



دروس شبکه

Network Courses

دانشگاه علمی و کاربردی خیام الکترونیک

ویزیت اول: خرداد ماه ۱۴۰۳

گردآوری: سیدمرتضی علم پرور

توسعه ارتباطات

چهارراه بعثت دارایی، ساختمان ۵۶

Phone: +9851 4334 9 555 | **Mobile:** +98 915 009 3070 | **Web:** <https://tovse.com>

۸	فصل اول : نظارت بر شبکه
۹	بخش اول : مانیتورینگ شبکه چیست ؟
۱۱	بخش دوم : چرا سازمان ها باید از راهکارهای مانیتورینگ شبکه استفاده کنند؟
۱۲	بخش سوم : انواع راهکارهای مانیتورینگ شبکه چه هستند؟
۱۲	انتخاب نوع ابزار مانیتورینگ شبکه به چه عواملی بستگی دارد؟
۱۳	بهترین ابزارهای مانیتورینگ شبکه کدامند؟
۱۴	بخش چهارم : آموزش مانیتورینگ شبکه
۱۵	بخش پنجم : دانش عمومی شبکه های کامپیوتری
۱۵	مدل OSI چیست ؟
۱۶	دستگاه های رایج شبکه کدامند؟
۱۶	روتر Router چیست ؟
۱۷	سوئیچ Switch چیست ؟
۱۷	فایروال Firewall چیست ؟
۱۷	سرور Server چیست ؟
۱۷	داده ها چگونه از طریق شبکه منتقل می شوند؟
۱۸	کاربرد فایروال در انتقال داده چیست؟
۱۹	کاربرد سوئیچ در شبکه چیست ؟
۱۹	مبانی پایگاه داده
۲۰	طراحی پایگاه داده رابطه ای
۲۰	جست و جوی SQL

۲۰	چرا مانیتورینگ شبکه ضرورت دارد؟
۲۱	توافق نامه سطح خدمات یا SLA چیست ؟
۲۲	اجزای عمومی مانیتورینگ در ویندوز چه هستند ؟
۲۳	روش ها و پروتکل های کلی مانیتورینگ شبکه
۲۳	پینگ
۲۴	دستورالعمل ساده مدیریت شبکه(SNMP – Simple network Management Protocol)
۲۵	Syslog
۲۵	استفاده از اسکرپت
۲۵	فلسفه طراحی مانیتورینگ شبکه چیست؟
۲۶	FCAPS در مانیتورینگ شبکه چیست ؟
۲۷	مدیریت خطا
۲۷	مدیریت پیکربندی
۲۷	مدیریت حسابداری
۲۸	مدیریت کارایی
۲۸	مدیریت امنیت
۲۸	وظایف پنج گانه مانیتورینگ شبکه چیست؟
۲۹	اکتشاف
۳۰	نقشه کشی
۳۰	نظارت
۳۱	هشداردهی
۳۲	گزارش گیری
۳۳	یک ابزار مانیتورینگ شبکه چطور کار می کند ؟
۳۴	پروتکل SNMP چیست ؟
۳۴	پروتکل WMI چیست ؟
۳۶	مروری بر مانیتورینگ مبتنی بر عامل یا Agent

۳۷	مروری بر مانیتورینگ بدون عامل
۳۸	قواعد مشترک مانیتورینگ شبکه
۳۹	مانیتورینگ دسترس پذیری
۴۰	مانیتورینگ واسط تعاملی
۴۰	مانیتورینگ دیسک
۴۱	مانیتورینگ سخت افزار

بخش ششم : آموزش مانیتورینگ شبکه با SolarWinds ۴۳

۴۳	SolarWinds چیست ؟
۴۴	پلتفرم SolarWinds Orion چیست ؟
۴۴	SolarWinds بر چه دستگاه هایی نظارت می کند؟
۴۴	امکانات SolarWinds NPM چیست ؟
۴۵	شناسایی خودکار شبکه با SolarWinds NPM
۴۶	مانیتورینگ دستگاه های شبکه با SolarWinds NPM
۴۷	تنظیم شرایط هشدار با SolarWinds NPM
۴۹	قابلیت تحلیل عملکرد در SolarWinds NPM
۵۰	گزارش گیری و به اشتراک گذاری داده در NPM
۵۱	پشتیبانی از چند برند در SolarWinds NPM
۵۲	نمونه برداری وایرلس در SolarWinds NPM
۵۳	مانیتورینگ محیط مجازی در SolarWinds NPM
۵۳	تحلیل NetPath با SolarWinds NPM
۵۴	نیازمندی های سیستمی SolarWinds NPM چه هستند؟

بخش هفتم : آموزش مانیتورینگ شبکه با Zabbix ۵۶

۵۶	Zabbix چیست ؟
۵۷	Zabbix چه ویژگی هایی دارد؟

۵۹	معماری Zabbix
۶۰	مانیتورینگ خارجی و داخلی در Zabbix
۶۱	مانیتورینگ خارجی با Zabbix
۶۲	مانیتورینگ داخلی با Zabbix
۶۲	جمع بندی فصل اول
۶۳	فصل دوم : تلفن تحت شبکه VOIP – سخت افزار و نرم افزار
۶۴	مقدمه
۶۵	فصل اول : تعریف VOIP
۶۷	فصل دوم : شناخت و عملکرد VOip، مزایا و معایب
۶۷	مزایای VoIP
۶۷	مقرون به صرفه بودن
۶۸	نصب و استفاده آسان
۶۸	دورکاری و قابلیت حمل
۶۸	کنفرانس و ارتباط صوتی و تصویری
۶۸	انعطاف پذیری
۶۹	مقیاس پذیری
۶۹	یکپارچه سازی
۶۹	کیفیت تماس بالا
۷۰	امنیت بالا
۷۰	معایب VoIP
۷۰	وابستگی به اینترنت
۷۰	وابستگی به برق

۷۱	امنیت
۷۱	سازگاری
۷۱	مزایای VoIP نسبت به سانترال
۷۲	امکانات VoIP
۷۳	تفاوت خطوط تلفن ثابت و فناوری VoIP چیست؟
۷۳	بررسی انواع VoIP
۷۳	۱. Integrated Access
۷۴	۲. SIP Trunks
۷۴	۳. Hosted IP PBX
۷۴	۴. Managed IP PBX
۷۵	بررسی نحوه عملکرد فناوری VoIP
۷۵	سیستم ویپ معمول شامل اجزای اضافی زیر است:
۷۶	نحوه راه اندازی سیستم ویپ
۷۶	۱. شناخت نیازهای خانه یا محل کار خود
۷۶	۲. امتحان کردن اتصال اینترنت
۷۶	۳. شناخت انواع ویپ و تفاوت آن ها
۷۷	۴. تعیین بودجه
۷۷	۵. انتخاب شرکت ارائه دهنده VoIP
۷۷	۶. دریافت یا حفظ شماره تلفن برای کسب و کار
۷۸	۷. نصب و راه اندازی سیستم ویپ
۷۸	دلیل خرید ویپ چیست؟
۷۹	فصل سوم : سخت افزار VoIP
۷۹	PSTN
۸۰	PBX
۸۱	انواع سیستم تلفن PBX

۸۲	مزایای سیستم-های تلفن PBX میزبانی شده (Hosted PBX) چیست؟
۸۲	مزایای تلفن PBX درون سازمانی چیست؟
۸۲	ATA
۸۳	Channel Bank
۸۳	تلفن‌های تحت شبکه یا IP Phone
۸۴	تکنولوژی POE
۸۴	UPS - Uninterruptible Power Supply
۸۵	VoIP headset
۸۵	IP-PBX Server
۸۶	فصل چهارم : نرم افزارهای VoIP
۸۷	مراجع

فصل اول: نظارت بر شبکه

شبکه‌های سازمانی برای پاسخگویی به نیازهای رو به رشد کسب و کار دیجیتال، روز به روز در حال پیچیده‌تر شدن هستند. یک سازمان باید همواره از سرعت و بازدهی شبکه خود اطمینان حاصل کند. مانیتورینگ شبکه ابزاری حیاتی برای سازمان‌ها جهت سنجش عملکرد و کارایی شبکه است. در ادامه مانیتورینگ شبکه، مفاهیم پایه و مهم در این حوزه به طور کامل و بیانی ساده ارائه شده است.

برخی از مهم‌ترین مباحث مطرح شده در این مقاله شامل معرفی و تعریف مانیتورینگ شبکه، انواع ابزارها و راهکارهای مانیتورینگ شبکه، پیش‌نیازها، ضرورت استفاده، اجزای عمومی و پروتکل‌ها، نحوه عملکرد و وظایف مانیتورینگ شبکه و بسیاری از موارد دیگر است. همچنین دو ابزار کاربردی و رایج در مانیتورینگ شبکه یعنی SolarWinds و Zabbix نیز معرفی شده‌اند. پیش از شروع آموزش مانیتورینگ شبکه، بهتر است به این سوال پاسخ داده شود که مانیتورینگ شبکه چیست؟

بخش اول: مانیتورینگ شبکه چیست؟

مانیتورینگ شبکه ، به کارگیری سیستمی است که به طور مداوم بر یک شبکه کامپیوتری نظارت می‌کند تا اجزایی را شناسایی کند که دچار مشکل هستند یا باعث بروز کندی شده‌اند. در صورت بروز قطعی یا مشکل در شبکه، سیستم مانیتورینگ ، مدیران شبکه را مطلع می‌سازد. در این بخش از آموزش مانیتورینگ شبکه ، چپستی آن را از دیدگاهی مقدماتی شرح داده و به این مسئله پرداخته شده است که چگونه مانیتورینگ شبکه می‌تواند عملیات شبکه یک سازمان را به حداکثر کارایی برساند. به بیانی کاربردی‌تر، مانیتورینگ شبکه به یک جز یا قطعه سخت‌افزاری یا نرم‌افزاری گفته می‌شود که به طور دائم بر شبکه و داده‌های عبوری از آن نظارت دارد.

بسته به نحوه کارکرد راهکار مانیتورینگ شبکه ، ممکن است داده‌ها مستقیماً در حین عبور از شبکه نمونه‌برداری شوند یا از داده‌های ذخیره شده یک گره در شبکه استفاده شود. در مانیتورینگ شبکه ، داده‌ها تفسیر و در یک داشبورد نمایش داده می‌شوند تا بتوان عملکرد شبکه را به صورت تصویری تحت نظر داشت. در صورتی که برنامه مانیتورینگ شبکه هر گونه مشکل یا نشانه‌ای از خرابی را در شبکه شناسایی کند، هشدار برای تیم IT سازمان ارسال می‌شود تا آن‌ها بتوانند به سرعت وارد عمل شده و نقایص را برطرف سازند.



یک راهکار مانیتورینگ شبکه به سازمان کمک می‌کند تا شبکه خود را تحت کنترل نگاه داشته و از کارکرد عملیات شبکه به نحو احسن اطمینان حاصل کند. سیستم‌های مانیتورینگ شبکه معمولاً مجهز به ردیابی عملکرد شبکه به روش‌های مختلف هستند. با پیاده‌سازی مانیتورینگ شبکه می‌توان اطلاعات مورد نیاز یک کسب و کار را از برخی سنجش‌های خاص راجع به شبکه جمع‌آوری کرد. برای مثال، در صورتی که نیاز به سنجش میزان پهنای باند مورد استفاده در یک شرکت تجاری وجود داشته باشد، می‌توان یک سیستم مانیتورینگ را تنها برای نظارت بر نرخ تبادل پهنای باند راه‌اندازی کرد. با این کار، می‌توان میزان مصرف پهنای باند را در یک بازه زمانی مشخص سنجید.

بنابراین، در صورتی که سیستم مانیتورینگ شناسایی کند که مصرف پهنای باند در حال رسیدن به سطوح بحرانی است، این سیستم به سازمان اطلاع می‌دهد که کدام دستگاه‌ها یا وب‌سایت‌ها در حال ایجاد اختلال در شبکه هستند.

بخش دوم: چرا سازمان‌ها باید از راهکارهای مانیتورینگ شبکه استفاده کنند؟

مزیت اصلی به کارگیری راهکارهای مانیتورینگ شبکه این است که تیم‌های IT می‌توانند به سرعت ریشه مشکلات در شبکه سازمان را کشف و آن‌ها را برطرف کنند. اکثر راهکارهای مانیتورینگ شبکه نظارت لحظه‌ای روی شبکه اعمال می‌کنند تا مشکلات به سرعت شناسایی شوند. لحظه وقوع یک مشکل تا لحظه‌ای که یک سازمان از بروز آن مطلع می‌شود، یک بازه زمانی حیاتی به حساب می‌آید. می‌توان با استفاده از یک راهکار مانیتورینگ شبکه این بازه زمانی را به میزان زیادی کاهش داد که منفعت به سزایی برای سازمان به همراه دارد. همچنین، می‌توان بروز وقفه را در شبکه شناسایی کرد؛ وقفه‌هایی که در صورت عدم استفاده از مانیتورینگ برای تیم‌های شبکه غیرقابل ردیابی هستند.

حتی در صورتی که ایرادهایی جزئی در شبکه وجود داشته باشد، این ایرادها می‌توانند به مشکلات بزرگ‌تری دامن بزنند. بهبود امنیت شبکه یکی دیگر از مزیت‌های راهکارهای مانیتورینگ محسوب می‌شود. تهدیدهایی مانند بدافزارها یکی از رایج‌ترین علل بروز مشکلات عملکردی در شبکه‌ها به شمار می‌روند. بدافزارها اغلب می‌توانند با مخفی شدن از فایروال‌ها و سیستم‌های امنیتی نقاط انتهایی شبکه عبور کنند. بسیاری از ابزارهای مانیتورینگ شبکه امکان جستجو مصرف منابع مشکوک را فراهم می‌کنند و آن را گزارش می‌دهند.

بخش سوم: انواع راهکارهای مانیتورینگ شبکه چه هستند؟

از جمله رایج‌ترین نرم‌افزارهای مدیریت شبکه می‌توان به SolarWinds NMP و Zabbix اشاره کرد. البته، دامنه گسترده‌ای از نرم‌افزارها و ابزارهای مانیتورینگ شبکه وجود دارد. چالش اصلی، انتخاب راهکار مناسبی است که با شرایط محیطی و بودجه یک سازمان مطابقت داشته باشد.

با وجود ملاحظات بسیار در مدیریت شبکه، به هیچ وجه جای تعجب نیست که دامنه وسیعی از ابزارها به عنوان «ابزارهای مدیریت شبکه» وجود داشته باشند. اما، با توجه به این دامنه گسترده و انواع ابزارهای مانیتورینگ و مدیریت شبکه، چطور می‌توان ابزار مناسبی را انتخاب کرد و انتخاب یک راهکار مانیتورینگ شبکه به چه عواملی بستگی دارد؟



انتخاب نوع ابزار مانیتورینگ شبکه به چه عواملی بستگی دارد؟

عوامل بسیاری در انتخاب نوع راهکار مانیتورینگ شبکه دخالت دارند که از جمله می‌توان به میزان بودجه و اندازه شبکه اشاره کرد. به عنوان مثال، یک برنامه تحلیلگر شبکه محلی (LAN Analyzer) یا یک نرم‌افزار ردیاب بسته (Packet Sniffer) که شبکه را برای نمایش داده‌های در حال انتقال شنود می‌کند، نوعی ابزار شبکه به حساب می‌آیند.

اما چنین ابزارهایی تمام فاکتورهای مورد نیاز مدیریت شبکه را برای رسیدن به اهداف مورد نظر فراهم نمی‌کنند. انتخاب نوع ابزارها و راهکارهای مدیریت شبکه به عوامل مختلفی بستگی دارد:

➤ **وسعت عملیات و شبکه**

➤ **پیکربندی عناصر تشکیل دهنده شبکه**

➤ **میزان بودجه**

➤ **اندازه تیم مدیریت شبکه**

با در نظر داشتن این عوامل، تعدادی از ابزارهای مانیتورینگ که می‌توانند فارق از اندازه و پیکربندی سازمان به نظارت بر عملکرد شبکه بپردازند.

بهترین ابزارهای مانیتورینگ شبکه کدامند؟

فهرست بهترین ابزارهای مانیتورینگ شبکه به شرح زیر است:

- *SolarWinds*
- *Datadog*
- *ManageEngine OpManager*
- *Progress WhatsUp Gold*
- *Site24x7 Network Monitoring*
- *Paessler PRTG Network Monitor*
- *Nagios Core*
- *Zabbix*
- *Icinga*
- *Spiceworks Connectivity Dashboard*

ابزارهای مانیتورینگ SolarWinds و Zabbix از راهکارهای محبوب در ایران به حساب می‌آیند. بنابراین، در پایان و پس از ارائه مفاهیم پایه و اساسی آموزش مانیتورینگ شبکه، این دو ابزار معرفی و ویژگی‌های آن‌ها شرح داده شده‌اند.

یک شبکه کامپیوتری از تعدادی کامپیوتر تشکیل شده است که از پروتکل‌های ارتباطی برای اتصال دیجیتال با هدف به اشتراک‌گذاری منابع موجود در شبکه استفاده می‌کنند. ارتقای دانش در حوزه شبکه‌های کامپیوتری برای جلوگیری از نفوذ و مقابله با حملات مختلف در این بستر بسیار اهمیت دارد. کسب دانش و مهارت در حوزه شبکه‌های کامپیوتری پیش‌نیاز آموزش مانیتورینگ شبکه محسوب می‌شود. پیش از پرداختن به آموزش ابزارهای مانیتورینگ شبکه نظیر SolarWinds NPM و Zabbix، بهتر است ابتدا شرحی از مفاهیم پایه در آموزش مانیتورینگ شبکه ارائه شود.

بخش چهارم: آموزش مانیتورینگ شبکه

در این بخش از آموزش مانیتورینگ شبکه، مفاهیم مقدماتی و پایه مانیتورینگ شبکه از جمله مدل هفت لایه OSI، انواع دستگاه‌های رایج شبکه، پنج قابلیت سیستم‌های مانیتورینگ شبکه و سایر موارد شرح داده شده‌اند. پیش از شروع آموزش مانیتورینگ شبکه، لازم است درک کلی از شبکه‌های کامپیوتری وجود داشته باشد.

همچنین باید آشنایی کافی با ملزومات سیستم‌های ویندوزی وجود داشته باشد. زیرا، عمدتاً در اکثر سازمان‌ها در سراسر جهان از سیستم‌عامل ویندوز استفاده می‌شود. دانش کافی درباره ملزومات شبکه‌های کامپیوتری و اجزایی که یک شبکه کامپیوتری را تشکیل می‌دهند به مدیریت و مانیتورینگ بهتر شبکه کمک می‌کند.

بخش پنجم: دانش عمومی شبکه های کامپیوتری

مهارت ها و دانش عمومی شبکه های کامپیوتری به موضوعات زیر تقسیم می شوند:

➤ تعریف شبکه های کامپیوتری

➤ انواع شبکه های کامپیوتری

➤ مدل OSI

➤ اجزای اساسی شبکه های کامپیوتری

اجزای بسیاری در تشکیل یک شبکه کامپیوتری نقش دارند که امکان ارتباط میان گره های مختلف شبکه را فراهم می سازند. برخی از این اجزا شامل آدرس دهی در شبکه، پروتکل های ارتباطی و انتقال داده و روش هایی که برای انتقال بسته بین گره های یک شبکه یا شبکه های دیگر استفاده می شود. برخی از اجزای پایه ای که در هر شبکه کامپیوتری وجود دارند، در ادامه فهرست شده اند:

➤ آدرس IP و Subnetting

➤ سیستم نام دامنه (DNS)

➤ پروتکل پیکربندی پویای میزبان (DHCP)

مدل OSI چیست ؟

یکی از مفاهیم پایه در آموزش مانیتورینگ شبکه ، درک مدل اتصال متقابل سامانه های باز (OSI) است. مدل OSI کارکردهای کلیدی یک شبکه را با استفاده از پروتکل های شبکه استانداردسازی می کند. با استفاده از استاندارد OSI ، دستگاه هایی با برندهای مختلف می توانند از طریق یک شبکه با یکدیگر ارتباط برقرار کنند.

در مدل OSI ارتباطات شبکه در هفت لایه منطقی دسته بندی می شوند. دو دستگاه، در هر لایه با استفاده از پروتکل های استانداردسازی شده OSI ارتباط برقرار می کنند. مدل هفت لایه OSI در تصویر زیر نشان داده شده است.



لایه‌های (پیوند داده | Data-Link لایه ۲)، لایه شبکه (لایه ۳) و لایه کاربرد (لایه اپلیکیشن | لایه ۷) پراستفاده‌ترین لایه‌ها در مانیتورینگ شبکه به حساب می‌آیند. سیستم‌های مانیتورینگ شبکه از لایه‌های دو، سه و هفت برای شناسایی دستگاه‌های شبکه و چگونگی اتصال آن‌ها برای ایجاد نقشه‌های ساختاری (توپولوژی) و نظارت بر شبکه استفاده می‌کنند. کسب شناخت کافی از انواع دستگاه‌های شبکه یکی دیگر از موضوعاتی است که در آموزش مانیتورینگ شبکه اهمیت دارد.

دستگاه‌های رایج شبکه کدامند؟

در این بخش از آموزش مقدماتی مانیتورینگ شبکه، برخی از دستگاه‌های رایج شبکه معرفی و شرح داده شده‌اند. ابتدا به طور مختصر شرحی از چپستی روتر ارائه شده است.

روتر Router چیست ؟

روترها شبکه‌ها را به هم متصل می‌کنند. برای مثال اتصال یک شبکه خصوصی به اینترنت از طریق یک روتر انجام می‌شود. روتر به مانند یک راهبر عمل می‌کند؛ یعنی بهترین مسیر برای انتقال اطلاعات را برمی‌گزیند. روترها کاربران را به اینترنت متصل می‌کنند. روترها دستگاه‌های لایه سه به شمار می‌روند.

سوئیچ Switch چیست ؟

سوئیچ‌ها در یک شبکه خصوصی، کامپیوترها، پرینترها، سرورها و سایر دستگاه‌ها را به هم متصل می‌کنند. یک سوئیچ به عنوان یک کنترلر عمل می‌کند و امکان ارتباط میان دستگاه‌های یک شبکه محلی را با یکدیگر فراهم می‌سازد. سوئیچ‌ها دستگاه‌های لایه دویی محسوب می‌شوند. البته لازم به توضیح است که سوئیچ‌هایی با قابلیت Routing و مسیریابی، در لایه سوم هم فعال می‌باشند.

فایروال Firewall چیست ؟

فایروال‌ها از شبکه‌ها محافظت می‌کنند. یک فایروال یا دیوار آتشین، عبور و مرور ورودی-خروجی را بر اساس قوانین مشخصی مدیریت می‌کند. این کار یک مانع ایمن را میان یک شبکه خصوصی مورد اعتماد و یک شبکه غیر قابل اعتماد مثل اینترنت، ایجاد می‌کند.

