Morgan Sehlberg
T1 Dec. 99
Lars-Olof Friberg
WM-data D&D

Mentorprojekt del 1

Innehållsförteckning

Inledning

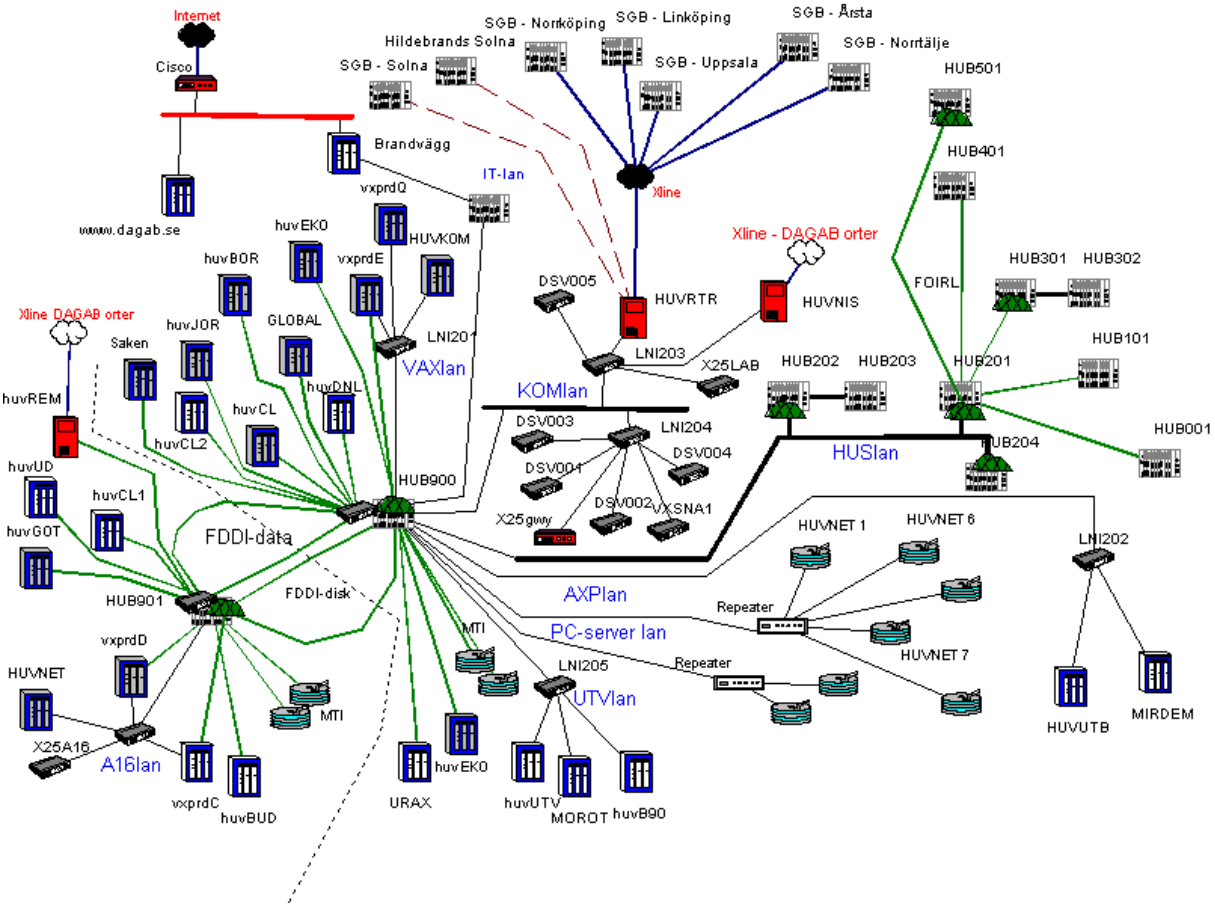
Jag har fått tillfälle att tillbringa en kort tid med min mentor Lars-Olof Friberg på WM-data D&D. Företaget ägs till hälften av D&D AB, till hälften av WM-data och har som enda kund D&D Dagligvaror som i sin tur är en sammanslagning av gamla Dagab på grossistsidan och D-gruppen i detaljistledet.
WM-data D&D sysselsätter ca 40 personer i allt från system- och programutveckling till support på användarnivå. Företaget ansvarar således för utveckling, förvaltning och drift av D&D´s nätverk och applikationer.
Under tiden jag var på företaget pågick som bäst Y2K-säkring av server och klientmiljöer, vilket gjorde det svårt för mig att få en riktig uppfattning om nätverkets topologi men jag fick chans att studera hårdvarans konfiguration och rutiner kring dokumentation och kundstöd/support.

