

UNIVERSITAT OBERTA DE CATALUNYA

Enginyeria Tècnica en Informàtica de Sistemes

Implantació d'una eina de gestió de xarxes i sistemes

Alumne: Albert Timoneda Martínez
Dirigit per: Jordi Serra i Ruiz
Co-dirigit per: Miquel Colobran Huguet

CURS Gener-2004

Resum

Implantació d'una eina de gestió de xarxes i sistemes

Actualment, les empreses i organitzacions disposen de sistemes de la informació distribuïts en diferents seus o ubicacions, interconnectades per sistemes de comunicacions, i així es poden organitzar grups de treball distribuïts, compartir recursos o comunicar informació ràpidament.

Resulta imprescindible disposar d'eines de gestió per poder administrar tots aquest dispositius, ja que necessitem tenir una visió global de la xarxa per poder saber les implicacions que comporta la fallada de certs elements d'aquesta xarxa. També una gestió centralitzada de la xarxa i dels sistemes comporta una important reducció en les despeses d'administració de la xarxa.

Mitjançant una eina de gestió de xarxes i sistemes podem realitzar una gestió centralitzada de tots aquests de recursos, la qual cosa ens permetrà la detecció ràpida de fallades, una millor accessibilitat als components de xarxa i als sistemes, i per tant una administració més eficient i còmoda.

L'obtenció i l'anàlisi d'informes de rendiment dels equipaments, informes de serveis i informes de nivell de servei, conjuntament amb el control dels inventaris de programari i maquinari ens permetran poder efectuar anàlisi ràpids i eficients de l'estat de la xarxa, la detecció d'errors i colls d'ampolla.

La comparació d'informes periòdics ens permetrà seguir tendències i comportaments de la xarxa, preveure futurs problemes i prendre les accions preventives. D'aquesta forma, anticipant-nos als problemes, obtindrem el màxim rendiment i eficàcia dels nostres recursos tan de maquinari i programari, com humans.

Índex

1. Introducció	1
1.1. Necessitat d'una eina de gestió	1
1.2. Objectius	1
1.3. Enfocament i mètode seguit	2
2. Per què OpenView?	3
2.1. Administració de fallades i representació gràfica de la xarxa	3
2.2. Informes	5
2.3. Facilitat d'ús	6
2.4. Conclusions i elecció del producte	6
3. Escenari	8
3.1. Seu A	9
3.2. Seus B i C	11
3.3. Seus 1, 2 i 3	12
3.4. Seus 11, 12, 13, 21, 22, 23, 31, 32 i 33	13
4. Network Node Manage	14
4.1. Funcionament bàsic de NNM	14
4.2. Descobriment inicial de la xarxa	15
4.2.1. Funcionament del descobriment inicial	15
4.3. Fonaments per la creació de mapes	20
4.3.1. Mapes	20
4.3.2. Submapes	20
4.3.3. Submapa principal	20
4.3.4. Submapa inicial	21
4.3.5. Gràfics en segon pla	21
4.3.6. Objectes	21
4.3.7. Símbols	21
4.3.8. Mapes personalitzats	22

4.4. Control dels objectes	23
4.4.1 Estats compostos	24
4.5. Sistema d'events	25
4.5.1. Alarm Browser	25
4.5.2. Categoria d'alarmes	26
4.5.3. Configuració d'alarmes	27
4.6. Sistema de correlació d'events	29
5. OpenView Operations for Windows	30
5.1. Introducció	30
5.2. Smart Plug-ins	31
5.2.1. SPI for Windows Operating System	32
5.2.2. SPI for Active Directory	32
5.2.3. SPI per servidors Web	33
5.2.4. SPI for Microsoft Exchange Server	33
5.2.5. SPI for Microsoft SQL	35
5.3. Integració amb altres productes de la família OpenView	36
5.3.1. Reporter	36
5.3.2. Network Node Manager	36
5.4. Instal·lació d'OpenView Operations for Windows	37
5.4.1. Tasques prèvies	37
5.4.2. Requeriments de seguretat per utilitzar OVO for Windows	38
6. System Management Server	40
6.1. Introducció	40
6.2. Disseny i instal·lació de la Site SMS	40
6.2.1. Jerarquia de Sites SMS	40
6.2.2. Instal·lació i configuració de SQL Server	41
6.2.3. Instal·lació i configuració del Site Server	42
6.2.4. Instal·lació i configuració de site systems addicionals	43

6.2.5. Instal·lació de clients	44
6.2.5.1. Descobriments selectiu per subxarxes IP	45
6.2.5.2. Instal·lació selectiva del client SMS	45
6.2.5.3. Instal·lació i configuració d' agents	47
6.3. Consultes i col·leccions	52
6.4. Integració amb Network Node Manager	53
6.5. Control remot	54
6.6. Inventaris de maquinari i programari	55
7. Informes	56
7.1. Organització	57
7.2. Accés als informes	57
7.2.1. Accés de consulta als informes automàtics	57
7.2.2. Accés per generar informes personalitzats	58
7.3. Disseny de la base de dades reports	58
7.4. Descripció dels informes	59
8. Conclusions	62

1.Introducció

1.1. Necessitat d'una eina de gestió

Si una estació de treball d'una xarxa no pot accedir a una bústia de correu, com podem saber si falla l'estació de treball, algun dels commutadors, encaminadors o línies de comunicacions fins arribar al servidor al servidor de correu o si és el mateix servidor de correu?

Un servidor de fitxers s'ha quedat sense espai en disc, ha estat perquè era el seu creixement normal o per què un usuari s'ha copiat diversos DVD en el servidor?

Aquest parell d'exemples justifiquen la necessitat de disposar d'eines, els administradors de xarxes necessitem tenir una visió global de la xarxa, ja que una xarxa no és una sèrie de dispositius, aplicacions i serveis aïllat, sense dependències entre aquests elements, sinó que hem d'entendre una xarxa com un conjunt de dispositius aplicacions i serveis interrelacionat entre ells.

L'eina de gestió de xarxes ens ha de permetre detectar fàcilment els errors de xarxa, i ha de proporcionar un accés ràpid a tots els elements de la xarxa per poder solucionar aquests errors.

També és útil disposar d'eines d'anàlisi de la xarxa, que ens proporcionin informes sobre utilització, disponibilitat i rendiment dels elements de la xarxa, per poder detectar errors, efectuar tasques preventives o justificar la substitució o ampliació de certs components de la xarxa. Això ens permetrà poder anticipar-se a les fallades, estar preparat i saber com reaccionar en el cas que es produeixin.

1.2. Objectius

L'objectiu d'una eina de gestió de xarxes i sistemes és obtenir un major rendiment dels sistemes de la informació i dels sistemes de comunicacions. Aquesta finalitat l'assolirem optimitzant els recursos disponibles adequadament, realitzant una administració centralitzada i eficient de la xarxa de comunicacions i dels sistemes de informació, amb la detecció ràpida d'errors i de colls d'ampolla, i realitzant les pertinents tasques preventives.

En resum, les funcionalitats bàsiques de l'eina de gestió de xarxes i sistemes per obtenir el seu objectiu són:

- Monitorització activa de sistemes i de la seva disponibilitat mitjançant l'obtenció de diversos mapes i vistes, com per exemple: el mapa físic de comunicacions, les vistes de servidors, les vistes d'encaminadors i commutadors, les vistes de serveis i aplicacions (correu, fitxers, bases de dades), la vista d'elements crítics, etc. Mitjançant aquests mapes i vistes podrem detectar errors i fallades, accedir als encaminadors, commutadors, servidors o estacions de treball per poder interactuar més fàcilment.

- Recepció d'events i de fitxers de registres generats pels sistemes, a través de la implantació d'agents obtindrem un repositori d'alarmes i events categoritzats per criticitat i classificats per tipus (comunicacions, rendiment dels servidors, còpies de seguretat, etc.). També podrem realitzar l'automatització d'accions davant de determinats events, definició d'umbrals per generar alarmes i la correlació d'events.
- Obtenció d'informes a partir del repositori d'alarmes i events i de la recollida de dades dels agents instal·lats en el maquinari. Mitjançant l'anàlisi dels informes podrem detectar i corregir errors, també podrem realitzar actuacions preventives en la xarxa i en els sistemes de informació, a partir de les tendències que reflecteixen aquests informes.
- Obtenció d'un inventari de programari i maquinari del parc informàtic.
- Control remot d'estacions de treball i servidors de la nostra xarxa.
- Distribució desatesa de programari a les estacions de treball.

1.3. Enfocament i mètode seguit

Partim d'una organització fictícia distribuïda en diferents seus, tal com veurem en el capítol 2, on volem implantar una eina de gestió de sistemes, com no disposem d'un escenari real per poder realitzar la implantació, realitzarem una simulació del desplegament amb els següents dispositius:

- Un encaminador-commutador Cisco 3550 Series: per poder simular LAN's i WAN's, sense haver de disposar de línies de comunicacions i més d'un encaminador i commutadors.
- 2 servidors ML370, un servidor per instal·lar els productes de la eina de gestió i l'altre per instal·lar les diferents aplicacions: Exchange 2000, SQL 2000, etc. On poder anar realitzant els diferents descobriments, instal·lar els agents de monitorització, obtenir els diferents inventaris, etc.
- 1 estació de treball Compaq Evo D300v per realitzar descobriment de clients i instal·lar agents de Server Management Server.

L'enfocament del projecte és anar instal·lar un per un els diferents productes que componen l'eina de gestió en aquest ordre:

1. OpenView Network Node Manager.
2. OpenView Operations for Windows.
3. System Management Server.
4. Desenvolupament d'informes.

Seguidament realitzarem una comprovació del funcionament de cada producte amb la resta de dispositius dels quals disposem per realitzar els bancs de proves, i un cop provat poder extreure les conclusions oportunes per obtenir la simulació del resultat del desplegament del producte en la nostra xarxa fictícia.

2. Per què OpenView?

La diversitat de recursos, el tamany de la xarxa, els elements fora de control són motius que justifiquen l'important despesa d'implementar una eina d'administració de xarxes i sistemes.

En el mercat existeix una gran varietat de productes per administrar xarxes i sistemes, en la seva gran majoria es tracta de productes modulars, dels quals hem de seleccionar els paquets que necessitem segons els dispositius, servidors, sistemes operatius o aplicacions que hem d'administrar.

Realitzar una comparativa de tots els productes era totalment impossible, per la qual cosa hem realitzat un preselecció de tres productes, basant-nos en una primera impressió a partir de la informació més general d'aquests productes, i també perquè no dir-ho, hem considerat la quota de mercat d'aquest productes.

Els productes preseleccionat han estat:

- OpenView de Hewlett-Packard
- Unicenter de Computer Associates
- VitalSuite de Lucent

La valoració general dels tres productes és excel·lent, quasi tots els productes complien les nostres expectatives de funcionament en tots els apartats en que hem dividit aquesta comparativa. Per la qual cosa ha estat especialment difícil l'elecció d'un d'ells, com podrem comprovar a continuació:

2.1. Administració de fallades i representació gràfica de la xarxa.

OpenView de Hewlett-Packard té una gran capacitat d'administrar dispositius mitjançant una interfície molt consistent. Monitoritza els recursos de xarxa i produeix informes d'activitat de xarxa d'una enorme utilitat. OpenView és fàcilment escalable, funciona en diverses plataformes, adaptant-se especialment al nostre escenari i facilita enormement l'administració de la xarxa.

El component principal de l'OpenView, Network Node Manager (NNM), és una eina molt eficient en el descobriment de la xarxa, molt precisa determinant dispositius de xarxa, generant gràfics de mapes de xarxa, capturant i proporcionant estadístiques de dispositius, i processant les alertes SNMP entrants.

NNM utilitza Management Information Base (MIB), que recull a partir de diverses fonts, incloent encaminadors i commutadors. Proporciona i visualitza dades de Capa 2 (enllaç de dades), però la part més important de NNM són els mapes detallats de Capa 3 (xarxa).

També utilitza expressions MIB predefinides i proporcionades per HP com per exemple les d'utilització i percentatges d'error, les de total de paquets per categoria, les de retransmissions, les de memòria utilitzada en els dispositius Cisco, i les de percentatge d'utilització full-duplex, especialment útils per determinar fallades i coll d'ampolla d'una xarxa.



El punt fort d'Unicenter de Computer Associates són l'administració d'events, proporciona una bona organització i accessibilitat al catàleg d'activitat i d'events de la xarxa. La consola d'events dintre de l'Unicenter Enterprise Manager facilita enormement la gestió dels events. Crear un nou tipus d'event és simplement qüestió de substituir paràmetres, tals com el domini, el node ID, el tipus de dispositiu, una condició d'error característica o l'acció a efectuar quan es produeix una errada.

L'eina Network and System Management alerta dels problemes en el nivell superior, estalviant-nos de revisar d'errors de nivells inferiors derivats per aquest problema. Mitjançant els seus agents, l'Unicenter monitoritza segments de la nostra xarxa, dispositius i servidors. El paquet Performance Management és una potent eina per detectar potencials problemes de xarxa i servidors, però pobre per la interpretació d'anàlisi. Es basa en umbrals establerts per l'administrador, els agents detecten problemes imminents i envien traps o events al Distributed State Machine d'Unicenter, que analitza l'event, l'enregistra en un repositori d'events i senyala la categoria de criticitat de l'objecte en el Network and Systems Management.

Per detectar problemes abans que passin, Unicenter Historian analitza l'activitat i els events de xarxa comparant gràfiques, tendències i projeccions per períodes seleccionats.

VitalSuite de Lucent és un conjunt de col·leccions de dispositius disposats gràficament i també monitoritza l'activitat de xarxa. VitalSuite detecta acuradament i fàcilment errors de connectivitat, ajudant d'aquesta manera a solucionar-los.

VitalNet recull dades dels dispositius SNMP i de les estacions de treball que tenen instal·lat el client VitalAgent. VitalNet transmet la informació a VitalAnalysis i a VitalHelp. VitalAnalysis monitoritza aplicacions i manté una anàlisi històrica del sistema amb gràfics i tendències. S'emmagatzemen dades de diversos anys en una base de dades de Microsoft SQL Server amb finalitats de planificació d'actuacions sobre la xarxa i servidors.

VitalHelp calcula l'estat de les aplicacions TCP-IP. Quan determina la causa del problema, VitalHelp envia alertes a l'administrador via e-mail, busques o traps SNMP a l'igual que OpenView.

2.2. Informes

OpenView mitjançant NNM genera informes periòdics de disponibilitat general, i de rendiment dels encaminadors Cisco; estadístiques de generació de tràfic i dels valors més interessants per poder realitzar anàlisi sobre el tràfic de paquets i sobre els protocols de xarxa utilitzats. Aquest informes poden ser enviats via e-mail, amb enllaços HTML als dispositius.

OpenView Reporter és una eina flexible i entenedora que ens permet explotar les dades que extreu OpenView per conèixer tots els detall de la nostra xarxa, també permet personalitzar informes fàcilment. Podem obtenir informes per imprimir o com a pàgines Web, les gràfiques ens seran de gran utilitat per visualitzar les dades proporcionades.

Mitjançant un portal d'administració d'informes basat en Java, Unicenter proporciona una gran varietat d'informes de gran utilitat. Consisteix en un sumari de pàgines Web, de vistes d'entitats de negoci definides per l'administrador en forma d'arbre expansible. L'estructura d'arbre permet una gran accessibilitat a tots els elements relacionats entre si.

Unicenter Topology Browser permet seleccionar porcions de xarxa, per poder efectuar una administració segmentada, mentre que Severity Browser ens identifica els events dels recursos seleccionats.

Lucent Technologies
Bell Labs Innovations



VitalSuite utilitza Heat Chart per detectar colls d'ampolla fàcilment, per identificar-los a primera vista i determinar les seves possibles causes. També proporciona gràfics i estadístiques d'aplicacions i recursos del sistema.

Els informes de VitalSuite ofereixen tres tipus de vistes personalitzables: negoci, aplicacions i informes. També proporciona informes amb format Web. La vista d'aplicacions conté informes indexats per grups com dominis, grups, clients i servidors. Cada índex inclou dades sobre paquets perduts, disponibilitat, temps de resposta, etc.

2.3. Facilitat d'ús

OpenView disposa d'un client Java que ens proporciona una interfície gràfica molt intuïtiva, la qual ens permet construir mapes per administrar la xarxa fàcilment, alhora que obtenim informes, notificació d'events, disposem de diferents opcions de configuració i filtres, per últim també ens proporciona informació detallada dels dispositius, estadístiques i alarmes.



La interfície gràfica de NNM disposa d'un bon disseny de pàgines Web dinàmiques, la seva simplicitat d'ús i d'aplicació de filtres fa possible l'administració de grans xarxes amb NNM.

Unicenter ofereix vistes tabulars, 2D i unes espectaculars 3D per administrar objectes. Les vistes 3D permeten visualitzar la xarxa sencera d'una companyia multinacional en una representació rotativa de la Terra. Si hi ha problemes en una seu, apareix un punt vermell, des d'on podrem arribar al dispositiu conflictiu i als problemes relacionats.

Les vistes 2D que proporciona Unicenter fan servir una llegenda de colors molt útil per representar els possibles errors dels dispositius o serveis.

La interfície gràfica que proporciona VitalSuite és especialment amigable i intuïtiva, sap utilitzar els colors per donar aquest enteniment dintre de la complexitat de la xarxa. La arquitectura flexible de VitalSuite es fa patent en la diversitat i varietat d'entorns d'aplicacions de negoci.

2.4. Conclusions i elecció del producte

La selecció d'un dels tres productes ha estat francament difícil, ja que tots tres productes superen les nostres expectatives a priori, cobreixen amb escreix les nostres necessitats: ofereixen excel·lents vistes de la xarxa, proporcionen eines d'administració, de notificació d'events i alarmes, i faciliten informes d'una gran utilitat.

Les millors característiques de VitalSuite són la monitorització de la xarxa i les seves eines d'administració, a més a més, la seva interfície gràfica és força intuïtiva, però li falta desenvolupar una mica més la gestió d'events i alarmes.

De Unicenter és immillorable la seva interfície gràfica, sobretot les seves vistes 3D, i els informes que proporcionen els seus agents són de gran utilitat. En canvi, hauria de proporcionar millors eines d'administració de xarxa.

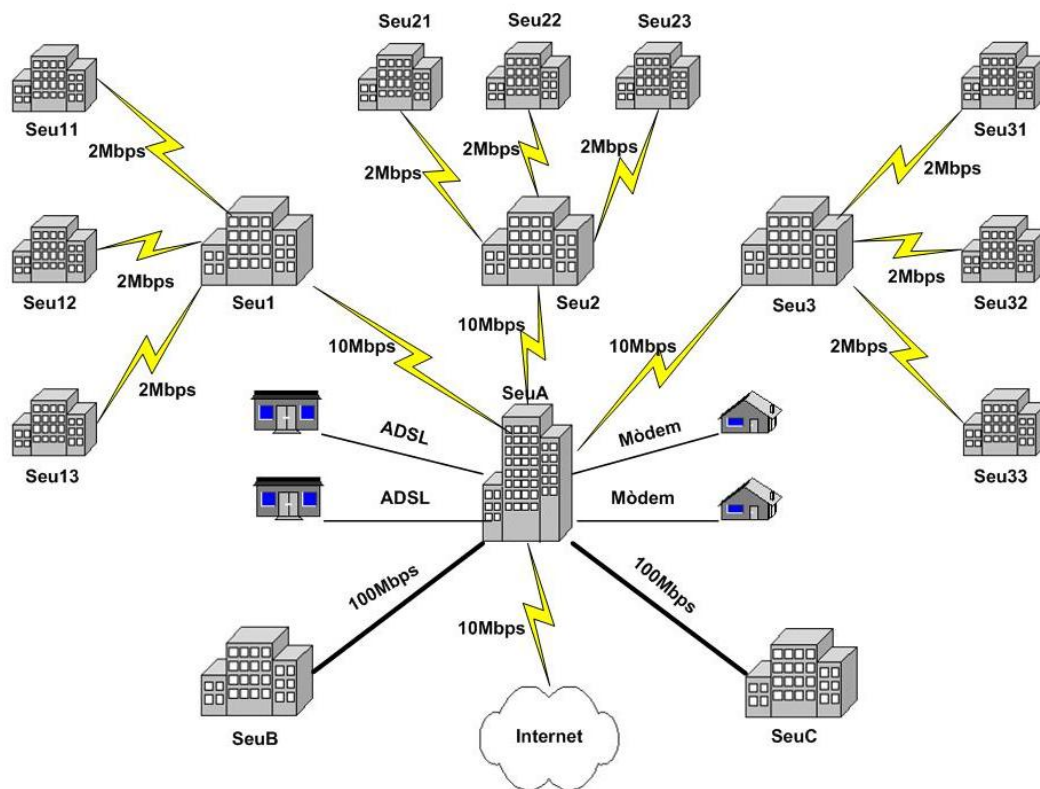
OpenView té una interfície gràfica molt intuïtiva amb gran diversitat de vistes, genera informes de gran utilitat, i proporciona una gran solidesa en la integració de tots els productes que formen part d'OpenView. Potser no és un producte espectacular, però en conjunt hem trobat que OpenView és un producte molt més compacte que la resta de productes. Això conjuntament amb la seva escalabilitat i la integració amb els productes que hem seleccionat pel nostre escenari de desenvolupament, ens ha fer decantar-nos finalment per OpenView.

