SPS brengt business & IT samen

Veel beheerorganisaties hebben een rijk gevuld portfolio aan beheertools, maar hebben ondanks die rijkdom geen inzicht in de status van de dienstverlening. Juist door de diversiteit aan beheertools zijn elementaire zaken als capaciteitsplanning om paniekaankopen te voorkomen niet mogelijk. Daarom hebben veel organisaties de behoefte om eens flink de bezem te halen door hun *tooling*-portfolio of om het portfolio beter in te zetten en alle mogelijkheden te benutten. SPS (Service Provider Solutions) heeft hiervoor een pragmatische en effectieve aanpak ontwikkeld. Dit artikel beschrijft een oplossingsrichting voor deze problemen aan de hand van het *business service management*-concept (BSM) van SPS.

Bart de Best

Door vele innovaties, overnames, veroudering van *tooling* en andere zaken ontstaan bij vele beheerorganisaties complete lappendekens aan tools die een te laag niveau van operationele en bestuurlijke informatievoorziening bieden. Dit leidt onder meer tot:

- Paniekaankopen: er kan niet geanticipeerd worden op te verwachten *resource*-knelpunten, waardoor er 'paniekaankopen' plaatsvinden.
- Lokalisatieproblemen: als er een verstoring plaatsvindt, kan niet nagegaan worden welke informatiesystemen daar last van hebben. Met de monitoring kan evenmin snel een fout worden gelokaliseerd.
- Proactiviteit: er is behoefte om een verstoring sneller te zien aankomen.
- Imagoschade: doordat de status van de dienstverlening niet bekend is, kan imagoschade worden opgelopen.
- Omzetverlies: door het niet tijdig kunnen reageren op verstoringen ontstaat onnodig productieverlies en omzetverlies.
- Tijdverlies: alerts worden niet automatisch als een incident geregistreerd. Ook is het niet mogelijk incidenten in de servicedesktool te matchen met alerts in de monitortools (alleen buiten de tools om en handmatig).
- Complexiteit: doordat er zo veel verschillende, verouderde en overbodige tools aanwezig zijn, is het beheer van deze tools complex en inefficiënt.

BSM-projectaanpak

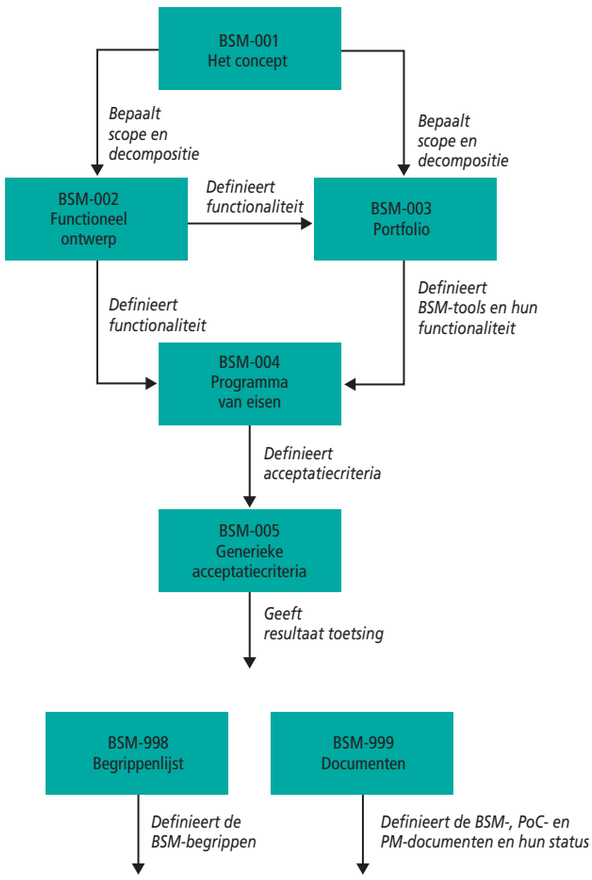
Om genoemde problemen op te lossen wordt doorgaans een project opgestart met één of meer doelstellingen zoals hieronder weergegeven.

