و عملکرد HTTP/2 در ویندوز سرور 2019 را بهبود بخشیده و بعد از آن به ویرایش کنترل ازدحام TCP بپردازد. اگر بگوییم دنیا برای مصرف‌کنندگان و مدیران سرور که پلتفرم آن‌ها ویندوز سرور 2019 است سریع‌تر و امن‌تر شده و تمام آن چیزی که باید انجام دهند مراجعه به خود ویندوز سرور 2019 است، اغراق نکرده‌ایم.

برای مطالعه تمام بخش‌های آموزش ویندوز سرور 2019 تهیه شده در سایت ماهنامه شبکه اینجا کلیک کنید.

**تاریخ انتشار:**

20 دی 1398

---

**نشانی منبع:**
https://www.shabakeh-mag.com/networking-technology/16192/%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D8%B3%D8%B1%DB%8C%D8%B9%E2%80%8C%D8%AA%D8%B1-%D9%88-%D8%A7%DB%8C%D9%85%D9%86%E2%80%8C%D8%AA%D8%B1-%D8%A8%D9%87-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%A8%D8%A7-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019