ManageEngine
OpManager

Grunderna i nätverksövervakning

Grunderna i nätverksövervakning som varje IT-proffs bör känna till

-Nithin.S

www.opmanager.com

Introduktion

När företag och organisationer växer så blir inte bara deras nätverk större, utan det blir även mer komplext och en integrerad del av verksamheten. Oavsett hur stor en organisation är, så kommer nätverket att vara ett arkiv med data och information. Det är viktigt att förstå nätverket, dess komplexitet och att vara informerad om tillgängligheten för att upprätthålla nätverkets och organisationens integritet. Det är här nätverksövervakning spelar en avgörande roll.

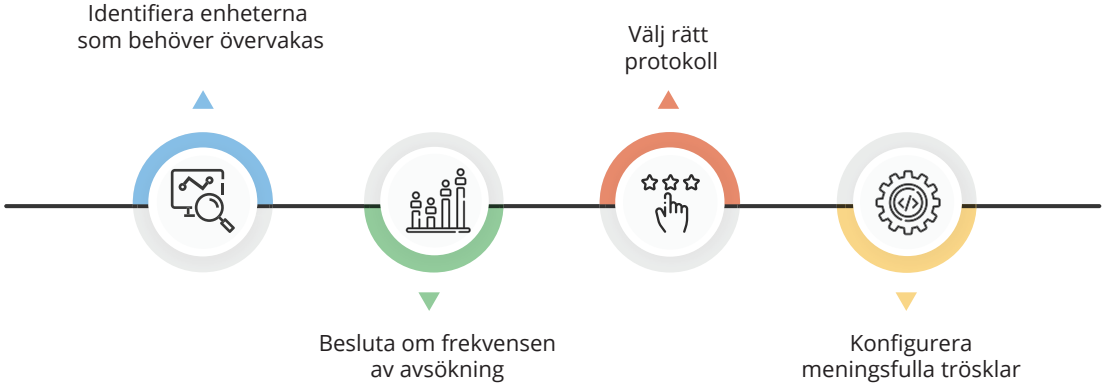
Vad är nätverksövervakning?

I dagens värld är termen nätverksövervakning välkänd inom IT-branschen. Nätverksövervakningär en kritisk IT-process där alla nätverkskomponenter som till exempel routrar,switchar, brandväggar, servrar och VM:er övervakas med avseende på fel och prestanda, de utvärderas även kontinuerligt för att upprätthålla och optimera deras tillgänglighet.

En viktig aspekt av exceptionell nätverksövervakning är att vara proaktiv. Att hitta prestationsproblem och flaskhalsar hjälper proaktivt till med arbetet att identifiera problem innan de orsakar nätverksavbrott eller fullständiga nätverksfel.

Viktiga aspekter i nätverksövervakning:

- Övervaka allt väsentligt
- Optimera övervakningsintervallet
- Välj rätt protokoll
- Ställa in trösklar



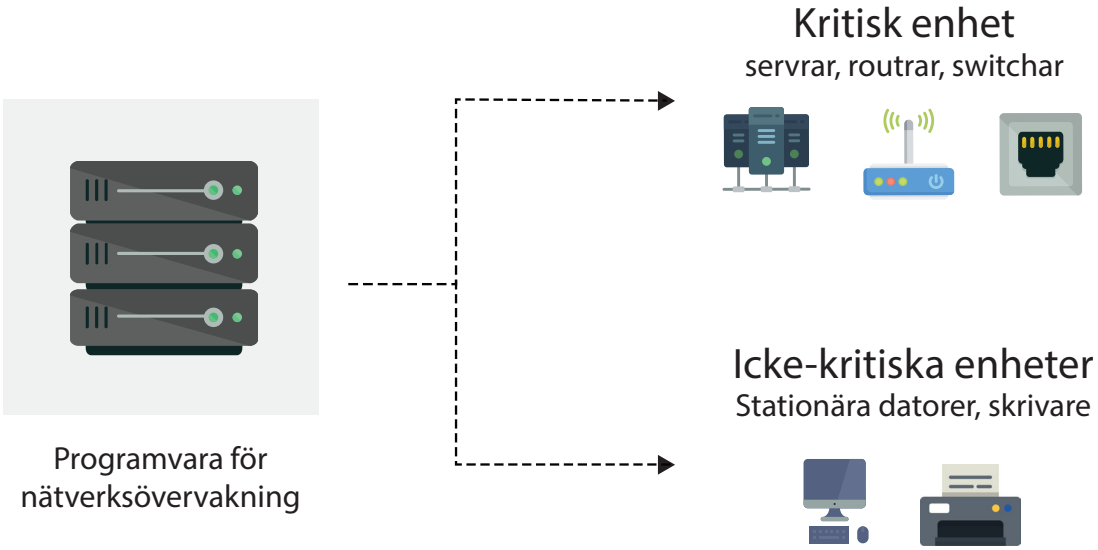
Visste du?