سرور Server چیست ؟

شبکه‌ها، اپلیکیشن‌ها و اطلاعات را به کاربران تحویل می‌دهند. اپلیکیشن‌ها و اطلاعات در سرورها نگهداری و ذخیره می‌شوند. سرورها (سرویس دهنده‌ها) درخواست‌ها را از کاربران دریافت می‌کنند و مطابق آن پاسخ می‌دهند. برای مثال، وقتی کاربر یک وبسایت را باز می‌کند، یک وبسرور صفحات وب را به دستگاه کاربر تحویل می‌دهد. از جمله دیگر انواع سرورها می‌توان به سرورهای ایمیل و پایگاه داده اشاره کرد.

داده‌ها چگونه از طریق شبکه منتقل می‌شوند؟

اکثر شبکه‌های خصوصی به اینترنت متصل هستند. برای مثال، اینترنت، کاربران راه دور را به دفاتر مرکزی متصل می‌کند و مشتریان را به وبسایت‌ها ارتباط می‌دهد. شبکه‌های خصوصی با استفاده از روترها به اینترنت متصل می‌شوند.

اطلاعات با استفاده از بسته‌های داده از طریق اینترنت ارسال می‌شوند. هر بسته داده شامل یک آدرس آی‌پی مقصد است که روترها برای ارسال اطلاعات از یک محل به محل دیگر از آن استفاده

می‌کنند. وقتی یک روتر بسته داده‌ای را از اینترنت دریافت می‌کند، آن را به شبکه خصوصی انتقال می‌دهد (فوروارد می‌کند).

کاربرد فایروال در انتقال داده چیست؟

در اکثر شبکه‌ها، بسته‌های داده باید ابتدا از سد یک فایروال عبور کنند. هدف فایروال این است که بسته‌های آلوده را مسدود کند و شبکه خصوصی را ایمن نگاه دارد. یک فایروال این کار را به وسیله تصفیه (فیلتر) کردن ترافیک تبادل شده میان اینترنت و شبکه خصوصی انجام می‌دهد. وقتی که یک بسته داده ورودی بر اساس قوانین فایروال علامت‌گذاری شده باشد، از ورود به شبکه خصوصی منع خواهد شد.



همچنین، فایروال‌ها دسترسی کاربران را میان اینترنت و شبکه خصوصی کنترل می‌کنند. برای مثال، یک فایروال می‌تواند به گونه‌ای تنظیم شده باشد که استفاده کاربران شبکه خصوصی را از برخی پروتکل‌ها، مانند پروتکل‌های نظیر به نظیر منع کند. این یکی از روش‌هایی است که فایروال‌ها از شبکه‌های خصوصی در برابر دسترسی غیرمجاز، بدافزارها و سایر تهدیدات امنیتی محافظت می‌کنند.

کاربرد سوئیچ در شبکه چیست ؟

بسته‌های داده‌ای که از فایروال عبور می‌کنند، توسط یک سوئیچ در شبکه خصوصی دریافت می‌شوند. سوئیچ‌ها لپ‌تاپ‌ها، سرورها، پرینترها و سایر دستگاه‌ها را به شبکه خصوصی متصل می‌کنند. این دستگاه‌ها با استفاده از یک کارت واسطه تعاملی شبکه (NIC | Network Interface Card) که به اختصار کارت شبکه خطاب می‌شود، به یکدیگر متصل هستند.

هر کارت شبکه دارای یک آدرس کنترل دسترسی رسانه (Media Access Control | MAC) یا همان آدرس فیزیکی (Physical Address) است. سوئیچ‌ها داده‌ها را با استفاده از مک آدرس‌ها بین دستگاه‌ها انتقال می‌دهند.

مبانی پایگاه داده

پایگاه داده مجموعه‌ای از داده‌ها یا اطلاعات ساختاریافته است. هر پایگاه داده شامل یک DBMS (سیستم مدیریت پایگاه داده) می‌شود. DBMS یک برنامه نرم‌افزاری است که اعمالی مثل ایجاد، به‌روزرسانی، بازیابی یا حذف داده‌ها را بر اساس کاربر یا سایر ورودی‌های برنامه انجام می‌دهد. علاوه بر قابلیت‌های مدیریت داده، DBMS امنیت داده‌ها را فراهم می‌کند، به پشتیبان‌گیری و بازیابی داده‌ها کمک می‌کند و درستی و صحت داده‌ها را حفظ می‌کند.

به دلیل ارتباط نزدیک داده‌ها و DBMS، معمولاً این دو با هم به عنوان پایگاه داده در نظر گرفته می‌شوند. از جمله DBMS‌های محبوب در حال حاضر می‌توان به SAP ASE، Oracle، DB2، PostgreSQL، Microsoft SQL و MySQL و سایر موارد اشاره کرد. پایگاه‌های داده و DBMS‌های مرتبط با آن‌ها، معمولاً روی سرورهای اختصاصی اجرا می‌شوند که سرورهای پایگاه داده نام دارند. این سرورها ممکن است در آرایه‌های ذخیره‌سازی برای افزونگی و کارایی از فناوری RAID استفاده کنند.

طراحی پایگاه داده رابطه‌ای

در حالی که چندین مدل پایگاه داده وجود دارد، محبوب‌ترین آن‌ها مدل پایگاه داده رابطه‌ای (RDBMS) است که اکثراً از آن استفاده می‌شود. یک RDBMS به کاربران اجازه می‌دهد تا داده‌ها را در اشیایی به نام جدول ایجاد و ذخیره کنند. هر جدول، مجموعه‌ای از داده‌ای ورودی مرتبط و شامل سطرها و ستون‌ها است. ساختار جدول RDBMS، امکان دیدن یک پایگاه داده یکسان را به چندین روش فراهم می‌سازد. اعمال و دستورهای SQL شامل ایجاد، حذف، به‌روزرسانی و سایر تغییرات روی داده‌های ذخیره شده در یک پایگاه داده است.



جست و جو SQL

زبان جست‌وجوی ساختار یافته (SQL) یک زبان استاندارد برای دسترسی به اطلاعات یا داده‌ها از پایگاه داده است. جست‌وجو (Query) SQL برای انجام اعمال مختلف روی داده‌ها مورد استفاده قرار می‌گیرد. اکنون، با ارائه مفاهیم مقدماتی مورد نیاز برای آموزش مانیتورینگ شبکه، زمان آن فرا رسیده است تا دلیل اهمیت و ضرورت به کارگیری مانیتورینگ شبکه بیان شود.

چرا مانیتورینگ شبکه ضرورت دارد؟

چرا مانیتورینگ شبکه و نظارت بر شبکه‌های کامپیوتری اهمیت دارد؟ شبکه شاهراه و خط حیات زیرساخت سازمان‌ها به حساب می‌آید. اختلال در شبکه منجر به متوقف شدن جریان اطلاعاتی مورد نیاز اپلیکیشن‌ها و عملیات تجاری خواهد شد. شبکه‌ها محیط‌هایی پویا هستند و به طور مداوم از مدیران

شبکه درخواست می‌شود تا کاربران، فناوری‌ها و کاربردهای جدیدی را به شبکه اضافه کنند. این تغییرات می‌تواند توانایی آن‌ها را برای ارائه شبکه‌ای با عملکرد استوار و قابل پیش‌بینی تحت تاثیر قرار دهد.

وقتی که ایرادی در شبکه به وجود می‌آید، مدیران شبکه تحت فشار هستند تا ریشه مشکل را پیش از تحت تاثیر قرار گرفتن کاربران، اپلیکیشن‌ها و کسب و کار شناسایی کنند. در صورتی که مشکلات عملکردی به طور متناوب تکرار شوند، تشخیص و رفع مداوم مشکلات بسیار دشوارتر هم خواهد بود. بسیاری از سازمان‌های ارائه دهنده خدمات فناوری اطلاعات مشمول توافق‌نامه سطح خدمات یا (Service Level Agreement | SLA) هستند. مفهوم SLA در آموزش مانیتورینگ شبکه اهمیت دارد.

توافق نامه سطح خدمات یا SLA چیست ؟

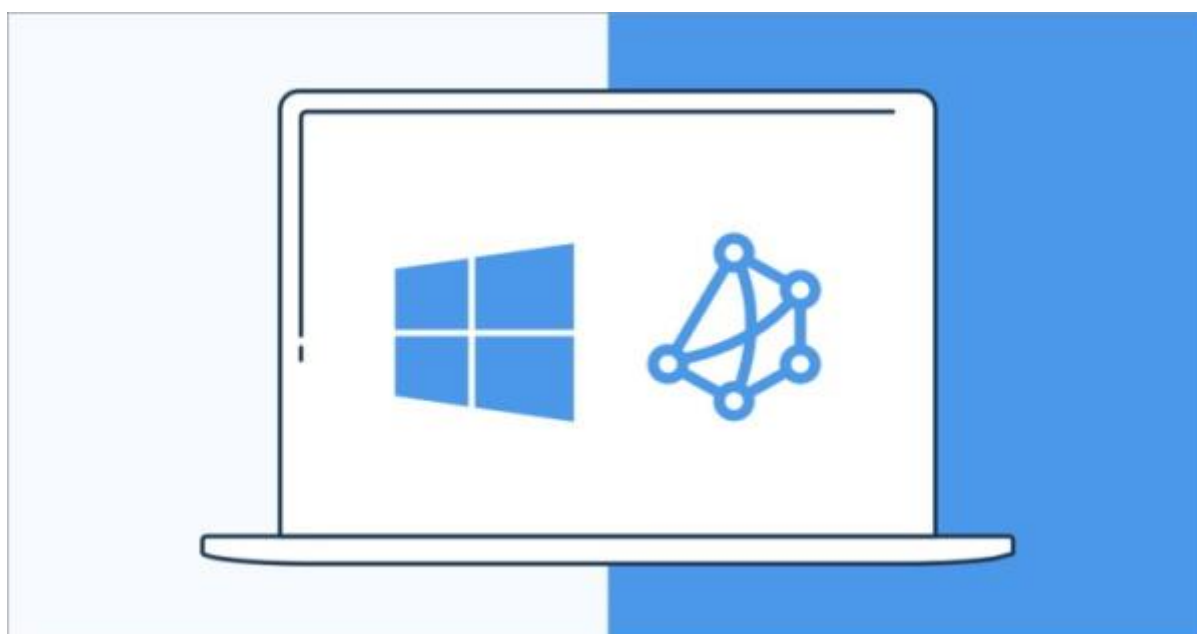
در این بخش از آموزش مانیتورینگ شبکه به این سوال پاسخ داده شده است که SLA چیست و چگونه صنعت IT را تحت تاثیر قرار می‌دهد؟ SLA قراردادی میان ارائه دهنده خدمات IT و صاحبان یک حوزه کسب و کار است. رعایت تعهدات SLA اغلب در طرح‌های غرامت فناوری اطلاعات گنجانده می‌شود. در واقع، قراردادهای SLA ضمانت‌نامه عملکرد هستند. معیارهای SLA اندازه‌گیری و گزارش داده می‌شوند. اما، چرا SLA اهمیت دارد؟ قراردادهای SLA به این دلیل دارای اهمیت هستند که عملکرد ضعیف و مدت از کار افتادگی شبکه بسیار هزینه‌بر است.

برای مثال، در خصوص یک فروشگاه آنلاین بزرگ، یک ساعت زمان از کار افتادگی می‌تواند چند صد میلیون تومان درآمد از دست رفته در پی داشته باشد. الزامات قرار داد SLA می‌تواند بسیار سختگیرانه باشد. برای مثال، زمان ارائه سرویس در قرارداد SLA می‌تواند ۹۹.۹۹ درصد باشد (که به آن SLA چهار نه گفته می‌شود)؛ به این معنی که در طول یک سال، مدت از کار افتادگی کم‌تر از یک ساعت باشد. هرچه SLA سختگیرانه‌تر باشد، پیاده‌سازی و نگهداری خدمات IT و شبکه هزینه بیش‌تری خواهد داشت. بنابراین، مانیتورینگ شبکه برای اندازه‌گیری SLA و برآورده کردن انتظارات کارفرما بسیار ضرورت دارد.

اجزای عمومی مانیتورینگ در ویندوز چه هستند ؟

کسب و کارها از اپلیکیشن‌های سازمانی مختلفی استفاده می‌کنند که روی سرورهای شبکه سازمان یا یک مرکز داده نصب شده‌اند تا خدماتی را به میزبان‌های داخل سازمان ارائه دهند. همچنین، سرویس‌های مدیریت شبکه دیگری نظیر DHCP، Active Directory، DNS و سایر موارد نیز در شبکه‌های سازمانی اجرا می‌شوند. علاوه بر آن، کاربران یا کلاینت‌های یک سازمان نیز به سیستم‌عامل نیاز دارند.

در میان انتخاب‌های مختلفی که برای یک سیستم‌عامل وجود دارد، سیستم‌عامل‌های مبتنی بر ویندوز، هم برای نیازمندی‌های سرور و هم میزبان‌های کلاینت در یک سازمان، پراستفاده‌ترین به حساب می‌آیند. اجرای اپلیکیشن‌های سازمانی روی سرورها، نظارت بر مصرف منابع را از قبیل حافظه، فضای دیسک، حافظه موقت (Cache)، پردازنده مرکزی و سایر موارد ایجاب می‌کند. همچنین، مانیتورینگ به شناسایی مشکلات احتمالی که عملکرد سرور را تحت تاثیر قرار می‌دهند نیز کمک می‌کند.



علاوه بر سرورها، دستگاه‌های کلاینت Client نیز جهت فراهم کردن تجربه بدون دردسر برای کاربران نهایی، باید تحت نظارت و مانیتورینگ قرار بگیرند. سیستم‌های تحت ویندوز می‌توانند برای

سیستم‌های مانیتورینگ داده فراهم کنند. این سیستم‌ها، داده‌ها را پردازش کرده و از آن‌ها برای گزارش کارایی و سلامت سرورها و ماشین‌های میزبان استفاده می‌کنند. داده‌هایی که برای نظارت استفاده می‌شوند را می‌توان با استفاده از روش‌های مختلف از یک ماشین ویندوزی جمع‌آوری کرد.

روش‌ها و پروتکل‌های کلی مانیتورینگ شبکه

پس از دانستن اینکه چه چیزهایی شبکه‌های کامپیوتری را تشکیل می‌دهند و اجزای در دسترس برای مانیتورینگ ویندوز چه هستند، در این بخش از آموزش مانیتورینگ شبکه روش‌های کلی مانیتورینگ شرح داده شده‌اند.

برای مانیتورینگ موفق شبکه و حتی سرورها و سیستم‌ها، در دسترس بودن گزینه‌های زیر لازم است:

- **داده‌ها یا اطلاعاتی از عناصر مختلف در شبکه؛ داده‌ها شامل اطلاعاتی درباره کارکرد، وضعیت فعلی، عملکرد و سلامت اجزای تحت نظارت است.**
- **یک نرم‌افزار یا اپلیکیشن مانیتورینگ باید بتواند داده‌ها را در یک قالب کاربر پسندانه جمع‌آوری، پردازش و ارائه کند. نرم‌افزار حتی باید بر اساس حد آستانه در خصوص مشکلات قریب‌الوقوع به کاربران هشدار بدهد.**
- **نیاز به یک پروتکل یا روش برای انتقال اطلاعات بین عنصر تحت نظارت و نرم‌افزار مانیتورینگ وجود دارد.**

اطلاعات جمع‌آوری شده به مدیریت بهتر و تحت نظر گرفتن شبکه، شناسایی مشکلات احتمالی شبکه پیش از بروز قطعی و رفع سریع ایرادات در زمان رخداد مشکل کمک می‌کند. به طور خلاصه، مانیتورینگ پیوسته، در ایجاد یک شبکه با کارایی بالا بسیار موثر است. در ادامه برخی از روش‌های کلی موجود برای مانیتورینگ معرفی شده‌اند. این تکنیک‌ها برای جمع‌آوری داده‌های مانیتورینگ از شبکه به کار می‌روند.

پینگ

پینگ (Ping) ابزاری برای اطمینان شبکه است که جهت تست دسترس‌پذیری یک میزبان در یک شبکه IP به کار گرفته می‌شود. داده‌های به دست آمده از نتایج پینگ می‌توانند مشخص کنند که آیا یک

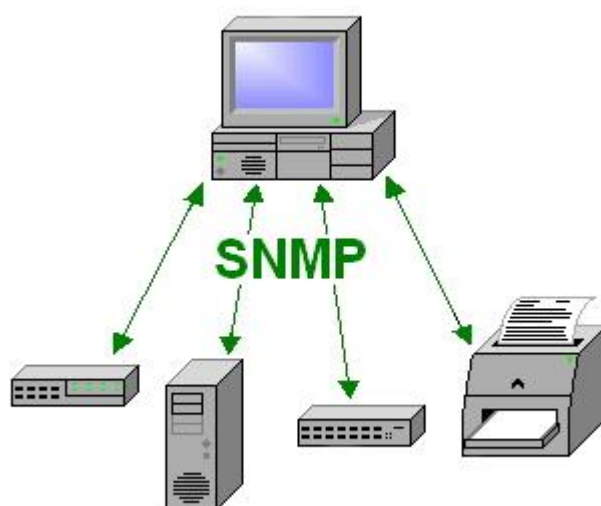
میزبان در شبکه فعال است یا خیر؟ علاوه بر این، دستور پینگ می‌تواند زمان انتقال و اتلاف بسته (Packet Loss) را در زمان ارتباط با یک میزبان تخمین بزند.

دستورالعمل ساده مدیریت شبکه (SNMP – Simple network Management Protocol)

SNMP یک پروتکل مدیریت شبکه است که برای تبادل اطلاعات بین میزبان‌ها در یک شبکه دارای نرم‌افزار مانیتورینگ مورد استفاده قرار می‌گیرد.

پروتکل SNMP پرکاربردترین پروتکل برای مدیریت و مانیتورینگ شبکه است. SNMP شامل اجزای زیر است:

- **دستگاه‌های تحت مدیریت:** گره‌ای در شبکه که از SNMP و دسترسی به اطلاعات خاص پشتیبانی می‌کند.
- **عامل (Agent):** نرم‌افزاری که بخشی از دستگاه تحت نظارت است. یک عامل به MIB (بنیان اطلاعاتی مدیریتی) دسترسی دارد و به سیستم‌های مدیریت مانیتورینگ شبکه اجزای خواندن و نوشتن در MIB را ارائه می‌دهد.
- **سیستم مدیریت شبکه (NMS):** اپلیکیشنی در سیستم است که دستگاه‌های تحت مدیریت را از طریق عامل با استفاده از دستورات SNMP نظارت و کنترل می‌کند.



داده‌های SNMP از یک دستگاه تحت مدیریت جمع‌آوری یا به آن ارسال می‌شود. این کار به روش نمونه‌برداری (Polling) یا با استفاده از دام (تله) انجام می‌شود. دام به یک عامل اجازه می‌دهد تا اطلاعاتی را درباره رویدادها در یک دستگاه به NMS ارسال کند. MIB اطلاعاتی را درباره ساختار داده در یک دستگاه برای مدیریت داده‌ها نگهداری می‌کند. MIB ها حاوی OID (شناسه شی Object Identification) هستند. شناسه متغیری است که باید از دستگاه خوانده یا در آن تنظیم شود.

Syslog

Syslog نباید با Eventlog ویندوز اشتباه گرفته شود. Syslog یک سیستم رویدادنگاری پیام است که اجازه می‌دهد یک دستگاه اعلان‌های رویداد را در شبکه IP ارسال کند. می‌توان از اطلاعات این پیام‌ها برای مدیریت سیستم و همچنین حسابرسی امنیتی استفاده کرد. Syslog ها در دستگاه‌های مختلفی از پرینترها تا روترها و فایروال‌ها، تحت پشتیبانی هستند.

استفاده از اسکریپت

در شبکه‌هایی که یک NMS برای مانیتورینگ در دسترس نیست یا NMS فعلی از برخی قابلیت‌ها پشتیبانی نمی‌کند، مدیران شبکه می‌توانند از اسکریپت‌ها استفاده کنند. اسکریپت‌ها از دستورات مشترکی مانند Snmpwalk ،Lynx ، netstat ، Ping و سایر موارد استفاده می‌کنند.

این دستورات در اکثر اجزا شبکه برای انجام عملیاتی نظیر جمع‌آوری اطلاعات از اجزا، اعمال تغییرات در پیکربندی دستگاه یا اجرای یک وظیفه زمان‌بندی شده پشتیبانی می‌کنند. اسکریپت‌های Bash ، Perl و سایر موارد، ابزارهای اسکریپ‌نویسی رایجی هستند که توسط مدیران شبکه مورد استفاده قرار می‌گیرند.

فلسفه طراحی مانیتورینگ شبکه چیست؟

به جهت اینکه مانیتورینگ شبکه ارزش افزوده‌ای برای شبکه فراهم کند، طراحی مانیتورینگ شبکه باید از برخی قواعد پایه پیروی کند. به عنوان یکی از این قواعد، مانیتورینگ شبکه باید همه جانبه باشد

و همه جنبه‌های یک سازمان نظیر شبکه و اتصال، سیستم‌ها و امنیت را پوشش دهد. همچنین، ترجیح داده می‌شود که سیستم، دیدگاه یکپارچه‌ای از همه چیز در شبکه شامل شناسایی مشکل، رفع مشکل و نگهداری شبکه داشته باشد.

علاوه بر این، هر سیستم مانیتورینگ باید امکان تهیه گزارش‌هایی را برای مخاطبین با سطوح مختلف از مدیران شبکه و سیستم تا مدیران سازمان فراهم کند. از همه مهم‌تر، درک و استفاده از یک سیستم مانیتورینگ نباید بیش از حد پیچیده باشد و همچنین نباید دارای کمبود امکانات گزارش‌گیری و امکانات ورود به جزئیات باشد. در ادامه، به معرفی و بیان مفهوم FCAPS پرداخته شده است.

FCAPS در مانیتورینگ شبکه چیست ؟

مدیریت شبکه یک زمینه وسیع است که قابلیت‌های گوناگونی را در بر می‌گیرد. **اهداف مختلف مدیریت شبکه در پنج بخش (گروه) مختلف دسته‌بندی می‌شوند.** این بخش‌ها شامل موارد زیر است:

➤ مدیریت خطا (Fault Management)

➤ مدیریت پیکربندی (Configuration Management)

➤ مدیریت حسابداری (Accounting Management)

➤ مدیریت کارایی (Performance Management)

➤ مدیریت امنیت (Security Management)

این پنج بخش در مدیریت شبکه، با ترکیب حروف اول هر یک از بخش‌های فوق یا همان سرنام FCAPS شناخته می‌شوند. در شبکه‌هایی که هزینه‌ای بابت استفاده از پهنای باند و ترافیک پرداخت نمی‌شود، حسابداری با سرپرستی یا مدیریت شبکه (Administration) جایگزین می‌شود.

