

بدینوسیله این شرکت آمادگی خود، جهت همکاری با آن سازمان محترم در زمینه ارائه خدمات جامع شبکه، سخت افزار و نرم افزار را به شرح ذیل به حضورتان اعلام می‌دارد.

- راهکارهای مجازی سازی

مجازی سازی چیست؟

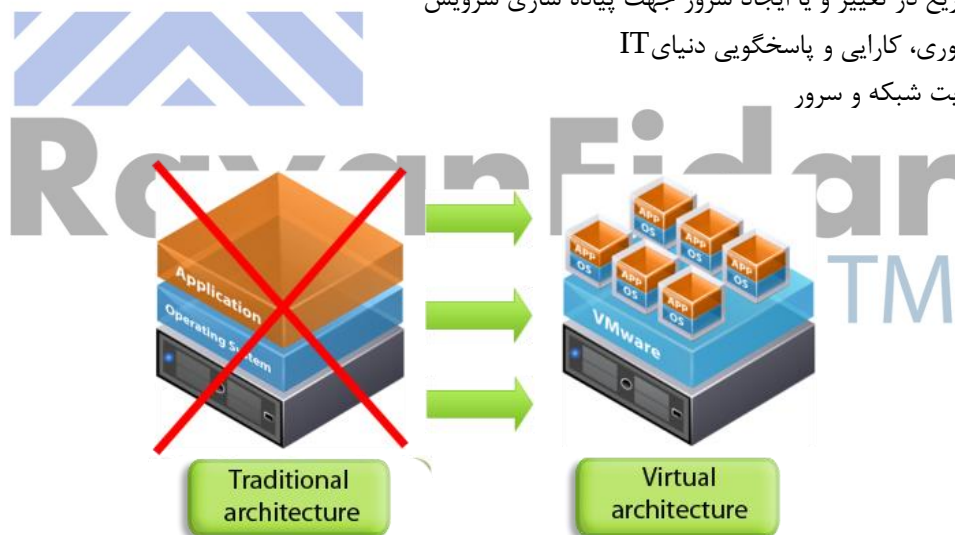
در سالهای اخیر، فناوری های مجازی سازی به عنوان یکی از روندهای پیشرو در حوزه فناوری اطلاعات مطرح گردیده و فرصتهای جدیدی نظیر رایانش ابری را فراهم نموده است. در این راستا، تمرکز اصلی به منظور استفاده از مجازی سازی در زمینه هایی نظیر قابلیت اطمینان، دسترسی پذیری، امنیت و کارایی در حوزه های متعدد کاربردهای سخت افزاری و نرم افزاری میباشد. مجازی سازی فناوری است که با قرارگیری یک لایه بین سخت افزار کامپیوتر و OS سیستم عامل ها مانند Windows, Linux ارائه میشود و با یک دید منطقی از محاسبات منابع (سخت افزار) امکان استفاده از چندین سیستم عامل را به صورت همزمان بر روی یک دستگاه فراهم میکند. شرکت دارای تجربه غنی در ارائه مشاوره، طراحی، پیاده سازی و پشتیبانی، بهینه سازی و آموزش زیر ساخت مجازی در سازمانهای مختلف می باشد. این شرکت بر پایه دانش و تخصص کارشناسان خود این افتخار را دارد که به عنوان یکی از شرکت های دانش محور در زمینه توسعه و ارائه راهکارهای روزآمد فناوری های ذخیره سازی، سرور، شبکه و امنیت در سطوح مختلف فعالیت دارد.



چرا مجازی سازی؟

این تکنولوژی با به کارگیری یک سخت افزار امکان استفاده همزمان از چندین سیستم عامل را فراهم میکند که این امر خود از مزایای زیر بهره مند است :

- 1 صرفه جویی در فضا
- 2 کاهش هزینه ها به واسطه کاهش تعداد سرورها به ازای هر سرویس
- 3 کنترل منابع سخت افزاری به صورت یکپارچه و پویا
- 4 افزایش کارایی و بهره وری از منابع سخت افزاری سرور ها
- 5 آماده سازی سریع تر برنامه ها و منابع
- 6 کاهش گرمای تولید شده در اتاق سرور
- 7 تسهیل و تسریع در تغییر و یا ایجاد سرور جهت پیاده سازی سرویس
- 8 افزایش بهره وری، کارایی و پاسخگویی دنیای IT
- 9 تسهیل مدیریت شبکه و سرور



