2014

بررسی Xinetd در لینوکس

نویسنده : حسام الدین توحید

SKYWAN13@YAHOO.COM

مقدمه مولف :

آنچه پیش رو دارید به صورت رایگان و تحت لیسانس GNU GPLv3 به علاقه مندان لینوکس هدیه می گردد . در تهیه این مقاله از سر فصل های درسی گفته شده در دوره هایLPIc2 و RHCE استفاده شده ولازم می دانم از مهندس مهدوی فر به خاطر راهنمایی های مفیدشان و مرکز آموزشهای پیشرفته دانشگاه شریف (لایتک) تشکر کافی را داشته باشم. این مطالب با نگاهی کاربردی و بدون پرداختن به بحث های تئوریک گردآوری و عرضه شده است. امیدوارم مطالب ارائه شده بتواند باعث ارتقاء دانش فنی کاربران لینوکس و متخصصین IT شود. این آموزش بر اساس توزیع CentOSمی باشد، لذا خواهشمندم هرگونه نقص در محتوا را به ایمیل نگارنده ارسال فرمائید. انتشار این فایل با ذکر منبع بلامانع است و هر گونه استفاده نامناسب از محتوای ارائه شده بر عهده کاربر بوده و تمام حقوق معنوی این اثر به نویسنده آن تعلق دارد.

زکات علم نشر آن است.

موفق باشید

حسام الدین توحید

خرداد 1393

فهرست مطالب :

xinetd در لینوکس

اگر init نباشد یا درست کار نکند می توان گفت که عملا سیستم غیرعملیاتی است.چون هر نرم افزاری بخواهد کار کند init هم به طریقی درگیر می شود.اما وظیفه init نیست که ping کند یا telnet راه اندازی کند بلکه وظیفه اش این است که یک سری نرم افزار وارد چارت سازمانی کند:

اسم مدیر شبکه در لینوکس xinetd یا super server است. نرم افزارهای تحت سیستم عامل Linux به دو صورت زیر به کاربران تحت شبکه سرویس می دهند:

به صورت مستقل (Standalone)

.تحت نظارت و کنترل پروسس xinetd

بسیاری از سرویس های شبکه ای از جمله telnet تحت نظارت و سرپرستی پروسسی به نام xinetd که اصطلاحا" Super Server خوانده می شود قرار دارند.

سوپر سرور یک سرویس قدرتمند است که سرویس های دیگر می توانند در قالب آن کار کنند. شما باید در سازمانتان تصمیم بگیرید که کدام یک از نرم افزارهایتان زیر نظر init باشد و کدام یک زیر نظر xinetd کار کند. Xinetd فقط مدیریت درخواست عای یک سرویس را به عهده می گیرئ ، مدیریت کارهای یک سرویس یه عهده خود آن است .اگر نرم افزاری به تنهایی در حافظه قرار بگیرد در مد Standalone قرار دارد.

xinetd نرم افزاری است که می تواند نرم افزارهای سرویس دهنده شبکه را مدیریت کند. مثلا وقتی در لینوکس آپاچی سرور را راه اندازی کردیم در قسمت از پارامترهای config می توانیم مشخص کنیم که آیا به صورت standalone اجرا شود یا تحت نظر xinetd اجرا شود.

هرکس از هر جای دنیا به هر سرویسی وصل شود سرویس دهنده باید به پورت گوش کند. نرم افزار stand alone خودش گوش می کند اما نرم افزار هایی که فرزند xinetd هستند xinetd به جایشان به پورت گوش می دهد ودر مواقع ضروری آنها را آگاه می کند.همه نرم افزار های جدی در همه سیستم عامل ها فایل پیکربندی دارند. سرویس ها زمانی که بالا می آیند فایل conf مربوط به خود را می خوانند تا بدانند چه کاری باید انجام دهند.

سرویس xinetd که در بعضی از گونه های Linux و یا Unix با نام inetd شناخته می شود در زمان فعال شدن، به فایل ها و دایرکتوری زیر مراجعه نموده و با آنالیز نمودن اطلاعاتی که به دست می آورد آماده سرویس دهی می شود:

etc/xinetd.conf/

etc/xinetd.d/

فایل متنیxinetd.conf که همانند اکثر فایل های پیکربندی تحت دایرکتوری etc میباشد، شامل اطلاعات کلی برای سرویس دهی تحت شبکه بوده و تحت دایرکتوی/etc/xinetd.d نیز تعداد زیادی فایل متنی قرار داشته و به ازای هر سرویس (مثلا" telnet) میتوان فایل متنی با همان نام مشاهده نمود. مدیر سیستم با تغییر دادن در فایل های فوق می تواند کنترل بیشتری را بر روی سرویس دهی داشته باشد. در لینوکس اکثر فایل های پیکربندی text base هستند و با ویرایشگرهای متن مانند Vim قابل تغییر هستند ولی در ویندوز این نوع فایل ها داخل رجیستری قرار دارند و با regedit باید آنها را مورد تغییر قرار داد .

shell مانند یگ گارسون در رستوران است ، پشت صحنه عوامل بسیار زیادی فعالیت می کنند که آن رستوران میتواند سرویس بدهد به این عوامل Daemon می گویند که یک معنی آن پشت پرده است .xinetd هم خودش هیچ وقت شخصا برای سرویس دادن عمل نمی کند مانند سرپرست راننده هاست که اگر شخصی تماس بگیرد و ماشین می خواهد سرپرست هم برایش ماشین می فرستد.