مدیریت خطا

مدیریت خطا با فرآیند شناسایی، جداسازی و برطرف کردن خطاهایی سر و کار دارد که در شبکه رخ می‌دهند. شناسایی مشکلات بالقوه شبکه نیز در حیطه مدیریت خطا یا Fault Management قرار می‌گیرد.



مدیریت پیکربندی

مدیریت پیکربندی شامل شناسایی دستگاه‌های شبکه، نگهداری از تجهیزات شبکه، پیکربندی پشتیبان، نظارت بر تغییرات پیکربندی و انطباق، ردیابی فعالیت کاربر و عیب‌یابی به وسیله اجرای عملیات صحیح شبکه در زمان لازم است.

مدیریت حسابداری

این بخش از مدیریت شبکه در شبکه‌های ارائه‌دهنده سرویس کاربرد دارد. در این شبکه‌ها، مصرف ترافیک شبکه ردیابی و سپس از اطلاعات به دست آمده برای دریافت هزینه استفاده می‌شود. در شبکه‌هایی که هزینه‌ای بابت ترافیک سرویس دریافت یا پرداخت نمی‌شود، حسابداری با مدیریت شبکه

جایگزین می‌شود. مدیریت یا Administration به سرپرستی و مدیریت کاربران نهایی در شبکه با استفاده از رمز عبور، اجازه دسترسی و سایر موارد گفته می‌شود.

مدیریت کارایی

مدیریت کارایی شامل مدیریت عملکرد و کارایی کلی شبکه است. داده‌های پارامترهای مربوط به کارایی نظیر توان عملیاتی، از دست رفتن بسته، زمان‌های پاسخگویی، میزان مصرف و سایر موارد معمولاً با استفاده از پروتکل SNMP جمع‌آوری می‌شوند.

مدیریت امنیت

مدیریت امنیت یکی دیگر از بخش‌های مهم در مدیریت شبکه است. مدیریت امنیت در FCAPS فرایند کنترل دسترسی به منابع شامل داده‌ها، تنظیمات و محافظت از کاربران در برابر کاربران غیرمجاز در شبکه است. در ادامه آموزش مانیتورینگ شبکه، به شرح وظایف پنج‌گانه در مانیتورینگ شبکه پرداخته شده است.

وظایف پنج‌گانه مانیتورینگ شبکه چیست؟

سیستم‌های مانیتورینگ شبکه دارای پنج وظیفه یا کارکرد اساسی هستند:

➤ **اکتشاف**

➤ **نقشه‌کشی**

➤ **نظارت (دیدهبانی / مانیتور کردن)**

➤ **هشدار**

➤ **گزارش‌گیری**

سیستم‌های مانیتورینگ شبکه مختلف، در خصوص قابلیت‌ها و امکاناتی که در قالب هر یک از این وظایف ارائه می‌دهند با یکدیگر تفاوت دارند.

اکتشاف

اکتشاف یا شناسایی (Discovery) به معنی پیدا کردن دستگاه‌های داخل شبکه است. مانیتورینگ شبکه با فرآیند اکتشاف آغاز می‌شود. به بیان ساده، اگر درباره آنچه در شبکه وجود دارد و نحوه اتصال دستگاه‌ها اطلاعی در دست نباشد، نمی‌توان نظارتی انجام داد. سیستم‌های مانیتورینگ شبکه دستگاه‌های داخل شبکه از جمله روترها، سوئیچ‌ها، فایروال‌ها، سرورها، پرینترها و سایر موارد را کشف و شناسایی می‌کنند. سیستم‌های مانیتورینگ شبکه کتابخانه‌ای از قالب‌هایی را شامل می‌شوند که چگونگی نظارت بر یک دستگاه را تعیین می‌کنند.

می‌توان این قالب‌ها را «نقش دستگاه» (Device Role) نامید. نقش دستگاه‌ها بسته به نوع و تولیدکننده متفاوت هستند. برای مثال، نظارتی که از یک روتر سیسکو انجام می‌شود با مانیتور کردن یک سرور Dell متفاوت است. وقتی که یک سیستم مانیتورینگ شبکه فرآیند اکتشاف را به اتمام می‌رساند، به صورت خودکار یک نقش دستگاه متناسب را به هر دستگاه کشف شده اختصاص می‌دهد. سیستم‌های مانیتورینگ شبکه از دیدگاه قابلیت‌های اکتشافی با یکدیگر متفاوت هستند.

تمام سیستم‌های مانیتورینگ، دستگاه‌های موجود در یک شبکه را شناسایی می‌کنند. اما، همه آن‌ها نمی‌توانند چگونگی اتصال دستگاه‌ها به شبکه را شناسایی کنند. برای مثال، یک سیستم مانیتورینگ شبکه ممکن است یک سرور را روی شبکه شناسایی کرده باشد. اما، ممکن است از اینکه آن سرور به کدام سوئیچ متصل شده اطلاعی نداشته باشد. یک سیستم مانیتورینگ با امکان اکتشاف لایه دو/سه، اتصال پورت به پورت میان دستگاه‌های شبکه را شناسایی می‌کند.

به منظور مانیتورینگ موثر شبکه، تنها دانستن اینکه چه دستگاه‌هایی در شبکه وجود دارند کافی نیست. بلکه باید اطلاعاتی از نحوه اتصال دستگاه‌ها نیز در دست باشد. زیرا یک مشکل عملکردی در یک دستگاه می‌تواند در عملکرد دستگاه دیگر نیز اختلال ایجاد کند. مثلاً وقتی یک سوئیچ قطع می‌شود، ارتباط تمام دستگاه‌های متصل به آن سوئیچ قطع خواهد شد. اگر این مشکل برای سوئیچی رخ دهد که به سرورهای سیستم CRM یک سازمان متصل است، مشکلی بزرگ و اساسی به وجود خواهد آمد. در ادامه آموزش مانیتورینگ شبکه به کارکرد نقشه‌کشی به عنوان یکی از وظایف پnjگانه مانیتورینگ شبکه پرداخته شده است.

نقشه‌کشی

نقشه‌کشی به معنی بصری‌سازی (مصورسازی) شبکه است. چشمان یک مدیر شبکه ارزشمندترین ابزار تشخیصی او به حساب می‌آیند. با امکان بصری‌سازی شبکه می‌توان ساعت‌ها یا حتی روزها در زمان عیب‌یابی مشکلات شبکه صرفه‌جویی کرد. متأسفانه، گمدهای سیم‌کشی شبکه بسیار پیچیده و به هم ریخته می‌شوند. این مسئله امکان بصری‌سازی ادمین شبکه را از بین می‌برد و مانع حل مسئله می‌شود. سیستم‌های مانیتورینگ شبکه نقشه‌هایی از شبکه ایجاد می‌کنند. نقشه‌های شبکه ابزارهای واکنش اولیه‌ای هستند که امکان بصری‌سازی شبکه را برای مدیران شبکه فراهم می‌کنند.

نقشه‌ها بازنمایی شفاف و منظمی از کمد سیم‌کشی ارائه می‌دهند. نقشه‌های شبکه دستگاه‌ها و وضعیت به‌روز شده آن‌ها را نمایش می‌دهند. در بسیاری از سیستم‌های مانیتورینگ شبکه برای ایجاد یک نقشه از شبکه نیاز به پردازش‌های دستی زیادی وجود دارد. برخی دیگر از NMS ها نیز فقط یک ابزار نقشه‌کشی (رسم) ارائه می‌دهند و به دانش ادمین شبکه برای کشیدن نقشه شبکه وابسته هستند.

نظارت

همان‌طور که بیان شد، سیستم‌های مانیتورینگ شبکه نقش دستگاه‌ها را تعیین می‌کنند تا مشخص شود چه چیزی را باید نظارت کنند. مدیران شبکه می‌توانند نقش دستگاه‌ها را ویرایش کنند یا نقش‌های جدیدی را از صفر ایجاد کنند. سیستم‌های مانیتورینگ شبکه انتخاب‌های نظارتی بسیاری را در اختیار مدیران شبکه قرار می‌دهند.

معمولاً به عنوان یک نقطه شروع، مدیران شبکه می‌خواهند پنج مشخصه اصلی هر دستگاه شبکه را مانیتور کنند. این پنج مشخصه شامل موارد زیر است:

- پینگ داشتن دستگاه
- میزان تاخیر (Latency)
- میزان مصرف CPU
- میزان مصرف حافظه



اکثر ابزارهای مانیتورینگ شبکه امکان نظارت را برای سایر اجزا سخت‌افزاری نظیر خنک‌کننده‌ها و منابع تغذیه در یک سوئیچ فراهم می‌کنند و حتی بر دمای یک کمد سیم‌کشی نظارت می‌کنند. همچنین، آن‌ها می‌توانند بر سرویس‌های شبکه مانند TCP/IP، HTTP و FTP نیز نظارت داشته باشند.

هشداردهی

هشداردهی به معنی مطلع شدن از بروز خرابی یا نقص در شبکه است. سیستم‌های مانیتورینگ مدیران شبکه را در زمان وقوع یک مشکل مطلع می‌کنند. این سیستم‌ها از طریق ایمیل، متن و رویدادننگاری (Logging) | هشدار می‌دهند.

هشدار مبتنی بر آستانه این امکان را برای مدیران شبکه فراهم می‌کند تا آن‌ها بتوانند پیش از تحت تاثیر قرار گرفتن کاربران، اپلیکیشن‌ها یا سازمان به مشکلات رسیدگی کنند. برای مثال، NMS به‌گونه‌ای تنظیم می‌شود تا در صورت مصرف بیش از ۸۰ درصد از منابع CPU در یک روتر، هشدار برای ادمین شبکه ارسال شود. این هشدار به ادمین شبکه امکان می‌دهد تا به صورت فعالانه و پیش از خرابی کامل روتر، بررسی‌های لازم را انجام دهد و وارد عمل شود.

معیارهای عملکردی نظیر CPU، حافظه و مصرف واسط در طول روز نوسان می‌کنند. ممکن است این معیارها در طول روز برای چند ثانیه یا چند دقیقه در مقاطع اوج مصرف از سطح آستانه عبور کنند. مدیران شبکه نمی‌خواهند این نوسان‌های جزئی و لحظه‌ای برای آن‌ها مزاحمت ایجاد کنند. برای جلوگیری از چنین مزاحمت‌هایی، هشدارهای سیستم‌های مانیتورینگ شبکه با عناصر زمانی تنظیم می‌شوند. برای مثال، در صورتی که مدت زمان تجاوز ۸۰ درصدی میزان مصرف CPU از ۱۰ دقیقه بیش‌تر شود، آنگاه یک هشدار ارسال خواهد شد.

گزارش‌گیری

اثبات رعایت SLA به وسیله گزارش‌گیری لحظه‌ای و همچنین گزارش بر اساس داده‌های گذشته انجام می‌شود. مدیران شبکه همواره درگیر چرخه حیات طراحی، تحلیل و بازطراحی شبکه هستند. برای پشتیبانی از این چرخه حیات، سیستم‌های NMS داده‌های نظارتی لحظه‌ای و تاریخی فراهم می‌کنند. این اطلاعات به مدیران شبکه کمک می‌کنند تا کارهای زیر را انجام دهند:

➤ **تایید اینکه طراحی شبکه فاقد مشکل است و نتایج مطلوب‌اند.**

➤ **کشف روندهایی که توانایی شبکه را در تامین عملکرد مورد نیاز کاربران، اپلیکیشن‌ها و سازمان تحت تاثیر قرار می‌دهند.**

➤ **محافظت از کارایی و رفع سریع مشکلات**

➤ **اثبات رعایت تعهدات SLA**

سیستم‌های مانیتورینگ شبکه، در صفحات وب اطلاعات نظارتی ارائه می‌دهند. به این صفحات وب، داشبورد Dashboard گفته می‌شود. داشبوردها از نماهای آماده اختصاصی تشکیل شده‌اند. برای مثال، می‌توان نمایی (View) را نام برد که ۱۰ سی‌پی‌یو با بیش‌ترین میزان مصرف را نشان می‌دهد. مدیران شبکه از داشبوردهای خلاصه برای ارزیابی کارکرد صحیح و سلامت کل شبکه استفاده می‌کنند.

مدیران شبکه داشبوردهای جزئی‌تر مربوط به دستگاه‌های خاص را مورد بررسی قرار می‌دهند تا بتوانند به سرعت از شبکه در برابر مشکلات عملکردی محافظت کنند. اکثر سیستم‌های مانیتورینگ شبکه

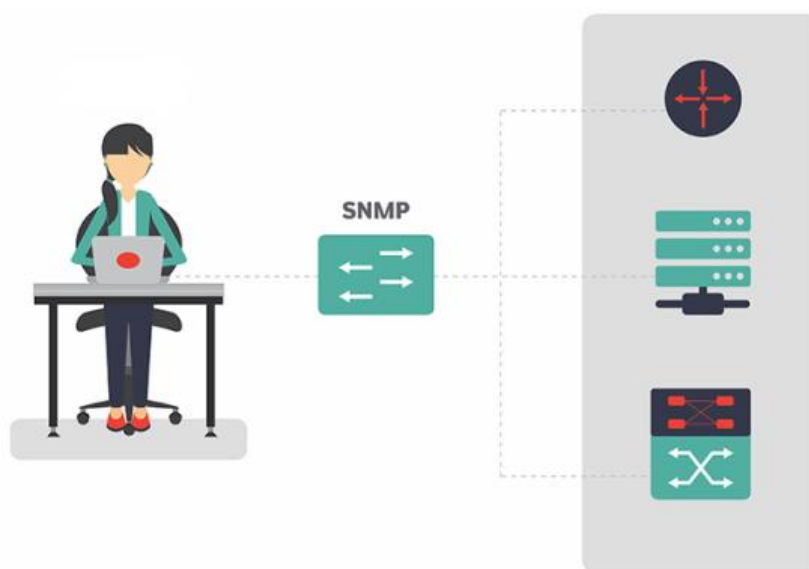
قابل شخصی سازی هستند. مدیران می توانند داشبوردهایی را برای مشتریان داخلی، مدیران، صاحبان کسب و کار، واحد Help Desk و همتایان سیستم های مدیریتی و اپلیکیشن ها فراهم کنند.

یک ابزار مانیتورینگ شبکه چطور کار می کند ؟

سیستم های مانیتورینگ شبکه با استفاده از پروتکل های زیر داده های عملکردی را از دستگاه های شبکه و سرورها استخراج می کنند.

- **SNMP:** *(Simple Network Management Protocol)* پروتکل ساده مدیریت شبکه
- **WMI:** *(Windows Management Instrumentation)* ابزار دقیق مدیریت ویندوز
- **SSH:** *(Secure Shell for Unix and Linux server)* و لینوکس شل ایمن برای سرور یونیکس

برخی از سیستم های مانیتورینگ شبکه از زبان های اسکریپتی مثل Powershell جهت ایجاد مانیتورینگ سفارشی برای سرورهای ویندوز و کوئری های SQL جهت ایجاد مانیتورینگ سفارشی برای پایگاه های داده پشتیبانی می کنند. دو تا از پروتکل هایی که به طور گسترده استفاده می شوند، SNMP و WMI نام دارند. این پروتکل ها امکان مانیتورینگ گسترده ای را جهت ارزیابی سلامت شبکه و دستگاه ها فراهم می کنند.



پروتکل SNMP چیست ؟

SNMP یک پروتکل استاندارد است که داده‌ها را تقریباً از هر دستگاه متصلی جمع‌آوری می‌کند. این دستگاه‌ها شامل روترها، سوئیچ‌ها، کنترلرهای شبکه محلی وایرلس، اکسس پوینت‌های وایرلس، سرورها، پرینترها و سایر موارد است. نحوه عملکرد پروتکل SNMP از طریق جست‌وجوی اشیا انجام می‌شود. یک شی به آنچه گفته می‌شود که یک سیستم مانیتورینگ شبکه راجع به آن اطلاعات جمع‌آوری می‌کند. برای مثال، «میزان مصرف CPU یک شی SNMP به حساب می‌آید. جست‌وجو برای شی مصرف CPU مقداری را باز می‌گرداند که یک NMS از آن برای هشدار و گزارش‌گیری استفاده می‌کند. اشیا که به وسیله SNMP جست‌وجو می‌شوند، در یک پایگاه مدیریت اطلاعات (MIB) نگهداری می‌شوند.

یک MIB تمام اطلاعاتی را تعریف می‌کند که توسط دستگاه تحت نظارت نشان داده می‌شوند. برای مثال، MIB یک روتر سیسکو حاوی تمام اشیا تعریف شده توسط سیسکو خواهد بود که می‌توان از اشیا برای نظارت آن روتر شامل نظارت بر مصرف CPU، حافظه و وضعیت واسط تعاملی استفاده کرد.

اشیا در یک MIB با استفاده از یک سیستم شماره‌گذاری استانداردسازی شده فهرست‌بندی می‌شوند. هر شی شناسه منحصر به فردی دارد که به اختصار به آن OID گفته می‌شود. برخی از سیستم‌های مانیتورینگ شبکه یک مرورگر MIB فراهم می‌کنند. مرورگر MIB به مدیران شبکه اجازه می‌دهد تا در یک MIB جست‌وجو کنند و اشیا بیش‌تری را از یک دستگاه برای نظارت پیدا کنند.

پروتکل WMI چیست ؟

پروتکل WMI یا «ابزار دقیق مدیریت ویندوز»، پیاده‌سازی مبتنی بر وب مدیریت سازمانی (Enterprise Management) است که توسط شرکت مایکروسافت ارائه می‌شود. WMI یک طرح نوآوری جهت توسعه استاندارد برای دسترسی به اطلاعات مدیریتی در سازمان محسوب می‌شود. این پروتکل، یک واسط سیستم‌عامل ایجاد می‌کند که این واسط، اطلاعاتی را از دستگاه‌های دارای عامل WMI دریافت می‌کند. WMI جزئیاتی را پیرامون موارد زیر دریافت می‌کند:

➤ سیستم‌عامل

➤ داده‌های سخت‌افزاری یا نرم‌افزاری

➤ وضعیت یا خصوصیت‌های سیستم‌های محلی یا راه دور

➤ پیکربندی و اطلاعات امنیتی

➤ اطلاعات پردازشی و خدماتی

سیس، WMI تمام این جزئیات را به نرم‌افزار مدیریت شبکه انتقال می‌دهد. نرم‌افزار مدیریت شبکه نیز بر سلامت شبکه، عملکرد و در دسترس بودن آن نظارت می‌کند. با وجود اینکه WMI یک پروتکل اختصاصی برای سیستم‌ها و کاربردهای مبتنی بر ویندوز به حساب می‌آید، می‌تواند با پروتکل SNMP و سایر پروتکل‌ها کار کند. اگرچه، شرکت مایکروسافت دستورات WMI در ویندوز را به نفع CIM cmdlet منسوخ کرده است. به همین دلیل در صورت استفاده از پاورشل ویندوز برای مدیریت WMI، باید از CIM cmdlet به جای دستورات WMI استفاده کرد.



سیستم‌های مانیتورینگ شبکه برای عملیات مختلف مرتبط با مانیتورینگ داده‌های بسیاری را از اجزای شبکه گردآوری می‌کنند. همچنین، شبکه‌ها نیازمند مانیتورینگ پیوسته هستند تا اطمینان حاصل شود که مشکلات پیش از بروز قطعی در شبکه شناسایی خواهند شد. این جمع‌آوری پیوسته داده‌ها برای مانیتورینگ به انباشت حجم عظیمی از داده‌ها منجر می‌شود. **پیامدهای انباشت داده‌ها** در ادامه فهرست شده‌اند:

- **کندی در عملکرد راهکار مانیتورینگ؛ زیرا ابزار مانیتورینگ شبکه باید داده‌های بیش‌تری را برای تولید گزارش‌های مورد نیاز تجزیه و تحلیل کند.**
- **تأثیر بر فضای ذخیره‌سازی مورد نیاز برای ذخیره داده‌های مانیتورینگ که به نوبه خود هزینه کلی مالکیت بر سیستم مانیتورینگ را افزایش می‌دهد.**
- **بروز کندی در عیب‌یابی به دلیل حجم بیش‌تر داده‌هایی که باید تحلیل شوند.**

سیستم‌های مانیتورینگ از تجمیع داده‌ها برای جلوگیری از سناریوهای فوق بهره می‌برند. تجمیع داده به فرآیندی گفته می‌شود که در آن اطلاعات جمع‌آوری شده در طول زمان خلاصه‌سازی (دانه‌بندی) می‌شوند و به صورت داده‌هایی با جزئیات (دانه‌دانه) کم‌تر درمی‌آیند که برای تولید سریع‌تر گزارش‌های تاریخی مورد استفاده قرار می‌گیرند. دانه‌بندی یک گزارش تولید شده از داده‌های تجمیع شده به الگوی تجمیع سیستم مانیتورینگ بستگی خواهد داشت.

بسیاری از سیستم‌های مانیتورینگ با ذخیره داده به صورت دانه‌بندی یک دقیقه‌ای شروع می‌کنند. در طول زمان، داده‌ها متعادل و در جداول داده با دانه‌بندی کم‌تر مثلاً ۱۰ دقیقه‌ای، ساعتی یا حتی هفتگی بسته‌بندی می‌شوند. این به یک سیستم مانیتورینگ اجازه می‌دهد تا گزارش‌هایی را پیرامون یک گره در شبکه ایجاد کند که می‌توانند در زمان به عقب بروند یا یک دوره زمانی طولانی را شامل شوند و هیچ مشکلی در عملکرد و فشار بر نیازهای فضای ذخیره‌سازی نداشته باشند.

مروری بر مانیتورینگ مبتنی بر عامل یا Agent

ابزارهای مانیتورینگ شبکه و سیستم به صورت عامل محور Agent Base و یا بدون عامل Agent Less و یا ترکیبی از این دو حالت هستند. یک عامل یا Agent، نرم‌افزاری در یک دستگاه تحت نظارت است که به داده‌های عملکردی دستگاه دسترسی دارد. این داده‌ها بر اساس درخواست‌های ایجاد شده از جانب NMS یا در برخی موارد، بر اساس خط‌مشی‌های تعریف شده در داخل عامل به یک سیستم NMS ارسال می‌شوند. حضور یک عامل در دستگاه تحت نظارت، دسترسی به داده‌های دانه‌دانه را فراهم می‌کند که به نوبه خود به نظارت بهتر، گزارش‌گیری و رفع ایرادات کمک می‌کند. مانیتورینگ مبتنی بر عامل یا مانیتورینگ Agent base یا عامل محور، برتری‌هایی فراهم می‌کند که به شرح زیرند:

➤ داده‌های دانه‌بندی شده

➤ امکان مانیتورینگ معیارهای غیراستاندارد در دستگاه

➤ قابلیت اجرای عملیات در دستگاه تحت نظارت



اما، یک رویکرد مبتنی بر عامل می‌تواند زمان‌بر هم باشد. زیرا نیازمند این مسئله است که عامل‌ها در هر دستگاه تحت نظارت نصب شوند و همچنین به‌روزرسانی و نگهداری تمام عامل‌های مستقر در شبکه نیز باید انجام شود.