3. Escenari

L'escenari sobre el qual implementarem l'eina de gestió de xarxes i sistemes serà una empresa o organització fictícia, distribuïda en diferents seus o edificis, que depenent de la seva importància comptarà amb uns determinats recursos.

En primer lloc mostrem un mapa topològic d'aquesta xarxa:

Mapa Topològic



L'empresa consta de 12 seus interconnectades per línies commutades i per línies punt a punt, a més a més, també permet l'accés des de petites oficines o des de casa, hotels, etc. a alguns dels seus empleats mitjançant línies ADSL, XDSI o analògiques.

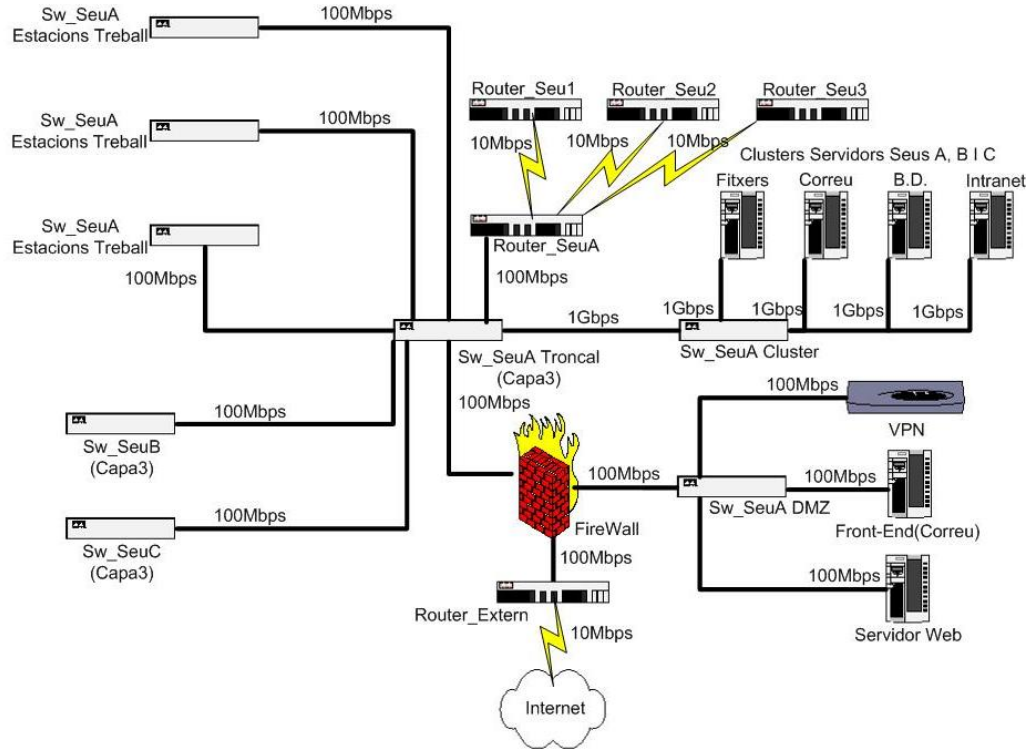
La seu A és la seu central, i per tant la seu principal de l'organització, punt clau de l'estructura topològica d'estrella estesa. Connecta amb les seus B i C que són departaments de la Seu A amb una línia commutada de 100 Mbps., i amb les seus 1, 2 i 3 que són delegacions territorials amb línies punt a punt de 10 Mbps. Aquestes delegacions territorials connecten amb les seus comarcals (seus 11, 12, 13, 21, 22, 23, 31, 32 i 33) amb línies de 2 Mbps.

Per últim, la sortida a Internet de tota l'empresa es realitza a través de la seu A.

3.1. Seu A

Anem a veure detalladament la Seu A:

Seu A



La seu A té un FireWall amb tres segments:

1. Segment d'Internet
2. Segment de la DMZ amb els serveis de VPN (accés remot a la xarxa), servidor de correu i servidor web.
3. Segment intern

El segment intern consta d'un commutador troncal de capa 3 que connecta:

- Els commutadors amb les estacions de treball
- Les seus B i C.
- El commutador amb els clusters de fitxers, correu, bases de dades i intranet.
- L'encaminador que connecta amb la resta de les seus de l'organització.

La relació del maquinari de la Seu A és el següent:

Comunicacions:

- Commutador - Encaminar Sw_SeuA Troncal: Cisco Catalyst 3550 amb 24 ports FastEthernet + 2 ports Gigabit.
- Commutador - Encaminador Sw_SeuA Cluster: Cisco Catalyst 3550 amb 12 ports Gigabit.
- Commutadors Sw_SeuA Estacions de Treball: Cisco Catalyst 2950 amb 24 ports FastEthernet.
- Commutador Sw_SeuA DMZ: Cisco Catalyst 2950 amb 24 ports FastEthernet.
- Encaminador Router_SeuA: Cisco 2640 amb 1 port FastEthernet i 4 ports sèrie.
- Encaminador Router_Extern: Cisco 1750 amb 1 port FastEthernet i 1 port sèrie.
- Concertador Cisco VPN 3005.
- FireWall: Cisco PIX 501.

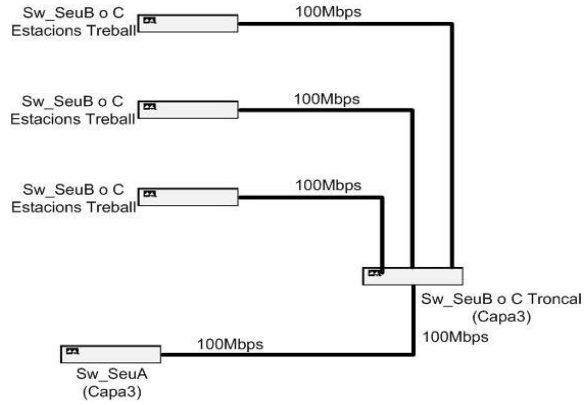
Servidors:

- 2 servidors hp Proliant DL 380 per cluster de Fitxers.
- 2 servidors hp Proliant DL 380 per cluster de l'Intranet.
- 2 servidors hp Proliant DL 580 per cluster de Correu.
- 2 servidors hp Proliant DL 580 per cluster de Bases de Dades.
- 1 servidor hp Proliant DL 380 per Controlador de Domini del Active Directory del domini de Windows 2000, DNS i WINS.
- 1 servidor hp Proliant DL 380 per servidor correu Front End (accessibilitat correu des d'Internet).
- 1 servidor hp Proliant DL 580 per servidor Web Internet.
- Robot de còpies de seguretat: hp Storage Works MS5000 series library.
- Cabina de discos: modular san array 1000.
- Commutador cluster: hp Storage Works SAN switch 2/16.

3.2 Seus B i C

Les seus B i C estan estructurades així:

Seus B i C



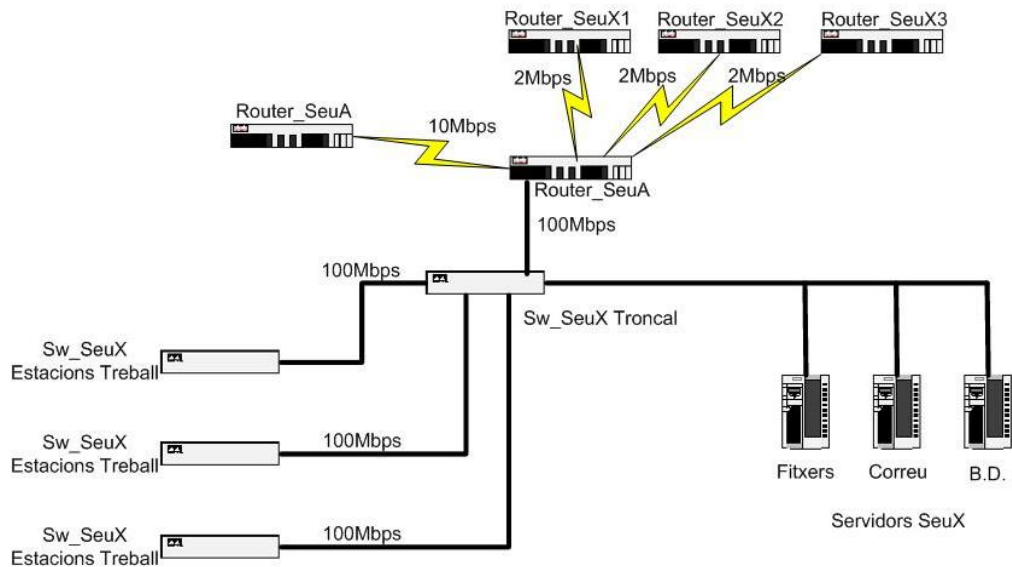
Les Seu B i C disposen d'un commutador-encaminador Cisco 3550 que connecta la Seu Central A amb els commutadors Cisco 2950 amb estacions de treball.

Aquestes seus no disposen de servidors, ja que la Seu A concentra tots els servidors d'aquestes seus.

3.3. Seus 1, 2 i 3

Les delegacions territorials 1, 2 i 3 tenen aquesta composició:

Seus 1, 2 i 3



Aquestes delegacions estan compostades per un encaminador que connecta amb la Seu Central A, això ens permet la connexió a Internet i a la Intranet, accés des de la VPN o del correu des d'Internet. L'encaminador també enllaça les delegacions territorials amb les seus comarcals.

L'encaminador està connectat amb un commutador troncal que, a més a més, enllaça les estacions de treball amb els servidors de la seu.

Maquinari de comunicacions:

- Commutador Sw_SeuX Troncal: Cisco Catalyst 2950 amb 12 ports FastEthernet + 4 ports Gigabit.
- Commutadors Sw_SeuX Estacions de Treball: Cisco Catalyst 2950 amb 24 ports FastEthernet.
- Encaminador Router_SeuA: Cisco 2640 amb 1 port FastEthernet i 4 ports sèrie.

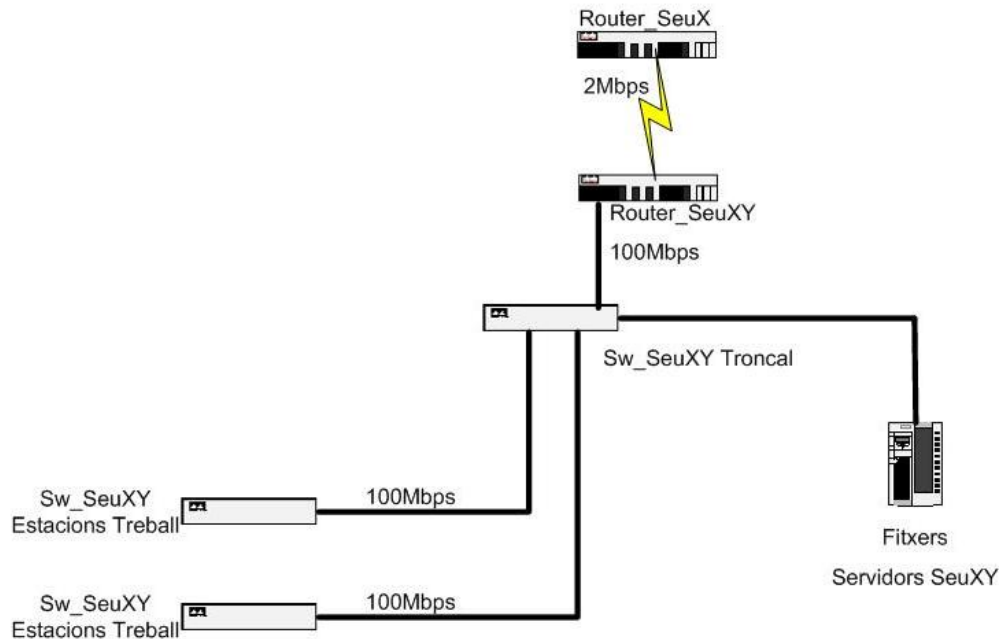
Servidors:

- 1 servidor hp Proliant DL 380 per Fitxers.
- 1 servidor hp Proliant DL 580 per Correu.
- 1 servidor hp Proliant DL 580 per Bases de Dades.

3.4 Seus 11, 12, 13, 21, 22, 23, 31, 32 i 33

Per últim les seus comarcals 11, 12, 13, 21, 22, 23, 31, 32 i 33 estan representades gràficament:

Seus 11, 12, 13, 21, 22, 23, 31, 32 i 33



Aquestes seus comarcals estan compostes per un encaminador que connecta amb les delegacions territorials, això ens permet l'accés al correu i a les bases de dades que es troben concentrades en les delegacions, i la connexió a Internet i a la Intranet, accés des de la VPN o del correu des d'Internet.

L'encaminador està connectat amb un commutador troncal que, a més a més, enllaça les estacions de treball amb els servidors de la seu.

Maquinari de comunicacions:

- Commutador Sw_SeuXY Troncal: Cisco Catalyst 2950 amb 12 ports FastEthernet + 1 port Gigabit.
- Commutadors Sw_SeuXY Estacions de Treball: Cisco Catalyst 2950 amb 24 ports FastEthernet.
- Encaminador Router_SeuA: Cisco 1750 amb 1 port FastEthernet i 1 port sèrie.

Servidors:

- 1 servidor hp Proliant DL 380 per Fitxers.

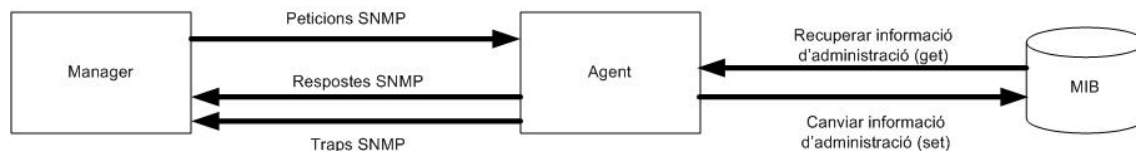
4. Network Node Manage

4.1. Funcionament bàsic de NNM

OpenView NNM utilitza els protocols SNMP, TCP/IP, UDP, ICMP i ARP/RARP, per mantenir canals de comunicació amb cadascun dels dispositius administrats de la xarxa.

El protocol SNMP és el protocol primari utilitzat en les comunicacions NNM, també utilitza protocols de la família ARPA, Berkeley i NFS per funcions com transferència de fitxers, e-mail, o remote logon. NNM utilitza SNMP per comunicar-se amb altres protocols com TCP/IP o UDP.

El model d'administració de xarxa consisteix en una estació d'administració de xarxa, administrant nodes amb agents, i el protocol SNMP com protocol d'administració de xarxa.



Funcionament NNM.

El *manager* és una aplicació que executa operacions de monitorització d'administració de xarxa i controla sistemes agents. La implantació d'aquestes operacions d'administració de xarxa són cridades pel manager.

Un *agent SNMP*, resident en un node administrat, és una aplicació que actua en nom d'un *objecte* que realitza operacions de peticions SNMP pel manager.

Un *objecte* és qualsevol recurs que pot ser administrat (un host, un servidor, un commutador, un encaminador, una aplicació o una base dades).

Un *manager* i un *agent* poden existir en un mateix sistema. El *manager* i l'*agent* és comuniquen utilitzant SNMP. El protocol SNMP permet les activitats següents:

- Un *manager* pot recuperar informació d'administració des d'un *agent* mitjançant l'operació get.
- Un *manager* pot canviar informació d'administració en l'*agent* del sistema (operació set).
- Un *agent* pot enviar informació al *manager* sense una petició explícita des del *manager* (trap o notificació).

4.2. Descobriment inicial de la xarxa

El primer pas abans de configurar NNM és instal·lar el programari i permetre executar un descobriment inicial.

NNM descobreix automàticament tots dels dispositius de la xarxa i la connectivitat entre dispositius. Les bases de dades d'objectes i de topologia emmagatzemen la informació descoberta. NNM utilitza aquesta informació per realitzar el mapa principal i establir el sistema d'events i d'alarmes. Després de finalitzar el descobriment inicial, ja podem utilitzar el mapa principal per detectar problemes en la nostra xarxa.

En el nostre cas, com que la nostra xarxa és exclusivament un entorn IP, per tant només ens cal indicar-li a NNM els nostres rangs d'adreçament IP (adreça IP i màscara de subxarxa) dels dispositius de la nostra xarxa que volem administrar. Si volem excloure una sèrie de dispositius que no volguéssim administrar aplicariem el filtre adient.

A partir del mapa principal obtingut del descobriment inicial, ja podem deduir problemes de configuració de la nostra xarxa, com agents SNMP que no es comuniquen correctament, màscares de subxarxa incorrectes, noms de comunitat SNMP equivocats, i connexions inesperades de segments de xarxa dels quals no som propietaris. El mapa és la representació visual entre NNM i els dispositius de la xarxa, per això és força important repassar totes les connexions, per assegurar-nos que NNM ens proporciona dades, events i alarmes de tots els segments, dispositius i nodes de la xarxa.

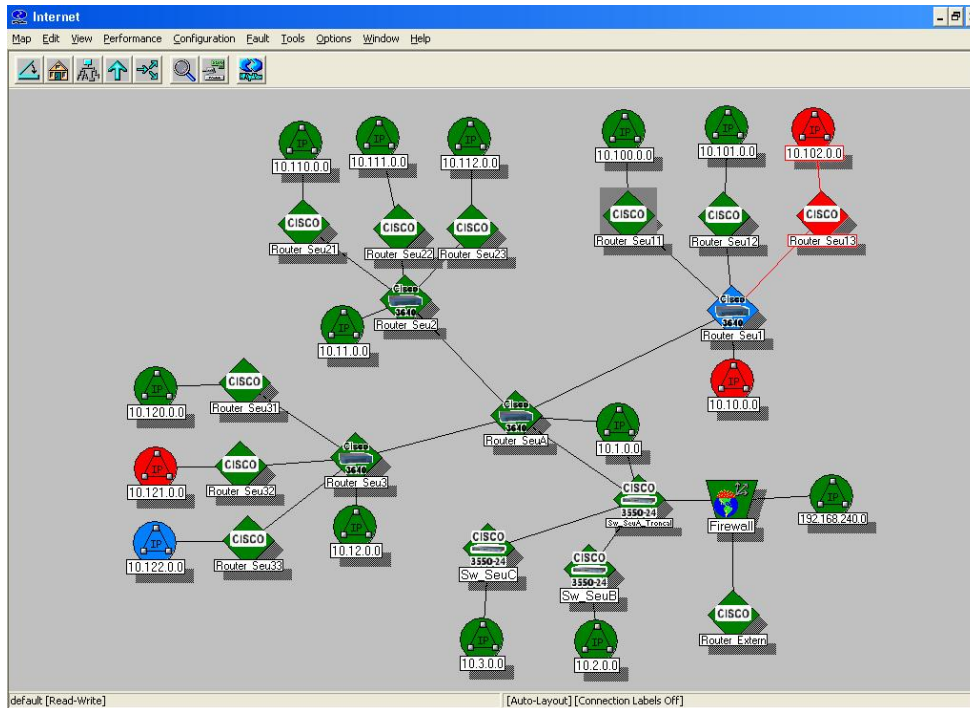
4.2.1. Funcionament del descobriment inicial

Un cop instal·lat NNM, en primer lloc s'arrenquen els serveis de monitorització de xarxa, que descobreix el dispositius de xarxa enviant un *ping ICMP* a totes les adreces de la nostra xarxa. Quan identifica un dispositiu l'afegeix a la taula ARP i li envia una petició *snmpwalk* per obtenir tota la informació possible d'aquest dispositiu.

Quan es descobreix un enllaç sèrie WAN, NNM comprova la taula d'encaminament de l'encaminador per saber com continuar amb el descobriment. En la primera fase del descobriment la freqüència del *testeig* és alta, la qual cosa comporta un elevat tràfic, després aquesta freqüència disminueix tal com es descobreixen nous dispositius.

