بسمه تعالی

عنوان مستند

امنیت حجیم‌داده

بخش ۲ : لاگ، مانیتورینگ و کنترل دسترسی

سرفصل مطالب

فهرست اشکال

چکیده

در سال‌های اخیر، رشد سریع اینترنت و فراگیر شدن فن‌آوری‌های جدیدی نظیر اینترنت اشیاء، محاسبات ابری و شبکه‌های اجتماعی باعث رشد انفجاری تولید و جمع‌آوری داده‌ها در حوزه‌های مختلف حوزه فن‌آوری اطلاعات شده است. در کنار امکانات جدید سخت‌افزاری و روش‌های کلاسیک علوم داده، دانش یا فن‌آوری جدیدی به نام "حجیم‌داده" پایه‌گذاری شده است که به چالش‌های جدید این حوزه می‌پردازد. اصطلاح حجیم‌داده، یک واژه برای توصیف مجموعه داده‌هایی است که دارای حجم بزرگ، سرعت تولید زیاد و ساختار متنوع و پیچیده نسبت به پایگاه‌داده‌های معمولی هستند. از اینرو، برای ذخیره‌سازی، بازیابی، پردازش، تحلیل و همچنین بصری‌سازی آنها نیازمند ساختارها، الگوریتم‌ها و ابزارهایی متفاوت از گذشته هستیم. با پیشرفت‌های صورت گرفته در این چند سال در حوزه حجیم‌داده، کاربردهای این فن‌آوری روزبه‌روز بیشتر گسترش یافته و میزان داده‌هایی که در بسترهای مبتنی بر حجیم‌داده، ذخیره‌سازی و پردازش می‌شوند افزایش چشم‌گیری داشته است. یکی از چالش‌های اساسی در این زمینه، نحوه تامین امنیت داده در بستر حجیم‌داده است. یک بستر حجیم‌داده کارآمد نباید تنها روی حجم، سرعت یا تنوع داده‌ها تمرکز کند، بلکه با توجه به انبوده داده‌های مهم موجود در آن، باید حفاظت آنرا نیز تضمین نماید. تنوع در ساختار داده‌ها و امکان دسترسی گسترده به آن‌ها توسط کاربران متعدد، موجب شده تا روش‌های سنتی حفاظت در حجیم‌داده کارآمد نباشند و امنیت داده را با چالش‌های جدیدی روبرو سازند. از این روی شاهد پیدایش و رشد ابزارها و چارچوب‌های متنوع در بخش‌های مختلف حجیم‌داده در حوزه امنیت هستیم، که مدیران و صاحبان صنایع، کارشناسان حوزه علوم داده و کاربران علاقه‌مند و یا مجبور به رعایت و استفاده از این ابزارها و چارچوب‌ها در راستای حفاظت از داده می‌باشند. در این سلسله مستندات، ما قصد داریم مهمترین چالش‌ها و مباحث را در حوزه امنیت حجیم‌داده تشریح کرده و برای هرکدام از این چالش‌ها، ابزارهای کاربردی را معرفی نماییم. در نهایت، برخی از این ابزارها را که بیشتر مورد استفاده قرار می‌گیرند، مورد بررسی اجمالی قرار خواهیم داد.

در این گزارش، ما قصد داریم موضوع امنیت حجیم‌داده را از سه منظر مختلف، یعنی ۱) ثبت وقایع یا لاگ فعالیت‌ها و اتفاقات در سامانه، ۲) نظارت بر کارکرد سامانه و ۳) کنترل دسترسی، مورد بررسی قرار دهیم و ابزارهایی برای هر کدام از این زمینه‌ها در محیط حجیم‌داده معرفی نماییم.

۱. مقدمه

با رشد روز افزون اطلاعات و نیاز افراد به جمع‌آوری و طبقه‌بندی آنها، تهدیدات مخربی که متوجه سامانه‌های اطلاعاتی (از جمله سامانه‌های حجیم‌داده) هستند نیز هر روز در حال افزایش است. برای نمونه، یکی از این تهدیدات، ورود غیرمجاز به سامانه اطلاعاتی است که مستلزم طراحی و راه‌اندازی سامانه‌های کنترل دسترسی می‌باشد. به دلیل رشد چشمگیر تعداد کاربران و همینطور حجم زیاد داده‌ها و پردازش‌های سنگین مربوط به آنها، هم اکنون هسته اصلی صنعت فن‌آوری اطلاعات مدرن را زیرساخت‌های تحت شبکه و توزیع شده تشکیل می‌دهند و امکان استفاده روزمره از خدمات آنلاین نظیر نرم‌افزارهای تحت وب، وب‌سایت‌های شرکت‌ها، پلتفرم‌های خرید آنلاین، خدمات به اشتراک گذاری ویدیو و هزاران سرویس دیگر را فراهم می‌آورند. ازکارافتادگی لحظه‌ای این سامانه‌ها، به عنوان یک تهدید امنیتی جدی، منجر به عدم دسترسی کاربران شده و در نتیجه خسارات مالی شدیدی به وجود می‌آورد. بنابراین، به سامانه‌های توزیع‌شده قابل اعتماد به ویژه در حوزه حجیم‌داده موردنیاز است.

به‌منظور اصلاح ساختار امنیتی سامانه‌های اطلاعاتی، داشتن یک راه‌حل امنیتی کامل که ساختار انواع تهدیدها را به‌طور کامل پوشش دهد، ضروری است. یکی از ارکان برقراری امنیت در سامانه‌های کامپیوتری امروزی، آگاه شدن برخط از فعالیت‌های در حال اجرا در کل سامانه از جمله در سطح میزبان، سرور، شبکه، پایگاه‌داده و ارتباطات مابین آن‌ها و همینطور شناخت فوری تهدیدات بالقوه و یا بالفعل آنها می‌باشد. این فرآیند معمولا توسط ابزارهای نظارت بر سامانه یا مانیتورینگ انجام می‌شود. این ابزارها به کشف هرچه سریعتر تهدید، خطا و یا نقص در سامانه (چه به صورت سهوی توسط افراد مجاز انجام گرفته باشد و چه به صورت عمدی در قالب نفوذ از طرف افراد غیرمجاز) کمک می‌کند. کشف به موقع این رویدادها از بروز هرچه بیشتر خسارت جلوگیری می‌کند.

در سامانه‌های حجیم‌داده، ابزارهای مانیتورینگ وضعیت لحظه‌ای سرورها و داده‌ها را جمع‌آوری و ذخیره می‌کنند که از طریق آن، مدیران و کارشناسان بتوانند اطلاعات کافی برای تشخیص وضعیت هر زیرسامانه و هشدارهای مربوط به اتفاقات روی داده در آنرا داشته باشند. همچنین این ابزارها اطلاعات مربوط به عملکرد هر یک از خدمات را با استفاده از داشبورد عملکرد خدمت جمع‌آوری کرده و آنها را از طریق رابط وب، نمایش می‌دهد.

۲. نظارت

نظارت بر سامانه‌های کامپیوتری یا اصطلاحا مانیتورینگ یک مؤلفه امنیتی بسیار ضروری می‌باشد. این نظارت به طور معمول شامل نصب نرم‌افزار مدیریت بر روی دستگاه یا مجموعه‌ای از دستگاه‌ها به صورت یکپارچه است که هشدارهایی را به مدیر سامانه درباره هرگونه تغییر وضعیت یا مشکلاتی که در دستگاه‌ها ممکن است رخ دهد، ارسال می‌کند. در حالی که اهمیت این سامانه‌ها به تنهایی ارزش نظارت مستقیم و پیوسته را دارد، عوامل دیگری چون امنیت، جمع‌آوری و تحلیل داده‌های سامانه و واکنش فعالانه در مقابل تهدیدات و مشکلات دلایل دیگری هستند که مانیتورینگ را ضروری می‌سازند.

یکی از مهم‌ترین دلایل نظارت بر سامانه این است که به یک مدیر سامانه اجازه می‌دهد تا به جای ماهیت انفعالی، حالت فعالی داشته باشد. برخی از شرکت‌ها تصمیم گرفتند از روش "break-fix" استفاده کنند و این بدان معنی است که اگر چیزی خراب شود، آن را رفع کنند. این منجر به طولانی شدن زمان خاموشی می‌شود که شرکت‌ها قادر به پرداخت هزینه‌ها و خسارات آن نیستند. نظارت فعال قبل از وقوع چیزی از طریق ارسال هشدار به مدیر سامانه کمک می‌کند و به وی امکان می‌دهد تا قبل از قطع شدن، مسئله را حل کنند. به عنوان مثال، نظارت ممکن است به یک مدیر سامانه هشدار دهد که یک هارد دیسک در یک سرور خراب شده است. مدیر سامانه از این امر آگاهی می‌یابد و دیسک تخریب‌شده را با یک نسخه جدید تعویض می‌کند. بدون نظارت، هارد دیسک تخریب شده می‌تواند به یک‌هارد دیسک بدون استفاده تبدیل شود که باعث توقف طولانی فعالیت و از دست رفتن اطلاعات احتمالی می‌شود.

یکی دیگر از مزایای نظارت، جمع آوری داده‌های تاریخی و زمان‌دار برای بهینه‌سازی مصرف منابع است، برای مثال در چه شرایطی چه سامانه‌های دارای بیشترین بار پردازش و یا حافظه هستند و کدامیک دارای کار کمتری هستند. این اطلاعات به یک مدیر سامانه اجازه می‌دهد تا عملکرد هر بخش از سامانه را مشاهده کند. این ویژگی می‌تواند در تصمیم‌گیری در مورد منابع اضافی یا مؤلفه‌هایی که برای اطمینان از یک سامانه مطمئن‌تر مورد نیاز هستند، کمک کند. نظارت بر سامانه کامپیوتری به همان اندازه خود سامانه اهمیت دارد. نظارت امکان پاسخگویی فعال، امنیت و جمع‌آوری داده‌ها و سلامت کلی سامانه را فراهم می‌آورد. در حالی که نظارت به تنهایی مشکلی را برطرف نمی‌کند اما منجر به پایداری و اطمینان بیشتر سامانه‌های می‌گردد.

۲-۱ کنترل دسترسی

داده‌های شرکت‌ها و سازمان‌ها از با ارزش‌ترین دارایی‌های آنها است. نهادها و کسب‌وکارهای مختلف می‌خواهند اطمینان حاصل کنند که داده‌های آنها در محلی امن و غیرقابل نفوذ ذخیره می‌شود. به همین دلیل، کارشناسان امنیت سخت تلاش می‌کنند تا اطمینان حاصل کنند که داده‌ها فقط توسط افراد صلاحیت‌دار و مجاز، که نیاز به آن اطلاعات دارند قابل دسترسی است. این کار با پیاده‌سازی نرم‌افزارهای امن و سامانه‌های سخت‌افزاری که این قابلیت را فراهم می‌کنند انجام می‌شود. با این حال، افرادی که تلاش می‌کنند بدون اجازه دسترسی به داده‌های یک شرکت دسترسی پیدا کنند، همیشه تکنیک‌های جدیدی را به کار می‌بندند که باید مداوم آنها را رصد و کنترل نمود. ابزارهای کنترل دسترسی به مدیر سامانه اجازه می‌دهد تا امنیت و محرمانگی داده‌های یک شرکت را تضمین کند. بسته به نوع نرم افزار کنترل دسترسی مورد استفاده، این نرم‌افزار می‌تواند اطلاعاتی در مورد تاریخچه دسترسی به فایل‌ها، عملیات انجام شده، نفوذ به شبکه و غیره ارائه دهد. داشتن این اطلاعات نه تنها به یک مدیر سامانه اجازه می‌دهد تا هرگونه نقص امنیتی فعلی را متوقف کند یا جلوی آنرا در آینده بگیرد.

۲-۲ انواع سامانه‌های نظارتی

سامانه‌های نظارتی در بالاترین سطح سامانه حجیم‌داده، برخی از ویژگی‌های امنیتی استاندارد را ارائه می‌دهند که می‌توان برای محافظت از داده‌ها و ماشین‌ها از آن‌ها استفاده کرد. در سطح سامانه و شبکه، مسائل امنیتی اکثراً یکسان است. در محیط کار تعدادی سامانه که به یک سرور متصل هستند را می‌توان به عنوان یک سامانه بزرگ چند وجهی تصور کرد. مدیر سامانه مسئولیت امنیت این سامانه یا شبکه را بر عهده دارد. نه تنها دفاع از شبکه در مقابل عوامل خارجی که سعی در دستیابی به شبکه دارند، مهم است بلکه اطمینان از یکپارچگی داده‌ها بر روی سامانه‌های درون شبکه نیز مهم است. به عنوان سرپرست سامانه، شما باید با آگاهی از کلیه جنبه‌های سامانه، از جمله اینکه بار عادی چقدر است؟ چه کسی به سامانه دسترسی دارد؟ چه زمانی افراد به سامانه دسترسی پیدا می‌کنند؟ و سوالات متعدد دیگر، فعالیت سامانه را کنترل کنید.

نظارت بر هر بخش ملزومات خاص خود را دارد و ابزارهای مختلفی برای نظارت بر بخش‌های مختلف طراحی شده‌اند که هر یک دانش خاصی را به کاربر می‌دهند. همینطور ابزارهایی برای ایجاد سامانه حسابرسی و نظارت بر فعالیت‌های کاربران طراحی شده‌اند و اجازه دسترسی آنها را به منابع مختلف منوط به داشتن مجور می‌کنند.

۲-۲-۱ نظارت لاگ

مدیریت ثبت وقایع رخ داده یا همان لاگ (log) در سامانه‌های نرم‌افزاری و سخت‌افزاری مختلف و تجزیه و تحلیل آن جزو وظایف مهم واحد مانیتورینگ است. می‌توان گفت که تمامی سامانه‌ها و برنامه‌های کاربردی امروزی که این روزها از آنها استفاده می‌شود، به نوعی قادر به تولید فایل‌ها یا پرونده‌های لاگ هستند که در مورد اتفاقات و فعالیت‌های رخ داده در سامانه، هشدارها، خطاها و پیام‌های مهمی که باید به آنها توجه شود، به صورت لحظه‌ای اطلاع می‌دهند. میزان این لاگ‌های تولید شده به ویژه در سیستم‌های مقیاس بزرگ اینترنتی و یا حجیم‌داده به قدری زیاد است که عملا به عنوان معضلی برای مدیران یا ناظران مطرح است، به گونه‌ای که بازبینی کلیه این داده‌ها بصورت روزانه برای کارشناسان وجود ندارد.

۲-۲-۲ نظارت نرم‌افزار

گسترش استفاده از نرم‌افزارها در سازمان‌ها به ویژه در راهکارهای مبتنی بر اینترنت و ابر (Cloud)، نیاز به پایش و نظارت نرم افزار را بسیار ضروری می‌سازد تا در هر لحظه مطمئن باشیم که نرم افزارها در حال کار و انجام عملکرد صحیح می‌باشند. استفاده از راهکارهای نظارت نرم افزاری، عملکرد آنرا به صورت لحظه‌ای کنترل نموده و زمان بازیابی نرم‌افزار را کاهش می‌دهد و همچنین امکان نظارت بدون نیاز به عامل انسانی را فراهم می‌نماید. این راهکارها، به سادگی با نصب و پیکربندی ابزارها استفاده می‌شوند. گفتنی است از این نوع نظارت می‌توان برای پایش پارامترهای سیستمی نظیر میزان بار کاری پردازنده، میزان حافظه آزاد و یا مشغول، کارکرد صحیح سیستم‌عامل و غیره نیز بهره برد.

شکل۱: نظارت نرم افزار

از قابلیت‌های نظارت نرم‌افزار می‌توان به موارد زیر اشاره نمود:

- نظارت و پیکربندی اتوماتیک نرم‌افزارها در محیط‌های مجازی‌سازی و مبتنی بر ابر
- تنظیم نظارت پارامترها و حسگرها به صورت پویا: می‌توان پارامترهای حساس و کنتورهای مختلف جهت ارزیابی آنها را به صورت پویا تعریف نمود و بر اساس اطلاعات مانیتور شده تغییر داده و کنترل نمود.
- راه‌اندازی سریع: در کمتر از ۶۰ دقیقه پس از نصب راهکار و به روزرسانی ابزارهای آن، سرویس‌دهی آغاز می‌گردد.
- تنوع پارامترها و نرم افزارهای مورد پشتیبانی از کمپانی‌های مختلف: میزان مصرف منابع، زمان پاسخگویی، میزان استفاده از نرم‌افزار و پایداری نرم‌افزار بر روی هاست‌های مختلف و پلتفرم‌های نرم افزاری مختلف شامل Cisco، Citrix، Microsoft ، Oracle ، SAP، Siebel و ..... را نظارت می‌کنند.

۲-۲-۳ نظارت شبکه

نقش شبکه‌های کامپیوتری در ایجاد و تسهیل کسب‌وکارهای امروزی نیازی به توضیح ندارد و بالتبع، هرگونه از کارافتادگی شبکه در سازمان‌ها به معنی از کارافتادگی فرآیندهای اصلی می‌باشد. پایش لحظه‌ای شبکه و اطمینان از صحت و سلامت اجزاء و نمایش نحوه ارتباطات مابین اجزاء شبکه و اطمینان از پیکربندی اجزاء در شبکه، همگی از پارامترهای مهم و مورد نیاز مدیران فنی می‌باشند. عملیات نظارت شبکه می‌بایست به صورت خودکار و لحظه ای صورت بگیرد و علاوه بر توانایی شناسایی اجزاء شبکه، امکان بررسی صحت و سلامت و چک نمودن تنظیمات اجزآء را فراهم نماید. در کنار این مورد، بسیاری از ابزارهای نظارت نیز خود به صورت شبکه‌ای فعالیت می‌کنند، بدین معنی که نرم‌افزارهای مجزا به اسم عامل (agent) به صورت توزیع شده بر روی دستگاه‌های مختلف نصب می‌شوند و اطلاعات مربوط به وضعیت دستگاه‌ها را به صورت شبکه‌ای به یک سرور مرکزی ارسال می‌کنند.

۳. سامانه‌های مدیریت لاگ

۳-۱ مقدمه

همانطور که قبلا نیز گفته شد، یکی از بخش‌های مهم نظارت، مدیریت لاگ در سامانه‌های نرم‌افزاری و سخت‌افزاری مختلف و تجزیه و تحلیل آنها می‌باشد، به ویژه آنکه امروزه تمامی سامانه‌ها و برنامه‌های کاربردی به صورت لحظه‌ای و در حجیم زیاد در حال تولید فایل‌های لاگ هستند. روال تولید و رسیدگی لاگ در سامانه‌های مختلف متفاوت است. برای مثال در سامانه‌های اینترنتی، این روال از شروع درخواست کاربر تا پاسخ‌گویی ادمین شامل موارد ذیل است:

۱. ارسال درخواست کاربر به سامانه
۲. پاسخ سامانه به درخواست کاربر
۳. ایجاد لاگ
۴. ارسال لاگ برای سامانه نظارت
۵. آنالیز کردن فایل‌های لاگ و ایجاد هشدار
۶. پاسخ ادمین به هشدار داده شده

در نهایت، ابزارها و تکنولوژی‌هایی که بتوانند به بهترین وجه این فایل‌های لاگ تولید شده در سامانه را جمع‌آوری کرده و پردازش نمایند و در ضمن، ارتباط بین این اطلاعات را برقرار نموده و در نهایت به درستی ایجاد هشدار نمایند به عنوان تکنولوژی مناسب جهت استفاده در سامانه نظارت شناخته می‌شوند. انواع سامانه‌هایی که در جمع‌آوری و پردازش فایل‌های لاگ استفاده می‌شود شامل موارد زیر می‌باشد:

۱. سامانه‌های صرفا جمع‌کننده داده لاگ که اطلاعات را از سامانه‌های مختلف جمع آوری کرده و نگهداری می‌کنند.
۲. سامانه‌هایی که لاگ‌های جمع آوری شده را پردازش نموده و به صورت گرافیکی نمایش می‌دهند. از جمله این سامانه‌ها می‌توان به نرم‌افزارهای SolarWinds و PRTG اشاره کرد.
۳. سامانه‌های نظارت که علاوه بر جمع آوری اطلاعات و پردازش آنها ارتباط بین لاگ دستگاه‌های مختلف را با هم برقرار می‌کنند. از جمله این سامانه‌های می‌توان به Cisco MARS اشاره نمود.
۴. سامانه‌های پاسخ سریع به اتفاقات رخ داده در سیستم نظیر Trap و Syslog
۵. سامانه‌های جمع‌کننده لاگ که بر اساس داده‌های دریافت شده تصمیم‌گیری و اقدام نیز می‌نمایند، مانند سامانه‌های IDS/IPS

همچنان که اهمیت و مزایای استفاده از سامانه‌های جمع‌آوری و مدیریت لاگ بر کسی پوشیده نیست، این موضوع چالش‌های مخصوص به خود را نیز دارد. برای مثال، مدیریت و نگهداری انبوهی از لاگ‌ها (به ویژه در سیستم‌های مقیاس بزرگ اینترنتی و حجیم‌داده)، تحلیل حجم

عظیمی از رویدادها و بررسی دستی و زمانبر آنها، تشخیص و رسیدگی به هشدارهایی که اشتباه تشخیص داده شده‌اند، درک و سازگاری فرمت‌های مختلف لاگ‌ها و نیازمندی‌های سازمان در حوزه رگولاتوری، همه راهکارهای مناسبی را طلب می‌کنند.

