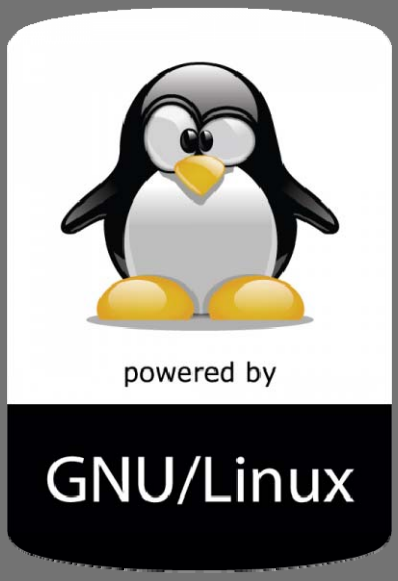
2015

راه اندازی FTP در لینوکس V.3

مولف: حسام الدین توحید



skywan13@chmail.ir

نویسنده : حسام الدین توحید skywan13@chmail.ir

مقدمه مولف :

آنچه پیش رو دارید ویرایش سوم مقاله راه اندازی FTP در لینوکس است که 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 و RHCSA 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 و بر اساس توزیع CentOS گردآوری و عرضه شده است. امیدوارم مطالب ارائه شده بتواند باعث ارتقاء دانش فنی کاربران لینوکس و متخصصین IT شود. زکات علم نشر آن است.

موفق باشید

حسام الدین توحید

آذر 1395

فهرست مطالب :

آشنائی با پروتکل FTP

امروزه از پروتکل های متعددی در شبکه های کامپیوتری استفاده می گردد که صرفا" تعداد اندکی از آنان به منظور انتقال داده طراحی و پیاده سازی شده اند . اینترنت نیز به عنوان یک شبکه گسترده از این قاعده مستثنی نبوده و در این رابطه از پروتکل های متعددی استفاده می شود. برای بسیاری از کاربران اینترنت همه چیز محدود به وب و پروتکل مرتبط با آن یعنی HTTP است ، در صورتی که در این عرصه از پروتکل های متعدد دیگری نیز استفاده می شود. File Teransfer Protocol نمونه ای در این زمینه است.

پروتکل FTP چیست؟

تصویر اولیه اینترنت در ذهن بسیاری از کاربران، استفاده از منابع اطلاعاتی و حرکت از سایتی به سایت دیگر است و شاید به همین دلیل باشد که اینترنت در طی سالیان اخیر به سرعت رشد کرده و متداول شده است . بسیاری از کارشناسان این عرصه اعتقاد دارند که اینترنت گسترش و عمومیت خود را مدیون سرویس وب می باشد .

فرض کنید که سرویس وب را از اینترنت حذف نمائیم. برای بسیاری از ما این سوال مطرح خواهد شد که چه نوع استفاده ای را می توانیم از اینترنت داشته باشیم؟ در صورت تحقق چنین شرایطی ، یکی از عملیاتی که کاربران قادر به انجام آن خواهند بود دریافت داده، فایل های صوتی، تصویری و سایر نمونه فایل های دیگر است. این کار با استفاده از پروتکل FTP قابل انجام است.

ویژگی های پروتکل FTP

پروتکل FTP ، اولین تلاش انجام شده برای ایجاد یک استاندارد به منظور مبادله فایل بر روی شبکه های مبتنی بر پروتکل TCP/IP است که از اوایل سال 1970 مطرح و مشخصات استاندارد آن طی RFC 959 در اکتبر سال 1985 ارائه گردید.

پروتکل FTP دارای حداکثر انعطاف لازم و امکان پذیر به منظور استفاده در شبکه های مختلف با توجه به نوع پروتکل شبکه می باشد .

پروتکل FTP از مدل کلاینت – سرور تبعیت میکند . برخلاف HTTP که یک حاکم مطلق در عرصه مرورگرهای وب و سرویس دهندگان وب است ، نمی توان ادعای مشابهی را در رابطه با پروتکل FTP داشت چون هم اینک مجموعه ای گسترده از سرویس گیرندگان و سرویس دهندگان FTP وجود دارد .

برای ارسال فایل با استفاده از پروتکل FTP به یک سرویس گیرنده FTP (در سمت کلاینت) نیاز است . ویندوز دارای یک برنامه سرویس گیرنده FTP از قبل تعبیه شده بوده ولی دارای محدودیت های مختص به خود می باشد . در این رابطه نرم

افزارهای متعددی تاکنون طراحی و پیاده سازی شده است که WsFTP Professional، FTP Explorer و Smart FTP نمونه هائی در این زمینه می باشند .

پروتکل FTP را می توان به عنوان یک سیستم پرس وجو نیز تلقی نمود چراکه سرویس گیرندگان و سرویس دهندگان گفتگوی لازم به منظور تائید یکدیگر و ارسال فایل را انجام می دهند. علاوه بر این، پروتکل فوق مشخص می نماید که سرویس گیرنده و سرویس دهنده، داده را بر روی کانال گفتگو ارسال نکنند. در مقابل ، سرویس گیرنده و سرویس دهنده در خصوص نحوه ارسال فایل ها بر روی اتصالات مجزا و جداگانه (یک اتصال برای هر ارسال داده) با یکدیگر گفتگو خواهند کرد (نمایش لیست فایل های موجود در یک دایرکتوری نیز به عنوان یک ارسال فایل تلقی می گردد) .

پروتکل FTP امکان استفاده از سیستم فایل را مشابه پوسته یونیکس و یا خط دستور ویندوز در اختیار کاربران قرار می دهد . سرویس گیرنده در ابتدا یک پیام را برای سرویس دهنده ارسال و سرویس دهنده نیز به آن پاسخ خواهد داد و در ادامه ارتباط غیرفعال می گردد. وضعیت فوق با سایر پروتکل هائی که به صورت تراکنشی کار می کنند متفاوت می باشد (نظیر پروتکل HTTP) . برنامه های سرویس گیرنده زمانی قادر به شبیه سازی یک محیط تراکنشی می باشند که از مسائلی که قرار است در آینده محقق شوند ، آگاهی داشته باشند . در واقع ، پروتکل FTP یک دنباله statefull از یک و یا چندین تراکنش است.

سرویس گیرندگان ، مسئولیت ایجاد و مقداردهی اولیه درخواست ها را برعهده دارند که با استفاده از دستورات اولیه FTP انجام می گردد. دستورات فوق، عموما" سه و یا چهار حرفی می باشند (مثلا" برای تغییر دایرکتوری از دستور cwd استفاده می شود). سرویس دهنده نیز بر اساس یک فرمت استاندارد به سرویس گیرندگان پاسخ خواهد داد(یک عدد سه رقمی که به دنبال آن از space استفاده شده است به همراه یک متن تشریحی). سرویس گیرندگان می بایست صرفا" به کد عددی نتیجه استناد نمایند چراکه متن تشریحی تغییر پذیر بوده و در عمل برای اشکال زدائی مفید است (برای کاربران حرفه ای) .

پروتکل FTP دارای امکانات حمایتی لازم برای ارسال داده با نوع های مختلف می باشد. دو فرمت متداول، اسکی برای متن (سرویس گیرنده با ارسال دستور TYPE A ، موضوع را به اطلاع سرویس دهنده می رساند) و image برای داده هایی که باینری هستند (توسط TYPE I مشخص می گردد) . ارسال داده با فرمت اسکی در مواردی که ماشین سرویس دهنده و ماشین سرویس گیرنده از استانداردهای متفاوتی برای متن استفاده می نمایند ، مفید بوده و یک سرویس گیرنده می تواند پس از دریافت داده آن را به فرمت مورد نظر خود ترجمه و استفاده نماید. مثلا" در نسخه های ویندوز از یک دنباله carriage return و linefeed برای نشان دادن انتهای خط استفاده می گردد در صورتی که در سیستم های مبتنی بر یونیکس صرفا" از یک linefeed استفاده می شود. برای ارسال هرنوع داده که به ترجمه نیاز نداشته باشد، می توان از ارسال باینری استفاده نمود.