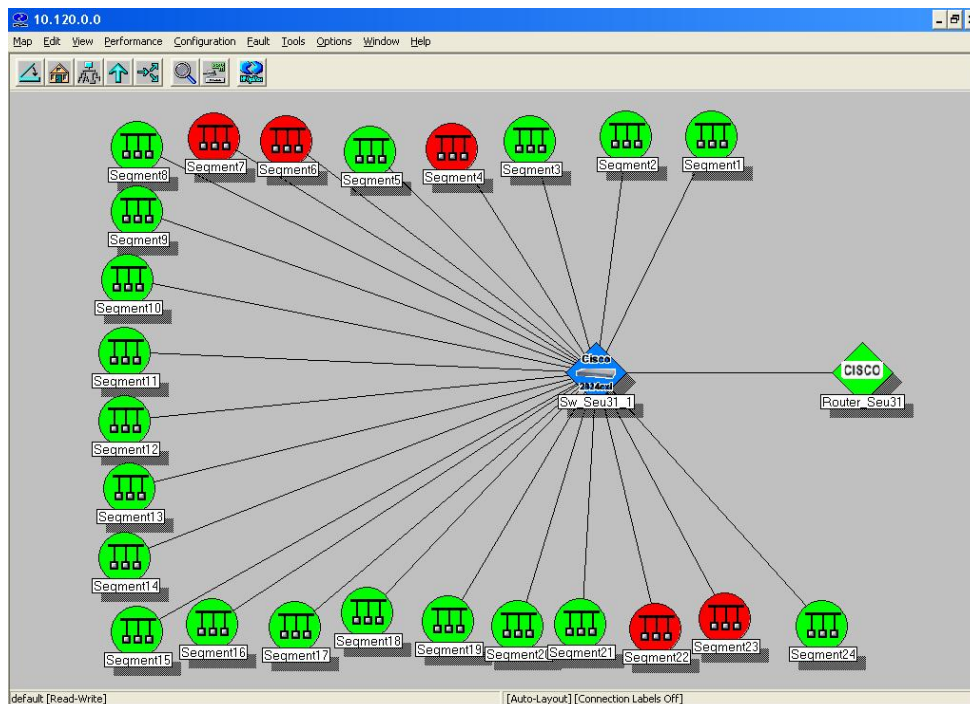
NNM realitza el descobriment dels objectes i els situa en els següents submapes del mapa per defecte:

- *Submapa del nivell de Internet: xarxes IP, gateways, encaminadors i estacions més d'una adreça IP. En el nostre cas obtenim el següent submapa a partir del descobriment inicial de la xarxa:*



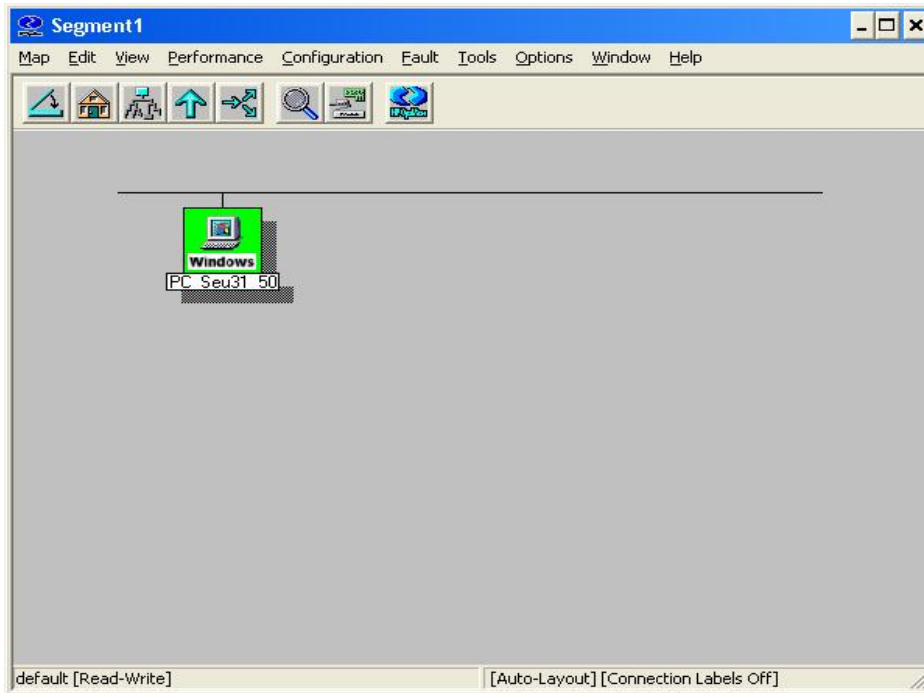
Descobriment inicial de la xarxa - Submapa del nivell Internet.

- *Submapes del nivell de xarxa: segments Ethernet; gateways, encaminadors, commutadors, concentradors i ponts.*



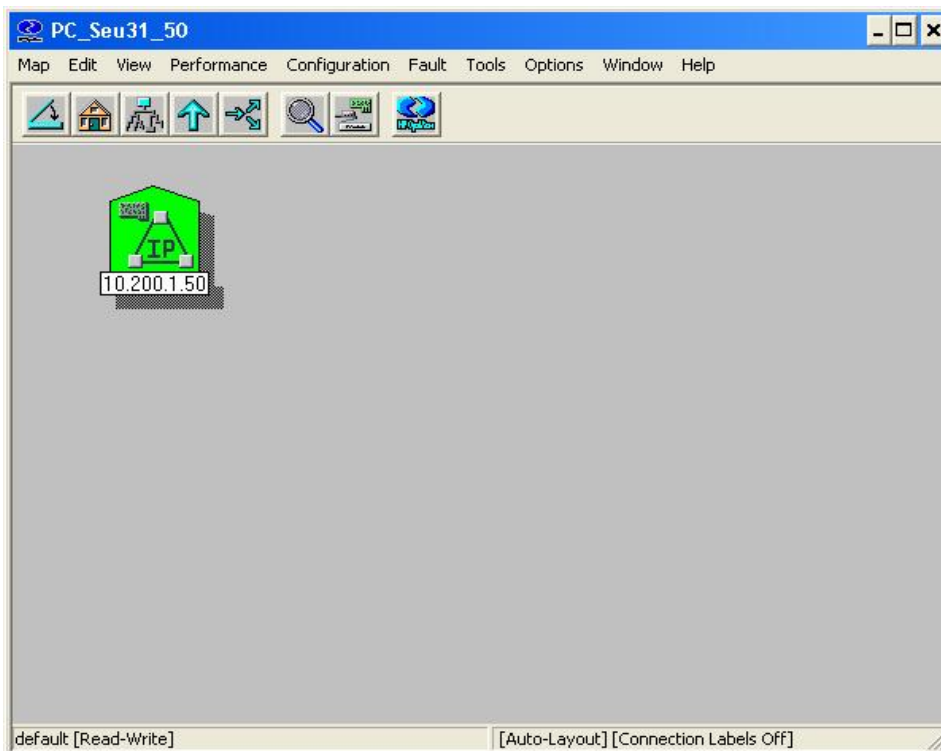
Submapa del nivell de xarxa de la Seu 31.

- *Submapes del nivell de segment:* estacions de treball i servidors, encaminadors, commutadors, concentradors i ponts. En una xarxa commutada cada segment està format per un únic dispositiu.



Submapa de nivell de segment.

- *Submapes del nivell de node:* targetes adaptadores de xarxa.



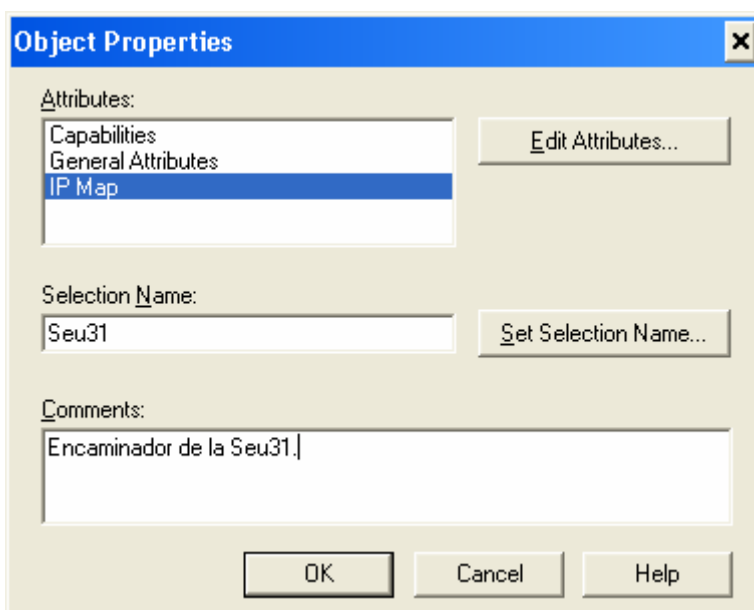
Submapa de nivell de node.

Cada dispositiu descobert i identificat es representat pel seu símbol identificatiu, si NNM no pot relacionar el camp *sysObjectID* amb un símbol específic, aleshores li assigna un símbol genèric.

A partir de qualsevol dels diferents mapes, podem accedir als serveis d'informació *IP Map*, que descriu els dispositius de xarxa i dels sistemes i les configuracions. La informació proporcionada a partir de les propietats de l'*objecte* ens pot ajudar a determinar si els dispositius estan presents i integrats en el mapa inicial.

Les propietats dels objectes que administrem mitjançant NNM s'emmagatzemen i s'actualitza a través de l'últim cicle de testeig de NNM en la base de dades d'objectes, podem accedir a elles seleccionant l'objecte i clicant el botó dret de ratolí:

- La descripció d'un *Objecte Internet* consta del següents camps:
 - El nombre de xarxes de la Internet.
 - El nombre de segments de la Internet.
 - El nombre de nodes continguts en la Internet.
 - El nombre d'interfícies contingudes en la Internet.
 - El nombre de gateways/encaminadors de la Internet.
 - Qualsevol estat o missatges d'error poden aparèixer en el camp Messages.



Pantalla de propietats d'un objecte.

- La descripció d'un *Objecte Segment* consta del següents camps :
 - L'estat del segment.
 - El nombre de nodes del segment.
 - Qualsevol estat o missatges d'error poden aparèixer en el camp Messages.

- La descripció d'un *Objecte Node* consta del següents camps:
 - El nom de host que ha estat assignat quan el node va ser descobert inicialment.
 - L'estat del node.
 - La informació relativa a l'estat de cada interfície instal·lada en el node.
 - La descripció i la localització del sistema retornada per l'agent SNMP.
 - L'ID del objecte del node.
 - Qualsevol estat o missatges d'error poden aparèixer en el camp Messages.

- La descripció d'un *Objecte Interfície* consta del següents camps:
 - L'adreça de la interfície.
 - La màscara de subxarxa.
 - La seva adreça física (adreça MAC).
 - El tipus d'interfície.
 - L'estat.
 - Qualsevol estat o missatges d'error poden aparèixer en el camp Messages.

Podem utilitzar l'opció *Edit:Find* per buscar objectes amb característiques comuns. Per exemple:

- Buscar objectes en un mapa determinat o en snapshot obert a partir del valor d'un atribut específic.
- Crear una llista d'objectes seleccionats amb una característica particular, com podria ser: *crear una llista de tots els encaminadors*.
- Crear un submapa amb els objectes seleccionats a partir d'una cerca.

Realitzarem cerques a partir del següents criteris:

- *Selection Name*: selecciona objectes a partir del nom o si forma part del seu nom.
- *Attribute*: cerca objectes a partir dels atributs d'un objecte, com per exemple *isRouter*.
- *Comments*: busca en tots els objectes aquell que tenen un comentari específic o una porció del comentari.
- *Symbol Status*: recerca objectes que estan representats pels símbol en un mateix estat. Cada símbol trobat es llista separatament.
- *Symbol Type*: selecciona els objectes representats per un mateix símbol (classe o subclasse).
- *Label*: cerca objectes que contenen un cadena de caràcters en un comentari afegit per nosaltres.

4.3. Fonaments per la creació de mapes

4.3.1. Mapes

Un mapa és un conjunt d'objectes relacionats, símbols, i submapes representats en un gràfic i amb una presentació jeràrquica de la nostra xarxa i sistemes. Podem crear múltiples mapes, però només un pot estar obert en cada sessió de NNM.

No podem veure directament un mapa, sempre visualitzem submapes que formen part del mapa. En canvi, si que podem visualitzar múltiples submapes a la vegada. El submapes tenen una típica organització jeràrquica que incrementa el grau de detall a cada nivell.

Mapes diferents poden ser utilitzats per definir diferents àrees d'administració, o per presentacions diferents de la mateixa àrea d'administració. També podem personalitzar mapes per les necessitats dels diferents administradors. Mapes diferents poden visualitzar informació d'un mateix objecte perquè els mapes obtenen la seva informació de la mateixa font, la base de dades d'objectes. NNM pot generar nous mapes, esborrar mapes, i crear un mapa des d'on seleccionar un dels mapes existents.

Quan arrenquem NNM, automàticament obre un mapa, que pot ser el mapa per defecte o un mapa especificat per nosaltres. Un mapa es pot obrir des de diverses sessions de NNM però només el primer que l'obre té accés de lectura i escriptura, la resta només tenen accés de lectura.

4.3.2. Submapes

Un submapa és una vista particular de l'entorn de xarxa, consistent en símbols relacionat agrupats en una pantalla. Cada submapa ofereix una perspectiva diferent d'un mapa. NNM crea un submapa principal per cada mapa. L'arrel del submapa proporcionada és estàndard, i és el nivell més alt de cada mapa. A partir d'aquest submapa es creen la resta de submapes organitzats de forma jeràrquica. També podem crear submapes independents que no estan associats amb cap jerarquia.

A partir d'una llista de submapes d'un mapa o obrint un mapa i seleccionant els submapes, podem obrir i visualitzar diversos submapes alhora del mateix mapa.

4.3.3. Submapa principal

El submapa principal és el submapa de més alt nivell del mapa. El primer cop que obrim un mapa, el submapa principal és el submapa inicial per defecte. El submapa principal és un submapa creat pel sistema, on estan situats els objectes principals per diverses aplicacions. El submapa principal no es pot esborrar. Es pot retornar fàcilment al submapa principal pressionant el botó *Home* des de la barra d'eines.

4.3.4. Submapa inicial

El submapa inicial és el primer submapa que apareix quan obrim un mapa. Podem assignar qualsevol submapa d'un mapa com a submapa inicial.

4.3.5. Gràfics en segon pla

Un gràfic en segon pla pot ser visualitzat en segon pla des d'una finestra d'un submapa. El gràfic en segon pla pot ser diferent per cada submapa.

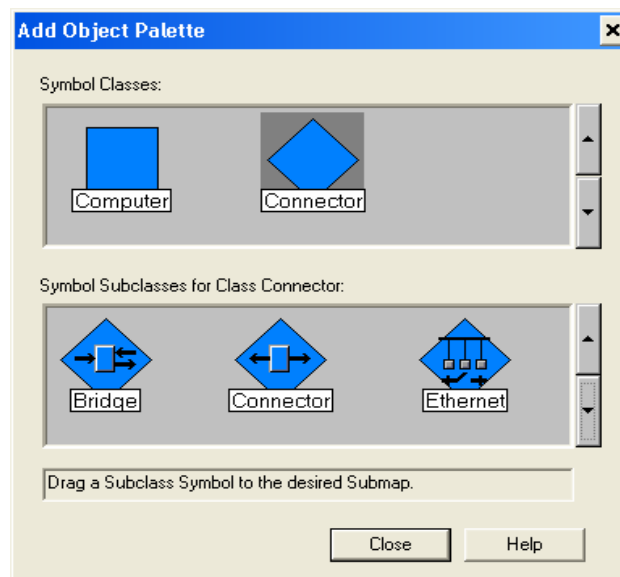
4.3.6. Objectes

Un objecte representa una entitat particular o un recurs en un entorn de xarxa. Un objecte pot ser un component físic d'un equipament de xarxa, els components d'un node de la xarxa, o parts de la xarxa mateixa. L'objecte representa el recurs per representar les seves característiques.

4.3.7. Símbols

Un símbol es la representació gràfica d'un objecte. Un objecte simple pot estar representat per diversos símbols, és a dir, poden existir múltiples símbols per un mateix objecte en un submapa, diversos submapes d'un mapa o un submapa en diferents mapes. Un símbol mai pot representar més que un objecte en el mateix temps. Altres funcions dels símbols són:

- Els símbols permeten navegar a través dels submapes del mapa. Molts símbols són explorables –quan fem un doble-click en un símbol explorable, una nova finestra amb un submapa s'obre.
- Alguns símbols executen accions. Fent doble-click en un símbol executable, podem executar una acció predefinida.
- Els símbols es poden configurar per reflectir l'estat del objecte que representen.

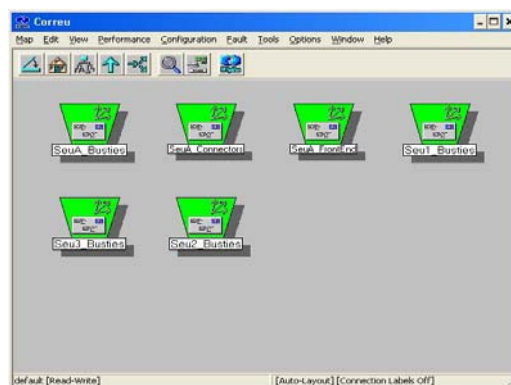
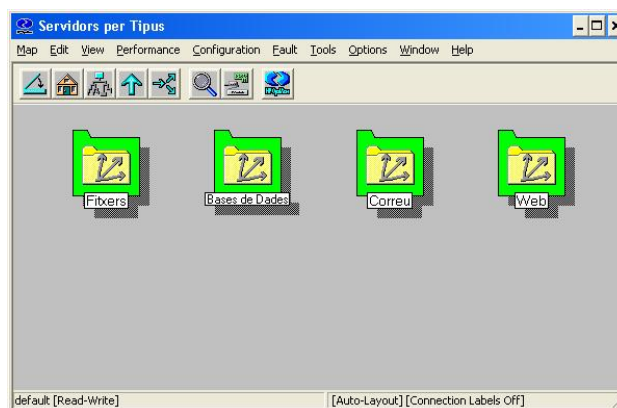
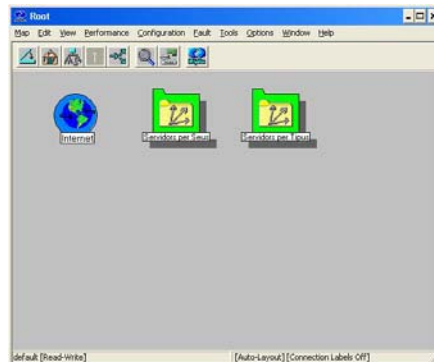


Alguns dels símbols disponibles en NNM.

4.3.8. Mapes personalitzats

Després del descobriment inicial obtenim el mapa per defecte, la finalitat del qual es tenir una vista completa de la nostra xarxa quan executem NNM. Ara realitzarem còpies del mapa per defecte per personalitzar aquestes còpies segons les nostres necessitats específiques.

Podem crear diversos mapes i personalitzar-los amb la informació dels objectes que visualitzem en cada mapa. Tractarem de distribuir els objectes per obtenir vistes organitzades dels recursos. Diversos mapes poden visualitzar informació del mateix objecte perquè tots els mapes obtenen la informació de la mateixa font, la base de dades d'objectes.



Exemple de jerarquia de mapes personalitzats.

4.4. Control dels objectes

NNM utilitza els colors per indicar l'estat dels objectes de la xarxa. Quan l'estat d'un dispositiu és *critical*, aquest estat es propaga als objectes que hi ha per sota dintre del mapa jeràrquic de xarxa.

Existeixen dues categories de condicions d'estat: l'administratiu i l'operacional. Les normes que regeixen els esquemes de propagació de l'estat són diferents depenent de la categoria a la que pertanyin. Les condicions d'estat administratiu són ignorades pels esquemes de propagació, això significa que des d'un submapa fill no es transfereix la informació d'estat al símbol pare. En canvi, les condicions d'estat operacional indiquen problemes que ha de ser propagats mitjançant la utilització dels esquemes de propagació de l'estat.

NNM reconeix deu condicions d'estat, que veurem en la següent taula:

Categoria	Condicció d'estat	Significat de l'estat
Administratiu	Unmanaged	Els administradors poden establir aquest valor si l'objecte no pot ser monitoritzat o si els seu estat pot ser ignorat.
Administratiu	Testing	Una aplicació pot establir aquest estat quan l'objecte s'ha de sotmetre a un diagnòstic o per procediments de manteniment.
Administratiu	Restricted	Una aplicació pot establir aquest estat quan un objecte està funcionant correctament, però no està disponible per a tots els administradors.
Administratiu	Disable	Una aplicació estableix aquest estat quan l'objecte està inactiu.
Operacional	Unknown	Una aplicació estableix aquest estat quan l'estat de l'objecte no pot determinar-se.
Operacional	Normal	Una aplicació estableix aquest estat quan l'objecte està en un estat operacional normal.
Operacional	Warning	Una aplicació estableix aquest estat quan un objecte pot patir un potencial problema.
Operacional	Minor/Marginal	Una aplicació estableix aquest estat quan un objecte té un petit problema, i el dispositiu pot funcionar normalment.
Operacional	Major	Una aplicació estableix aquest estat quan un objecte pateix un problema seriós, el dispositiu probablement no funcionarà correctament molt temps més.
Operacional	Critical	Una aplicació estableix aquest estat quan un objecte deixa de funcionar.