۳-۲ معرفی سامانه‌های مدیریت لاگ

تاکنون ابزارهای مدیریت لاگ متعددی طراحی و ارائه شده‌اند که در این بخش به تعدادی از معروف‌ترین آنها اشاره می‌کنیم. اگرچه همه این ابزارها به نوعی کار یکسانی انجام می‌دهند، لیکن نمی‌توان یک معیار ارزیابی یکسان برای مقایسه آنها و انتخاب بهترین ابزار در نظر گرفت، زیرا هر کدام از این ابزارها برای کارکرد و محیط مشخصی طراحی شده‌اند و دارای عملکرد بهتری در برخی زمینه‌ها هستند در حالیکه ممکن است در زمینه‌های دیگر چندان قدرتمند نباشند. به طول کلی، ابزارهای معرفی شده در این قسمت را می‌توان به دسته‌های محصولات مبتنی بر رایانش ابری، محصولات منبع باز، محصولات جمع‌آوری کننده لاگ و محصولات تحلیل لاگ یا تلفیقی از این موارد تقسیم‌بندی نمود. بیشتر ابزارهای کنونی خدمات خود را بر بستر ابری ارائه می‌دهند.

۳-۲-۱ Logentries

یک بستر مدیریت لاگ مبتنی بر رایانش ابری است که باعث می‌شود هر نوع از داده‌های لاگ ایجاد شده با هر اندازه در دسترس توسعه‌دهندگان، مهندسان فناوری اطلاعات و گروه‌های تحلیل داده باشد. روند آسان کار با این ابزار تضمین می‌کند که هر تیم تجاری بتواند به سرعت و به طور موثر از آن استفاده کند. این بستر به طور خودکار تمام داده‌های لاگ را با هر قالب در یک مکان امن جمع‌آوری و متمرکز می‌کند، جایی که می‌توان داده‌های لاگ را جستجو و جمع‌آوری کرده و یا آنها را تحلیل نموده و نتایج تحلیل را نمایش داد. هنگامی که مشکلی رخ می دهد، نمایش لحظه‌ای را برای دیدن آنچه برای لاگ‌ها اتفاق می‌افتد در هر زمانی فراهم می‌آورد. از آنجا که بستر به صورت پویا مقیاس‌پذیر است، مولفه‌های جدید می‌توانند به راحتی پیکربندی شوند تا تمام لاگ‌ها را در زمان بلادرنگ به آن ارسال کنند. این بستر امکان تجزیه و تحلیل قدرتمند و کامل لاگ‌ها را با سهولت استفاده ادغام می‌کند. به توسعه‌دهندگان و تحلیل‌گران تجاری اجازه می‌دهد تا به سرعت و به‌راحتی بینش عملی را از داده‌های گزارش بدست آورند. مورد اعتماد مشتریان در سرتاسر جهان است و هر روزه میلیاردها رخداد مربوط به لاگ را تجزیه و تحلیل می‌کند[۱].

مزایا:

- بارگذاری، ذخیره‌سازی، جستجو و نظارت در محیط آنلاین و بلادرنگ
- مقیاس پذیری پویا برای انواع زیرساخت‌های مختلف با اندازه‌های متنوع
- تجزیه و تحلیل بصری جامع از روند داده‌ها
- ارائه انواع تکنیک‌های تحلیل داده بر پایه داده‌کاوی و یادگیری ماشین
- هشدارهای سفارشی‌سازی‌شده و گزارش‌های مربوط به پرس‌وجوهای از پیش تعریف‌شده
- ویژگی‌های امنیتی مدرن برای محافظت از داده‌ها

- امکان ادغام و یکپارچه شدن کامل با ابزارهای گفتگو و ابزارهای مدیریت عملکرد
- ارسال گزارش‌ها از طریق ایمیل
- پشتیبانی از مجموعه متنوعی از زبان‌های برنامه نویسی
- رایگان تا ۵ گیگابایت
- مستندسازی و مستندات کامل و عالی

معایب:

- چالش‌ها و محدودیت‌های مربوط به رایانش ابری
- بارگذاری و مدیریت منابع لاگ به صورت غیرخودکار
- عدم شناسایی و دنبال کردن خطاها در کتابخانه‌ها و کدهای ثالث
- دارای محدودیت برای تعداد لاگ‌ها در هر سرور
- عدم وجود گزارش‌گیری مجزا برای زبانهایی نظیر جاواسکریپت
- عدم امنیت کافی در برخی کلاینت‌های وب

۳-۲-۲ GoAccess

یک نرم افزار تحلیل لاگ آنلاین (برخط) منبع‌باز است که از طریق ترمینال سیستم‌های مبتنی بر یونیکس یا لینوکس یا از طریق مرورگر اجرا می‌شود. این ابزار یک محیط ذخیره و پردازش لاگ سریع برای درخواست‌های وب (ارسالی به وب‌سرورها) فراهم می‌کند که می‌تواند حجم زیادی از داده‌های وب را در عرض چند ثانیه در سرور ذخیره می‌کند.

برنامه تحلیل لاگ اطلاعات را از لاگ وب‌سرور به صورت آنلاین دریافت نموده و امکان تجزیه، تحلیل و مشاهده لاگ‌های موجود در سرور را به سرعت و از طریق مرورگر وب میسر می‌سازد. همچنین گزارش‌های آماری مختصر و مفید وب‌سرور را برای مدیران ارائه می‌دهد. این برنامه قابلیت کار با وب‌سرورهای Apache و Ngnix را به صورت مستقیم دارد. به عبارت دیگر، گزارش‌های وب‌سرور شما را پردازش می‌کند و بر اساس نیاز شما، گزارش‌های کاربردی را در قالب‌های HTML، JSON یا CSV ایجاد می‌کند[۲].

مزایا:

- بروزرسانی داده‌های لاگ به صورت آنلاین و برخط در عرض چند میلی‌ثانیه
- قابلیت شخصی‌سازی قالب لاگ‌ها
- نظارت بر زمان پاسخ صفحات جستجو و پردازش
- پیکربندی آسان؛ به راحتی فایل یا پوشه لاگ خود را انتخاب کرده و برنامه را اجرا کنید

- مشاهده اطلاعات و آمار بازدیدکنندگان وب سایت به صورت آنلاین
- پردازش و جمع‌آوری لاگ بر اساس معیارهای مختلف مانند مکان جغرافیایی، مرورگر، سیستم‌عامل و غیره

۳-۲-۳ Logz.io

Logz.io یک پلتفرم نرم‌افزاری مبتنی بر رایانش ابری برای جمع‌آوری و تحلیل لاگ است که از روش‌های مختلف یادگیری ماشین و تحلیل پیش‌گویانه برای ساده کردن فرآیند یافتن رویدادهای مهم و داده‌های تولید شده توسط لاگ‌های مربوط به برنامه‌ها، سرورها و محیط‌های شبکه استفاده می‌کند. پلتفرم Logz.io با کمک پشته معروف ELK ساخته شده است (Elastic, Logstash, Kibana). این پلتفرم، امکان استخراج دانش و اطلاعات آنلاین را از لاگ‌هایی که کاربران در سامانه بارگذاری می‌کنند به راحتی فراهم می‌کند. کاربران می‌توانند هشدارهایی را برای پیام‌های گزارش ایجاد کرده و از طریق ایمیل یا یک برنامه پیام‌رسانی مطلع شوند. Logz.io قابلیت تحلیل خودکار را با لاگ‌های مربوط به نرم‌افزارهای مختلف نظیر MySQL، MongoDB ، HAProxy و Nagios فراهم می‌کند. همچنین به کاربران اجازه می‌دهد تا نتایج تحلیل و داشبورد را با اعضای تیم به اشتراک بگذارند و مدیر می‌تواند مجوز دسترسی اعضای تیم را برای دسترسی به داده‌ها مدیریت کند[۳].

مزایا:

- از پشته قدرتمند ELK به عنوان سرویس‌دهنده استفاده می‌کند و تجزیه و تحلیل لاگ‌ها را در فضای ابر انجام می‌دهد
- تجزیه و تحلیل شناختی، وجود رویدادها لاگ‌های مهم را قبل از ایجاد آنها، بررسی می‌کند
- پیکربندی و راه‌اندازی سریع
- مقیاس‌پذیری پویا که می‌تواند خود را با انواع کاربردها وفق دهد
- محافظت از داده‌های لاگ و نتایج تحلیلی، برای اطمینان از ایمن بودن و حفاظت بیشتر اطلاعات و داده‌های کاربران
- اشتراک‌گذاری نتایج

معایب:

- وجود محدودیت در تعداد پیام‌های گزارشات و یا رویدادهای کشف شده
- عدم قابلیت اعمال فیلترها در واسط گرافیکی پیش از انجام پرس‌وجو

۳-۲-۴ Graylog

یک پلتفرم قدرتمند مدیریت لاگ رایگان و منبع‌باز است که از مجموعه جامع و کاملی از ابزارهای جمع‌آوری و تحلیل لاگ پشتیبانی می‌کند. این پلتفرم به شما این امکان را می‌دهد که با استفاده از تعریف قوانین و اعمال آنها بر روی داده به درک علت اصلی هرگونه خطا یا مشکلی خاص که برنامه‌هایتان با آن روبرو هستند، برسید. این نرم‌افزار به زبان جاوا نوشته شده است و رابط وب آن با Ruby نوشته شده است. موتور ذخیره‌سازی آن بر پایه الاستیک‌سرچ می‌باشد و قادر به ذخیره‌سازی صدها ترابایت داده در یک پیکربندی توزیع شده می‌باشد. این پلتفرم جزو نرم‌افزارهای

محبوب تحلیل لاگ به حساب می‌آید که تاکنون بیش از ۳۵ هزار نسخه از آن در سراسر دنیا نصب شده است. نسخه ابری این محصول نیز در دسترس می‌باشد. این ابزار آمار داده‌های جمع‌آوری شده از منابع مختلف را برای ساده‌سازی نمایش در صفحه اصلی داشبورد نمایش می‌دهد و همچنین امکان تنظیم شرایط هشدارهای منابع داده و رخدادها را فراهم می‌کند. می‌توان با تغییر فیلترها و دانه‌بندی، اطلاعات و سوابق مفصلی از لاگ‌ها را مشاهده نمود. این باعث می شود که ابزار فوق به یک ابزار داده کاوی تبدیل شود[۴].

مزایا:

- پردازش لاگ‌های مربوط به سیستم با استفاده از الگوریتم‌های پردازش جامع
- جستجو در میان حجم بالای داده‌ها برای یافتن نتایج مورد انتظار
- داشبورد قابل سفارشی‌سازی برای خروجی بصری داده‌های قابل نمایش
- هشدارها و اعلان‌های سفارشی برای نظارت بر خرابی داده‌ها
- سیستم مدیریت متمرکز برای اعضای تیم
- مدیریت مجوزهای دسترسی سفارشی برای کاربران و نقش آنها
- در قیاس با GoAccess، کارایی و محبوبیت بیشتری برای کار با حجم زیاد داده دارد

۳-۲-۵ Splunk

این پلتفرم از قدیمی‌ترین و محبوب‌ترین پلتفرم‌های ذخیره‌سازی و تحلیل لاگ است که خدمات لاگ خود را به مشتریان سازمانی که نیاز به ابزاری کارآمد و آسان برای جستجو، تشخیص و گزارش هرگونه رویداد در حوادث موجود در لاگ دارند، معطوف می‌کند. نرم افزار Splunk برای پشتیبانی از فرآیند نمایه‌گذاری و رمزگشایی انواع لاگ‌های ساخت‌یافته یا غیرساخت‌یافته و همینطور لاگ انواع برنامه‌های کاربردی طراحی شده است. در این ابزار نسخه‌های متفاوتی وجود دارد که Splunk در اختیار شما قرار می‌دهد (برای مثال، سازمانی و ابری) که کاربری‌های متفاوت را در قالب نسخه‌های مختلف ارائه می‌دهند. نسخه سازمانی کمک می‌کند تا اطلاعات و دانش عملیاتی و کاربردی با ارزشی را از اطلاعات با ارزش موجود در سامانه‌های سازمان بدست آورده و با طیف گسترده‌ای از ابزارهای جستجوی قدرتمند، بصری‌سازی و مدل‌های از پیش تعریف‌شده، هر کاربر می‌تواند به سرعت اطلاعات و دانش موردنیاز خود را کشف و به اشتراک بگذارد. همچنین دارای قابلیت گزارش‌گیری داخلی بوسیله نمودارها و داشبوردهای پیشرفته و رابط کاربری مناسب برای تولید گزارش‌های بصری است. نسخه سازمانی آن با پلتفرم‌های مختلفی از جمله Microsoft Excel، Tableau، Okta، PingFerderate، Azure AD، CA SiteMinder، OneLogin و Optimal IdM یکپارچه می‌شود. خدمات ابری آن نیز به صورت گسترده مورد استفاده قرار می‌گیرد[۵].

مزایا:

- توانایی ذخیره‌سازی و پردازش حجم زیادی از داده‌ها به صورت برخط

- درک و پردازش انواع داده‌های تولید شده توسط ماشین (داده‌های به دست آمده از منابعی مانند سرورها، سرورهای وب، شبکه‌ها، تبادلات داده‌ای، سرورهای اصلی، دستگاه های امنیتی و غیره)
- رابط کاربری انعطاف‌پذیر برای جستجو و تجزیه و تحلیل داده‌ها آنلاین
- الگوریتم‌های مناسب برای یافتن ناهنجاری‌ها و الگوهای آشنا در فایل‌های لاگ
- سیستم نظارت و پایش و به همراه روش‌های کارای هشداردهی برای آگاهی به‌موقع از وقایع و اتفاقات مهم
- گزارش تصویری (بصری) با استفاده از خروجی داشبورد

۳-۲-۶ Sumo Logic

یک پلتفرم یکپارچه برای جمع‌آوری و پردازش لاگ در محیط رایانش ابری است که به کاربران کمک می‌کند تا داده‌های خود را به صورت آنلاین با استفاده از الگوریتم‌های یادگیری ماشین تجزیه و تحلیل نمایند. این ابزار می‌تواند به سرعت علت اصلی هر خطا یا رویداد خاص را به تصویر بکشد و همچنین می‌تواند با تنظیمات مناسب به طور مرتب آنچه در برنامه‌های شما در زمان واقعی اتفاق می‌افتد را رصد کند. نکته برجسته این ابزار، کار با داده‌ها با سرعت بالا، رفع نیاز به تجزیه و تحلیل داده‌های خارجی و ابزارهای مدیریت است. همچنین به شما امکان می‌دهد تا هشدارها و اعلان‌های ایمیل ایجاد کنید، مانند شناسائی خرابی، هک‌ها و غیره. Sumo Logic یک نسخه رایگان نیز ارائه می‌دهد که به شما امکانات محدودی می‌دهد اما امکان بروزرسانی را دارد[۶].

مزایا:

- پلتفرم یکپارچه برای جمع‌آوری لاگ‌ها از نرم‌افزارهای مختلف
- تجزیه و تحلیل پیشرفته با استفاده از یادگیری ماشین و الگوریتم‌های پیش‌بینی
- راه‌اندازی سریع
- کاربری آسان و ادغام با پلتفرم‌های رایانش ابری
- اشتراک‌گذاری خدمات و نتایج مابین کاربران

۳-۲-۷ Papertrail

یک سرویس مدیریت لاگ مبتنی بر رایانش ابری است که از تجمیع، جستجو و تجزیه و تحلیل انواع فایل‌های لاگ، لاگ‌های مربوط به سیستم یا فایل‌های لاگ متنی، استفاده می‌کند. ویژگی‌های پردازش آنلاین آن به توسعه‌دهندگان و مهندسان این امکان را می‌دهد که اتفاقات زنده را درون برنامه‌ها و سرورها در هنگام وقوع مشاهده کنند. همچنین یکپارچه سازی جامعی را با خدماتی مانند Slack، Librato و Email ارائه می‌دهد تا به کاربران برای ایجاد اعلان‌ها و هشدارهای مربوط به رخدادها و هرگونه ناهنجاری کمک کند. علاوه بر این، به دلیل اجرای بسیار آسان

شناخته می‌شود و مجموعه گسترده‌ای از ویژگی‌ها / ابزارهای اضافی را برای مدیریت لاگ در اختیار شما قرار می‌دهد. چیز دیگری که آنها موفق به توجه به آن شده‌اند، امکان مقیاس‌پذیری برای صدها سرور است[۴۳].

مزایا:

- رابط‌کاربری ساده و کاربرپسند
- نصب و کاربری آسان در جمع‌آوری لاگ‌ها
- رویدادها و جستجوی لحظه‌ای و آنلاین
- جستجوی پیشرفته متنی (جستجو در پیام‌ها، فراداده و زیررشته‌ها)
- نمایش نمودار با ابزارهایی مانند Librato، Geckoboard، یا ابزارهای مورد نظر کاربران

۳-۲-۸ Fluentd

این نرم‌افزار یک نوع جمع‌آوری کننده لاگ حرفه‌ای و قدرتمند است که در حجیم‌داده مورد استفاده قرار می‌گیرد. حوادث و رخدادها را از منابع مختلف داده جمع‌آوری می‌کند و آنها را در قالب‌های فایل‌های متنی، RDBMS، NoSQL، IaaS، SaaS، Hadoop و غیره می‌نویسد. این ابزار به شما کمک می‌کند تا زیرساخت‌های جمع‌آوری لاگ را با رغم ورودی و خروجی‌های مختلف، یکپارچه و یکسان کنید. ویژگی مهم این ابزار یک کتابخانه توسعه‌یافته است که هرگونه عملیات و کاربری درباره لاگ و مدیریت داده‌ها در یک محیط توسعه دهنده را فراهم و پشتیبانی می‌کند. این ابزار می‌تواند جریان‌های داده زنده را برای ایجاد فایل‌های لاگ و همچنین نظارت و مدیریت فایل‌های موجود جمع‌آوری کند. یکی از منابع داده‌ای که این ابزار برای مدیریت آن نوشته است، لاگ‌های وب‌سرور Apache است. این نرم‌افزار جمع کننده جریان داده منبع‌باز در محصولات صدها شرکت بزرگ از جمله Nintendo و Slideshare استفاده می‌شود. Fluentd جمع‌آوری و ذخیره داده‌های لاگ را از بسیاری از منابع و جریان‌های داده‌ای آسان می‌کند[۷].

مزایا:

- یکپارچه‌سازی لایه ورود داده و لاگ که می‌تواند داده‌ها را از چندین منبع جدا تهیه و جمع‌آوری کند
- تبدیل لاگ‌های غیر ساخت‌یافته به لاگ‌های ساخت‌یافته
- انعطاف پذیر، اما ساده
- سازگار با اکثر منابع داده امروزی

۳-۲-۹ Syslog-ng

یک ابزار جمع‌آوری کننده لاگ منبع‌باز است که به مهندسان و توسعه‌دهندگان کمک می‌کند تا داده‌های لاگ را از طیف گسترده‌ای از منابع جمع‌آوری نموده تا آنها را پردازش کرده و در نهایت به یک ابزار تجزیه و تحلیل تحویل دهند. با این ابزار می‌توان داده‌های لاگ را از انواع پشته‌های

داده جمع‌آوری، طبقه‌بندی و یکپارچه کرد و بعد از اعمال یکسری قوانین فیلترسازی (مبتنی بر محتوای و یا فراداده) آن را به سمت تجزیه و تحلیل سوق داد. همچنین دارای انتقال و ذخیره‌سازی امن داده‌ها، معماری مقیاس‌پذیر، مسیریابی انعطاف‌پذیر لاگ‌ها، تبدیلات و موارد دیگر است. این ابزار در نسخه‌های منبع باز رایگان و سازمانی در دسترس است[۸].

مزایا:

- منبع‌باز با تعداد زیادی منبع و استفاده‌کننده
- مقیاس‌پذیری انعطاف‌پذیر با هر زیرساخت و اندازه داده
- قابلیت فیلترسازی لاگ بر اساس محتوی و فراداد
- پشتیبانی از افزونه‌های مختلف برای قابلیت‌های اضافی و توسعه‌یافته
- استفاده از ابزار مناسب برای یافتن الگوهای ثابت موجود در لاگ
- ذخیره داده‌ها در پایگاه داده‌های موجود و اشتراکی

۳-۲-۱۰ Rsyslog

این ابزار یک نرم‌افزار منبع‌باز سریع و مطمئن برای جمع‌آوری، فیلترسازی و انتقال لاگ از منابع مختلف به مصرف‌کننده‌های مختلف است و از این منظر رقیب ابزار syslog-ng می‌باشد. این ابزار معیارهای عملکردی بالا در مواجهه با نرخ بالای ورود داده، ویژگی‌های امنیتی قدرتمند و طراحی ماژولار را برای تغییرات سفارشی ارائه می‌دهد. همچنین قابلیت توسعه و رشد از یک مجموعه لاگ جداگانه تا لاگ‌های مربوط به طیف وسیعی از منابع لاگ را دارا می‌باشد و در مرحله بعد عملیات مرتب‌سازی و یکپارچگی را انجام می‌دهد، که می‌تواند پس از آن خروجی یکپارچه از لاگ‌ها را برای استفاده در نرم‌افزار اختصاصی تجزیه و تحلیل لاگ فراهم کند[۹].