- Branschundersökningar uppskattar kostnaden för ett nätverksavbrott till cirka 5 600 dollar per minut. Detta blir över 300 000 USD per timme, vilket är ett dyrt pris för flera
- Endast 2 % av organisationerna återhämtar sig från driftstopp inom en timme. Majoriteten måste vänta längre – genomsnittet är 4,78 timmar

Övervaka allt väsentligt

Defekta nätverksenheter påverkar nätverksprestanda, men detta kan elimineras genom tidig upptäckt, vilket belyser vikten av kontinuerlig övervakning av ditt nätverk och dess relaterade enheter. Enhetens tillgänglighet är en viktig faktor när det gäller nätverksövervakning. Utöver att känna till enheternas tillgänglighet så finns det flera andra detaljer som påverkar om ett nätverks funktioner fungerar som de ska.

Det första steget mot effektiv nätverksövervakning är att identifiera vilka enheter och relaterade prestandavärden som måste övervakas. Enheter som stationära datorer och skrivare är inte kritiska och kräver inte regelbunden övervakning, medan servrar, routrar och switchar utför affärskritiska uppgifter och kräver konstant övervakning.



Övervakningsintervall

Ett övervakningsintervall bestämmer frekvensen vid vilken nätverksenheter och deras relaterade mätvärden avsöks för att identifiera prestanda och tillgänglighetsstatus. Inställning av övervakningsintervall kan bidra till att eliminera belastningen från systemet för nätverksövervakning och i sin tur dina resurser.

Övervakningsintervallet beror på typen av nätverksenhet eller parameter som övervakas. Tillgänglighetsstatus för enheter ska övervakas varje minut, processor- och minnesstatistik ska övervakas var femte minut och diskanvändning ska övervakas en gång var 15:e minut. Om enheterna övervakas med det kortaste intervallet leder det bara till onödiga belastningar i nätverket och det är inte nödvändigt för att upptäcka kritiska aspekter av nätverksprestanda.

Typer av protokoll

Vid övervakning av ett nätverk och dess enheter är en vanlig god praxis att anta ett säkert protokoll som inte använder bandbredd för att minimera protokollets inverkan på nätverksprestanda. De flesta nätverksenheter och Linux-servrar stöder SNMP- och CLI-protokoll, medan Windows-enheter stöder WMI-protokoll.

SNMP är ett allmänt accepterat protokoll för att hantera och övervaka nätverkselement. De flesta nätverkselement ingår i en SNMP-agent, så de behöver bara vara aktiverade och konfigurerad för att kommunicera med NMS (Network Management System). Om du tillåter läs-/skrivåtkomst för SNMP på en enhet ger det dig full kontroll över enheten. Med SNMP kan du ersätta hela enhetens konfiguration. Ett system för nätverksövervakning hjälper administratörer ta ansvar för nätverket genom att ställa in läs-/skrivbehörigheter för SNMP och begränsa kontrollen för andra användare.