- راهکارهای پشتیبان گیری

چرا پشتیبان گیری؟

یک عبارت قدیمی در صنعت فناوری اطلاعات وجود دارد: "به جلو نروید تا زمانی که بکاپ تهیه نکرده اید". در واقع از بین رفتن اطلاعات میتواند فاجعه آمیز باشد و یک کسب و کار را نابود کند. در بهترین شرایط خطراتی از جمله نوسانات برق، اشکالات نرم افزار، ویروس ها، باج افزار ها و یا حتی خراب شدن هارد دیسک اطلاعات یک مجموعه را تهدید میکند و همیشه زمانی پشتیبان گیری (Backup) اهمیت پیدا میکند که اطلاعات مجموعه از بین رفته باشد. "نوش دارو پس از مرگ سهراب" در بسیاری از کسب و کارها با توجه به وجود نرم افزارهایی از جمله حسابداری، CRM، اتوماسیون و ... اطلاعات در بستر شبکه مبتنی بر سرور میباشد، که این امر خود احتمال از دست رفتن اطلاعات را به دلیل اینکه تمامی اطلاعات بر روی یک سخت افزار است را زیاد میکند.

راه کار و یا راه حل؟

با استفاده از یک راه کار اصولی پشتیبان گیری، خیلی ساده میتوان به تمامی این احتمالات گفته شده پایان داد. در ارائه راهکار دو اصل خیلی مورد توجه است:

1- هزینه

2- ضریب امنیت

با توجه به بستر شبکه برای هر مجموعه راهکارهای متفاوتی برای ارائه وجود دارد و همین طور متناسب با نوع شبکه نیازمند سخت افزار و یا نرم افزار خاصی میباشد. از این رو کارشناسی دقیق میتواند با در نظر گرفتن هزینه بهترین پیشنهاد را ارائه دهد.



– راهکارهای امنیتی

امنیت شبکه چیست؟

امنیت شبکه در قالب هر فعالیتی که برای حفاظت از یکپارچگی شبکه و داده ها قابل استفاده است، طراحی شده است. این موضوع شامل تکنولوژی های سخت افزاری و نرم افزاری میباشد. امنیت شبکه موثر، دسترسی به شبکه را مدیریت میکند، و یا به معنای دیگر امنیت شبکه تهدیدات مختلف را هدف قرار میدهد و از وارد شدن و یا گسترش آنها در شبکه جلوگیری میکند. مدیریت امنیت شبکه امروزه بیش از هر زمان در دهه های اخیر چالش برانگیز است. اما شرکت با ارائه راه حل های امنیتی برتر شبکه میتواند در ساده تر کردن این کار به شما کمک نماید.

راه کار و یا راه حل؟

راه حل های امنیتی مناسب میتواند به بهبود مدیریت و امنیت و عملکرد شبکه کمک کند اما با فراوانی فناوری در دسترس، انتخاب بهترین راه حل های امنیتی شبکه، کار سخت و دشواری است و همچنین نیاز به یک تیم متخصص دارد که علاوه بر در نظر گرفتن هزینه های این کار بهترین راهکار را پیاده سازی نمایند. در زیر به مواردی که در این باره مورد تامل است میپردازیم:

- **کنترل دسترسی:** هر کاربری نباید به شبکه دسترسی داشته باشد. برای محافظت باید هر کاربر و هر دستگاه را شناسایی کرد سپس میتوان سیاست های امنیتی را اجرا کرد.
- **آنتی ویروس و آنتی اسپیم:** نرم افزار های مخرب شامل ویروس ها، تروجان ها، اسپیم ها، باج افزار ها و نرم افزار های جاسوسی میباشد، که گاهی اوقات اطلاعات شبکه را آلوده میکنند.
- **امنیت برنامه ها:** هر نرم افزار که برای اجرای یک کسب و کار مورد استفاده قرار میگیرد باید محافظت شود. زیرا ممکن است این نرم افزار ها حاوی حفره های امنیتی و آسیب پذیر باشند.
- **تحلیل رفتاری:** برای تحلیل رفتار غیر معمول شبکه، باید بدانید که رفتار طبیعی چگونه به نظر میرسد، ابزار تحلیل به طور خودکار رفتارهایی که غیر طبیعی به نظر میرسد را مشخص میکند.
- **امنیت ایمیل:** ایمیل هر سازمان میتواند تهدیدی بر امنیت به حساب آید. مهاجمان از تاکتیکهای مهندسی برای فریب دادن و هدف گیری اطلاعات از ارسال ایمیل و یا هرز نامه استفاده میکنند.
- **فایروال:** فایروال ها مانع بین شبکه مورد اعتماد داخلی و شبکه های بی اعتبار خارجی میشوند.
- **سیستمهای پیشگیری از نفوذ:** ایت سیستم ها (IPS) ترافیک شبکه را به طور فعال برای جلوگیری از حملات اسکن میکنند.
- **VPN:** یک شبکه خصوصی مجازی، اتصال از یک یا چند نقطه به یک شبکه (اغلب در اینترنت) را رمز گذاری میکند.
- **امنیت وب:** یک راه حل امنیتی وب، استفاده از اینترنت را برای کاربران کنترل میکند، تهدیدات وب را مسدود و دسترسی به سایتهای مخرب را ممنوع میکند.
- **امنیت شبکه بی سیم:** شبکه های بی سیم امنیت کمتری نسبت به شبکه های سیمی دارند، بدون اقدامات امنیتی دقیق، نصب شبکه های بی سیم مانند قرار دادن پورت شبکه در همه جا است.



- نصب و راه اندازی سرور

نصب و راه اندازی سرور

هدف از ایجاد شبکه بین کامپیوتر ها، به اشتراک گذاری خدماتی است که ارائه آنها به دلایلی اعم از هزینه بالا، پایین بودن امکانات کنترلی، به دور بودن از امنیت و ... در قالب تک کاربره غیر قابل راه اندازی است. لذا مهمترین دلیل راه اندازی شبکه های کامپیوتری اشتراک گذاری منابع و کنترل یکپارچه کامپیوتر ها و دستگاه های موجود در آن شبکه برای ارائه سرویس ها و خدمات مربوطه می باشد. جهت نصب و راه اندازی شبکه قبل از هر اقدامی نیاز به بررسی، امکانات سنجی و همچنین آماده سازی نقشه و تحلیل شبکه است و پس از بررسی ها و تحقیقات لازم راهکار مناسب ارائه شود.

شرکت نصب و اجرای انواع سرور ها و سرویس های مورد نیاز یک شبکه که در زیر آمده را با در نظر گرفتن نیاز هر مجموعه ارائه مینماید:



- نصب و راه اندازی انواع سرورهای مبتنی بر Windows
- راه اندازی شبکه تحت دامنه (Domain)
- نصب و راه اندازی DHCP Server ، DNS Server ، WSUS Server و ...
- راه اندازی اکتیو دایرکتوری RODC ، Additional و ...
- راه اندازی Routing & Remote Access server
- راه اندازی VPN Server
- راه اندازی Print Server
- راه اندازی Backup Server
- راه اندازی Raid Controller
- راه اندازی LMS و سامانه های آموزش و ویدئو کنفرانس آنلاین
- راه اندازی Web Server و سرویس های تحت وب
- راه اندازی Mail Server ، FTP ، SMTP
- راه اندازی سرور های مانیتورینگ شبکه (SNMP)
- مدیریت و کنترل سطح دسترسی ها کاربران (Group policy Management)
- ایجاد سرورهای Redundant و Load balance
- راه اندازی فایروال های نرم افزاری و سخت افزاری مانند kerio و ...
- و ...



- راه اندازی مانیتورینگ شبکه

مانیتورینگ شبکه چیست؟

سیستم های مانیتورینگ شبکه فعالیت کلیه تجهیزات درون شبکه و سرورها را با ارسال یک سیگنال به نام Ping به پورتهای مختلف سیستم ها بررسی میکند.