مزایا:

- کاربری آسان در محیط مبتنی بر وب
- امکان ساخت روش‌های پارس و تجزیه سفارشی
- امکان پیکربندی و عملکرد آنلاین
- استفاده از عبارات منظم بر فیلترسازی مبتنی بر محتوی و فراداده
- قابلیت توسعه سفارشی برای انجام کارهای خاص

۳-۲-۱۱ Logalyze

یک سیستم جمع‌آوری و تجزیه و تحلیل لاگ ساده با هزینه‌های عملیاتی کم و به صورت سیستم متمرکز است و قادر به جمع‌آوری داده‌های لاگ از منابع گسترده سیستم‌های اجرایی و عملیاتی (نرم‌افزارها و سخت‌افزارهای مختلف) است. این ابزار با پیش‌بینی دقیق وقایع به صورت برخط

و آنلاین به مدیر سیستم و پرسنل مدیریتی ابزارهای مناسبی برای نمایه‌سازی و جستجوی انبوه داده‌ها می‌دهد. علاوه بر این امکان تعامل با کاربران و نمایش نتایج را در قالب‌های مختلف فراهم می‌آورد[۱۰].

مزایا:

- پردازش لاگ‌ها با کارایی و سرعت بالا
- استخراج رویدادهای مختلف از لاگ و اعلام هشدار
- پارس انواع لاگ ورودی و نمایه‌سازی برای جستجو
- داشبورد کاربری یکپارچه برای دسترسی آنلاین
- انتقال امن داده‌ها
- گزارش خودکار به صورت PDF
- سازگار با نرم‌افزارهای دیگر مدیریت لاگ نظیر Syslog و Rsyslog
- تقسیم‌بندی لاگ‌ها به بخش‌ها و نام‌گذاری مجزای هر بخش

۳-۲-۱۲ Loggly

این سرویس مدیریت لاگ، مبتنی بر رایانش ابری است که برای کاربران متنوع چه مبتدیان و چه توسعه دهندگان با تجربه توصیه می‌شود. این ابزار می‌تواند به صورت آنلاین مهمترین اطلاعات، رویدادها و روندها را از طریق پردازش لاگ برای کاربران استخراج کند. محیط جمع‌آوری لاگ آن به نحوی است که می‌توان از استانداردهای سنتی مانند HTTP و Syslog استفاده کرد. داشبورد آن بسیار کاربرپسند است و در طی مدت کوتاه از شروع استفاده از آن برای نظارت بر لاگ موردنظر، می‌توان فهمید که در هر زمان در سامانه چه می‌گذرد. این یک نوع سامانه نظارت بر گزارش مستقیم " از لاگ خام تا نمایش بصری" است[۱۱].

مزایا:

- شناسائی و جمع‌آوری لاگ‌های متنی از منابع مختلف
- تجزیه و تحلیل خودکار لاگ‌های مربوط به نرم‌افزارهای نظیر Apache، Nginx و غیره
- امکان یافتن و برچسب‌گذاری خودکار خطاهای مرتبط با داده‌های لاگ
- الگوریتم جستجوی توانمند برای انجام جستجوی پیشرفته بر روی ترکیبی از فیلدها
- داشبورد تجزیه و تحلیل داده‌ها برای نمایش بصری از داده‌های لاگ

۳-۲-۱۳ Logstash

یکی از پرکاربردترین ابزارهای جمع‌آوری کننده لاگ است که به صورت منبع‌باز، رایگان و متمرکز (بر روی یک سرور) ارائه می‌شود. این ابزار بخشی از پشته معروف ELK (ElasticSearch, Logstash, Kibana) است که شاید بیش از هر پلتفرم دیگری برای مدیریت لاگ مورد استفاده قرار گرفته باشد (شکل ۱). این ابزار بر اساس الگوهای فیلتر/لوله طراحی شده و برای جمع‌آوری، پردازش و تولید لاگ‌ها یا رویدادها تهیه شده است. این امر در متمرکز ساختن و یکپارچه کردن لاگ‌ها از منابع مختلف، در زمان بلادرنگ موثر است.

شکل ۲: پشته ELK

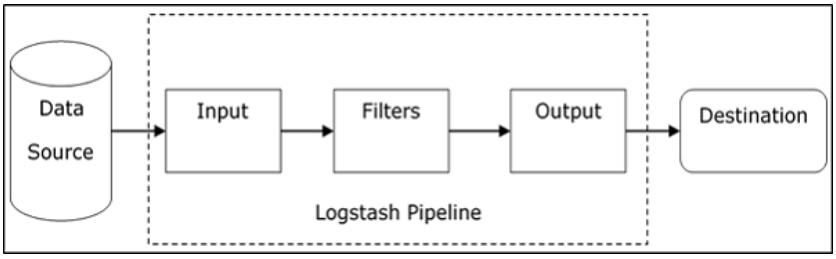
Logstash با زبان برنامه نویسی JRuby که روی JVM اجرا می‌شود، نوشته شده است. از این‌رو می‌توان آن را بر روی سیستم‌عامل‌های مختلف اجرا کرد. این ابزار داده‌ها را تقریباً از هر نوع منبع مختلف مانند لاگ‌ها، بسته‌ها، رویدادها، معاملات، داده‌های زمان‌دار و غیره جمع‌آوری می‌کند. منبع داده می‌تواند داده‌های اجتماعی، تجارت الکترونیکی، مقالات خبری، CRM، داده‌های بازی، درخواست وب، داده‌های مالی، اینترنت اشیاء، دستگاه‌های تلفن همراه و غیره باشد[۱۲].

مزایا:

- اجرای سبک و ساده
- توانایی جمع‌آوری لاگ در نرخ بالا و تبدیل آن به قالب‌های مختلف
- جمع‌آوری داده از منابع مختلف و فروارد به مقصدهای مختلف
- پشتیبانی پیش‌فرض از انواع داده‌های لاگ مانند لاگ Apache، لاگ رویدادهای ویندوز، داده‌های مربوط به پروتکل‌های شبکه، داده‌های ورودی استاندارد و موارد دیگر
- پارس خودکار درخواست‌ها و پاسخ‌های http
- اعمال فیلترهای متنوعی بر روی داده
- شناسائی رویدادها از طریق توالی‌های الگوی regex

۳-۲-۱۳-۱ مفاهیم اصلی Logstash

همانطور که شکل زیر نشان می‌دهد، تعدادی مولفه کلیدی در Logstash حضور دارند که در ادامه، هر یک را مختصرا توضیح می‌دهیم[۱۲].



شکل ۳: فرآیند کلی Logstash

۳-۲-۱۳-۱-۱ شیء رویداد

این شیء اصلی در Logstash است که جریان داده‌ها را در خط لوله Logstash کپسوله می‌کند. Logstash از این شیء برای ذخیره داده‌های ورودی و اضافه کردن فیلدهای اضافی ایجاد شده در مرحله فیلتر، استفاده می‌کند.

Logstash یک API برای کار با رویداد به توسعه‌دهندگان ارائه می‌دهد. معمولا این رویدادها با نام‌های مختلفی مانند Logging Data Event ، Log Event، Log Data، Input Log Data، Output Log Data و غیره معرفی می‌شوند.

۳-۲-۱۳-۱-۲ خط لوله

خط لوله شامل مراحل جریان داده در Logstash از ورودی به خروجی است. داده‌های ورودی در خط لوله وارد شده و در قالب یک رویداد پردازش می‌شوند. سپس به عنوان خروجی، در فرمت مطلوب به سیستم نهایی ارسال می‌شود.

۳-۲-۱۳-۱-۳ ورودی

ورودی، اولین مرحله در خط لوله Logstash است که برای تهیه داده‌ها و پردازش بیشتر استفاده می‌شود. Logstash افزونه‌های مختلفی را برای دریافت داده از سیستم عامل‌های مختلف ارائه می‌دهد. برخی از متداول‌ترین پلاگین‌ها عبارتند از: File، Syslog، Redis و Beats.

۳-۲-۱۳-۱-۴ فیلتر

فیلتر، مرحله میانی Logstash است، جایی که پردازش واقعی رویدادها صورت می‌گیرد. یک توسعه‌دهنده می‌تواند از الگوهای از پیش‌تعریف شده Regex یا همان عبارات منظم، توسط Logstash استفاده کند، تا توالی‌هایی را برای تمایز بین زمینه‌ها در رویدادهای ورودی ایجاد کند. Logstash افزونه‌های مختلفی را برای کمک به توسعه‌دهندگان ارائه می‌دهد. برخی از پلاگین‌های فیلتر متداول: Grok، Mutate، Drop، Clone و Geoip.

۳-۲-۱۳-۱-۵ خروجی

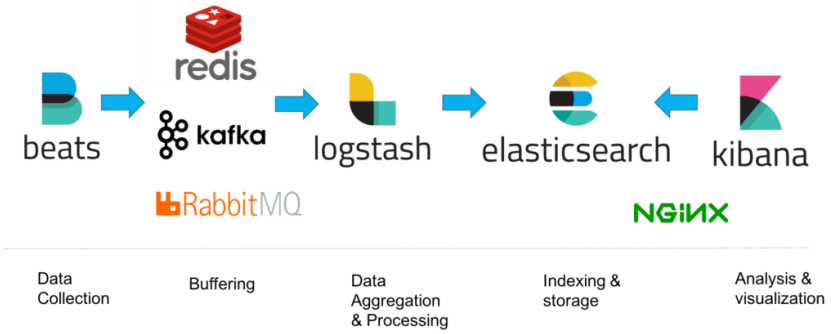
این آخرین مرحله در خط لوله Logstash است، جایی که رویدادهای خروجی را می‌توان در ساختار موردنیاز سیستم‌های مقصد، قالب‌بندی کرد. سرانجام، رویداد خروجی را پس از پردازش کامل با استفاده از افزونه‌ها به مقصد می‌فرستد. برخی از پلاگین‌های متداول استفاده شده در این قسمت عبارتند از: Elasticsearch، File، Graphite، Statsd و غیره.

۳-۲-۱۴ Beats

پشته معروف ELK به طور سنتی از سه مؤلفه اصلی تشکیل شده است: Elasticsearch، Logstash و Kibana. مدتهاست که این ترکیب دچار تغییر شده و یک عنصر چهارم به نام "Beats" به آن اضافه شده است که به عنوان یک عامل در دستگاه‌های مختلف نصب می‌شود و اطلاعات لاگ را در قالب یکسان به سرور ارسال می‌کند. این حرکت موجب سوق دادن تغییر نام پشته ELK به پشته Elastic شده است. Beats انواع مختلفی دارد از جمله، Filebeat، Packetbeat، Metricbeat، Auditbeat، Heartbeat، Winlogbeat، Journalbeat و Functionbeat، که در ادامه توضیحاتی در مورد هرکدام ارائه می‌شود[۱۳].

۳-۲-۱۴-۱ تاریخچه Beats

در سیستم متمرکز لاگ، یک خط لوله داده از سه مرحله اصلی تشکیل می‌شود: جمع‌آوری، پردازش و ذخیره‌سازی. در پشته ELK، دو مرحله اول به طور سنتی بر عهده Logstash بود که اجرای توامان این وظایف هزینه در برداشت. با توجه به مسائل ذاتی مربوط به نحوه طراحی Logstash، مسائل مربوط به عملکرد آن در خطوط لوله پیچیده که نیاز به پردازش زیادی دارند، به یک امر سنگین تبدیل شده بود. برای همین، ایده برون‌سپاری برخی از مسئولیت های Logstash، (به ویژه وظیفه استخراج داده‌ها) به سایر ابزارها مطرح شد. بعد از چند دوره توسعه، پروتکل جدید و اصلاح شده‌ای ارائه شد که به ستون فقرات آنچه اکنون خانواده "Beats" خوانده می‌شود تبدیل شد. این فرآیند در شکل زیر به تصویر کشیده شده است[۱۳].



شکل ۴: پشته الاستیک

۳-۲-۱۴-۲ Beats چیست؟

Beats، مجموعه‌ای سبک وزن (کارآمد، بدون وابستگی و کوچک) و منبع‌باز است، که به عنوان عامل روی سرورهای مختلف در زیرساخت‌های شما نصب شده و برای جمع‌آوری لاگ‌ها عمل می‌کند. داده‌های لاگ می‌توانند فایل‌های لاگ (Filebeat)، داده‌های شبکه (Packetbeat)، معیارهای سرور (Metricbeat) یا هر نوع دیگر از داده‌هایی باشند که با تعداد زیادی از Beats که توسط Elastic و سایر افراد ایجاد می‌شود، می‌توان جمع‌آوری کرد. پس از جمع‌آوری، داده‌ها مستقیماً به Elasticsearch یا Logstash برای ادامه پردازش، ارسال می‌شوند. Beats در فریم‌ورک Go به نام libbeat ساخته شده است

۳-۲-۱۴-۳ انواع Beats

در ادامه انواع رایج و معمول Beats را توضیح می‌دهیم[۱۳]:

۳-۲-۱۴-۳-۱ Filebeat

Filebeat، همان‌طور که از نام آن پیداست، برای جمع‌آوری و ارسال فایل‌های لاگ استفاده می‌شود، و همچنین رایج‌ترین نوع Beats است. یکی از واقعیت‌هایی که Filebeat را بسیار کارآمد می‌کند، نحوه برخورد با فشار ورود است، یعنی اگر Logstash مشغول باشد، Filebeat به صورت خودکار کند می‌شود و سرعت خواندن را کاهش می‌دهد. Filebeat را می‌توان تقریباً در هر سیستم‌عامل، از طریق کانتینر داکر نصب کرد و همچنین از طریق ماژول‌های داخلی برای سیستم‌عامل‌ها ونرم‌افزارهای خاص مانند Apache، MySQL، Docker، MariaDB، Percona، Kafka و موارد دیگر استفاده می‌شود. از نسخه هفتم به بعد، Filebeat پشتیبانی ازگزارش‌های لاگ‌های مربوط به حسابرسی، لاگ‌های مربوط به سرور و موارد متعدد دیگر را اضافه کرده است.

۳-۲-۱۴-۳-۲ Packetbeat

این نوع از Beats ترافیک شبکه بین سرورها را ضبط می‌کند و به همین ترتیب می‌تواند برای کاربرد و نظارت بر عملکرد آنها مورد استفاده قرار گیرد. Packetbeat را می‌توان در سرور مورد نظر که می‌خواهیم بر آن نظارت کنیم یا روی سرور اختصاصی خود نصب کرد. Packetbeat ترافیک شبکه را ردیابی می‌کند، پروتکل‌ها را رمزگشایی می‌کند و داده‌ها را برای هر تراکنش ضبط می‌کند. پروتکل‌های پشتیبانی شده توسط Packetbeat عبارتند از: DNS، HTTP، ICMP، Redis، MySQL، MongoDB، Cassandra و موارد دیگر. نسخه هفتم آن محاسبه گواهینامه اثر انگشت (SHA-256، SHA-1، MD5 و غیره) و همینطور از رمزگشایی MySQL و HTTP نیز پشتیبانی می‌کند.

۳-۲-۱۴-۳-۳ Metricbeat

یک نوع بسیار محبوب از Beats می‌باشد که معیارهای مختلف سطح سیستم را (مثلا میزان بار پردازنده، میزان استفاده از حافظه و غیره) برای سیستم‌ها و پلت‌فرم‌های مختلف جمع‌آوری و گزارش می‌کند. Metricbeat همچنین از ماژول‌های داخلی برای جمع‌آوری آمار از پلت‌فرم‌های خاص، پشتیبانی می‌کند. می‌توان فرکانس جمع‌آوری معیارها را با استفاده از ماژول‌ها و زیر تنظیماتی به نام metricsets، تنظیم کرد. از نسخه

هفتم به بعد، معیارهایی برای اندازه حافظه پنهان در ماژول Memcached اضافه شده است؛ یک فیلد service.type و از همه مهمتر یک ماژول AWS EC2 برای ذخیره‌سازی در محیط ابری، همچنین تغییراتی در ماژول‌های Redis و MSSQL وجود دارد.

۳-۲-۱۴-۳-۴ Heartbeat

Heartbeat برای "نظارت در لحظه" طراحی شده است. در اصل، آنچه این عامل انجام می‌دهد سرویس کاوش برای بررسی اینکه آیا به سرویس‌ها و سرورها زنده هستند یا خیر. تمام کاری که شما باید انجام دهید اینست که لیستی از URLها و معیارهای uptime برای بررسی و نظارت تهیه کنید.

۳-۲-۱۴-۳-۵ Auditbeat

Auditbeat می‌تواند برای حسابرسی کاربر و فعالیت‌های پردازشی وی در سرورهای لینوکس استفاده شود. مشابه سایر ابزارهای حسابرسی سنتی سیستم، Auditbeat می‌تواند برای شناسایی نقض امنیت نیز استفاده شود، برای مثال تغییرات فایل، تغییرات پیکربندی، رفتار مخرب و غیره.

۳-۲-۱۴-۳-۶ Winlogbeat

نوعی از Beat است که به طور خاص برای جمع‌آوری لاگ‌های Windows Event طراحی شده است. می‌توان از آن برای تحلیل حوادث امنیتی، به‌روزرسانی موارد نصب شده و موارد دیگر استفاده کرد.

۳-۲-۱۴-۳-۷ Functionbeat

Functionbeat به عنوان یک حمل کننده بدون سرور تعریف می‌شود که می‌تواند به عنوان تابعی برای جمع‌آوری و انتقال داده‌ها به پشته ELK ، مستقر شود. Functionbeat برای نظارت بر محیط‌های ابری طراحی شده و می‌تواند برای جمع‌آوری داده‌ها از آمازون CloudWatch، Kinesis و SQS مستقر شود.

۳-۲-۱۴-۳-۸ Journalbeat

Journalbeat یک حمل‌کننده جدید در خانواده Beats است، که به طور خاص برای لاگ systemd طراحی شده است.

۳-۲-۱۵ کافکا یا Apache Kafka

کافکا در لینکداین سرچشمه گرفت و بعداً در سال ۲۰۱۱ به یک پروژه منبع‌باز بنیاد Apache تبدیل شد که بسیار هم مورد استقبال قرار گرفت. کافکا به زبان اسکالا و جاوا نوشته شده است. کافکا سیستم پیام‌رسان بر اساس تحمل خطا را به اشتراک می‌گذارد. سریع و مقیاس‌پذیر است و به صورت توزیع شده، طراحی شده است و برای سامانه‌های مبتنی بر حجیم‌داده، به عنوان یک ابزار مطمئن و تاحدودی غیرقابل جایگزین

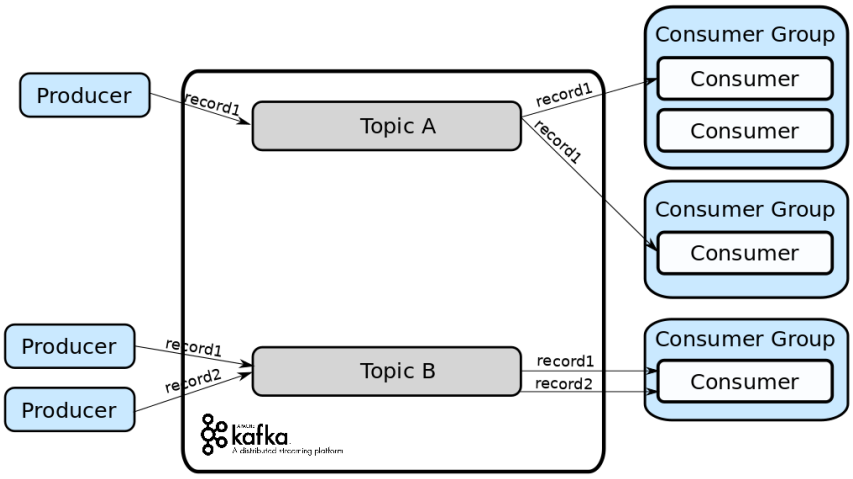
شناخته می‌شود. لازم به توضیح است که کافکا را نمی‌توان به صورت مستقیم به عنوان یک ابزار جمع‌آوری لاگ در نظر گرفت، بلکه معمولا در ترکیب با مابقی ابزارهای مدیریت لاگ نظیر پشته ELK در سیستم‌های حجیم‌داده استفاده می‌شود[۱۴].

در حجیم‌داده، حجم عظیمی از داده‌ها تولید و استفاده می‌شود. با توجه به حجم داده‌ها، ما با دو چالش اصلی روبرو هستیم. چالش اول، نحوه جمع‌آوری حجم زیادی از داده‌ها و چالش دوم، تجزیه و تحلیل داده‌های جمع‌آوری شده می‌باشد. برای غلبه بر این چالش‌ها، شما نیاز به یک سیستم پیام‌رسانی دارید.

یک سیستم پیام‌رسان وظیفه انتقال داده‌ها از یک برنامه به برنامه دیگر را دارد، بنابراین برنامه‌ها می‌توانند روی داده‌ها متمرکز شوند، اما در مورد نحوه اشتراک‌گذاری آن‌ها نگران نباشند. پیام‌های توزیع‌شده بر اساس مفهوم صف‌بندی پیام، قابل اعتماد است. پیام‌ها برای مثال همان رکوردهای لاگ، به صورت ناهمگام بین برنامه‌ها و سیستم پیام‌رسان، قرار می‌گیرند. دو نوع الگوی پیام‌رسانی وجود دارد، یکی نقطه به نقطه و دیگری سیستم پیام‌رسانی انتشار- اشتراک (pub-sub). بسیاری از الگوهای پیام‌رسانی همین مدل را دنبال می‌کنند.