مروری بر مانیتورینگ بدون عامل

مانیتورینگ بدون عامل، همان‌طور که از نامش پیداست، فاقد یک عامل مستقر در دستگاه تحت نظارت است. در این روش، مانیتورینگ با استفاده از API‌های راه دور انجام می‌شود. این کار به وسیله خدماتی که باید مانیتور شوند یا به وسیله تحلیل بسته‌های داده انتقالی به یا از دستگاه‌های تحت نظارت صورت می‌گیرد.

SNMP رایج‌ترین روش بدون عامل استفاده شده برای نظارت بر اجزای شبکه است WMI. یا ابزار دقیق مدیریت ویندوز نیز برای مانیتورینگ سیستم‌های ویندوزی به کار می‌رود. استفاده از مانیتورینگ بدون عامل مزایای زیر را به همراه دارد:

- عدم نیاز به استقرار عامل در هر دستگاه تحت نظارت
- هزینه‌های کمتر برای استقرار و نگهداری
- به دلیل نبود یک اپلیکیشن عامل یا نرم‌افزار روی کلاینت، هیچ تاثیر و باری بر دوش کلاینت ندارد.

اگرچه، مانیتورینگ بدون عامل کاستی‌هایی هم دارد. مهم‌ترین آن، کمبود گزارش‌های عمیق است، نسبت به آنچه مانیتورینگ عامل محور فراهم می‌کند. همچنین، مانیتورینگ بدون عامل، در خصوص پشتیبانی که می‌تواند برای دستگاه‌های سفارشی یا سرورهایی ارائه دهد که MIB ها یا داده‌هایی دارند که در روش‌های جمع‌آوری داده بدون عامل از طریق API ها آشکار نمی‌شوند، دارای محدودیت است.

قواعد مشترک مانیتورینگ شبکه

داشتن یک خط مشی در مدیریت و مانیتورینگ شبکه به اندازه طراحی شبکه و پیاده‌سازی آن اهمیت دارد. بدون مانیتورینگ شبکه، یک شبکه با طراحی مناسب نیز با کوچک‌ترین مشکلات دچار اختلال و قطعی خواهد شد. در پیاده‌سازی یک راهکار مانیتورینگ شبکه، قواعد مشترکی توسط سازمان‌ها و سرپرستان شبکه به کار گرفته می‌شوند. این قواعد مشترک، به تعریف یک خط‌مشی ابتدایی برای شروع کار با اطلاعات گره‌ها و پارامترهایی که نیاز به نظارت دارند، کمک می‌کنند. این بدان معنا نیست که مانیتورینگ شبکه تنها به این قواعد محدود می‌شود.

قواعد مشترک پایه‌هایی را تعریف می‌کنند که بخشی از مانیتورینگ شبکه هستند. علاوه بر قواعد مشترکی که در ادامه بیان شده‌اند، سرپرست یا ادمین شبکه باید طراحی و نیازمندی‌های شبکه‌ای را درک کند که تحت مدیریت خود دارد و بتواند سازکارهای مانیتورینگ افزوده‌ای را برای تحت نظر قرار دادن تمام معیارها و عناصر موجود در شبکه پیاده‌سازی کند

مانیتورینگ دسترس پذیری

مانیتورینگ دسترس پذیری یا Availability Monitoring ، نظارت بر تمام منابع در زیرساخت شبکه IT برای اطمینان از دسترس پذیری آنها با هدف پاسخ به نیازمندی های سازمان و کاربران آن تعریف می شود. امروزه، زیرساخت های شبکه نیاز به برقراری ۱۰۰ درصدی برای پاسخگویی به نیازهای کسب و کار دارند.

شبکه و خدماتی که در شبکه ارائه می شوند باید به طور دائم در دسترس باشند تا استمرار کسب و کار تضمین شود. مانیتورینگ دسترس پذیری در چنین موقعیتی کاربرد دارد. با مانیتورینگ پیوسته منابع و خدمات، از فعال بودن گره ها و سرویس ها برای اجرای وظایف اطمینان حاصل می شود. برخی از مثال های مانیتورینگ دسترس پذیری شامل موارد زیر است:

- مانیتورینگ دستگاه های شبکه برای اطمینان از کارکرد بدون مشکل آنها
- در دسترس بودن فضای ذخیره سازی برای ذخیره داده های سازمانی
- نظارت بر خدمات سطح سیستم برای اطمینان از اینکه برنامه های حیاتی سازمان به خوبی کار می کنند.

برخی از ابزارهای رایج برای مانیتورینگ دسترس پذیری شامل موارد زیر است:

- **پینگ:** رایج ترین روش مورد استفاده است. پینگ ها در پروتکل ICMP به یک دستگاه تحت نظارت ارسال می شوند و در دسترس بودن دستگاه یا خدمات بر اساس پاسخ های پینگ بررسی و تخمین زده می شوند.
- **Telnet:** تلنت برای بررسی دسترس پذیری دستگاه در شبکه هایی استفاده می شود که پینگ در آنها مسدود باشد.
- **SNMP:** برای تخمین دسترس پذیری یا وضعیت فعلی خدمات در یک دستگاه مورد استفاده قرار می گیرد.
- **WMI:** برای بررسی دسترس پذیری خدماتی به کار می رود که روی سیستم های ویندوزی اجرا می شوند.
- **IPSLA:** یک قابلیت سیسکوئی است که در دسترس بودن لینک های WAN و ظرفیت آنها برای حمل خدمات خاص را اندازه گیری می کند.

مانیتورینگ واسط تعاملی

چندین نوع مختلف واسط تعاملی در یک شبکه مورد استفاده قرار می‌گیرد. از جمله این واسط‌های تعاملی می‌توان به اترنت سریع و اترنت گیگابیت تا واسط‌های تعاملی فوق سریع کانال فیبر نوری اشاره کرد. رابط یا واسط تعاملی (Interface) در یک شبکه، به نقاط ورودی و خروجی بسته‌هایی گفته می‌شود که یک سرویس را برای سازمان فراهم می‌کنند. در صورتی که یک خطا وجود داشته باشد، بسته‌ها از دست بروند یا حتی خود واسط تعاملی از کار بیوفتد، منجر به افت کیفیت تجربه کاربری خواهد شد. مانیتورینگ واسط تعاملی (Interface Monitoring) شامل نظارت بر واسط‌های تعاملی برای شناسایی خطا، اتلاف بسته‌ها، از رده خارج شدن، محدودیت‌های کارکردی و سایر موارد است.

اطلاعات کسب شده از مانیتورینگ واسط تعاملی به شناسایی آن دسته از مشکلات احتمالی در شبکه کمک می‌کنند که عامل کاربرد یا عملکرد ضعیف شبکه هستند. سیستم‌های مانیتورینگ شبکه از پینگ یا SNMP برای گردآوری اطلاعات آماری از دستگاه‌های شبکه استفاده می‌کنند. در حالی که، پینگ با استفاده از بسته‌های ICMP وضعیت واسط‌های تعاملی نظیر نرخ بسته‌های از دست رفته، زمان سفر بازگشتی یا چرخشی (Round Trip) و سایر موارد را گزارش می‌دهد، جمع‌آوری داده مبتنی بر SNMP به نظارت بر مصرف پهنای باند واسط تعاملی، سرعت ترافیک در واسط، خطاها و سایر موارد کمک می‌کند. مجموع این اطلاعات، کمکی برای شناسایی مشکلات عملکردی کاربردها در شبکه است.

مانیتورینگ دیسک

داده‌ها یا اطلاعات یکی از مهم‌ترین منابع برای یک سازمان به حساب می‌آیند. سازمان‌ها برای برنامه‌ریزی تجاری و بهره‌وری مطلوب به داده‌ها نیاز دارند. داده‌هایی که مورد نیاز یک سازمان هستند، باید برای بایگانی یا استفاده در آینده در جایی ذخیره شوند. در سازمان‌ها، داده‌ها در آرایه‌های ذخیره‌سازی جمع‌آوری و ذخیره می‌شوند. این آرایه‌ها دارای چندین دیسک هستند. در صورت بروز هر گونه مشکل در دیسک‌ها یا آرایه‌های ذخیره‌سازی که داده‌های سازمانی را نگهداری می‌کنند، پیامدهای جدی در استمرار کسب و کار به وجود خواهد آمد. برخی از کارهایی که در مانیتورینگ دیسک (Disk Monitoring) انجام می‌شود، شامل موارد زیر است:

➤ مدیریت صحیح فضای دیسک با هدف دستیابی به مصرف حافظه موثر

➤ نظارت بر کارایی و عملکرد دیسک در برابر خطاها

➤ وضعیت فایل های بزرگ، فضای آزاد و تغییرات در مصرف فضای دیسک

➤ عملکرد ورودی/خروجی

➤ سایر موارد



مانیتورینگ دیسک به مدیران شبکه اجازه می‌دهد تا از قبل برای به‌روزرسانی‌های سیستم، فضا، شناسایی مشکلات مربوط به ذخیره‌سازی و کاهش زمان قطعی در صورت بروز یک مشکل برنامه‌ریزی کنند.

مانیتورینگ سخت‌افزار

یک شبکه شامل دستگاه‌های سخت‌افزاری بسیاری نظیر دستگاه‌هایی است که برای مسیریابی، سوئیچینگ، ذخیره‌سازی، اتصال، سرورهای اپلیکیشن و سایر موارد به کار می‌روند. سخت‌افزار، ستون فقرات کل زیرساخت IT را شکل می‌دهد. در صورتی که یک سخت‌افزار حیاتی برای عملیات روزمره در شبکه از کار بیوفتد، منجر به بروز زمان خاموشی در شبکه خواهد شد.

برای مثال، یک منبع تغذیه معیوب در سوئیچ مرکزی یا داغ کردن بیش از حد روتر مرزی می‌تواند قطعی شبکه را به همراه داشته باشد. برای کسب اطمینان از کارکرد صحیح شبکه، نظارت بر سلامت و عملکرد دستگاه‌های سخت‌افزاری دارای اهمیت است. برای درک جزئیات سلامت سخت‌افزاری، چندین معیار وجود دارد که باید نظارت شوند. برخی از معیارهای مهم و دلیل نیاز به نظارت فهرست شده‌اند:

➤ **CPU:** وظایف یک دستگاه به وسیله CPU مدیریت می‌شوند. در صورتی که مصرف CPU به مقدار بیشینه خود برسد، به کارایی دستگاه آسیب وارد خواهد شد.

➤ **دما:** در زمان اجرای وظایف، مصرف CPU دستگاه ممکن است افزایش یابد که به نوبه خود منجر به افزایش دما خواهد شد. رشد سریع دما می‌تواند باعث خرابی یا اختلال در عملکرد یک دستگاه و در نهایت ایجاد قطعی در شبکه شود.

➤ **وضعیت منبع تغذیه:** یک منبع تغذیه معیوب یا افزایش ناگهانی شدت جریان در یک دستگاه، باعث خرابی آن و در نهایت موجب وقوع زمان خاموشی خواهد شد. نظارت با هشدارهایی بر اساس آستانه، به یک ادمین کمک می‌کند تا مشکلات بالقوه را بیابد.

در ادامه، دو ابزار مانیتورینگ رایج و قدرتمند SolarWinds و Zabbix معرفی و ویژگی‌ها و امکانات هر یک بیان شده است. ابتدا به شرح ابزار مانیتورینگ شبکه SolarWinds پرداخته شده است.

بخش ششم: آموزش مانیتورینگ شبکه با SolarWinds

ابتدا به شرح چيستی SolarWinds و برنامه مانیتورینگ شبکه آن (NPM) پرداخته و سپس هر یک از عناصر و امکانات این محصول مورد بررسی قرار خواهد گرفت.



SolarWinds چیست ؟

SolarWinds یکی از تولید کنندگان پیشرو نرم افزارهای مدیریت IT در جهان به حساب می آید. دیده بان عملکرد شبکه SolarWinds یا Network Performance Monitor (NPM)، محصول کلیدی و شاخص SolarWinds به حساب می آید. این سیستم می تواند پایش سلامت دستگاه های متصل به شبکه را عهده دار شود. این محصول، یک ابزار مانیتورینگ عملکرد شبکه فراگیر است که می تواند بر وضعیت دستگاه های شبکه از طریق پروتکل SNMP نظارت داشته باشد.

SolarWinds می تواند به صورت خودکار دستگاه های متصل به شبکه را کشف کند. از طریق داشبورد SolarWinds می توان در دسترس بودن و کارایی دستگاه های متصل به شبکه را در یک چشم انداز همه جانبه تحت نظارت قرار داد. در داشبورد SolarWinds هر دستگاه، اپلیکیشن یا خدمات کشف شده را می توان روی یک نقشه ساختاری ملاحظه کرد. همچنین، در این نقشه می توان نحوه ارتباط زیرساخت ها با یکدیگر را دید. قابلیت NetPath در SolarWinds امکان ردیابی انتقال های بسته را به صورت گام به گام فراهم می کند. این کار می تواند به طور موثرتری به تشخیص منشأ ایرادهای عملکردی شبکه کمک کند.

پلتفرم SolarWinds Orion چیست ؟

SolarWinds طیف وسیعی از سیستم‌های مدیریت زیرساخت را تولید می‌کند که همه آن‌ها، از جمله مدیریت عملکرد شبکه (NPM) روی پلتفرم مشترکی به نام Orion توسعه داده شده‌اند. در صورتی که همه نرم‌افزارهای مبتنی بر Orion با هم خریداری شوند، این نرم‌افزارها به واسطه تعدادی نقاط مبادله داده و ماژول‌های مشترک با یکدیگر به صورت هماهنگ کار خواهند کرد.

پلتفرم Orion یک برنامه کاربردی مدیریت عملکرد پهنای باند و مدیریت خطا است که امکان دیدن اطلاعات آماری شبکه را مستقیماً از مرورگر وب فراهم می‌سازد.

SolarWinds بر چه دستگاه‌هایی نظارت می‌کند؟

سخت‌افزارهایی که محصول SolarWinds NPM بر آن‌ها نظارت می‌کند، شامل موارد زیر است:

- روترها و سوئیچ‌ها
- ترمینال‌ها
- کامپیوترهای رومیزی
- دستگاه‌های همراه
- تجهیزات دفتر کار نظیر پرینترها

در ادامه، امکانات مختلف SolarWinds NPM معرفی شده‌اند.

امکانات SolarWinds NPM چیست ؟

سیستم هشداردهی سفارشی امکان تنظیم شرط‌های اجرای هشدار را فراهم می‌کند. در صورتی که شرط اجرای هشدار برقرار شود، نرم‌افزار SolarWinds اعلانی از طریق ایمیل یا پیامک ارسال می‌کند تا رخداد یک رویداد را اطلاع‌رسانی کند. کاربر می‌تواند با مراجعه به صفحه هشدارهای فعال، فهرست جامعی از هشدارها را بر اساس میزان شدت آن‌ها مشاهده کند.

دیده‌بان عملکرد شبکه SolarWinds به واسطه مجموعه ویژگی‌ها و امکانات متنوع، یکی از بهترین سیستم‌های نظارت بر شبکه به شمار می‌رود. SolarWinds می‌تواند به راحتی بین نظارت SNMP و تحلیل بسته چرخش کند. به این ترتیب، می‌توان تعیین کرد که کدام بخش‌های شبکه تحت نظارت قرار بگیرند. به طور کلی، ویژگی‌ها، قابلیت‌ها و امکانات کلیدی SolarWinds به شرح زیر است:

➤ مانیتورینگ SNMP

➤ شناسایی خودکار دستگاه‌های متصل به شبکه

➤ تحلیل بسته‌های شبکه

➤ نقشه‌های شبکه هوشمند با NetPath

➤ ایجاد نقشه‌های حرارتی Wifi

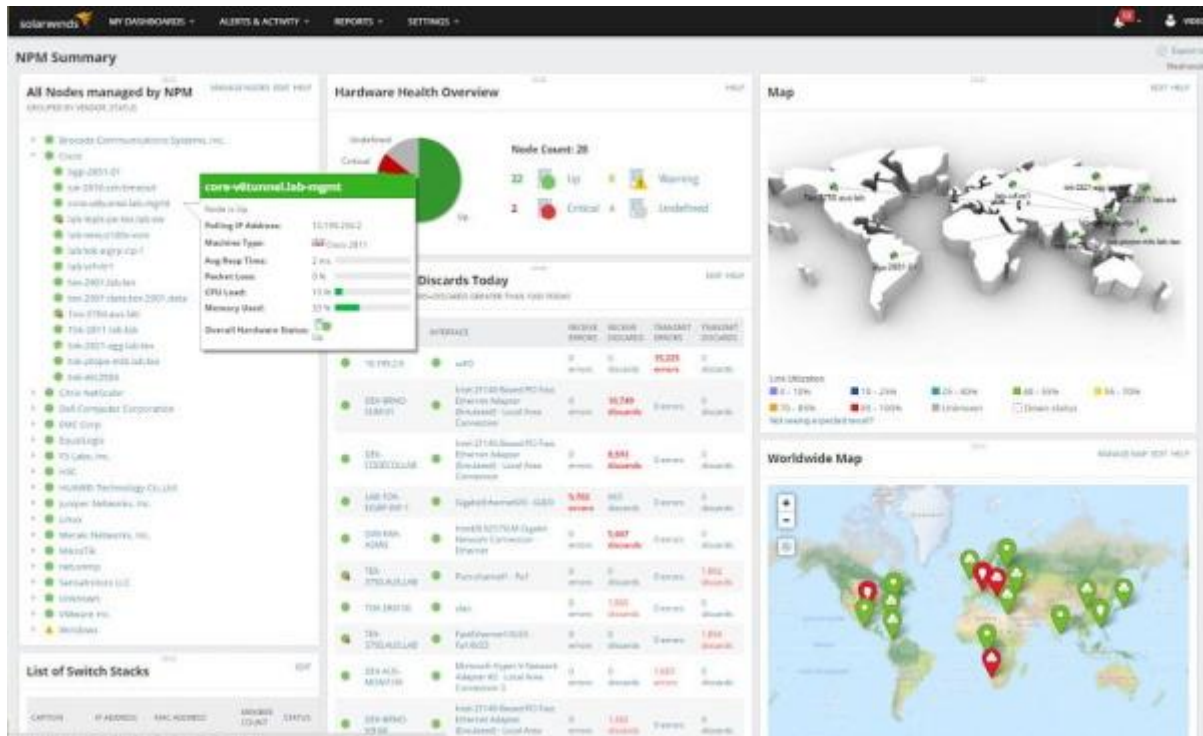
➤ سیستم‌های هشداردهی

➤ سیستم‌های گزارش‌گیری

همان‌طور که بیان شد، رویکرد دیده‌بان عملکرد شبکه سولارویندز بر پایه پروتکل نظارت ساده شبکه (SNMP) شکل می‌گیرد. یک استاندارد صنعت شبکه است که نیاز به نصب یک برنامه عامل روی هر دستگاه دارد. هر دستگاهی که بتواند به شبکه متصل شود، از قبل یک عامل SNMP را به عنوان بخشی از میان‌افزار (Firmware) خود به صورت نصب شده خواهد داشت. به یک کنترل کننده مرکزی نیاز دارد و دیده‌بان عملکرد شبکه سولارویندز این قابلیت را فراهم می‌کند.

شناسایی خودکار شبکه با SolarWinds NPM

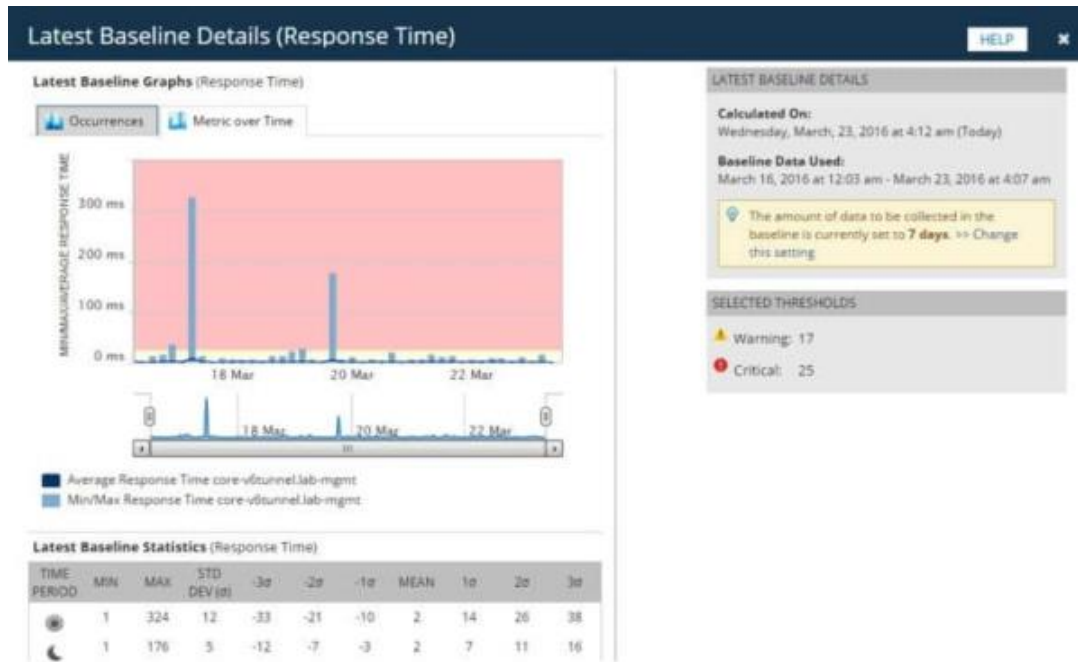
کنترلر SNMP با تمام عامل‌های نصب شده در دستگاه‌های شبکه ارتباط برقرار می‌کند. نیازی به راه‌اندازی و تنظیم سیستم به وسیله وارد کردن آدرس‌ها و نوع همه دستگاه‌ها وجود ندارد. زیرا سیستم SolarWinds NPM از پیام‌رسانی SNMP برای شناسایی تمام آن عامل‌ها استفاده خواهد کرد. سپس، شناسه‌های هر دستگاه در داشبورد نمایش داده خواهند شد.