اتخاذ تصمیم در رابطه با نوع ارسال فایل ها در اختیار سرویس گیرنده است (برخلاف HTTP که می تواند به سرویس گیرنده نوع داده ارسالی را اطلاع دهد). معمولا" سرویس گیرندگان ارسال باینری را انتخاب می نمایند و پس از دریافت

فایل ، ترجمه لازم را انجام خواهند داد . ارسال باینری ذاتا" دارای کارآئی بیشتری است چراکه سرویس دهنده و سرویس گیرنده نیازی به انجام تراکنش های on the fly نخواهند داشت. ارسال اسکی گزینه پیش فرض انتخابی توسط پروتکل FTP است و در صورت نیاز به ارسال باینری ، سرویس گیرنده می بایست این موضوع را از سرویس دهنده درخواست نماید یک اتصال پروتکل TCP/IP (نسخه شماره چهار) شامل دو نقطه مجزا می باشد که هر نقطه از یک آدرس IP و یک شماره پورت استفاده می نماید .

برقراری ارتباط بین یک سرویس گیرنده و یک سرویس دهنده منوط به وجود چهار عنصر اطلاعاتی است :

آدرس سرویس دهنده، پورت سرویس دهنده، آدرس سرویس گیرنده و پورت سرویس گیرنده . در زمان برقراری یک ارتباط ، سرویس گیرنده از یک شماره پورت استفاده می نماید. این شماره پورت می تواند متناسب با نوع عملکرد برنامه سرویس گیرنده به صورت اختیاری و یا اجباری باشد. مثلا برخی برنامه های سرویس گیرنده به منظور ارتباط با سرویس دهنده، نیازمند استفاده از یک شماره پورت خاص می باشند، نظیر برنامه های سرویس گیرنده وب و یا مرورگرهای وب که از پورت شماره 80 به منظور ارتباط با سرویس دهنده وب استفاده می نماید. در مواردی که الزامی در خصوص شماره پورت وجود ندارد از یک شماره پورت موقتی و یا ephemeral استفاده می گردد. این نوع پورت ها موقتی بوده و توسط IP stack ماشین مربوطه به متقاضیان اختصاص داده شده و پس از خاتمه ارتباط، پورت آزاد می گردد. با توجه به این که تا زمانی که تمام pool تکمیل نشده باشد اکثرا IP Stacks بلافاصله از پورت موقت آزاد شده استفاده نخواهند کرد، در صورتی که سرویس گیرنده مجددا درخواست برقراری یک ارتباط را نماید ، یک شماره پورت موقتی دیگر به وی تخصیص داده می شود .

پروتکل FTP منحصرا" از پروتکل TCP استفاده می نماید(هرگز از پروتکل UDP استفاده نمی شود) . معمولا" پروتکل های لایه Application (با توجه به مدل مرجع OSI) از یکی از پروتکل های TCP و یا UDP استفاده میکنند (به جزء پروتکل DNS). پروتکل FTP نیز از برخی جهات شرایط خاص خود را دارد و برای انجام وظایف محوله از دو پورت استفاده می نماید . *این پروتکل معمولا" از پورت شماره 20 برای ارسال داده و از پورت 21 برای گوش دادن به فرامین استفاده میکند* . توجه داشته باشید که برای ارسال داده همواره از پورت 20 استفاده نمی گردد و ممکن است در برخی موارد از پورت های دیگر استفاده شود .

اکثر سرویس دهندگان FTP از روش خاصی برای رمزنگاری اطلاعات استفاده نمیکنند و در زمان login سرویس گیرنده، اطلاعات مربوط به نام و رمز عبور کاربر به صورت متن معمولی در شبکه ارسال می گردد. افرادی که دارای یک Packet Sniffer بین سرویس گیرنده و سرویس دهنده باشند ، می توانند به سادگی اقدام به سرقت نام و رمز عبور نمایند . علاوه بر سرقت رمزهای عبور، مهاجمان می توانند تمامی مکالمات بر روی اتصالات FTP را شنود و محتویات داده های ارسالی را مشاهده نمایند. پیشنهادات متعددی به منظور ایمن سازی سرویس دهنده FTP مطرح می گردد ولی تا زمانی که رمزنگاری و

امکانات حفاظتی در سطح لایه پروتکل IP اعمال نگردد (مثل رمزنگاری توسط IPsecs)، نباید از FTP استفاده شود خصوصا" اگر بر روی شبکه اطلاعات مهم و حیاتی ارسال و یا دریافت می گردد .

همانند بسیاری از پروتکل های لایه Application ، پروتکل FTP دارای کدهای وضعیت خطاء مختص به خود می باشد (مانند HTTP) که اطلاعات لازم در خصوص وضعیت ارتباط ایجاد شده و یا درخواستی را ارائه می نماید . زمانی که یک درخواست (GET و یا PUT) برای یک سرویس دهنده FTP ارسال می گردد، سرویس دهنده پاسخ خود را به صورت یک رشته اعلام می کند. اولین خط این رشته معمولا" شامل نام سرویس دهنده و نسخه نرم افزار FTP است. در ادامه می توان دستورات GET و یا PUT را برای سرویس دهنده ارسال نمود. سرویس دهنده با ارائه یک پیام وضعیت به درخواست سرویس گیرندگان پاسخ می دهد .

FTP ، یک پروتکل ارسال فایل است که با استفاده از آن سرویس گیرندگان می توانند به سرویس دهندگان متصل و صرفنظر از نوع سرویس دهنده اقدام به دریافت و یا ارسال فایل نمایند. پروتکل FTP به منظور ارائه خدمات خود از دو حالت متفاوت Active Mode و Passive Mode استفاده می نماید.

مدهای کاری سرویس دهنده FTP

ActiveMode

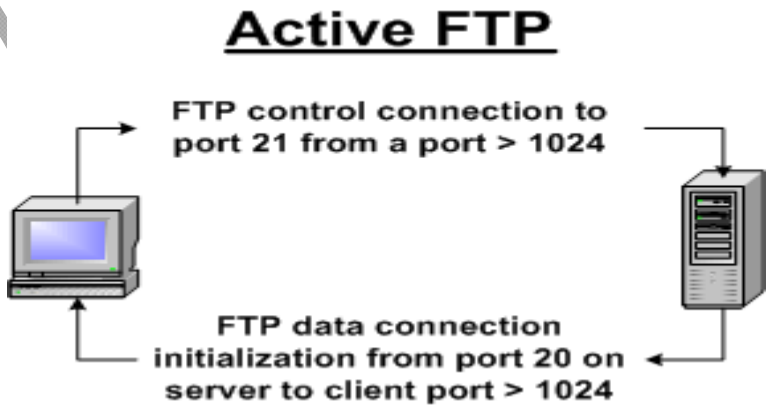
Active Mode ، روش سنتی ارتباط بین یک سرویس گیرنده FTP و یک سرویس دهنده می باشد، تمام FTP های دنیا در دو mode کار می کنند. یا Active هستند یا Passive . که البته به طور پیش فرض FTP ها در حالت اکتیو کار می کنند که عملکرد آن بر اساس فرآیند زیر است:

در این حالت کلاینت یک پورت بالاتر از 1024 باز کرده و از طریق آن یک ارتباط با پورت 21 سرویس دهنده FTP برقرار می کند و روی پورت 21 احراض هویت می شود. پورت 21 ، پورتی است که سرور به آن گوش فرا می دهد تا از صدور فرامین آگاه و آنان را به ترتیب پاسخ دهد. کلاینت برای برقراری ارتباط با سرور از یک پورت تصادفی و موقتی (بزرگتر از 1024) استفاده میکند.

