ManageEngine
OpManager

GRATIS E-BOK

11 BÄSTA PRAXIS FÖR ATT SKYDDA DITT FÖRETAG FRÅN NÄTVERSFALLGROPAR

Handbok för bästa praxis för nätverksadministration

-Vignesh Karthikeyan

WWW.OPMANAGER.COM

Innehållsförteckning

Introduktion	1
1. TA BORT ALLA INBYGGDA KONFIGURATIONER OCH OMKONFIGURERA	2
2. VÄLJ RÄTTA PARAMETRAR FÖR ÖVERVAKNING	3
3. ÖVERVAKA GRÄNSSNITTEN I DITT NÄTVERK	4
4. HÅLL UTKIK EFTER SYMPTOM – INTE PROBLEM	5
5. GRUPPERA ENHETER OCH AUTOMATISERA	6
6. ANVÄND SYSLOGS OCH TRAPS TILL DIN FÖRDEL	7
7. ENHETERNA SOM DU INTE ÖVERVAKAR ÄR VIKTIGA	9
8. PLANERA FÖRÄNDRINGAR	10
9. IGNORERA INTE SMÅ UPPDATERINGAR	11
10. AUTOMATISERA UPPGIFTER NÄR DITT NÄTVERK ÄR LITET	12
11. VÄLJ RÄTT PROGRAMVARA FÖR NÄTVERKSHANTERING	13

Introduktion

- För Quora, Business Insider, Giphy och många andra webbplatser, var den 18 februari 2017 bara en vanlig dag – det vill säga tills deras tjänster slutade svara. Anledningen? Dessa webbplatser använde Amazon S3, en populär molnbaserad tjänst, vilken plötsligt hade ett fem timmars långt avbrott som var så allvarligt att inte ens Amazon kunde uppdatera sin egen AWS-statuspanel.

- I maj 2017 strandsattes 75 000 passagerare som flög med ett internationellt känt flygbolag - inte i några timmar, utan i tre hela dagar. Rekordhöga 726 flygningar avbröts och flygbolaget led enligt uppgift en ekonomisk förlust på 80 miljoner pund, utöver ett skadat rykte.

- I april 2011 gjorde en georgisk kvinna så att hela landet Armenien blev utan internet i fem timmar när hon av misstag skadade en kopparkabel medan hon letade efter skrot.

Vad har alla ovanstående exempel gemensamt? De var alla instanser av nätverksavbrott som orsakade miljontals dollar i förluster. Bara omnämnandet av driftstopp kan få kunder, ledningar och nätverksadministratörer att känna kalla kårar.

Dålig strategiplanering, en bristfällig anställningsprocess och en ledning som bara fattar dåliga beslut – alla dessa faktorer kan bidra till att störta ett framgångsrikt företag. Men det finns ett problem som är ännu mer angeläget än ovanstående: ineffektiv nätverkshantering. Vad det skulle ta månader eller till och med år för dessa affärsproblem att åstadkomma, kan dålig nätverkshantering åstadkomma på bara några få sekunder.

Den här e-boken innehåller de 11 bästa praxis för nätverkshantering som hjälper dig att förebygga nätverksavbrott samt andra potentiella förluster till följd av ineffektivt nätverkshantering.

Bästa praxis nr 1

TA BORT ALLA INBYGGDA KONFIGURATIONER OCH OMKONFIGURERAVARJE ENHET I NÄTVERKET

Varje nätverksenhet har en lista med standardkonfigurationer. De flesta nätverksadministratörer tar bort dessa befintliga konfigurationer och omkonfigurerar dem för väsentliga parametrar, men de tenderar att hoppa över parametrar som inte är nödvändiga för nätverkets ekosystem. Dessa parametrar som bedöms som obetydliga blir då kvar med förinställda autentiseringsuppgifter och konfigurationer, vilket gör dem till en enorm säkerhetsrisk.

> Ett inte så roligt faktum: 80 % av databrott i organisationer inträffar till följd av att de har osäkra autentiseringsuppgifter eller förinställda autentisering-suppgifter.

Tänk dig en kritisk parameter vars konfiguration är oförändrad eftersom den inte används i organisationen. Detta kan utnyttjas av en extern part för enkelt intrång i nätverket, vilket gör hela organisationens nätverk exponerat. Du måste ta bort alla standardkonfigurationer av enheter – varken ”admin”, ”lösenord” eller en kombination av dessa autentiseringsuppgifter är tillåtet – inte ens för de konfigurationer som du inte använder.