در فایل xinetd.conf داخل {} مانند برنامه های c پارامترها ومقادیرشان تعریف شده اند که xinetd از روی اینها موقع بالا آمدن می فهمد که به چند نفر باید سرویس بدهد و مثلا صد نفر می توانند telnet کنند یا 50 نفر ftp کنند. در واقع xinetd فایلی دارد که از روی آن می تواند بخواند که چه کسی می تواند چه کسی نمی تواند و چه کسی نباید بتواند!.

همان طور که موقع ورود نگهبان از شما کارت تشخیص هویت می خواهد xinetd نیز برای هر ارتباطی identication طلب می کند و مجموعه این اطلاعات را نیز نگه داری می کند.

اگر کسی telnet کند xinetd هاستش (ip) را نگه می دارد و اینکه با چه کسی کار دارد. در نگهبانی نیز شماره شناسایی مراجعه کننده و شماره کارمندی کسی را که با او کار دارد ثبت می شود.حال اگر شخص شماره شناسایی نداشت log out failure اتفاق می افتد ولی سیستم هاست را ثبت می کند و همه این کارها توسط xinetd انجام می شود. به همین دلیل است که اگر به سایتی حمله کنید شناسایی می شوید ؛ userID ندارید ولی ip شما ثبت می شود.در لینوکس های سری 6 به بعد خانواده ردهت سرویس xinetd نصب نیست بلکه باید نصب و پیکربندی شود.

مزایا و معایب xinetd

به طور مثال اگر روی سروری 100 سرویس داشته باشیم و هر سرویس به تنهایی بخواهد در حافظه قرار بگیرد مطمئنا آن سرور در سرویس دهی با مشکل جدی مواجه خواهد شد .

Xinetd سرویس هایی که ضروری نیستند را از حافظه خارج کرده و مدیریت درخواست های آنها را به عهده گرفته و به جای آنها در حافظه قرار می گیرد. و سرویس مورد نظر را به حالت standby می برد . به محض اینکه درخواستی برای آن سرویس برسد xinetd آن را فراخوانی کرده و سرویسش مورد نظر را وارد چرخه سرویس دهی می کند. لازم به ذکر است تمام سرویس ها را نمی توان تحت xinetd راه اندازی کرد ، مثلا سرویس های پر تراکنشی مثل dhcp و یا dns را باید به صورت standalone راه اندازی کرد. اما سرویس های مثل ssh و ftp و یا telnet که listen دارند را می توان تحت xinetd اداره کرد. سرویس های جدی و پرتراکنش ، حتما باید به صورت standalone راه اندازی شود.

با xinetd یک لایه امنیتی به سیستم اضافه می شود و دست admin برایاعمال محدودیت در سرویس ها باز می شود. اگر سرویسی که دارای تراکنش بالائی باشد را تحت xinetd قرار دهیم مطمئنا خود xinetd با مشکل جدی مواجه خواهد شد . کانفیگ xinetd مربوط به سرویس خاصی نسیت. این فایل در مسیر /etc/xinetd.conf قرار دارد و در /etc/xinetd.d/ هم فایل های کانفیگ سرویس هایی که تحت xinetd اداره می شوند و می خواهند یکسری خواص گلوبال را به ارث نبرند قرار دارد.

بررسی آپشن های موجود در یک فایل xinetd

در زیر تعدادی از آپشن هایی که در یک فایل xinetd میتوان نوشت را توضیح می دهیم جهت اطلاع بیشتر به man xinetd رجوع فرمائید. مقادیر ثبت شده در جلوی هر آپشن فرضی می باشد.

instances =60

این آپشن مشخص می کند سرویس به چند درخواست هم زمان پاسخ می دهد. instances =60 یعنی به بیش تر از 60 نفر را سرویس نمی دهد حالا اگر 45 نفر telnet کنند و 15 نفر ftp .نفر 61ام که تلاش کند وصل شود با پیغام connection refused مواجه می شود.این عدد را در یک سازمان مثلا برابر 600 می گذاریم و برای شبکه های خانگی و کوچک 2 یا 3.پس این عدد در سازمان ها برای سرویس هایی که stand alone نیستند باید عوض شوند.

log_type =SYSLOGautjpriv

این خط مشخص می کند تمام لاگها را تحویل syslog سرور بدهد و log هایی را ثبت می کند که از نوع احراض هویت باشند.