- De nieuwe BSM-oplossing dient om de beschikbaarheid van de ICT-infrastructuur te vergroten, door het toepassen van zowel operationele informatievoorziening (*event management*) als bestuurlijke informatievoorziening (tactisch beheer).
- Event management moet de niet-beschikbaarheid vanwege verstoringen verlagen door de detectietijd te verkorten en

ITB08-05_v4.indd 40 11-06-2008 11:49:38

SPS

SPS is een leverancier van beheersoftware. Vanaf de oprichting in 1994 is de onderneming onlosmakelijk verbonden geweest met de beheersoftware Gensys. De combinatie van beheerdiensten, zoals de RES-Q *remote* beheerservices, met de beheersoftware Gensys vormt de totaaloplossing voor IT-beheer.
SPS hanteert de bedrijfsprocessen hierbij als uitgangspunt. Voor elk bedrijfsproces wordt de onderliggende IT-infrastructuur in kaart gebracht. Hierdoor wordt voor elke IT-component duidelijk welke bijdrage deze levert aan welk bedrijfsproces. Deze relatie van de IT-componenten met diverse bedrijfsprocessen maakt tevens de beschikbaarheid van de hele keten inzichtelijk.
Dit inzicht ontstaat op basis van proactief en preventief beheer met Gensys, over de hele keten, en garandeert een maximale beschikbaarheid door tijdig in te grijpen wanneer de SLA-normen van één of meer bedrijfsprocessen niet gehaald dreigen te worden.
SPS focust niet alleen op de middelenkant. Juist door het accent te leggen op kennisoverdracht in de vorm van consultancy en coaching wordt geborgd dat de beheersoftware rendeert. De combinatie van excellente beheersoftware en beheerders zorgt voor de optimale verbinding tussen de business en IT.



Figuur 1 De BSM-documenten

het vinden van de oorzaak van een verstoring te versnellen.
- Tactisch beheer moet capaciteitsincidenten en daarmee gepaard gaande paniekaankopen voorkomen en moet bestuurlijke informatie over beschikbaarheid en performance opleveren die nodig is om *service improvement plans* uit te voeren.
- Op strategisch niveau wordt een visie ontwikkeld op de koers qua monitorarchitectuur, productenportfolio en strategievorming. Op basis hiervan wordt een IST-SOLL-analyse verricht en kan een migratiestrategie worden ontwikkeld.

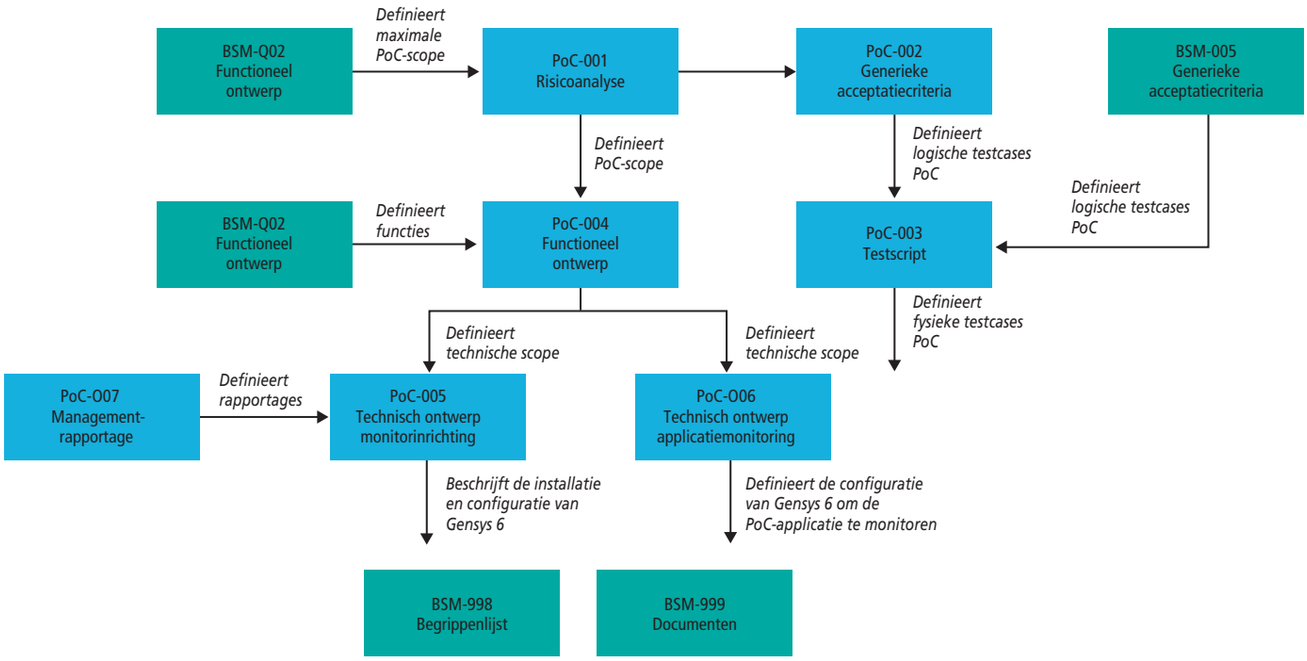
Om deze doelstellingen te verwezenlijken dient een plan van aanpak opgesteld te worden met de volgende stappen:
- Definieer een programma van eisen (PvE) voor het beheertoolportfolio inzake:
  - het monitoren van de beschikbaarheid, beveiliging, performance en capaciteit van de infrastructuur en applicaties;
  - het genereren van alerts die beheerders informeren in geval van ernstige verstoringen;
  - het monitoren en alerten van de bedrijfsprocessen;
  - rapportagemogelijkheden.
- Bepaal van het huidige beheertoolportfolio per beheertool in welke mate deze invulling geeft aan het PvE.
- Selecteer een tool die (grotendeels) invulling kan geven aan het PvE.
- Stel middels een *proof of concept* (PoC) vast of de gekozen tool inderdaad invulling kan geven aan de door de leverancier aangegeven score op het PvE.
- Verklaar de nieuwe tool leidend, elimineer de redundante beheertools en completeer de functionaliteit waar nodig met de nieuwe tool.
- Implementeer de beheertool voor de monitoring op systeemniveau en applicatieniveau in de productieomgeving.