در واقع یک سیستم مانیتورینگ شبکه تمامی شبکه داخلی شما را برای پیدا کردن مشکلات پایش می کند، این سیستم می تواند به شما کمک کند میزان دانلود کاربران شبکه و استفاده آنها از اینترنت را بدانید، فضاهای اشغال شده توسط ایمیل های اسپم و کاربرانی که بیهوده ایمیل ارسال می کنند را شناسایی کنید، سرورهایی که در حال بروز مشکل هستند یا مشکل ایجاد خواهند کرد را شناسایی کنید، ترافیک شبکه را مشاهده کنید و موارد غیرعادی را در قالب گزارش ببینید و در کنار همه اینها علاوه بر نرم افزارها سخت افزارهای موجود در شبکه را نیز پایش کنید. بصورت کلی شما می توانید با داشتن یک سیستم مانیتورینگ قوی در سازمان خود از تمامی اتفاقاتی که در شبکه خود چه از لحاظ نرم افزاری و چه از لحاظ سخت افزاری رخ می دهد آگاه شوید .



مزایای مانیتورینگ شبکه؟

- بررسی پهنای باند شبکه جهت جوابگویی به نیاز کاربران شبکه
- شناسایی کلاینت های مشکل ساز و فیلتر کردن آنها
- بهینه سازی کارایی شبکه (با توجه به بررسی و مانیتورینگ)
- تخمین میزان پهنای باند مورد نیاز در آینده بر اساس میزان استفاده فعلی
- استفاده بهینه از پهنای باند (جلوگیری از دانلود و آپلودهای نامربوط)

بخشهای مهم در زمان مانیتورینگ شبکه کجاست؟



- ✓ دمای CPU ، سرعت فن و ولتاژ تجهیزات شبکه
- ✓ شناسایی منبع تغذیه های نیم سوز بر اساس ولتاژ ورودی آنها
- ✓ میزان استفاده از حافظه در سرورها
- ✓ فعالیت های Proxy Server در شبکه
- ✓ بررسی نویز، نرخ انتقال داده و سیگنال در شبکه های بیسیم
- ✓ کنترل پهنای باند در حال استفاده در شبکه های بیسیم
- ✓ کنترل میزان Broadcast های شبکه
- ✓ میزان پهنای باند مصرفی توسط پروتکل های شبکه
- ✓ میزان پهنای باند مصرفی توسط هر پورت در یک سوئیچ



- نصب و راه اندازی VOIP (تلفن تحت شبکه)

VoIP چیست؟

صدا بر روی پروتکل اینترنت که مخفف کلمات Voice Over Internet Protocol است. VoIP به یک گروه از تکنولوژی هایی می گویند که برای انتقال صدا و چندرسانه از شبکه های مبتنی بر پروتکل، مانند اینترنت استفاده می کند. VoIP با عنوان های تلفن IP، تلفن اینترنتی، تلفن پهن باند، صدای پهن باند و صدا روی پهن باند نیز شناخته می شود. برخی از کاهش هزینه ها تا حدودی به دلیل استفاده از یک شبکه منفرد برای حمل صدا و اطلاعات است، مخصوصاً در جایی که استفاده کنندگان به شبکه ای دسترسی دارند که از ظرفیت آن کمتر استفاده شده و می تواند VOIP را بدون هیچ هزینه اضافی حمل کند. تماس های VoIP به برخی اوقات مجانی هستند، در حالی که تماس VOIP به شبکه های تلفن عمومی (PSTN) ممکن است هزینه ای در بر داشته باشد که باید توسط استفاده کنندگان VoIP پرداخت شود.

مزایای ویپ



از نقطه نظرهای متفاوتی می توان به بررسی مزایای این تکنولوژی پرداخت که بالطبع کاهش هزینه های جاری، از جمله جذاب ترین ویژگی های این تکنولوژی است که برخی از دلایل این امر عبارتند از:

1- بی نیازی از سیم کشی مجزا

این تکنولوژی از بستر شبکه برای ارتباطات تلفنی استفاده می کند که موجب کاهش کابل کشی مجزا می گردد. هم چنین در صورت جابجایی محل کاربر، دیگر دردسر سیم کشی به مکان جدید وجود نخواهد داشت.

۲- کنفرانس های صوتی

سازمان هایی که برای انجام امور خود از برقراری کنفرانس ها در بستر VoIP استفاده می نمایند از هزینه های برقراری ارتباطات تلفنی با توجه به مسافت های کاربران (حتی در ابعاد بین المللی) جلوگیری می کنند.