VIKTIGA STEG FÖR ATT SÄKERA ENHETSSÄKERHET I NÄTVERKSHANTERING

1. När du lägger till en ny enhet i nätverket ska du se till att alla standardkonfigurationer som medföljer enheten konfigureras om – även de konfigurationer som du
2. Tillåt inte simpla autentiseringsuppgifter för någon enhetskonfiguration, inte ens för konfigurationer som inte används.
3. Ändra autentiseringsuppgifterna med jämna mellanrum och inte bara för de konfigurationer som används i ditt nätverk, utan även för de som inte används.
4. Verkställ en stark lösenordspolicy för att implementera punkterna 2 och 3.

Bästa praxis nr 2

VÄLJ DE RÄTTA PARAMETRARNA FÖR ÖVERVAKNING BASERAT PÅ ENHETSTYP OCH KRITIKALITET

Det är viktigt att övervaka alla kritiska enheter och gränssnitt i ditt nätverk för att skydda ditt företag från nätverksrelaterade fallgropar. Men du måste överväga en annan viktig faktor: vilka parametrar som ska övervakas för varje enhet och gränssnitt.

Inte alla enheter kräver att alla parametrar övervakas och inte alla parametrar som du övervakar för en enhet är viktiga. Du måste besluta om rätt kombination av parametrar att övervaka för varje enhet i ditt nätverk.

VAD ÄR DITT ÖVERVAKNINGSINTERVAL?

En annan viktig faktor som bidrar till effektiv nätverksövervakning är övervakningsintervall. Håll detta intervall kort för kritiska enheter och parametrar, och öka det när du går ner i hierarkin över kritikalitet

Två faktorer måste beaktas när du beslutar vilka parametrar som ska övervakas i en enhet:

- **Enhetens kritikalitet:** Alla parametrar i primära servrar och andra kritiska enheter måste övervakas. Om en enhet är mindre kritisk, till exempel en skrivare eller testenhet, kan du övervaka de mest grundläggande parametrarna som bara berättar för digom enheten eller gränssnittet fungerar eller inte. Detta minskar den onödiga belastningen på din programvara och reducerar trafiken i nätverket.
- **Enhetstyp:** Olika enhetstyper har olika grundläggande parametrar som måste övervakas. Till exempel är temperatur en viktig parameter för en processor eftersom en brant temperaturökning är en indikation på att processorn används för mycket.

Använd stegen nedan för att ta reda på vilka parametrar du bör övervaka:

- Skapa en prioriteringslista genom att kategorisera varje enhet i ditt nätverk från mest kritisk till minst kritisk. Klassificera dem som mycket kritiska, medelkritiska och mindre kritiska.
- Övervaka alla parametrar för kör kritiska enheter.
- För medelstora enheter ska du övervaka de viktigaste parametrarna plus några ytterligare parametrar beroende på enhetstyp och leverantör.
- För mindre kritiska enheter (t.ex. test- eller dummy-enheter) ska du bara övervaka de grundläggande parametrarna som ger information om enhetens status.

Bästa praxis nr 3

ÖVERVAKA GRÄNSSNITTEN I DITT NÄTVERK LIKA INTENSIVT SOM ENHETERNA

Den allmänna definitionen av nätverksövervakning är att övervaka enheterna i ett nätverkför att förhindra driftstopp och potentiella affärsförluster. De flesta nätverksadministratörer hålla sig till denna definition och övervakar endast enheterna i deras nätverk.

> Ett inte så roligt faktum: Problem i enhetsgränssnitt bidrar till 25 procent av alla större driftstopp

Men här är haken: Enhetsfel eller nätverksfel behöver inte nödvändigtvis endast uppstå på grund av fel på enheter. Ibland kan problemet uppstå i gränssnitten som ansluter enheterna till varandra, och det är därför det är viktigt att övervaka gränssnitt lika intensivt som enheterna i ditt nätverk.

Begränsa inte gränssnittsövervakningen till att bara kontrollera om ett gränssnitt körs eller inte använder periodisk avsökning. Ställ in trösklar för gränssnitt i ditt verktyg för nätverksövervakning för att få varningar när parametrarna för gränssnitten överskrider tröskelvärdena.

