نظارت بر شبکه

دیده یابی شبکه استفاده از سیستمی است که شبکه رایانه ای را از نظر اجزای همراه با مشکل یا با سرعت پایین را به صورت متداوم تحت نظر دارد و در صورت قطع شدن یا هر مشکل دیگری، مدیر شبکه (از راه‌های مختلف مانند ایمیل، پیام کوتاه و غیره) را آگاه می‌سازد. نظارت بر شبکه قسمتی از مدیریت شبکه است.

محتویات

جزئیات

هنگامی که یک سیستم کشف کننده ورود بدون اجازه، تهدیدات شبکه را از بیرون تحت نظر دارد، یک سیستم نظارت کننده روی شبکه، آن را برای مشکل‌های به وجود آمده از بارگیری‌های بیش از حد سرورها یا مشکلات دیگر، اتصالات شبکه یا سایر دستگاه‌ها تحت نظر می‌گیرد.

برای نمونه، برای شناسایی شرایط یک وب سرور، نرم‌افزار نظارت ممکن است در فواصل معین درخواست HTTP را برای واکشی یک صفحه ارسال کند. برای سرورهای ایمیل، امکان دارد پیام آزمایشی به وسیله SMTP ارسال شود و به وسیله IMAP یا POP3 مجدداً حاصل شود.

معیارهای متداول سنجیده شده شامل زمان پاسخ، فراهم بودن و زمان کار. با وجود اینکه معیارهای تداوم و اعتبار دارای از معروفیت بیشتری می‌شوند. افزودن شایع دستگاه‌های بهینه‌سازی WAN تأثیر ناخوشایندی بر روی بیشتر ابزارهای نظارت بر شبکه دارد، به ویژه هنگامی که نوبت به اندازه‌گیری دقیق تأخیر پایان به انتها می‌رسد چون آنها باعث محدودیت دید زمان دیرکرد رفت و برگشت می‌شوند.

خرابی‌های درخواست وضعیت، همچون هنگامی که اتصال پابرجا نمی‌شود، زمان آن قطع شده یا مدرک یا پیام قابل دسترسی نیست، معمولاً عملی را از سیستم دیده یابی به وجود می‌آورد. این عملکردها متفاوت است. ممکن است یک زنگ هشدار (به واسطه پیام کوتاه، ایمیل و غیره) برای sysadmin موجود فرستاده شود، سیستم‌های خرابی اتوماتیک ممکن است فعال شوند تا سرور مشکل دار قابل تعمیر نباشد، آن را از وظیفه خود حذف کند.

همچنین دیده یابی بر عمل اتصال شبکه به عنوان اندازه‌گیری ترافیک شبکه نیز شناخته می‌شود.

پرتو نگاری مقطعی شبکه

پرتو نگاری مقطعی شبکه، یک محدوده با اهمیت برای اندازه‌گیری شبکه است، که با نظارت بر سلامت پیوندهای مختلف در یک شبکه با استفاده از کاوشگرهای انتها به انتهای ارسال شده توسط عوامل پایدار در مناطق با اهمیت شبکه / اینترنت در ارتباط است.

تجزیه و تحلیل مسیر

تجزیه و تحلیل مسیر دیگر زمینه با اهمیت اندازه‌گیری شبکه است که شامل روش‌ها، سیستم‌ها، الگوریتم‌ها و ابزارهایی برای پایش حالت مسیریابی شبکه‌ها است. مسیریابی نادرست یا مشکلات مسیریابی باعث افت نامطلوب عملکرد یا خرابی می‌شود.

انواع مختلف پروتکل‌ها

خدمات دیده یابی سایت می‌توانند صفحه هایSSH، DNS، IMAP، POP3، SMTP ،FTP، SNMP، HTTPS، HTTP UDP، SIP، ICMP، TCP، SSL، TELNET، رسانه جریان و رده‌بندی گسترده‌ای از دیگر ورودی‌ها را با تنوع بازه‌ها بررسی می‌کنند. از هر چهار ساعت تا هر یک دقیقه. به‌طور معمول، بیشتر سرویس‌های نظارت بر شبکه سرور شما را بین هر ساعت از یک بار در هر دقیقه آزمایش می‌کنند.