Nätverksbeskrivning

WM-data D&D´s nätverksmiljö är stor och komplex. Miljön är uppbyggd av allt från stordatorer som Digital och IBM för de centrala systemen, via NT och Novell-servrar för PC baserade sytem, till handdatorer och truckdatorer ute hos kunderna (livsmedelsbutiker) och distributionsanläggningarna. D&D´s mest centrala system Dialog snurrar på Digitalmaskiner med operativsystemet Open VMS. I Dialog hanteras företagets alla kunder, order, faktureringar etc. och kopplat till denna miljö finns PC-baserade system för statistik, redovisning, analyser etc. För jobb direkt mot stordatorerna används terminalemulatorer, oftast Attachmate 6.5 och Pathworks. Lösningarna varierar med syftet. För många system hanteras informationen av Oracle-databaser.

Gränssnittet mot stordator-miljön är för kunder och anställda dock helt PC-baserat. De olika systemen förvaltas och utvecklas mestadels av egna programmerare och systemerare. För underhåll och drift av nätverk och system svarar en drift- och en teknikeravdelning. D&D´s anställda erhåller support på användarnivå från en kundstödsavdelning som tar emot och loggar ärenden och en närstödsavdelning som ansvarar för support, uppdateringar av mjukvara, konfigurering av nya PC etc.

Nedan följer en schematisk bild över en del av bl.a. företagets NT- och Novellservrar, så långt det var möjligt och tillåtet för mig att notera och föra vidare information:



Förutom de applikationer som direkt används för åtkomst av information från de centrala systemen, inskränker sig applikationsfloran till Office-paket och Web-läsare. Företaget använder uteslutande Compaqdatorer och endast två olika konfigurationer av dessa förekommer. WM-data D&D´s egen stab av systemerare och programmerare tillåts ha en ”friare” konfiguration där man är administratör av sin egen PC, med tillåtelse att installera program och förändra miljön lokalt. Övriga anställda tillåts endast förändra den ”synliga miljön”, skrivbord och genvägar mm.
De båda konfigurationerna sparas centralt och installeras med programmet Ghost, vilket tar ned tiden för en nyinstallation till under 5 minuter. Programuppdateringar, nya drivrutiner etc. trycks ut till klienterna via SMS. Hela detta förfarande bygger på så mycket standardisering som möjligt av användarmiljön. Undantag görs endast för ett fåtal mobila användare vilka kör Windows 95 på bärbart. I övrigt tillåts inget annat än Windows NT Workstation 4.0 med Servicepack 5.

Driftsäkerhet

Brandvägg

Systemets tillgänglighet övervakas indirekt genom att den övervakning som sker av E-post och extern WEB-server går genom brandväggen.
Då grundidén med en brandvägg är att den skall vara en dedicerad vägg mellan internt och externt datanät skall det finnas så få applikationer som möjligt i ett brandväggssystem.
Som brandvägg har valts Digitals AltaVista Fire wall.
Då systemet är direkt anslutet till Internet är det viktigt med strikt behörighetskontroll.
Automatisk övervakning av systemresurser kan inte ske med hjälp av windows-NT prestandahanterare, då AVFW utnyttjar en privat ”Monitor service”
Övervakning med prestandahanteraren kan däremot aktiveras manuellt.
Larm genereras till centralt larmhanteringssystem.
AVFW noterar försök till intrång och rapporterar det via Internet E-post till utsedd adressat (Postmaster) Vid återkommande intrångsförsök stängs den attackerade tjänsten av.

Inloggning

Naturligtvis krävs lösenord för alla användare, till nätverket, Exchange-servern, liksom till samtliga vitala system där access till de centrala systemen är en del. Implementationen av säkerheten och alla installationer följer alltid en på förhand uppgjord standard. Denna standard är omfattande och väl dokumenterad och alltid ett resultat av förhandlingar med kunden, D&D Dagligvaror. Nedan följer ett exempel på namnstandard, i detta fall för novell-servrar:

NAMNSTANDARD FÖR NDS.
OBS! De tre små grisarna är NO-NO.

