COMPUTERWORLD

Windows XP services forklaret

Windows services kan godt være lidt af en jungel at finde rundt i, Hviske har man brug for, hvilke udgør en sikkerhedsrisiko og hvilke kan med fordel disables? Her er en oversigt. ARtiklen under udarbejdelse

Skrevet den **22. Feb 2009** af **bufferzone** I kategorien **Workstation / Windows XP** | ★★☆☆☆

Nedenstående tabel bør ikke ukritisk betragtes som en facitliste. Du bør tage stlling til hver enkelt service før du beslutter dig om den skal enables eller disables. Tabellen er et udtryk for min personlige holdning, hvor sikkerheden vejer tungt. Følgende generelle betragtninger er anvendt.

- Hvis en service ikke anvendes skal den mindst disables, heldst afinstalleres
- Hvis en services kun anvendes en gang imellem, bør den disables og kun enables i den tid den anvendes

Service	Beskrivelse	disable	koncekvens	Råd bemærkning
Alerter	Udsender ad-ministrative alarmer	Ja	Programmer der bruger disse vil ikke modtage nogle alarmer	Disable Ingen
Application Layer Gateway	Giver applikations- Level protokol plug-ins og enabler net- work/protocolconnec-tivity	Måske	MSN Messenge samt Windows Messenger og ligende programmer vil ikke virke	Bør kun enables Hvis en firewall er installeret
Application Managemen	Håndterer install, removal og enume-rations forespørg- ler for AD Intelli-Mirror group policy	Ja	IntelliMirror programmer vil ikke kunne bruges	Disable

	programmer			
Automatic Updates	Automatisk down-load og installarion af kritisk windows Sikkerhedsopdate-ringer	Ja	Sikkerhedsopdateringer vil ikke installeres automatisk, de kan dog installeres manuelt	Kan disables men bør enables, det vigtigste er at maskinen er fuldt opdateret
Background Intelligent Transfer	styre dataoverfør-sel mellem klient og server	Ja	Ting der kræver data-overførsel vil ikke virke ordentlig, f.eks windows update	se ovenfor
ClipBook	Muliggør at Clip-board vieweren kan dele informationer med remote maskiner	Ja	Clipboard vieweren kan ikke dele indhold med remote maskiner	Disable
COM+ Event System/System Application	Tillader management af Component Servi-ces via automatisk distripution af events til abonner-ende COM kombonenter	nej	System Event Notification vil ikke virke. Logon og logoff notofication vil ikke ske. Andre applika-tioner f.eks Volume Snap-Shot Service vil fejle	Enable
Computer Browser	Håndterer Browser listen og bruges af		Compute4ren kan ikke se de andre computere på	Hvis der skal deles filer og

	windows programmer til at se netværks domæner & ressourcer	ja	netværket	Enable ressourcer skal denne service enables
Cryptographic services	Indeholder følgende: Catalog Database Service (Fil Signatur), Protected Root Service (tilføjer og fjerner Trusted Root Certification Authority certifikater fra computeren) og Key Service (nødvendig for håndtering af certifikater	Nej	En meget væsentlig del af computerens sikkerhed vil ikke fungere ordentligt	Enable
DHCP Client	Håndterer DHCP og Dynamisk DNS	Måske	DNS vil ikke virke	Enable DNS ikke bruges Kan disables hvis
Distributed Link Tracking Client	sørger for at genveje og OLE-links virker selvom target flyttes eller renames via links i filsystemer.	ja	Link tracking vil ikke være til rådighed og andre computere vil ikke kunn tracke links på denne Computer	Disable
Distributed	Koordinere transak-		Distripuerede Transak-	

Transaction Coordinator Disable	tioner der spænder over flere ressource managers, f.eks. databaser, message queues og fil systemer	ja	tioner vil ikke kunne forekomme	
DNS Client	Opløser og cacher DNS navne. Nødvendig fpr at DNS fungerer	Nej	DNS vil ikke virke Kun IP adresser kan bruges	Enable
Error Reporting Disable	Håndterer fejlrappor tering i forbindelse med applikations crash	Ja	Kun kernel fejl og visse typer af User Mode fejl vil blive rapporteret	
Event Log	Håndterer event vieweren	Nej	Event vieweren vil ikke Virke	Enable
Fast User Switching Compatibility miljø	Håndterer management for applikationer ikke i et domæne der har behov for støtte i et fler- bruger miljø	Ja	Fast User Switching vil ikke være til rådighed	Virker alligevel
Help and Support Disable	Håndterer hjælp og support i windows	Ja	Windows hjælp og support center vil ikke være til	

| | | | |rådighed | |
| | |

HID Input Nogle keyboards med Hot buttons Disable	Håndterer Human Interface Devices. Aktivere predifine- vil ikke virke rede Hot Buttons, Remote controles og andre multimedia devices	Måske	Hot Buttons vil ikke virke		