Proaktiv övervakning och trösklar

Nätverksavbrott kan vara mycket dyra. I de flesta fall rapporterar slutanvändare nätverksproblem till teamet för nätverkshantering.

Detta är en reaktiv strategi för nätverks- övervakning. Den viktigaste utmaningen i nätverksövervakning är att proaktivt identifiera flaskhalsar för prestanda. Det är här trösklarna spelar en viktig roll inom nätverks- övervakning. Gränsvärden varierar från enhet till enhet baserat på företagets användningsfall.

Omedelbara varningar baserat på tröskelöverträdelser

Konfigurering av trösklar hjälper till att proaktivt övervaka resurserna och tjänsterna körs på servrar och nätverksenheter. Varje enhet kan ha ett intervall eller tröskelvärde som är baserat på användarens preferenser och behov. En tröskel på flera nivåer kan bidra till att klassificera och sammanfatta eventuella fel. Med trösklar kan varningar också skickas innan enheten stängs av eller når ett kritiskt tillstånd.

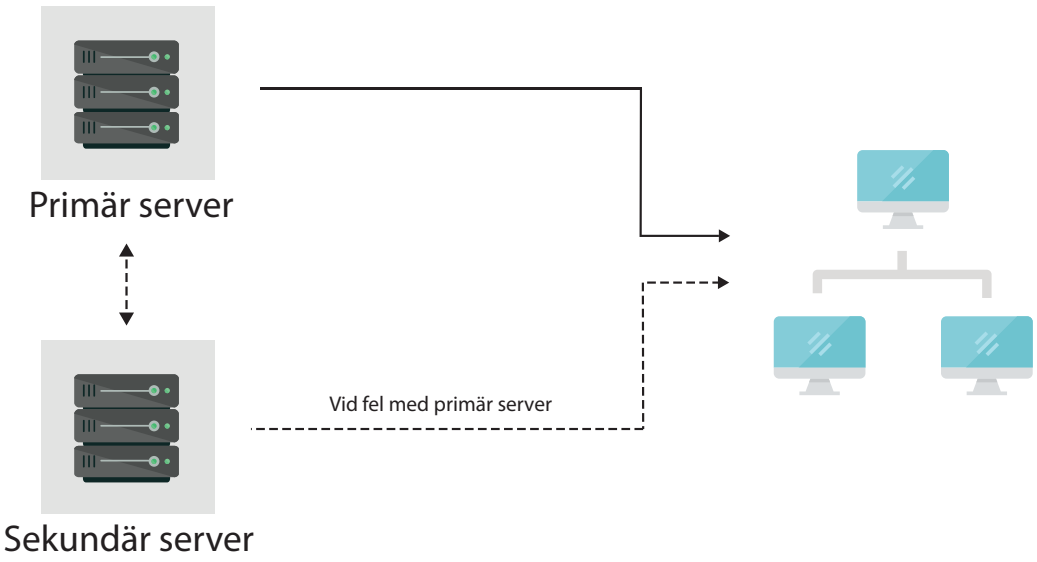
Instrumentpaneler och anpassning

Data blir endast användbara när de presenteras på ett tydligt sätt för rätt personer. Det är viktigt för IT-administratörer och användare att göras medvetna om kritiska mätvärden så snart de loggar in. En nätverkspanel ska ge en snabb översikt över ditt nätverks nuvarande, med kritiska mätvärden från nätverksenheter som t.ex. routrar, switchar, brandväggar, servrar, tjänster, skrivare och UPS, samt från applikationer och URL:er. Stöd för widgetar för att övervaka önskade specifika diagram över prestanda i realtid kan hjälpa administratörer snabbt felsöka problem och övervaka enheter på distans.

Hög tillgänglighet och växling vid fel

Vad händer när din betrodda nätverksövervakare körs på en server som kraschar eller förlorar nätverksanslutningen? Du vill få omedelbara varningar om detta och du vill förmodligen att situationen automatiskt ska åtgärdas med en extra nätverksövervakare. Hög tillgänglighet avser kontinuerlig tillgänglighet av ett övervakningssystem. Varje enskild nätverkshändelse – enhetsfel, ohälsosamma bandbreddnivåer,DoS-angrepp, o.s.v. – bör omedelbart uppmärksammas så att motåtgärder snabbt kan vidtas.

