

بررسی بهترین روش مستند سازی شبکه های کامپیوتری بزرگ (نسخه PDF)

با سلام و عرض خسته نباشید خدمت خانواده بزرگ توسینسو، یکی از معضلات قدیمی و همیشگی در زیرساخت های فناوری اطلاعات بزرگ و متوسط، documentation بوده و در اکثر مواقع اقدامات گسترده ای تو این زمینه انجام شده، هزینه های زیادی صرف شده، زمان زیادی از افراد فنی کلیدی و حتی افراد فنی غیر کلیدی سازمان صرف شده تا وضعیت موجود مکتوب بشه و در صورت ایجاد تغییرات فنی، مستندات و documentها به فراخور تغییرات فنی تغییر کنن. خب، بعد از این همه دردسر، خروجی چی بوده؟ یک یا چند داکيومنت word و چنتا نقشه visio و موارد مشابه. خب، نیازمندی و هدف کاملا درست و منطقی هست. که نمونه هایی از اونا موارد زیر هستند:

- کارفرما یا صاحب بیزینس، می خواد بدون تو زیرساخت IT ایش چه خبره و هر وقت خواست این اطلاعاتو به هر کی خواست انتقال بده
- کارفرما یا صاحب بیزینس، نمی خواد طوری وابسته مهندسش باشه که اگه اون نباشه کسب و کارش بخوابه
- یه اماری از تغییرات و توسعه های انجام شدش می خواد داشته باشه
- و...

ولی این خروجی ها اصلا مطلوب نیست و خیلی کم می تونن نیازمندیهایی که گفتیم رو تحت پوشش قرار بدن. " به جای این که دنبال مستند و داکيومنت باشید، دنبال جمع اوری همه config file های موجود توی زیرساخت فناوری اطلاعاتتون باشید با استفاده از یک سرویس config management. " من یه سوال می پرسم، شما کدوم کارشناس IT درست حسابی و دید که وقتی بخواد از یه محیط جدید شناخت کنه به جای نگاه کردن به config بره سراغ فایل های word تولید شده که حجمشون بعضی وقتا می رسه به بیش از ۱۰۰۰ صفحه !!!

به جرئت بگم داکيومنتای ۱۰۰ یا ۲۰۰ یا ۳۰۰ یا ۱۰۰۰ صفحه ای که در این خصوص نوشته شده، کلا تا حالا هیچ کدومشو یه نفرم نخونده و جالب بدونید که نگارنده های این مستندات و داکيومنت ها هم اینو خوب می دونن و تا اونجایی که جا داشته باشه توش اب می بدن. اصلا نگارنده ها معمولا دانش فنی خیلی پایینی دارن. به نظر شما یه مهندس کارکشته میاد وقتشو صرف نوشتن یه داکيومنت ۳۰۰ صفحه ای کنه؟ حالا فرض می کنیم یه داکيومنت متنی تولید شده که واقعا از نظر فنی خوبه. (من که تا حالا ندیدم!) یه مهندس براش اینکه متن زیرو بخونه راحت تره؟

```
ip dhcp snooping limit rate 20
```

یا متن زیر؟ "در شبکه هایی که با استفاده از مکانیزم های لایه دویی مکانیزم تخصیص ادرس دهی را به صورت خودکار و طبق rfc شماره فلان انجام می دهند، در تجهیزات لایه سه ای gateway از حملات مرسوم، استفاده از dhcp کلاینت های rogue بوده به صورتی که بتوانند فضاهای ادرس دهی در دسترس را به اتمام برسانند.

به جهت جلوگیری از چنین مخاطراتی از راهکار dhcp snooping با مکانیزم محدودسازی تعداد درخواست های per second این نوع بسته ها راه اندازی شده است." (حالا بماند که اصلا dhcp snooping رو راه اندازی نکرده و خالی بسته!) خب حالا بعد این همه قر زدن بنده، می خوایم بریم سراغ راهکار. خیلی ساده این کار هارو (به ترتیب از لحاظ اولویت) انجام بدید:

۱. دنبال جمع اوری فایل های کانفیگ تجهیزات و سرورهایتون باشید. همه config file های موجود در سطح زیرساخت فناوری اطلاعات! یعنی سرویس config management راه اندازی کنید و به شدت امنش کنید.