TREE	Organisation + *TREE*	MAX_TREE
USERS (login)	4 gemener. 2 första i förnamn + 2 första i efternamn. Vid lika, lägg på en siffra	Lars Trustor = latr Lars Trustor = latr1
ORGANISATION	Bolagsnamnets 3 första bokstäver Versaler	MAX
ORGANIZATIONAL UNIT (Distrikt)	Distriktets första bokstav Versa	VÄST = W
ORGANIZATIONAL UNIT (Land)	Landets kod enligt X.500 Versaler	TYSKLAND = DE
ORGANIZATIONAL UNIT (Stad)	Stadens 4 första bokstäver Versaler	SILICON VALLEY = SILI
ORGANIZATIONAL UNIT (Avdelningar)	Avdelningens namn Förkorta om mer än 6 tecken Versaler	PRODUCTION = PROD
SERVER	Stadscontainerns namn + Föräldracontainerns namn + SRV# Versaler	SILI-ECO-SRV1
VOLUMES	Servernamn_Volymnamn Versaler	SILI-ECO-SRV1_SYS

PRINT SERVER	Föräldracontainerns namn + Modellnamn + PS# Versaler	PROD-HP500C-PS1
PRINTER	Föräldracontainerns namn + Modellnamn + P# Versaler	PROD-HP500C-P1
PRINTQUEUE	Föräldracontainerns namn + Modelnamn + PQ# Versaler	PROD-HP500C-PQ1
ORGAN. ROLE	Fullständigt namn Första versal, resten gemener	Marketing director

Backup

Backup-rutinerna är lika komplexa som nätverksmiljön totalt. Strategin för backup växlar med vilken typ av maskin och information det handlar om. Generellt kan sägas att backup förfarandet till stor del är automatiserat med olika typer av tredjeparts-lösningar. Ofta backup-robotar som administreras och bevakas centralt av driftsgruppen. För varje separat maskin finns rutiner, scheman, åtgärdplaner etc dokumenterat enligt följande exempel.
Backupschema (Observera att detta är för bara en Dator i hela nätverket)

Nod: HUVBOR
SYSTEM: OPENWMS
ROBOT: ULLA

Class1: Omkörning utan Fel-Sökning
Class2: Omkörning efter Fel-Sökning
Class3: Ingen omkörning

Typ: A

OBJEKT	POOL	MÅN	TIS	ONS	TOR	FRE	LÖR	SÖN	KÖR-TID	KÖR-TYP	BANDTYP
BOR$EOD	HUVBOR		20-23		20-23		20-23	20-23	00:05	FULL	TK88-C
BOR$BOD	HUVBOR	20-23		20-23		20-23			00:15	FULL	TK88-C
BOR$AIJ	HUVBOR	20-23	20-23	20-23	20-23	20-23	20-23	20-23	00:20	FULL	TK88-C
BOR$MIRDB	HUVBOR	20-23	20-23	20-23	20-23	20-23	20-23	20-23	01:00	FULL	TK88-C
BOR$INTF	HUVBOR	20-23	20-23	20-23	20-23	20-23	20-23	20-23	00:25	FULL	TK88-C
BOR$DISK6	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							00:20	FULL	TK88-C
BOR$DISK10	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							01:00	FULL	TK88-C
BOR$DISK20	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							01:30	FULL	TK88-C
BOR$DISK30	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							00:30	FULL	TK88-C
BOR$OPENWMS	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							00:20	FULL	TK88-C
BOR$ARCDB	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							00:30	FULL	TK88-C
BOR$ARKIV	HUVBOR	KÖRES MÅNDAGAR BEROENDE AV NATTBACTH							01:00	FULL	TK88-C
BOR$DISK6	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:10	CUM	TK88-C
BOR$DISK10	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:20	CUM	TK88-C
BOR$DISK20	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:10	CUM	TK88-C
BOR$DISK30	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:20	CUM	TK88-C
BOR$OPENWMS	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:20	CUM	TK88-C
BOR$ARCDB	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:30	CUM	TK88-C
BOR$ARKIV	HUVBOR	EJ MÅNDAGAR BEROENDE AV NATTBACTH							00:20	CUM	TK88-C
BOR$DAY	HUVBOR	KÖRES TVÅ GÅNGER I MÅNADEN KRÄVER 1 TAPE STARTTID : 10:00							00:10	FULL	TK88-C

Förvaltning

Den dagliga driften eller förvaltningen av nätet ansvaras av en Driftgrupp som i samråd med andra grupper som Systemutveckling, Teknikergruppen och gruppen Närstöd, hela tiden övervakar och arbetar kontinuerligt med nätet för det ska gå så smidigt som möjligt gentemot Kunden.
Driftgruppen består av ett antal personer som är experter på olika områden och tillsammans har ett övergripande ansvar över nätverket. Personalen i driftgruppen roterar dagligen i ett jourschema.
Systemutveckling är den grupp av personal som först kommer i kontakt med kunden. Gruppen Systemutveckling består av programmerare och systemerare som själva utvecklar system unika för kunden och deras kravspecifikationer. De bistår även med hjälp av implementering av tredje parts system och program.
Teknikergruppen arbetar med nätverkets servrar och den fysiska nätverksmiljön i sammarbete med Driftgruppen och Närstödsgruppen som är en supportgrupp först och främst för de interna PC datorerna.