L'estat s'obté de tres possibles fonts. Aquesta propietat és utilitzada principalment per aplicacions que poden establir l'estat del símbol específic. En general, Hewlett-Packard recomana no canviar la font de l'estat d'un símbol. La font de l'estat d'un símbol s'estableix automàticament depenent de l'aplicació que administra l'objecte. Les tres fonts d'estat són:

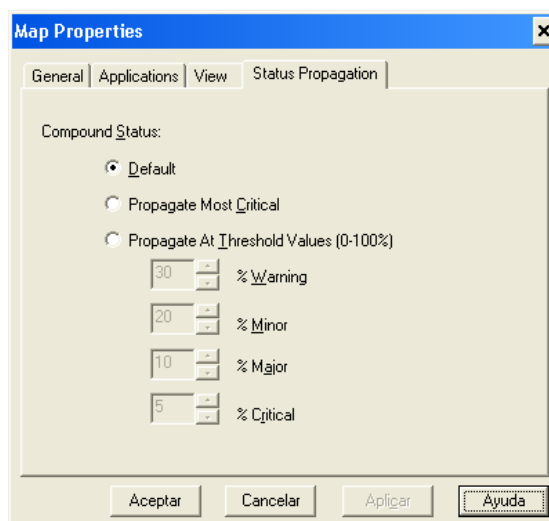
- Font d'estat símbol: aquesta font d'estat es utilitzada per aplicacions que poden voler establir un estat a un símbol d'un objecte. Així altres aplicacions podran establir un estat diferent a altres símbols del mateix objecte.
- Font d'estat objecte: aquesta font d'estat es utilitzada per aplicacions que volen establir i visualitzar el mateix estat en tots els símbols d'un mateix objecte.
- Font d'estat composta: NNM determina un estat d'un símbol a partir d'un conjunt de regles. L'estat compost determina com propagar l'estat des de símbols en submapes fills a símbols en submapes pares.

4.4.1 Estats compostos

NNM utilitza estats compostos per propagar l'estat d'un símbol d'un submapa fill als submapes pares, alertant-nos d'aquesta forma del problema. La propagació només és produïda en objectes que són de la categoria de condició d'estat operacional.

Des de la perspectiva d'un esquema d'estat compost, un símbol pot ser:

- **Unknown:** un símbol en aquest estat encara no ha estat determinat per una aplicació.
- **Normal:** un símbol que està funcionant correctament quan ha contactat amb una aplicació.
- **Abnormal:** un símbol amb problemes potencials o efectius que es troba en un d'aquestes quatre estats anormals: warning, minor/marginal, major o critical.



Pantalla de configuració dels valors de propagació de l'estat.

Els valors de propagació de l'estat són:

- **Default:** seleccionant l'esquema de propagació per defecte NNM propaga l'estat d'acord amb els algorismes de la següent taula:

Condicció dels símbols en el submapa fill	Estat dels símbols en l'objecte pare
No hi ha símbols normal ni <i>abnormal</i> .	<i>Unknown</i>
Tots els símbols són <i>normals</i> .	<i>Normal</i>
Un símbol és <i>abnormal</i> , i la resta són <i>normals</i> .	<i>Warning</i>
Més d'un símbol és <i>abnormal</i> i més d'un de la resta són <i>normals</i> .	<i>Minor/Marginal</i>
Un símbol és <i>normal</i> i la resta són <i>abnormal</i> .	<i>Major</i>
Tots els símbols són <i>abnormal</i> .	<i>Critical</i>

- **Propagate Most Critical:** l'estat del símbol més crític del submapa fill és el que es propaga al l'objecte pare.
- **Propagate At Threshold Value(0-100%):** podem seleccionar el valor del umbral que determina quan NNM propaga un estat.

4.5. Sistema d'events

Molts serveis dintre de NNM i altres programes compatibles amb OpenView, recullen informació i generen events que són enviats a NNM. Els events també poden ser enviats des d'agents dels nodes administrats, o des d'aplicacions d'administració residents en les estacions administrades o en nodes específics de xarxa. Els events SNMP no sol·licitats o notificacions s'anomenen traps. NNM proporciona una localització centralitzada, el Alarm Browser, on els events i els traps són visibles en el seu conjunt. Els events i traps que considerem important podrem visualitzar-los com a alarmes, a les quals podrem associar-li una acció a efectuar quan es produeixin.

4.5.1. Alarm Browser

L'Alarm Browser és una eina útil per les següents operacions:

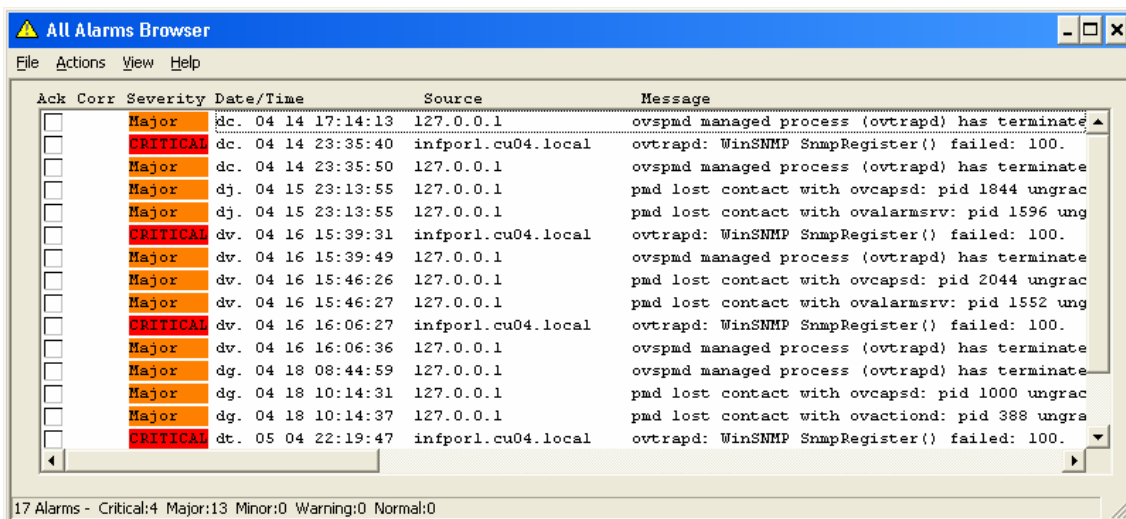
- Visualitzar informació útil sobre les alarmes.
- Ordenar les alarmes per categories.
- Reconèixer que el problema causant d'una alarma ha estat tractat.
- Filtrar dinàmicament la llista d'alarmes per diverses condicions, i així poder disposar d'informació més útil.
- Esborrar alarmes de la llista després de haver estat resolta.
- Especificar accions addicionals que poden ser executades al produir-se una alarma.

4.5.2. Categoria d'alarmes

NNM ordena les alarmes per categories. La finestra d'*Alarm Categories* conté botons que corresponen a cadascuna de les categories d'alarmes. Pitjant un d'aquests botons podrem visualitzar totes les alarmes d'una mateixa categoria.

El color dels botons indica quin tipus d'alarmes s'han rebut en cada categoria. El color del botó és el de l'alarma més greu en la categoria, o sense color si no existeixen alarmes. Per defecte, la severitat de les alarmes són indicades pels següents colors:

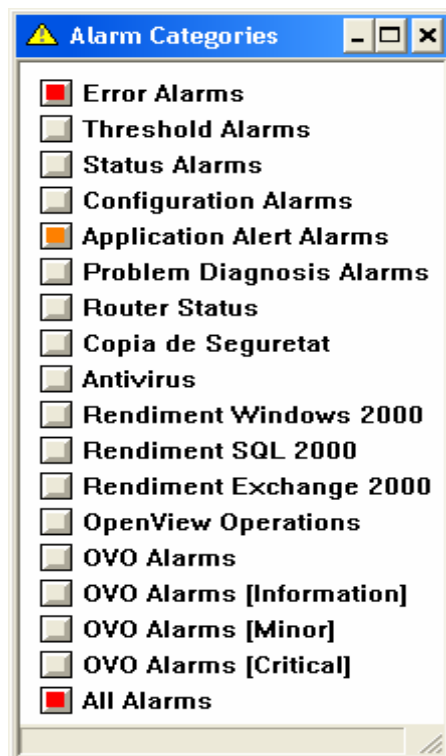
Categoria	Color
Normal	Verd
Warning	Blau
Minor	Groc
Major	Taronja
Critical	Vermell
Sense alarmes	Sense color



Alarmes categoritzades.

4.5.3. Configuració d'alarmes

Les categories de les alarmes les hem personalitzat atenen els possibles perfils dels administradors de xarxes i sistemes. A continuació es descriuen les alarmes que s'enviaran cap a cadascuna d'aquestes categories.



Categoria d'alarmes de l'Alarm Browser.

- *Error Alarms*: missatges d'error rebuts dels equips administrats. Normalment, es corresponen a traps que no s'han pogut identificar a cap MIB concreta.
- *Threshold Alarms*: avisos que s'envien quan s'activa qualsevol de les condicions d'alerta als paràmetres que es controlen de forma periòdica.
- *Status Alarms*: s'activen quan es detecta qualsevol canvi en l'estat dels equips de la xarxa, per exemple quan es tanca una estació de treball. Donada la poca importància d'aquests events, aquests missatges els filtrarem.
- *Configuration Alarms*: mostren errors de configuració en els dispositius de xarxa.
- *Application Alert Alarms*: alarmes que afecten al sistema HP OpenView o a qualsevol dels seus serveis o processos.
- *Router Status*: els traps generats pels encaminadors quan es produeix una situació anòmla s'envien a aquest apartat. A aquest grup pertanyen els traps de categoria genèrics, com ara *LinkDown*, *LinkUp ColdStart*...
- *Copia de Seguretat*: els cluster i servidors disposen del sistema ArcServe per a fer les còpies de seguretat, i s'envia a l'estació central un informe indicant la correcta execució de la mateixa o el motiu del problema.
- *Antivirus*: a aquesta categoria s'envia qualsevol missatge relacionat amb el programari d'antivirus, tant la detecció d'un virus com la caiguda dels serveis propis de l'antivirus.

- *Rendiment Windows 2000*: alarmes de superació dels nivells establerts des de OpenView Operations. S'envia a aquesta categoria quan el paràmetre en qüestió correspon a comptadors genèrics de tots els servidors de Windows 2000.
- *Rendiment SQL*: alarmes de superació dels nivells establerts des del OpenView Operations. S'envia a aquesta categoria quan el paràmetre en qüestió correspon a comptadors concrets dels servidors SQL. S'enviaran també a aquesta categoria els indicadors de caiguda dels serveis de SQL.
- *Rendiment Exchange*: alarmes de superació dels nivells establerts des del OpenView Operations. S'envia a aquesta categoria quan el paràmetre en qüestió correspon a comptadors concrets dels servidors Exchange. S'enviaran també a aquesta categoria els indicadors de caiguda dels serveis d'Exchange.
- *Server Status*: les caigudes dels servidors seran reflectides en aquesta categoria. Per fer-ho s'han redireccionat els mateixos traps ja esmentats a la categoria *Router Status* però en cas que l'origen sigui una IP corresponent a un servidor.
- *OVO Alarms*: aquesta categoria recull totes les alarmes procedents d'OVO i que no hagin estat redireccionades a cap altre categoria. A la pràctica, només arribaran alarmes molt genèriques o esporàdiques que estan pendents de ser redireccionades.
- *OVO Alarms [Information]*: aquesta categoria recull totes les alarmes que s'envien des d'OVO amb indicatiu d'event tipus .1.3.6.1.4.2427.0.3. Aquest indicatiu és el aplica el propi OVO a les alarmes de tipus *Information* que recull dels visors d'events dels diferents servidors.
- *OVO Alarms [Minor]*: aquesta categoria recull totes les alarmes que s'envien des d'OVO amb indicatiu d'event tipus .1.3.6.1.4.2427.0.2. Aquest indicatiu és el aplica el propi OVO a les alarmes de tipus *Warning* que recull dels visors d'events dels diferents servidors.
- *OVO Alarms [Critical]*: aquesta categoria recull totes les alarmes que s'envien des d'OVO amb indicatiu d'event tipus .1.3.6.1.4.2427.0.1. Aquest indicatiu és el aplica el propi OVO a les alarmes de tipus *Error* que recull dels visors d'events dels diferents servidors.
- *All Alarms*: recull de totes les alarmes de les quals disposa el sistema, independentment de la seva categoria.

4.6. Sistema de correlació d'events

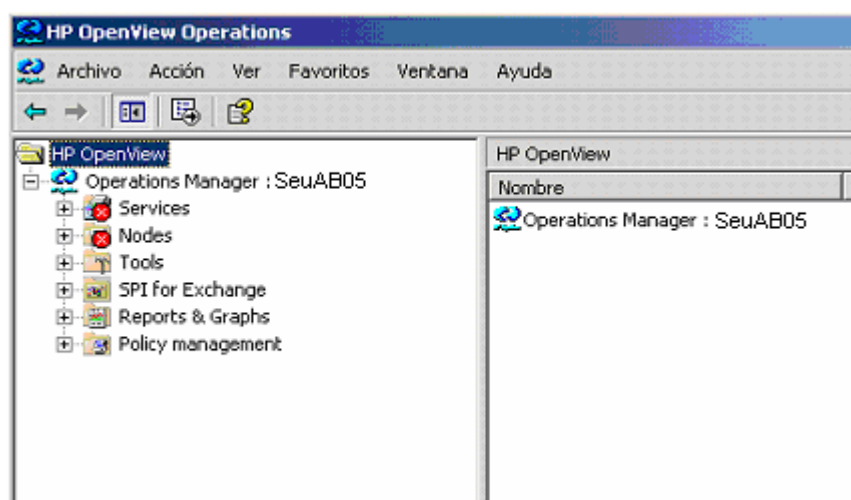
La correlació d'events modifica el flux dels events per reconeixement d'events relacionats i redundants, els quals són descartats o reemplaçats per uns pocs events significatius.

La correlació d'events disminueix dràsticament el nombre d'events en l'Alarm Browser, enlloc de rebre una multitud d'events generats per la caiguda d'un enllaç per exemple, només rebem les alarmes més significatives relacionades amb aquesta caiguda, la qual cosa en facilita la tasca d'identificar els problemes de xarxa.

5. OpenView Operations for Windows

5.1. Introducció

OpenView Operations for Windows constitueix la solució de programari distribuït client/servidor, dissenyat per proveir d'una consola per de la gestió d'events, aplicacions i serveis crítics dels servidors amb sistema operatiu Windows, dintre de la família d'eines de gestió de HP OpenView.



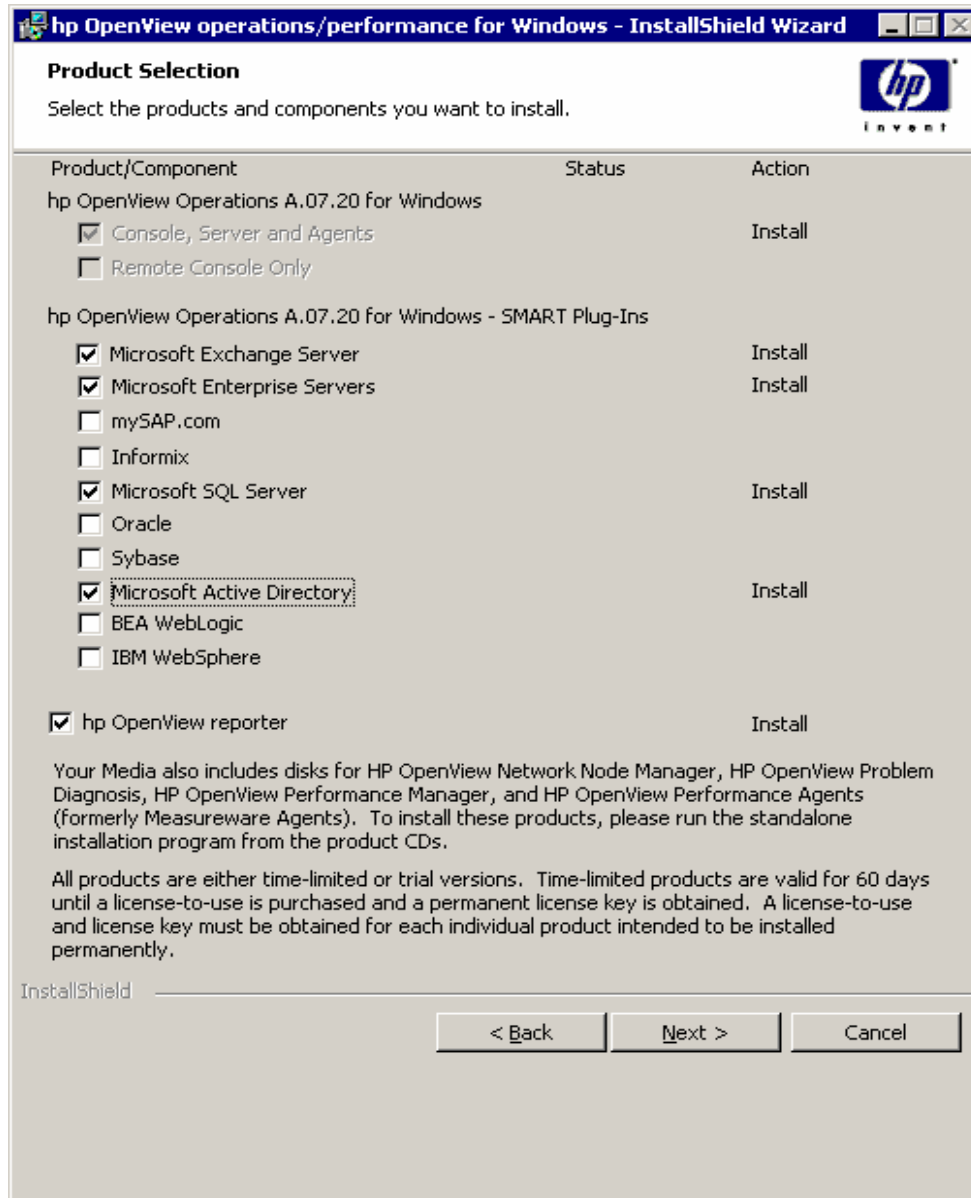
Consola d'OpenView Operations

Aquest programari monitoritza l'estat dels comptadors seleccionats dels servidors Windows, tan a temps real, per poder generar alertes de nivell d'ús, com per a poder generar informes periòdics amb les dades emmagatzemades.

Les funcionalitats bàsiques de l'OVO es basen en tres Smart Plug-ins (SPI), que formen part d'aquest producte. Aquestes funcionalitats són proporcionades com a part d'OpenView Operations for Windows, incloent sistemes i aplicacions bàsiques d'administració. De fet, aquestes polítiques predefinides les poden utilitzar sense modificacions per administrar fàcilment nodes sense especificacions especials, és a dir, a servidors sense serveis o aplicacions crítics on necessitem modificar les polítiques predefinides pels SPI's.

5.2. Smart Plug-ins

Durant la instal·lació de HP OpenView Operations disposem de l'opció de poder seleccionar els Smart Plug-Ins que necessitem, posteriorment podrem afegir-los o esborrar-los.



Pantalla de selecció de SPI durant la instal·lació d'OVO.

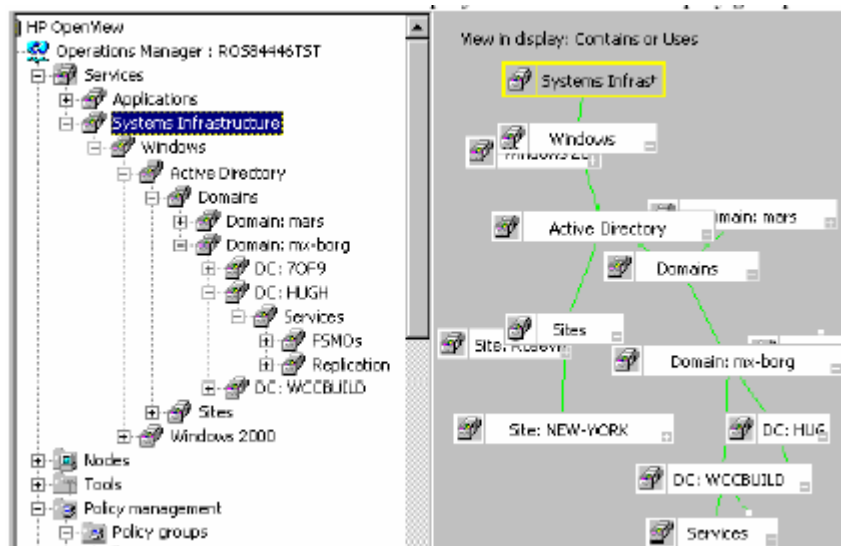
A continuació, realitzarem un resum dels Smart Plug-ins que necessitem instal·lar en el nostre servidor administratiu:

5.2.1. SPI for Windows Operating System

El Smart Plug-in for Windows Operating System (Windows OS SPI), proporciona polítiques preconfigurades i eines addicionals per administrar el funcionament dels nostres servidors Windows. També disposa d'un potent servei de descobriment automàtic per ajudar-nos a monitoritzar i administrar els nostres sistemes de fitxers i de processos distribuïts.