Deliverables

In het plan van aanpak dienen een aantal *deliverables* en hun onderlinge relaties te worden gedefinieerd. In figuur 1 zijn aan de deliverables gerelateerde documenten weergegeven. We zullen eerst even kort door deze documenten heen lopen. Daarna volgt een aantal best practices, waarbij gerefereerd wordt aan deze documenten.

Het conceptdocument (BSM-001) definieert de afbakening van het werkterrein in de vorm van een opdeling van *system management*- en *service management*-tools, monitordomeinen en monitorfunctionaliteit. Op basis van deze definities wordt een functioneel ontwerp (BSM-002) opgesteld voor de beoogde BSM-functionaliteit. Tevens wordt op basis van het conceptdocument (BSM-001) het portfolio aan beheertools geïnventariseerd en geclassificeerd (BSM-003). Vanuit het door deze documenten verkregen inzicht wordt een programma van eisen opgesteld (BSM-004). Aan de hand van het PvE worden ten slotte de generieke acceptatiecriteria opgesteld voor de BSM-tooling (BSM-005).

ITB08-05_v4.indd 41 11-06-2008 11:49:39



Figuur 2 De PoC-documenten

Voor het uitvoeren van de PoC kan gebruikgemaakt worden van de opgestelde BSM-documenten. De PoC-documenten zijn opgenomen in figuur 2. De BSM-documenten zijn hier in groene vierkanten weergegeven.

De belangrijkste twee aandachtspunten bij de proof of concept-documenten zijn:

1. Zorg dat de testscripts (PoC-003) gebaseerd zijn op de risicoanalyse (PoC-001).
2. Stel niet voor elk te monitoren informatiesysteem een technisch ontwerp op. Stel in plaats daarvan een algemeen technisch ontwerp op met alle generieke monitorfuncties (PoC-005) en een specifieke technisch ontwerp voor applicatiespecifieke monitorfuncties (PoC-006).

Functionaliteit

Het opgeschoonde en aangevulde beheertoolportfolio moet gaan voorzien in de bestuurlijke en de operationele informatievoorziening. De bestuurlijke informatievoorziening is gericht op het inzichtelijk maken van de beschikbaarheid, performance en capaciteit van de ICT-infrastructuur op systeemniveau (fysiek = infrastructuurcomponentniveau) en op applicatieniveau (logisch = informatiesysteemniveau). Deze informatie moet periodiek worden gerapporteerd. De operationele informatievoorziening is gericht op het dagelijks (operationeel) beheer. De systeembeheerders moeten de beschikking krijgen over een monitoring van infrastructurele componenten, applicaties en in de toekomst ook bedrijfsprocessen. Deze monitoring moet in ieder geval de beschikbaarheid, performance en capaciteit monitoren en alerts genereren. Deze informatie moet realtime beschikbaar zijn.

Best practices

In de loop van de tijd heeft SPS een aantal best practices ontwikkeld die generiek van toepassing zijn. Per best practice is een verwijzing opgenomen naar de deliverables zoals in figuur 1 weergegeven.
De volgende best practices worden behandeld:

- BSM001/1 Het lagenmodel
- BSM001/2 Domeinen
- BSM002/1 Prestatiemeting
- BSM003/1 IST & SOLL

Hierbij wordt ook kort stilgestaan bij het aspect beheerarchitectuur. In *IT Beheer Magazine* nummer 5 2007[1] is een uiteenzetting gegeven over beheerarchitectuur. Hierbij zijn de begrippen 'architectuurprincipes' en 'architectuurmodellen' voor beheer besproken aan de hand van het BEheren onder Architectuur (BEA-)stappenplan. Het BSM-concept is gebaseerd op dit stappenplan. Binnen het BSM-concept is invulling gegeven aan een aantal architectuurmodellen en architectuurprincipes. In de hierna genoemde best practices zal in ieder geval het monitorlagenmodel (architectuurmodel) en een aantal architectuurprincipes en passant worden besproken.