De flesta av dagens övervakningsverktyg har mallar för leverantörsspecifika gränssnitt. Utnyttja dem för att få en djupgående analys av prestandan för gränssnitten i dina nätverk.

Se till att hålla ett öga på alla viktiga gränssnitt i ditt nätverk som t.ex. Ethx för Linux-enheter; loopback, ethernet och överordnad länk för routrar och switchar; och fiberkanal och loopback för lagringsenheter. Det är särskilt viktigt att hålla ett öga på gränssnitt som är anslutna till enheterna som övervakas av ditt övervakningsverktyg, och att övervaka dem för prestanda och varningstecken för potentiella problem. Det kan vara nödvändigt att begränsa övervakningsparametrarna för gränssnitten som är anslutna till mindre kritiska enheter, men se till att ditt övervakningsverktyg omfattar alla de viktiga gränssnitten i ditt nätverk.

Se till att uppgraderingarna och ändringarna du gör i något av dina gränssnitt uppdateras i ditt övervakningsverktyg. Detta är avgörande för att skydda ditt nätverk från problem på grund av defekta gränssnitt.

Bästa praxis nr 4

HÅLL UTKIK EFTER SYMPTOM - INTE PROBLEM

Målet med nätverksövervakning är att förhindra att fel uppstår i nätverket eller oplanerad nedtid som kan leda till ett affärsstopp. De flesta nätverksadministratörer ställer in verktyg för nätverksövervakning för att övervaka problem i deras nätverk, som t.ex. ett serveravbrott eller en nätverksswitch.

Problemet med övervakning av problem i ett nätverk är att problemet i sig själv är en följd och inte en orsak.

Det innebär att varje gång ett problem uppstår i ditt nätverk (till exempel nedtid eller brist på tillgänglighet till vissa enheter) så är chansen stor att problemet

inte uppstod ur intet. Det är sannolikt att en serie incidenter som uppstod tidigare problem orsakade det slutliga problemet. Om dessa händelser (utlösare) identifieras och upptäcks i ett tidigt skede kan du vidta lämpliga åtgärder och i de flesta fall hindra dessa symtom från att förvandlas till det slutliga problemet. Metoden för övervakning av symptom är en mycket mer proaktiv metod för nätverkshantering

Hur övervakar du symptom?

- Ställ in flera trösklar: De flesta övervakningsverktyg låter dig ställa in flera varningströsklar som kan användas för att varna dig i god tid. Använd den funktionen för att konfigurera
- Analysera, analysera, analysera: För en historik med varningar och analysera dem. Sök efter mönster, särskilt vid återkommande varningar. Det är mycket möjligt att mönster kan peka på en vanlig orsak som kan ha missats.

Bästa praxis nr 5

GRUPPERA ENHETER EFFEKTIVT OCH AUTOMATERA UPPGIFTEN ATT ASSOCIERA VISSA ÖVERVAKARE NÄR DU LÄGGER TILL EN ENHET TILL DITT ÖVERVAKNINGSVERKTYG

Målet med nätverksövervakning är att förhindra att fel uppstår i nätverket eller oplanerad nedtid som kan leda till ett affärsstopp. De flesta nätverksadministratörer ställer in verktyg för nätverksövervakning för att övervaka problem i deras nätverk, som t.ex. ett serveravbrott eller en nätverksswitch.

Kunskapen om effektiv enhetsgruppering, om den behärskas, kommer att ge följande fördelar:

- Förenklar övervakning och underhåll av enheterna.
- Underlättar bulkändringar av konfigurationer och enhetsuppdateringar.

- Gruppering av enheter baserade på specifika parametrar hjälper dig att granska analyser av nätverksprestanda i större detalj.

Du måste ha flera grupper baserade på olika parametrar, som till exempel enhetstyp, leverantör och hög bandbreddförbrukning. Klassificera varje enhet under flera grupper för bättre förståelse av enhetens prestanda.

Till exempel kan en Cisco-server läggas under kategorierna för server (enhetstyp), Cisco (leverantör) och hög bandbreddförbrukning (en anpassad kategori som gör att du kan hantera nätverket bättre). Denna typ av klassificering gör det enklare att installera uppdateringar och utföra selektiva konfigurationsändringar.

Varje enhet som läggs till övervakningsverktyget behöver vissa viktiga övervakare. Dessa övervakare spårar specifika grundläggande parametrar för att ge viktig information om enhetens status och prestanda.