5.2.2. SPI for Active Directory

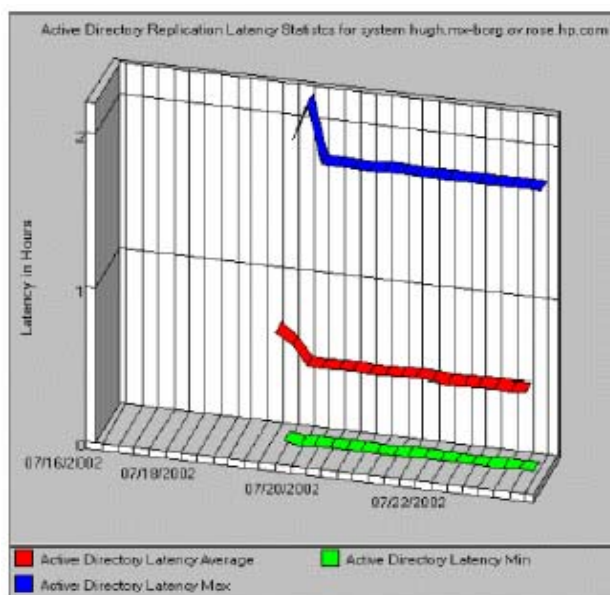
El Smart Plug-in for Active Directory afegeix utilitats, control de les rèpliques, capacitat de descobriment de les funcionalitats dels servidors (Primary Domain Controller, Domain Controller, Global Catalog, DNS, etc.) i monitorització i mapes relacionats amb l'Active Directory.



Mapa dels dominis i controladors de domini descoberts per OVO.

L'SPI for Active Directory ens manté contínuament informats dels següents punts:

- Si les dades de l'Active Directory són consistents en tots els controladors de domini.
- Si les rèpliques funcionen periòdicament i correctament.
- Si els sistemes són capaços de fer front altes càrregues puntuals.
- Si totes les funcionalitats principals funcionen.
- Si les CPU dels controladors de domini es troben col·lapsades.
- Si l'Active Directory té problemes de capacitat i errors suportables.
- Si els global catalog's de l'Active Directory es repliquen periòdicament.



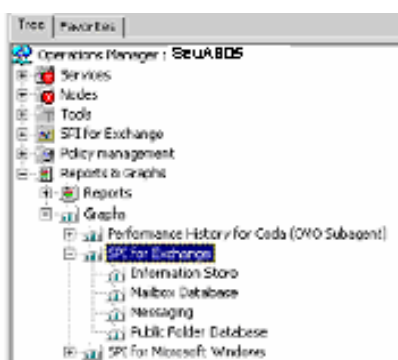
Gràfic d'estadístiques del temps de latència en la replicació de l'Active Directory.

5.2.3. SPI per servidors Web

OpenView Operations for Windows proporciona Smart Plug-ins per servidors Web Microsoft IIS, Microsoft Proxy Server, Microsoft Site Server, entre d'altres. L'administració es basa principalment en la monitorització dels Events Logs, dels serveis de Windows, dels processos de Windows i dels Performance Monitors de Windows.

5.2.4. SPI for Microsoft Exchange Server

El SPI per Microsoft Exchange Server 2000 són instal·lats, configurats i desplegats, per rebre missatges i alarmes, obtenir gràfiques de funcionament, incrementar la disponibilitat, l'administració i la planificació dels servidors Exchange.



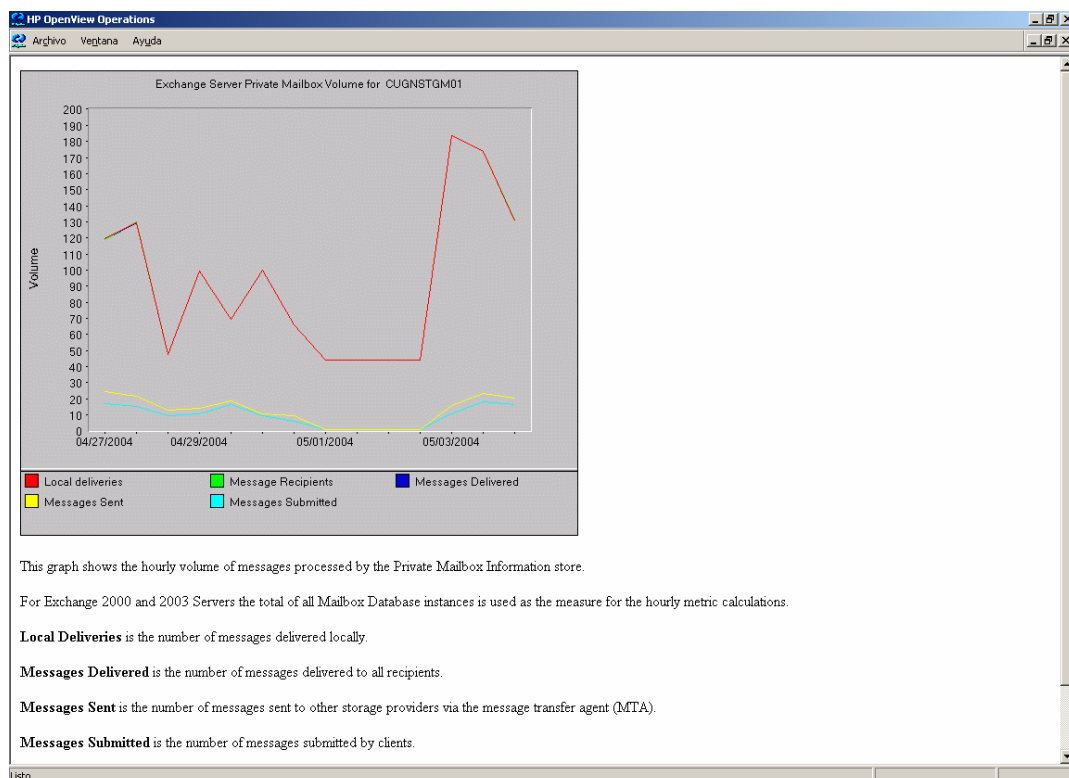
Gràfics disponibles llistats per tipus.

Name	Description
Internet Mail Queue	This graph shows the Exchange Server Internet Mail Service.
Internet Mail Volume	This graph shows Exchange Server Internet Mail Connector.
MTA Volume	This graph shows Exchange Server Message Transfer Agent.
Newsfeed Volume	This graph shows Exchange Server newsfeed volume.
Queues	This graph shows Exchange Server queue lengths.
SMTP Queues	This graph shows SMTP Server queues on the Exchange Server.
SMTP Volume	This graph shows SMTP Volume on the Exchange Server.

Gràfics disponibles de missaging

Les funcionalitats adicional d'aquest Smart Plug-in són:

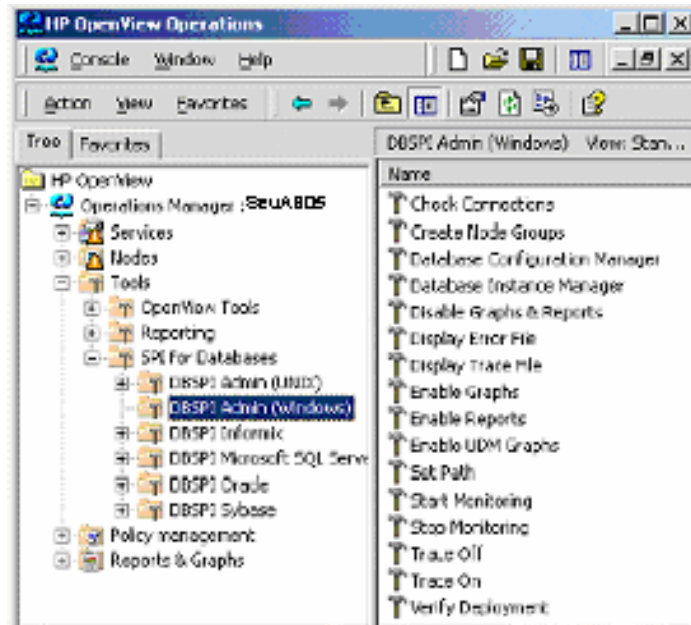
- Monitor de processos: monitoritza la quantitat de temps de CPU que consumeixen el processos d'Exchange 2000 Server.
- Monitor de processos inactius: monitoritza l'activitat dels principals processos d'Exchange 2000 Server.
- Monitor dels servei d'Exchange: monitoritza l'activitat dels principals serveis d'Exchange 2000 Server.
- Proporciona dades dels processos dels missatges de la Message Transfer Agent (MTA) i SMTP.
- Proporciona dades de les cues de treball de la MTA i de les cues SMTP.
- Proporciona estadístiques de l'entrega de la IS Public.
- Proporciona estadístiques de l'entrega de la IS Private.



Gràfic del Private Mailbox Information store d'un servidor Exchange 2000.

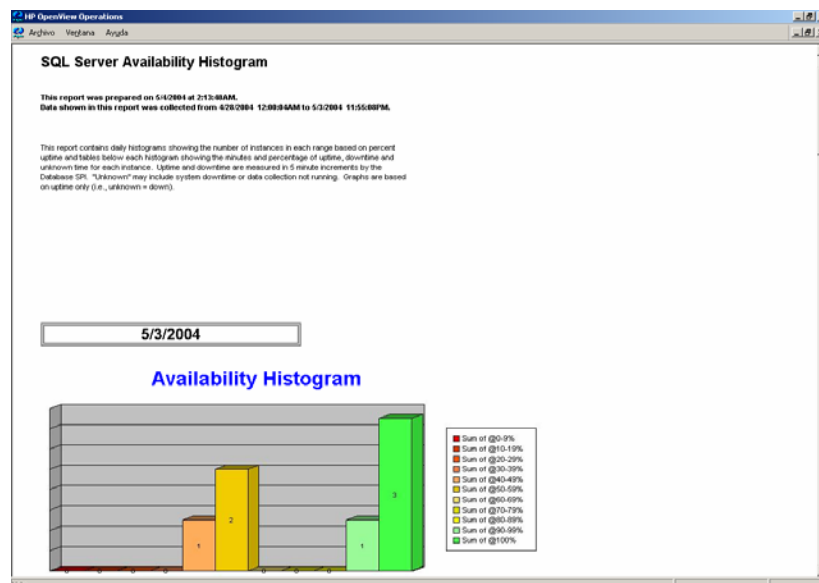
5.2.5. SPI for Microsoft SQL

El Smart Plug-in per Microsoft SQL ajuden a administrar els entorns SQL, per facilitar aquestes tasques inclouen:



Eines disponibles per administrar tot tipus de bases de dades.

- Més de 30 umbrals d'events predefinits i varis log file condicionals.
- Administració d'espai, problemes de concurrència i mètriques de càrrega de treball.
- Intercepció de més d'un centenar de missatge d'error com per exemple missatges de corrupció o missatge relacionats amb poc espai.



Gràfic de disponibilitat dels servidors SQL.

5.3. Integració amb altres productes de la família OpenView

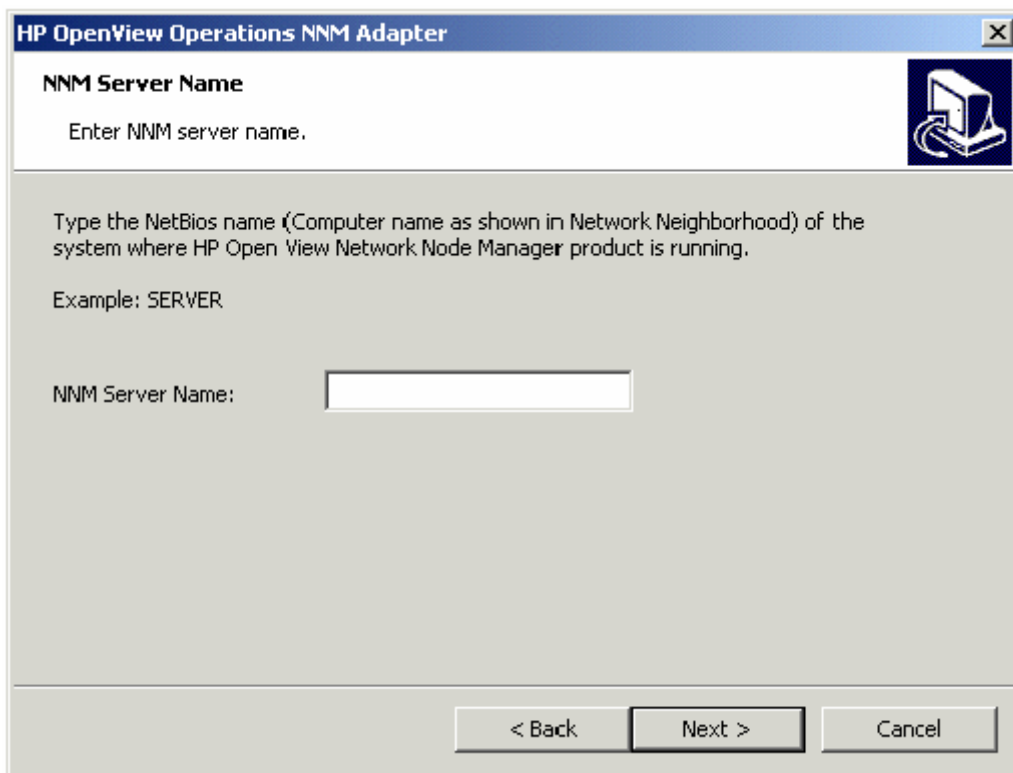
5.3.1. Reporter

Reporter és el producte que proporciona una administració flexible d'informes d'un entorn distribuït com el nostre. Els agents OVO converteixen automàticament les dades capturades en format Web, i les transformen al moment en informes de gran utilitat per l'anàlisi de l'entorn.

5.3.2. Network Node Manager

NNM proporciona un entorn per gestionar sistemes, que pot ser fàcilment adaptat a les nostres necessitats d'administració. NNM inclou la possibilitat de solucionar problemes abans d'arribar a estats crítics del nostre entorn, alhora que recull i proporciona informació clau de la nostra xarxa per evitar imprevistos.

El NNM Adapter és un component d'integració que permet visualitzar els nodes de NNM com un grup que pot ser vist de la mateixa que veiem la resta de nodes procedents d'OVO. Podem seleccionar-los i afegir-los com un grup d'OVO, per tal de definir polítiques basades en el tipus de node.



The image shows a Windows-style dialog box titled "HP OpenView Operations NNM Adapter". The dialog has a blue title bar with a close button (X) in the top right corner. Below the title bar, there is a section labeled "NNM Server Name" with a small icon of a computer monitor and mouse. The text "Enter NNM server name." is displayed. Below this, there is a larger text area containing the instruction: "Type the NetBios name (Computer name as shown in Network Neighborhood) of the system where HP Open View Network Node Manager product is running." followed by "Example: SERVER". At the bottom of this section, there is a label "NNM Server Name:" followed by an empty text input field. At the very bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Pantalla d'instal·lació del NNM Adapter de OpenView Operations.

La instal·lació del NNM Adapter afegeix aquestes funcionalitats a OVO:

- Afegeix el <NNMSERVER> (Servidor NNM) al grup de nodes *root*, si el servidor NNM no era un dels nodes administrats per OVO.
- Crea els serveis: NNM, NNM Adapter i Network Infrastructure.
- Crea el grup d'eines NNM Web Tools, que conté les eines NNM en format Web. Aquestes eines estan associades amb el grup de nodes NNM Managed Nodes. Tots els nodes que són descoberts com a nodes NNM són automàticament associats amb aquestes eines per pertànyer al grup NNM Managed Nodes. També crea el grup de polítiques NNM Policies que permeten que els missatges i els events puguin ser enviats a la vegada a OVO i a NNM.

5.4. Instal·lació d'OpenView Operations for Windows

5.4.1. Tasques prèvies

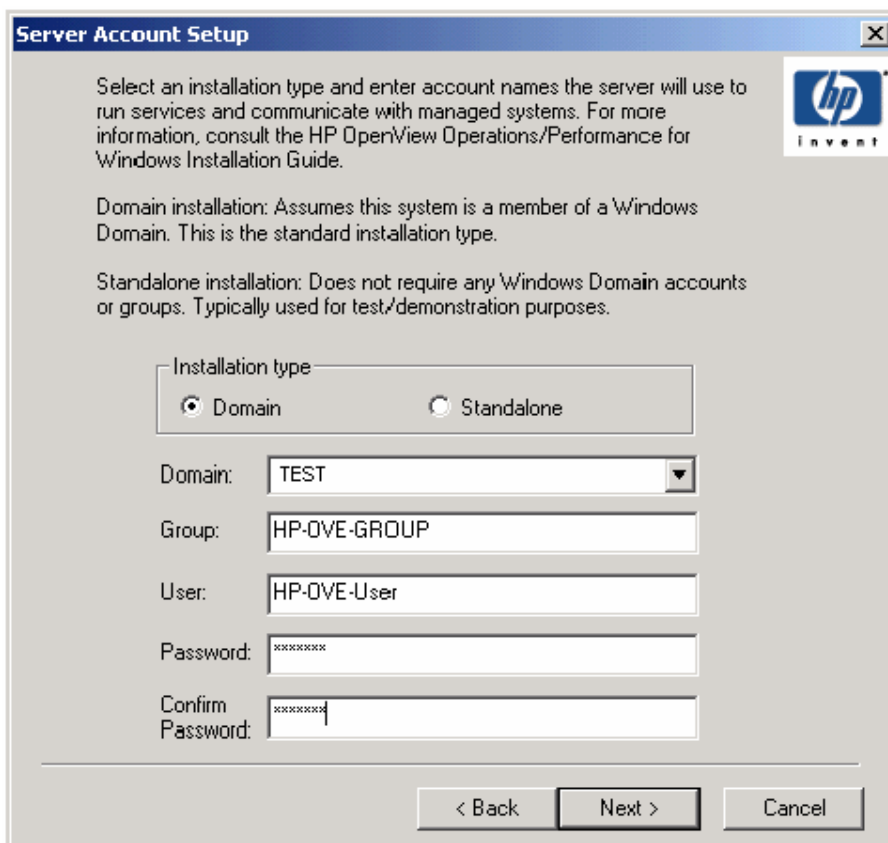
Abans d'instal·lar i utilitzar OVO, necessitem crear els següents grups i comptes d'usuari en el nostre Active Directory:

- El grup HP OV Enterprise Administrators: HP-OVE-ADMINS. Els usuaris d'aquest grup poden realitzar totes les tasques d'administració, com per exemple: afegir, administrar i configurar nodes, desenvolupar polítiques, crear i modificar polítiques i eines, crear automàticament comandes d'operador i inicialitzar-les.
- El grup HP OV Enterprise Operators: HP-OVE-OPERATORS. Els usuaris d'aquest grup poden realitzar totes les tasques excepte les tasques específiques abans llistades dels administradors. Són tasques dels operadors: contestar missatges, crear i usar filtres de missatges, i enviar missatges de resposta al visor de missatges. També poden executar les eines, visualitzar mapes de serveis i crear els gràfics de funcionament que estiguin autoritzats.
- El compte d'usuari HP-OVE-GROUP: aquest compte s'afegeix al grup d'administradors locals dels nodes Windows 2000/NT administrats, i permet l'administració automàtica del servidor quan instal·lem programari (agents o paquets) en aquest node.
- El compte d'usuari HP-OVE-USER: aquest compte és membre del grup HP-OVE-Group. L'administració dels processos del servidor s'executen en el context d'aquest compte d'usuari, això permet que aquests processos puguin accedir als nodes administrats configurats pel grup HP-OVE-Group.
- Els comptes d'usuari HP ITO i opc-op: quan un paquet d'agent OVO s'instal·la en un node, es creen aquests dos comptes d'usuari i es generen contrasenyes aleatòries. El compte HP ITO té privilegis administratius i s'afegeix automàticament al grup local Administrators quan es crea el compte. El compte opc-op, és un compte d'usuari del grup Domain Controllers, i un usuari local a

la resta de sistemes, que sempre està disponible després d'haver instal·lat el paquet d'agent OVO en el node administrat. Aquest compte és membre del grup Guest User i no té cap privilegi especial.

- El compte HP-TRC-Account: compte utilitzat per suportar el tracing.