۱. در مورد تجهیزاتی که فایل کانفیگ text based دارن و بخش عمده تجهیزات و سرویس هارو شامل میشن که تکلیف مشخصه
۲. در مورد سرویس هایی که پیکربندیشون فقط با GUI هست (که تو کل دنیا فقط سرویس های مایکروسافتی این جورین!) از کانفیگها print screen بگیرید.
۳. در مورد سرویس هایی که هم GUI دارن و هم فایل کانفیگ text based ولی با GUI کار کردنش متداول تره، مثل اجزای محیط vSphere، حالت اول رو حتما انجام بدید ولی در کنارش انجام دادن حالت دوم هم بد نیست.

۲. نقشه های visio بکشید از توی لایو، جا نمایی رک ها، و تک تک ارتباطات فیزیکی، و ارتباطات لایه سه ایتون،

۳. به جدول اکسل سلسله مراتبی درست کنید از طرح کلی تا جزئی ip addressing

۴. پیشنهاد میکنم راه اندازی سرویس config management و حتی operation های مربوطه رو هم بسپورید به بچه های لینوکسیتون. غوغا خواهند کرد.

ali-apple

با سلام و احترام

ممنون از مقاله خوبتان ولی ای کاش به توضیحی در مورد راه اندازی سرویس config management بدهید

اصلاً چی هستند چه جوری میشه راه اندازی کرد نرم افزار یا چی هستند؟؟

در چه سیستم عاملی نصب می شوند اگر ممکن اسم نرم افزار و نحوه راه اندازی در حد مختصر توضیح دهید

سپاس

مهیار کباری

با سلام و عرض خسته نباشید و تشکر از سؤالی که پرسیدید.

عرضم به خدمتتون که شما بدون نرم افزار هم می تونید بحث Config Management رو انجام بدید، ولی خب قاعدتاً با استفاده از نرم افزار و سرویس بهتر هستش. منظورم از بدون نرم افزار این هست که به صورت دوره ای (مثلاً هفته ای یک بار یا ماهی یک بار) لاگین کنید به تجهیز و فایل config ها رو انتقال بدید یا به show runn چیزی بگیرید. این راهکار برای محیط های کوچیکتر مناسب تر هست.

در راه حل های فنی حرفه ای تر، سرویسی یا سرویس هایی مخصوص بحث Config Management راه اندازی میشه.

توی نرم افزارهای مانیتورینگ و مدیریت شبکه مثل Cisco Prime، Juniper Space و... یکی از کارهایی که می کنن همین هست که البته برای محصولات خودشون این کارو می کنن. این دسته برای تیم های شبکه ای که دانش لینوکسی توشون نیست یا کمه می تونه مناسب تر باشه.

راهکار بهتر، استفاده از سرویس های لینوکسی است که توی این حوزه Solution زیاد هست. در درجه اول Ansible خیلی محصوله خوبیه. Puppet هم خوبه. بدون استفاده از محصول هم میشه پیاده سازی کرد با استفاده از Shell Scripting. یعنی مثلاً به Script می نویسید که مثلاً هر ۲۴ ساعت به بار، ssh یا pssh زده بشه و حالا با مکانیزم های مختلفی که هست بره file های کانفیگ رو بخونه و در جایی خاص ذخیره کنه

فقط توجه داشته باشید که راه اندازی این دسته از سرویس ها به دانش تخصصی خودش نیاز داره و یادگیریشون به کم زحمت خواهد داشت. به خاطر همین این راهکار رو برای زیرساخت های فناوری اطلاعات بزرگ و متوسط پیشنهاد می کنم نه محیط های کوچیک.

مطلب اصلی