Lagenmodel

Het is belangrijk om de monitorfunctionaliteit op te delen in losstaande functionaliteiten die samen een logisch geheel vormen. Het architectuurmodel zoals in figuur 3 is weergegeven, is hier een voorbeeld van. Dit model is gebaseerd op de functionele decompositie, zoals gedefinieerd in het boek *Ketenbeheer in de praktijk*[6]. De basis is de systeemmonitoring. Hierin zijn de componentmetingen gedefinieerd, zoals *event monitoring* en *resource monitoring*. Deze monitoring geeft dus alleen een beeld van de geïsoleerd gemeten objecten zoals hardware en software.
Een abstractieniveau hoger wordt gemeten op applicatieniveau. Om bijvoorbeeld de beschikbaarheid van een applicatie

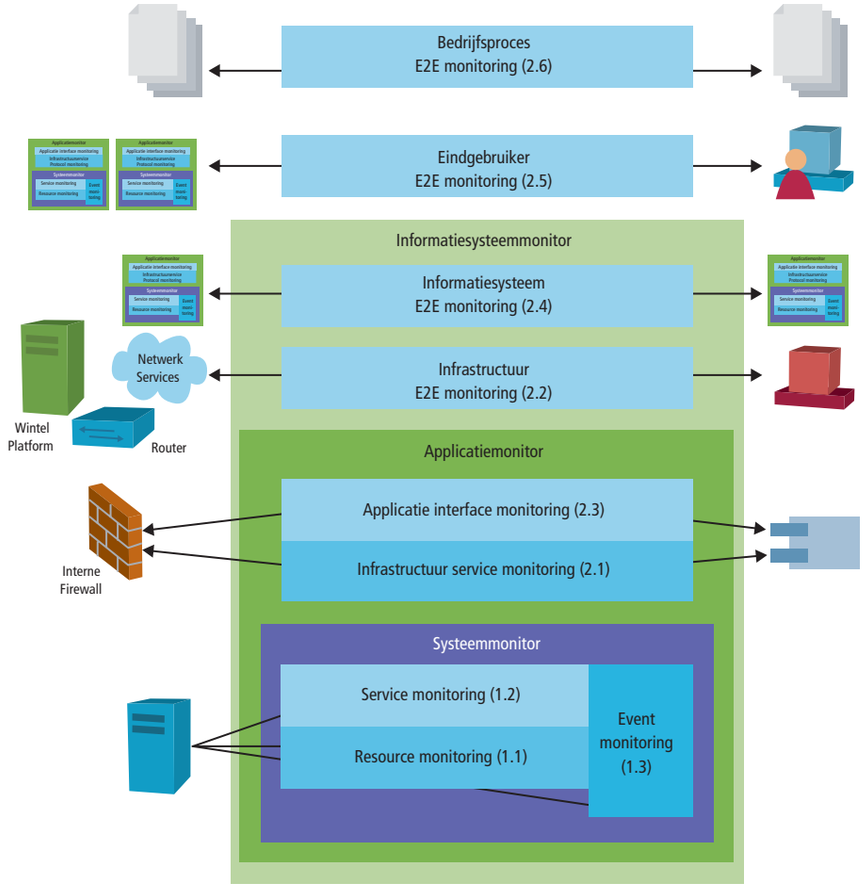
ITB08-05_v4.indd 42 11-06-2008 11:49:39

te meten, worden drie typen metingen met elkaar vergeleken, te weten de systeemmonitoring van de bij de applicatie betrokken hardware en software, de infrastructurele services die de applicatie gebruikt, zoals een autorisatieservice, en ten slotte de applicatie-interfaces waarmee de applicatie in verbinding staat.
Als gemeten wordt op informatiesysteemniveau, wordt gemonitord over de gehele keten die het informatiesysteem doorloopt. Zo ook de gehele keten van de infrastructuur. Tevens valt binnen deze monitoring de verwerking van alle betrokken applicatiemonitorinformatie en de betrokken systeemmonitorinformatie.
Ten slotte blijft het ketenmonitorniveau over, waarbinnen bedrijfsprocessen- en eindgebruikersmetingen vallen.
Naast deze monitorfunctionaliteit zijn nog een aantal additionele functionaliteiten onderkend, zoals koppelingen- en rapportagefunctionaliteiten. Dit lagenmodel heeft de volgende toegevoegde waarde:

1. het biedt een eenvoudige praatplaat (figuur 3), die gebruikt kan worden in managementpresentaties, workshops, risicoanalyses, leveranciersmeetings et cetera;
2. het is de basis voor de functionele decompositie (figuur 1, BSM-002);
3. het definieert de klassen waarin de beheertools zijn ingedeeld (figuur 1, BSM-003);
4. het biedt een mogelijkheid om een eenduidige fasering te definiëren van volwassenwording van monitoring;
5. het geeft een referentie voor functionaliteit, eisen in het PvE (figuur 1, BSM-004), acceptatiecriteria (figuur 1, BSM-005), testcases, planning et cetera.

Een belangrijk architectuurprincipe dat aan de hand van deze plaat uit te leggen valt, is het nevenstaande.

Domeinen
Om tientallen tools met elkaar te kunnen vergelijken, is het handig gebleken



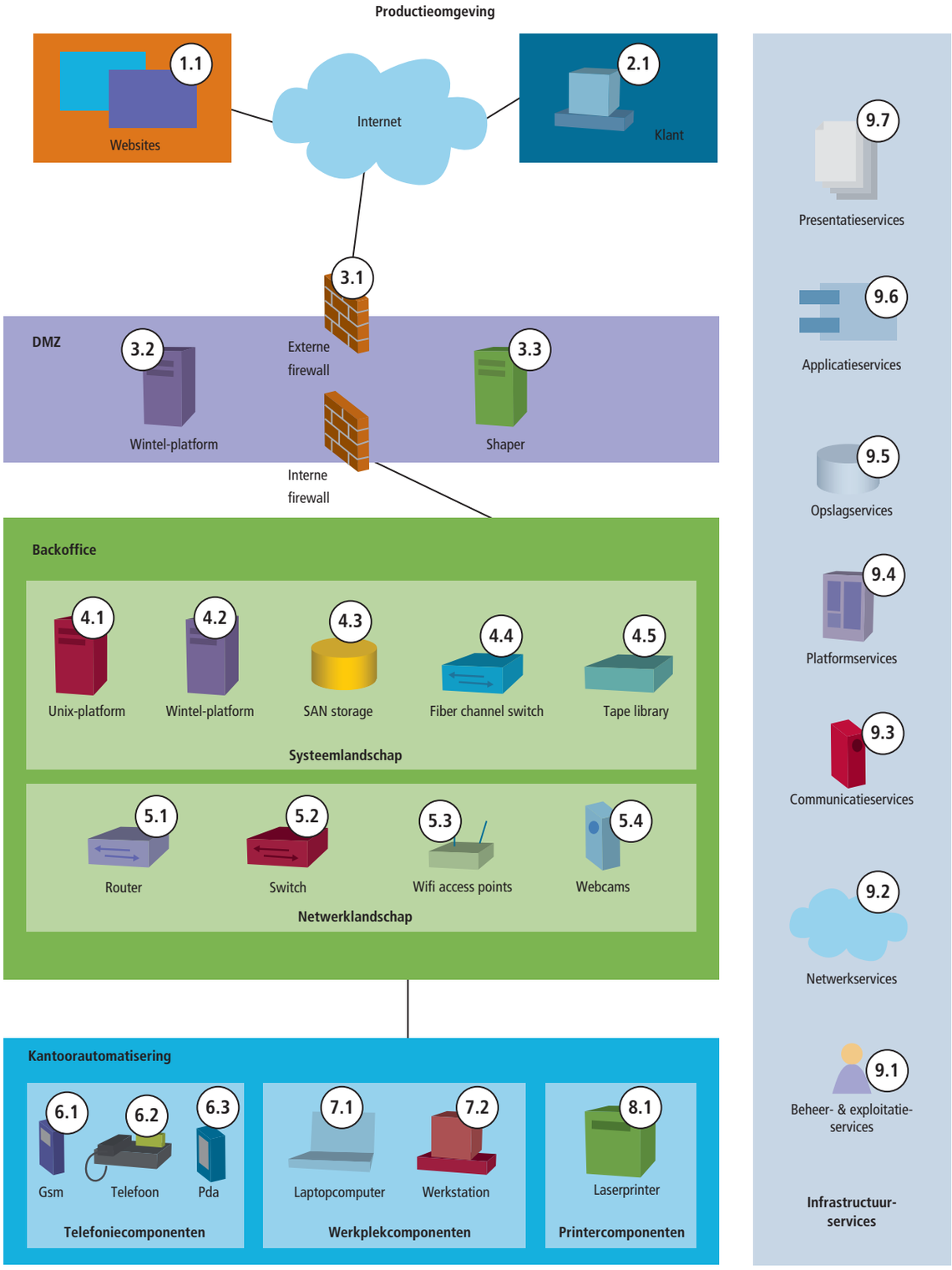
Figuur 3 Monitorlagenmodel

om een classificatie van te monitoren objecttypen te definiëren. Hierbij wordt meestal gekozen voor een opdeling in de volgende domeinen: procesdomein, applicatiedomein en infrastructuurdomein. Binnen elk domein zijn hiertoe unieke objecttypen gedefinieerd, zoals in figuur 4 is weergegeven voor het infrastructuurdomein.