Si hem de canviar les contrasenyes dels comptes d'usuari HP ITO o HP-TRC-Account hem de reconfigurar els serveis que utilitzen aquests comptes amb la nova contrasenya. Si necessitem canviar la contrasenya de l'usuari HP-OVE-User, hem d'utilitzar la comanda chgpass d'OVO, per canviar la contrasenya dels comptes d'usuari de Windows 2000/NT de tots els serveis afectats per aquest canvi.



Pantalla de configuració de grups i comptes d'usuari durant la instal·lació de OVO.

5.4.2. Requeriments de seguretat per utilitzar Openview Operations for Windows

Els administradors i operadors d'OVO han d'envoltar de mesures de seguretat les tasques de funcionament, així com la instal·lació del servidor OVO, afegint nodes per administrar, i utilitzant la consola administrativa, administrant el servidor o administrant nodes.

Quan instal·lem OVO, devem utilitzar un membre del grup local Administrators. Durant la instal·lació es crearan els grups HP-OVE-ADMINS i HP-OVE-OPERATORS. Els grups, comptes d'usuari i contrasenya que volem que utilitzin OVO han de ser validades per l'Active Directory.

Igualment, quan instal·lem una consola administrativa d'OVO necessitem ser membres del grup local Administrators. Per afegir un node administrat, també hem de ser administradors del servidor Windows 2000/NT o membres del grup HP-OVE-ADMINS.

Els administradors d'OpenView Operations for Windows, poden especificar els comptes d'usuari que poden executar una eina, d'acord amb els següents requeriments:

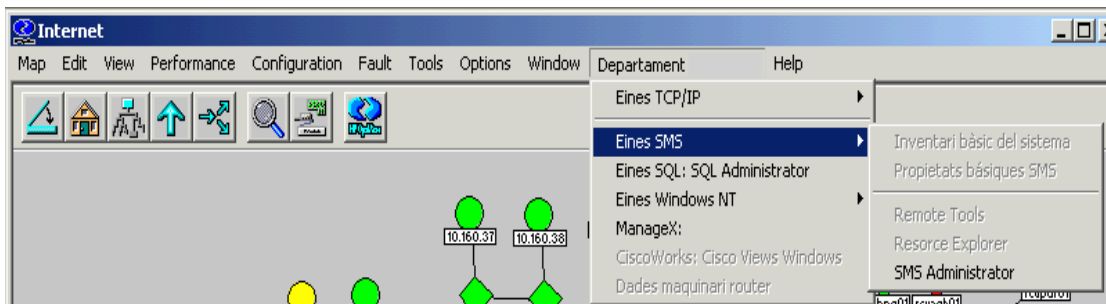
- Automàticament i executant comandes d'operador des del node administrat com a compte d'usuari HP ITO.
- Si la localització de l'eina és la consola administrativa d'OVO, no cal especificar cap usuari, l'eina s'executa amb els privilegis de l'usuari autenticat en la consola.
- Si substituïm l'usuari i deixem la contrasenya en blanc, això ens permet accedir a un mòdul de seguretat desenvolupat per OVO, que ens deixa validar un nou usuari amb permisos per executar una eina.

6. System Management Server

6.1. Introducció

La implantació de SMS s'engloba dins del projecte general de gestió de xarxes i sistemes de la nostra organització. En aquest projecte s'ha implantat una Site SMS, instal·lant el client SMS ens els servidors i en les estacions de treball per poder aprofitar les funcionalitats principals que aporta SMS, especialment el control remot per les estacions de treball, els inventaris de maquinari i de programari, i la distribució de programari.

També hem realitzat el desenvolupament necessari per tal d'integrar aquestes funcions pròpies de SMS per tal de poder utilitzar-les des de la consola general de Network Node Manager.



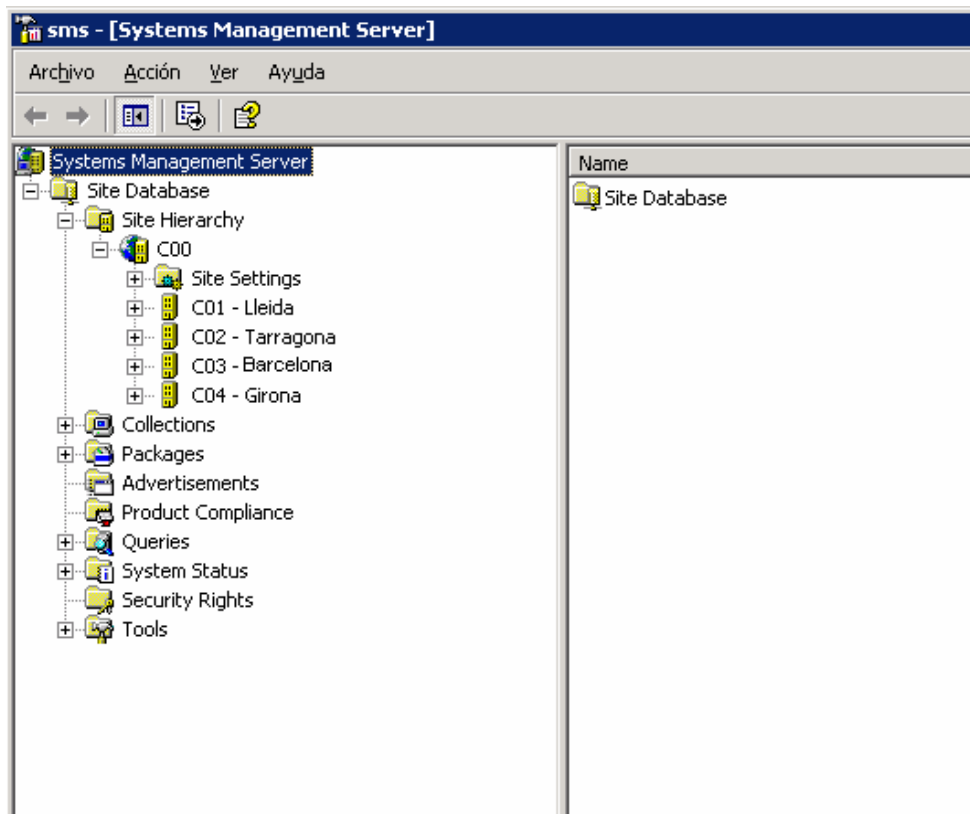
Integració de NNM amb SMS, mitjançant la introducció el menú d'opcions d'eines SMS.

6.2. Disseny i instal·lació de la Site SMS

6.2.1. Jerarquia de Sites SMS

El disseny de la jerarquia SMS consisteix en definir el nombre de sites necessàries i el seu tipus (primàries i secundàries), així com la necessitat de configurar servidors que realitzin funcions especials de suport al Site Server (Client Access Point, Distribution Point, Logon Point, Software Metering Server, etc.)

En aquesta instal·lació, donat el nombre de clients de la nostra organització, no es justifica la creació de cap site addicional al site principal. Així doncs, la jerarquia està formada per un únic Site Server integrat en el nostre Active Directory.



Jerarquia de sites de la nostra organització.

6.2.2. Instal·lació i configuració de SQL Server

Un element indispensable en una implantació de SMS és la disponibilitat d'un servidor SQL. Aquest requeriment es deu a que SMS emmagatzema tota la configuració del site i totes les dades que es recullen, en una base de dades de format SQL. És per això, que durant la instal·lació de SMS hem d'especificar el servidor SQL Server que desenvoluparà les funcions de servidor de base de dades SQL Server dins de la site, és a dir, el servidor que emmagatzemarà totes les dades que SMS gestiona.

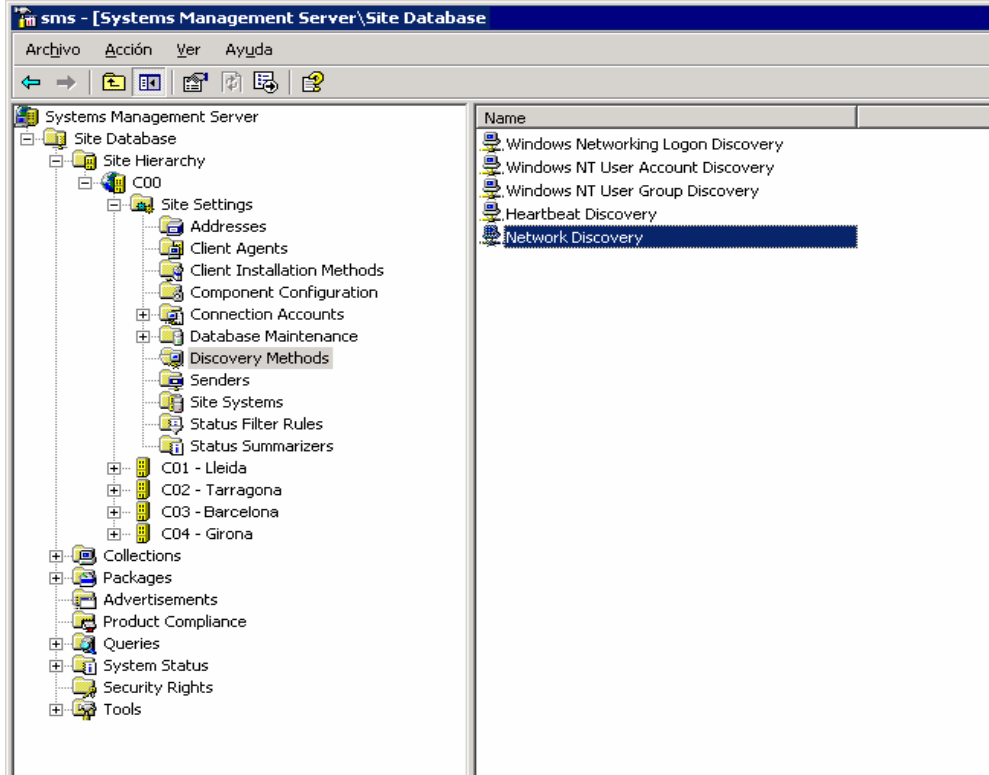
Per optimitzar el rendiment de la xarxa i dels sistemes, hem decidit instal·lar el servidor SQL Server en el mateix servidor SMS, així doncs, tots els processos que s'executen en la site SMS estan centralitzats en el mateix servidor, per això, ens cal un maquinari prou potent per complir el requeriments d'instal·lació d'aquests programaris.

6.2.3. Instal·lació i configuració del Site Server

Hem activat la instal·lació l'agent de Control Remot que descobreixi el SMS, a més a més, també hem activat els inventaris de maquinari i de programari per a totes les estacions de treball i servidors.

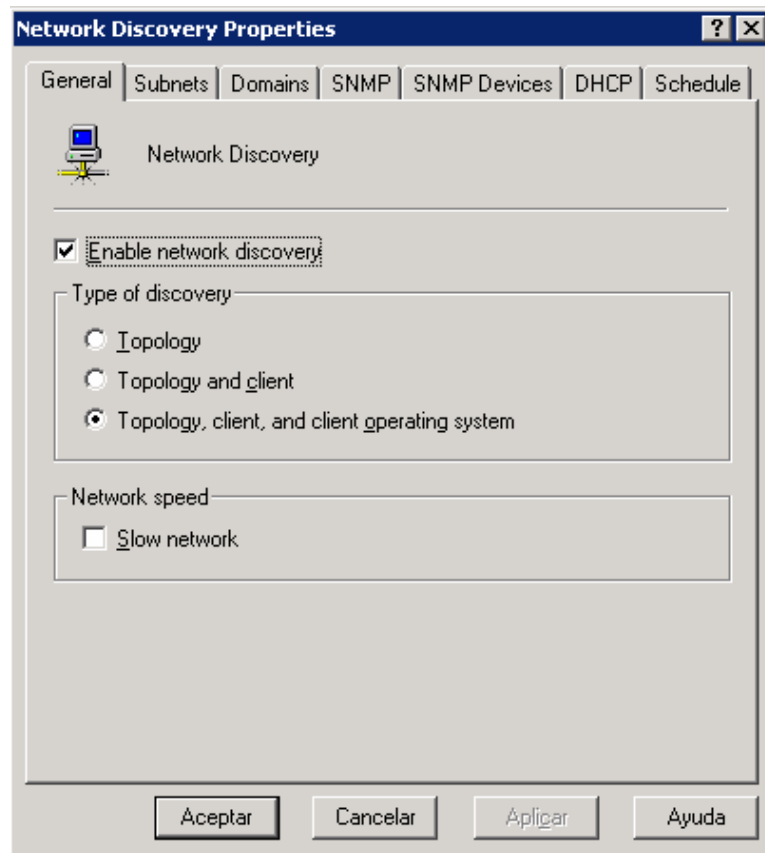
Per no col·lapsar la xarxa realitzarem una instal·lació dels agents del SMS progressiva, utilitzant els següents mètodes de descobriment i instal·lació de clients:

- *Network Discovery*: permet fer un descobriment selectiu dels equips, basant-se en domini d'Active Directory, subxarxes IP i comunitats SNMP. Per aquesta instal·lació hem seleccionat el descobriment d'equipaments segons la subxarxa IP a la que pertanyen. El descobriment s'ha anat fent de manera progressiva, afegint subxarxes a descobrir de forma paulatina durant diversos dies.
- *Remote Client Installation*: aquest mètode instal·la el client SMS en equips amb sistema operatiu. Aquest tipus d'instal·lació només es porta a terme si es compleixen els següents requisits:
 - L'equip ha estat prèviament descobert, és a dir, la seva subxarxa ha estat inclosa al Network Discovery.
 - La subxarxa de l'equip ha estat configurada com a Site Boundary, això vol dir que està a la llista de subxarxes gestionades per la site SMS.



Pantalla des d'on podem seleccionar els diferents valors de configuració de la site.

Un cop s'ha complert aquests requisits s'ha activat primer l'activació als controladors de domini, després a la resta de servidors i per últim a les estacions de treball.



Pantalla de propietats de Network Discovery.

6.2.4. Instal·lació i configuració de site systems addicionals.

En una site SMS, diferents sistemes poden assumir funcions per tal de descarregar de processos al Site Server, i així poder optimitzar les diferents tasques que es realitzen a la site: inventaris, distribució de programari, software metering, etc. Les funcions que poden assumir altres sistemes són:

- *Client Access Point*: és el punt de contacte entre el client i el site server. Emmagatzema temporalment les dades dels inventaris de maquinari i de programari abans de passar-les al site server. També és l'encarregat de l'anunci de paquets de distribució de programari. Hem decidit convertir els servidors de fitxers de les diferents seus, excepte de les seus A, B i C, on aquestes tasques seran assumides pel Site Serve, en Client Acces Point, perquè és important tenir un servidor amb aquestes tasques en cada seu de la nostra organització.

- *Distribution Point*: és l'encarregat d'emmagatzemar els paquets de programari que han de ser distribuïts als clients. Excepte en les seus A, B i C, els servidors de fitxers tindran aquesta funcionalitat.
- *Logon Point*: és l'encarregat de la instal·lació del client SMS en el cas que la instal·lació del client per Logon estigui activada. A l'igual que en els casos anterior, els servidors de fitxer seran els Logon Point .

Name	Type	Roles
\\CSEU1F01	Windows NT Server	SMS Logon Point
\\CSEU2F01	Windows NT Server	SMS Client Access Point; SMS Component Server; SMS Distribution I
\\CSEU3F01	Windows NT Server	SMS Logon Point
\\CSEUAF01	Windows NT Server	SMS Client Access Point; SMS Component Server; SMS Distribution I
\\CSEU11F01	Windows NT Server	SMS Client Access Point; SMS Component Server; SMS Distribution I
\\CSEU21F01	Windows NT Server	SMS Client Access Point; SMS Component Server; SMS Distribution I
\\CSEU31F01	Windows NT Server	SMS Logon Point
\\CSEU12F01	Windows NT Server	SMS Client Access Point; SMS Component Server; SMS Site Server
\\CSEU22F01	Windows NT Server	SMS Logon Point
\\CSEU32F01	Windows NT Server	SMS Logon Point
\\CSEU13F01	Windows NT Server	SMS Client Access Point; SMS Component Server; SMS Distribution I
\\CSEU11B05	Windows NT Server	SMS Component Server; SMS SQL Server
\\CSEU23F01	Windows NT Server	SMS Logon Point
\\CSEU33F01	Windows NT Server	SMS Logon Point

Funcions dels servidors de les diferents seus.

La càrrega a suportar per part del Site Server no ha de ser excessiva, però aquesta situació no justifica la creació d'altres Sites Systems de suport al Site Server (especialment Control Accés Points o Distribution Points). No obstant, la posada en marxa d'un nou Site System no ens comportaria cap procediment crític, i per tant, en qualsevol moment que estíem necessari es pot procedir a la configuració de qualsevol servidor Windows 2000 com a Site System.

6.2.5. Instal·lació de clients

La instal·lació de clients SMS a les diferents subxarxes s'ha de fer de manera progressiva, i així no provocar un col·lapse en la nostra xarxa. Com ja s'ha comentat anteriorment, la instal·lació d'un client SMS té dos pre-requisits:

- El descobriment del recurs.
- L'assignació de la subxarxa corresponent als boundaries de la site.

6.2.5.1. Descobriment selectiu per subxarxes IP

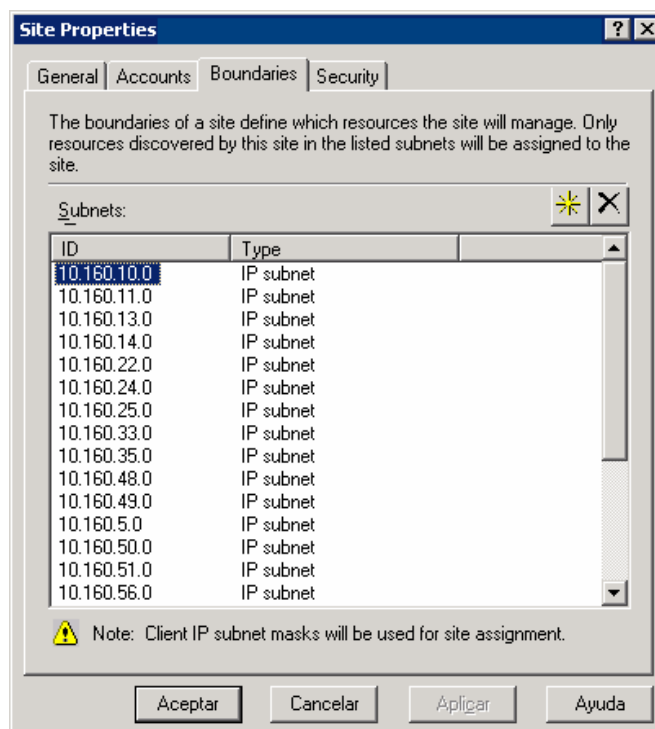
El mètode utilitzat per al descobriment ha estat el de *Network Discovery*. Aquest mètode permet descobrir els recursos de la xarxa en funció de diverses variables, com poden ser el domini, la subxarxa IP, les comunitats SNMP o els servidors DHCP. La nostra xarxa disposa de diverses subxarxes, la qual cosa ens ha permès fer un descobriment segmentat i controlat dels recursos.

En primer lloc, descobrirem la subxarxa on està instal·lat el servidor de la site SMS, és a dir, la subxarxa de la seu A. De manera progressiva, s'ha d'anar afegint les altres subxarxes de les altres ubicacions de la nostra organització.

Cada cop que descobrim un recurs, es crea un registre DDR (Discovery Data Record) a la base de dades de la site. En aquest moment, si s'activa algun mètode de instal·lació de client SMS, si el recurs ha estat seleccionat el client s'instal·larà en aquest recurs.

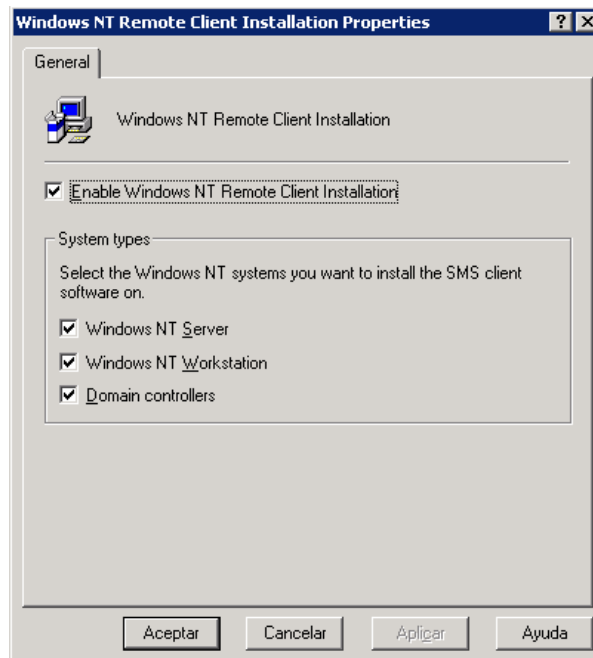
6.2.5.2. Instal·lació selectiva del client SMS

L'assignació d'un client per a la instal·lació del client SMS consisteix en configurar els *bounderies* de la site de manera que aquesta inclogui la subxarxa IP del client en qüestió. En aquest cas, si el client ha estat prèviament descobert per qualsevol dels dos mètodes explicats anteriorment, el client SMS s'instal·larà en l'estació de treball.