Växling vid fel och återställning vid fel garanterar att nätverksmiljöer alltid övervakas med en sekundär standby-server. Om ett fel inträffar i den primära server är den sekundära servern redo att ta över så att databasen förblir säker.



Fördelarna med ett system för växling vid fel:

- Identifierar direkt fel med den primära servern.
- Skickar omedelbart ett meddelande via e-post i händelse av ett fel med den primära servern.
- 100 procent drifttid och oavbruten nätverkshantering.
- Automatisk, sömlös växling från den primära servern till standby-servern och vice versa.

Välja rätt verktyg för nätverksövervakning

Artificiell intelligens och maskininlärning

Verktyg för nätverksövervakning har potential att införliva artificiell intelligens (AI) och maskininlärning (ML) eftersom båda använder data. Med maskininlärning kan verktyg för nätverksövervakning anpassa sig till nätverksmiljön och ge förslag baserat på tillgängliga data.

Möjligheterna med nätverksövervakning med AI och ML:

- Lastdelning baserat på användning.
- Smartare meddelandeprofiler.
- Nätverksanpassning och möjligheten att automatiskt vidta korrigerande åtgärder.
- Prognostisering

Automatisering

Automatisering befinner sig vid en brytpunkt tack vare snabba utvecklingar inom AI. Automatisering hjälper verktyg för nätverksövervakning att reagera baserat på trösklar eller en uppsättning regler/kriterier som uppfylls. Med automatisering kan ett övervakningsverktyg automatiskt identifiera och felsöka problem (proaktiv övervakning), skicka varningsmeddelanden och ge förslag för bättre nätverksprestanda och underhåll baserat på användning och prioritering.

Fördelarna med automatisering vid nätverksövervakning:

- Möjligheten att automatisera repetitiva uppgifter.
- Automatiserad konfiguration och säkerhetskopiering i olika enheter.
- Automatisk identifiering och övervakning av nya enheter.
- Proaktiv felsökning och arbete för att vidta korrigerande åtgärder.
- Generering av schemalagd rapport.

Funktioner

Varje lösning för nätverksövervakning tillhandahåller övervakning av grundläggande kärnkrav,som t.ex. bandbredd, tillgänglighet och användning. Ett effektivt verktyg för nätverksövervakning bör stödja vanliga protokoll (SNMP, WMI och CLI) och teknik (NetFlow, sFlow, jFlow och paketkontroll). Konfigurerbara varningsmeddelanden, rapporteringsfunktioner och anpassningsbara instrumentpaneler är funktioner som både gör ett verktyg för nätverksövervakning tillgängligt och enkelt att använda. Det är viktigt att förstå dina grundläggande krav och överväga de väsentliga funktionerna för nätverksövervakning vid val av rätt lösning för nätverkshantering. Men bortsett från funktionerna finns det flera mer kritiska aspekter att tänka på när du väljer rätt verktyg för nätverksövervakning.

Distribuerade nätverk

Det händer ofta att två företag slås samman eller att ett företag köper upp ett annat, vilket utökar storleken på nätverket avsevärt. Den största utmaningen är att slå samman företagskulturerna och naturligtvis de två datornätverken. När detta händer växer det nya nätverket avsevärt på kort tid och distribueras över nya lokala nätverk, filialer, kundnätverk (i händelse av MSP), datacentra och i molnet. Robusta nätverk kan vara kostsamma att hantera och svårt att felsöka. Det är avgörande att ständigt övervaka tillgängligheten och bandbreddanvändningen i distribuerade nätverk.