Om du automatiserar processen av att aktivera dessa viktiga övervakare för enheter när du lägger till en enhet i övervakningsverktyget kommer det att bespara dig mycket manuellt arbete och tid.

Du kan skapa förregler i ditt övervakningsverktyg för att automatiskt aktivera vissa övervakare när en viss typ av enhet upptäcks. Detta beror däremot på verktyget som du använder för nätverksövervakning. De flesta verktyg stöder automatisering, men ett par gratisverktyg och grundläggande versioner stöder inte automatisering av uppgifter.

Bästa praxis nr 6

ANVÄND SYSLOGS OCH TRAPS TILL DIN FÖRDEL

Sysloggs och traps är information som skickas av en enhet till nätverksövervakning. Till skillnad från andra data som övervakningsverktyget hämtar genom periodisk avsökning av enheter, så skickas syslogs och traps automatiskt av en enhet till övervakningsverktyget.

Vad kan syslogs och traps göra för att förbättra effektiviteten i din nätverksövervakning?

De flesta parametrar och enheter i ett nätverk övervakas genom periodisk avsökning i vilken övervakningsverktyget undersöker enheten i ett visst intervall för att kontrollera dess status. Problemet med denna teknik är att

- inte alla fel på enheten är synliga vid periodisk avsökning.
- Varningsmeddelanden för vissa fel måste utlösas omedelbart när de inträffar. Detta kan inte göras vid periodiska avsökningar.

Föreställ dig till exempel när ditt övervakningsverktyg undersöker en enhet för dess tillgänglighet varannan minut. De grafiska data som du ser på ditt övervakningsverktyg visar enhetens status under den andra minuten, fjärde minuten och så vidare. Anta nu att enheten stängs av under den tredje minuten och startar igen en halv minut senare. Det innebär att ingen bearbetning skedde i ditt nätverk under dessa 30 sekunder, men grafen i ditt övervakningsverktyg skulle inte ens visa minsta spår av den nedtiden, och än mindre vilken inverkan den hade.

Vad skulle du göra i en situation som denna? Det är här syslogs och traps kommer in i bilden. När nedtid inträffade under den tredje minuten skulle enheten ha skickat en trap till övervakningsverktyg och syslog-informationen skulle ha registrerat att systemet slutade fungera.

Du kan använda dessa traps och syslog-meddelanden till din fördel genom att konfigurera ditt verktyg för nätverksövervakning till att utfärda en varning när en sådan trap eller syslog med ett felmeddelande tas emot.

Om du konfigurerar ditt verktyg för nätverksövervakning till att utnyttja data som tillhandahålls av syslogs och traps kan du snappa upp fel som du annars skulle ha missat.

Bästa praxis nr 7

DE ENHETER SOM DU INTE ÖVERVAKAR ÄR LIKA VIKTIGA SOM DE SOM DU ÖVERVAKAR

De flesta nätverksadministratörer övervakar inte varje enhet. De övervakar antingen endast kritiska enheter, eller så inkluderar de inte icke-kritiska enheter i övervakningsverktyget. Anledningen är att licensiering för de flesta övervakningsverktyg bygger på antalet enheter som övervakas, och det är därför en vanlig uppfattning att det leder till onödiga licenskostnader om man lägger till icke-kritiska enheter.

Även om detta licensargument är giltigt, så har det också ett enormt kryphål. Varenda erfaren nätverksadministratör kommer att säga följande till dig:

Du kan aldrig förutsäga när en enhet blir kritisk.

> Ett inte så roligt faktum: Den genomsnittliga timkostnaden för nätverksstopp för små och medelstora företag är cirka 42 000 USD. Och den främsta orsaken till nätverksstopp är

Det är viktigt att hålla reda på enheter som inte läggs till i ditt övervakningsverktyg, t.ex. testmaskiner och icke-kritiska enheter. När du lägger till ytterligare funktioner på sådana enheter ska du omedelbart lägga till enheten i ditt övervakningsverktyg om du anser att tillägget av funktionaliteten kan göra det kritiskt.

När du lägger till en tidigare icke-kritisk enhet till ditt övervakningsverktyg kanske du vill begränsa antalet parametrar du övervakar, men se till att de ändå övervakas. Dina övervakningskostnader överskuggas av de förluster du kan förhindra om dessa enheter blir mycket kritiska och orsakar eventuella problem.