برای دیده یابی بر عملکرد شبکه، بیشتر ابزارها از پروتکل‌هایی مانندPacket Sniffing، NetFlow، SNMP یا WMI استفاده می‌کنند.

نظارت بر سرور اینترنت

نظارت بر یک سرور اینترنت یعنی صاحب سرور همیشه می‌داند که یکی یا تمام سرویس‌های او دچار مشکل است. امکان دارد نظارت بر سرور **داخلی باشد**، یعنی نرم‌افزار وب سرور وضعیت خود را مورد بررسی قرار می‌دهد و در صورت دچار مشکل شدن بعضی از آن‌ها مالک را با خبر می‌کند. و **خارجی**، یعنی بعضی از شرکت‌های نظارت بر وب سرور شرایط خدمات را با فرکانس بخصوصی بررسی می‌نمایند. نظارت بر سرور می‌تواند شامل مورد بررسی قرار دادن معیارهای سیستم مثل استفاده از پردازنده، استفاده از حافظه، عملکرد شبکه و گنجایش دیسک باشد. همین‌طور می‌تواند شامل نظارت بر برنامه‌ها، مانند بررسی روند برنامه‌هایی مانند سرور Postgres، Nginx، MySQL، Apache HTTP و غیره باشد.

نظارت خارجی دارای اطمینان بیشتری است، چون زمانی که سرور کاملاً به مشکل می‌خورد، همچنان کار می‌کند. ابزارهای مناسب نظارت بر سرور دارای معیار عملکرد، قابلیت اخطار و توانایی پیوند آستانه‌های خاص با مشاغل خودکار سرور مانند تأمین حافظه بیشتر یا انجام پشتیبان‌گیری هستند.

سرورهای سرتاسر جهان

سرویس‌های نظارت بر شبکه عموماً دارای چند سرور در سرتاسر جهان هستند - به‌طور مثال در آمریکا، اروپا، آسیا، استرالیا و دیگر مکان‌ها. با دارا بودن چند سرور در مکان‌های متفاوت جغرافیایی، یک سرویس نظارت می‌تواند بگوید که آیا وب سرور توسط شبکه‌های متفاوت در سرتاسر جهان در دسترس است. هر قدر مکان‌هایی که مورد استفاده قرار می‌گیرد بیشتر باشد، در دسترس بودن تصویر شبکه کامل تر است.

فرایند نظارت بر وب سرور

هنگام نظارت بر وب سرور برای مسائل احتمالی، یک سرویس دیده یابی بر وب خارجی تعدادی از پارامترها را مورد بررسی قرار می‌دهد. اول از همه، آن را برای یک کد بازگشت HTTP متناسب مورد نظارت قرار می‌دهد. با مشخصات HTTP RFC

2616، هر وب سرور چند کد HTTP را بازمی‌گرداند. تجزیه و تحلیل کدهای HTTP سریعترین راه برای تعیین وضعیت

فعلی وب سرور تحت نظارت است. ابزارهای نظارت بر عملکرد برنامه‌های شخص سوم قابلیت نظارت، هشدار و گزارشگری وب سرور اضافی را فراهم می‌کنند.

اطلاع

از آنجایی که اطلاعات ارائه شده به وسیله سرویس‌های دیده یابی وب سرور در بیشتر موارد ضروری است و امکان دارد که دارای اهمیت زیادی باشد، امکان دارد از روش‌های متفاوت اطلاع‌رسانی استفاده شود: پست الکترونیکی، تلفن‌های ثابت و تلفن‌های همراه، پیام رسان‌ها، پیامک‌ها، فکس، پیام رسان‌ها و غیره.

جستارهای وابسته

- مدیریت خدمات بازرگانی
- مقایسه سیستم‌های نظارت بر شبکه
- در دسترس بودن بالا
- کارت رابط نظارت بر شبکه
- اندازه‌گیری ترافیک شبکه
- شیر شبکه
- مانیتور سیستم
- توافق‌نامه در سطح خدمات

پیوند به بیرون

- Network Management (https://curlie.org/Computers/Software/Networking/Network_Management) در کرلی
- لیست ابزارهای نظارت و مدیریت شبکه در دانشگاه استنفورد (http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html)