Het monitordomein is opgedeeld in zones met een uniek nummer. Binnen elke zone is aan elk onderkend objecttype een uniek volgnummer toege-

TI01	**Door de monitorfunctionaliteit aan te laten sluiten op het niveau van de SLA-afspraken, wordt voorkomen dat de gebruikers perceptie van de gehaalde norm afwijkt van de meting.**
Toelichting	ITIL stelt terecht dat alleen meetbare normen in een SLA mogen worden opgenomen. Het begrip 'meetbaar' is echter rekbaar. Het is heel belangrijk om additionele voorwaarden aan de meting te stellen, zijnde: 1. Het abstractieniveau van de SLA-norm en de monitorfunctie moeten gelijk zijn. 2. De nauwkeurigheid van de SLA-norm moet overeenkomen met de monitoring. Daarom moeten in de SLA ook het meetinstrument en het meetvoorschrift worden benoemd.
Te beheersen risico's	De SLA-normen worden gehaald, maar de gebruiker is niet tevreden met het geleverde serviceniveau.
Indicatie van toepassing	Dit architectuurprincipe is van toepassing bij het selecteren van een nieuwe monitor-*tooling*, opschonen van het beheertoolportfolio en vaststellen van nieuwe SLA-normen.

ITB08-05_v4.indd 43 11-06-2008 11:49:40



Figuur 4 Infrastructuurmonitordomein

kend. Voor de andere twee monitordomeinen (proces en applicatie) is ook een dergelijke hiërarchische indeling toegepast. De voordelen hiervan zijn analoog aan die van het lagenmodel (praatplaat, decompositie, classificatie, fasering en referentie). Deze best practice is gebaseerd op architectuurprincipe TI03.

Prestatiemeting

Door in het functioneel ontwerp de relatie te onderkennen tussen het object en het type monitoring, kan op een een-

ITB08-05_v4.indd 44 11-06-2008 11:49:40

ID	Functioneel	SubID	Product	AVI	CAP	CAP	CAP	CAP	CAP	CAP	CAP	CAP	CAP
				Host Alive	CPU-belasting	RAM Utilisation	RAM Swap Space	Disk Partitie Free Space	Disk Partitie Available	Disk I/O	NIC Utilisation	NIC Broadcast	Netwerkbandbreedte
I3	DMZ												
I3.1	Firewall	I3.1.1	Extern xyz firewall	1	1	1	1	X	X	X	1	1	X
		I3.1.2	Intern xyz firewall	1	1	1	1	X	X	X	1	1	X
I3.2	Wintel-platform	I3.5.1	Windows NT	2	3	3	3	3	3	3	3	3	X
		I3.5.2	Windows 2000/2003	2	3	3	3	3	3	3	3	3	X
		I3.5.3	Hardware	2	1	1	1	1	1	1	1	1	X
I3.3	Shaper	I3.2	Packeteer	2	1	1	1	X	X	X	1	1	1
I4	Systeemlandschap												
I4.1	Unix-platform	I4.1.1	RS/6000 AIX	2	4	4	4	4	4	4	4	4	X
I4.2	Wintel-platform	I4.2.1	Windows NT	2	3	3	3	3	3	3	3	3	X
		I4.2.2	Windows 2000/2003	2	3	3	3	3	3	3	3	3	X
		I4.2.3	Hardware	2	1	1	1	1	1	1	1	1	X
I5	Netwerklandschap												
I5.1	Routers	I5.1.1	Cisco xyz	2	1	1	1	1	1	1	1	1	1
I5.2	Switches	I5.2.1	Cisco xyz	2	1	1	1	X	X	X	X	X	1

1 = SNMP get
2 = Ping
3 = RPC

Figuur 5 Functioneel ontwerp

voudige wijze de monitorbehoefte worden vastgelegd.

Tevens kan in deze matrix het meetprotocol worden aangegeven waarmee de meting verricht kan worden. In figuur 5 is dit gedaan met de nummers 1, 2, 3 en 4. Op deze manier ontstaat ook een gevoel van compleetheid. Deze is niet waterdicht, maar geeft wel veel houvast.