کلاینت شماره پورت لازم برای ارتباط سرویس دهنده با خود را از طریق صدور دستور PORT N+1 به وی اطلاع می دهد. سرور یک ارتباط را از طریق پورت 20 خود با یکی از پورت های بالای 1024 کلاینت برقرار کرده و واگذاری دیتا از طریق پورت شماره 20 سرور به یکی از پورت های بالای 1024 آن آغاز می شود.

در صورتی که کلاینت از سیستم ها و دستگاه های امنیتی خاصی نظیر فایروال استفاده کرده باشد، می بایست تهمیدات لازم به منظور ارتباط کامپیوترهای میزبان راه دور به کلاینت پیش بینی شود تا آنان بتوانند به هر پورت بالاتر از 1024 کلاینت دستیابی داشته باشند. بدین منظور لازم است که پورت های اشاره شده بر روی ماشین کلاینت open باشند. این موضوع می تواند تهدیدات و چالش های امنیتی متعددی را برای سرویس گیرندگان به دنبال داشته باشد. هنگامی که کلاینتها برای دسترسی به اینترنت از NAT استفاده می کنند Active FTP با شکست مواجه می شود چرا که دیوار آتش نمی داند که چه کلاینتی باید داده های بازگشتی را دریافت کند.

شکل زیر چگونگی برقراری ارتباط و پورتهای استفاده شده در حالت Active را نشان می دهد.



Passive Mode

در Passive Mode ،که به آن" مدیریت و یا اداره سرویس گیرندگان FTP" نیز گفته می شود از فرآیند زیر استفاده میگردد :

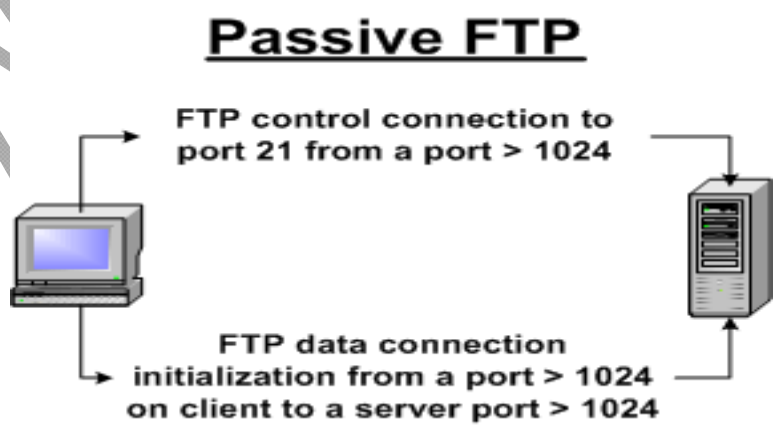
در این حالت کلاینت با پورت 21 خود به سرور FTP متصل شده و عمل احراض هویت و ارسال دستورات کنترلی از همین محل انجام می شود. اما داده ها توسط پورتهای بالای 1024 سرور به پورتهای بالاتر از 1024 کلاینت منتقل می شوند.

Passive FTP سروری است که درخواست فعالی برای ارتباط با کلاینتها جهت تبادل دیتا نمی سازد. به دلیل اینکه کلاینتها معمولا ارتباط مورد درخواست را، خود راه اندازی می کنند این حالت کاری برای کلاینت هایی که به وسیله دیوارآتش محافظت می شوند و یا پشت Nat قرار دارند بهتر است.

در فرآیند فوق، کلاینت دارای نقش محوری است و فایروال موجود بر روی کلاینت می تواند درخواست های دریافتی غیرمجاز به پورت های بالاتر از 1024 را به منظور افزایش امنیت بلاک نماید. در صورتی که بر سر راه کامپیوترهای سرور نیز فایروال نصب شده باشد ، می بایست پیکربندی لازم به منظور استفاده از پورت های بالاتر از 1024 بر روی آن انجام گردد . باز نمودن پورت های فوق بر روی فایروال و یا سرور می تواند چالش های امنیتی خاصی را به دنبال داشته باشد. متاسفانه تمامی کلاینتهای FTP از Passive Mode حمایت نمی کنند.

اگر یک کلاینت بتواند به یک سرور login کند ولی قادر به ارسال داده بر روی آن نباشد ، نشان دهنده این موضوع است که فایروال و یا Gateway برای استفاده از PassiveMode به درستی پیکربندی نشده است. فایروال ها اجازه ایجاد ارتباط به درون خود را نمی دهند، هنگامی که فایروال نادرست پیکربندی شود، ارتباط کلاینتها به هیچ وجه برقرار نمی شود چه برای Active و چه برای Passive .

شکل زیر چگونگی برقراری ارتباط و پورتهای استفاده شده در حالت Passive را نشان می دهد.



مقایسه بین اکتیو و پسیو به زبان ساده :

مهمترین تفاوت بین روش های فوق جایگاه سرویس دهنده و یا سرویس گیرنده در ایجاد و خاتمه یک ارتباط است. در حالت Active باید فایروال کلاینتها پیکربندی شود ولی در حالت Passive فایروال سمت سرور کانفیگ میشود. مشکل Active در همین است که باید فایروال سمت کلاینت توسط خود کاربر پیکربندی شودکه این می تواند مشکل آفرین باشد. اما در حالت Passive تنظیمات فایروال توسط مدیر شبکه انجام می شود بنابراین لازم است به فایروال سمت سرور اجازه داده شود که به اتصالات هر پورت بالاتر از 1024 پاسخ دهد. ترافیک فوق، معمولا" توسط فایروال سمت سرور بلاک می گردد. در چنین شرایطی امکان استفاده از Passive Mode وجود نخواهد داشت .

حالت Passive دارای سرعت بالاتر و overhead کمتری است و نداشتن مشکلات فایروالی هم جزو محسنات این مد به حساب می آید. با توجه به مستندات درج شده در RFC 1579 ، *استفاده از Passive Mode به دلایل متعددی به Active Mode ترجیح داده می شود.* تعداد سرویس دهندگان موجود بر روی اینترنت به مراتب کمتر از سرویس گیرندگان می باشد. با استفاده از امکانات موجود می توان سرویس دهندگان را طوری پیکربندی کرد تا بتوانند از مجموعه پورت های محدود و تعریف شده ای با در نظر گرفتن مسائل امنیتی ، استفاده نمایند.معروف ترین و بهترین این سرویس دهنده ها از نظر ردهت VSFTP می باشد که در این فصل به طور اجمالی مورد بررسی قرار می گیرد.

FTP از دیدگاه کاربران

از دیدگاه کاربران دو نوع FTP وجود دارد که عبارتند از:

Regular FTP
Anonymous FTP

تعریف Regular FTP: در این روش دسترسی به FTP نیازمند احراض هویت است و ارسال و دریافت و دسترسی به فایل ها بوسیله کد کاربری و پسورد یوزرهای Local سیستم انجام می شود. در حالت پیش فرض VSFTP به کاربران لینوکس اجازه می دهد که به دایرکتوری Home خود کپی و یا دانلود داشته باشند. اشکال این نوع از FTP این است که امکان دانلود/آپلود از سایر کاربران گرفته می شود.

تعریف Anonymous FTP : در این روش دسترسی همگانی وجود دارد و برای پایگاه هایی که نیاز به تبادل فایل با تعداد زیادی کاربر ناشناخته که از طریق راه دور ارتباط برقرار می کنند روش خوبی است.

در این شیوه کاربر پس از اتصال، به شاخه /var/ftp/ هدایت شده و زیر پوشه های آن دسترسی دارد.