Selecció de subxarxes de la xarxa.

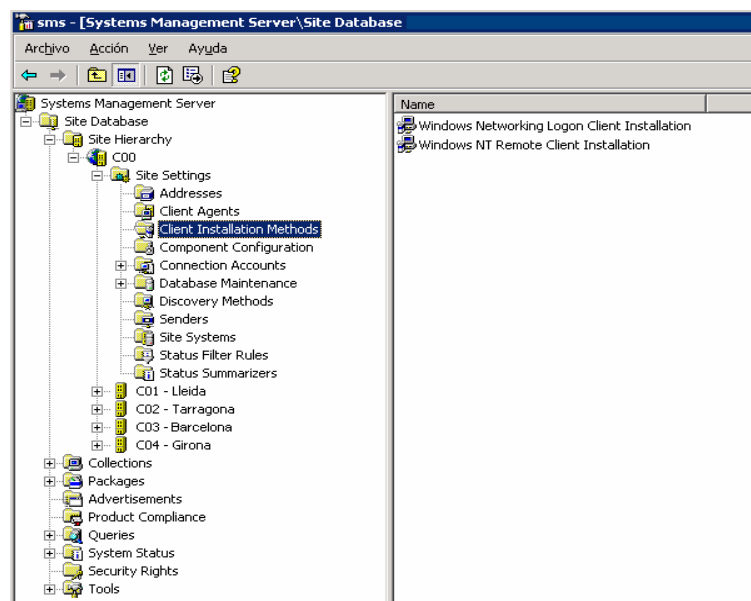
El mètode d'instal·lació seleccionat ha estat *Remote Client Installation*, consistent en una instal·lació remota i totalment desatesa dels servidors i de les estacions de treball.



Opcions de la pantalla de *Remote Client Installations*.

El procediment que s'ha seguit per instal·lar el client SMS de forma progressiva ha estat el següent:

- Especificar la subxarxa per descobrir a *Network Discovery*.
- Configurar la subxarxa com a *Site Boundary*.
- Activar la instal·lació de *Remote Client Installation* en els controlador de domini del nostre Active Directory.
-



Mètodes d'instal·lació dels agents de SMS.

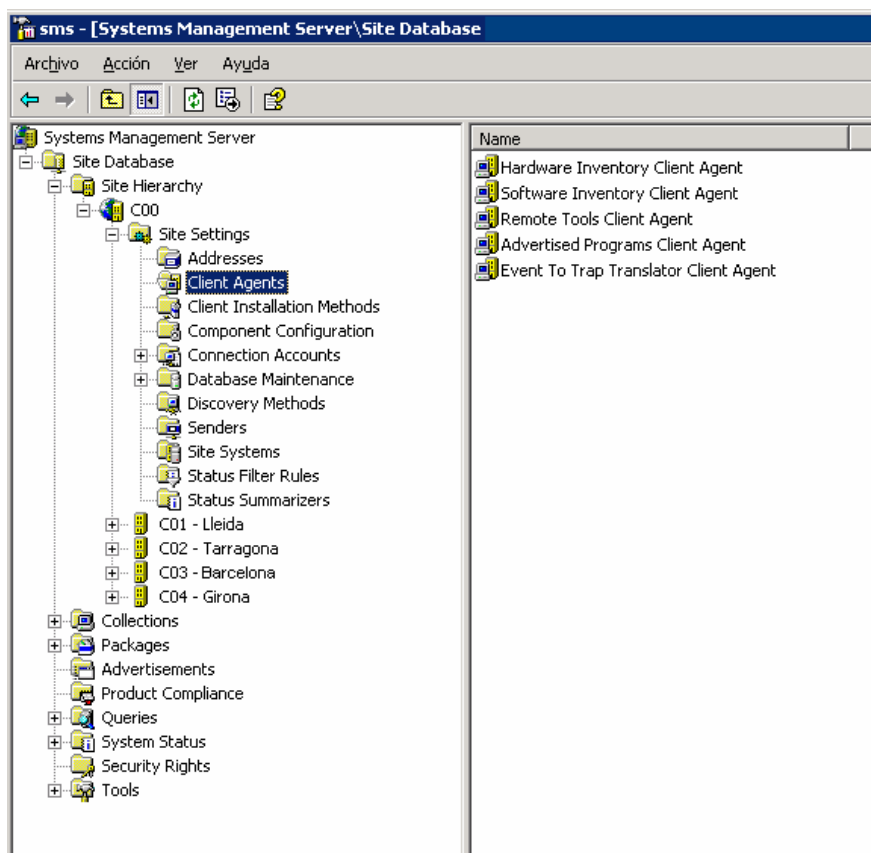
La instal·lació del client SMS en un sistema amb Windows NT crea i arrenca un servei temporal (SMS Client Bootstrap). Un cop el client s'ha instal·lat correctament, aquest servei desapareix i un altre servei queda arrencat de manera definitiva (SMS Client).

6.2.5.3. Instal·lació i configuració d'agents

Hem activat els següent quatre agents per la nostra site:

- Inventari de maquinari.
- Inventari de programari.
- Control remot.
- Distribució de programari.

Cal tenir present que l'activació d'un agent s'aplica a tots els clients de la site, i per tant, no es pot diferenciar a quins grups de màquines s'instal·larà un agent. Per poder aconseguir aquesta diferenciació, ens caldria crear diferents sites dintre de la jerarquia.

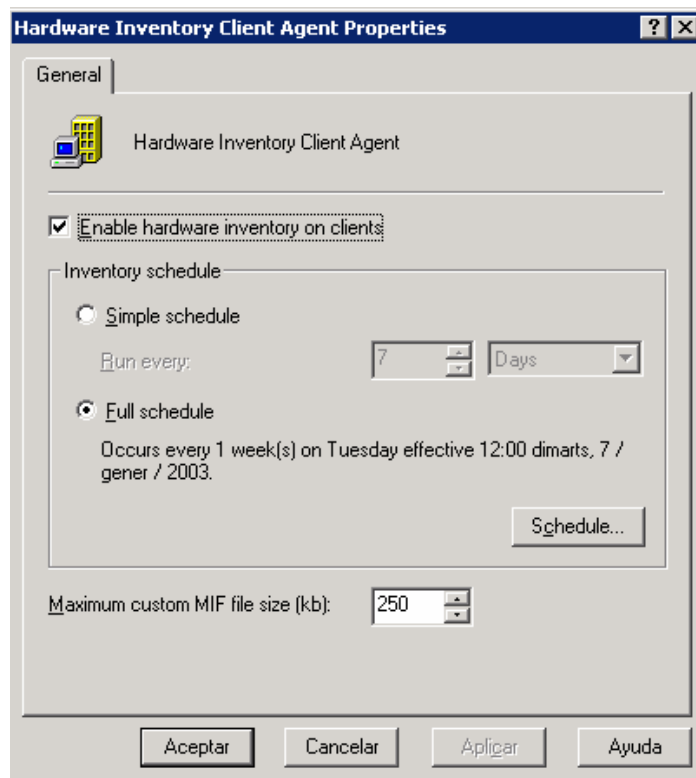


Agents disponibles en SMS.

Inventari de maquinari

L'agent d'inventari de maquinari, és el que s'ocupa d'inventariar el maquinari dels equips clients, amb la freqüència d'actualització que nosaltres vulguem especificar-li.

Aquest agent l'activarem per a què s'executi un cop per setmana. Les dades es recullen dels clients, i són transferides al Control Access Point (servidor de fitxers de cada seu) per posteriorment ser processades pel Site Server.



Propietats de l'agent d'inventari de maquinari.

Per personalitzar les dades que es recullen en l'inventari de maquinari es pot modificar el fitxer:

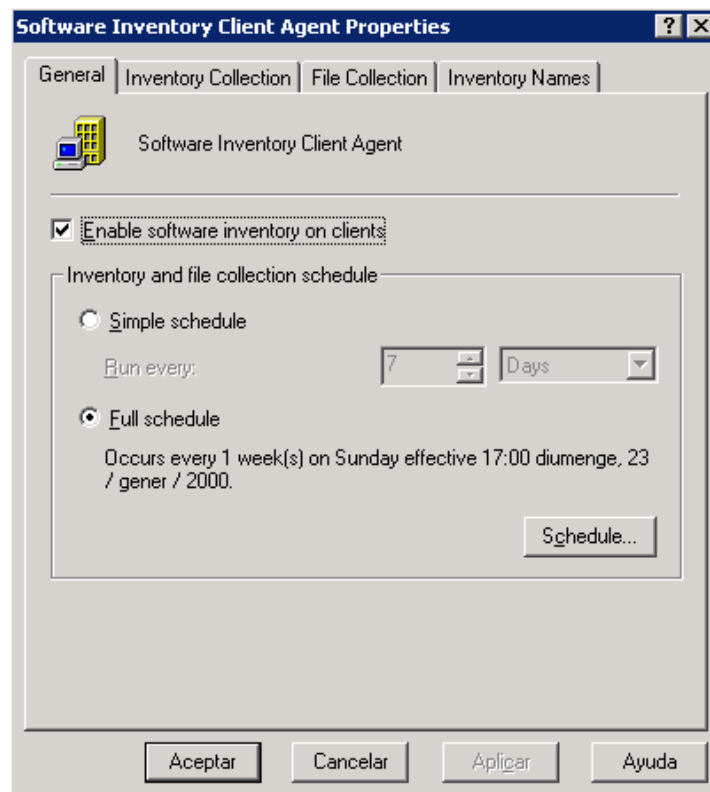
\\NOM_SERVIDOR\SMS_S00\inboxes\clifiles.src\hinv\sms_def.mof

Aquesta modificació es pot realitzar mitjançant la utilitat MOFMAN.exe del Resource Kit de SMS, o bé amb qualsevol editor de text.

Inventari de programari

L'agent d'inventari de maquinari s'ocupa d'inventariar el programari dels equips clients, amb la freqüència d'actualització que nosaltres li especifiquem.

Aquest agent l'hem activat per a què s'executi un cop per setmana. Les dades es recullen dels clients, i són transferides al Control Acces Point (servidor de fitxers de cada seu) per posteriorment ser processades pel Site Server.



Propietats de l'agent d'inventari de programari.

Per personalitzar les dades que es recullen en l'inventari de programari es pot modificar el fitxer:

\\NOM_SERVIDOR\SMS_S00\inboxes\clifiles.src\hin\sms_def.mof

Es pot personalitzar quins tipus de fitxers poden ser inclosos a l'inventari de programari (de defecte fitxers de tipus exe), però també es podem configurar l'agent per a què reculli fitxers sencers dels clients, com per exemple els fitxers autoexec.bat, config.sys o fitxers de tipus ini.

Control remot

L'activació i configuració de l'agent de control remot es realitza des de la següent ruta:

SMS\Site Database\Site Hierarchy\S00\Site Settings\Client Agents

Un cop aquí, es selecciona Remote Tools Client Agent, que s'hem configurat de la següent manera:

- Els clients no poden modificar les opcions de control remot.
- El control remot del client és total, és a dir, no cal la conformitat del client per interactuar amb la seva estació de treball.
- L'agent de control remot crea i arrenca un servei en els clients de SMS amb sistema operatiu Windows NT, Windows 2000 i Windows XP (Remote Control).



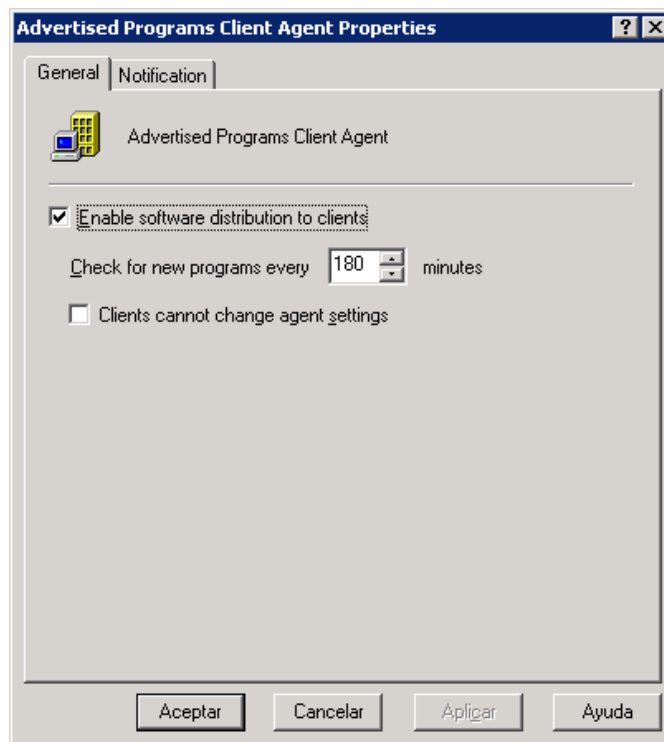
Propietats de l'agent de control remot.

Malgrat que la instal·lació de l'agent remot no seria necessària en un principi per clients amb Windows 2000 i Windows XP, ja que aquests sistemes operatius incorpora el programari Terminal Service, procedirem a la instal·lació d'aquest agent ja que el propi fabricant, Microsoft, recomana no instal·lar Service Packs des de la utilitat Terminal Service. La instal·lació de Service Packs a servidors mitjançant paquets de distribució de programari, també queda totalment descartada, degut a la seva criticitat.

Distribució de programari

La distribució de programari consisteix en el seguiment dels següent passos:

- Creació d'un paquet d'instal·lació mitjançant Microsoft Installer. Mitjançant aquest programari podem crear paquets d'instal·lació automatitzats, que s'instal·len en el client de forma silenciosa ja que totes les opcions d'instal·lació ja estan predeterminades.
- Creació de col·leccions dels clients on vulguem instal·lar el paquet de programari. Es convenient crear diverses col·leccions de clients per no col·lapsar la xarxa, si el paquet de programari és de molts MB.
- Creació d'un advertiment per a cadascuna de les col·leccions creades anteriorment.

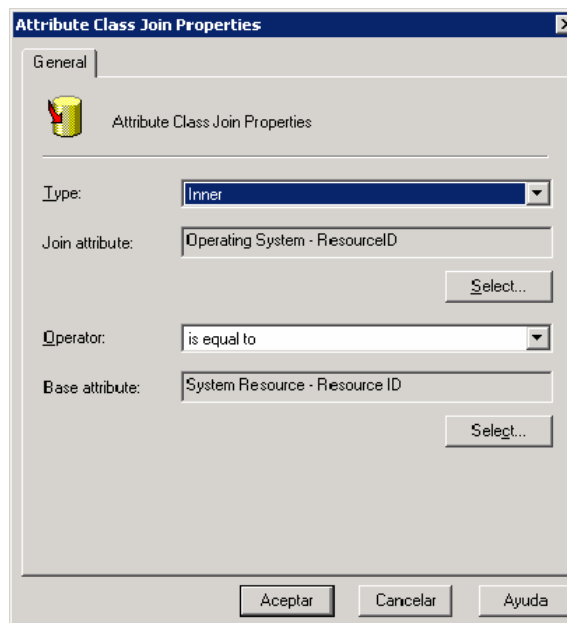
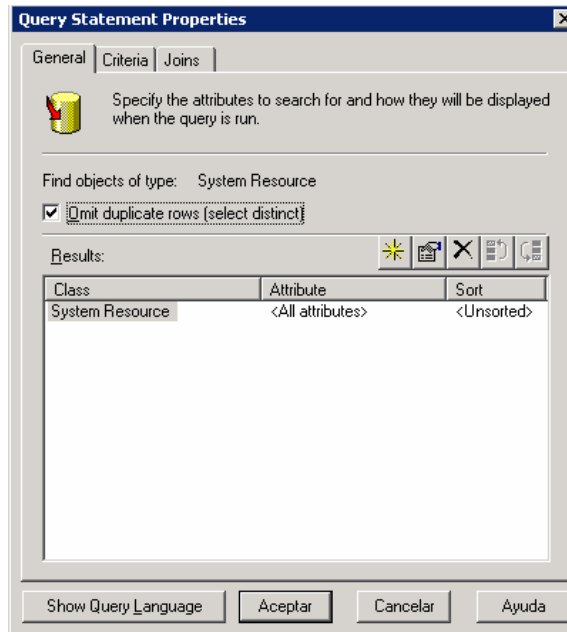


Configuració de l'agent d'advertiment de distribució de programari.

6.3. Consultes i col·leccions

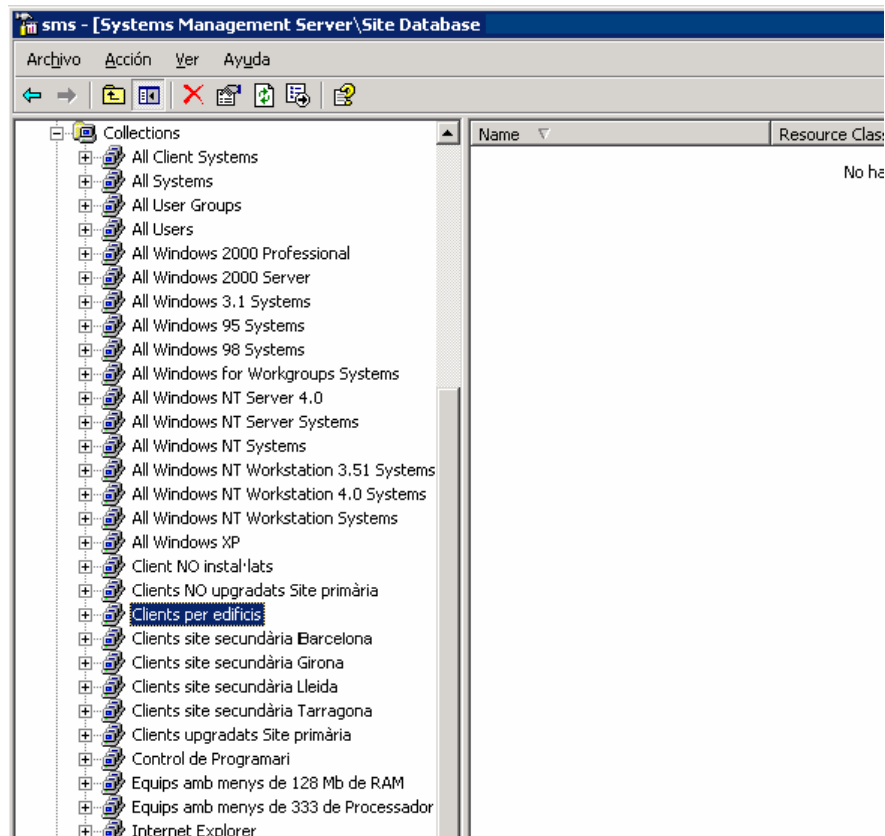
Hem definit diverses consultes i col·leccions per facilitar la gestió dels diferents servidors i les diferents subxarxes de la nostra organització.

Les consultes creades s'han definit en base a les dades dels servidors i de les estacions de treball recollides pels inventaris de maquinari i programari per tal de poder efectuar consultes com per exemple, servidors amb dos processadors, estacions de treball amb menys de 128 MB. De memòria RAM, etc.



Exemple de consulta.

Les col·leccions són agrupacions d'equips en base a una consulta SQL de les dades dels inventaris, o mitjançant una assignació directa d'una sèrie d'equips determinats. En primer lloc, hem creat en la site de SMS una col·lecció anomenada *Seus* que conté una subcol·lecció per cada seu de l'organització (SeuA, SeuB, SeuC, Seu1, etc.). Cadascuna d'aquestes subcol·leccions conté en base a assignacions directes els servidors i les estacions de treball que estan ubicades en cadascuna d'aquestes localitzacions.



Col·leccions definides.