صفحه اول داشبورد، داده‌های جمع‌آوری شده را نشان می‌دهد. اما علاوه بر آن، فهرست‌هایی از دستگاه‌ها با امکان ورود به جزئیات آن‌ها و آزمایش وضعیت فعلی هر گره قابل دسترسی است. عضویت شبکه به طور مرتب به‌روزرسانی می‌شود. بنابراین، در صورتی که دستگاهی اضافه یا حذف شود، نامش تغییر کند یا محلش تغییر داده شود، بدون هیچ‌گونه دخالت دست تغییرات در داده‌های NPM بازتاب داده خواهند شد.

مانیتورینگ دستگاه‌های شبکه با SolarWinds NPM

وظیفه اصلی SolarWinds NPM این است که برای جمع‌آوری اطلاعات پیرامون وضعیت تمام دستگاه‌هایی که تحت حمایت هستند، از عامل‌های SNMP استفاده کنند. این کارکرد جمع‌آوری داده و جمع‌بندی، هدف اصلی نظارت بر عملکرد شبکه به حساب می‌آید. اطلاعات به راحتی از طریق یک داشبورد قابل دسترسی هستند. در داشبورد، برای برجسته‌سازی و مشخص کردن وضعیت تجهیزات شبکه، از عناصر گرافیکی و کدگذاری رنگی استفاده می‌شود.



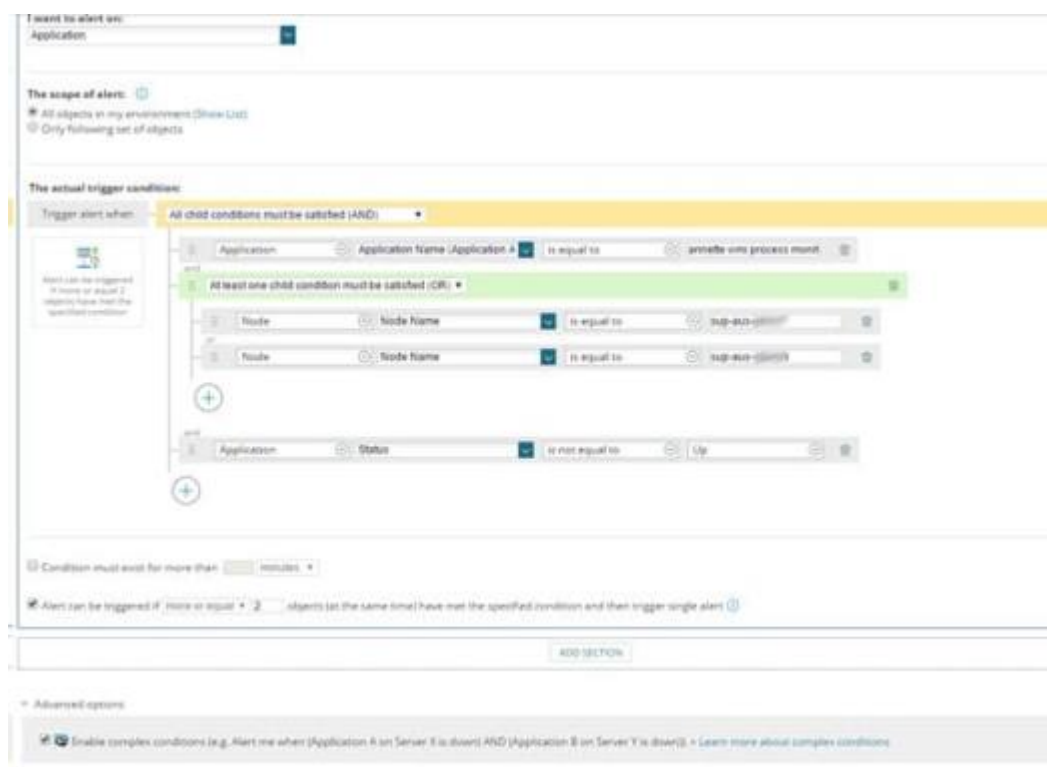
قابلیت مانیتورینگ شبکه با SolarWinds NPM دارای امکانات زیر است:

- تنظیم شرایط هشدار
- قابلیت تحلیل عملکرد
- گزارش گیری و به اشتراک گذاری داده
- پشتیبانی از چندین برند
- نمونه برداری وایرلس
- مانیتورینگ محیط مجازی

تنظیم شرایط هشدار با SolarWinds NPM

یکی از قابلیت های کلیدی عامل های SNMP ، توانایی آن ها در نادیده گرفتن حالت گزارش گیری انفعالی و ارسال یک پیام «دام» در زمان وقوع تغییر وضعیت بین درخواست های اطلاعات از جانب کنترلر است. برنامه SolarWinds NPM این هشدارها را بلافاصله در داشبورد نمایش می دهد. می توان وضعیت کلی شبکه را به عنوان یکی از هشدارهای سفارشی تنظیم کرد.

تنظیم محدودیت‌های خط مشی برای ایجاد اخطارهایی که تنها جلسات دام SNMP را گزارش می‌دهند، ساده است. این قابلیت در SolarWinds NPM، امکان تصفیه هشدارهای تغییر حالت غیر ضروری را نیز فراهم می‌کند. تصفیه تغییر حالت‌های غیر ضروری، برای جلوگیری از شلوغی و ازدیاد پیام‌های نگهداری و تعمیرات، مانند اخطارهای کمبود پودر چاپ پرینترها، انجام می‌شود. بدین صورت، می‌توان نارسایی‌های ضروری واقعی را شناسایی کرد و به سرعت وارد عمل شد.



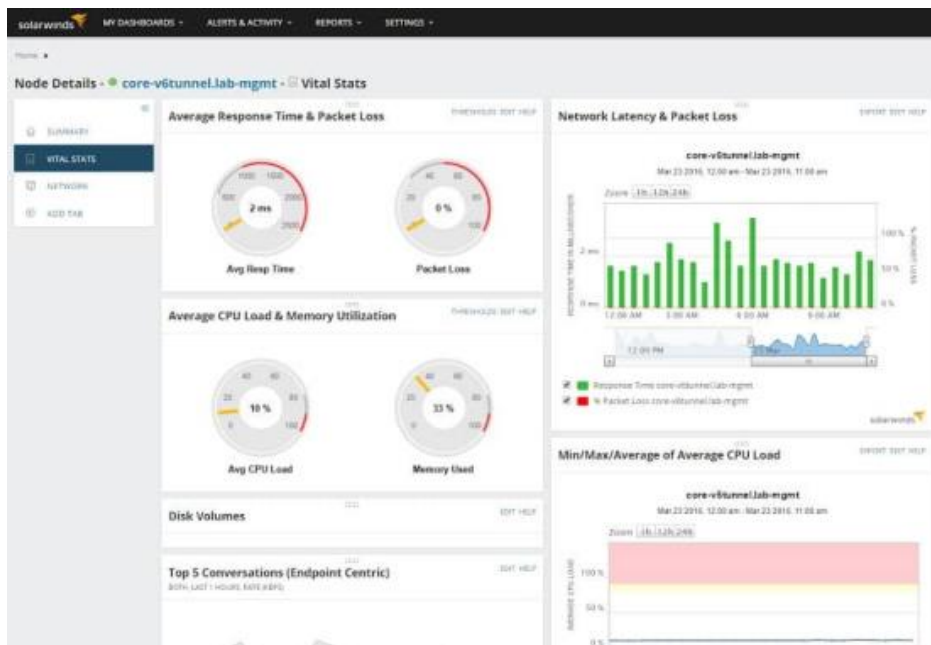
رفتار هشدارها در SolarWinds NPM قابل تصفیه و طبقه‌بندی است تا اینکه هشدارهای غیراضطراری بتوانند به فایل‌های ثبت وقایع (Log) بروند. اگرچه، این بدان معنا نیست که از هشدارهای نسبتاً جزئی غفلت شده است؛ زیرا می‌توان ترکیبی از شرایطی که ممکن است منجر به یک مشکل جدی شود را مشخص و تعیین کرد. داشبورد امکان اجرای برنامه‌های خارجی را در زمان رخداد شرایط یک هشدار خاص فراهم می‌کند. همچنین، می‌توان حساب‌های ایمیلی را برگزید که باید در خصوص هشدار مربوطه باخبر شوند و همچنین این اعلان‌ها قابل ارسال از طریق پیامک نیز هستند.

این قابلیت‌ها در SolarWinds NPM امکان خودکارسازی برخی از واکنش‌ها و همچنین هدایت اطلاعات به مسئولین دستگاه‌های مربوطه را فراهم می‌کنند. بنابراین، در صورتی که توافق ارائه خدمات با یک طرف خارجی وجود داشته باشد، می‌توان تنظیمات را به گونه‌ای انجام داده که یک اعلان خرابی تجهیزات به واحد Help Desk آن شرکت ارسال شود. این کار باعث جلوگیری از تماس گرفتن و انتظار در صف مکالمه و در نتیجه، صرفه‌جویی در زمان خواهد شد.

قابلیت تحلیل عملکرد در SolarWinds NPM

یکی از خدمات کلیدی در یک بسته مانیتورینگ شبکه، اطلاع‌رسانی در خصوص نارسایی‌های بالقوه پیش از وقوع آن‌ها است. اگرچه، مانیتورینگ عملکرد شبکه SolarWinds در پشتیبانی از عیب‌یابی و تلاش برای جلوگیری از نارسایی سیستم یک گام فراتر می‌رود. برخی از ابزارهای شبکه می‌توانند در شناسایی یک منبع بالقوه از اطلاعات با اهمیت به مدیران شبکه کمک کنند.

جمع‌آوری داده‌ها از گره‌های مختلف در شبکه جهت تحلیل آن‌ها می‌تواند کار پیچیده‌ای باشد. اغلب برای اینکه بتوان تصویر واضح‌تری از تاثیر وضعیت و میزان آسیب‌دیدگی به دست آورد، باید به وارد کردن داده‌ها در یک صفحه حسابرسی متکی شد.



قابلیت‌ها و ویژگی‌های تحلیل عملکرد NPM SolarWinds امکان جمع‌آوری داده از گره‌های مختلف و دیدن انواع مختلف داده‌ها در کنار یکدیگر را فراهم می‌کند. با کارکرد Drag and Drop امکان گردآوری گزارش‌های عملکردی برای دیدن آن‌ها در کنار هم و مشاهده داده‌های لحظه‌ای یا داده‌های قدیمی وجود دارد. ابزارهای (ویجت) نمایش تصویری نمودارها، وقتی که منابع داده در یک خط زمانی مشترک مورد هدف قرار می‌گیرند، ردیابی تاثیر عملکرد را آسان می‌کنند.

نتیجه تحلیل را می‌توان به نمایشگر بازگرداند. زیرا وقتی اطلاعات عملکردی بهتری از تجزیه تحلیل‌ها جمع‌آوری شوند، امکان پالایش خط مشی‌های هشدارهای وضعیتی وجود خواهد داشت.

گزارش‌گیری و به اشتراک‌گذاری داده در NPM

قابلیت‌های تحلیل و بصری‌سازی داده در داشبورد NPM SolarWinds ابزارهای عالی برای شناسایی مشکلات عملکردی محسوب می‌شوند. امکانات گزارش‌گیری سیستم، امکان عکس گرفتن از داده‌های لحظه‌ای، تجمیع منابع و نمایش تحلیلی از داده‌های تاریخی (گذشته) را فراهم می‌کنند.

Node SLA report - business hours



Summary of Orion Objects: Datasource 1

Custom Table for Datasource 1

Ordered by sla_day - Descending

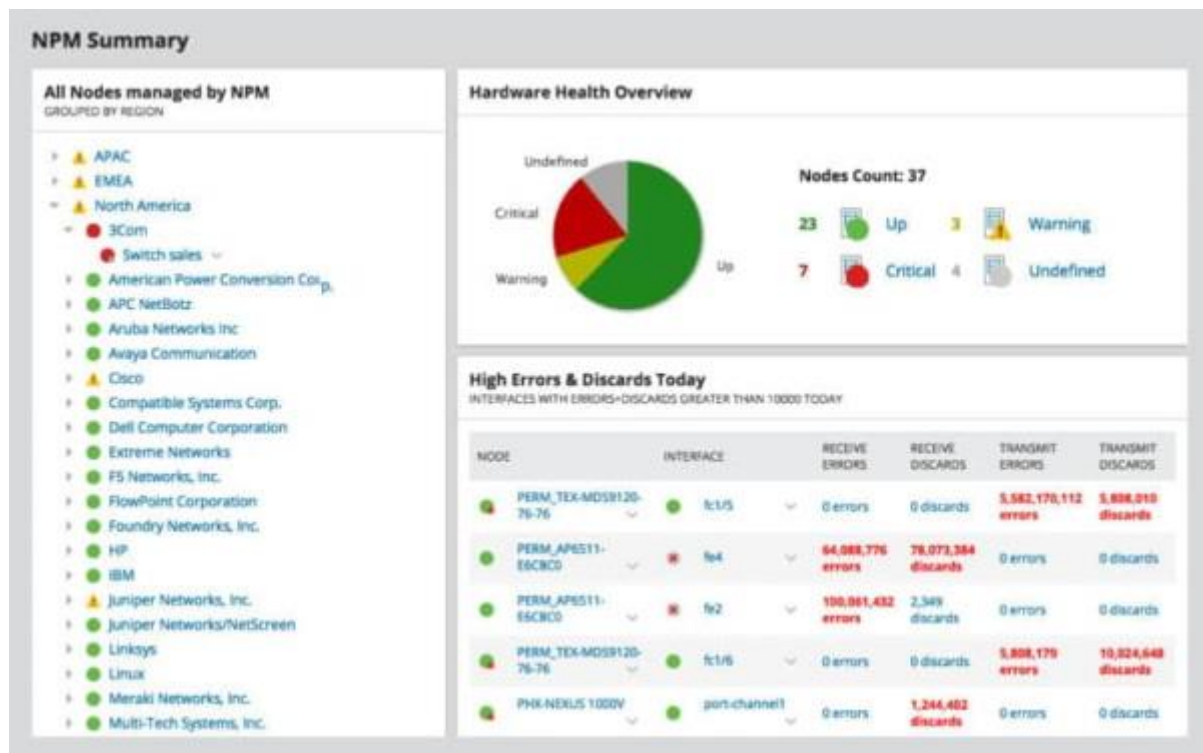
CAPTION	SLA_AVAILABILITY	SLA_DAY	TIME_FROM	TIME_TO
Network 10.10.10.10	100	10/18/2016 12:00:00 AM	7	15
Network 10.10.10.11	100	10/18/2016 12:00:00 AM	8	16
Network 10.10.10.12	100	10/18/2016 12:00:00 AM	8	16
Network 10.10.10.13	100	10/18/2016 12:00:00 AM	8	16
Link 10.10.10.14	100	10/18/2016 12:00:00 AM	7	15
Network 10.10.10.15	100	10/18/2016 12:00:00 AM	7	15
Network 10.10.10.16	100	10/18/2016 12:00:00 AM	8	16
Link 10.10.10.17	100	10/18/2016 12:00:00 AM	7	15
Link 10.10.10.18	0	10/18/2016 12:00:00 AM	8	16
Link 10.10.10.19	100	10/18/2016 12:00:00 AM	7	15
Link 10.10.10.20	100	10/18/2016 12:00:00 AM	8	16
Link 10.10.10.21	100	10/17/2016 12:00:00 AM	7	15
Link 10.10.10.22	100	10/17/2016 12:00:00 AM	7	15
Link 10.10.10.23	100	10/17/2016 12:00:00 AM	8	16

این خروجی می‌تواند به صورت یک قالب قابل توزیع تحویل داده شود تا امکان نمایش رسیدن به مقاصد، ارائه گزارش از عملکرد گروه و بررسی اهداف SLA وجود داشته باشد. مازولی به نام PerfStack ،

یک آدرس URL را از نماهای داده گردآوری شده ایجاد می‌کند که می‌توان آن را با هدف استفاده در بحث‌ها و همکاری‌ها به سایر گروه‌های ذینفع ایمیل کرد.

پشتیبانی از چند برند در NPM SolarWinds

احتمال اینکه تجهیزات شبکه توسط تولید کننده‌ها و فروشنده‌های مختلفی تامین شده باشد، زیاد است. جهان شمول بودن ساختار پروتکل SNMP در SolarWinds NPM که توسط مانیتورینگ عملکرد شبکه استفاده می‌شود، بر مشکل ناسازگاری و عدم همخوانی نرم‌افزاری غلبه می‌کند.



اگرچه، نرم‌افزار مانیتورینگ و داشبورد تنها قابلیت نصب در ویندوز را دارند، درنظر داشتن نوع سیستم‌عامل و ثابت‌افزار (Firmware) دستگاهی که قصد نظارت بر آن وجود دارد، ضرورتی ندارد. سیستم نظارتی می‌تواند فارق از اینکه آیا سیستم‌عامل زیربنایی از دستگاه‌های شبکه پشتیبانی می‌کند یا خیر، با عامل‌های SNMP ارتباط برقرار کند.

نمونه برداری وایرلس در SolarWinds NPM

ابزار مانیتورینگ SolarWinds NPM تنها به نظارت و مانیتورینگ در شبکه‌های محلی کابلی محدود نمی‌شود. قابلیت‌های این سیستم به شبکه‌های وایرلس و سیستم‌های ترکیبی (هیبریدی) نیز گسترش می‌یابد. ابزار مانیتورینگ SolarWinds NPM می‌تواند بر قدرت سیگنال وایرلس نظارت داشته باشد و نقاط کور را شناسایی کند. داشبورد وایرلس شامل بصری‌سازی عالی است که رد پای سیگنال تجهیزات وایفای را نمایش می‌دهد. این اطلاعات امکان تصمیم‌گیری درباره محل فیزیکی روترها و تقویت کننده‌های وایرلس را فراهم می‌کنند.

Wireless Summary View

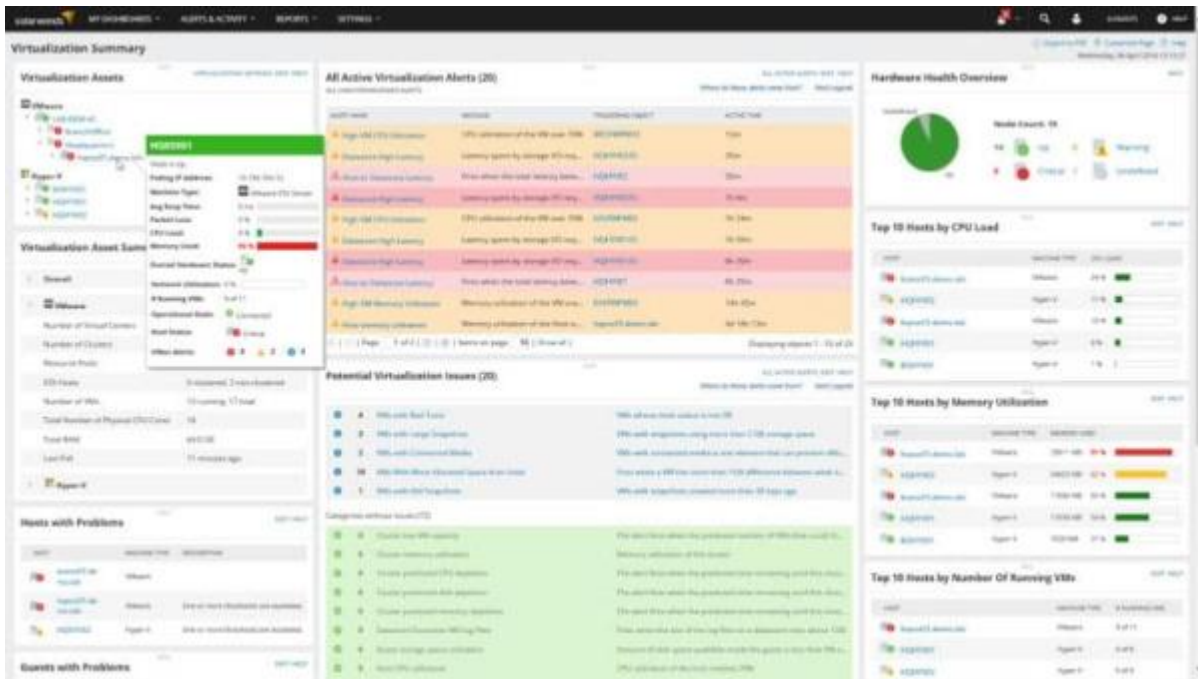
Show: Access Points SEARCH

Group by:	Access Point	IP Address	Type	SSIDs	Channels
Location					
[Unknown] (1)	OMSEAAP102	10.199.17.89	Thin		6, 44
Cairo (6)	OMSEAAP502	10.199.17.88	Thin		6, 44
Indianapolis, IN (12)	zf7363 - 06C4017	10.199.17.90	Thin		1, 132
L 30 (1)	zf7363 - 06C4017	10.199.17.91	Thin		10, 132
Seattle - 201 5th (14)					
Sydney (8)					
Texas (8)					
Tokyo (11)					
	Client Name	SSID	IP Address	MAC Address	
	vprice	lab	10.199.17.184	C4017C057620	
	mprice	lab	10.199.17.19	001B207F5216	
	zf7363 - 06C4017	10.199.17.92	Thin		6, 161
	zf7363 - 06C4017	10.199.17.93	Thin		4, 48
	zf7363 - 06C4017	10.199.17.94	Thin		3, 56
	zf7363 - 06C4017	10.199.17.95	Thin		9, 44
	zf7363 - 06C4017	10.199.17.96	Thin		2, 104
	zf7363 - 06C4017	10.199.17.97	Thin		4, 153
	zf7363 - 06C410E	10.199.17.98	Thin		11, 64
	zf7363 - 06C410E	10.199.17.99	Thin		4, 56
	zf7363 - 06C410E	10.199.17.100	Thin		3, 44
	zf7363 - 06C410E	10.199.17.101	Thin	lab	44

Page 1 of 1 30

امکانات وایرلس در SolarWinds NPM مزیت بزرگی محسوب می‌شود، زیرا امکان شناسایی دستگاه‌های سرگردان (Rogue) در شبکه وجود دارد. این یک قابلیت امنیتی مهم است که امکان استفاده کارکنان از دستگاه‌های خودشان را در محل کار آسان‌تر می‌کند. محیط BYOD نیازمند کاربرد خط مشی‌های متنوع برای تعیین نوع دستگاه‌ها و دسترسی گروهی است. SolarWinds NPM این قابلیت‌ها را دارد.