Dokumentation

Dokumentation görs av alla i grupperna. Den sammanställs av ansvarige i respektive grupp och sparas beroende av dess syfte i olika ”Böcker” eller Lathundar.
Ett exempel på vad som kan dokumenteras som en lathund:
Denna ”lathund” är i första hand ämnad att vara ett stöd för den personal som sköter driftövervakningen.
System Watchdog (PSW)
Innehåller en eller flera databaser som beskriver vilka system som skall övervakas samt olika larmnivåer för t.ex. fyllnadsgraden på diskar.
För att säkerställa driften av de av D&D ägda systemen har en driftövervakning skapats. Denna övervakning bygger på övervakning av konsolterminalerna samt pollning av de olika systemen efter specifika händelser och avvikelser.
Console Manager (PCM)
Övervakar konsolterminalerna på de övervakade systemen. Denna produkt innehåller även larmdetektering, eventhantering mm.
Denna rutin används för att säkerställa funktionaliteten i larmkedjan. Det innebär att den skickar in ett larm i den ena änden och förväntar sig att en åtgärd startas i den andra änden. Ett batchjob på GLOBAL(server) skickar ett externt meddelande till PSW och definierar ett logiskt namn. När meddelandet detekteras av PCM, startas en actionrutin som tar bort meddelandet och definierar om det logiska namnet. Skulle detta inte ske, kommer batchjobbet att skicka ett meddelande till den GSM-telefon som tillhör den som har teknikjouren.

Säkerhetspolicy

Dokumentation, drift- och backuprutiner bestäms av WM-data D&D i samråd med kundens representant, systemägaren. Denne är aldrig densamma för de olika systemen varför rutinerna varierar. Hela verksamheten bygger just på detta förhållande mellan leverantören av tjänsten och kunden och hela tiden görs ett viktigt avvägande mellan säkerhetsnivå och användarvänlighet. Då de vitala applikationerna är egna produkter, satsas ordentligt på att dessa skall motsvara vad användaren behöver för att kunna jobba effektivt. Detta tillsammans med en strikt standardisering av användarmiljön lägger grunden till en enkel men effektiv och lättövervakad säkerhetpolicy.

Slutord

WM-data D&D har som sagt ett mycket stort och komplex nätverk,
med dess stordatorer och avancerade system som skiftar beroende på kundernas behov.
Det är därför svårt att ha en annat än en generell uppfattning om vad som är bra och dåligt.
Det som slog mig under den korta tid jag var på plats var det att det fanns väldigt många med djupa kunskaper inom specifika ämnen som t.ex. Open VMS eller Oracle. Men som novis inom ämnet så är det svårt att ifrågasätta delar av personalens ibland ”nischade” arbetsuppgifter.
Med åtanke på nätverkets avancerade uppbyggnad och min ringa insyn kan jag inte ge förslag på specifika förbättringar, jag ger istället ett exempel på ett problem.
Problemet har en gång uppstått inom min mentors ansvarsområde varvid han fick stort besvär att återställa det ”drabbade” nätet.

En avdelning på ett (okänt!) företag har 3 Ethernetsegment (10Base2 koaxialkabelnät med bus-topologi) som är sammanbundna till ett nätverk med en transparent 3-portsbrygga. Systemadministratören får ett nytt välbetalt jobb och slutar tvärt vid institutionen. En ersättare skaffas dock snabbt fram. Det visar sig att han är en gammal IBM-anställd och token-ring-fanatiker. Han upptäcker snabbt att segmentens ena ände inte är ansluten och blir en aning förvirrad. Det får till följd att han snabbt skaffar in ytterligare en brygga och ansluter varje segments lediga ände till en port på den nya bryggan. Min mentor var inte token-ring fanatikern! Vad skedde då på nätverket?

Kommunikationen inom ett segment påverkades inte, men när ett ethernetpaket skulle till en maskin på ett annat segment blev det problem. Båda bryggorna skulle då vidarebefordra paketet till det andra segmentet och mottagarmaskinen fick dubbel uppsättning av paketet. Dessutom var det så att bryggornas paketsändning resulterade i kollisioner eftersom de började sända ungefär samtidigt och långt ifrån varandra.

Sammanfattningsvis kan sägas att jag har upptäckt ännu en gång, att det finns mycket att lära! Även erfarna tekniker förivrar sig och gör misstag.
I en stor organisation är det inte en och samma person som sitter inne med all dokumentation eller som har ensamt ansvar för nätets förvaltning, driftsäkerhet eller utbyggnad.
Det kan alltså vara fördelar med många specialister som samarbetar och har gemensamt ansvar för företagets nätverk.