در یک سیستم نقطه به نقطه، پیام‌ها در یک صف به صورت دائم ادامه دارند. یک یا چند مشتری می‌توانند پیام‌های موجود در صف را مصرف کنند، اما یک پیام خاص توسط حداکثر فقط یک مشتری، قابل مصرف است. هنگامی‌که یک مشتری یک پیام را در صف خواند، از آن صف ناپدید می‌شود. نمونه بارز این سیستم، سیستم پردازش سفارش است، که در آن هر پردازش توسط یک پردازنده سفارش پردازش می‌شود، اما پردازنده‌های چند منظوره می‌توانند به صورت همزمان، کار کنند[۱۴].

در سیستم انتشار- اشتراک، پیام‌ها در یک موضوع، ادامه می‌یابد. بر خلاف سیستم نقطه به نقطه، مشتریان می‌توانند در یک یا چند موضوع مشترک شوند و تمام پیام‌های موجود در آن موضوع را استفاده کنند. در سیستم انتشار- اشتراک، تولیدکنندگان پیام به ناشران گفته می‌شود و مصرف‌کنندگان پیام را مشترکان، می‌نامند. یک مثال، در زندگی واقعی دیش تلویزیون است که کانال‌های مختلفی از جمله ورزش، فیلم، موسیقی و ... را منتشر می‌کند و هر کس می‌تواند در مجموعه کانال‌های خود مشترک شود و هر زمان که کانال‌های مشترک آنها در دسترس باشد، اطلاعات را دریافت کنند[۱۴].



شکل ۵: مدل کاری کافکا به صورت انتشار- اشتراک

کافکا یک سیستم ارسال پیام مشترک و توزیع‌شده قوی است که می‌تواند حجم بالایی از داده‌ها را (مثلا داده‌های لاگ) در قالب پیام و به صورت آنلاین از یک نقطه انتهایی به نقطه دیگر منتقل کند. پیام های کافکا بر روی دیسک باقی می‌ماند و در داخل خوشه، همانندسازی می‌شود تا از هدر رفتن داده جلوگیری شود. کافکا در بالای سرویس هماهنگ کننده ZooKeeper کار می‌کند. کافکا برای سیستم‌های توان بالا به صورت توزیع شده طراحی شده است. در مقایسه با سایر سیستم‌های پیام‌رسان، کافکا از توان بهتر، پارتیشن‌بندی داخلی، تکثیر و تحمل خطا برخوردار است که باعث می‌شود برای پردازش پیام در مقیاس بزرگ، مناسب باشد[۱۴].

فواید

- کافکا توزیع‌شده، پارتیشن‌بندی شده، تکرار شده و دارای تحمل خطا است
- سیستم پیام‌رسان کافکا به راحتی و بدون کمبود، قابلیت مقیاس‌پذیری در سرعت بالای پیام‌رسانی را دارد
- کافکا از سیستم توزیع شده لاگ استفاده می‌کند و این بدان معنی است که پیام‌ها بر روی دیسک با بیشترین سرعت ممکن باقی می‌مانند
- کافکا توانائی بالایی هم برای انتشار و هم برای ارسال پیام دارد و در ضمن، عملکرد پایداری دارد

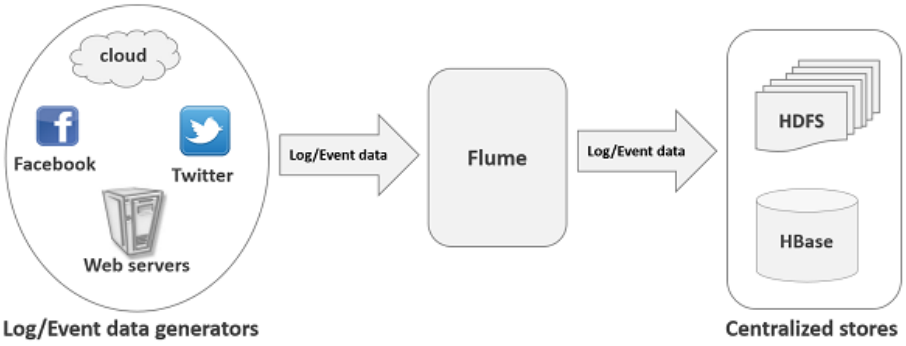
موارد استفاده:

- کافکا اغلب برای داده‌های نظارت عملیاتی، استفاده می‌شود. این شامل جمع‌آوری آمار از برنامه‌های توزیع شده است.
- کافکا را می‌توان در یک سازمان برای جمع آوری لاگ‌های مربوط از چندین سرویس استفاده کرد، و آن‌ها را در قالب استاندارد برای چندین مشترک، در دسترس قرار داد.
- کافکا امکان تعامل با چارچوب‌های محبوبی مانند Storm و Spark Streaming برای پردازش داده را دارد.

- کافکا از ارسال پیام با تاخیر کم، پشتیبانی می‌کند و در صورت بروز خرابی دستگاه، تحمل خطا را تضمین می‌کند. این توانایی را دارد که بتواند تعداد زیادی از مشتریان متنوع را اداره کند. کافکا بسیار سریع است. کافکا تمام داده‌ها را بر روی دیسک قرار می‌دهد، که در واقع به این معنی است که همه نوشته‌ها به حافظه نهان صفحه سیستم عامل می‌روند.

۳-۲-۱۶ فلوم یا Apache Flume

فلوم ابزاری استاندارد، ساده، مستحکم، انعطاف‌پذیر و توسعه‌پذیر برای استفاده از داده‌ها از تولیدکنندگان داده‌های مختلف (وب سرور) به فایل سیستم هدوپ (HDFS) و مابقی سامانه‌های ذخیره‌سازی حجیم‌داده برای پردازش‌های آتی است. فلوم بستری برای جمع‌آوری و انتقال مقادیر زیادی از جریان‌های داده مانند لاگ فایل‌ها، رویدادها و غیره از منابع مختلف به یک مخزن داده متمرکز است. فلوم ابزاری قابل اعتماد، توزیع‌شده و قابل پیکربندی است. شکل زیر نمای کلی عملکرد فلوم را نشان می‌دهد.



شکل ۶: نحوه عملکرد فلوم

فرض کنید یک برنامه وب تجارت الکترونیک، می‌خواهد رفتار مشتری از یک منطقه خاص را تجزیه و تحلیل کند. برای انجام این کار، باید داده‌های لاگ موجود برای تجزیه و تحلیل به هدوپ منتقل شود. فلوم برای انتقال اطلاعات لاگ ایجاد شده توسط سرورهای کاربردی به HDFS با سرعت بالاتر، استفاده می‌شود[۱۵].

مزایا:

- با استفاده از آپاچی فلوم می‌توان داده‌ها را در انواع بسترهای ذخیره‌سازی حجیم‌داده (HBase و HDFS) ذخیره کرد
- هنگامی‌که سرعت داده‌های ورودی از میزان نوشتن اطلاعات به مقصد فراتر رود، فلوم به عنوان واسطه بین تولیدکنندگان داده و منابع ذخیره‌سازی عمل می‌کند و جریان ثابتی از داده‌ها را بین آن‌ها، فراهم می‌سازد
- فلوم ویژگی مسیریابی متنی را ارائه می‌دهد، یعنی چه داده‌هایی بر اساس محتوی در کجا ذخیره شوند
- فلوم تراکنش‌ها را مابین فرستنده‌ها و گیرنده‌ها پشتیبانی می‌کند
- فلوم تحویل پیام قابل اعتماد را تضمین می‌کند
- فلوم تحمل‌پذیر نسبت به خطا، مقیاس‌پذیر، قابل کنترل و قابل تنظیم است

- با استفاده از فلوم، می‌توان داده‌ها را از چندین سرور، بلافاصله وارد فایل سیستم هدوپ کرد
- در کنار فایل‌های لاگ، از فلوم همچنین برای وارد کردن حجم عظیمی از داده‌های رویداد تولید شده توسط سایت‌های شبکه‌های اجتماعی مانند فیس‌بوک و توییتر و وب‌سایت‌های تجارت الکترونیک مانند آمازون و فلیپ‌کارت استفاده می‌شود
- فلوم، مجموعه بزرگی از انواع منابع و مقاصد را پشتیبانی می‌کند

۴. مدیریت و نظارت

امروزه یکی از اصلی ترین و مهمترین راهکارها در مدیریت شبکه‌های بزرگ، پیاده‌سازی ساختارهای مرکز عملیات شبکه و مرکز عملیات امنیت (اصطلاحا NOC و SOC) می‌باشد. این سامانه‌ها برای سازمان‌ها، امکان مدیریت هر چه آسان تر تجهیزات، سرویس‌ها و همچنین مقابله با رخدادهای امنیتی را فراهم آورده و تدوین سیاست‌های کلان در جهت بهبود سرویس‌دهی و خدمت‌رسانی هر چه بهتر را برای مدیران شبکه امکان‌پذیر می‌سازند. همچنین امکان تشخیص صحیح و به‌موقع رخدادها را با توجه به خروجی‌های ایجاد شده، میسر ساخته و سازمان‌ها را در جهت کاهش خطا و بالا رفتن ضریب تصمیم‌گیری‌های صحیح، یاری می‌رسانند. پیاده‌سازی این ساختارها، مستلزم شناخت کافی از ابزار و نرم‌افزارهای مختلف در جهت یکپارچه‌سازی و مدیریت آنها و همچنین آنالیز دقیق از نیاز سازمان‌ها و شرکت‌های بزرگ است. در غیر این صورت، سازمان‌ها از تمامی امکانات این سامانه‌ها بهرمند نشده و ممکن است در بلند مدت به دلیل پیچیدگی در راهبری و یا استفاده غیرعلمی و مغایر با استانداردها، این سامانه‌ها کمک چندانی به بهبود عملکرد شبکه سازمان‌ها ننمایند.

مطابق با استانداردهای متداول، ۵ حوزه مدیریتی در این زمینه وجود دارد که در ادامه هریک را مختصر توضیح می‌دهیم:

- **مدیریت خطا یا Fault Management**: شناسایی، ایزوله‌سازی، اطلاع رسانی و اصلاح خطای رخ داده در شبکه
- **مدیریت تنظیمات یا Configuration Management**: تنظیم تنظیمات مربوط به تجهیزات شبکه، تنظیمات مدیریت فایل، مدیریت لیست موجودی و مدیریت نرم‌افزار
- **مدیریت حساب‌های کاربری یا Accounting Management**: جمع آوری اطلاعات میزان استفاده از منابع شبکه
- **مدیریت عملکرد یا Performance Management**: نظارت و سنجش جنبه‌های گوناگونی که باعث بهبود عملکرد در یک لایه‌ی خاص از سامانه می‌گردد
- **مدیریت امنیت یا Security Management**: امنیت دسترسی به تجهیزات شبکه، منابع شبکه و سرویس‌ها برای افراد مجاز

۴-۱ مدیریت خطا

مدیریت خطا مجموعه‌ای از راهکارهایی است که توانایی شناسایی، ایزوله کردن و تصحیح عملیات‌های غیرطبیعی و خطادار را در شبکه ارتباطی به وجود می‌آورد. معیار تضمین کیفیت برای مدیریت خطا شامل اندازه‌گیری اجزای اتکاپذیری، دسترسی و پایداری می‌باشد. مدیریت خطا در مرکز عملیات شبکه و امنیت خود شامل بخش‌های ذیل است:

- ایجاد تضمین کیفیت به هدف بهبود شاخص اتکاپذیری با استفاده از سیاست‌های مختلف نظیر تکرارسازی
- نظارت بر هشدارها به معنی قابلیت نظارت بر اجزای از کار افتاده شبکه در سریع ترین زمان ممکن
- محلی سازی خطا بدین معنی که چه زمانی اطلاعات اولیه یک خطا برای شناسایی موقعیت آن کافی است
- تصحیح خطا، شامل اصلاح کد و نرم‌افزار، تغییر تنظیمات، استفاده از منابع اضافی موجود و جایگزینی تجهیزات یا امکانات مشکل‌دار
- بررسی و آزمایش که معمولا به دو روش داخلی (از درون شبکه) و خارجی (از بیرون شبکه) انجام می‌پذیرد
- مدیریت ایرادات که مشکلات گزارش شده توسط مشتریان و یا توسط آزمایشات خطایابی را مدنظر قرار می‌دهد
- پشتیبانی برای بررسی و پاک‌سازی مشکلات و دسترسی به وضعیت سرویس‌ها و روال‌ها قبل و بعد از رفع خطا می‌باشد

۴-۲ مدیریت تنظیمات

مدیریت تنظیمات، روش‌هایی را برای شناسایی، جمع‌آوری داده‌های مربوط به تنظیمات دستگاه‌ها، کنترل بر دستگاه‌ها و امکان پیکربندی تجهزیات از شبکه را فراهم می‌نماید.

۴-۳ مدیریت حساب‌های کاربری

مدیریت حساب‌های کاربری به شما اجازه می‌دهد تا میزان استفاده از سرویس‌های شبکه و هزینه‌ای را که برای ارائه سرویس به مشتری برای هر بار استفاده تحمیل می‌شود بدست آورد و همچنین به ارزیابی میزان هزینه انجام شده برای یک سرویس کمک می‌نماید. مدیریت حساب‌های کاربری شامل بخش‌های ذیل می‌گردد:

- اندازه گیری میزان استفاده
- تعرفه بندی و قیمت‌گذاری
- پرداخت مالی مشتریان و شارژ باقیمانده
- کنترل شرکت از بابت بودجه‌بندی، ممیزی و تجزیه و تحلیل سودآوری

۴-۴ مدیریت عملکرد

مدیریت عملکرد مجموعه فعالیت‌هایی است که به منظور ارزیابی و گزارش‌گیری بر روی وضعیت سخت‌افزارها و نرم‌افزارهای مختلف، تجهیزات ارتباطی و کارایی شبکه یا عناصر دیگر صورت می‌پذیرد. یکی از نقش‌های اصلی آن جمع‌آوری و تجزیه و تحلیل آماری داده‌ها به منظور نظارت و تصحیح وضعیت و کارایی شبکه یا دیگر تجهیزات می‌باشد.

۴-۵ مدیریت امنیت

مدیریت امنیت در مرکز عملیات شبکه و امنیت شامل دو بخش اصلی می‌باشد:

۱. خدمات امنیت در حوزه ارتباطات، شامل: احراز هویت، کنترل دسترسی، محرمانگی داده، صحت داده و عدم انکارپذیری
۲. شناسایی رخدادهای امنیتی و گزارش‌دهی از فعالیت‌هایی که ممکن است به عنوان تخلف امنیتی تفسیر گردد

۴-۶ معرفی سامانه‌های نظارت

در این بخش، قصد داریم تعدادی از معروف‌ترین سامانه‌های نظارت را که به ویژه در محیط حجیم‌داده مورد استفاده قرار می‌گیرند معرفی کنیم. مجددا تاکید می‌کنیم که اگرچه همه این سامانه‌ها وظیفه مشابهی را انجام می‌دهند، لیکن نمی‌توان یک معیار ارزیابی یکسان برای مقایسه آنها و انتخاب بهترین سامانه در نظر گرفت، زیرا هر کدام از آنها برای کارکرد و محیط مشخصی طراحی شده‌اند و دارای عملکرد بهتری در برخی زمینه‌ها هستند.

۴-۶-۱ Apache Ambari

پروژه Ambari با هدف مدیریت و اجرای ساده‌تر هدوپ با تهیه نرم‌افزار برای مدیریت و نظارت بر سرورهای موجود در خوشه‌های هدوپ ایجاد شد. Ambari یک رابط کاربری بصری آسان برای اجرای هدوپ و استفاده از آن با پشتیبانی از RESTful API ارائه می‌دهد [۱۶]. Ambari مدیران سامانه را قادر می‌سازد تا فعالیت‌های زیر را انجام دهند:

- تهیه خوشه هدوپ: این نرم‌افزار امکان نصب به صورت گام به گام برای سرویس هدوپ در هر تعداد میزبان را فراهم می‌کند. Ambari پیکربندی سرویس هدوپ را برای کل خوشه انجام می‌دهد.
- مدیریت خوشه هدوپ: Ambari مدیریت مرکزی را برای شروع/ متوقف کردن و پیکربندی مجدد سرویس هدوپ، در کل خوشه فراهم می‌کند.
- نظارت بر خوشه هدوپ: داشبوردی را برای نظارت بر سلامتی وضعیت خوشه هدوپ فراهم می‌کند.
  - از سامانه‌های اندازه‌گیری Ambari Metrics برای ارزیابی مجموعه معیارها استفاده می‌کند.
  - از چارچوب هشدار سامانه Ambari برای هشدار یک خرابی و یا یک رویداد در سامانه استفاده می‌کند.

به همین ترتیب، Ambari توسعه‌دهندگان برنامه‌ها و یکپارچه‌سازان سامانه را قادر می‌سازد تا به راحتی قابلیت‌های تهیه، مدیریت و نظارت بر برنامه هدوپ در برنامه‌های خود را با APIهای Ambari REST ادغام نمایند. Ambari در حال حاضر از نسخه ۶۴ بیتی سیستم عامل‌های مختلف لینوکس پشتیبانی می‌کند.

۴-۶-۲ Nagios

Nagios که اکنون با نام Nagios Core شناخته می‌شود، یک نرم افزار معروف، رایگان و منبع‌باز است که بر سامانه‌ها، شبکه‌ها و زیرساخت‌ها نظارت دارد. Nagios خدمات نظارت و هشدار را برای سرورها، سوئیچ‌ها، برنامه‌ها و سرویس‌ها ارائه می‌دهد. با ایجاد مشکل و خطا به کاربر اخطار می‌دهد، همچنین با رفع شدن خطا اخطار دیگری برای کاربر ارسال می‌کند [۱۷]. در ابتدا Nagios برای اجرا تحت لینوکس طراحی شده بود، اما در سایر انواع یونیکس نیز خوب عمل می‌کند. این نرم‌افزار رایگان تحت مجوز GNU General Public License نسخه ۲ است که توسط بنیاد نرم‌افزار آزاد منتشر شده است. این نرمافزار یکی از پرکاربردترین نرمافزارهای نظارت سامانه‌ها به ویژه سامانه‌های حجیم‌داده می‌باشد.

خدماتی که Nagios ارائه می‌دهد:

- نظارت بر سرویس‌های شبکه (SMTP، POP3، HTTP، NNTP، ICMP، SNMP، FTP، SSH)
- نظارت بر منابع میزبان (بار پردازنده، استفاده از دیسک، لاگ‌های مربوط به سامانه) در اکثر سیستم عامل‌های شبکه از جمله ویندوز با استفاده از عوامل نظارت
- نظارت بر هر سخت‌افزاری (مانند کاوشگرهای دما، هشدارها و...) که توانایی ارسال داده‌های جمع‌آوری شده از طریق شبکه به افزونه‌های خاص نوشته شده را داشته باشند
- نظارت از طریق اجرای اسکریپت‌های از راه دور از طریق افزونه Nagios Remote Plugin
- نظارت از راه دور از طریق تونل‌های رمزگذاری شده گه از SSH یا SSL پشتیبانی می‌کنند
- طراحی افزونه ساده‌ای که این امکان را می‌دهد که با استفاده از ابزارهای مورد نظر خود (اسکریپت‌های پوسته، C++، پرل، روبی، پایتون، PHP، C# و...) چک‌های سرویس خود را به راحتی توسعه دهند
- ارائه پلاگین‌های نمودار اطلاعات
- گردش خودکار لاگ فایل‌ها
- پشتیبانی از اجرای میزبان نظارت بر کارآیی
- پشتیبانی از اجرای نمودارهای داده عملکرد
- پشتیبانی از پایگاه داده برای نگهداری اطلاعات نظارت
- رابط وب برای مشاهده وضعیت فعلی شبکه، اعلان‌ها، سابقه مشکل، لاگ‌های ورود به سامانه و....

مولفه‌های موجود در Nagios به صورت زیر می‌باشند:

- NRPE (Nagios Remote Plugin Executor): یک عامل Nagios است که امکان نظارت بر سامانه از راه دور را با استفاده از اسکریپت‌هایی که روی سامانه‌های از راه دور میزبان هستند، می‌دهد. این امکان نظارت بر منابعی از قبیل استفاده از دیسک، بار سامانه یا تعداد کاربرانی که در حال حاضر وارد سامانه شده‌اند را فراهم می‌کند.
- NRDP (Nagios Remote Data Processor): یک عامل Nagios با مکانیسم و پردازشگر انتقال داده به آدرس‌ها و سرورهای دیگر است.
- NSClient++: این برنامه عمدتا برای نظارت بر دستگاه‌های ویندوز استفاده می‌شود.
- NCPA: این برنامه اجازه می‌دهد تا چندین کنترل بر روی معیارهایی از قبیل استفاده از حافظه، استفاده از CPU، استفاده از دیسک، فرایندها، خدمات و استفاده از شبکه را انجام دهد.