IMAPI CD- Diasble hvis der Burning COM ikke findes en CD	Håndtere CD brænding med Image Mastering Applications Program ming Interface	Måske	CD brænder vil ikke virke	Enable	

Indexing Denne service bør Service Disable	Índexere indhold og properties af filer afinstalleres på lokale og remote computere	ja	Filer vil ikke blive indexseret	

Internet Installer en Connection - anden firewall Firewall(ICF) Disable Sharing(ICS) god nok	Håndterer network address translation (NAT), Navne opløs- denne er ikke ning og intrusion prevention services	Måske	Internet sharing, name resolution og firewall vil ikke virke	

IPSEC Hvis du bruger services	Håndterer IPSec support til VPN	Måske	IPSec baseret VPN vil ikke virke	

|Disable|SEC baseret VPN |
|så enable denne |

|Logical Disk Manager|Håndterer dynamiske disk informationer tilsluttes nye diske sendes nødvendige data til LDM admini- strative service|ja|Nytilsluttede diske vil ikke automatisk blive opdaget af windows|enable|Kan sagtens dis- ables hvis du forventer at til- flere nye diske|

|Logical Disk Manager Disable|Håndterer disk og partitions konfigura tion af nye diske|Ja|Startes automatisk når der er behov derfor|Måske stående service Administrative service|

|Machine Debug Manager|Håndterer Visual Studio debugging|Ja|Visual Studio debugging vil ikke virke|Disable|

|Messenger Har inter med|Håndterer Alerter service og net send|Ja|Net send vil ikke virke|Disable|Messenger at gøre|
| | beskeder mellem server og klienter | | | |

|Microsoft Disable hvis du Software Disable|Håndterer software- baseret shadow|Ja|volume shadow copies vil ikke virke|ikke ønsker at Shadow Copy anvende Shadow Provider copies|copies af Volume Shadow Copy service|

NetMeeting Remote Desktop Sharing	Tilader en autoriseret bruger at tilgå computeren remotely via NetMeeting	Ja	Remote Desktop sharing via NetMeeting vil ikke virke	NetMeeting udgør en sikkerheds-risiko
Network Connections	Håndterer dial-up connections for servere herunder network status notification og konfiguration	Nej	Network konfiguration vil ikke virke, Andre services vil også fejle	Enable
Network DDE	Håndterer network transport og sikkerhed for Dynamic Data Exchange (DDE)	Ja	DDE transport og sikkerhed vil ikke virke	Disable
Network DDE DSDM	Håndterer Dynamic Data Exchange (DDE) network shares	Ja	DDE Netvwork shares vil ikke virke	Disable
Network	En del af ICS		ICF og ICS vil ikke virke	Enable hvis ICF bruges
Location Awareness (NLA)	Håndtere konfigurations- og placeringsoplysninger	Måske		Disable
NT LM	Håndterer NT 4.0		NT 4.0 klienter vil ikke	

|bør kun enables |
|Security |(pre win 2000) logon|Disable|kunne logge på
|disable|hvis NT 4.0 klien|
|Support | | | |
|ter skal logge på|
|Provider | | | |
| |

|Performance |Håndterer logging og| |Performance data vil ikke |
| |
|Logs and |Displaing af perfor | Ja |blive logget
|Disable| |
|Alerts |mance data | | |
| |

|Plug and Play |Håndterer Plug and | |Plug and Play vil ikke |
| |
| |Play | Nej |virke |Enable
| |

|Portable |Håndterer serienumre| |beskyttet materiale vil |
| |
|Media Serial |til externe media | Ja |ikke altid kunne
downloade|Disable| |
|Number |players | | |
| |

|Print Spooler |Håndterer print jobs| |man vil ikke kunne printe |
|Kan disables |
| |og network print | Nej | |Enable
|hvis maskinen |
| |queues | | |
|ikke skal printe |

|Protected |Håndtere beskyttelse| |De beskyttede informatio- |
| |
|Storage |af følsomme informa-| Ja |ner vil være utilgænge |Enable
| |
| |tioner, f.eks. | |lige |
| |
| |private keys | | |
| |

|QoS RSVP |Håndterer network | |QoS-aware applikationer |
| |
| |signaling, trafik | ja |vil ikke virke ordentligt
|Disable| |
| |kontrol og setup for| | |
| |