Bästa praxis nr 8

PLANERA IMPLEMENTERING AV FÖRÄNDRINGAR BASERAT PÅ TILLGÄNGLIGHET OCH KRITIKALITET

Alla förändringar måste implementeras med minimalt driftsstopp och får inte påverka avgörande affärsverksamhet. Det är viktigt att planera förändringarna i ditt nätverk för att hantera ditt nätverk effektivt. Vanligtvis är bästa praxis att implementera eventuella förändringar i ditt nätverk utanför produktionstimmar. Detta säkerställer att det inte sker några negativa konsekvenser på företagsnivå, och kommer också att ge dig tid att återställa förändringarna om något skulle gå fel.

Att veta när man ska genomföra en förändring beror däremot på fyra faktorer:

- **Förändringens kritikalitet:** Om ändringen är en kritisk korrigering av ett säkerhetsfel måste den görs så snart som möjligt.

- **Ändringens varaktighet:** En korrigering av ett kritiskt fel som bara tar några minuter att implementera och inte skadar det befintliga systemet kan genomföras under produktionstimmar. En korrigering av ett kritiskt fel som det dröjer flera timmar att implementera måste implementeras utanför produktionstimmar.
- **Nätverksstorlek:** Om ditt nätverk är litet och inte har reservservrar måste du tyvärrvänta med även de mest kritiska förändringarna tills efter produktionstimmar.Återställningstid: Hur lång tid tar det för dina system att återställas sig om något går fel under implementeringsprocessen? Det spelar ingen roll hur liten ändringen kan vara – du måste se till att nedtiden som du planerar för ändringen också inkluderar tid för återställning.

- **Återställningstid:** Hur lång tid tar det för dina system att återställas sig om något går fel under implementeringsprocessen? Det spelar ingen roll hur liten ändringen kan vara – du måste se till att nedtiden som du planerar för ändringen också

Ha en godkännandehierarki: En hierarki för ändringsgodkännande är en grupp personer som måste godkänna alla ändringar. Hierarkin måste börja med personen som implementerar ändringen på den lägsta nivån och går sedan hela vägen upp till personer i den övre ledningen. Mellanivåerna kan utgöras av personer med en kombination av domänkunskap och nätverkskunskap som kan förstå konsekvenserna av ändringen. Varje ändring, oavsett hur kritisk den är och vilken inverkan den har, måste implementeras först efter det att den har gått igenom godkännandehierarkin.

Bästa praxis nr 9

IGNORERA INTE SMÅ UPPDATERINGAR

På grund av komplexiteten i processen att implementera en förändring i ett nätverk och hantera de relaterade riskerna, så genomför inte de flesta nätverksadministratörer ändringar såvida de inte inkluderar en kritisk uppdatering, felkorrigering eller konfigurationsändring. På grund av den inställning tenderar nätverksadministratörer att ignorera små uppdateringar som tillhandahålls av enhetsleverantörer.

> Ett inte så roligt faktum: Enhetens sårbarheter ökar om icke-kritiska uppdateringar inte installeras. Därför tillåter de flesta leverantörer inte installation av uppdateringar förrän alla tidigare uppdateringar har installerats.

Även om du kanske slipper onödig nedtid och ändringsprocesser genom att hoppa över de obetydliga uppdateringarna, så utgör detta ett problem: Även om inte alla uppdateringar som utfärdats av en leverantör är kritiska, så utfärdar leverantörer vanligtvis flera små uppdateringar före en kritisk uppdatering. Vissa delar av de små uppdateringarna är nödvändiga för att den kritiska uppdateringen ska kunna köras.

Så nästa gång du hoppar över de små uppdateringarna och hoppar direkt till den kritiska uppdateringen för en enhet. bidrar du indirekt till att den kritiska uppdateringen installeras felaktigt. Och ibland när du hoppar över de små uppdateringarna kan du faktiskt förvandla de kritiska uppdateringarna till ett enormt säkerhetsproblem.

Här är några tips på hur du kan hålla jämna steg med även de minsta uppdateringarna utan att behöva schemalägga nedtid varje dag:

- Läs specifikationerna för varje uppdatering (enhetsspecifika och leverantörspecifika)som enhetstillverkarna utfärdar. Detta hjälper dig att förstå syftet med uppdateringen.
- Senarelägg installation av kritiska uppdateringar, men var noga med att aldrig hoppar över uppdateringar.
- Gruppera flera små uppdateringar och installera dem på en och samma gång. Du kan schemalägga veckovis nedtid under vilken du installerar alla små uppdateringar som utfärdats av tillverkare.