IST & SOLL

Bij het vergelijken van de toolfunctionaliteit is het handig om van elke tool eerst te bepalen welke monitorfunctionaliteit wordt ondersteund, zoals in figuur 6 is weergegeven. De derde reeks kolommen met het label 'IST Situatie' geeft de huidige invulling van het portfolio van beheertools aan. De vierde reeks kolommen met het label 'SOLL' geeft de gewenste situatie aan.

Duidelijk is te zien dat de geselecteerde tool de meeste monitorfunctionaliteit van de overige tools kan overnemen.

Toch zal in de praktijk deze functionaliteit niet altijd 100 procent dekkend zijn. Bijvoorbeeld door het eenvoudigweg ontbreken van functionaliteit van de primaire monitortool. Er zijn echter meer oorzaken waardoor niet één tool overblijft. Zo is in de SOLL-situatie tool D gekozen terwijl deze functionaliteit bij de geselecteerde tool ook aanwezig is. Tool D kan gekozen worden in geval van:

- punt 1: een specifieke monitortool die als collector (verzamelaar) wordt gebruikt voor de primaire tool;
- punt 2: een primaire tool die de functionaliteit wel biedt maar niet voor alle objecttypen (figuur 7);
- punt 3: een primaire tool die punten 1 en 2 ondersteunt, maar niet voor bepaalde prestatie-indicatoren (figuur 7);
- punt 4: een primaire tool die punten 1, 2 en 3 ondersteunt, maar niet voor het vereiste monitorprotocol (figuur 7).

Daarom is het verstandig om de portfolioanalyse te verdiepen, zoals in figuur 7 is weergegeven. In deze figuur zijn de beheertools namelijk uitgezet tegen de monitorobjecttypen. Hierbij is in de relatie aangegeven welke klassen van prestatie-indicatoren mogelijk zijn. Toch zitten ook hier nog risico's aan. De ideale mapping is gebaseerd op de in het functioneel ontwerp aangegeven gewenste functionaliteit zoals in figuur 5.

TI03	**Door alle te monitoren objecten te classificeren en voor elke klasse zo veel mogelijk één monitortool te selecteren, kan de diversiteit aan tools beperkt blijven en wordt een consolidatie van monitorinformatie verkregen.**
Toelichting	In de praktijk zal niet ontkomen kunnen worden aan een pluriforme monitoring. De redundantie kan beperkt worden door een analyse van te monitoren objecten, de te meten prestaties en de door de monitortools geboden functionaliteit.
Te beheersen risico's	• Alle ICT-producten die betrokken zijn bij een SLA-norm worden gemeten, maar de consolidatie van de monitorinformatie kost erg veel tijd en dus geld. • Er wordt te veel betaald aan licentiekosten door een hoge mate van onnodige monitorredundantie. • Door de onoverzichtelijkheid van vele monitortools en ICT-producten wordt vergeten om de monitoring van ICT-producten in te regelen.

Lessons learned

1. Bij het schonen van het monitortool-portfolio moet niet vergeten worden dat tools ook gebruikt worden voor de ondersteuning van het dagelijks (operationeel) beheer. Hoewel een tool niet meer gebruikt wordt voor monitoring moeten er toch nog licenties betaald worden voor het operationele beheer.
2. De mogelijkheden van monitoring zijn praktisch oneindig. De gewenste hoeveelheid prestatie-indicatoren, de te meten objecten en het meetinter-

ITB08-05_v4.indd 45 11-06-2008 11:49:40

		Tool A	Tool B	Tool C	Tool D	Tool E	Tool F	Tool G	Tool H	Tool I	Tool J	Tool K	Tool L	Tool M	Tool D	Tool M
1	Systeemmonitor	IST-situatie													SOLL	
1.1	Resourcemonitor	Y	Y	Y	D	Y	Y	Y	Y	N	Y	Y	D	N	D	Y	Y	D
1.2	Servicemonitor	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	D	N	Y	Y	N
1.3	Eventmonitor	Y	Y	N	N	N	Y	Y	Y	N	N	Y	N	N	N	Y	N	N
2	Applicatiemonitor																	
2.1	Infrastructuurservice protocol monitor	Y	Y	N	N	N	N	Y	N	N	N	N	Y	N	N	Y	N	Y
2.2	Applicatie-interfacemonitor	Y	N	N	N	N	Y	Y	N	N	N	N	?	?	?	Y	N	?
3	Koppelingen																	
3.1	Export / import functionaliteit	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y
3.2	System management - Service	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y
3.3	Alarmeringsystemen	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y
4	Rapportage																	
4.1	Trendanalyse	Y	Y	Y	N	N	Y	Y	N	N	Y	N	?	Y	Y	D	N	Y
4.2	Performance	Y	Y	Y	N	N	Y	Y	D	N	N	Y	Y	Y	Y	D	N	Y
4.3	SLA-bewaking	Y	Y	N	N	N	Y	Y	N	N	N	N	N	N	Y	D	N	Y