	QoS-aware applikatio ner			
Remote Access Auto Connection Manager	Håndterer remote access. Finder alternativer ved mislykkedes connection forsøg	Ja	brugere må connecte manuelt til andre systemer	Enable
Remote Access Startes On-Demand Connection af Remote Access Manager	Håndterer Dial-up og VPN forbindelser	Måske	Operativsystemet fungere ikke ordentligt	Enable
Remote Desktop Help Session Disable Manager	Håndterer Remote Assistance	Ja	Remote Assistance vil ikke virke	
Remote Procedure Call (RPC)	håndterer RPC name service	Nej	Flere OS komponenter vil ikke fungere ordentligt Exchange og andre tredie- parts utils vil ikke virke	Enable
Remote Registry bør ikke Registry Disable remote. Enable ved behov	Håndterer remote management af system kunne tilgås registry	Ja	Hfnetchk, patch utility og tilsvarende applikatio- ner vil ikke virke	
Removable	Håndterer flytbare		applikationer og systemer	

Enable hvis flyt				
Storage	medier og automatisk	Ja	der bruger flytbare medier	Disable
	afbrydelse af disse		vil virke langsomt	
	medier anvendes			
Routing og	Håndterer multiproto		Routing og Remote Access	Undlad at instal
Remote	kol LAN-to-LAN, LAN-	Ja	vil ikke virke	Disable
Access	to-WAN, VPN og NAT			
	routing services			
	lere denne servi			
	ce vil muligt			
Secondary	Håndterer "RUN AS"	Ja	Run AS vil ikke virke	Disable
Logon				
	Enable ved behov			
Security	Håndterer account		services der kræver ad-	Hvis DHCP ikke
Accounts	informationer for		gang til SAM vil ikke	
Manager	de lokale security	Ja	virke. F.eks. GPO	Enable
	accounts og dermed		kan fejle	
	services afgang til			
	SAM			
	anvendes kan den- ne service dis- ables			
Server	Håndterer fil og		Fil og print, RPC	Enable hvis du
	print deling samt	Ja	requests samt pipe	
	fil deler			Disable
	pipe communication		kommunikation vil ikke	
			virke	
Shell Hardware	Håndterer notifika		CD-rom og andre devices	
Detection	tion for AutoPlay	Ja	vil ikke virke	Enable
	hardware events		automatisk	

Smart Card Enable hvis smart Disable	Håndterer adgang til smart Cards Cards anvendes	Ja	Smart Cards vil ikke kunne læses
Smart Card Helper Disable	Håndterer adgang til ældre Smart Cards	Ja	Ældre smart Cards vil ikke kunne læses
SSDP Discovery Disable	Håndterer sammen med Universal Plug and Play Device Host UPnP devices	Ja	UPnP devices vil ikke virks
System Event Bærbare kan Notification Disable	Håndterer Event Log notificere COM+ sub-enable denne scribers om Logon og power-relaterede events	Ja	Noticificering og synchronisering vil virke
System Restore Enable hvis der Disable	Håndterer system restore herunder ændres meget ved genskabelses punkter	Ja	Automatisk system gendan- nelse vil ikke virke systemet
Task Scheduler Enable kun ved Disable	Håndterer schedule- ring af opgaver behov	Ja	schedulering vil ikke virke
TCP/IP NetBIOS Enable kun ved Helper Disable	Håndterer NetBIOS over TCP/IP og ved behov NetBIOS name lookups	Ja	NetBIOS over TCP/IP samt deling af ressourcer vil ikke virke

	bruges af GPO			
	software distribu.			