Bästa praxis nr 10

AUTOMATISERA UPPGIFTER NÄR DITT NÄTVERK ÄR LITET

> Ett inte så roligt faktum: Var femte nätverksadministratörer uppgav att de önskar att de hade automatiserat grundläggande uppgifter när deras organisations nätverk var en femtedel av dess nuvarande storlek.

Det är lätt för organisationer att hantera sitt nätverk medan det fortfarande är litet. I nätverkets tidiga stadier utförs de flesta nätverkshanteringsuppgifter (som t.ex. schemaläggning av nedtid och installation av enhetsuppdateringar) manuellt av nätverksadministratörer. De flesta organisationer överväger bara att utnyttja automatisering när deras nätverk blir större.

Alla erfarna personer inom domänen för nätverkshantering kommer att berätta för dig att denna strategin för nätverkshantering är mycket bristfällig. Varför? För och främst eftersom, **den manuella metoden är mycket felbenägen och för det andra eftersom i takt med att nätverket skalas upp och blir allt mer komplext och heterogent, blir det allt svårare att implementera någon form av automatisering.**

Därför ska du, även om du inte ser ett behovet för det, utnyttja kraften i automatisering när det är möjligt, även för de minsta uppgifterna – du kommer att tacka dig själv senare.

Här är en lista över saker du kan automatisera i de tidiga stadierna i ditt nätverk som hjälper dig på lång sikt:

- Processen att lägga till nya enheter till ditt verktyg för nätverksövervakning.
- Planera och schemalägga nedtid för nätverksenheter.
- Utföra underhållsuppgifter och fjärråtgärder.
- Utföra åtgärder när någon enhet passerar en viss tröskelgräns för en viss parameter.
- Säkerhetskopiera databaser samt konfigurationer på enhetsnivå och nätverksnivå.
- Utföra ny avsökning av enheter för att kontrollera deras tillgänglighet.

Bästa praxis nr 11

VÄLJ RÄTT PROGRAMVARA FÖR NÄTVERKSHANTERING

Av alla bästa praxis som ges i denna e-bok är detta den viktigaste. Det spelar ingen roll vad dina krav är, hur stort ditt nätverk är eller vilka strategier du följer för nätverkshantering, eftersom framgångsrik nätverkshantering i slutändan beror på en sak: att du väljer rätt programvara för nätverkshantering.

Det finns många olika typer av programvara för nätverkshantering på marknaden. Var och en har sina egna funktioner såväl som för- och nackdelar. Det är endast möjligt att välja rätt verktyg för nätverkshantering för din organisation genom en försiktig utvärdering av dina övervakningskrav och analys av verktygen på marknaden.

Fel programvara för nätverkshantering kan liknas vid att anställa fel person för jobb. Det komplicerar inte bara ditt arbete som nätverksadministratör, utan leder dig även raka vägen ned i nätverksfallgropar.

Så här kan du rädda dig själv från att använda fel verktyg för ditt nätverk:

- Var först och främst tydlig med dina mål och krav.
- De flesta applikationer har en gratis provperiod. Testa dem.
- Be om en demo-version. Läs recensionerna.
- Kolla in deras supportforum.
- Analysera deras enkla installation och användning kontra deras funktioner.
- Testa att köra provversioner av olika applikationer parallellt för att besluta vilket som passar dina behov bäst.

I slutändan är balansen mellan användbarhet och komplexa funktioner avgörande och du får betala ett dyrt pris om du inte balanserar de båda. Vid frågor kring att välja rätt verktyg kan du skicka e-post till support@opmanager.com, så hjälper vi dig gärna att göra rätt val.

KRITISKA VÄRDEN FÖR ATT HJÄLPA DIG ATT VÄLJA RÄTT VERKTYG FÖR NÄTVERKSHANTERING

- Stämmer dina primära krav överens med programmets funktioner?
- Är dina primära krav lätt konfigurerbara i applikationen?
- Överensstämmer antalet enheter som applikationen stöder med din nätverksstorlek?
- Stöder applikationen alla olika typer av enheter i ditt nätverk?
- Hur är det tekniska stödet?
- Hur är det med onlineforum och användargrupper?
- Hur är det med skalbarhet?
- Passar priset för ditt företag?