نصب راه اندازی VSFTP

معروفترین در بین سرویس دهندگان خدمات فایل VSFTP و ProFTP می باشد که VSFTP از امنیت بالاتری برخوردار بوده و به شدت Stable می باشد و از مهمترین قابلیت های آن می توان به Multi Homing بودن آن اشاره کرد. این قابلیت اجازه می دهد چندین Ftp Daemon روی یک سرور اجرا شود که هر کدام از اینها تنظیمات مختص به خود را دارند. مبنای احراض هویت VSFTP برای کاربران local فایل /etc/passwd است. یعنی به صورت پیش فرض بانک جداگانه ای برای یوزرها ندارد بلکه از یـــوزرهایLocal پشتیبانی میکند. تنها عیب VSFTP راه اندازی مشکل و سرعت پائین آن به نسبت ProFTP است. VSFTP به صورت پیش فرض به صورت Standalone بالا می آید ولی قابلیت این را دارد که تحت نظر Xinetd ارائه سرویس کند. اکثر Hostingها از ProFTP استفاده می کنند چون سرعت احراض هویت بالاتری دارد و علت آن هم نداشتن ماژول امنیتی بر روی آن است که باعث می شود به راحتی مورد حمله هکرها قرار گیرد. مهمترین مزیت آن فقط سرعت بالای احرض هویت و اتصال آن است و البته بسیاری از فیچرهای VSFTP را هم ندارد.ProFTP به صورت پیش فرض از فایل /etc/passwd استفاده نمی کند بلکه برای احرض هویت یوزرها از فایل جداگانه ای بهره می برد.

جهت نصب این سرویس دهنده میتوان از سرویس Yum و یا اگر پکیج آن از قبل موجود باشد می توان از دستور rpm استفاده کرد. ولی توصیه می شود در صورت امکان از Yum برای نصب نرم افزارها استفاده کنید زیرا نیازمندی های لازم را دانلود و نصب می کند. این قابلیت در rpm وجود ندارد لذا جهت نصب از دستورات زیر استفاده می کنیم .

ابتدا باید از نصب بودن پکیج vsftp اطمینان حاصل کنیم لذا با دستور زیر از سیستم query می گیریم :

#rpm -qa | grep vsftp

- در صورت نصب نبودن ، در سیستم های ردهت جهت نصب vsftpd از yum استفاده می کنیم :

#yum -y install vsftp

- بعد از نصب ، باید اطمینان حاصل کنیم گه آیا پکیج vsftp بر روی سیستم نصب شده است یا خیر

#rpm -qa | grep vsftp

- سپس با دستور زیر شاخه ها و مسیرهایی که فایل های این سرویس در آن ایجاد شده است را چک می کنیم :

#rpm -ql vsftpd

- و با این دستور هم اطلاعات لازم در مورد پکیج این سرویس را به دست می آوریم :

#rpm -qi vsftpd

- سپس با دستور chkconfig مشخص می کنیم در چه runlevel هایی فعال باشد :

#chkconfig vsftpd on

و در انتها سرویس را reset می کنیم :

#service vsftpd restart

مهمترین مسیرهای ایجاد شده توسط VSFTP

با نصب این سرویس چندین شاخه و مسیر جدید به سیستم اضافه می شود که مهمترین آنها در زیر مختصرا توضیح داده شده است :

/etc/vsftpd/
/etc/logrotate.d/vsftpd.log
/etc/pam.d/vsftpd
/etc/rc.d/init.d/vsftpd
/var/ftp/pub/
/usr/sbin/vsftpd/

/etc/vsftpd/

در زیر این دایرکتوری چهار فایل مهم پیکربندی این سرویس قرار دارند که شامل فایل های زیر می شوند :

vsftpd.conf
user_list
ftpusers
vsftpd_conf_migrate.sh

- **vsftpd.conf**: این فایل، اصلی ترین فایل پیکربندی سرویس vsftpd می باشد.
- **user_list**: این فایل شامل لیست یوزرهایی است که به آنها دسترسی یا عدم دسترسی به FTP داده می شود، به شرط آنکه گزینه **userlist_deny** را در فایل پیکربندی اصلی، مقدار دهی کرده باشیم.
- **ftpusers**: هر یوزری که نام آن در این فایل قرار بگیرد به آن یوزر اجازه login به FTP داده نمی شود. در اصل این فایل یک blacklist می باشد.
- **vsftpd_conf_migrate.sh:** برای migrate کردن و جابه جایی بین دو FTP سرور از این اسکریپت استفاده میشود.

و در ادمه :

/etc/logrotate.d/vsftpd.log

فایل کانفیگ rotate لاگ این سرویس در این آدرس قرار دارد.

/etc/pam.d/vsftpd

Pam یک مکانیزم امنیتی است که برای کنترل سرویس ها به کار می رود. اگر بخواهیم مکانیزم احراض هویت vsftpd در اختیار pam باشد باید در این فایل تنظیمات لازم را اعمال کنیم.

/etc/rc.d.init.d/vsftpd

اسکریپت اجرای سرویس در این مکان قرار دارد. vsftpd به صورت standalone اجرا میشود و در زیر مجموعه init قرار دارد.

/var/ftp/pub/

این مسیر برای قرار دادن فایل، و دایرکتوری جاری یوزرهایی که لاگین می کنند به کار می رود. به این مسیر ftproot گفته می شود. تمام یوزرهای anonymous به طور پیش فرض وارد این دایرکتوری می شوند و کاربران local هم بعد از ورود به FTP به دایرکتوری home مربوط به خودشان هدایت خواهند شد مگر اینکه ما این مسیر را تغییر دهیم .

/usr/sbin/vsftpd

فایل اجرایی دستور vsftpd در این مسیر قرار دارد .

مروری بر تنظیمات فایل کانفیگ اصلی VSFTP

Syntax این فایل بدین گونه است که هر چیزی که درون آن نوشته می شود باید بدون فاصله باشد. کلا برای اتصال به vsftpd دو نوع یوزر داریم. این یوزرها یا یوزر local سیستم هستند یا یوزرهای anonymous . کانفیگ کلی vsftpd بدون آپشن خاصی 13 خط بیشتر نمی شود که در زیر 51 عدد از مهمترین این آپشن ها توضیح داده شده است . در این فصل کاربران anonymous به اختصار anon نامیده می شوند.

#vi /etc/vsftpd/vsftpd.com

anonymous_enable=YES

Yes بودن این گزینه به کاربران anonymous اجازه می دهد که از طریق محیط گرافیکی بدون پسورد وارد دایرکتوری pub سرور FTP شوند. یوزرهای anon اجازه **chroot** ندارند .

anon_root=/opt/dir_anon

اگر بخواهیم کاربران anon به محض ورود به FTP به دایرکتوری مشخصی هدایت شوند در جلوی این گزینه مسیر مورد نظر را وارد می کنیم.

anon_upload_enable=YES

Yes بودن این آپشن اجازه می دهد یوزرهای anon بتوانند در FTP فایل آپلود کنند.

anon_mkdir_enable=YES

با Yes قرار دادن مقدار این خط یوزرهای anon می توانند در FTP دایرکتوری ایجاد کنند.

anon_max_rate=4000

مقدار این خط نرخ حداکثری سرعت دانلود و آپلود یوزرهای anon را مشخص می کند. این نرخ بر اساس بایت می باشد.

no_anon_passwd=YES

با فعال کردن این خط، برنامه ftp در محیط cli از یوزرهای anon پسورد نمی خواهد.

anon_umask=???