Telephony	Håndterer Telephony		TAPI applikationer vil	
	API (TAPI) herunder	Ja	virke dårligt	
Disable				
	IP-based voice			

Telnet	Håndtere TelNet	Ja	TelNet vil ikke virke	
Disable				

Terminal	Håndterer windows		Terminal services	
Services	Terminal. bruges af		vil ikke virke	
	Remote Desktop, Fast	Ja		
Disable				
	User Switching, Re-			
	mote Assistance og			
	Terminal Server			

Themes	Håndterer theme		theme kan ikke bruges	
Disable				
	Management	Ja		

Uninterruptibl	Håndterer UPS manage		UPS management kan	
e Power Supply	ment	Ja	ikke gennemføres	
Disable				

Universal Plug	Bruges sammen med		uPnP devices kan ikke	
and Play Device	SSDP Discovery ser-	Ja	findes på nettet	
Disable				
Host	vice			

Upload Manager	Håndterer synchron		Nogle former for fil	
	og asynchron fil-	Ja	overførsel vil ikke	

Disable				
	overførsel		virke	

Volume Shadow Copy Disable	Håndterer Volume shadow copies	Ja	Shadow copies vil ikke virke	

WebClient Disable	Giver Windows-baserede programmer mulighed for at oprette, tilgå og modificere web baserede filer	Ja	Web baserede filer kan ikke tilgås	

Windows Audio Disable	Håndterer audio devices	Ja	Audio devices vil ikke virke ordentligt	

Windows Image Acquisition(WIA) Disable	Håndterer billedoverførsel fra kamera eller scanner	Ja	Billedoverførsel vil ikke virke	enable hvis anvendes

Windows Installer	Håndterer MSI pakker	Ja	Installering vil give problemer	Enable

Windows Management Instrumentation (WMI)	Håndterer system management informa-tion. Bruges til implementering af performance alerts	Nej	performance alerts vil ikke virke	Enable

WMI Driver Extensions	Håndterer alle drev og event trace providers konfigureret til WMI eller event trace information	Ja	extension til WMI virker ikke	Enable
Windows Time Brug altid NTP i et netværk miljø	Bruger NTP til tidssynchronisering	Ja	NTP vil ikke virke	Enable
Wireless Zero Configuration	Wifi Plug'n Play	Ja	Wifi plug'n play vil ikke virke	Enable hvis Wifi Disable anvendes
WMI Performance Adapter	Håndterere performance library information fra VMI	Ja	startes når Performance Data Helper startes	Enable
Workstation	Håndterer Microsoft Network services	Ja	Computeren vil ikke kunne tilgå netværks ressourcer	Enable

Tillæg til denne artikel kan findes gratis her

http://www.eksperten.dk/artikler/737

Kommentare og forslag modtages som sædvaneligt med kyshånd. Spørgsmål er også velkomne, både på eksperten og på kim@bufferzone.dk. Undlad venligst at stille spørgsmål i artiklens kommentare, dem kan jeg jo ikke besvare

Kommentar af snowball d. 16. Jul 2005 | 1

En OK liste, men det bør fremgå at navnene er taget fra en engelsk WinXP, og du bør efter min mening bestemme dig for om du vil holde dig til engelske eller dansk udtryk i artiklen - det er ikke så kønt at blande det hele sammen. Du bør desuden selv gennemlæse artiklen og/eller køre en stavekontrol på den da der er mange stave- / tastefejl.

Kommentar af nanoq d. 15. Aug 2005 | 2

En god og nyttig artikel.

Jeg forstår ikke, hvorfor wickedd giver dårlig karakter, for en så god og nyttig information. At artiklen ligner noget der allerede eksisterer, er da ligegyldigt. Faktisk vil langt størsteparten af artikler på Eksperten, ligne noget der eksisterer i forvejen, alene i kraft af det ENORME antal artikler der findes på internettet.

Kommentar af lenk d. 05. Aug 2005 | 3

Endnu en nyttig artikel som XP brugere bør kikke på. Selvom man kan negelsk, er fagsproget når man taler om services ofte lidt svært, det letter det hele en del at det er på dansk

Kommentar af barbarbo d. 02. Aug 2005 | 4

Dejligt med en brugbar oversigt på dansk og med tillæget har man faktisk mulighed for at styre sine services som man ønsker. At skemaet ligner andre på nettet er vel ganske naturligt, det er jo de samme services der er tale om så det kan vel ikke være meget anderledes

Kommentar af serverservice d. 21. Apr 2006 | 5

Der er en del services man lige bør overveje om de bør disables.
Alerter, Netbios, Logical disk management, System event notification oa.
Artiklen virker lidt nem og ikke så gennemarbejdet som normalt fra bufferzone.

Kommentar af wickedd d. 27. Jul 2005 | 6

Ligner den her lidt for meget: http://www.majorgeeks.com/page.php?id=12

Kommentar af wollsen (nedlagt brugerprofil) d. 09. Nov 2005 | 7

nice, god og nyttig info!

Kommentar af jensen5 d. 31. Jul 2005 | 8

Kommentar af michaelthr d. 03. Nov 2005 | 9