مانیتورینگ محیط مجازی در NPM SolarWinds



در صورت استفاده از مجازی سازی در شبکه، می توان مانیتورینگ اجزای مجازی را نیز در NPM SolarWinds انجام داد. بخشی در داشبورد به محیط های مجازی اختصاص داده شده است که حتی خدمات ابری را نیز در بر می گیرد و این خدمات نیز مشمول فرآیند شناسایی شبکه می شوند

تحلیل NetPath با NPM SolarWinds

قابلیت تجزیه-تحلیل مسیر شبکه (Network Path | NetPath) در NPM SolarWinds یک بازنمایی بصری از ساختار (توپولوژی) شبکه ارائه می دهد. الزامی در استفاده از طرح بندی NetPath در داشبورد وجود ندارد، زیرا به صورت خودکار در طول فرآیند اکتشاف شبکه آماده سازی می شود.

نقشه شبکه حجم ترافیک را در هر اتصال و در طول کل مسیر نمایش می دهد. نقشه شبکه شامل محیط های مجازی می شود و حتی جریان داده را از طریق اینترنت دنبال می کند تا مسیرهای دسترسی را به سرویس های ابری نشان دهد NetPath. شامل یک عنصر ردیابی مسیر (Traceroute) برای کمک به عیب یابی تاخیرهای ترافیکی است.



جریان‌های ترافیکی می‌تواند توسط کاربر، اپلیکیشن، پروتکل یا دستگاه نظارت شود. نقشه‌های شبکه به مشخص کردن تنگناها و خرابی‌های شبکه کمک می‌کنند. با این اطلاعات، می‌توان وظایف رفع مشکلات را به متخصصین گروه و ارائه دهندگان خدمات تخصصی محول کرد.

نیازمندی‌های سیستمی SolarWinds NPM چه هستند؟

باید به یاد داشت که نرم‌افزار SolarWinds NPM تنها روی ویندوز قابل نصب شدن است. بسته SolarWinds NPM دو سرویس ایجاد می‌کند که سرور اپلیکیشن و سرور پایگاه داده هستند. این دو بخش نباید روی یک دستگاه نصب شوند. با سطح بالاتری از قابلیت‌های نظارت بر عناصر، نیازهای سخت‌افزاری برای سیستم نیز افزایش پیدا می‌کنند. به این معنا که برای استفاده از ۲۰۰۰ NPM SL نیاز به کامپیوتر قوی‌تری نسبت به اجرا و استفاده از ۱۰۰ NPM SL وجود دارد. برای هر دو عنصر سیستم، نیاز به استفاده از ویندوز سرور ۲۰۱۲ یا ویندوز سرور ۲۰۱۶ وجود دارد.

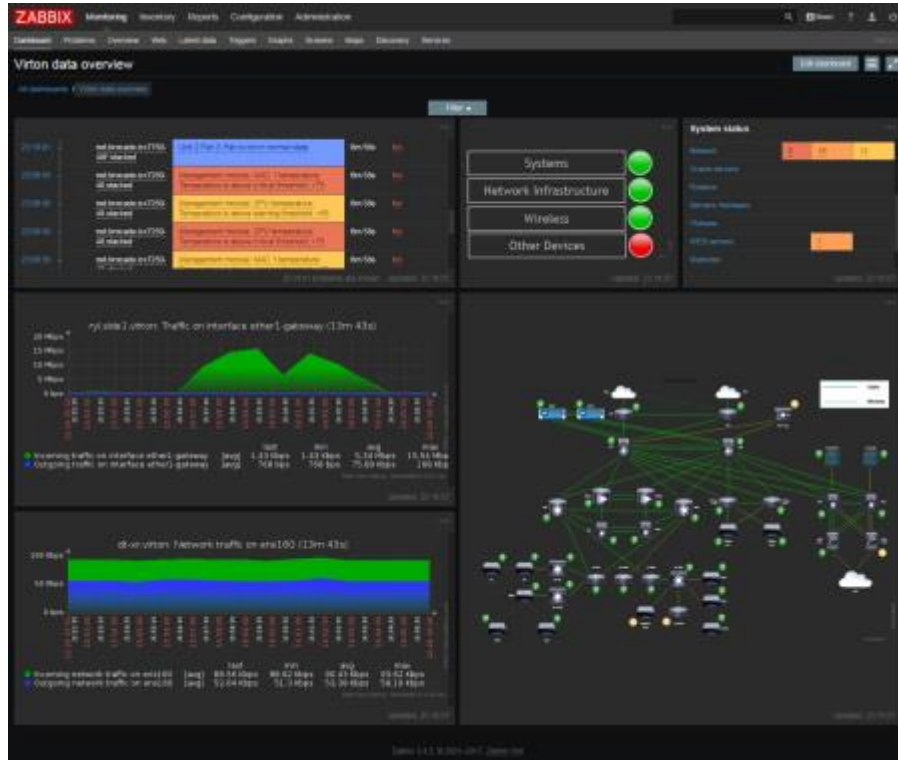
محیط پایگاه داده نیز باید مبتنی بر Microsoft SQL Server نسخه ۲۰۱۲، ۲۰۱۴ یا ۲۰۱۶ باشد. کامپیوتری که قصد انجام مانیتورینگ با آن وجود دارد، باید حداقل دارای پردازنده چهار هسته‌ای با سرعت ساعت ۲.۵ گیگاهرتز باشد. برای نسخه SLX، این سرعت باید حداقل به سرعت سه گیگاهرتز برسد. کامپیوتری که از پایگاه داده میزبانی می‌کند، باید یک پردازنده چهار هسته‌ای داشته باشد، اما نیازمند حداقل سرعت سه گیگاهرتز حتی برای NPM SL ۱۰۰ است. حافظه مورد نیاز برای کامپیوتر میزبان نرم‌افزار مانیتورینگ و میزبان پایگاه داده، برای هر یک از نسخه‌های SolarWinds NPM در جدول زیر قابل ملاحظه است.

نسخه	رم سرور پایگاه داده	رم سرور اپلیکیشن
NPM SL100	8 GB	6-8 GB
NPM SL250	8 GB	6-8 GB
NPM SL500	10 GB	8-10 GB
NPM SL2000	10-64 GB	10-16 GB
NPM SLX	64-128 GB	18-32 GB

در استفاده از تمام نسخه‌ها به دو هارد دیسک ۱۴۶ گیگابایت 15K نیاز است. کارت شبکه نیز باید حداقل سرعت یک گیگابیت را پشتیبانی کند.

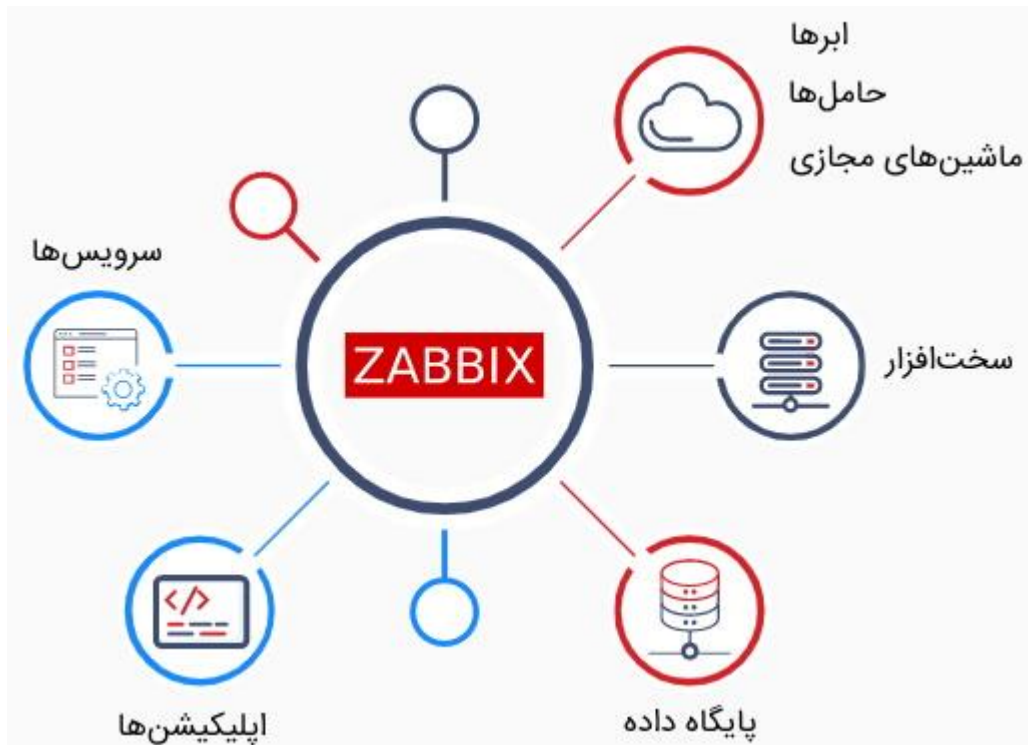
بخش هفتم: آموزش مانیتورینگ شبکه با ZABBIX

ابتدا به طور مختصر به این سوال پاسخ داده شده است که Zabbix چیست؟



Zabbix چیست ؟

Zabbix یک ابزار مانیتورینگ ساخته شده توسط شرکت Zabbix SIA از کشور لیتوانی است .
در بسیاری از کشورها و صنایع گوناگون مورد استفاده قرار می‌گیرد.
استفاده از ابزار مانیتورینگ شبکه Zabbix در کشور ژاپن بسیار همه‌گیر شده است. در ایران هم از راهکار Zabbix به میزان زیادی استفاده می‌شود.

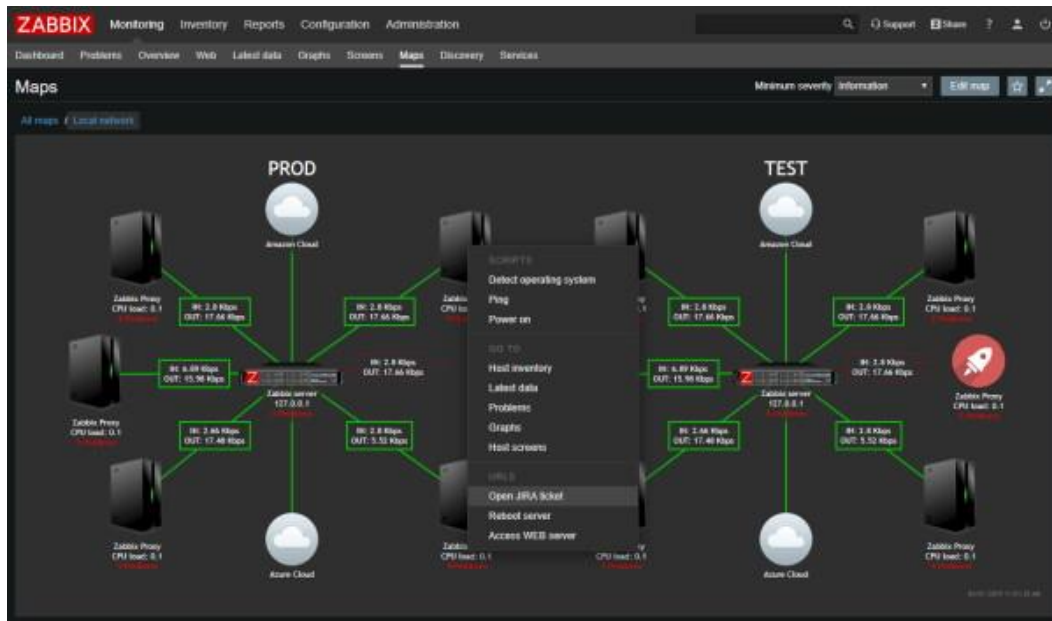


Zabbix چه ویژگی‌هایی دارد؟

ویژگی‌های ابزار مانیتورینگ شبکه Zabbix در ادامه فهرست شده‌اند:

- Zabbix به عنوان یک نرم‌افزار متن‌باز توسعه داده شده است.
- Zabbix چندین روش مانیتورینگ شبکه را ارائه می‌دهد. این روش‌ها به صورت زیر هستند:
- مانیتورینگ خارجی بدون عامل مثل مانیتورینگ با *TCP*، *SNMP*، *SSH* و *PING*
- مانیتورینگ عامل داخلی با پشتیبانی از سیستم‌عامل‌های مختلف
- مجموعه داده‌های محاسبه شده و تجمعی
- مانیتورینگ ماشین‌های مجازی
- مانیتورینگ خودکار
- جمع و حذف خودکار اقلام مانیتورینگ

- مانیتورینگ ماشین‌های مجازی و حامل‌ها
- افزودن خودکار نظارت با عامل مانیتورینگ
- پیکربندی بسیار انعطاف‌پذیر از تعریف شناسایی مشکل
- جمع‌آوری ماتریسی و تشخیص خودکار وضعیت ایرادات
- تنظیم سطح سختی
- پیش‌بینی روند
- مانیتورینگ چندین میزبان با داشبورد
- نمایش پیشرفته گراف
- اعمال پیشرفته در حین بروز مشکل
- تشدید پیام
- بازیابی خودکار ایرادات
- مانیتورینگ توزیع شده
- مانیتورینگ داده‌های چندین هزار اقلام نظارتی
- مانیتورینگ فایروال و فراتر از DMZ
- مانیتورینگ ایمن
- رمزگذاری مسیر ارتباطی داده‌های مانیتورینگ
- تفکیک نظارت بر امتیازات کاربر
- احراز هویت کاربر با استفاده از *ActiveDirectory* و *OpenLDAP*



معماری Zabbix

Zabbix از اجزای زیر تشکیل شده است:

- **سرور Zabbix:** کارکردهای مانیتورینگ مرکزی Zabbix را فراهم می‌کند. مانیتورینگ را اجرا می‌کند، پیکربندی و داده‌های مانیتورینگ را در پایگاه داده‌ها ذخیره می‌کند
- **وب سرور Zabbix:** رابط کاربری تحت وب برای تنظیم و نمایش داده‌های مانیتورینگ Zabbix
- **سرور پروکسی Zabbix:** سرورها در محل‌های ناواضح شبکه توزیع می‌شوند. انجام مانیتورینگ به جای سرور Zabbix و تبادل پیکربندی مانیتورینگ و داده‌های نظارتی با سرور Zabbix
- **عامل Zabbix یا Zabbix Agent:** عاملی که در هدف تحت نظارت عمل می‌کند و داده‌های مانیتورینگ هدف را به سرور Zabbix ارسال می‌کند.

سرور Zabbix و وب سرور Zabbix ممکن است در یک محل مستقر شوند. اگرچه، به دلیل اینکه آن‌ها فقط باید از پایگاه داده یکسانی استفاده کنند، استفاده از سروهای Zabbix متفاوت، چندان اهمیتی ندارد. سرور پروکسی Zabbix برای نظارت از طریق یک فایروال مورد استفاده قرار می‌گیرد. همچنین، از سرور پروکسی Zabbix برای توزیع بار مانیتورینگ استفاده می‌شود.

مانیتورینگ خارجی و داخلی در Zabbix

مانیتورینگ شبکه در Zabbix شامل مانیتورینگ خارجی اهداف و مانیتورینگ داخلی آن‌ها است. مانیتورینگ خارجی به معنی خدمات مانیتورینگ از خارج است. مانیتورینگ خارجی مشابه آزمون جعبه سیاه است که در آن هدف تحت نظارت به صورت یک جعبه در نظر گرفته می‌شود که محتویات داخلش قابل مشاهده نیست. در این حالت، مانیتورینگ نزدیک به خط دید کاربر اتفاق می‌افتد.

به عنوان مثال در مورد مانیتورینگ خدمات وب، اقلام مانیتورینگ شامل این هستند که آیا کاربر می‌تواند به وب دسترسی داشته باشد یا وارد حساب کاربری خود شود یا اینکه آیا صفحات وب به شکل مورد انتظار نمایش داده می‌شوند؟ از طرف دیگر، مانیتورینگ داخلی را می‌توان مثل یک آزمایش جعبه شفاف در نظر گرفت. با هدف تحت نظارت به عنوان جعبه‌ای رفتار می‌شود که محتوایش قابل مشاهده است. به عنوان مثال، در خصوص نظارت سرویس وب، اقلام مانیتورینگ شامل موارد زیر است:

➤ آیا سرویس‌های لازم در حال اجرا هستند؟

➤ آیا شبکه در حال اجرا است؟

➤ آیا بار CPU، حافظه، محل ذخیره و شبکه زیاد است؟

➤ آیا دسترسی غیرمجاز از خارج اتفاق افتاده است؟

برای مانیتورینگ خارجی، Zabbix نه تنها می‌تواند مانیتورینگ Ping یا همان ICMP را انجام دهد، بلکه حتی از نظارت بر وضعیت ورود به حساب کاربری مبتنی بر سناریو وب نیز پشتیبانی می‌کند. مانیتورینگ داخلی به وسیله برنامه‌ای به نام **عامل Zabbix** انجام می‌شود. برنامه عامل یا Agent در داخل ماشین اجرا می‌شود. وضعیت سرویس‌ها، پردازش‌ها و بار ماشین توسط عامل Zabbix قابل نظارت و مانیتورینگ است. در خصوص تجهیزات شبکه‌ای که عامل Zabbix برای آن‌ها قابل اجرا نیست، می‌توان تجهیزات را با استفاده از پروتکل SNMP مانیتور کرد.

مانیتورینگ داخلی و مانیتورینگ خارجی هر دو به یک اندازه اهمیت دارند و برای تداوم ارائه خدمات ضروری هستند Zabbix. می‌تواند هر دو نوع مانیتورینگ خارجی و داخلی را انجام دهد Zabbix. یک ابزار مانیتورینگ یکپارچه است که می‌تواند مدیریت تاریخچه و پیکربندی را انجام دهد.

مانیتورینگ خارجی با Zabbix

مانیتورینگ خارجی نظارت بر یک آیتم (یا همان شی) به عنوان یک جعبه سیاه است.

به طور کلی، Zabbix اقلام زیر را مانیتور می‌کند:

- **مانیتورینگ خدمات:** نظارت می‌کند که آیا سرویس‌هایی نظیر *SMTP*، *HTTP* و *SSH* در حال اجرا هستند؟
- **مانیتورینگ TCP/UDP:** نظارت می‌کند که آیا پورت سرویس *TCP/UDP* برای آدرس *IP* تعیین شده باز است؟
- **مانیتورینگ با Ping یا ICMP:** نظارت می‌کند که آیا ارتباط شبکه با یک آدرس *IP* خاص برقرار است؟
- **مانیتورینگ با SNMP:** بر تجهیزات شبکه، تجهیزات منابع تغذیه و تجهیزات سرور نظارت می‌شود.

SNMP واقعاً مانیتورینگ خارجی نیست؛ بلکه، مانیتورینگ به وسیله برقراری ارتباط با ماژول داخلی *SNMP* است. با این حال، این روش اغلب برای نظارت بر تجهیزات شبکه‌ای نظیر سوئیچ‌های لایه دو، سوئیچ‌های لایه سه و متعادل کننده بار به کار گرفته می‌شود. به همین دلیل، اغلب با مانیتورینگ *SNMP* به عنوان یک روش مانیتورینگ خارجی برخورد می‌شود.

در واقع، Zabbix به این دلیل پروتکل *SNMP* را مانیتورینگ خارجی در نظر می‌گیرد که از عامل Zabbix برای مانیتورینگ در آن استفاده نمی‌شود. نظارت خارجی در محدوده‌های نزدیک به کاربر نهایی بسیار مهم است. در صورت امکان، باید ارائه دهنده شبکه و ارائه دهنده سرویس ابری را جداسازی کرد. در صورتی که نظارت بر سرویس *HTTP* انجام می‌شود، باید نظارت موارد زیر را انجام داد:

- متصل بودن کاربر با پروتکل *HTTP*
- صحت اطلاعات *TLS*
- آیا محتوای حاصله همان چیزی است که انتظار می‌رود؟
- تست ورود به حساب کاربری (در صورتی که سرویس *HTTP* نیاز به *login* داشته باشد)

تنها ارائه دهنده سرویس است که می‌تواند قضاوت درستی از این مسئله داشته باشد که چه چیزی به شکل عادی کار می‌کند و چه چیزی به طور عادی کار نمی‌کند. با قرار دادن سرور مانیتورینگ در یک

شبکه خارجی، کاربر می‌تواند از Zabbix برای نظارت بر سرویس‌هایی نظیر SMTP ، HTTP و SSH استفاده کند. همچنین، Zabbix دسترسی شبکه را با اقلام نظارتی مانند پورت سرویس TCP ، پروتکل ICMP و SNMP نظارت می‌کند. علاوه بر آن، امکان تایید ورود به حساب و کسب محتوا مطابق با سناریوهای کاربر امکان‌پذیر است.

علاوه بر بخش مربوط به کاربر نهایی، همچنین لازم است تا شبکه در داخل یک سرویس و اتصالات سرویس (مثل اتصال پایگاه داده) بین سرورها نیز نظارت شود. به خصوص، در صورتی که تاثیر یک پایگاه داده از کار افتاده بسیار زیاد باشد، باید جدول‌هایی را برای سرویس‌های مانیتورینگ آماده کرد تا مشخص شود که آیا عملیات خواندن/نوشتن برای برخی از جدول‌های خاص قابل انجام هست یا خیر؟

مانیتورینگ داخلی با Zabbix

در مانیتورینگ داخلی، کاربر باید عامل Zabbix را در سرور مانیتورینگ هدف، نصب و اجازه ارتباط با سرور Zabbix را صادر کند. سرور Zabbix پردازش‌های مانیتورینگ مرکزی را اجرا می‌کند. معمولاً، برای دریافت اطلاعات مانیتورینگ اتصال از سرور به عامل برقرار می‌شود.

جمع‌بندی فصل اول

ابتدا به طور کامل به شرح چستی مانیتورینگ شبکه پرداخته شد. سپس مباحث و مفاهیم مقدماتی شبکه‌های کامپیوتری شامل مهارت‌ها و دانش عمومی شبکه‌های کامپیوتری، مدل OSI ، دستگاه‌های رایج شبکه، نحوه انتقال داده‌ها در شبکه و سایر موارد مورد نیاز برای آموزش مانیتورینگ شبکه شرح داده شدند. در ادامه نیز مفاهیم اساسی مانیتورینگ شبکه از جمله ضرورت مانیتورینگ، توافق SLA، اجزای عمومی مانیتورینگ در ویندوز، روش‌ها و پروتکل‌های کلی مانیتورینگ شبکه و بسیاری از مطالب دیگر بیان شدند.

در انتهای نیز به شرح نکات مهمی پیرامون دو تا از ابزارهای مهم و رایج مانیتورینگ شبکه شامل SolarWinds NPM و Zabbix پرداخته شد.