log_on_success =HOSTPID

اگر کلاینت موفق شود از سرویس مورد نظر استفاده کند از id پروسس های آن log گرفته می شود.

log_on_failure =HOST

اگر کلاینت موفق به سرویس گرفتن نشد از IP یا نام سیستم log برداری می کند.

cps =25 30

در جلوی این آپشن دو عدد وجود دارد اولین عدد مشخص می کند چند درخواست هم زمان را در ثانیه بپذیرد و دومین عدد هم بیان می کند اگر ارتباط برقرار نشد چند ثانیه بعد مجدا retry کند. عدد دوم همان زمان time out است در این خط مشخص کرده ایم در ثانیه 25 درخواست بیشتر نمی توانند به سیستم وصل شوند حال اگر درخواست 26 رسید باید 30 ثانیه صبر کند تا اتصال برقرار شود. این کار برای جلوگیری از حملات DDOS می

باشد. عدد cps باید متناسب با instances باشد. در مورد cps یا connection per second باید توجه شود که اگر 10000 کاربر ظرفیت داشته باشیم و همه با هم وصل شوند مثل این است که 10000 نفر یک دفعه وارد یک اتاق شوند پس منطقی این است که هر دفعه (ثانیه) مثلا 25 نفر وارد شوند .اکثر سرویس های موجود در دایرکتوری xinetd (xinetd.d) تحت مدیریت xinetd اجرا می شوند مانند telnet ، ftp و chargen و بقیه سرویس ها نیز شبیه این سه سرویس کار می کنند. به ازای هر سرویسی در دایرکتوری xinetd.d یک فایل کانفیگ داریم.

disable =yes or no

اگر yes باشد سرویس غیر فعال می شود و اگر no باشد بر عکس آن را اجرا می کند.

wait =yes or no

این آپشن مشخص می کند نرم افزار مربوطه Multi Thread باشد یا Single Thread . اگر yes باشد باید ابتدا به درخواست رسیده پاسخ دهد سپس به درخواست بعدی رسیدگی کند، اما اگر no باشدمی تواند هم زمان به چند درخواست پاسخ دهد.

server =/usr/sbin/sshd

مقابل این گزینه باید آدرس اسکریپت باینری فایل اجرایی سرویس مورد نظر را وارد کنیم. این فایل حتما باید باینری باشد یعنی اگر یک سرویس نوشتید باید فایل آن را تبدیل به باینری کنید.

user =root

مشخص میکند اسکریپت اجرایی سرویس توسط چه یوزری اجرا می شود.

sock_type =stream or dgram

اگر مقدار این خط بر روی stream تنظیم شود یعنی پکتها از نوع tcp می باشند و ار بر روی dgram باشد یعنی پکتهای این سرویس از نو udp خواهند بود.

server_args =/etc/ssh/sshd_conf

هر سرویسی یکسری ارگومان دارد که ممکن است xinetd آنها را نشناسد. مثلا در یک سرویس می توانیم کاری کنیم که اگر یوزر یک دایرکتوری یا فایل ایجاد کرد با پرمیژن خاصی ذخیره شود . این می تواند قابلیت داخلی یک سرویس باشد ولی ممکن است در xinetd وجود نداشته باشد. اگر بخواهیم این قابلیت ها را به xinetd معرفی کنیم باید در جلوی این آپشن آدرس مسیر فایل کانفیگ سرویس مورد نظر را وارد می کنیم چون معمولا ارگومانها و فیچرها در فایل کانفیگ یک سرویس تعریف می شوند.

bind =192.168.1.1

این آپشن معلوم میکند این سرویس درخواست های رسیده از کدام کارت شبکه را پاسخ دهد.

access_time =19:12-19:16

در این خط مشخص میکنیم کاربران در چه زمانهای بتوانند از این سرویس استفاده کنند.

نمونه ای از فایل ایجاد شده در Xinetd برای سرویس Vsftpd

سرویس vsftpd به صورت standalone کار می کند حال اگر بخواهیم این سرویس زیر نظر xinetd اداره شود باید گزینه listen=??? را در فایل کانفیگ آن برابر YES شده و در زیر دایرکتوری xinetd یک فایل کانفیگ بسازیم. در زیر نمونه ای از فایل آورده شده است :

```
Servicevsftp

   {

socket_type      =stream      یعنی پکتها از نوع tcp می باشند
user             =root  مشخص میکند اسکریپت اجرایی سرویس توسط چه یوزری اجرا می شود
server           =/usr/sbin/vsftpd  آدرس اسکریپت باینری فایل اجرایی سرویس مورد نظر
server_args      =/etc/vsftod/vsftpd.conf آدرس فایل کانفیگ جهت شناختن آرگومانها
nice             =10
disable          =no  نشان می دهد سرویس فعال است
flags            =ipv4

}
```

منابع :

مطالب متفرقه منتشر شده در اینترنت

سر فصل دوره های RHCE و LPIc2

راهنما Openssh

سایت centos .org