مجوز های پیش فرض ایجاد فایل و دایرکتوری، برای کاربرanonymous را تعیین می کند.

anon_other_write_enable = NO

اگر این خط برابر YES باشد کاربران anon به غیر از آپلود و ایجاد دایرکتوری مجاز به انجام عملیات نوشتن، حذف و تغییر نام خواهند شد. به طور کلی این کار توصیه نمی شود اما برای تکمیل مطالب این بخش آورده شده است.

allow_anon_ssl = YES

این خط اگر YES باشد کاربران anon مجاز به استفاده از ارتباطات امن SSL می باشند.

force_anon_logins_ssl =YES

در صورت فعال بودن ssl_enable و این گزینه، کاربران anon مجبور به برقراری یک اتصال امن SSL برای ارسال رمز عبور خواهند بود.

nopriv_user=ftpsecure

اگر اجازه آپلود را به یوزرهای anon بدهیم باید قابلیت اجرا را از آنها بگیریم. برای این کار مثلا یک یوزر به نام ftpsecure ساخته و اجازه اجرای فایل را از آن می گیریم. با وارد کردن نام یوزر مربوطه در اینجا، از این به بعد سطح دسترسی این یوزر به یوزرهای anon اعمال می شود. این کار برای امن سازی FTP لازم است.

chown_uploads=YES

chown_username= نام یوزر

اگر بخواهیم مالک (owner) فایل های که یوزرهای anon آپلود می کنند یوزر دیگری باشد تا خاصیت اجرا را از یوزر anon بگیریم خط اول را برابر YES قرار داده و در خط دوم نام یوزری که می خواهیم owner فایل ها باشد را وارد می کنیم. مثل یوزری که قابلیت لاگین را از آن گرفته باشیم.

local_enable=YES

با فعال کردن این گزینه یوزرهای local ای که داخل فایل passwd واقع در دایرکتوری /etc هستند این اجازه را پیدا می کنند با یوزر و پسورد خود به FTP لاگین کرده و وارد دایرکتوری خانگی خودشان بشوند. یوزرهای local اجازه **changroot** را دارند که برای سیستم یک خطر امنیتی محسوب شده و باید این قابلیت را از آنها گرفت.

chroot_local_user=YES

اگر این خط برابر YES باشد از تمام یوزرهای local قابلیت change root گرفته می شود.

write_enable=YES

این گزینه به یوزرهای local اجازه آپلود فایل را می دهد. این آپشن زمانی کاربرد دارد که فایل را تحت FTP بسازیم .

local_umask=022

این umask، پرمیژن پیش فرضی است که به فایلهای آپلود شده توسط کاربران local اعمال می شود.

local_max_rate=10000

مقدار این خط نرخ حداکثری سرعت دانلود و آپلود یوزرهای local را مشخص می کند. این نرخ بر اساس بایت می باشد .

local_root=/var/tmp

اگر بخواهیم کاربران local به محض ورود به FTP به دایرکتوری مشخصی هدایت شوند در جلوی این گزینه مسیر مورد نظر را وارد می کنیم.

dirmessage_enable=YES

این گزینه فقط مختص یوزرهایی است که تحت CLI به FTP لاگین می کنند. ما می توانیم برای هر دایرکتوری یک message ایجاد کنیم تا به محض ورود کاربر به آن دایرکتوری پیام مورد نظر برای کاربر به نمایش داده شود. برای ایجاد پیام به داخل دایرکتوری مورد نظر رفته و یک فایل به نام message. ایجاد می کنیم و پیام مورد نظرمان را درون آن ذخیره می کنیم. با yes بودن این خط ، vsftpd به محض ورود کاربر به دایرکتوری از قبل مشخص شده ، ابتدا آنجا را چک می کند تا ببیند آیا چنین فایلی وجود دارد یا خیر . در صورت وجود داشتن، پیام داخل آن را برای کاربر نمایش می دهد.

xferlog_enable=YES

لاگ های vsftpd به دو صورت ذخیره می شوند. یا با فایل vsftpd.log درون خود vsftpd ذخیره می شود که باید این گزینه NO باشد. یا با YES قرار دادن این خط کاری می کنیم log آن توسط log سرور در دایرکتوری مربوطه ذخیره شود.

listen=YES

اگر این گزینه برابر YES باشد FTP در مد standalone و تحت نظر init کار می کند. اگر بخواهیم این سرویس تحت نظر xinetd اداره شود باید این گزینه را برابر NO قرار داده و در زیر xinetd یک فایل کانفیگ به نام vsftpd بسازیم. در انتهای این فصل نمونه ای از این فایل آورده شده است.

max_per_ip=20

این خط مشخص می کند چه تعداد کانکشن می تواند از هر IP به سرور متصل شود.

max_cllient=100

این خط بیان می کند در یک زمان حداکثر چند یوزر می توانند هم زمان به FTP متصل شوند. (عدد 100 مثال است)

ftp_banner=welcome to FTP
banner_file=/opt/ftp/ftp.txt

هر متنی که در جلوی عبارت خط اول نوشته شود برای یوزرهایی که با محیط CLI لاگین کرده اند نمایش درمی آید. *باید دقت داشت در جلو این عبارت نمی توان بیش از یک خط نوشت*. اگر متن ما بیش از چند خط بود آن را در یک فایل جداگانه نوشته و آدرس آن را در جلوی خط دوم وارد میکنیم.

pam_service_name=VSFTPD
tcp_wrappers=YES

این دو خط مکانیزم های امنیتی کنترل سرویس FTP را مشخص می کند. اگر بخواهیم رنجی از IP را Block کنیم تا به FTP دسترسی نداشته باشند باید از مکانیزم امنیتی tcp_wrappers استفاده شود. البته باید از قبل IP های مجاز و غیر مجاز را درون فایل های /etc/hosts.allow **و** /etc/hosts.deny وارد کنیم .

userlist_enable=YES
userlist_file=/etc/vsftpd/user_list

اگر مقدار این خط YES باشد محتویات فایلی که در خط دوم، مسیر دهی شده خوانده می شود و فقط به یوزرهای که در این فایل ثبت شده اند اجازه دسترسی به FTP داده می شود.

userlist_deny=YES
userlist_file=/etc/vsftpd/user_list

اگر مقدار این خط YES باشد محتویات فایلی که در خط دوم مسیر دهی شده خوانده می شود و اسامی یوزرهایی که در این فایل قرار دارند نمی توانند به FTP دسترسی داشته باشند.

chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list

این خطوط برای jail کردن یوزرها به کار می رود. *اگر قابلیت change root را از یوزری بگیریم اصطلاحا می گوییم یوزر را jail کرده ایم*. اگر بخواهیم بعضی از یوزرهای local قابلیت change root نداشته باشند خط اول را برابر YES قرار داده و در خط دوم آدرس لیست یوزرهای انتخابی را وارد می کنیم. این فیچر مخصوص یوزرهای local می باشد .

deny_email_enable=YES
banned_email_file=/etc/vsftpd/banned_emails

وقتی کاربر با مرورگر خود به یک FTP وصل میشود، در صورتی که یوزر local نباشد به صورت یوزر anon لاگین کرده و به صورت پیش فرض وارد مسیر /var/ftp/ می شود. اگر دقت کرده باشید بسیاری از سایتهای ftp موقع ورود از شما یوزر و پسورد نمی خواهد در صورتی که برای ورود، یوزر و پسورد anon نیاز است . توضیحی که برای این اتصال بدون پسورد وجود دارد این است که همه مرورگرها یک یوزر و پسورد پیش فرض داخلی برای احراض هویت دارند که در چنین مواقعی از آن استفاده میکنند. به طور مثال پسورد داخلی فایرفاکس mozila@example.com است . حال اگر این پسورد را در فایل banned_email وارد کنیم هیچ کاربری نمی تواند با مرورگر فایرفاکس به FTP متصل شود. این کار را برای محدود سازی اتصال با مرورگرهای خاص است. به این کار banned کردن ایمیل گفته می شود.

port_enable=YES
pasv_enable=YES

خط اول مشخص می کند FTP ما در Active mode کار کند و خط دوم حالت Passive را فعال میکند.

idle_session_timeout=300

این خط بیان میکند در صورتی که کاربر غیر فعال بود بعد از چند ثانیه ارتباط او توسط سرور قطع شود.

delete_failed_uploads=YES

اگر این گزینه فعال (YES) باشد تمامی آپلود هایfailed شده پاک خواهند شد .

download_enable=YES

اگر این گزینه فعال (YES) باشد تمامی درخواست های دانلود **رَد** خواهند شد.

listen_port=21

به طور پیش فرض پورت این سرویس ۲۱ است که برای امنیت بیشتر می توان این پورت را تغییر داد. البته همزمان باید در فایل کانفیگ این سرویس در Xinetd و فایل /etc/services تغییراتی را اعمال نمود.