Groen	Wordt gemeten	Y	Kan worden gemeten
Geel	Wordt deels gemeten	D	Kan deels worden gemeten
Rood	Wordt niet gemeten	N	Kan niet worden gemeten

Figuur 6 'Portfolio mapping' op functionaliteiten

ID	Resource	SubID	Product	Tool A	Tool B	Tool C	Tool D	Tool E	Tool F	Tool G	Tool H	Tool I	Tool J	Tool K	Tool L	Tool M
I3	DMZ															
I3.1	Firewall	I3.1.1	Extern xyz firewall	ABCP	X	BP	X	X	X	X	X	X	X	X	X	ABCP	X
		I3.1.2	Intern xyz firewall	ABCP	X	BP	X	X	X	X	X	X	X	X	X	ABCP	X
I3.2	Wintel-platform	I3.5.1	Windows NT	ABCP	X	BCP	BP	ABCP	X	X	X	X	X	X	X	X	X
		I3.5.2	Windows 2000/2003	ABCP	ABCP	BCP	BP	ABCP	B	X	P	X	X	X	X	X	X
		I3.5.3	Hardware	ABCP	BP	BCP	BP	X	X	X	X	X	X	X	X	X	X
I4	Systeemlandschap															
I4.1	Unix-platform	I4.1.1	RS/6000 AIX	ABCP	X	X	BP	ABCP	B	P	P	X	X	X	X	X	X
I4.2	Wintel-platform	I4.2.1	Windows NT	ABCP	X	BCP	BP	ABCP	X	X	X	X	X	X	X	X	X
		I4.2.2	Windows 2000/2003	ABCP	ABCP	BCP	BP	ABCP	B	X	P	X	X	X	X	X	X
		I4.2.3	Hardware	ABCP	BP	BCP	BP	X	X	X	X	X	X	X	X	X	X
I5	Netwerklandschap															
I5.1	Routers	I5.1.1	Cisco xyz	ABCP	X	P	X	X	X	X	X	X	X	X	ABCP	X	X
I5.2	Switches	I5.2.1	Cisco xyz	ABCP	X	P	X	X	X	X	X	X	X	X	ABCP	X	X

	Functionaliteiten
A	Auditing
B	Beschikbaarheid
C	Capaciteit
P	Performance
X	Geen

Figuur 7 Toolfunctionaliteit per infrastructuurobject

val moeten afgestemd worden op de behoefte die voortvloeit uit een SLA-afspraak.

3. Monitorwensen kunnen indruisen tegen zaken als beveiligingsbeleid. Neem voor de risicosessie in overweging welke beperkingen het beveiligingsbeleid oplegt.
4. Met het opschonen van de toolportfolio moet niet vergeten worden de menselijke factor te betrekken in het project, in de zin van betrokkenheid en opleidingen. De betrokkenheid kan bijvoorbeeld ingevuld worden door deelname van beheerders aan risicosessies, vaststellen van een PvE, acceptatiecriteria, en opstellen en uitvoeren van testplannen.
5. Het gebruik van architectuurprincipes en architectuurmodellen vergroot de risicobeheersing doordat de analyses completer worden (monitorlagenmodel, monitordomeinmodellen) en gericht zijn op de juiste aspecten van monitoring (keuze van monitorniveau et cetera).

Hierbij dank ik Roeland Kool, Louis van Hemmen en Said El Aoufi voor hun inspirerende bijdrage aan dit artikel en SPS in het algemeen voor het mogen publiceren van deze aanpak.

Drs. ing. B. de Best RI (bartb@qforce.nl).

Noten

1. 'Beheren onder architectuur', *IT Beheer* nr. 5 / 2007
2. 'Beheerarchitectuur in projecten', *IT Beheer* nr. 8 / 2007
3. 'Regie onder beheerarchitectuur', *IT Beheer* nr. 10 / 2007
4. 'Beheerarchitectuur heeft nog een lange weg te gaan', *IT Beheer* nr. 10 / 2007
5. *Acceptatiecriteria*, B. de Best ISBN 9039524998
6. *Ketenbeheer in de praktijk*, B. de Best, ISBN 9789012116633

ITB08-05_v4.indd 46 11-06-2008 11:49:41