6.4. Integració amb Network Node Manager

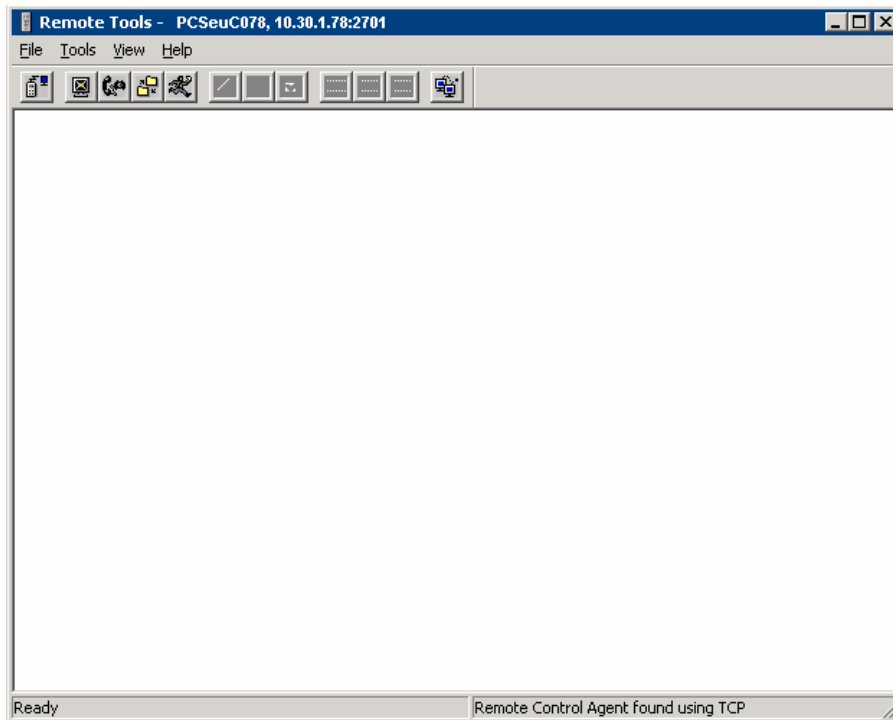
La implantació de la site de SMS per afegir les funcionalitats ja explicades anteriorment als servidors i a les estacions de treball de la nostra empresa, són prou interessants com per integrar-les a la consola del NNM, la interfície de gestió centralitzada del HP OpenView, el sistema implantat per oferir una gestió global de la xarxa i els sistema de la nostra organització.

Aquesta integració consisteix bàsicament, en la inclusió d'un menú personalitzat en la consola del NNM, des d'on podem executar diferents utilitats del SMS, com per exemple: Remote.exe o Explorer.exe.

6.5. Control remot

La utilitat Remote.exe executa el control remot de SMS, acceptant com a paràmetre un nom NetBIOS o una adreça IP. Nosaltres hem optat per executar la comanda des del menú personalitzat del NNM de la següent manera:

REMOTE adreça_IP_equip



Pantalla resultat de l'execució de la comanda REMOTE.

On el paràmetre adreça_IP_equip prové d'una programació de codi que obté l'adreça IP de l'equip seleccionat de la consola del NNM.

Des d'aquesta pantalla podem agafar el control remot de la màquina, reiniciar l'equip, obrir un xat amb el client, executar comandes des d'una línia de comandes, gravar o executar una macro o transferir fitxers entre les dues màquines.

6.6. Inventaris de maquinari i programari

La utilitat *mmc* (Microsoft Management Console) permet mitjançant el pas de paràmetres personalitzar la informació que es mostra. D'aquesta forma, des del menú personalitzat del NNM cridem el Resource Explorer del SMS per poder mostrar els inventaris de maquinari i de programari d'un equip prèviament seleccionat en la consola del NNM. La sintaxi de la comanda és la següent:

```
mmc explore.msc -s -sms:ResourceID=n -sms:Connection=<namespace path>
```

on *n* és el ResourceID del client SMS del que es vol consultat l'inventari i on <namespace path> és la ruta a la base de dades que conté les dades del client.

Exemple:

```
mmc explore.msc -s -sms:ResourceID=1 -sms:Connection =  
\\NomServidor\root\sms\site_A
```

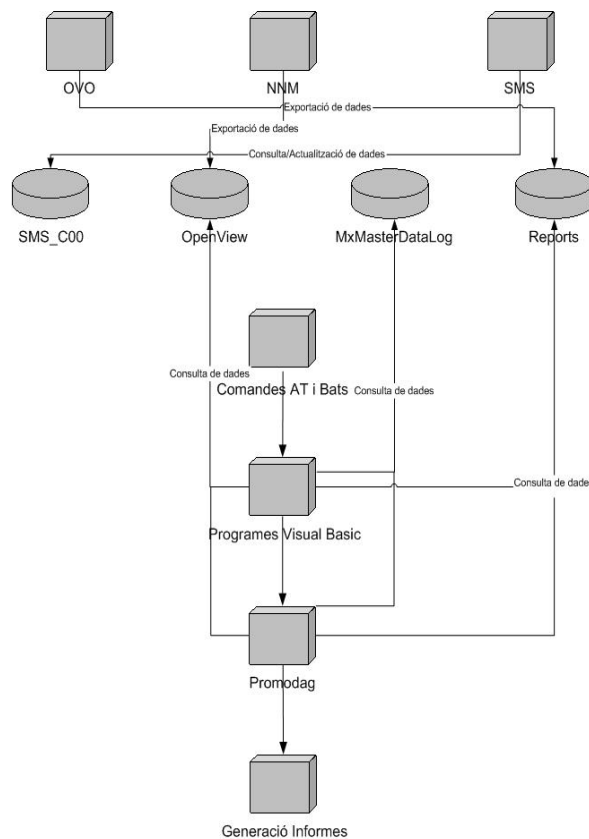
7. Informes

A continuació anem a descriure els diferents informes que realitzarem, indicant els seus aspectes més rellevants.

7.1. Organització

L'execució dels informes es basa en les següents fonts d'informació:

- Base de dades reports (inventari dels informes).
- Base de dades OpenView.
- Base de dades MXMasterDataLog (OpenView Operations).
- Base de dades SMS
- Taules de servidors, encaminadors, seus, interfícies, etc. (extracció de les bases de dades d'OpenView i MxMasterDataLog).
- Tracking Log dels servidors Exchange 2000.



Esquema del funcionament dels informes.

Executarem els informes de forma automàtica els dia 1 de cada mes, obtenint les dades corresponents al mes anterior. D'aquesta forma podrem realitzar comparatives i evolucions de les dades mes a mes.

7.2. Accés als informes

Podrem accedir de dues formes als informes:

- Accés de consulta, per visualitzar els informes automàtics.
- Accés per executar informes de forma personalitzada.



Pàgina Web d'accés als informes disponibles.

7.2.1. Accés de consulta als informes automàtics

L'accés el podrem realitzar mitjançant un navegador HTML, accedint a l'adreça del servidor OpenView. A continuació només caldrà seleccionar l'informe concret que desitgem visualitzar, accedirem a l'informe ja executat, per la qual cosa els paràmetres seran els predeterminats.

7.2.2. Accés per generar informes personalitzats

Des de la pàgina principal del servidor Web, tindrem un accés directe a la pàgina de generació d'informes personalitzats. En aquest cas, sí que serà possible configurar exactament quins paràmetres desitgem donat que l'informe es generarà en temps real.

Degut al gran número de dades de les que consta cadascuna de les bases de dades, l'obtenció dels informes no serà immediat, tindrem un petit temps d'espera.

7.3. Disseny de la base de dades reports

La base de dades dels informes l'hem anomenada *reports* que conté la taula amb el mateix nom, aquesta taula serà utilitzada per a emmagatzemar els diferents informes que podrà generar l'usuari, amb una descripció i el camí d'on es troba l'executable generador de l'informe. D'aquesta forma, des de la pàgina principal de la Web, podrem visualitzar una llista desplegable amb les diferents descripcions existents en aquesta taula. Un cop l'usuari realitzi una selecció d'una descripció d'un informe, podrem visualitzar en la part inferior de la pàgina el camí on pertany l'executable generador d'aquest informe.

També emmagatzemarem l'adreça de la corresponent pàgina Web, on ens caldrà anar a buscar aquest informe per a la seva visualització.

En aquesta taula hi afegirem un camp, anomenat *log*, que serà necessari pels informes executats mitjançant el programa *RepUptime.exe*, ja que el funcionament d'aquest informe és sensiblement diferent a la resta.

A continuació definim els camps de la taula *reports*:

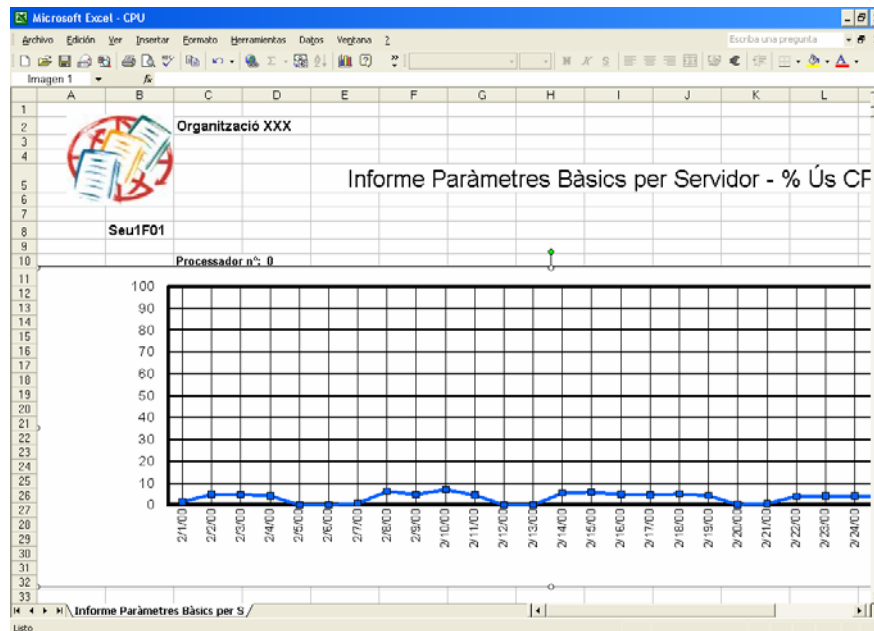
- *ID*: camp identificatiu de format numèric.
- *Descripció*: camp de text de longitud 255 caràcters, on indicarem una breu descripció per identificar els informes. Aquesta serà la descripció utilitzada a la llista desplegable de la pàgina principal.
- *Fitxer*: camp de text de longitud 255 caràcters, per senyalar el camí de l'executable generador de l'informe.
- *DestiHTML*: camp de text de longitud 255 caràcters, per donar nom al fitxer HTML (només el nom, el camí està definit en la pàgina Web) que ha de visualitzar la pàgina Web.

- Log: camp de text de longitud 255 caràcters que utilitzarem per donar nom al fitxer log que ha de visualitzar la pàgina Web.

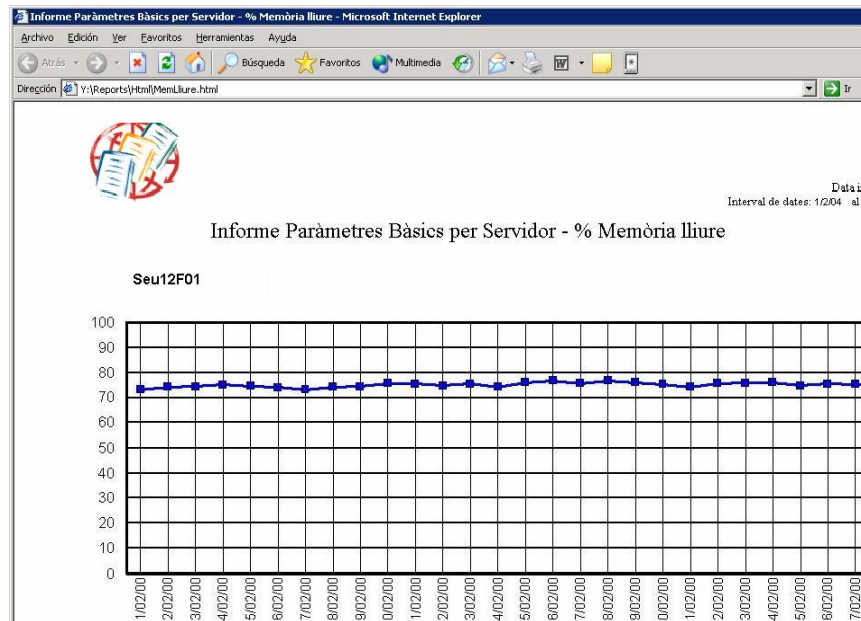
7.4. Descripció dels informes

Informes de paràmetres bàsics:

- Informe gràfic de percentatge d'ús de CPU per cada servidor. En el cas d'un servidor multiprocessador obtenim la informació de cadascun dels processadors.
- Informe gràfic de percentatge d'espai lliure de disc de cada servidor desglossat en les diferents unitats lògiques.
- Informe gràfic de percentatge de memòria lliure de cada servidor.



Exemple d'informe de paràmetres bàsics (ús de CPU) per servidors en format XLS.



Exemple d'informe de paràmetres bàsics (%Memòria lliure) per servidors en format HTML.

Informes de usuaris concurrents en servidors de fitxers:

- Informe que presenta el promig i el màxim de sessions concurrents establertes a cada servidor desglossat per dies.

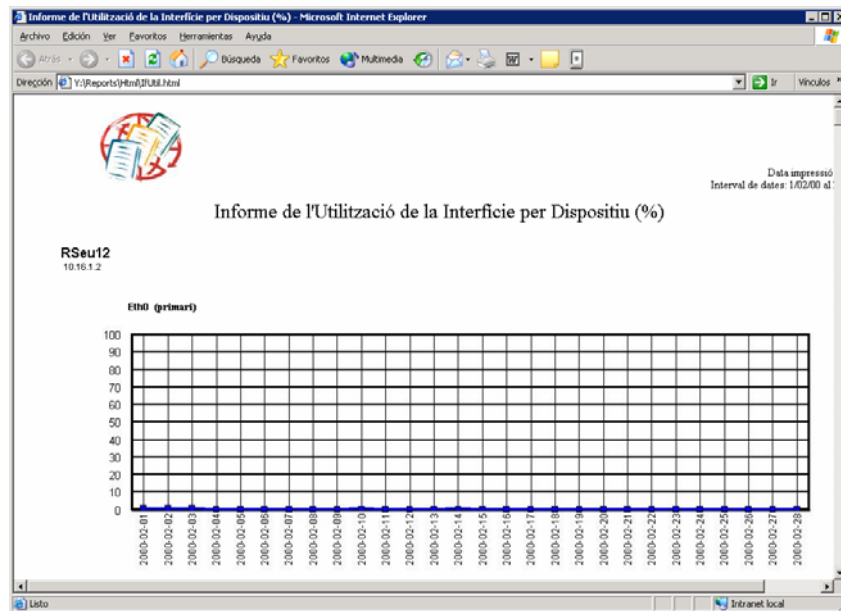
Informes de SQL 2000

- Informe de promig i màxim d'usuaris concurrents.
- Informe de la caché Hit Radio.
- Informe del total blocking locks
- Informe I/O pages reads/sec.
- Informe que proporciona el llistat de caigudes i nivell de servei dels servidors SQL 2000.

Informes de xarxa

- Informe gràfic que presenta per cada encaminador i commutador el percentatge d'ús de CPU.
- Informe gràfic que mostra el número total de bytes de memòria lliure disponible en cada encaminador i commutador.
- Informe gràfic sobre el número total de fallades causades per memòria insuficient alhora de crear un nou buffer.
- Informe gràfic que proporciona el percentatge d'utilització de cada interfície dels encaminadors i commutadors.

- Informe que proporciona el llistat de caigudes de cada encaminador i commutador, així com el seu percentatge de servei. Aquest mateix informe estarà disponible amb dades de l'horari laboral.



Exemple d'informe d'utilització de interfícies d'encaminadors.

Informes d'Exchange 2000

- Informe de missatges enviats a Internet.
- Informe de missatges rebuts de Internet.
- Informe de missatges enviats internament.
- Informe de missatges rebuts internament.
- Informe de les 10 i 20 bústies que més missatges envien.
- Informe de les 10 i 20 bústies que més missatges reben.
- Informe dels missatge enviats per servidor.
- Informe dels missatge rebuts per servidor.
- Informe que proporciona el llistat de caigudes i nivell de servei dels servidors Exchange 2000.

Top N Message Receivers Report - Microsoft Internet Explorer


Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia Ir Vinculos >>

Dirección Y:\Reports\Html\Cinfo\Topreceivers.htm

Top N Message Receivers Report

Print Date: 3/2/04



External Recipient	Bytes Received	Total Msgs	Avg Length of Msgs	Largest Msg
S12RPC	4 MB	1,639	2 KB	456 KB
SAMAC	2 MB	1,446	1 KB	133 KB
ADMINISTRATOR	3 MB	583	6 KB	11 KB
SAJPC	1 MB	518	2 KB	26 KB
SCLPJ	9 MB	275	34 KB	1 MB
SCLLP	1 MB	254	5 KB	1 MB
S1MGP	10 MB	224	49 KB	197 KB
S11FMZ	3 MB	195	17 KB	1 MB
S33PER	5 MB	193	27 KB	716 KB
S21JUP	5 MB	167	30 KB	1 MB
Others	198 MB	3,269	62 KB	7 MB
Totals:	245 MB	8,508	28 KB	7 MB

Others Recipient	Bytes Received	Total Msgs	Avg Length of Msgs	Largest Msg
S21JMP	4 MB	1,655	2 KB	456 KB
SARPC	2 MB	1,450	1 KB	133 KB
SBJGF	11 MB	1,532	7 KB	1 MB

Listo Intranet local

Exemple d'informe d'Exchange 2000

8. Conclusions

A partir d'un escenari d'una organització fictícia, organitzada en diverses seus, on el sistema de la informació són distribuïts per poder organitzar grups de treball distribuïts, compartir recursos o comunicar informació ràpidament, hem justificat la necessitat de disposar d'una eina de gestió que ens ha de permetre:

- Obtenir una visió global de la xarxa.
- Gestionar de forma centralitzada de la xarxa.
- Monitorització activa de sistemes i de la seva disponibilitat.
- Detecció ràpida de fallades.
- Recepció d'events i de fitxers de registres (logs) generats pels sistemes.
- Obtenir d'informes a partir del repositori d'alarmes i events i de la recollida de dades dels agents instal·lats en el maquinari.
- Accessibilitat als components de la xarxa.
- Control remot d'estacions de treball i servidors de la nostra xarxa
- Obtenció d'un inventari de programari i maquinari del parc informàtic.
- Distribució desatesa de programari a les estacions de treball.

Hem realitzat una comparativa de tres productes especialitzats en l'administració de xarxes: OpenView de Hewlett-Packard, Unicenter de Computer Associates i VitalSuite de Lucent. Hem valorat diferents aspectes com els relacionats a l'administració de fallades, la representació gràfica de la xarxa, la facilitat de generació i la qualitat dels informes, la facilitat d'ús de l'eina, per poder seleccionar de forma adequada el producte més adient. Hem decidit que el millor producte dels tres és OpenView de Hewlett-Packard.

En primer lloc, hem instal·lat OpenView Network Node Manager, hem executat el descobriment inicial de la xarxa, i hem pogut observar alguns dels mapes obtinguts a partir del descobriment inicial, és d'especial importància el mapa principal. Hem explicat com crear nous mapes i submapes; com es representen els objectes i quina és la seva representació gràfica, els símbols, que mitjançant els colors d'aquests podem saber el seu estat.

El sistema d'events recull informació dels agents instal·lats als dispositius, de les aplicacions, serveis i nodes de xarxa, i proporciona una localització centralitzada d'events i traps anomenada Alarm Browser. Els events i traps que considerem importants podem visualitzar-los com a alarmes, a les quals podem associar-li una acció determinada. L'Alarm Browser categoritza i classifica les alarmes.

Després hem implantat OpenView Operations for Windows, que ens ha proveït d'una consola per la gestió d'events, aplicacions i serveis crítics dels servidors. Hem explicat les funcionalitats dels Smart Plug -Ins que hem instal·lat:

- SPI for Windows Operating System
- SPI for Active Directory
- SPI per servidors Web
- SPI for Microsoft Exchange Server
- SPI for Microsoft SQL

També hem considerat temes de seguretat d'usuaris i grups relacionats amb els serveis associats a OVO.

Hem dissenyat la jerarquia de System Management Server, consistent en determinar el nombre de sites necessàries, el seu tipus i hem decidit quin servidor hem de configurar per a què realitzin funcions especials de suport al Site Server (Client Acces Point, Distribution Point, Logon Point, etc.), alhora d'implantar SMS dins del projecte general de gestió d'administració de xarxes i sistemes.

També hem decidit que el mètode de descobriment i instal·lació dels clients sigui Network Discovery, per poder així realitzar un descobriment i una instal·lació segmentada i controlada dels recursos, de manera progressiva i sense causar col·lapses en la xarxa.

Hem explicat com configurar els agents activats per la instal·lació dels clients de la site:

- Inventari de maquinari.
- Inventari de programari.
- Control remot.
- Distribució de programari.

Finalment hem desenvolupat la part relativa als informes, explicant de quines bases de dades extraurem les dades per obtenir els informes, i hem fet referència al disseny de la base de dades reports per emmagatzemar els informes generats pels usuaris.

Mitjançant una pàgina web podem consultar els informes mensuals o executar informes de forma personalitzada, també hem fet una petita descripció dels informes mensuals.

Com podem veure, l'eina de gestió de xarxes implantada ha complert amb tots els objectius i funcionalitats que ens havíem proposat com a resposta d'una solució a l'administració d'un entorn distribuït .