فصل دوم: تلفن تحت شبکه VoIP - سخت افزار و نرم افزار

از جمله فناوری‌هایی که تاکنون در زمینه ارتباطات تلفنی ارائه شده، سیستم ویپ (VoIP) بهترین گزینه است. این فناوری امکان برقراری تماس صوتی را از طریق وسایل الکترونیکی نظیر لپ تاپ و کامپیوتر، گوشی هوشمند و تلفن تحت شبکه VoIP و برخی از مرورگرها فراهم می‌آورد. به همین دلیل ممکن است سوال بسیاری از افراد این باشد که ویپ VoIP چیست و چه کاربردی دارد. از آنجایی که پیش زمینه موفقیت یک کسب و کار ارتباط مطمئن و اصولی است، استفاده از جدیدترین و بهترین امکانات نیز ضرورت پیدا می‌کند. بدیهی است که پروتکل انتقال صدا در بستر اینترنت (VoIP) بهترین انتخاب ممکن در صنعت ارتباطات مدرن به شمار می‌رود.

راه اندازی تلفن اینترنتی برای کسب و کارهایی که به دنبال برقراری ارتباطات موثر با مشتریان خود هستند، واجب و ضروری است. تا چند سال گذشته کسی اصلاً تصور نمی‌کرد که تلفن‌هایی روی کار بیایند که بر مبنای اینترنت فعالیت کنند. در واقع ذهنیت هر فرد به استفاده از خطوط تلفن آنالوگ محدود می‌شد. با راه اندازی تلفن‌های ویپ این تصور به طور کلی از میان رفت. افراد متوجه شدند که می‌توان در بستر اینترنت نیز تماس برقرار کرد. هم اکنون تمامی افراد به خصوص افرادی که سازمان خاصی را اداره می‌کنند می‌توانند به اینترنت TD-LTE پر سرعت وصل شوند و از خدمات تلفن اینترنتی بهره مند گردند.

فصل اول: تعریف VOIP

تلفن تحت شبکه VoIP که مخفف عبارت "Voice over IP" است، نوعی تلفن برای انتقال صوت در بستر شبکه به شمار می‌آید. در حقیقت ویپ یک خط تلفن تحت شبکه به شمار می‌آید که دارای قابلیت‌های متعددی است. به کمک ویپ کاربران تنها با اتصال به شبکه می‌توانند با ارگان‌های داخلی یا حتی خارج از کشور تماس برقرار کنند. توجه داشته باشید که برای راه اندازی تلفن اینترنتی به تجهیزات چندانی نیاز ندارید. این سیستم‌ها به شما کمک می‌کنند تا مکالمات را ضبط کنید و بدون نیاز به سیم کشی از تلفن‌های ارتباطی استفاده کنید.

VoIP (Voice over Internet Protocol) فناوری است که تماس صوتی را از طریق اینترنت یا سایر شبکه‌های مبتنی بر IP امکان‌پذیر می‌کند. در سیستم ویپ، سیگنال‌های صوتی به بسته‌های دیجیتالی تبدیل می‌شوند و از طریق اینترنت یا سایر شبکه‌های مبتنی بر IP منتقل می‌شوند؛ در انتها به صورت سیگنال‌های صوتی به دست گیرنده می‌رسند.

به‌طور سنتی، سیگنال‌های صوتی در سیستم‌های تلفن قدیمی از طریق خطوط تلفن آنالوگ منتقل می‌شوند. از آن‌جاکه در این سیستم سیگنال‌ها از طریق خطوط تلفن جابه‌جا می‌شوند، برقراری تماس فقط با ایجاد سیم‌کشی مدار امکان‌پذیر می‌شود.

در تجهیزات سخت‌افزاری سیستم تلفن آنالوگ، از قطعه‌ای تخصصی به نام Private Branch Exchange (به اختصار PBX) استفاده می‌شود. این قطعه اتصال داخلی تلفن را به شبکه تلفن عمومی تعمیم و بسط می‌دهد.

امروزه، فناوری ویپ در میان اکثر افراد به جایگزین اصلی تماس‌های تلفنی سنتی تبدیل شده است و علاوه بر VoIP، با نام‌های دیگری همچون تلفن مجازی، سیستم تلفن آنالاین، سیستم تلفن مبتنی بر ابر، تلفن IP و ابزار تماس مجازی شناخته می‌شود. اگر به اینترنت پرسرعت و دستگاه هوشمند و ارائه‌دهنده خدمات ویپ دسترسی داشته باشید، از این طریق می‌توانید به راحتی با مخاطبانتان تماس بگیرید.

فصل دوم: شناخت و عملکرد VoIP، مزایا و معایب

مزایای VoIP

استفاده از نرم افزار ویپ (VoIP) مزایای زیادی برای کسب و کارها دارد. از جمله مهم‌ترین امکانات ویپ میتوان به مواردی مانند مکالمه چندنفره، ارسال و دریافت پیام‌های صوتی و متنی، امکان انتقال تماس‌ها، مدیریت تماس‌ها و ارتباطات گروهی اشاره نمود. در ادامه چند نمونه از بارزترین مزایای این فناوری را ادامه شرح می‌دهیم.

مقرون به صرفه بودن

هزینه عملیاتی، یکی از مهم‌ترین نکاتی است که هر کسب و کاری باید به آن توجه کند. VoIP از بسیاری جهات ارزان‌تر از سیستم‌های تلفن سنتی است. از آنجایی که VoIP از اینترنت یا سایر شبکه‌های مبتنی بر IP برای انتقال سیگنال‌های صوتی استفاده می‌کند، هیچ هزینه‌ای برای تماس‌های از راه دور یا بین‌المللی وجود ندارد و مشترک بودن زیرساخت ویپ با بستر شبکه مهم‌ترین دلیل هزینه پایین استفاده از این تکنولوژی است. این امر، خرید VoIP را به یک راه حل ایده آل برای مشاغل و افرادی تبدیل می‌کند که تماس‌های بین‌المللی زیادی برقرار می‌کنند. استفاده از سیستم ویپ نسبت به تلفن سانترال از جنبه‌های مختلفی مقرون به صرفه تر است از جمله:

- **تلفن‌های سنتی به لحاظ تجهیزات سخت افزاری و فضای نگهداری، هزینه بالایی را می‌طلبند؛ در حالی که نگهداری از سیستم ویپ وابسته به کامپیوتر یا موبایل مورد استفاده کاربر است و نیازی به سیم کشی مجزا ندارد. حتی برای استفاده از VoIP نیاز به تجهیزات اضافی وجود ندارد. تنها کفایت یک سیستم کامپیوتری و یک همدست برای پاسخ به تماس‌ها داشته باشید.**
- **علاوه بر اینکه تماس‌های داخلی برای مجموعه شما رایگان خواهد بود، برای برقراری ارتباط در تلفن‌های معمولی، به ازای هر دقیقه باید هزینه پرداخت کرد؛ اما در سیستم VoIP، تنها با اتصال به اینترنت و پرداخت مبلغ ماهیانه می‌توانید به صورت نامحدود تماس برقرار کنید. این ویژگی به خصوص برای تماس‌های بین‌المللی بسیار کارآمد است.**
- **نگهداری، نصب و راه اندازی سیستم‌های تلفن قدیمی سخت‌تر و پرهزینه‌تر از نگهداری سیستم‌های اینترنتی مانند ویپ است.**

نصب و استفاده آسان

نصب VoIP با پیچیدگی زیادی روبرو نمی‌باشد. در حقیقت، فرآیند نصب آسان و دینامیک بودن این نوع سیستم، مزیت بالایی نسبت به تلفن‌های معمولی دارد.

به عنوان مثال، با نصب و راه اندازی ویپ برای کسب و کارها، دیگر نیازی به کابل کشی مجدد وجود ندارد. بنابراین علاوه بر کاهش هزینه‌های اضافی، خطرات ناشی از سیم‌کشی و... نیز کاهش می‌یابد.

دورکاری و قابلیت حمل

دورکاری و وجود تیم‌های مختلف در نقاط جغرافیایی گوناگون برای بسیاری از مشاغل یک ویژگی کلیدی است. یکی از مزیت های سیستم تلفن اینترنتی یا ویپ این است که به کسب و کارها امکان می‌دهد تا حد امکان قابل حمل باشند. یعنی **کارکنان می‌توانند با اتصال به اینترنت از هر نقطه‌ای به سیستم تلفنی خود دسترسی داشته باشند**. با این اوصاف این ویژگی برای سازمان هایی که کارمندان با کار هیبریدی یا دورکاری دارند، بسیار مفید است. این ویژگی یک دلیل مهم برای کاربرد ویپ در برقراری ارتباطات تجاری است؛ زیرا زمینه مورد نیاز برای برقراری ارتباطات موثر و مقرون به صرفه در شرکت‌ها و سازمان‌ها را فراهم می‌کند.

کنفرانس و ارتباط صوتی و تصویری

VoIP با ارائه خدمات صوتی و تصویری اینترنتی، به تیم‌ها این امکان را می‌دهد تا در هر زمان و مکانی که باشند، به صورت پویا و بدون وقفه، با مخاطبین و دیگر اعضای تیم ارتباط برقرار کنند و به فایل‌ها و ویژگی‌های مختلف دسترسی داشته باشند.

انعطاف پذیری

VoIP امکان دسترسی به ویژگی‌هایی را می‌دهد که با سیستم های تلفن سنتی در دسترس نیستند. VoIP همچنین به کاربران این امکان را می‌دهد که خدمات تلفن خود را با سایر خدمات

ارتباطی مانند ایمیل، پیام رسانی و ویدئو کنفرانس یکپارچه کنند. به طور مثال قابلیت اتصال به تلفن گویا (IVR) از این دست ویژگی ها است.

مقیاس پذیری

سیستم تلفنی ویپ را می توان به راحتی مطابق با نیازهای مشاغل در هر اندازه ای کوچک یا بزرگ کرد. از آنجایی که VoIP به هیچ زیرساخت فیزیکی نیاز ندارد، مشاغل می توانند بدون نیاز به نصب سخت افزار اضافی، خطوط تلفن را در صورت نیاز اضافه یا حذف کنند. به علاوه سازمان ها می توانند در صورت اضافه کردن نیرو یا بخش های دیگر، با هزینه بسیار اندک نرم افزار ویپ را به واحدهای دیگر نیز متصل کنند.

یکپارچه سازی

VoIP را می توان با سایر برنامه های کاربردی تجاری مانند سیستم های مدیریت ارتباط با مشتری (CRM) ادغام کرد تا یک تجربه ارتباطی یکپارچه برای کارکنان و مشتریان فراهم کند.

کیفیت تماس بالا

فناوری VoIP از کدک های پیشرفته Codec و الگوریتم های فشرده سازی استفاده می کند که امکان انتقال صدای با کیفیت بالا را از طریق اینترنت فراهم می کند. برخلاف خطوط تلفن سنتی، تماس های VoIP بسیار واضح تر و بدون نویز و اکو هستند. علاوه بر این، فناوری VoIP از طیف گسترده ای از پهنای باند پشتیبانی می کند، به این معنی که حتی با اتصال محدود به اینترنت، کاربران همچنان می توانند از تجربه تماس با کیفیت بالا لذت ببرند. توانایی برقراری تماس های با کیفیت بالا با VoIP، آن را به گزینه ای جذاب برای مشاغلی تبدیل می کند که برای فعالیت های روزمره خود به شدت به ارتباطات صوتی متکی هستند.

امنیت بالا

در مراکز تماس VoIP، تماس‌های شما کاملاً رمزگذاری انجام می‌شوند. این امر سبب می‌شود امنیت سیستم ویپ بالا رفته و امکان استراق سمع و یا هک سیستم از بین برود و عوامل خارجی نتوانند در سیستم اختلال ایجاد کنند.

معایب VoIP

طبیعتاً استفاده از هر سیستمی در کنار مزایای بی شمار، دارای معایبی می باشد. حالا نگاهی به معایب و مشکلات ویپ می اندازیم.

وابستگی به اینترنت

یکی از معایب استفاده از ویپ، وابستگی آن به اینترنت و یا شبکه است. هرچند این ویژگی مزایای زیادی برای فناوری VoIP به همراه دارد؛ اما در صورت وجود مشکل یا قطع شدن زیرساخت شبکه یا اینترنت، کیفیت تماس‌های ویپ نیز دچار اختلال خواهد شد.

وابستگی به برق

از آنجایی که VoIP برای کار کردن به برق نیاز دارد، هرگونه قطع برق می تواند منجر به از دست دادن خدمات شود. این را می توان با استفاده از پشتیبان های باتری یا ژنراتورها کاهش داد، اما این راه حل ها می توانند گران بوده و نیاز به تعمیر و نگهداری داشته باشند. لازم به ذکر است که در سیستم های سنتی سانترال هم این معضل وجود دارد و نقطه مشترک هر دو سیستم می باشد.

امنیت

تماس‌های VoIP می‌توانند در برابر فیشینگ، هک، استراق سمع و دیگر اشکال حملات سایبری آسیب‌پذیر باشند. این به این دلیل است که تماس‌های VoIP از طریق شبکه یا اینترنت، منتقل می‌شود. در واقع امنیت در VoIP هم نقطه قوت و هم در صورت عدم پیاده سازی صحیح، نقطه ضعف آن می‌باشد.

به عنوان کاربر ویپ، مهم است تا از نشانه های هک سیستم ویپ باخبر باشید. پس از آگاهی از این نشانه ها باید راهکارهای لازم جهت امنیت ویپ را نیز بدانید تا بتوانید تماسی امن برقرار کنید.

سازگاری

VoIP ممکن است با همه دستگاه ها یا سیستم ها سازگار نباشد. به عنوان مثال، برخی از تلفن های IP قدیمی ممکن است با پروتکل های VoIP جدیدتر سازگار نباشند، و برخی از سیستم های تلفن قدیمی ممکن است نتوانند با VoIP یکپارچه شوند. بنابراین قبل از راه اندازی ویپ VoIP باید تمام این موارد را در نظر بگیرید. با توجه به رشد سریع فناوری های ارتباطات، این گزینه غالباً مود توجه نمیباشد.

مزایای VoIP نسبت به سانترال

اولین مزیت برتر ویپ نسبت به سانترال، افزایش انعطاف‌پذیری در مرکز تماس است. در سیستم VoIP، تماس‌ها بر بستر اینترنت انجام می‌شوند، این قابلیت به کاربران امکان می‌دهد که از هر نقطه‌ای با اتصال به اینترنت به سیستم تلفنی خود دسترسی داشته باشند. چنین امکانی باعث می‌شود که کاربران به راحتی و با کمترین هزینه به سیستم تلفنی خود دسترسی داشته باشند. علاوه بر این، ساختار ویپ دارای قابلیت‌های پیشرفته‌تری مانند تماس‌های ویدیویی و مشارکت در تماس‌های گروهی است؛ ولی در سانترال‌های سنتی، امکان دسترسی به این سطح از انعطاف‌پذیری وجود ندارد.

از دیگر مزایای تلفن VoIP نسبت به سنترال، میتوان به کاهش هزینه‌های کلی و اجرایی اشاره کرد. با استفاده از این فناوری، سازمان‌ها می‌توانند به وسیله اینترنت به صورت رایگان تماس بگیرند یا هزینه‌های تماس‌های بین‌المللی را به حداقل برسانند. علاوه بر این، در سیستم ویپ کاربران می‌توانند از طریق تلفن هوشمند خود به راحتی به سیستم تلفنی سازمان دسترسی داشته باشند و هزینه‌های مربوط به تماس‌های موبایل را نیز کاهش دهند.

امکانات VoIP

در بخش قبل به تفصیل در خصوص مزایا و معایب ویپ بحث شد. اما در ادامه مهمترین امکانات ویپ بیان شده است :

- تعداد داخلی بالا
- دریافت پیام صوتی و تصویری
- تماس صوتی Voice Call
- تماس تصویری Video Call
- ضبط مکالمات
- تلفن های نرم افزاری Soft-Phone
- فکس و Fax-to-Mail
- پست صوتی Voice Mail
- سامانه پاسخگویی خودکار IVR (Interactive Voice Response)
- صف انتظار
- تنظیم ساعت اداری
- ارتباط با CRM و نرم افزارهای سازمانی
- گزارش گیری

تفاوت خطوط تلفن ثابت و فناوری VoIP چیست؟

در جدول زیر، تفاوت خطوط تلفن ثابت (آنالوگ) و فناوری VoIP بیان شده است:

خطوط تلفن آنالوگ	فناوری VoIP
امواج صوتی از طریق کابل‌های مسی و فیبر نوری منتقل می‌شوند.	داده‌های صوتی از طریق پروتکل اینترنت منتقل می‌شوند.
عملکرد آن به تلفن آنالوگ وابسته است.	عملکرد آن فقط از طریق اتصال شبکه امکان‌پذیر است.
تمام تماس‌ها با هزینه همراه و تماس‌های بین‌المللی بسیار گران هستند.	تماس‌های محلی رایگان و تماس‌های بین‌المللی مقرون به صرفه هستند.
برای دسترسی به ویژگی‌های محدود، به خطوط تلفن سیمی و تجهیزات اضافی نیاز است.	مقیاس‌پذیری آسان و امکان افزودن ویژگی‌های جدید فراهم است.
معمولاً خطوط تماس در صورت قطع برق همچنان کار می‌کند.	معمولاً با قطع برق امکان برقراری تماس نیز وجود نخواهد داشت؛ مگر اینکه کاربر از اینترنت خط استفاده کند.

بررسی انواع VoIP

بر اساس نوع فناوری، سیستم ویپ به انواع مختلفی تقسیم می‌شود. به طور کلی در ساخت انواع ویپ، چهار نوع فناوری مختلف استفاده شده است. در ادامه، انواع VoIP را معرفی می‌کنیم.

1. Integrated Access

Integrated Access یکی از سرویس‌های ویپ است و بیشترین شباهت را به خطوط تلفن ثابت سنتی دارد. با استفاده از این سرویس ویپ، کسب‌وکارها می‌توانند نرم‌افزارهای VoIP را با سیستم تلفن‌های سنتی ادغام کنند. این نوع ویپ به کاربران امکان می‌دهد تا در کنار دسترسی به امکانات مخابراتی پیشرفته، شماره تماس و تجهیزات قدیمی خود را نیز حفظ کنند.

۲. SIP Trunks

یکی دیگر از انواع ویپ، سرویس SIP Trunks است. سیستم SIP اطلاعات صوتی و تصویری را در طول یک شبکه داده منتقل می‌کند و به کاربران VoIP امکان می‌دهد تا از خطوط مشترک استفاده کنند. این امر سبب افزایش انعطاف‌پذیری ارتباطات کاربران خواهد شد. از آن‌جاکه تمام داده‌ها از طریق یک شبکه ارتباطی (Network) ارسال می‌شوند، کسب‌وکارها می‌توانند سیستم SIP Trunk را جایگزین سیستم آنالوگ سنتی کنند. از مزایای سیستم SIP می‌توان به این‌ها اشاره کرد:

➤ **انعطاف‌پذیری**

➤ **کار با فناوری ابری**

➤ **ادغام با تلفن‌های Private Branch Exchange (به اختصار PBX)**

➤ **صرفه‌جویی در هزینه‌ها**

➤ **مناسب برای مشاغل مختلف**

۳. Hosted IP PBX

از طریق این نوع VoIP، کسب‌وکار می‌تواند با شبکه IP خود به شبکه مبتنی بر ابر Hosted IP PBX متصل شوند. در این سیستم، فروشنده Hosted IP PBX سخت‌افزار سیستم تلفن را در خارج از سایت نگهداری می‌کند. تمام مسئولیت سخت‌افزار، نرم‌افزار، نگهداری، امنیت و به‌روزرسانی نیز برعهده ارائه‌دهنده میزبان است. معمولاً این نوع ویپ برای کسب‌وکارهای کوچک تا متوسط مناسب است و کنترل پنل کاربرپسندی ارائه می‌دهد. از طریق این کنترل پنل صاحبان کسب‌وکارها می‌توانند سیستم‌های تلفن را مدیریت و نظارت کنند.

۴. Managed IP PBX

Managed IP PBX یکی دیگر از انواع ویپ به‌شمار می‌آید که مانند نوع قبلی، به‌صورت برون‌سپاری به شخص ثالث سپرده می‌شود. در این نوع ویپ، تمامی الزامات مدیریتی برعهده شخص ثالث است؛ اما به‌جای اینکه سخت‌افزار تلفن خارج از محل باشد، این تجهیزات در محل و در اختیار کسب‌وکار قرار

می‌گیرد. ارائه‌دهنده Managed PBX بسته به تعداد خطوط تلفن معمولاً هزینه ثابتی دریافت می‌کند. نکته دیگر اینکه نصب تجهیزات، نگهداری، به‌روزرسانی و ارتقای تجهیزات نیز برعهده ارائه‌دهنده است.

بررسی نحوه عملکرد فناوری VoIP

سرویس VoIP ابتدا صدای کاربر را از سیگنال‌های صوتی به داده‌های دیجیتال تبدیل و سپس داده‌های دیجیتالی را از طریق اینترنت به کاربر یا گروهی از کاربران ارسال می‌کند. فناوری ویپ برای انجام کار از Codec‌ها استفاده می‌کند. Codec‌ها با انجام فرایندهای مبتنی بر سخت‌افزار یا نرم‌افزار، می‌توانند حجم بزرگی از داده‌های VoIP را فشرده یا از حالت فشرده خارج کنند.

با اینکه فشرده‌سازی داده‌ها نیاز به پهنای باند را کاهش می‌دهد، این احتمال نیز وجود دارد که با فشرده‌سازی داده‌ها، کیفیت صوت کاهش پیدا کند. حال این سؤال مطرح می‌شود که فرایند سیستم ویپ چگونه است و شامل چه مراحل می‌شود؟ به‌طورکلی، فرایند انتقال داده از کاربری به کاربر دیگر عبارت است از:

➤ کپسوله‌کردن صوت در بسته‌های داده

➤ انتقال بسته‌ها از طریق شبکه IP

➤ تبدیل مجدد بسته‌های کپسوله‌شده به صوت در مقصد

سیستم ویپ معمول شامل اجزای اضافی زیر است:

➤ IP PBX برای مدیریت شماره تلفن‌های کاربر

➤ دستگاه‌ها

➤ امکانات و مشتریان

➤ ارائه درگاه‌هایی برای اتصال شبکه در صورت قطع شبکه

➤ ارائه کنترل‌کننده‌های مرزی برای تأمین امنیت

➤ مدیریت خط‌مشی تماس و اتصالات شبکه

نحوه راه اندازی سیستم ویپ

متخصصان و شرکت‌های ارائه‌دهنده حرفه‌ای، سیستم ویپ را راه‌اندازی می‌کنند؛ چراکه درغیراین‌صورت احتمال بروز ایراد بسیار زیاد است. بااین‌حال، این بدان‌معنا نیست که افراد نمی‌توانند شخصاً در منزل یا محل کارشان سیستم ویپ را راه‌اندازی کنند. درادامه مقاله، مراحل راه‌اندازی سیستم VoIP را توضیح می‌دهیم.