۳- ادغام دستگاه تلفن با کامپیوتر شخصی

همان طور که می دانید امروزه استفاده از نرم افزارهای تلفنی (SoftPhone) در سازمان ها و حتی سیستم های خانگی به صورت روزافزون در حال گسترش می باشد. استفاده از این نرم افزارها جایگزینی برای IP-Phone به شمار می رود که تنها نیاز به Headset دارد. لذا بدین صورت می توانید از هزینه های موجود بکاهید.



۴- تماس با کاربران خارج از سازمان به صورت رایگان از بستر اینترنت

کاربران این سیستم از طریق اینترنت قادر به تماس با سازمان مورد نظر خود می‌باشند. این ویژگی برای کارکنانی که خارج از محیط دفتر هستند علاوه بر کسر هزینه‌ها موجب تسهیل تماس‌های تلفنی نیز می‌شود.

۵- گسترش آسان

گسترش و افزودن کاربر در این سیستم‌ها به سادگی انجام پذیر است و برخلاف سیستم‌های پیشین نیاز به سیم کشی مجدد برای هر کاربر وجود ندارد.

۶- مدیریت متمرکز و آسان

مراکز تلفن مبتنی بر VoIP محیطی را تحت شبکه در اختیار کاربر قرار می‌دهند که از طریق آن می‌تواند تنظیمات را تغییر داده، کاربر اضافه کرده و یا گزارش گیری نماید.

۷- تلفن گویا (IVR)

سیستم تلفنی ویپ به صورت پیش فرض و به صورت نرم افزاری و بدون نیاز به هیچ سخت افزاری دارای امکان تلفن گویا می‌باشد که این امکان را برای هر تعداد و هر چند لایه تلفن گویا بدون هیچ محدودیتی فراهم می‌کند.

۸- ضبط مکالمات

امکان ضبط مکالمات در سیستم ویپ بدون نیاز به هیچ سخت افزاری و بدون محدودیت بر روی تماسهای داخلی به داخلی و همچنین تماسهای خارجی به داخلی و بالعکس فراهم می‌باشد و نیاز به هزینه مجزا جهت تامین سخت افزارهای گران قیمت ضبط مکالمات را ندارد.



- آنتی ویروس سازمانی

آنتی ویروس سازمانی یا تحت شبکه



آنتی ویروس سازمانی یا تحت شبکه این امکان را برای مجموعه ها فراهم میکند که به صورت یکپارچه و توسط یک سرور کلیه آنتی ویروس های داخل شبکه را مدیریت و آپدیت کنید. در واقع فرق آنتی ویروس های معمولی یا خانگی با سازمانی در این است که در آنتی ویروس های خانگی بر روی هر سیستم یک کنسول آنتی ویروس نصب شده و به صورت مستقل تنظیمات لازم بر روی آن انجام میشود و در نهایت خود به صورت مستقل آپدیت های جدید را توسط شرکت تولید کننده از اینترنت میگیرد،

حال تصور کنید در یک مجموعه 10 یا 20 کامپیوتر وجود دارد، در این حالت به تعداد کامپیوتر ها ، کنسول مدیریتی بر روی سیستمها وجود دارد و هر کامپیوتر آپدیت های جدید را از اینترنت دریافت میکند و حجم زیادی از اینترنت مصرف میشود در صورتی که در آنتی ویروس های

سازمانی کنسول اصلی بر روی یک سرور نصب شده و بر روی کامپیوتر ها فقط Agent آنتی ویروس نصب میشود. مزیت این کار در این است که یک کنسول مدیریتی وجود دارد و مدیر شبکه به راحتی توسط یک کنسول کلیه کامپیوترهای درون شبکه را چک و مدیریت میکند و همچنین سرور یکبار آپدیت های جدید را از اینترنت دریافت کرده و خودش Client ها را آپدیت میکند که این مورد در شبکه های بزرگتر از 10 کامپیوتر بسیار مفید و حتی الزامیست.