listen_address=192.168.1.1

اگر چندین کارت شبکه روی سرور داشته باشیم می توانیم یکی از آنها را به سرویس FTP اختصاص دهیم. حتی اگر درخواست ها زیاد باشد می توان چندین کارت شبکه را به این امر اختصاص داد. اگر این پارامتر مقدار دهی نشود تمامی کارت های شبکه برای این کار استفاده می شوند.

ascii_download_enable=YES

YES این خط انتقال داده به صورت اسکی را فعال می کند.

force_dot_file=YES

در صورتی که این خط مقدار YES داشته باشد حتی اگر دستور فهرست کردن دایرکتوری ها بدون سوییچ a باشد باز هم فایل های که ابتدایشان نقطه دارند نشان داده خواهد شد(فایل های مخفی)

ls_recurse_enable=YES

اگر این آپشن فعال باشد اجازه اجرای دستور ls –R را دارید. فقط یک مشکلی که دارد این است که بکارگیری این آپشن در سایت های که حجم فایل بالایی بر روی آنها وجود دارد باعث هدر رفتن منابع سیستم می گردد.

dirlist_enable =NO

اگر این خط NO باشد به هیچ کدام از دستورات directory list اجازه اجرا داده نمی شود.

hide_ids=YES

اگر این گزینه فعال باشد همه اطلاعات کاربر و گروه ، در لیست دایرکتوری را نمایش می دهد.

dual_log_enable=YES

اگر این گزینه را فعال کنیم دو نوع لاگ برای ما تهیه می کند. یکی xferlog که لاگ پیش فرض است و یکی هم لاگ vsftpd را ثبت می کند.

force_dot_files=YES

اگر بخواهیم فایل های مخفی برای کاربران به نمایش در بیاید این گزینه را برابر YES قرار می دهیم.

جهت اطلاعات بیشتر لطفا man vsftpd.conf را مطالعه بفرمائید.

تغییر مسیر یوزرهای Local بعد از login به FTP

یوزرهای anon به صورت پیش فرض بعد از login به مسیر /var/ftp/ هدایت می شوند ولی یوزرهای Local سیستم بعد از Login به دایرکتوری Home خود وارد می شوند.

ما می توانیم کارکنیم که یوزرهای Local به جای اینکه به دایرکتوری Home خودشان بروند به /var/ftp/ هدایت شوند و یا قابلیت ساخت دایرکتوری، فایل، آپلود و دانلود را هم به آنها داده ، یا آنها را بنا بر سیاست های کاری محدود کنیم.

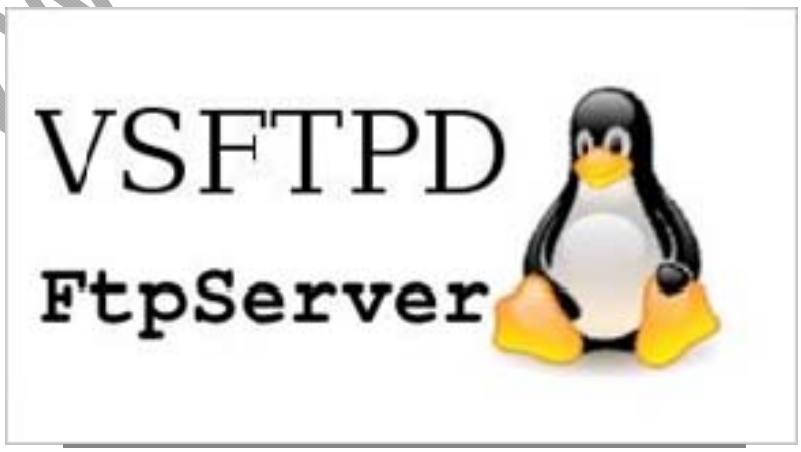
برای چنین کاری خطوط زیر را در فایل اصلی پیکربندی اصلاح می کنیم :

#vi /etc/vsftpd/vsftpd.conf

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=002
dirmessage_enable=YES
local_root=/var/ftp/pub
```

نکته : معمولا سیستم های گرافیکی، کانکشن FTP را cash میکنند.

نکته مهم : اگر گزینه ای را بخواهیم غیر فعال کنید بهتر است به جای کامنت کردن ، در جلوی آن NO را بنویسیم .



محدود کردن دسترسی یوزرها به FTP

اگر بخواهیم تعداد خاصی از یوزرهای Local به FTP دسترسی داشته باشند باید اسامی آنها را داخل یکی از فایل های ftpusers و یا user_list وارد کرده و در فایل کانفیگ تغییراتی را اعمال کنیم. اگر بخواهیم از بین تعداد زیادی ازیوزرها فقط بعضی اجازه دسترسی به FTP داشته باشند باید گزینه userlist_deny=??? را در فایل کانفیگ برابر NO قرار دهیم. در صورت NO بودن این گزینه فقط یوزرهای موجود در فایل user_list می توانند به FTP دسترسی داشته باشند.

YES بودن گزینه userlist_deny=??? چندان هم منطقی نیست. اگر این گزینه برابر YES باشد و اسامی تعریف شده در فایل user_list در ftpusers هم موجود باشند آنوقت YES بودن این گزینه بی معنی می شود چون از طریق بررسی فایل ftpusers به یوزرها اجازه دسترسی داده می شود. در این حالت هر دو فایل جهت اعطا حق دسترسی مورد بررسی قرار می گیرند. اما اگر این مقدار برابر NO باشد دیگر فایل ftpusers مورد بررسی قرار نمی گیرد.

Jail کردن یوزرها در FTP

وقتی کاربری به FTP لاگین می کند نباید بتواند به ریشه دایرکتوری، که به آن وارد شده اند برود. به طور مثال اگر تعریف کرده باشیم یوزر به محض ورود به دایرکتوری /var/ftp/ هدایت شود ، نباید بتواند به سمت دایرکتوری بالایی تغییر دایرکتوری بدهد . به جلوگیری از چنین کاری **Jail** کردن یوزر گفته می شود.

با این کار قابلیت chroot را از یوزرها سلب کردیم. برای Jail کردن یوزرها آپشن زیر باید مقدار **YES** داشته باشد تا قابلیت chroot غیر فعال شود.

chroot_local_user=YES

اگر هم بخواهیم قابلیت chroot برای بعضی از یوزرها فعال شود کافی است اسم آنها را در یک فایل قرار داده و در خط زیر آدرس دهی کنیم .

chroot _list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list

بر طرف کردن Error 500

در centos سری 6 ممکن است در هنگام login یوزرهای local ، به آنها error 500 نشان داده شود . ممکن است نتوانند به دایرکتوری Home خود بروند یا اجازه write پیدا نکنند. یا فرضا ما یکسری از قابلیت ها را فعال می کنیم ولی در عمل کار نمی کنند. دلیل آن هم به خاطر عدم پیکربندی متغیرهای بولین Selinux است. این متغیرها را با دستور زیر می توان مشاهده کرد :

#getsebool -a

یکی از مهمترین این متغیرها **allow_ftpd_anon_write=off** می باشد. مثلا اگر در فایل کانفیگ اجازه رایت به یوزرهای anon داده شده باشد، تا این متغیر on نشود اجازه write به یوزرهای anon داده نمی شود .یکی دیگر از مهمترین متغیرها، **ftp_home_dir = off** می باشد . این متغیر به یوزرهای local اجازه می دهد تا بتوانند از طریق FTP وارد دایرکتوری home خود بشوند. فعال بودن این متغیر است که باعث می شود که error 500 برای یوزرها نمایش داده شود و از رفتن به دایرکتوری خانگی آنها ممانعت به عمل آید. با دستور setsebool میتوان مقدار این متغیر ها را تغییر داد:

#setsebool -P ftp_home_dir=1

در Selinux برای هر سرویس مقدار زیادی متغیر وجود دارد که باید بعد از راه اندازی هر سرویس متغیرهای آن را پیکربندی کنیم . بزرگترین اشتباه آن است که Selinux را غیر فعال کنیم.

Selinux در سه مد کار می کند:

1. enforcing : این مد بالاترین درجه امنیت در Selinux را دارا میباشد. اگر این مد را فعال کنیم تمام ماژول های امنیتی سیستم enable می شود.
2. permissive : در این مد Selinux فعال نیست و چیزی را denay نمی کند اما از همه چیز log برداری میکند .
3. disable : با فعال کردن این مد Selinux کاملا غیر فعال می شود.

فایل کانفیگ Selinux در مسیر **/etc/selinux/config** قرار دارد. برای تغییر در مدهای آن این فایل را باز کرده و در مقابل کلمه SELINUX مد مربوطه را وارد می کنیم و برای اعمال شدن آن حتما باید سیستم را یکبار ریست کنیم. از دستورات زیر هم جهت تغییر مد آن می توان استفاده کرد :

#setenforce 0
#echo 0 > /selinux/enforce

با دستور زیر هم می توان از وضعیت Selinux و مدهای کاری آن کسب اطلاع کرد :

#setstatus

ایجاد Mullti Homing در FTP

به طور معمول بر روی هر سیستم فقط یک سرویس دهنده FTP راه اندازی می شود در حالی که با Vsftpd می توان چندین سرویس دهنده مستقل FTP را روی یک سرور راه اندازی کرد. فرض کنید یک سرور داریم که هم زمان به اینترنت و شبکه داخلی سرویس می دهد و می خواهیم یک FTP به کاربران اینترنتی و یک FTP به کاربران شبکه داخلی سرویس بدهد. در چنین شرایطی از خاصیت Mullti Homing استفاده می کنیم. لذا باید برای هر سرور یک فایل کانفیگ جداگانه با نام منحصر به فرد، در زیر دایرکتوری /etc/vsftpd/ ایجاد کنیم و برای هر کارت شبکه یک آدرس IP اختصاصی تنظیم کرده و در هر فایل کانفیگ یکی از آنها را وارد میکنیم. مهمترین گزینه ای که در فایل کانفیگ باید آورده شود listen_address است که به کارت شبکه مختص به سرویس اشاره دارد.

طبق توصیه اکید Redhat، مکان ذخیره لاگ هر کدام از این سرورها باید با دیگری فرق داشته باشد. قبلا گفته شد که vsftpd به دو صورت log برداری میکند که xferlog نحوه پیش فرض لاگ گرفتن این سرویس می باشد.

می توانیم به یک کارت شبکه سرور دو IP اختصاص داده و هر IP را مختص یک سرویس دهنده فایل قرار دهیم به این کار Virtual Host گفته می شود. برای این کار باید از فایل کانفیگ اصلی یک کپی با یک نام دلخواه ایجاد کرده و تنظیمات مربوطه به آدرس IP مورد نظر و پورت دلخواه را درون آن وارد کنیم.

#vi /etc/vsftpd/vsftpd2.conf