Utmaningar i distribuerad övervakning:

- Centraliserad kontroll: Övervaka flera fjärrplatser från en central plats med sondspecifik kontroll för att visualisera prestandaproblem.
- Nätverksunderhåll: Underhålla nätverket och felsöka nätverksproblem.
- Språkbarriärer: Visa språkspecifik statistik över sondplatsen i ett centralt läge.

Område

Ett vanligt problem som IT-operatörer och systemadministratörer ställs inför är bristen på synlighet. Ett verktyg för nätverksövervakning som ger omfattande, konsoliderad och detaljerad insyn i olika övervakningsaspekter i nätverket samt flexibiliteten att välja vad du vill se, hjälper dig att hålla jämna steg med ditt nätverk. Informationen från dessa olika verktyg måste vara tillgänglig på en enda skärm med översiktsdiagram och intuitiva grafer. Vissa verktyg för nätverksövervakning kan förbättras för att utföra mer avancerade åtgärder, vilket betyder att det är viktigt för det verktyg du väljer att erbjuda stöd för tillägg och integrationer så att du kanövervaka en bredare aspekt av ditt nätverk.

Skalbarhet

Nätverksskalbarhet är en viktig aspekt när det gäller att välja ett effektivt verktyg för nätverksövervakning. Ett verktyg för nätverksövervakning

anses skalbart när det är mer anpassningsbart till ett förtags och dess användares föränderliga behov och krav. Skalbarhet hjälper ett nätverk att hålla jämna steg med ökad produktivitet, trender, föränderligabehov och nya anpassningar för att säkerställa att den övergripande nätverksprestandan inte försämras, oavsett nätverkets storlek.

Igenkännande

När du väljer ett verktyg för nätverksövervakning är en vanlig bästa praxis att analysera och bekanta dig med lösningarna på marknaden. Recensionswebbplatser förenklar det här jobbet genom att ge insikter om olika aspekter av varje verktyg och hur specifika funktioner sticker ut från mängden. Analytiker bedriver grundlig och sekundär forskning baserat på ett stort nätverk av källor, inklusive slutanvändarklienter, teknikleverantörer och branschledare. De kan också införliva innehåll från akademiska, journalistiska och vetenskapliga källor. Erkännande från etablerade recensionswebbplatser som t.ex. Gartner och EMA kan vara fördelaktiga när det gäller att besluta om rätt verktyg för nätverksövervakning för ditt företag.

Prissättning

Det finns olika licensieringsmodeller på marknaden baserat på antalet enheter, noder eller servrar. Det lämpliga licenssystemet kan fastställas baserat på nätverkets storlek, typ av lösning (övervakning eller hantering), och skalbarheten i nätverket. Det är viktigt att beakta både kostnaden för produkten (inklusive sådant som årligt underhåll, installationstid, tillägg, integrationer och utbildning) och potentiella besparingar. En transparent prispolicy säkerställer att det inte finns några dolda kostnader.

Utvärdering

Många programvaruleverantörer tillhandahåller en kostnadsfri testversion för att ge dig en förstahandsupplevelse av produkten, så att du vet exakt vad du får. Det är viktigt att du provar produkten för att bekanta dig med funktionerna och få en känsla för användargränssnitt.

Så utför OpManager nätverksövervakning

OpManager är en proaktiv lösning för nätverksövervakning som är fullpackad med kraftfulla funktioner som hjälper IT-administratörer att åtgärda nätverksavbrott snabbt och ta kontroll över deras nätverk.

Med OpManager är det enkelt att:

- övervaka hälsa och prestanda för alla nätverksenheter.
- få insyn i nätverkstrafikmönster.
- övervaka ditt nätverk proaktivt med trösklar på flera nivåer.
- automatisera hanteringen av nätverksändringar och -konfigurationer.
- analysera och felsöka WAN-problem och VoIP-prestanda.
- få detaljerad nätverksinsikt med anpassningsbara instrumentpaneler.
- hålla dig uppdaterad tack vare OpManagers avancerade felövervaknings- och larmhanteringssystem.
- säkerställa kontinuitet med hög tillgänglighet och stöd för växling vid fel.