۴-۶-۲-۱ نصب

ابتدا پیش‌نیازهای نرم‌افزار باید نصب شوند:

```
useradd nagios
groupadd nagcmd
usermod -a -G nagcmd nagios
usermod -a -G nagios,nagcmd www-data
```

سپس هسته Nagios را دانلود و استخراج کنید [۱۸]:

```
cd ~
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.2.0.tar.gz
tar -xzf nagios*.tar.gz
cd nagios-4.2.0
```

Nagios را کامپایل کنید. قبل از اینکه بخواهید Nagios را ایجاد کنید، باید آن را با گروه و کاربری که قبلا ایجاد کرده‌اید پیکربندی نمایید.

```
./configure --with-nagios-group=nagios --with-command-group=nagcmd
```

حال می‌توانید Nagios را نصب کنید:

```
make all
sudo make install
sudo make install-commandmode
sudo make install-init
```

```
sudo make install-config
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf
```

دایرکتوری evenhandler را به دایرکتوری Nagios کپی کنید:

```
cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
```

افزونه‌های این نرم‌افزار را نیز به کمک دستور زیر دانلود و از حالت فشرده، خارج کنید:

```
cd ~
wget https://nagios-plugins.org/download/nagios-plugins-2.1.2.tar.gz
tar -xzf nagios-plugins*.tar.gz
cd nagios-plugin-2.1.2/
```

به کمک دستور زیر افزونه‌های nagios را نصب نمایید:

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl
make
make install
```

بعد از اینکه فرآیند نصب کامل شد می‌توانید فایل پیکربندی پیش‌فرض را در مسیر /usr/local/nagios مشاهده کنید. به کمک دستور زیر می‌توان

فایل پیکربندی پیش‌فرض را ویرایش نمود:

```
vim /usr/local/nagios/etc/nagios.cfg
```

برای پیکربندی مانیتورینگ هاست یا سرور، خط زیر را فعال کنید (یعنی از حالت کامنت بیرون آورید).

```
cfg_dir=/usr/local/nagios/etc/servers
```

فایل را ذخیره کنید و خارج شوید. حالا فولدر جدیدی به نام Servers اضافه نمایید:

```
mkdir -p /usr/local/nagios/etc/servers
```

تماس‌های Nagios (یا همان contact) را می‌توان در فایل Contact.cfg پیکربندی کرد. برای باز کردن آن از دستور زیر استفاده کنید:

```
vim /usr/local/nagios/etc/objects/contacts.cfg
```

حالا ایمیل پیش‌فرض را با ایمیل خود جایگزین نمایید. برای شروع به کار Nagios از دستور زیر استفاده کنید:

```
service nagios start
```

زمانی که Nagios آغاز به کار می‌کند، ممکن است خطای زیر را مشاهده کنید:

```
Starting nagios (via systemctl): nagios.serviceFailed
```

دستور زیر این خطا را برطرف می‌کند:

```
cd /etc/init.d/
cp /etc/init.d/skeleton /etc/init.d/nagios
```

فایل Nagios را ویرایش کنید:

```
vim /etc/init.d/nagios
```

کد زیر را به آن اضافه نمایید:

```
DESC="Nagios"
NAME=nagios
DAEMON=/usr/local/nagios/bin/$NAME
DAEMON_ARGS="-d /usr/local/nagios/etc/nagios.cfg"
PIDFILE=/usr/local/nagios/var/$NAME.lock
```

Nagios را استارت کنید:

```
chmod +x /etc/init.d/nagios
servuce nagios start
```

۴-۶-۳ Cloudera

Cloudera یا کلودرا در سال ۲۰۰۸ توسط سه مهندس گوگل، یاهو و فیس‌بوک ساخته شد و به عنوان توزیع منبع آزاد با ترکیبی از پروژه‌های بنیاد آپاچی نظیر هدوپ شروع به کار کرد. کلودرا اظهار می‌دارد که بیش از ۵۰٪ از تولید مهندسی آن به پروژه‌های متنوع با منبع آزاد با مجوز آپاچی اهدا می‌شود که برای تشکیل بسترهای نرم‌افزاری مبتنی بر هدوپ ساخته می‌شوند [۱۹]. البته بستر کلودرا را به خودی خود نمی‌توان یک سامانه نظارت در نظر گرفت، ولی در داخل این بستر حجیم‌داده، از ابزارهای نظارتی استفاده و پشتیبانی می‌شود. نرم‌افزار کلودرا، خدمات و پشتیبانی را در پنج بسته نرم‌افزاری موجود و در قالب چندین ارائه‌دهنده ابر ارائه می‌دهد:

- Cloudera Enterprise Data Hub: پلتفرم جامع مدیریت داده‌های کلودرا، شامل علوم و مهندسی داده‌ها، پایگاه داده عملیاتی، پایگاه داده تحلیلی و Cloudera Essentials.
- Cloudera Analytic DB: فن‌آوری‌های کلودرا که بر روی پلت‌فرم اصلی Cloudera Essentials ساخته شده‌اند.
- Cloudera Operative DB: فن‌آوری‌های NoSQL با مقیاس بالا.

- علوم و مهندسی داده‌های Cloudera: فن‌آوری‌های کلودرا که پردازش داده‌های کارآمد و مقیاس بالا، و اجرای تکنیک‌های علوم داده و یادگیری ماشین را در بالای سکوی اصلی هسته امکان‌پذیر می‌سازد.
- Cloudera Essentials: هسته اصلی مدیریت داده‌های کلودرا برای مدیریت پردازش سریع، آسان و ایمن داده‌ها در مقیاس بزرگ، که شامل قابلیت‌های مدیریت سازمانی کلودرا (مدیر کلودرا) و توزیع سکوی منبع باز (CDH) است.

کلودرا نسخه‌های نرم‌افزاری رایگان زیر را نیز ارائه می‌دهد:

- Cloudera Express: شامل پلتفرم منبع آزاد CDH و نسخه بدون هزینه استقرار، نظارت و مجموعه مدیریتی آن
- CDH (توزیع کلودرا از جمله آپاچی هدوپ): توزیع سیستم عامل منبع آزاد کلودرا به همراه هدوپ، اسپارک و موارد دیگر

۴-۶-۴ Apache Ranger

این ابزار چارچوبی برای فعال‌سازی، نظارت و مدیریت امنیت جامع داده در پلتفرم هدوپ است. چشم‌انداز Ranger ارائه امنیت جامع در سراسر زیست‌بوم آپاچی هدوپ است. با ظهورApache YARN ، پلت‌فرم هدوپ هم اکنون می‌تواند از یک معماری واقعی توزیع شده و کانتینری پشتیبانی کند: شرکتها به طور بالقوه می‌توانند بارهای مختلف کار را در هر ماشین به صورت کانتینترهای مجزا اجرا کنند. امنیت داده‌ها در هدوپ برای پشتیبانی از موارد استفاده چندگانه برای دسترسی به داده‌ها، در عین حال باید چارچوبی برای مدیریت مرکزی سیاست‌های امنیتی و نظارت بر دسترسی کاربران فراهم کند [۲۰].

این چارچوب اهداف زیر را دنبال می‌کند:

- مدیریت امنیتی متمرکز برای مدیریت کلیه وظایف مربوط به امنیت در یک رابط کاربری مرکزی
- مجوزهای ریزدانه و دقیق برای انجام یک عمل خاص و یا عملیاتی با مؤلفه‌های هدوپ و مدیریت از طریق یک ابزار مدیریت مرکزی
- استاندارد کردن روش اعطای مجوز در تمام اجزای هدوپ
- پشتیبانی کامل از روش‌های مختلف مجوز کنترل دسترسی مبتنی بر نقش، کنترل دسترسی مبتنی بر ویژگی و غیره
- متمرکز کردن رسیدگی و حسابرسی عملیات و کاربری‌ها در کلیه مؤلفه‌های هدوپ

کارکردهای جنبی این چارچوب نیز به شرح زیر می‌باشند:

- ارائه آمارهای دسترسی به داده با دانه‌بندی مختلف
- ارائه هشدار جهت اقدام به دسترسی‌های غیرمجاز در زیست‌بوم هدوپ
- مدیریت جامعیت داده‌ها و بررسی محرمانگی
- تعامل با ابزارها و چارچوب‌های امنیتی و کارکردی دیگر

۴-۶-۵ Ganglia

یک سامانه نظارت برای سامانه‌های محاسباتی توزیع شده مقیاس‌پذیر با کارایی بالا مانند خوشه‌ها و شبکه‌ها است. این ابزار مبتنی بر یک ساختار سلسله مراتبی است. این فن‌آوری از فن‌آوری‌های گسترده‌ای مانند XML برای نمایش داده‌ها، XDR برای انتقال داده‌ها و RRDtool برای ذخیره‌سازی و نمایش اطلاعات استفاده می‌کند. در عین، از ساختارها و الگوریتم‌های داده برای دستیابی به سربار پردازشی بسیار کم و همزمانی بالا استفاده می‌کند. اجرای پایدار به مجموعه گسترده‌ای از سیستم عامل‌ها و معماری‌های پردازنده منتقل شده است، و در حال حاضر در هزاران خوشه در سراسر جهان مورد استفاده قرار گرفته است، به ویژه از این سامانه برای ارتباط خوشه‌های پردازشی در پردیس‌های دانشگاهی در سراسر جهان استفاده شده است و می‌تواند مقیاس‌پذیری لازم برای مدیریت خوشه‌ها با ۲۰۰۰ گره را دارا باشد [۲۱].

مزایا:

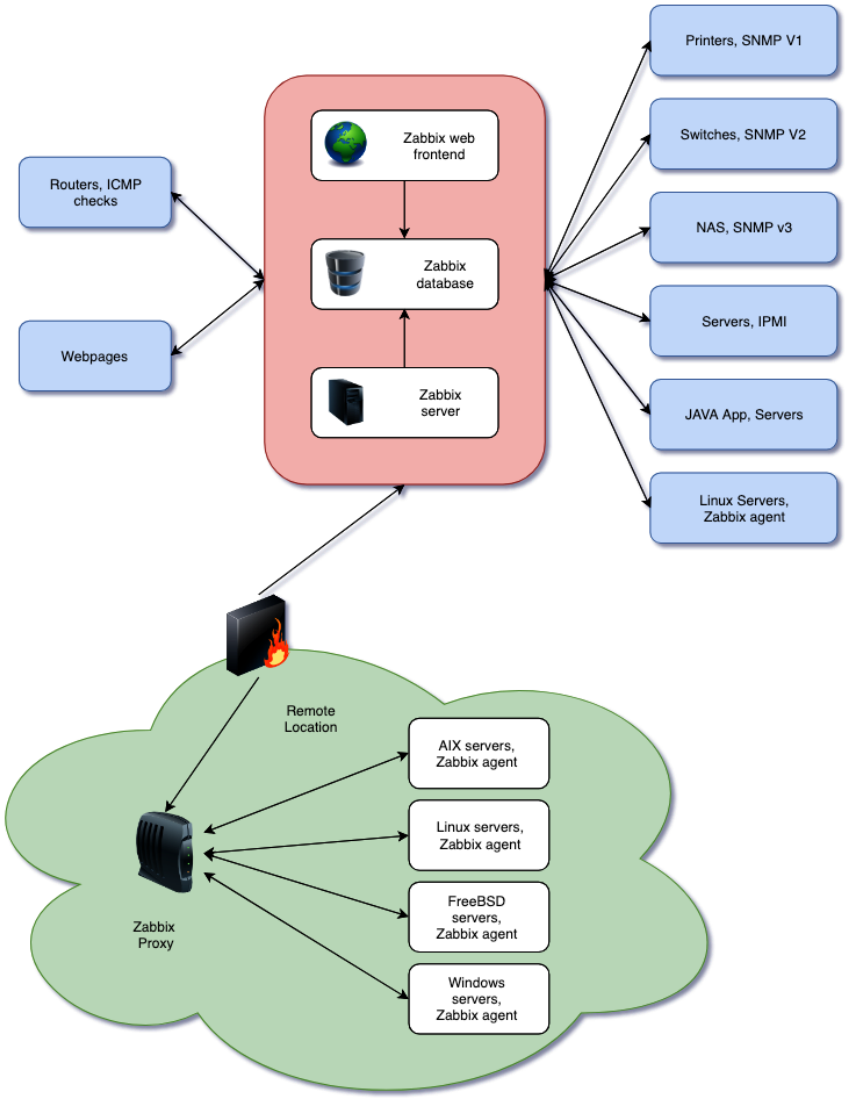
- پروتکل گوش دادن / اعلام چندگانه
- بازه‌ها و وقفه‌های نظارتی مبتنی بر زمان
- سربار پایین
- استفاده از پهنای باند غیرمصرفی سامانه‌ها
- مقیاس‌پذیری با استفاده از توزیع‌شدگی سامانه‌های حجیم‌داده

۴-۶-۶ Sematext

این ابزار یک نظارت تمام عیار را برای مدیران سامانه‌های کامپیوتری فراهم می‌آورد. مهم‌ترین عملیات و مولفه‌هایی که می‌توان با آن تحت نظارت قرار داد عبارتنداز نظارت نرم‌افزاری مانند برنامه‌ها، کاربران،بانک اطلاعاتی، پارامترها و لاگ‌ها، فرآیندها، کانتینرها و نظارت سخت‌افزاری مانند: سرورها، اجزای شبکه و غیره [۲۲].

۴-۶-۷ Zabbix

Zabbix یا زبیکس یک نرم‌افزار متن‌باز و رایگان برای پایش شبکه‌ها و نرم‌افزارها در سطح سازمانی است. به جرات می‌توان این نرم‌افزار را یکی از قویترین و محبوب‌ترین نرم‌افزارهای نظارت برشمرد. این نرم‌افزار توسط الکسی ولادیشو ایجاد شده و برای پایش و تشخیص وضعیت سرویس‌های شبکه‌ها، سرورها و دیگر سخت افزارهای شبکه طراحی شده است. روال معمول برای اجرای زبیکس به این صورت هست که یک سرور مرکزی وجود دارد که سرویس اصلی زبیکس را اجرا می‌کند و همینطور، عامل‌هایی که بر روی سیستم‌های دیگر نصب می‌شوند و اطلاعات مربوط به آن سیستم‌ها را برای سرویس اصلی ارسال می‌کنند. معماری کلی و نحوه عملکرد زبیکس در شکل زیر نشان داده شده است.



شکل ۷: معماری و فرآیند اجرا در زبیکس

زبیکس پارامترهای بی‌شماری از شبکه، و سلامت و یکپارچگی سرورها را رصد می‌کند. زبیکس از یک مکانیسم اعلان انعطاف‌پذیر استفاده می‌کند که به کاربران امکان پیکربندی هشدارهای مبتنی بر پست الکترونیکی را برای تقریباً هر رویدادی می‌دهد. این امکان موجب می‌شود تا یک واکنش سریع به مشکلات سرور داده شود. زبیکس ویژگی ارائه گزارش عالی و تجسم داده‌ها، براساس داده‌های ذخیره‌شده را دارد. این امر زبیکس را برای برنامه‌ریزی ظرفیت، ایده‌آل می‌کند [۲۳]. زبیکس از مای‌اس‌کیوال، پست‌گرس‌کیوال، اس‌کیوال لایت، Oracle و دی‌بی۲ برای ذخیره داده‌ها پشتیبانی می‌کند. برنامه‌نویسی سمت سرور از زبان C بهره میبرد و برنامه‌نویسی سمت کاربری آن از زبان PHP استفاده می‌کند. زبیکس گزینه‌های بسیاری برای مانیتورینگ تجهیزات ارائه می‌دهد [۲۳]:

- زبیکس می‌تواند پایداری و پاسخگویی سرویس‌های استاندارد، مانند SMTP یاHTTP، را بدون نصب نرم‌افزار بر روی سیستم مانیتور شده تأیید کند.

- یک عامل زبیکس می‌تواند بر روی سیستم‌های یونیکس و ویندوز نصب شود و آماری همچون بار پردازنده، فضای ذخیره‌سازی، کاربرد شبکه و غیره را مانیتور نماید.
- برای جایگزین کردن عامل زبیکس بر روی میزبان‌ها، زبیکس از مانیتورینگ SNMP ، TCP و ICMP و همچنین از IPMI، JMX، SSH ، Telnet و پارامترهای سفارشی پشتیبانی می‌کند.

مزایا:

- عملکرد و ظرفیت بالا (توانایی پایش صدها هزار دستگاه)
- کاوش خودکار تجهیزات شبکه
- کاوش سطح پایین (انواع پارامترهای سطح پایین سیستمی و سخت‌افزاری)
- پایش توزیع شده با مدیریت تحت وب یکپارچه
- استفاده از دو مکانیزم رای‌گیری و به دام انداختن
- عامل‌هایی با کارایی بالا برای سیستم عامل‌های مختلف
- پایش بدون نیاز به عامل نرم‌افزاری
- پایش JMX
- پایش وب
- شناسایی امن کاربر
- مجوزهای کاربری انعطاف‌پذیر
- رابط کاربری تحت وب
- معیارهای SLA و ITIL KPI هنگام گزارش‌دهی
- اطلاع رسانی با ایمیل در رخدادهای از قبل تعریف شده و کاملاً انعطاف‌پذیر
- نمایش سطح بالایی از منابع پایش شده در داشبورد و صفحه نمایش‌های تعریف شده
- بازرسی لاگ
- رایگان و منبع‌باز بودن
- پیکربندی، راه‌اندازی و یادگیری آسان
- ذخیره‌سازی کلیه اطلاعات در پایگاه‌داده رابطه‌ای

۱-۷-۶-۴ نصب

پس از دانلود زبیکس از منابع موجود، با دستور زیر فایل منبع را از حالت فشرده خارج کنید [۲۴]:

```
$ tar -zxvf zabbix-4.2.0.tar.gz
```

برای کلیه مراحل پردازش سرویس زبیکس، کاربر غیرشخصی نیاز است. اگر یک سرویس زبیکس، از یک حساب کاربری غیرشخصی آغاز شود، به عنوان آن کاربر اجرا می‌شود. اما اگر یک سرویس از یک حساب "root" شروع شود، به یک حساب کاربری "zabbix" تغییر می‌کند، که باید در سیستم وجود داشته باشد. برای ایجاد چنین حساب کاربری (در گروه خود، "zabbix")، دستور زیر را اجرا کنید:

```
$ groupadd --system zabbix

$ useradd --system -g zabbix -d /usr/lib/zabbix -s /sbin/nologin -c "Zabbix Monitoring System" zabbix
```

برای سرورهای زبیکس و سرویس‌های آن مانند پروکسی زبیکس، یک بانک اطلاعاتی لازم است. البته برای اجرای عامل زبیکس لازم نیست. اسکریپت‌های SQL برای ایجاد شمای پایگاه‌داده و درج در آن ارائه شده است. پس از ایجاد بانک اطلاعاتی زبیکس، مراحل زیر را برای کامپایل زبیکس انجام دهید. برای پیکربندی منابع برای سرور و عامل زبیکس، باید دستوری مانند زیر را اجرا کنید:

```
./configure --enable-server --enable-agent --with-mysql --enable-ipv6 --with-net-snmp --with-libcurl --with-libxml2
```

برای پیکربندی منابع برای سرور زبیکس (با PostgreSQL و غیره):

```
./configure --enable-server --with-postgresql --with-net-snmp
```

برای پیکربندی منابع برای یک پروکسی زبیکس (با SQLite و غیره):

```
./configure --prefix=/usr --enable-proxy --with-net-snmp --with-sqlite3 --with-ssh2
```

برای پیکربندی منابع برای یک عامل Zabbix:

```
./configure --enable-agent
```

این مرحله باید به صورت کاربر دارای مجوزهای کافی (معمولاً "root" یا با استفاده از sudo) اجرا شود.