```
listen=YES
local_enable=NO
anonymous_enable=YES
write_enable=YES
anon_max_rat=YES
an0n_root=/opt
listen_address=192.168.1.1
listen_port=2020
```

#vsftpd /etc/vsftpd/vsftpd2.conf

با این دستور فقط فایل vsftpd2.conf ریست می شود و بقیه FTP ها به کارشان ادامه می دهند. چون نیازی نیست همه آنها با هم ریست شوند پس بهتر است فقط فایل کانفیگ مربوطه را ریست کنیم.

استفاده از دستور ftp به عنوان ابزار کلاینتی

نرم افزار پیش فرض کلاینتی اکثر توزیع های لینوکس ابزار ftp می باشد که برای کپی، انتقال، rename، حذف ، ساختن یک فایل و همچنین تغییر سطح دسترسی می توان از آن استفاده کرد. برای جلوگیری از سرقت اطلاعات بسیار بهتر است که همواره از sftp یا همان secure ftp استفاده کنید که انتقال امن را فراهم می آورد. اگر ارتباط FTP به صورت امن راه اندازی نشود اطلاعات را به صورت clear Text رد و بدل می کند. توصیه می شود بجای ftp از دستور lftp که دارای خصوصیات پیشرفته تر و در عین حالی کار با آن نیز آسانتر است، استفاده کنید. دستور lftp یک دستور تعاملی است یعنی یک چیزی به آن می دهیم و یک چیزی به ما بر می گرداند و نیازی نیست برای هر کاری یک دستور به آن بدهیم. با دستور ftp به طور پیش فرض نمی توان به صورت anon به سرور متصل شد بلکه باید حتما نام یوزر local را وارد کنیم، این دقیقا بر عکس دستور lftp می باشد، چون lftp به صورت پیش فرض با یوزر anon و بدون پسورد به سرور متصل می شود که البته به جای پسورد باید یک کاراکتر دلخواه را وارد کنیم. lftp قادر است همزمان عمل احراض هویت و برقراری اتصال را انجام دهد ولی ftp قادر به انجام این دو کار به صورت همزمان نیست.

نکته : اگر اول یک کامند از علامت ! استفاده کنیم یعنی این دستور را روی سرور اجرا نکن بلکه باید آن را روی سیستم local اجرا کند.

نکته : زمانی که به سرور لاگین می کنیم یکسری کد به همراه پیامهایی به نمایش در می آید. این کدها از قبل تعریف شده هستند و برای ثبت log استفاده می شوند. در اخر این فصل جدول کدهای ftp آمده است.

برای اتصال به یک سرویس دهنده فایل با استفاده از دستور ftp به شیوه زیر عمل کنیم :

```
$ftp  ftp.example.com
      username
      password
```

و شیوه همزمان آن در lftp

```
$lftp  admin@ftp.example.com
```

و یا

```
$lftp  -u  admin  ftp.example.com
```

به جای ftp.example.com می بایست hostname سرور مربوطه و یا نام یکی از دامنه های مستقر بر روی آن را بنویسیم و برای ورود ، اطلاعات اکانت کاربری ftp متعلق به سرور مقصد را وارد نمائید. با دستور ftp نمی توان همزمان هم احراض هویت و هم اتصال برقرار کرد اما در lftp می توان با یک دستور هم لاگین کرده و هم احراض هویت کنیم.

به طور مثال ، مراحل زیر را مشاهده می فرمائید:

```
Trying 87.51.34.132...
Connected to ftp.freebsd.org.
220 ftp.beastie.tdk.net FTP server (Version 6.00LS) ready.
Name (ftp.freebsd.org: vivek): ftp
331 Guest login ok, send your email address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

از این پس، به سبب اینکه از پروتکل ftp بهره می گیرید، اعلان پرامپت شما مطابق زیر خواهد بود:

```
ftp>
```

برای نمایش فایل ها و فولدر ها می توانید از دستور زیر استفاده نمائید:

```
ftp>ls
```

برای مثال احتمالا، اطلاعاتی شبیه به اطلاعات زیر را دریافت می کنید:

```
229 Entering Extended Passive Mode (|||60692|)
150 Opening ASCII mode data connection for '/bin/ls'.
total 10
drwxrwxr-x  2 0    5     512 Jul 19  2007 .snap
drwx------  2 0    0    2048 Jul 19  2007 lost+found
drwxr-xr-x  3 1006  1006   512 Sep 21  2009 pub
drwxr-xr-x  3 1006  1006   512 Jun  5  2007 sup
drwxr-xr-x  4 1006  0     512 Sep 18  2009 www
226 Transfer complete.
ftp>
```

دقت نمائید که ستون آخر نمایش دهنده نام فایل ها و فولدر ها می باشد.