دیگر مزیت ها و امکانات

علاوه بر صحبت های بالا آنتی ویروس های سازمانی و یا تحت شبکه از امکانات و مزایای زیر بهره مند هستند:

- آگاهی سریع از ویروسی شدن یک کلاینت در شبکه
- دریافت گزارش های متعدد مدیریتی
- نظارت مستقیم بر نحوه عملکرد و سلامت کلیه کلاینت های موجود در شبکه
- اجرای عملیات نصب و یا حذف آنتی ویروس از راه دور
- کاهش قابل توجه مصرف اینترنت سازمان یا شرکت
- بستن پورتهای USB کلاینت ها در صورت تمایل
- عدم توانایی کاربر در uninstall نمودن آنتی ویروس بوسیله پسورد گذار
- اسکن نمودن کلیه درایوهای کامپیوتر کاربر از راه دور
- آگاهی از کامپیوترهای فاقد آنتی ویروس در شبکه
- قابلیت اجرا در شبکه های تحت Domain یا Work group
- به روز نمودن سیاستها و رفتار آنتی ویروس از راه دور
- قابلیت مسدود سازی وب سایتهای مشکوک و آلوده به ویروس



- پشتیبانی و نگهداری شبکه

یکی از معضلات و مشکلات سازمان ها و شرکت ها در حوزه فناوری اطلاعات و ارتباطات ، نگهداری و مدیریت آن می باشد .پشتیبانی شبکه هم برای افرادی که خدمات شبکه خود را از **شرکت** گرفته باشند و هم برای افرادی که خدمات راه اندازی شبکه خود از همکاران ما گرفته باشند، قابل ارائه می باشد.

ما با بررسی وضعیت و موقعیت IT در سازمان ها و شرکت ها ، خدمات متنوعی در زمینه **پشتیبانی و نگهداری شبکه** ، زیرساخت شبکه و همینطور پشتیبانی از تجهیزات رایانه ای و اداری را با استفاده از تجربیات با ارزش خود در این زمینه و با بهترین کیفیت به شما ارائه می دهیم.



مراحل کار:

الف) نیاز سنجی : پس از دریافت تماس از سوی مجموعه ها، در بررسی های اولیه، با توجه به نیاز و وسعت هر مجموعه طرح پشتیبانی متناسب با آن مجموعه را ارائه خواهیم کرد. پس از عقد قرارداد، بررسی های تکمیلی شروع شده و فعالیت صورت می گیرد.

ب) بررسی شبکه و مستند سازی :

- بررسی شبکه موجود از لحاظ نوع ارتباط (کابلی یا بی سیم)، تعداد سرورها، تعداد کلاینتها، نوع سرورها، نوع تجهیزات در حال استفاده
- بررسی سرورها از لحاظ سخت افزاری، تست قطعات در صورت نیاز
- بررسی وضعیت و نحوه کارکرد شبکه
- بررسی سرویس های نصب شده روی سرورها
- بررسی نحوه ارتباط سرورها و کلاینتها با اینترنت
- بررسی نرم افزارهای کاربردی و سامانه های مورد استفاده در سازمان
- تهیه شناسنامه از تجهیزات سخت افزاری

ج- استاندارد سازی : پس از آماده سازی اطلاعات و نیز آماده بودن بستر جهت استاندارد سازی شبکه کارشناسان شرکت شروع به رفع ایرادات و نیز ارائه پیشنهاد به منظور بهبود اوضاع و نیز اصولی سازی شبکه با توجه به استانداردهای شبکه خواهند کرد.

ح- ارائه راهکار : با توجه به نیاز سازمان و نیز امکانات در دسترس و یا قابل فراهم سازی ، راهکارهایی به منظور رشد و بهبود فعالیت های سازمانی ارائه خواهد شد تا در صورت موافقت و امکان راه اندازی، سرویس موردنظر روی شبکه فعال و قابل استفاده گردد.

خ- چکاپ دائم : کارشناسان پشتیبانی با توجه به برنامه ریزی و نیاز سازمان به صورت مستمر اقدام به بکاپ گیری و همچنین چکاپ شبکه به منظور جلوگیری از بروز هرگونه مشکل را انجام میدهند.





RayanFidar
TM

شرکت توسعه فناوری رایان فیدار



RayanFidar
TM



www.raynfidar.ir



۰۵۱-۹۱۰۹۱۹۵۶



میدان سپاد، مجتمع سپاد، فاز 5، طبقه همکف، پلاک 2/6