۱. شناخت نیازهای خانه یا محل کار خود

قبل از هر اقدامی، لازم است نیازهای کسب‌وکار یا منزل خود را مشخص و سپس براساس آن، یکی از انواع VoIP را انتخاب کنید. برای این کار، سیستم تلفن فعلی و حجم تماس‌ها و نوع تماس‌های خود را باید در نظر بگیرید.

۲. امتحان کردن اتصال اینترنت

ازآن‌جاکه کیفیت تماس‌های ویپ تا حد زیادی به کیفیت و سرعت اتصال اینترنت شما مرتبط است، باید اینترنت پرسرعت دراختیار داشته باشید.

۳. شناخت انواع ویپ و تفاوت آن‌ها

قبل از انتخاب سیستم ویپ، باید با انواع VoIP آشنا باشید. بدین‌ترتیب، براساس نیازها و شرایط خود می‌توانید مناسب‌ترین گزینه را انتخاب کنید.

➤ **VoIP مبتنی‌بر دستگاه:** در این نوع ویپ، با هدف تسهیل در تماس‌ها از یک دستگاه ویپ و اتصال آن به دستگاه تلفن موجود استفاده می‌شود.

➤ **PBX:** مخفف عبارت *Private Branch Exchange* است و به شبکه تلفن خصوصی اطلاق می‌شود. *PBX* ارتباطات کاربر را تسهیل و VoIP اختصاصی شما را میزبانی می‌کند. در صورت دراختیار داشتن سرور اختصاصی VoIP، به تیم IT و تیم تعمیر و نگهداری و سیستم به‌روزرسانی نیاز خواهید داشت.

➤ **Cloud-Based PBX**: برخلاف نوع قبلی، در این نوع ویپ ارائه‌دهنده‌ای شخص ثالث تمام امور مربوط به تعمیر و نگهداری سیستم را برعهده می‌گیرد. PBXهای مبتنی بر ابر به‌جای استفاده از تجهیزات سخت‌افزاری، از سیستم‌های نرم‌افزاری استفاده می‌کنند.

۴. تعیین بودجه

در این مرحله، بودجه اختصاص‌یافته برای راه‌اندازی باید مشخص شود. به‌عنوان مثال، اگر ویپ‌های مبتنی بر دستگاه را انتخاب کرده باشید، بخش بزرگی از هزینه‌های شما صرف خرید تجهیزات فیزیکی خواهد شد. همچنین در صورت انتخاب On-Premise PBX، بودجه شما به مواردی همچون نصب سیستم و سرویس‌های IT و نگهداری اختصاص داده می‌شود. علاوه‌براین در صورت انتخاب PBX مبتنی بر ابر، براساس تعداد خطوط تلفن باید هزینه‌های ماهانه را پرداخت کنید.

۵. انتخاب شرکت ارائه دهنده VoIP

در این مرحله، تمام امکانات و خدمات شرکت ارائه‌دهنده VoIP را بررسی و سپس هریک از آن‌ها را با نیازها و شرایط خود مقایسه کنید. برخی از نکات مهمی که قبل از انتخاب شرکت ارائه‌دهنده باید در نظر بگیرید، عبارت‌اند از:

➤ امکان مدیریت تماس‌ها (Call Management)

➤ یکپارچگی شخص ثالث (Third-Party Integrations)

➤ ارائه ارتباطات یکپارچه (Unified Communications)

➤ ارائه اپلیکیشن‌های موبایلی

➤ ارائه پروتکل‌های امنیتی مناسب

۶. دریافت یا حفظ شماره تلفن برای کسب و کار

بسیاری از برنامه‌های ویپ، شامل شماره‌های تلفن‌های محلی می‌شوند. این گزینه برای کسب‌وکارهایی ایده‌آل است که بازار هدف محدودی دارند و می‌خواهند در منطقه‌ای محدود فعالیت

کنند. همچنین، این امکان وجود دارد تا بدون تغییر شماره، شماره تلفن قبلی خود را به شماره تلفن مجازی تبدیل کنید. در هر دو صورت، برنامه انتخابی خود را باید با شرکت ارائه‌دهنده VoIP در میان بگذارید.

۷. نصب و راه اندازی سیستم ویپ

نحوه نصب تلفن ویپ براساس نوع سیستم انتخابی متفاوت است و تجهیزات متفاوتی لازم دارد؛ پس بهتر است مراحل نصب و راه‌اندازی ویپ را به افراد کاربلد و حرفه‌ای بسپارید. در ادامه، نحوه نصب انواع ویپ را به اختصار توضیح می‌دهیم:

- **سیستم‌های ویپ مبتنی بر دستگاه: تلفن موجود خود را به آداپتورهای مودم وصل کنید.** همچنین از تلفن‌های IP می‌توانید استفاده کنید که از طریق WIFI به اینترنت متصل می‌شوند.
- **سیستم‌های On-Premise VoIP: نصب PBX در محل نیازمند حضور مدیران پروژه و مدیران سیستم و برق‌کاران متخصص در زمینه VoIP است.**
- **سیستم‌های Cloud-based PBX: در این سیستم، به سادگی می‌توانید اپلیکیشن را از شرکت ارائه‌دهنده دریافت و روی دسکتاپ و دستگاه تلفن همراه خود نصب کنید.**

دلیل خرید ویپ چیست؟

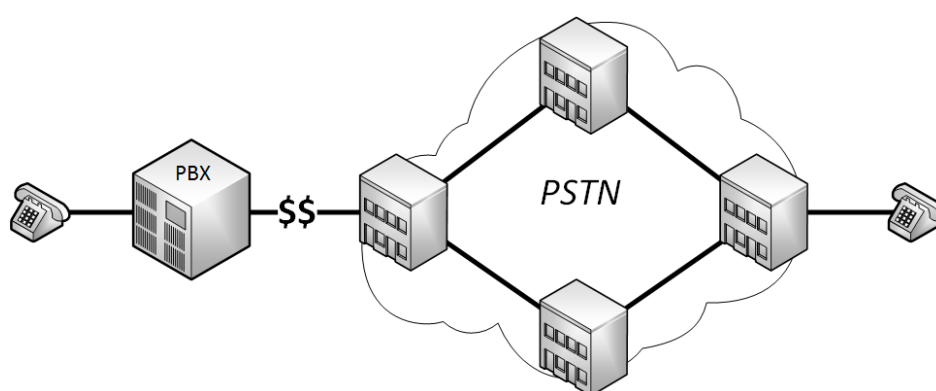
پس از بررسی کاربرد ویپ و مزایا و معایب آن، می‌توان گفت یکی از دلایل اصلی خرید ویپ، تنوع خدمات و کیفیت و سرعت فراوان ارتباط و کاهش هزینه‌هاست. کاربران خانگی و کسب‌وکاری ویپ با راه‌اندازی این سیستم، به راحتی می‌توانند از طریق خدمات صوتی، تصویری، گروه‌های چت و... با مخاطبان خود ارتباط برقرار و تماس‌های باکیفیتی تجربه کنند. همچنین، دردسترس بودن انواع ویپ سبب شده است تا کاربران بتوانند براساس شرایط و نیازهای خود، مناسب‌ترین سیستم را انتخاب کنند و با پرداخت حداقل هزینه‌ها، بیشترین بهره را از خدمات ارائه‌شده ببرند.

فصل سوم: سخت افزار VoIP

در این بخش به معرفی مهمترین سخت افزارهای سامانه های آنالوگ و سپس سیستم های VoIP می پردازیم.

PSTN

عبارت اختصاری PSTN مخفف جمله public switched telephone network است که معنی لغوی آن " شبکه تلفن عمومی سوئیچ شده" است.



این شبکه که همان زیرساخت شرکت های مخابراتی است، موظف است ارتباط تماس های تلفنی و انتقال پیام های صوتی را برقرار و مدیریت کند. هر public switched telephone network یا به اختصار network pstn شامل خطوط تلفنی، کابل های فیبرنوری، لینک های انتقال ماکروویو، شبکه موبایل، انتقال ارتباطات ماهواره ای و کابل های ارتباطی زیر دریایی است. تمام این موارد که بیان کردیم به وسیله سوئیچینگ به یکدیگر متصل می شوند و در نتیجه امکان ارتباط صوتی و تصویری از نقطه ای به نقطه ای دیگر دنیا را فراهم می سازد.

PSTN ، فناوری انتقال صدا صدای آنالوگ با استفاده از سیم های مسی است. در واقع PSTN ، یک سرویس قدیمی و متداول است که امروزه همه ی ما در منازل استفاده می کنیم. اما این سیستم با گذشت زمان ، بسیار پیشرفته تر از آن چه که در زمان های قدیمی بوده است ، گردید. به این ترتیب که با استفاده از مبدل هایی در مبدا و مقصد ، می توان اطلاعاتی که ترانسفر میشود را دیجیتالی کرد. البته

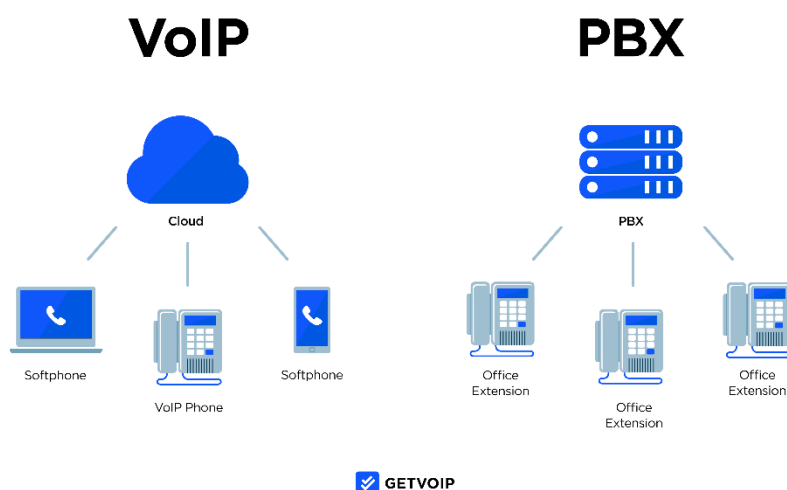
این تغییرات به طور کلی ماهیت PSTN را عوض نمی کنند و در اصل استفاده ی امروزه ما از این سیستم ، تنها برقراری تماس صوتی محدود است.

PBX

PBX مخفف Private Branch Exchange، یک سیستم تلفنی است که تماس‌ها را بین افراد در خطوط داخلی تقسیم می‌کند. این سیستم به کاربران امکان می‌دهد تا از چندین خط تلفن خارجی نیز بصورت مشترک استفاده کنند. برخلاف شبکه تلفن سنتی، هدف اصلی تلفن PBX صرفه جویی در هزینه خطوط تلفن مورد نیاز، به ازای هر کاربر در شرکت شما است.

در واقع با یک سیستم تلفن PBX، خط تلفن فیزیکی وارد شده به سازمان شما به چندین خط تقسیم می‌شود و این امکان را ایجاد می‌کند تا از تماسهای بیشتری پشتیبانی کنید. امتیاز دیگر این سیستم، تماس رایگان بین کارمندان شرکت است.

تلفن PBX معمولاً ویژگی‌های ویژه تلفن تجاری، مانند انتقال تماس، صف تماس، پست صوتی و غیره را در اختیار شما قرار می‌دهد. PBX به عنوان یک سیستم تلفن تجاری یا شبکه تلفن خصوصی استفاده می‌شود، و بصورت اختصاصی متعلق به شرکت شما خواهد بود. البته همچنان به یک شرکت مخابراتی (یا تأمین کننده خدمات ویپ) به عنوان ارائه دهنده خدمات تلفنی نیاز دارید.

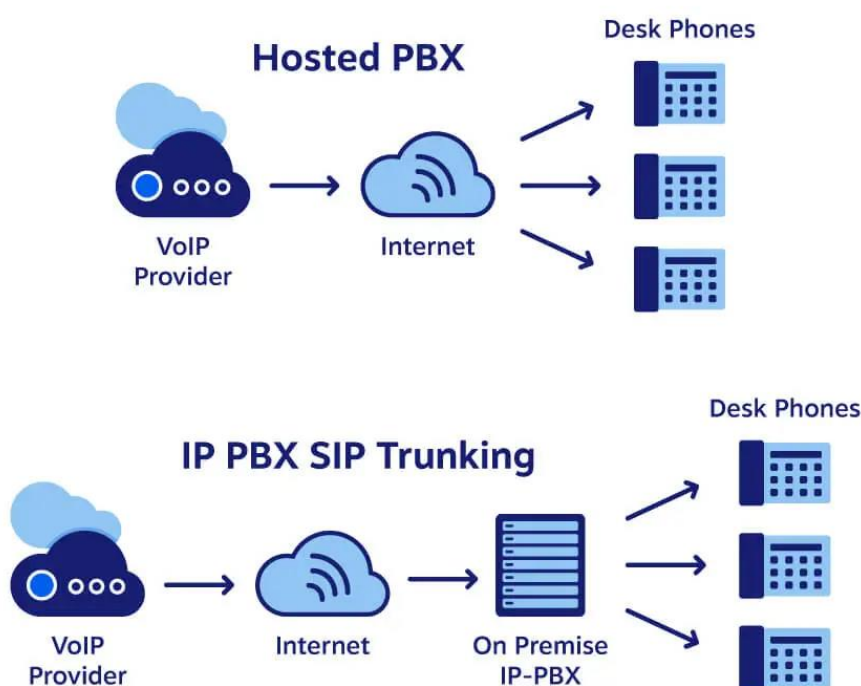


انواع سیستم تلفن PBX

اگر قصد دارید از سیستم تلفن PBX برای کسب‌وکار خود استفاده کنید، بهتر است ابتدا همه گزینه‌های موجود را بررسی کنید تا بتوانید بهترین و مناسب‌ترین انتخاب را در این زمینه داشته باشید.

➤ **تلفن PBX آنالوگ:** این سیستم تلفن، قدیمی و درون سازمانی است. ده‌ها سال است که سازمان‌ها از این سیستم برای ارتباطات تجاری خود استفاده می‌کنند و از طریق خطوط تلفن سنتی "POTS" به "PSTN" (شبکه تلفن سوئیچ شده عمومی) متصل می‌شوند. تماس‌های تلفنی و حتی ارسال فکس در PBX با استفاده از خطوط تلفن فیزیکی انجام می‌شود. سیستم تلفن سانترال آنالوگ امکان برقراری تماس و انتقال تماس‌ها در داخل شرکت را برای شما ایجاد می‌کند. این تلفن‌ها همچنین تماس‌های ورودی و خروجی شما را مدیریت می‌کنند.

➤ **تلفن VoIP PBX یا IP PBX:** نسخه جدیدتری از تلفن‌های سانترال است. این دستگاه عملکردی مشابه یک PBX سنتی دارد، اما ویژگی‌های بیشتری را نیز به کاربران خود ارائه می‌دهد. در حالت کلی این سیستم گزینه مقرون به صرفه‌تری نسبت به نسخه قدیمی سانترال است. IP PBX به جای استفاده از خطوط تلفن سنتی، از بستر اینترنت برای انتقال صدا استفاده می‌کند. در این سیستم ابتدا صدا به داده تبدیل می‌شود تا از طریق اینترنت منتقل شود، سپس زمانی که به مقصد می‌رسد مجدداً داده‌ها به فایل صوتی تبدیل می‌شوند.



مزایای سیستم‌های تلفن PBX میزبانی شده (Hosted PBX) چیست؟

اگر به دنبال سیستم تلفن برای یک کسب‌وکار روبه‌رشد هستید، PBX میزبانی شده را بررسی کنید:

- راه‌اندازی *Plug-and-play*
- مقیاس‌پذیری
- حمایت از کارکنان در محل شرکت یا دورکار
- ویژگی‌های همکاری مانند کنفرانس، اشتراک‌گذاری صفحه و پیام‌رسانی فوری
- عدم نیاز به تجهیزات سخت‌افزاری و کارکنان حرفه‌ای IT
- ساده‌ترین سیستم ارتباطی یکپارچه در نصب و نگهداری
- دارای ویژگی‌های پیشرفته برای توانمندسازی تیم پشتیبانی مشتریان
- ادغام با CRM و سایر پلتفرم‌های مورد استفاده در سازمان
- گزینه‌ای مقرون به‌صرفه برای مشاغل کوچک بدون نیاز به سرمایه‌گذاری در زیرساخت‌های تلفن

مزایای تلفن PBX درون سازمانی چیست؟

داشتن یک سانترال درون سازمانی دارای مزایای زیر است:

- هزینه‌های عملیاتی کم
- تسلط و کنترل کامل به دلیل داشتن تجهیزات
- نداشتن نیاز به خرید اعتبار یا پرداخت هزینه اشتراک
- قابلیت تعیین یا تغییر سطح امنیت دلخواه

ATA

ATA یا Analog Telephone Adapter ، آداپتور یا واسط آنالوگ تلفنی می باشد که رایج ترین راه

ارتباطی برای اتصال به ویپ می باشد.

ATA ها ، دستگاه هایی هستند که با ایجاد ارتباط میان تلفن های آنالوگ قدیمی و شبکه شما ، امکان استفاده از ویپ را به سادگی و بدون نیاز به تغییر سخت افزار فراهم می کند.



Channel Bank

این دستگاه سیگنال های آنالوگ که معمولاً از طریق خطوط تلفن منتقل می شود را به سیگنال های دیجیتالی که از طریق اینترنت منتقل می شوند تبدیل می کند.

تلفن های تحت شبکه یا IP Phone



تلفن های تحت شبکه، نوعی از تلفن های ثابت محسوب می شوند که می توانند در کنار سرورهای ویپ کار کنند. این تلفن ها اگرچه از نظر ظاهری تفاوت زیادی با تلفن های معمولی ندارند؛ اما در عمل قابلیت های منحصر به فرد زیادی دارند. این دستگاه ها به گونه ای طراحی شده اند که می توانند از طریق اتصال به یک شبکه محلی، صدا و تصویر را در بستر شبکه، انتقال دهند.

تلفن های تحت شبکه به هر دو روش آداپتوری و یا PoE قابل طراحی و موجود در بازار میباشد.

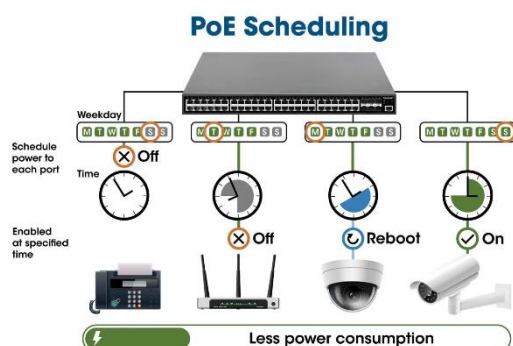
تکنولوژی POE

Power over Ethernet (PoE) یکی از فناوری های جدید شبکه های محلی، اترنت سیمی (LAN) است که جریان الکتریکی لازم برای کارکرد هر دستگاه را قادر می سازد تا به جای سیم های برق و سیم کشی استاندارد، توسط کابل های داده اترنت منتقل شود. علاوه بر خانه ها، در محل های تجاری نیز قابل استفاده است. در این فناوری جدید که برای شبکه های اتصال طراحی شده است، از کابل های اترنت ارزان تر استفاده می شود که بتوان نیرو و داده را همزمان انتقال داد.

در استاندارد شبکه سیمی یا Ethernet سیم های نارنجی و سبز جهت انتقال داده، و سیم های آبی و قهوه ای جهت انتقال جریان الکتریکی استفاده میشود.

برای استفاده از این تکنولوژی ۲ راهکار وجود دارد :

➤ **پاور PoE:** یا PoE Injector استفاده از یک مبدل جریان برق شهری به ولتاژ استاندارد مورد نیاز در تجهیزات.



➤ **سوئیچ PoE:** در شبکه های ساخت یافته می توان از سوئیچ هایی استفاده نمود که پورت های اترنت سوئیچ، قابلیت PoE را داشته و جریان الکتریکی را همزمان با انتقال داده، منتقل می نماید.

UPS - Uninterruptible Power Supply

VoIP headset

هدفون های تحت شبکه برای کاربرانی که روزانه تماس هایی زیادی را پاسخگو هستند طراحی شده است. کاربران با استفاده از هدست تحت شبکه میتوانند تماس های خود را با راحتی و بدون در دست گرفتن گوشی و آزار دست و گردن پاسخ داده و در تمام ساعات روز بدون خستگی به فعالیت خود بپردازند. هدست های متعددی با تلفن تحت شبکه سازگار هستند، اما یافتن آمپلی فایر صحیح یا کابل اتصال مستقیم کلید کار مناسب هدست ویپ با تلفن سانترال شماست.

IP-PBX Server

سیستم تجاری ارتباطات سازمانی است که تماس ها را هدایت می کند و سوئیچینگ مختلف درون سازمان ها را ممکن می سازد

حتماً در فیلم های قدیمی دیده اید که فردی درون اتاقکی شلوغ و پر از سیم نشسته است و به صورت دستی به انتقال و ارتباط تماس ها می پردازد. شاید گمان کنید با تکنولوژی های امروزی، کار این فرد که برای نخستین بار به معنای امروزی کلمه اپراتور نامیده می شد، از رونق افتاده است و دیگر خبری از آن اتاق های شلوغ و پر از سیم نیست. البته تمام این اتفاقات، امروز هم جریان دارد. ارتباطات در سازمان های مختلف به مراتب گسترده تر شده اند و انتقال تماس ها با پیچیدگی بیشتری جریان دارد. PBX وظیفه ی اپراتورهای سابق را بر عهده دارد. اخیراً این سیستم ها با استفاده از بستر IP ، به جای پروتکل های مخابراتی، شبکه را به استخدام گرفته اند تا بتواند ارتباطات را تسهیل کند و IP-PBX ها را پدید آورده اند.

فصل چهارم: نرم افزارهای VOIP

جهت راه اندازی مراکز تلفن تحت شبکه، باید از یک نرم افزار استفاده کرد. غالب این نرم افزارها به صورت OpenSource ارائه میگردد و امکان اصلاح و افزایش کاربری ها و ماژول های مختلف با توجه به نیاز هر سازمان را دارند.

نرم افزار نصب شده بر روی یک سرور سخت افزاری یا ماشین مجازی، تشکیل یک IP-PBX Server را می دهد.

مهمترین نرم افزارهای سرور VoIP:

- *Ring Central*
- *Nextiva*
- *DialPad*
- *Elastix*
- *Issabel*
- *CloudTalk*
- *Grasshopper*
- *GoToConnect*
- *Avaya*
- *Vonage*

مراجع

1. Faradard.org
2. Barghchi.com
3. Taknet.ir
4. Iranhost.com
5. Parspack.com
6. Voiping.ir
7. Alovoip.ir
8. Novinvoip.com
9. Elmparvar.com