برای ورود به یک فولدر دیگر می توانید از دستور زیر استفاده کنید ، NOT دستور cd ، کامند lcd است.

```
ftp> cd  folder-name
```

برای دریافت یک فایل می توانید از دستور get مطابق مثال زیر استفاده کنید. اگر بخواهیم فایل های دانلودی در یک مسیر مشخص ذخیره شوند باید در محیط دستور ftp ابتدا به آن مسیری که روی سیستم local قرار دارد lcd کرده و سپس اقدام به دانلود فایل ها نمائیم و اگر از سوئیچ **–c** استفاده کنیم در هر مرحله از دانلود یا آپلود ارتباط ما قطع شود در ارتباط بعدی از باقی مانده کار شروع به دانلود یا آپلود می کند :

```
ftp> get  –c resume.pdf
```

و مطابق ذیل مشاهده خواهید کرد که فایل مربوطه دانلود می گردد:

```
local: resume.pdf remote: resume.pdf
229 Entering Extended Passive Mode (|||55093|)
150 Opening BINARY mode data connection for 'resume.pdf' (53077 bytes).
100% |53077      12.58 KiB/s    00:00 ETA
226 Transfer complete.
53077 bytes received in 00:04 (12.57 KiB/s)
```

اگر در همین زمان می خواهید، محل دایرکتوری خود در سیستم Local و مبدا را تغییر دهید، دستور زیر مفید خواهد بود:

```
ftp>lcd  /path/to/new/dir
```

مثل:

```
ftp>lcd  /tmp
```

حتی می توانید با دستور زیر محل دایرکتوری خود در سرور اصلی مشخص نمائید:

```
ftp>lpwd
```

برای دریافت چندین فایل می توانید از دستور زیر استفاده نمائید:

```
ftp>mget *
```

و یا :

```
ftp>mget *.jpg
```

برای حذف یک فایل:

```
ftp>deletefileName
ftp> delete output.jpg
```

و اما دستور زیر که شاید برای خیلی ها تازگی داشته باشد؛ اگر می خواهید فایلی را در سرور از طریق shell آپلود نمائید، یعنی به سروری که متصل شده اید منتقل کنید، کافی است دستور زیر را استفاده کنید:

```
ftp> put  FileName
```

مثلا می خواهید فایل logo.jpg را از کامپیوتر محلی خود به سرور از طریق shell انتقال دهید:

```
ftp> put  logo.jpg
```

و برای آپلود چندین فایل:

```
ftp>mput *
ftp>mput *. jpg
```

اضافه کردن یک دایرکتوری:

```
ftp>mkdir dirName
```

حذف کردن یک دایرکتوری:

```
ftp>rmdir dirName
```

و در نهایت، برای خروج از ftp می توانید دستورات زیر را بکار ببرید:

```
ftp> quit
```

فرق بین مد باینری و اسکی در ftp کلاینت

کلا در دنیا دو نوع کلی فایل وجود دارد 1- اسکی 2 – باینری . فایل های اسکی فایل های text base می باشند مثل فایل های php,asp,html,pdf و کلا هر فایلی که بتوان محتوای آن را خواند فایل اسکی است ، به غیر از این ، تمام فایل ها باینری هستند مثل عکس ، فیلم ، آهنگ و ...

دستور ftp می تواند در دو مد اسکی و باینری فایل ها را منتقل کند. اگر مد انتقال فایل با فایل دریافتی هم خوانی نداشته باشد فایل ها در مقصد برای باز شدن دچار مشکل خواهند شد. پس اگر فایل باینری باشد باید در مد باینری و اگر اسکی باشد باید در مد اسکی نقل و انتقال صورت پذیرد. برای تغییر مد کافی است کلمه ascii را تایپ کنیم . به همین سادگی مد ترانسفر از باینری به اسکی تغییر می کند. نکته : دستور ftp همانند سرویس دهنده آن در دو مد active و passive ارتباط برقرار می کند.

ftp>ascii

SCP یک جایگزین امن برای ftp

از دیدگاه شبکه، سرویس FTP سرویس امنی نیست، زیرا نام کاربری، کلمه عبور و داده ها همگی بدون هیچ گونه رمزنگاری برروی شبکه مبادله می شوند. شکل امن این سرویس SFTP وSCP هستند، که به عنوان جزئی از بسته Openssh در دسترس بوده و به شکل پیش فرض در سیستم های Redhat و CentOS نصب می باشد. به خاطر داشته باشید که SCP برخلاف FTP قابلیت پشتیبانی از بارگیری بی نشان (Anonymous Download) را دارا نیست. فرمان SCP در لینوکس، قالبی همانند فرمان cp را داراست. اولین پارامتر فایل مبدا و دومین پارامتر فایل مقصد را مشخص می کند. در هنگام کپی کردن یا گذاشتن فایل ها در سرویس دهنده SSH ، کاربر باید توسط scp وارد سرویس دهنده شود که برای این کار باید نام سرویس دهنده، نام کاربری و کلمه عبور را با موفقیت به عنوان آرگومان های ورودی به آن ارسال کند. پس از این، فایل موردنظر با پیشوندی از نام کاربری و سرویس دهنده که با یک @ از یکدیگر جدا شده اند، در سمت سرویس دهنده پردازش می شود. قالب مربوط به این موضوع بدین شکل است:

username@servername:filename
username@servername:directoryname

به طور مثال فرض کنید نیاز به کپی کردن فایل etc/syslog.conf/ بر روی سرویس دهنده ای با آدرس 192.168.1.100 و نام کاربری ali داریم. بدین منظور از قالب

etc/syslog.conf/: ali@192.168.1.100

استفاده می کنیم . در صورت تمایل به کپی برداری از کل شاخه etc/ قالب فوق بدین شکل تغییر می یابد.

/etc/:1.100 . ali@192.168

متداولترین کدهای وضعیت FTP

متداولترین کدهای وضعیت FTP به همراه مفهوم هریک در جدول زیر نشان داده شده است .

کدهای وضعیت سری 100	
110	Restart reply
120	Service ready in x minutes
125	Connection currently open, transfer starting
150	File status okay, about to open data
کدهای وضعیت سری 200	
200	Command okay
202	Command not implemented, superfluous at this site
211	System status/help reply
212	Directory status
213	File status
214	System Help message
215	NAME system type
220	Service ready for next user.
221	Service closing control connection. Logged off where appropriate
225	Data connection open; no transfer in progress.
226	Closing data connection. Requested action successful
227	Entering Passive Mode
230	User logged in, continue
250	Requested file action okay, completed
257	"PATHNAME" created.
کدهای وضعیت سری 300	
331	User name okay, need password.
332	Need account for login
350	Requested file action pending further information.
کدهای وضعیت سری 400	
421	Service not available, closing control connection.

425	Can't open data connection
426	Connection closed; transfer aborted.
450	Requested file action not taken. File not available - busy etc..
451	Request aborted: error on server in processing.
452	Requested action not taken. Insufficient resources on system
کدهای وضعیت سری 500	
500	Syntax error, command unrecognized
501	Syntax error in parameters or arguments.
502	Command not implemented.
503	Bad sequence of commands
504	Command not implemented for that parameter.
530	Not logged in.
532	Need account for storing files
550	Requested action not taken. File unavailable
552	Requested file action aborted. Exceeded storage allocation
553	Requested action not taken. File name not allowed
مفهوم برخی از کدهای متداول	
226	دستور بدون هیچگونه خطائی اجراء گردید .
230	زمانی این کد نمایش داده می شود که یک سرویس گیرنده رمز عبور خود را به درستی درج و عملیات login با موفقیت انجام شده باشد .
231	کد فوق نشاندهنده دریافت username ارسالی سرویس گیرنده توسط سرویس دهنده می باشد و تائیدی است بر اعلام وصول Username (نه صحت آن) .
501	دستور تایپ شده دارای خطاء گرامری است و می بایست مجددا" دستور تایپ گردد .
530	عملیات login با موفقیت انجام نشده است . ممکن است Username و یا رمز عبور اشتباه باشد .
550	فایل مشخص شده در دستور تایپ شده نامعتبر است .