```
make install
```

اجرای make install بصورت پیش فرض سرویس‌های زبیکس را (zabbix_server، zabbix_agentd، zabbix_proxy) در / usr / local / sbin / و کلاینت‌ها را (zabbix_get، zabbix_sender) در / usr / local / bin نصب می‌کند.

در نهایت فایل‌های پیکربندی عامل زبیکس و پراکسی زبیکس باید ویرایش شوند:

۱. فایل پیکربندی عامل زبیکس /usr/local/etc/zabbix_agentd.conf باید به ازاء هر هاست با نصب zabbix_agentd ویرایش و پیکربندی شود.
۲. شما باید آدرس IP سرور زبیکس را در فایل تعیین کنید. اتصالات از هاست‌های دیگر رد خواهد شد.
۳. فایل سرور زبیکس /usr/local/etc/zabbix_server.conf را ویرایش کنید، شما باید نام بانک اطلاعات، کاربر و رمز ورود (در صورت وجود) را مشخص کنید.
۴. اگر سامانه کوچکی داشته باشید (حداکثر ده میزبان تحت نظارت)، بقیه پارامترها با مقادیر پیش‌فرض‌شان خواسته شما را برآورده می‌کنند. اگر می‌خواهید عملکرد سرور زبیکس (یا پروکسی) را به حداکثر برسانید، باید پارامترهای پیش فرض را تغییر دهید.
۵. اگر پروکسی زبیکس را نصب کرده‌اید ، پیکربندی پروکسی /usr/local/etc/zabbix_proxy.conf را ویرایش کنید.
۶. شما باید آدرس IP سرور و نام هاست پروکسی و همچنین نام بانک اطلاعاتی، کاربر و رمز عبور (در صورت وجود) را تعیین کنید.

در نهایت، برای راه‌اندازی سرویسها نیز از دستورات زیر استفاده کنید. zabbix_server را در سمت سرور اجرا کنید:

```
$ zabbix_server
```

zabbix_agentd را در تمام دستگاه‌های تحت نظارت اجرا کنید:

```
$ zabbix_agentd
```

اگر پروکسی زبیکس را نصب کرده‌اید، zabbix_proxy را اجرا کنید:

```
$ zabbix_proxy
```

۴-۶-۸ NetData

NetData یا نت‌دیتا، ابزاری متن باز برای نمایش و نظارت بر معیارهای زمان واقعی مانند استفاده از CPU، فعالیت دیسک، نمایش داده‌های SQL، بازدید از وب سایت و غیره است [۲۵]. این ابزار برای نمایش فعالیت با بیشترین جزئیات ممکن طراحی شده است و به کاربر این امکان را می‌دهد تا از آنچه اتفاق می‌افتد و اتفاقاتی که اخیراً در سیستم یا برنامه آن‌ها رخ داده است، دید کلی بدست آورد. نت‌دیتا متشکل از یک سرویس

است که در هنگام اجرا، مسئول جمع‌آوری و نمایش اطلاعات در زمان واقعی را برعهده دارد. این سرویس یک ابزار سبک است که با زبان C نوشته شده است و از حداقل منابع استفاده می‌کند.

مزایا:

- نت‌دیتا، طراحی شده است که بر روی هر سیستم نصب شود، بدون اینکه وقفه‌ای در کار برنامه‌های در حال اجرا روی دهد.
- با توجه به نیازهای حافظه‌ای که توسط کاربر مشخص شده است، فقط از چرخه‌های CPU بیکار استفاده می‌کند.
- هنگام شروع برنامه، اطلاعات عملیات را بر روی لاگ (خارج از دیسک) ذخیره می‌کند.
- در پایان اجرا بر روی دیسک ذخیره می‌کند و در هنگام شروع، مجددا بارگیری اجام می‌دهد.
- به طور پیش‌فرض شامل پلاگین‌های خاصی است که معیارهای کلیدی سیستم را جمع‌آوری می‌کنند.
- نت‌دیتا را می‌توان در هر جایی که هسته لینوکس اجرا می‌شود، اجرا کرد، و گرافیک‌های آن در صفحات وب قابل تعبیه است.
- هیچ وابستگی وجود ندارد، زیرا این شبکه با وب‌سرور وب خود عمل می‌کند.

۴-۶-۸-۱ نصب

با استفاده از دستور زیر می‌توان نت‌دیتا را در تمام توزیع‌های لینوکس نصب کرد [۲۶]:

```
bash <(curl -Ss https://my-netdata.io/kickstart.sh)
```

۴-۶-۹ LibreNMS

LibreNMS یک سیستم نظارت بر شبکه، مبتنی بر PHP، منبع آزاد، قدرتمند و دارای قابلیت کشف خودکار است؛ که از پروتکل SNMP استفاده می‌کند. این سیستم از طیف گسترده‌ای از سیستم عامل‌ها از جمله Linux، FreeBSD و همچنین دستگاه‌های شبکه از جمله Cisco، Juniper، Brocade، Foundry، HP و بسیاری دیگر پشتیبانی می‌کند [۲۷].

مزایا:

- کشف تجهیزات موجود در شبکه به طور خودکار با استفاده از پروتکل‌های CDP، FDP، LLDP، OSPF، BGP، SNMP و ARP
- دارای رابط کاربری وب موبایل کاربرپسند، با داشبورد قابل تنظیم
- پشتیبانی از سیستم عامل یونیکس
- پشتیبانی از یک سیستم هشدار بسیار انعطاف‌پذیر و قابل تنظیم (ارسال اعلان‌ها از طریق ایمیل، irc، slack و موارد دیگر)
- پشتیبانی از یک API برای مدیریت، نمودار و بازیابی داده‌ها
- ارائه گزارش ترافیک سیستم
- پشتیبانی از برنامه‌های Android و iOS

- پشتیبانی از چندین روش تأیید هویت مانند MySQL، HTTP، LDAP، Radius و Active Directory
- امکان به‌روزرسانی خودکار

۱-۹-۶-۴ نصب

ابتدا پکیج‌های لازم را نصب کنید:

```
apt install software-properties-common
add-apt-repository universe
apt update
apt install curl apache2 composer fping git graphviz imagemagick libapache2-mod-php7.2 mariadb-client mariadb-server mtr-tiny nmap php7.2-cli php7.2-curl php7.2-gd php7.2-json php7.2-mbstring php7.2-mysql php7.2-snmp php7.2-xml php7.2-zip python-memcache python-mysqldb rrdtool snmp snmpd whois
```

سپس، کاربر LibreNMS را اضافه کنید:

```
useradd librenms -d /opt/librenms -M -r
usermod -a -G librenms www-data
```

LibreNMS را دانلود کنید:

```
cd /opt

git clone https://github.com/librenms/librenms.git
```

سپس مجوزها را تنظیم کنید:

```
chown -R librenms:librenms /opt/librenms
chmod 770 /opt/librenms
setfacl -d -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/
setfacl -R -m g::rwx /opt/librenms/rrd /opt/librenms/logs /opt/librenms/bootstrap/cache/ /opt/librenms/storage/
```

آپاچی را پیکربندی کنید:

```
vi /etc/apache2/sites-available/librenms.conf
```

پیکربندی زیر را اضافه کنید، در صورت لزوم ServerName را ویرایش کنید:

```
<VirtualHost *:80>
  DocumentRoot /opt/librenms/html/
  ServerName  librenms.example.com
  AllowEncodedSlashes NoDecode
  <Directory "/opt/librenms/html/">
    Require all granted
    AllowOverride All
    Options FollowSymLinks MultiViews
  </Directory>
```

```
</VirtualHost>
```

سپس دستورات زیر را اجرا کنید:

```
a2ensite librenms.conf
a2enmod rewrite
systemctl restart apache2
```

از طریق دستورات زیر، سرویس snmpd را پیکربندی نمایید:

```
cp /opt/librenms/snmpd.conf.example /etc/snmp/snmpd.conf
vi /etc/snmp/snmpd.conf
```

متنی را که RANDOMSTRINGGOESHERE در آن آمده را ویرایش کنید و رشته خود را تنظیم کنید:

```
curl -o /usr/bin/distro https://raw.githubusercontent.com/librenms/librenms-agent/master/snmp/distro
chmod +x /usr/bin/distro
systemctl restart snmpd
```

آنرا به عنوان Cron job به سیستم اضافه کنید:

```
cp /opt/librenms/librenms.nonroot.cron /etc/cron.d/librenms
```

LibreNMS لاگ‌ها را در / opt / librenms / log نگه می‌دارد. با گذشت زمان، این‌ها می‌توانند بزرگ شوند و سربار زیادی به سیستم تحمیل کنند.

برای چرخاندن لاگ‌های مربوط می‌توانید از فایل پیکربندی ارائه شده در logrotate استفاده کنید:

```
cp /opt/librenms/misc/librenms.logrotate /etc/logrotate.d/librenms
```

در نهایت، به سراغ نصب‌کننده وب در آدرس زیر بروید و دستورالعمل‌های آنرا دنبال کنید.

```
http://librenms.example.com/install.php
```

۴-۶-۱۰ NetCrunch

NetCrunch یا نت‌کرانچ، یک سیستم جامع مانیتورینگ بدون عامل می‌باشد که قادر به مانیتور کردن هزاران نود شبکه (سوییچ، روتر، فایروال، پرینتر، سنسورها و غیره) می‌باشد. این سیستم بر روی ویندوز نصب شده و دارای کنسول وب، موبایل (Android, iOS (Blackberry و دسکتاپ است .نت‌کرانچ به صورت موثر داده‌های شبکه را سازماندهی کرده، به صورت خودکار شبکه را پویش کرده و نماها و نقشه‌های (منطقی و فیزیکی) شبکه را ایجاد می‌کند. این نرم افزار، تمامی‌سیستم عامل‌های مرسوم از قبیل ویندوز، لینوکس، VMware ESX/ESXi، Mac OS X و BSD را پشتیبانی می‌کند. همچنین انواع ترافیک‌های مرسوم شبکه مانند NetFlow, IPFix و غیره در این سیستم قابل نظارت هستند. در مورد اکثر نرم‌افزارهای مرسوم مانند MS SQL و MS Exchange، این نرم‌افزار بسته‌های نظارتی از پیش تعیین شده دارد که باعث سهولت، دقت و سرعت در تعریف و نظارت این نرم‌افزارها می‌شود [۲۸].

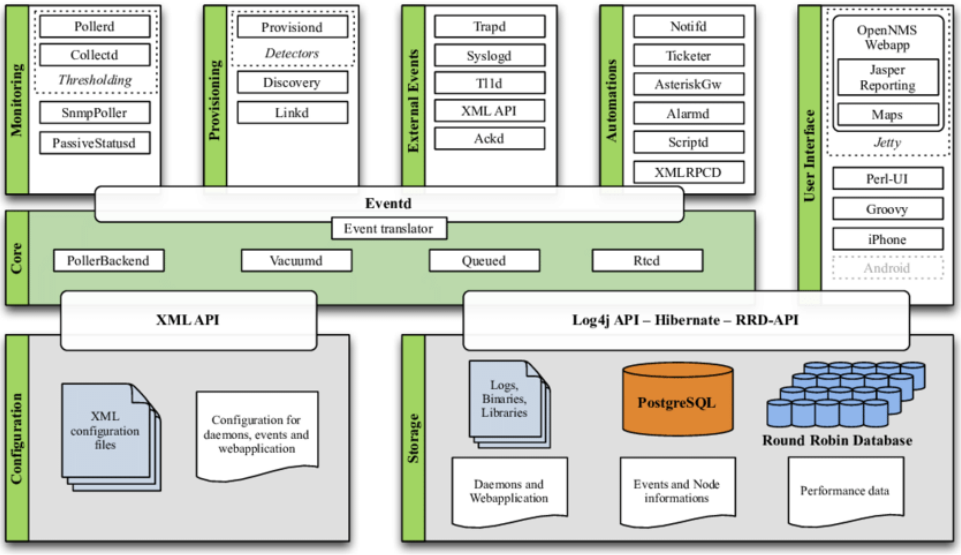
مزایا:

- نت‌کرانچ قادر به مانیتورینگ کارایی سیستم‌عامل‌های مختلف مانند Linux، BSD و Mac OS X از راه دور و از طریق SSH می‌باشد. مانیتورینگ ویندوز با ActiveDirectory یکپارچه شده و قادر به مانیتورینگ کارایی و Log Event است.
- نت‌کرانچ از فناوری‌های مختلف سیسکو مانند VOIP پشتیبانی می‌کند. همچنین از فناوری NBAR سیسکو پشتیبانی می‌شود.
- نت‌کرانچ قادر به مانیتورینگ VMware و V-Hyper به همراه وضعیت سخت‌افزاری و ماشین‌های مجازی می‌باشد.
- برای مانیتورینگ برنامه‌هایی مانند MS SQL وExchange، نت‌کرانچ بیش از ۱۰۰ بسته از پیش‌تعریف شده ارایه کرده است.
- نت‌کرانچ از SNMP برای مدیریت دستگاه‌های شبکه (سویتچر، پرینتر و غیره) استفاده می‌کند.
- نت‌کرانچ از مانیتورینگ بیش از ۶۰ سرویس شبکه (PING، HTTP، DNS، SSH و غیره) پشتیبانی می‌کند. برای مانیتورینگ برنامه‌های پیچیده، از سنسورهایی استفاده می‌کند که شامل: سرور آپاچی، لاگ‌های متنی، صفحات وب، پاسخ HTTP، مانیتورینگ فایل و فولدر (ویندوز،HTTP وFTP) صندوق‌پستی و مانیتورینگ ایمیل ارسالی و دریافتی، پرس‌وجوی DNS و مانیتورینگ معکوس می‌باشد.
- سرور flow نت‌کرانچ امکان گردآوری اطلاعات ترافیک شبکه از منابع مختلف flow با استفاده از IPFix، NetFlow، JFLOW، sFow، netStream، CFlowT، AppFlow و پروتکل‌های rflow میسر می‌سازد.
- نت‌کرانچ دارای امکان برنامه نویسی و API بوده و از بسیاری از نرم‌افزارها و برنامه‌ها مانند NetApp، Juniper، HP, IBM, Avaya, APC, Oracle و بسیاری از آنتی‌ویروس‌ها پشتیبانی می‌کند.
- مانیتورینگ انواع نرم‌افزارها و تجهیزات
- مدیریت لاگ‌ها و سامانه هشداردهی
- چرخه کامل مانیتورینگ، هشداردهی، بازیابی خطا و گزارش‌دهی
- دارای Heartbeat و syslog
- امکان ایجاد داشبوردهای مختلف
- دارای کمپایلر جهت اضافه کردن اسکریپت‌های MIB

۴-۶-۱۱ OpenNMS

OpenNMS یک نرم‌افزار مدیریت شبکه منبع‌باز سطح سازمانی است که امکان خودکارسازی مدیریت رویدادها و اطلاع‌رسانی‌ها، اندازه‌گیری وضعیت عملکرد و ویژگی‌های تضمین عملکرد را فراهم می‌کند. علاوه بر رابط کاربری تحت وب، OpenNMS به یک اپلیکیشن موبایلی برای دسترسی همیشگی به این ابزار مجهز است و به شما این امکان را می‌دهد تا امکانات موجود را به صورت سفارشی در یک رابط گرافیکی کاربرپسند در اختیار داشته باشید [۲۹]. بعد از این‌که با موفقیت به رابط کاربری تحت وب OpenNMS وارد شدید، می‌توانید از طریق داشبورد تعبیه‌شده به

سرعت به تمام اطلاعیه‌ها و هشدارها دسترسی پیدا کنید. همچنین می‌توانید اطلاعات دقیق‌تری درباره هر یک از بخش‌های موجود از طریق منوی Status به دست آورید. بخش گزارش‌ها به شما اجازه می‌دهد گزارش‌های تولیدشده را از طریق ایمیل یا دانلود فایل PDF به دست آورید. معماری کلی این نرم‌افزار در شکل زیر نشان داده شده است. پیکربندی نرم‌افزار از طریق فایل‌های XML و توابع API امکان‌پذیر است و همینطور، برای ذخیره‌سازی نیز از پایگاه‌داده و بانک‌های اطلاعاتی مختلف بهره گرفته می‌شود. در هسته نرم‌افزار، سرویس eventd مسئول شناسایی رویدادهای رخ داده در سیستم می‌باشد.



شکل ۸: معماری OpenNMS

مزایا:

- پشتیبانی از چند سیستم‌عامل از جمله ویندوز، مک، لینوکس / یونیکس و سولاریس
- مدیریت عملکرد و مدیریت خطا
- ارسال اطلاع از طریق ایمیل
- داشبورد قابل دسترس از وب
- امکان پردازش صدها هزار پیام Syslog در هر دقیقه، به طور مداوم

۱-۱۱-۶-۴ نصب

ابتدا باید پیش‌نیازهای زیر در سیستم نصب شوند:

- یک سرور در حال اجرا اوبونتو ۱۶.۰۴
- کاربر غیر از root با تنظیمات sudo در سرور
- یک آدرس IP ایستا مانند ۱۹۲.۱۶۸.۰.۱۸۷ در سرور

مراحل نصب با به‌روزرسانی سیستم خود به آخرین نسخه پایدار شروع می‌شود. می‌توان این کار را با اجرای دستور زیر انجام داد [۳۰]:

```
sudo apt-get update-so
sudo apt-get upgrade -y
```

پس از به روز رسانی سیستم، باید نام دامنه مناسب کامل را تعیین کرد. شما می‌توانید با ویرایش فایل / etc / hosts این کار را انجام دهید:

```
sudo nano / etc / hosts
```

خط زیر را به آن اضافه کنید:

```
192.168.0.187 server.opennms.local server
```

فایل hostname / etc / را باز کرده و در آن خط بعد را اضافه کنید:

```
server.opennms.local
```

پس از اتمام ذخیره فایل، در نهایت سیستم خود را برای اعمال تغییرات راه اندازی مجدد کنید.

OpenNMS نیاز به PostgreSQL برای هدف پایگاه‌داده دارد. شما می‌توانید PostgreSQL را با اجرای دستور زیر نصب کنید:

```
sudo apt-get install postgresql -y
```

پس از نصب PostgreSQL، شما باید اجازه دسترسی به پایگاه داده را به کاربر بدهید. PostgreSQL فقط به شما اجازه اتصال می‌دهد اگر شما به نام حساب محلی منطبق با نام کاربری PostgreSQ وارد شوید. از آنجا کهOpenNMS به عنوان root اجرا می‌شود، بنابراین شما نیاز به تغییر تنظیمات برای اجازه کاربر root داری. که این کار با ویرایش فایل pg_hba.conf امکان‌پذیر است:

```
sudo nano /etc/postgresql/9.5/main/pg_hba.conf
```

خطوط زیر را پیدا کنید:

```
local   all     all                     local
host    all     all     127.0.0.1/32    md5
host    all     all     ::1/128         md5
```

آن‌ها را مشابه خطوط زیر تغییر دهید:

```
ocal   all     all                     trust
host    all     all     127.0.0.1/32    trust
host    all     all     ::1/128             trust
```

پس از اتمام ذخیره و بستن فایل، سرویس PostgreSQL را راه اندازی مجدد و آن را با دستور زیر فعال کنید:

```
sudo systemctl restart postgresql
sudo systemctl enable postgresql
```

در گام بعد جاوا را نصب کنید. از آنجا که OpenNMS هنوز جاوا ۸ را پشتیبانی نمی‌کند ناگزیر به نصب جاوا ۷ می‌باشیم.

به طور پیش فرض OpenNMS در مخزن پیش‌فرض اوبونتو موجود نیست. بنابراین شما باید مخزن OpenNMS را به دایرکتوری /etc/apt/sources.list.d اضافه کنید. شما می‌توانید این کار را با اجرای دستور زیر انجام دهید:

```
sudo nano /etc/apt/sources.list.d/opennms.list
```

خطوط زیر را اضافه کنید:

```
deb http://debian.opennms.org stable main
deb-src http://debian.opennms.org stable main
```

پس از اتمام ذخیره فایل، سپس کلید OpenNMS را با فرمان زیر وارد کنید:

```
wget -O - http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -
```

اکنون فهرست لیست مخزن را با استفاده از دستور زیر به‌روز کنید:

```
sudo apt-get update -y
```

هنگامی‌که مخزن به روز شد، OpenNMS را با اجرای دستور زیر نصب کنید:

```
sudo apt-get install default-mta opennms -y
```

پس از نصب OpenNMS، شما باید یک پایگاه‌داده برای OpenNMS ایجاد کنید. شما می‌توانید این کار را با اجرای دستور زیر انجام دهید:

```
sudo /usr/share/opennms/bin/install -dis
```

خروجی زیر نمایش داده می‌شود:

```
OpenNMS Installer
================================================================================
Configures PostgreSQL tables, users, and other miscellaneous settings.
.
.
.
- Running post-execution phase
```

```
Removing backup /usr/share/opennms/etc/discovery-configuration.xml.zip
Finished in 0 seconds
```

درنهایت، سرویس OpenNMS را با دستور زیر شروع کنید:

```
sudo systemctl start opennms
```

به طور پیش‌فرض، OpenNMS روی پورت ۸۹۸۰ اجرا می‌شود. بنابراین باید به پورت ۸۹۸۰ از طریق فایروال UFW اجازه دهید. اما به طور پیش فرض UFW در سیستم شما غیرفعال است، بنابراین باید ابتدا آن را فعال کنید. با دستور زیر می‌توان آن را فعال کرد:

```
sudo ufw enable
```

پس از فعال کردن فایروال UFW ، می‌توانید با اجرای دستور زیر، پورت ۸۹۸۰ را مجاز کنید:

```
sudo ufw allow 8980
```

اکنون می‌توانید با اجرای دستور زیر ، وضعیت فایروال UFW را بررسی کنید:

```
sudo ufw status
```

۴-۶-۱۳ Icinga

Icinga یک نرم‌افزار منبع‌باز برای نظارت بر عملکرد شبکه و نرم‌افزارها و دستگاه‌های مختلف است. این برنامه به عنوان انشعابی از برنامه معروف Nagios که قبلا معرفی شد، در سال ۲۰۰۹ ایجاد شد [۳۱]. Icinga در تلاش است تا خود را به روند توسعه Nagios برساند، و همچنین درصدد اضافه کردن ویژگی‌های جدید مانند رابط کاربری مدرن به سبک Web 2.0، اتصالات پایگاه‌داده اضافی (برای MySQL، Oracle و PostgreSQL) و توابع REST API می‌باشد. همچنین به مدیران اجازه می‌دهد کاربران متعددی را بدون اصلاح هسته پیچیده Icinga تعریف و ادغام کنند. توسعه‌دهندگان Icinga همچنین به دنبال انعکاس بیشتر نیازهای جامعه کاربران این حوزه هستند. اولین نسخه پایدار، ۱.۰، در دسامبر ۲۰۰۹ منتشر شد و از ژانویه ۲۰۱۰ هر دو ماه یک نسخه جدید ارائه شده است.

مزایا:

- Icinga ویژگی‌های Nagios را با برخی از موارد اضافی مانند ماژول گزارش اختیاری، اتصالات پایگاه‌داده اضافی برای PostgreSQL و Oracle ارائه می‌دهد و روال‌هایی را برای نظارت بر کاربری، ایجاد می‌کند.
- Icinga همچنین پیکربندی و سازگاری افزونه را با Nagios حفظ کرده و مهاجرت بین دو نرم‌افزار نظارت را تسهیل می‌کند.
- امکان نظارت بر سرویس‌ها و پروتکل‌های شبکه (SMTP، POP3، HTTP، NNTP، پینگ و غیره)
- امکان نظارت بر منابع دستگاه (بار پردازنده، استفاده از دیسک و غیره)

- امکان نظارت بر اجزای سرور (سوئیچ‌ها ، روترها ، سنسور دما و رطوبت ، و غیره)
- طراحی افزونه ساده‌ای که به کاربران امکان می‌دهد چک‌های سرویس خود را به راحتی توسعه دهند
- امکان تعریف سلسله مراتب شبکه با استفاده از میزبان‌های والد و فرزند
- امکان تشخیص و تمایز بین میزبان‌هایی که پایین آمده و غیر قابل دستیابی هستند
- امکان تعریف کارگزاران رویداد در حین سرویس برای حل مشکل پیش آمده
- اطلاع به افراد مخاطب (از طریق ایمیل، پیجر، پیام فوری) در صورت بروز مشکلات سرویس یا میزبان
- ارسال هشدارها به سایر کاربران یا کانال‌های ارتباطی
- ارائه داشبورد برای نمایش گزارشات
- دو رابط کاربری اختیاری (Icinga Classic UI و Icinga Web) برای نمایش وضعیت میزبان و سرویس، نقشه‌های شبکه و گزارش‌ها
- ماژول Reporting Icinga، برپایه نرم‌افزار منبع‌باز Jasper Reports، برای رابط‌های کاربری Icinga Classic و Icinga Web
- گزارش‌های مبتنی بر الگوی پیش‌فرض و کاربردی (به عنوان مثال، مشاهده ۱۰ میزبان یا خدمات اول دارای مشکل، خلاصه‌ای از نظارت کامل محیط، گزارش‌های در دسترس بودن و غیره)
- گزارش مخزن با سطوح مختلف دسترسی و تولید و توزیع گزارش خودکار
- پسوند اختیاری برای گزارش SLA که بین وقایع مهم از وقفه‌های برنامه‌ریزی شده و غیر برنامه‌ریزی شده و دوره‌های تأیید تمایز قائل می‌شود.
- گزارش استفاده از ظرفیت سامانه
- نمودار عملکرد از طریق افزودنی‌هایی مانند PNP4Nagios، NagiosGrapher و InGraph

۱-۱۲-۶-۴ نصب

بهترین روش برای نصب Icinga، استفاده از منبع پکیج برنامه با توجه به سیستم‌عامل مورد استفاده، می‌باشد [۳۱]. برای اینکار، شما باید مخزن Icinga را به پیکربندی مدیریت پکیج خود اضافه کنید. دستورات زیر باید با مجوز root اجرا شوند.

```
apt-get update
apt-get -y install apt-transport-https wget gnupg

wget -O - https://packages.icinga.com/icinga.key | apt-key add -
```

```
. /etc/os-release; if [ ! -z ${UBUNTU_CODENAME+x} ]; then DIST="${UBUNTU_CODENAME}"; else DIST="$
(lsb_release -c| awk '{print $2}')"; fi; \
 echo "deb https://packages.icinga.com/ubuntu icinga-${DIST} main" > \
 /etc/apt/sources.list.d/${DIST}-icinga.list
 echo "deb-src https://packages.icinga.com/ubuntu icinga-${DIST} main" >> \
 /etc/apt/sources.list.d/${DIST}-icinga.list

apt-get update
```

سپس، می‌توان Icinga را با استفاده از مدیر پکیج توزیع خود برای نصب بسته Icinga، نصب کرد. دستور زیر باید با مجوزهای root اجرا شود:

```
apt-get install icinga2
```

بدون پلاگین، Icinga نمی‌داند چگونه خدمات خارجی را بررسی کند. Icinga مجموعه وسیعی از افزونه‌ها را ارائه می‌دهد که می‌توانند با Icinga مورد استفاده قرار گیرند؛ تا بررسی کنند آیا خدمات به درستی کار می‌کنند یا خیر. با دستور زیر می‌توان افزونه‌ها را نصب کرد:

```
apt-get install monitoring-plugins
```

۱۳-۶-۴ PRTG Network Monitor

PRTG Network Monitor را می‌توان به عنوان یک ابزار حرفه‌ای نظارت و کنترل شبکه‌های کامپیوتری معرفی کرد که با کمک آن می‌توان کارهایی از قبیل نظارت بر سخت‌افزار، نرم‌افزار، برنامه‌های نصب شده، سیستم‌عامل‌ها، up/downtime، ترافیک شبکه، packet sniffing و غیره را به راحتی انجام داده و گزارش‌های کلی یا جزئی به منظور ارائه تجزیه و تحلیل دقیق از عملکرد شبکه تهیه کرد. رابط کاربری مبتنی بر وب این برنامه امکان پیکربندی سریع تنظیمات دلخواه مربوط به نظارت بر دستگاه‌های شبکه و سنسورهای آن‌ها را برای کاربران فراهم می‌کند. اغلب روش‌های متداول مربوط به اکتساب داده در شبکه، مانند Packet Sniffing & SNMP ، WMI و NetFloa توط این نرم‌افزار پشتیبانی می‌شوند. PRTG Network Monitor را می‌توان برای شبکه‌هایی همچون شبکه‌های موجود در یک ISP و روترها و سوئیچ‌های مورد استفاده در آن‌ها استفاده نمود. از ویژگی‌های مهم این نرم‌افزار می‌توان به بهینه‌سازی دستگاه‌های مورد استفاده به منظور کاهش Downtime، مدیریت بر گروه‌ها و کاربران مدیریتی در شبکه، مشاهده چگونگی فعالیت تجهیزات در روزهای مختلف و دوره‌های تعیین شده، ارسال آلارم‌های تعریف شده به گوشی همراه اشاره کرد. این نرم‌افزار به گفته شرکت سازنده ساده‌ترین و آسان‌ترین راهکار مانیتورینگ شبکه است که می‌توان آن را بدون دردسر در عرض ۵ دقیقه تنظیم کرد تا در شبکه مشغول فعالیت شود. این نرم‌افزار می‌تواند به محض بروز اتفاق‌های غیرعادی در شبکه برای شما پیام اخطار صادر

کند، بیش از ۱۵۰ هزار مدیر سیستم در دنیا از این نرم افزار استفاده می‌کنند و در شرکت‌هایی با سایزهای کوچک تا سازمان‌هایی با ابعاد بزرگ نیز قابل استفاده است [۳۲].

مزایا:

- تشخیص خودکار دستگاه‌های موجود در شبکه پس از نصب
- رابط کاربری تعاملی و قابل تنظیم
- نظارت کامل و دقیق بر کلیه دستگاه‌های موجود در شبکه
- نمایش تنظیمات پیکربندی به صورت سلسله مراتبی درختی با پشتیبانی از ویژگی ارث‌بری تنظیمات
- معماری مدرن و عملکرد بهینه نرم‌افزار
- کنترل پهنای‌باند مورد استفاده
- بیش از ۵۰ سنسور به منظور فراهم آوردن یک نظارت جامع درشبکه‌های کوچک یا بزرگ
- نظارت بر کارایی و در دسترس بودن اعضای شبکه
- امکان کنترل روترها و سوئیچ‌های شبکه

۴-۶-۱۴ Monitorix

monitorix یا مانیتوریکس یک ابزار قدرتمند و رایگان و به صورت منبع‌باز بوده که به منظور نظارت بر منابع شبکه و سیستم طراحی شده است. این نرم‌افزار به صورت منظم اطلاعات شبکه و سیستم را جمع‌آوری کرده و این اطلاعات را به صورت گراف و با استفاده از رابط‌کاربری وب نمایش می‌دهد. مانیتوریکس بر بازدهی تمامی‌بخش‌های سیستم نظارت می‌کند و همچنین به شناسایی مشکلات پردازش، نقایص، مدت زمان پاسخ‌های ناخواسته و دیگر فعالیت‌های غیر طبیعی کمک می‌کند [۳۳].

این برنامه به زبان Perl نوشته شده و تحت مجوز GNU General Public License می‌باشد و توسط FSB Free Software Foundation منتشر شده است. این نرم‌افزار برای ایجاد گراف‌ها و نمایش آن‌ها تحت رابط‌کاربری وب از RRDtool استفاده می‌کند. این ابزار مخصوص مانیتورینگ سیستم‌عامل‌های لینوکس Red Hat , Centos , Fedora ایجاد شده است؛ اما امروزه روی توزیع‌های دیگر GNU/Linux و حتی روی سیستم‌های UNIXمانند OpenBSD , NetBSD و FreeBSD اجرا می‌شود.

مزایا:

- نظارت بر میانگین بار سیستم، پراسس‌های فعال، میزان استفاده کرنل به ازای هر پردازنده و وضعیت Memory
- نظارت بر دما و سلامت Disk Drive
- نظارت بر میزان استفاده Filesystem و فعالیت I/O فایل سیستم‌ها

- نظارت بر میزان استفاده ترافیک شبکه تا ۱۰ کارت شبکه
- نظارت بر سرویس‌های سیستم از جملهSPAM , VIRUSMAIL , IMAP , POP3 SMTP , PROFTP , VSFTPD , FTP , SSH
- ارائه آمارهای MTA Mail شامل کانکشن‌های ورودی و خروجی
- نظارت ترافیک پورت شبکه شامل TCP , UDP
- ارائه آمارهای سرورهای FTP
- ارائه آمارهای آپاچی سرورهای Remote یا Local
- ارائه آمارهای MySQL سرورهای Remote یاLocal
- ارائه آمارهای Proxy Squid
- ارائه آمارهای Fial2ban
- ارائه آمار سرورهای ریموت (Multihost)
- ارائه توانایی نمایش آمار در گراف‌ها یا در جداول متنی ساده به ازای روز هفته ماه یا سال
- توانایی در بزرگ‌نمایی گراف‌ها برای نمایش بهتر
- دارای وب سرور درونی

۱-۱۴-۶-۴ نصب

ابتدا یک نسخه پشتیبان از منابع اصلی تهیه می‌کنیم:

```
cp -pf /etc/apt/sources.list /etc/apt/sources.list_bak
```

سپس فایل Source.list را در یک ویرایشگر باز کنید. در اینجا از nano استفاده شده است [۳۴]:

```
sudo nano /etc/apt/sources.list
```

در پنجره باز شده، مکان‌نما را در انتهای پرونده قرار دهید و این خط را اضافه کنید:

```
deb http://apt.izzysoft.de/ubuntu generic universe
```

پس از اضافه کردن منبع، ما باید کلید PGP را بارگیری (یا اضافه کنیم) و آن را درون سیستم "نصب" کنیم. می‌توان کلید را مستقیماً از طریق http://apt.izzysoft.de/izzysoft.asc با wget بارگیری کرد.

```
sudo apt-get -y install wget
cd /tmp
wget http://apt.izzysoft.de/izzysoft.asc
```

حال باید به دایرکتوری برویم که در آن پرونده asc. را ذخیره کردیم و یک پنجره ترمینال را باز کرده و دستور زیر را اجرا می‌کنیم:

```
sudo apt-key add izzysoft.asc
```

در نهایت، مخزن را به‌روز می‌کنیم:

```
sudo apt-get update
```

اکنون بسته "Monitorix" را نصب می‌کنیم. Apt وابستگی‌ها را به صورت خودکار نصب می‌کند.

```
sudo apt-get -y install monitorix apache2-utils
```

گزینه پیکربندی Monitorix.conf واقع در /etc/monitorix/monitorix.conf/ را داریم:

```
sudo nano /etc/monitorix/monitorix.conf
```

در پنجره باز شده، خطوط زیر را پیدا کنید:

```
<auth>
 enabled = n
 msg = Monitorix: Restricted access
 htpasswd = /var/lib/monitorix/htpasswd
 </auth>
```

با تغییر enabled به :"y" ، تایید اعتبار را فعال کنید:

```
<auth>
 enabled = y
 msg = Monitorix: Restricted access
 htpasswd = /var/lib/monitorix/htpasswd
 </auth>
```

پس از پیکربندی، باید سرویس مانیتور را مجدداً راه‌اندازی کنیم:

```
sudo service monitorix restart
```

یک نام کاربری و رمز ورود برای ورود به Monitorix اضافه کنید. در مثال زیر از نام کاربری "مدیر" با رمز "howtoforge" استفاده شده است.

```
sudo htpasswd -d -c /var/lib/monitorix/htpasswd admin
```

ما از پارامتر d- برای رمزگذاری رمز عبور با استفاده از()crypt استفاده می‌کنیم، چون توسط Monitorix خواسته شده است. دستورات رد و بدل شده مشابه زیر خواهد بود:

```
david@desktop:/tmp# sudo htpasswd -d -c /var/lib/monitorix/htpasswd admin
New password:
Re-type new password:
Adding password for user admin
```

در نهایت برای اجرا و دسترسی به واسط کاربری، مرورگر را به آدرس http://192.168.1.100:8080/monitorix/ باز می‌کنیم. (آدرس را با IP سرور خود جایگزین کنید)

۵. کنترل دسترسی

یکی از مباحث مهم در حوزه امنیت اطلاعات آگاهی از الزامات کنترل دسترسی و پیاده‌سازی مطمئن یک سامانه از نظر محرمانگی و صحت دسترسی و کنترل آن می‌باشد. در این قسمت تلاش می‌کنیم انواع کنترل دسترسی و ابزارهای موجود برای پیاده‌سازی آنرا بیان کنیم.

کنترل دسترسی در سامانه‌های اطلاعاتی و شبکه‌های ارتباطی به منظور حفظ محرمانگی و صحت داده‌ها و دسترس‌پذیری استفاده می‌شود، زیرا باعث می‌شود که افراد غیرمجاز به داده‌های محرمانه دسترسی نداشته باشند. به طور کلی، کنترل دسترسی در جهت صحت داده‌ها سه هدف زیر را دنبال می‌کند:

- پیشگیری از دستکاری داده‌ها توسط کاربران غیرمجاز
- پیشگیری از تغییر داده‌ها به صورت عمدی یا غیرعمدی توسط کاربران مجاز و ردیابی دسترسی آنها
- حفظ ثبات داده‌های داخلی و خارجی
  - **حفظ ثبات داخلی** به این معنی که فرض کنیم که یک پایگاه داده داخلی دارای تعدادی اقلام داده تکراری از یک مورد خاص در هر بخش از سازمان است که تمامی آنها دارای مقدار برابر و سازگار می‌باشند.
  - **حفظ ثبات خارجی** تضمین می‌کند که داده‌های ذخیره شده در پایگاه داده سازگار با جهان واقعی هستند.

به صورت کلی، کنترل دسترسی می‌تواند به دو شکل کنترل منطقی و فیزیکی اعمال شود. کنترل منطقی شامل ایجاد محدودیت دسترسی به سامانه و حفاظت اطلاعاتی از طریق تعریف نام‌کاربری و رمز، کارتهای هوشمند، لیستهای کنترل دسترسی، پروتکل‌های انتقال و سایر موارد می‌باشد. کنترل فیزیکی شامل استفاده از نگهبانان، کنترل امنیتی ساختمان با استفاده از دوربین‌های مداربسته، درب‌های ضدسرقت، امنیت اتاق

سرور، محافظت از بستر کابل کشی، پشتیبان‌گیری از فایل‌ها، مراقبت از کامپیوترهای مستقر در سازمان و لپ تاپ‌های مورد استفاده مدیران که به نوعی باعث خروج اطلاعات از سازمان می‌شود می‌باشد.

قوانین مربوط به کنترل دسترسی را می‌توان به سه دسته یا مدل تقسیم کرد:

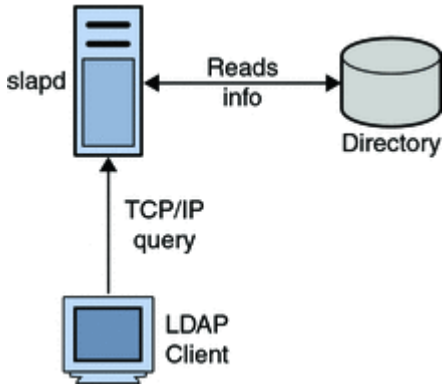
- **کنترل دسترسی اجباری:** مجوزهای اجباری دسترسی به یک موضوع حساس و طبقه‌بندی شده داده می‌شود. به عنوان مثال، می‌توان اسناد و مدارک محرمانه نظامی و یا به طور کلی‌تر هر موضوع با درجه طبقه‌بندی بالاتر را نام برد که افراد هرچند برای کارشان نیازمند استفاده از آنها می‌باشند ولی باز بر اساس قانون کنترل دسترسی باید مجوزهای لازم را دریافت کنند. در این نوع موارد، شناسایی هویت فرد تنها کافی نیست و نیاز به مکاتبات کتبی سازمان مربوطه را نیز دارد.
- **کنترل دسترسی اختیاری:** در برخی موارد، برای مشخص کردن اشیاء و موضوعات در دسترس از لیست‌های کنترل دسترسی (access control list) می‌توان استفاده کرد که همان فهرستی از کاربران است که نشان دهنده میزان دسترسی آنها به فایل‌ها و منابع خاص را مشخص می‌کند. لیست کنترل دسترسی معمولا به صورت سه‌گانه‌ای متشکل از کاربر، برنامه و فایل با امتیازات دسترسی مربوطه برای هر کاربر می‌باشد. این نوع از کنترل دسترسی در موقعیت‌های مختلف محلی و یا دامین به تشخیص مدیران برای مشخص کردن منابع مورد نیاز کاربران و سطح دسترسی‌های مجاز آنها مورد استفاده قرار می‌گیرد. در برخی موارد، کاربران می‌توانند به اختیار خود منابع مربوط به حوزه کاری خود را ویرایش کنند، به همین دلیل هم از آن به عنوان کنترل دسترسی اختیاری نام برده می‌شود که البته مبتنی بر هویت فرد است.
- **کنترل دسترسی غیراختیاری:** در حالت معمول، کنترل دسترسی می‌تواند بر اساس مسئولیت فرد در سازمان (مبتنی بر وظیفه) و یا نقش راهبردی افراد باشد و متاثر از محل، زمان، روز، و تاریخچه ای از دسترسی‌های قبلی که می‌تواند باعث قبول یا رد موضوعاتی توسط افراد شود.

۵-۱ معرفی سامانه‌های کنترل دسترسی

۵-۱-۱ OpenLDAP

این ابزار بر اساس پروتکل موفق LDAP که توسط تیم‌هاوز و همکارانش در دانشگاه میشیگان ایجاد شده است، ساخته شده است. LDAP با معماری سرور- کلاینت کار می‌کند که کلاینت پس از تأیید اعتبار، اطلاعات را درخواست می‌کند. هدف از خدمات در آن زمان، ایجاد پروتکل سبک وزن بود که امکان تأیید اعتبار و مجوز کاربران به سرورها و برنامه‌ها را می‌دهد. در حقیقت، LDAP آنقدر محبوب بود که در اواخر دهه ۹۰ و اوایل دهه ۲۰۰۰ به پروتکل احراز هویت استاندارد اینترنت تبدیل شد. این محبوبیت روزافزون، علیرغم اعلامیه شرکت‌هایی همچون RedHat و SUSE مبنی بر عدم استفاده از OpenLDAP در محصولات خود، OpenLDAP را به نرم‌افزار رایج در سرورها تبدیل کرد. صرف نظر از این، OpenLDAP برای بسیاری از سازمان‌ها یک پروتکل احراز هویت فوق‌العاده مهم است. بسیاری از سازمان‌ها برای راهکارهای فنی به این ابزار احتیاج

دارند. این نیازمندی‌ها شامل سرورها و برنامه‌های مبتنی بر لینوکس است. به همین دلیل، از لحاظ تاریخی، OpenLDAP مورد استقبال جمیع شرکت‌ها و افرادی است که عموماً طرفدار راه‌حل‌های منبع باز هستند. از سوی دیگر، انعطاف پذیری باورنکردنی که نتیجه طراحی و پیاده‌سازی فوق‌العاده آن است، مهندسین فناوری اطلاعات و توسعه‌دهندگان نرم‌افزار را قادر می‌سازد، به روش‌های مختلفی از آن استفاده کنند [۳۵]. معماری کلی این نرمافزار در شکل زیر نشان داده شده است. اطلاعات کاربران در پایگاه داده قرار دارد. سرویس slapd به عنوان سرور یا سرویس‌دهنده، درخواست‌های مشتریان را مورد بررسی قرار می‌دهد:



شکل ۹: معماری OpenLDAP

مزایا:

- پشتیبانی از احراز هویت ساده و امنیتی و امنیت لایه انتقال
- پشتیبانی از پروتکل اینترنت نسل بعدی (نسخه ۶)
- برخورداری از توابع CI API برای بهبود اتصال برنامه‌نویسان به سرورهای LDAP
- پشتیبانی DIF و سازگاری کامل با فرمت تبادل داده LDIF
- سرور به مستقل و مستقیم روی TCP / IP و SSL اجرا می‌شود
- استفاده توسط بسیاری از سرویس‌ها مانند TCP و DNS
- منبع باز همراه با معماری بسیار انعطاف پذیر

۱-۱-۱-۵ نصب:

ابتدا موارد پیش‌نیاز باید نصب شوند:

```
yum install *openldap* -y
```

سپس، سرویس OpenLDAP باید راه‌اندازی شود:

```
[root@ldap ~]# chkconfig --levels 235 ldap on
[root@ldap ~]# service ldap start
```

سپس حساب کاربری باید ایجاد شود:

```
[root@ldap ~]# slappasswd
  New password:
  Re-enter new password:
  {SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW
[root@ldap ~]#
```

پیکربندی و راه‌اندازی مجدد نرم‌افزار نیز به این صورت انجام می‌شود:

```
[root@ldap ~]# vi /etc/openldap/slapd.conf
  #68 database      bdb
  #69 suffix        "dc=adminmart,dc=com"
  #70 rootdn        "cn=Manager,dc=adminmart,dc=com"
  #71 rootpw        {SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW
[root@ldap ~]# service ldap restart
```

۵-۱-۲ FreeIPA

FreeIPA یک راه‌حل یکپارچه مدیریت اطلاعات امنیتی است که ترکیبی از لینوکس (فدورا)، ۳۸۹ سرور دایرکتوری، MIT Kerberos، NTP، DNS و Dogtag (سیستم گواهی) است. این ابزار شامل یک رابط‌کاربری وب و ابزارهای مدیریت خط فرمان است. ابزار فوق یک راه‌حل یکپارچه هویت و تأیید هویت برای محیط‌های شبکه‌ای Linux / UNIX است. به مدیران سیستم لینوکس اجازه می‌دهد تا با عملیات ساده‌ی نصب و با استفاده از خط فرمان و ابزارهای مدیریتی مبتنی بر وب، مدیریت هویت، تأیید هویت و جنبه‌های کنترل دسترسی سیستم‌های لینوکس و یونیکس را مدیریت کنند. سرور آن با ذخیره کردن داده‌ها در مورد کاربر، گروه‌ها، فضای میزبانی و سایر مؤلفه‌های لازم برای مدیریت جنبه‌های امنیتی شبکه رایانه‌ها، تأیید هویت متمرکز، مجوز و اطلاعات حساب را فراهم می‌کند. بالاترین سطح از راه‌حل‌های منبع‌باز و پروتکل‌های استاندارد با تمرکز بسیار زیاد بر سهولت مدیریت و خودکارسازی عملیات نصب و تنظیمات در این راه‌حل در نظر گرفته شده است. همچنین FreeIPA می‌تواند از طریق ابزارهای Kerberos به صورت یکپارچه در یک محیط Active Directory ادغام شود و عملیات حسابرسی دسترسی کاربران را انجام دهد [۳۶].

مزایا:

- به کاربران اجازه می‌دهد تا با حقوق دسترسی و تنظیمات امنیتی یکسان و مشابه به کلیه سیستم‌های کامپیوتری درون شبکه دسترسی پیدا کنند.
- به کاربران اجازه می‌دهد تا با روش‌های معتبر و ایمن به فایل‌های شخصی خود از هر دستگاهی، دسترسی شفاف و مطمئن داشته باشند.
- از یک مکانیسم گروه‌بندی برای محدودکردن دسترسی از طریق شبکه به خدمات و فایل‌ها، برای کاربران خاص استفاده می‌کند.

- مدیریت مرکزی مکانیسم‌های امنیتی مانند گذرواژه‌ها، کلیدهای عمومی SSH، و قوانین کنترل دسترسی را فراهم می‌کند.
- تفویض وظایف مدیریتی انتخاب‌شده را به دیگر کاربران با حقوق دسترسی بالا ممکن می‌سازد.
- با محیط‌های Active Directory ادغام می‌شود.

۵-۱-۲-۱ نصب :

برای نصب سرور لازمست دستورات زیر اجرا شود:

```
# yum install freeipa-server
# ipa-server-install
```

ساخت حساب کاربری با دستور زیر انجام می‌شود:

```
# ipa user-add
```

برای اختصاص کلمه عبور نیز از دستور زیر استفاده می‌کنیم:

```
ipa passwd <user>
```

۵-۱-۳ ApacheDS

ApacheDS یک سرور دایرکتوری قابل توسعه و به صورت توکار است که به طور کامل با جاوا پیاده‌سازی شده است و دارای مجوز نسخه ۳ از پروتکل LDAP است. بنابراین با استفاده از دستورات LDAP ارائه شده توسط کلاینت‌های OpenLDAP، آن را به راحتی در دسترس قرار می‌دهد.علاوه بر LDAP از Kerberos و پروتکل تغییر رمز عبور نیز پشتیبانی می‌کند. این ابزار برای ورود و معرفی برنامه‌ها، رویه‌های ذخیره شده و موارد دیگر نرم‌افزاری به دنیای ایمن LDAP طراحی شده است که پیش از این فاقد این توانمندی مهم بوده‌اند [۳۷].

ApacheDS بر روی نصب، پیکربندی و مدیریت ساده متمرکز است. مجموعه ابزارهای موجود در استودیو دایرکتوری، برای مدیران فناوری اطلاعات وجود دارد که بتوانند ApacheDS را راحت‌تر پیاده‌سازی کنند. ابزارهای رابط‌کاربری شامل یک ویرایشگر شمای LDAP، مرورگر LDAP، ویرایشگر LDIF، ویرایشگر کنترل دسترسی و موارد دیگر است.

وجه تمایز اصلی ApacheDS با OpenLDAP و سایر راه‌حل‌های منبع‌باز مبتنی بر LDAP این است که ApacheDS رویه‌های ذخیره‌شده و کدهایی را برای نگهداری و کار با پایگاه‌داده و فرآیند مدیریت بانک‌اطلاعاتی، به صورت بهینه‌تر معرفی کرده است.

مزایا:

- به عنوان یک پلتفرم مشترک و با استفاده از LDAP و X.500 طراحی شده است. مولفه‌های قابل اتصال و زیرسیستم‌ها باعث می‌شود تا ApacheDS به ابزاری کاملاً ماژولار و ایده‌آل برای کار با جنبه‌های مختلف پروتکل LDAP تبدیل شود.
- قابلیت جداسازی عملیات ابتدایی سرور از عملیات انتهایی، آن‌را برای اجرا و پیاده‌سازی دایرکتوری‌های مجازی، پراکسی سرورها و دروازه‌ها به دایرکتوری‌های X.500 بسیار انعطاف‌پذیر می‌کند.

- سرور از یک پارتیشن مبتنی بر BTree پشتیبانی می‌کند، اما از هر ترمینال پشتیبان می‌توان با داشتن مجوزها و رابطها برای اجرای پارتیشن استفاده کرد.
- سرور جنبه‌های مدیریتی مختلفی را از طریق عملیات انتهایی مشخص در دسترس مدیران قرار می‌دهد. LDAP می‌تواند برای مدیریت این موارد و جنبه‌های سیستم استفاده شود.
- سرور آن شامل یک سرویس‌دهندهLDAP است که به عنوان یک سرویس برای کل زیرسیستم انتهایی عملیات را مستقیماً در پارتیشن‌های مورد نظر ذخیره شده در ورودی سرور تبدیل می‌کند.
- کد اجرایی تحت شبکه سرورها (زیرساخت چند منظوره برای برنامه‌های شبکه) برای همه نوع ارائه‌دهندگان پروتکل و نه فقطLDAP طراحی شده است. این ویژگی به ApacheDS این امکان را می‌دهد که تا حد زیادی از همزمانی پشتیبانی کند.
- رویه‌های ذخیره‌شده LDAP برای نسخه اصلی بعدی ApacheDS برنامه‌ریزی و فراهم شده است.
- سازگار با نسخه سوم از LDAP می‌باشد که توسط OpenGroup تایید شده است.

۵-۱-۳-۱ نصب :

دستور نصب سرور به صورت زیر می‌باشد:

```
sudo dpkg -i apacheds-2.0.0-M11-i386.deb
```

دستور راه‌اندازی سرور نیز به این صورت است:

```
sudo /etc/init.d/apacheds-2.0.0-M11-default start
```

در نهایت، دستور تنظیمات و پیکربندی انجام می‌شود:

```
sudo pico /var/lib/apacheds-2.0.0-M11/default/conf/config.ldif
```

۵-۱-۴ Active Directory

دایرکتوری یک ساختار سلسله‌مراتبی است که اطلاعات مربوط به اجزا و مولفه‌ها را در شبکه ذخیره می‌کند. یک سرویس دایرکتوری، مانند خدمات دامنه Active Directory، روش‌هایی را برای ذخیره داده‌های دایرکتوری و در دسترس قرار دادن این داده‌ها در اختیار کاربران و مدیران شبکه قرار می‌دهد. به عنوان مثال، Active Directory اطلاعات مربوط به حساب‌های کاربری مانند نام‌ها، کلمه عبورها، شماره تلفن‌ها و غیره را ذخیره می‌کند و سایر کاربران مجاز در همان شبکه را قادر می‌سازد تا به این اطلاعات دسترسی پیدا کنند. Active Directory اطلاعات مربوط به اجزا و مولفه‌های موجود در شبکه را ذخیره می‌کند و دسترسی به این اطلاعات را برای مدیران و کاربران تسهیل می‌کند تا آنها را بیابند و استفاده کنند. Active Directory از یک فضای ذخیره‌سازی ساخت‌یافته به عنوان زیرساخت برای یک ساختار منطقی و سلسله‌مراتبی از اطلاعات دایرکتوری استفاده می‌کند. این اجزا به طور معمول شامل منابع اشتراکی مانند سرورها، چاپگرها و کاربر شبکه و حساب‌های کاربری هستند [۳۸].

امنیت از طریق تأیید هویت ورود به سیستم و کنترل دسترسی به اجزا موجود در هر دایرکتوری یکپارچه و پیاده‌سازی شده است. با ورود امن و تایید شده به شبکه، مدیران می‌توانند داده‌های دایرکتوری و سازمان را در سراسر شبکه خود مدیریت کنند و کاربران مجاز شبکه می‌توانند به منابع مورد تایید در هر نقطه از شبکه دسترسی پیدا کنند. مدیریت مبتنی بر سیاست‌های دسترسی مطمئن، حتی مدیریت پیچیده‌ترین شبکه‌ها را ممکن می‌سازد. مجموعه ای از قواعد که کلاس‌های اجزا و ویژگی‌های موجود در دایرکتوری را مشخص می‌کند و قیدها و محدودیت‌ها را در موارد این اجزا و قالب نام آنها تعیین می‌کند.

مزایا:

- مدیریت متمرکز منابع و امنیت
- ورود یکباره برای دسترسی به منابع سراسری
- مدیریت ذخیره‌سازی منابع به صورت ساده و یکپارچه
- مخزن متمرکز امنیتی برای اعتبارسنجی کاربر و تسهیل مدیریت و ایمن‌تر کردن آن
- مدیریت متمرکز پیکربندی ایستگاه کاری
- استفاده از گروه‌بندی کاربران برای اعطای الگوی کنترل دسترسی مبتنی بر نقش به برنامه‌ها و مدیریت دایرکتوری

۵-۱-۵ Zentyal

Zentyal یک سرور کوچک تجاری لینوکس است که می‌تواند به عنوان یک دروازه، مدیر زیرساخت، مدیر تهدید یکپارچه، سرور اداری، سرور ارتباطات یکپارچه یا ترکیبی از آنها پیکربندی شود. تمام خدمات شبکه‌ای که توسط Zentyal اداره می‌شوند کاملاً یکپارچه هستند و بیشتر وظایف را به صورت خودکار انجام می‌دهند. این باعث صرفه جویی در وقت می‌شود و به جلوگیری از خطا در پیکربندی شبکه و مدیریت کمک می‌کند. Zentyal منبع باز است و تحت مجوز عمومی (GNU GPL) منتشر شده و در بستر Ubuntu GNU / Linux اجرا می‌شود [۳۹].

این ابزار از یک سری بسته‌ها و قابلیت‌ها در قالب یک رابط کاربری وب (معمولاً یکی برای هر ماژول) برای پیکربندی سرورها یا خدمات مختلف تشکیل شده است. پیکربندی به شکل کلید-مقدار در یک پایگاه داده Redis ذخیره می‌شود، اما کاربران، گروه‌ها و پیکربندی مربوط به دامنه در OpenLDAP قرار دارند. هنگامی‌که هر یک از پارامترهای موجود را از طریق رابط وب پیکربندی می‌کنید، فایل‌های پیکربندی نهایی با استفاده از الگوهای پیکربندی ارائه شده توسط ماژول‌ها رونویسی می‌شوند. مهمترین مزیت استفاده از Zentyal یک رابط‌کاربری گرافیکی یکپارچه برای پیکربندی کلیه خدمات شبکه و یکپارچه‌سازی بالا است.

مزایا:

- مدیریت مرکزی و یکپارچه دامنه و دایرکتوری، کاربران، گروه‌های امنیتی، لیست‌های توزیع شده
- واحدهای سازمانی چندگانه (OU)، اهداف سیاست گروهی (GPO)

- تأیید اعتبار یک‌باره و مدیریت چندمنظوره سیستم (SSO)
- پشتیبانی از سیستم عامل‌های متفاوت و اشتراک‌گذاری فایل در محیط ویندوز
- مجوزهای دسترسی و تغییر کاربری کاربران و گروه‌ها
- مدیریت تصاویر پروفایل کاربر
- انتقال اطلاعات کاربران و گروه‌ها در رابط کاربری
- یکپارچه‌سازی با نرم‌افزارهای مدیریتی دیگر

۵-۱-۵-۱ نصب :

برای نصب، ابتدا باید مخزن حاوی نرم‌افزار را به apt اضافه نمود:

```
sudo add-apt-repository "deb http://archive.zentyal.org/zentyal 3.5 main extra”
```

تایید هویت مخزن از طریق دستور زیر انجام می‌شود:

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 10E239FF
wget -q http://keys.zentyal.org/zentyal-3.5-archive.asc -O-|sudo apt-key add -
```

برای نصب، ابتدا apt به‌روزرسانی شده:

```
sudo apt-get update
```

و سپس نرم‌افزار zentyal نصب می‌شود:

```
sudo apt-get install zentyal
```

نصب بسته‌های دیگر نیز به این صورت انجام می‌شود:

```
sudo apt-get install zentyal-all
```

۵-۱-۶ 389 Directory Server

این ابزار یک پیاده‌سازی LDAP منبع باز برای لینوکس در مقیاس سازمانی است. این ابزار در دنیای واقعی با بیشترین میزان استفاده روبرو شده است و توانسته است به‌خوبی از عهده وظایف محوله برآید. از چند نسخگی (replica) پشتیبانی می‌کند و در حال حاضر بسیاری از بزرگترین استقرار LDAP در جهان را کنترل می‌کند. این ابزار می‌تواند به صورت رایگان بارگیری شده و در کمترین زمان ممکن با استفاده از رابط گرافیکی پیکربندی و آماده بهره‌برداری شود. این ابزار با کارایی بالا که می‌تواند هزاران عملیات در ثانیه و ده‌ها هزار کاربر همزمان را اداره کند [۴۰].

مزایا:

- اجرای آنلاین، بدون زمان توقف، مدیریت مبتنی بر LDAP برای مواردی چون اطلاعات کنترل دسترسی
- وجود چند نسخگی غیرهمزمان به منظور تحمل خطا و عملکرد سازگاری در نوشتن

- با بیش از یک دهه استقرار و استفاده در دنیا
- مستندات گسترده و کامل
- تأیید اعتبار و انتقالات داده‌ای ایمن (TLS و SASL)
- سازگار با نسخه ۳ سرور LDAP

۵-۱-۶-۱ نصب : (Ubuntu)

برای نصب، ابتدا باید مخزن حاوی نرم‌افزار را به apt اضافه نمود:

```
sudo apt-get update -y
```

سپس خود ابزار نصب می‌شود:

```
sudo apt-get install -y 389-ds
```

۵-۱-۷ GLAuth

یک سرور احراز هویت LDAP برای توسعه دهندگان و کاربران در مقیاس متوسط می‌باشد. احراز هویت GLAuth (Go-lang LDAP) یک پشتیبان مطمئن و قابل تنظیم برای سرور LDAP است که پیکربندی و تنظیمات خوبی را ارائه می‌دهد [۴۱].

مزایا:

- حساب‌ها را به طور متمرکز در زیرساخت‌های خود مدیریت می‌کند.
- کلیدهایSSH، حساب‌های کاربری لینوکس و رمزهای عبور را برای سرورهای ابری به طور مرکزی مدیریت می‌کند.
- جایگزین سبک وزن برای OpenLDAP و Active Directory برای توسعه یا یک کاربرد کوچک است.
- اطلاعات دایرکتوری کاربری خود را در یک فایل محلی، پایگاه داده S3 یا با پراکسی در سرورهای LDAP موجود ذخیره می‌کند.
- از آن برای متمرکز کردن مدیریت حساب کاربران و حقوق دسترسی در سرورهای لینوکس، دستگاه‌های OSX و برنامه‌های پشتیبانی استفاده می‌شود.

۵-۱-۸ 2OAuth

نسخه دوم OAuth یک پروتکل استاندارد صنعتی-تجاری برای احراز هویت است. این ابزار ضمن ارائه جریان‌های احراز هویت و کنترل دسترسی خاص برای برنامه‌های وب، برنامه‌های کاربردی، تلفن‌های همراه و دستگاه‌های سرگرمی‌خانگی، روی سادگی برای توسعه‌دهنده متمرکز است. OAuth یک پروتکل مجوز-باز است که با فعال کردن برنامه‌های هویتی مشتری در سرویس‌های HTTP مانند گوگل، Facebook، GitHub و غیره امکان دسترسی به منابع دیگر را فراهم می‌کند و امکان استفاده از منابع ذخیره شده در یک سایت را به سایت دیگر بدون استفاده از

اعتبارسنجی مجدد می‌دهد. به جای آن از نام‌کاربری و رمزهای عبور مربوط به سایت مبدا استفاده می‌کند. این ویژگی‌ها و برنامه‌های کاربردی افزودنی آن در گروه کاری IETF OAuth در حال توسعه است [۴۲].

مزایا:

- می‌توانید از ۲.۰OAuth برای خواندن داده‌های کاربر از برنامه دیگری استفاده کنید.
- ایجاد مجوز و تایید هویت را برای وب، برنامه‌های کاربردی و دستگاه‌های تلفن همراه فراهم می‌کند.
- یک برنامه تحت وب است که از کد مجوز و هویت اولیه کاربر استفاده می‌کند و از اعتبارسنجی تعاملی کاربر استفاده نمی‌کند.
- ۲.۰OAuth یک پروتکل ساده است که امکان دسترسی به منابع کاربر را بدون به اشتراک گذاشتن گذرواژه‌ها فراهم می‌کند.
- این نرم افزار عملیات کاربری را برای اجرای برنامه‌های مشتری با استفاده از یک زبان اسکریپت مانند JavaScript فراهم می‌کند.
- ۲.۰OAuth یک پروتکل بسیار انعطاف‌پذیر است که از SSL استفاده می‌کند، که امنیت اطلاعات بین سرورهای وب را تضمین می‌کند و اطلاعات مرورگرها به صورت محرمانه و خصوصی باقی می‌مانند.
- این ابزار، امکان دسترسی محدود به داده‌های کاربر را فراهم می‌کند و اجازه می‌دهد تا هنگام منقضی شدن زمان دسترسی به داده‌ها دسترسی پیدا کنید.
- این ابزار قابلیت اشتراک گذاری داده‌ها برای کاربران را بدون نیاز به انتشار اطلاعات احراز هویت شخصی فراهم می‌کند.
- اجرای آن ساده است و تأیید هویت قوی را ارائه می‌دهد.

۵-۱-۸-۱ نصب :

ابتدا apt بروزرسانی شده:

```
sudo apt-get update -y
```

سپس ابزار نصب می‌گردد:

```
sudo apt-get install -y signon-plugin-oauth2
```

۶. مراجع

[1] https://logentries.com/product

[2] https://goaccess.io/features

[3] https://logz.io/platform

[4] https://www.graylog.org

[5] https://www.splunk.com

[6] https://www.sumologic.com

[7] http://www.fluentd.org

[8] https://www.syslog-ng.com

[9] https://www.rsyslog.com

[10] http://www.logalyze.com/product/major-features

[11] https://www.loggly.com

[12] https://www.tutorialspoint.com/logstash/

[13] https://logz.io/blog/beats-tutorial/

[14] https://www.tutorialspoint.com/apache_kafka/

[15] https://www.tutorialspoint.com/apache_flume/

[16] https://ambari.apache.org/

[17] https://www.nagios.org/

[18] https://www.howtoforge.com/tutorial/ubuntu-nagios/

[19] https://www.cloudera.com/

[20] https://ranger.apache.org

[21] http://ganglia.sourceforge.net

[22]http://www.sematext.com

[23] https://www.zabbix.com/documentation/

[24] https://www.howtoforge.com/tutorial/centos-zabbix-system-monitoring/

[25] https://docs.netdata.cloud/

[26] https://www.netdata.cloud/

[27] https://www.tecmint.com/install-librenms-monitoring-on-ubuntu-centos/

[28] https://altina.ir/netcrunch/

[29] Shihada,B., “Conceptual & Concrete Architectures of Open Network Management System (OpenNMS)”, University of Waterloo Dept. of Computer Science, 2002.

[30] https://www.howtoforge.com/tutorial/how-to-install-and-configure-opennms-on-ubuntu-1604/

[31] https://icinga.com/

[32] https://www.ittsystems.com/prtg-network-monitor-review/

[33] https://www.monitorix.org/

[34] https://www.howtoforge.com/tutorial/performance-monitoring-with-monitorix-on-ubuntu-16-04/

[35] www.openldap.org

[36] https://www.freeipa.org/page/Main_Page

[37] https://directory.apache.org/apacheds

[38] https://docs.microsoft.com/en-us/windows-server/identity/identity-and-access

[39]http://zentyal.com

[40] https://directory.fedoraproject.org

[41] https://github.com/glauth/glauth

[42] https://oauth.net/2

[43] https://www.papertrail.com