

ISA Server 2004 – Protokollierung - Von Marc Grote

Die Informationen in diesem Artikel beziehen sich auf:

- ? Microsoft ISA Server 2004

Im Artikel [Übersicht Monitoring](#) wurde eine Zusammenfassung aller Überwachungsfunktionen des ISA Server 2004 gegeben. Das vorliegende Kapitel beschreibt die Möglichkeit, die Protokollierungsfunktionen des ISA Server 2004 zu konfigurieren.

Einleitung

ISA Server 2004 protokolliert die Aktivität auf dem ISA Server-Computer. Diese Protokollierungen werden zum Erkennen von Sicherheitsverletzungen, zum Generieren von Berichten und zur Problembehandlung bei Netzwerkproblemen verwendet. Sie können festlegen, welche Informationen in den Protokollierungen in welchem der folgenden Formate gespeichert werden. Es stehen zur Auswahl:

- ? Datei
- ? SQL
- ? MSDE

In der Protokollanzeige kann die Firewallprotokollierung und/oder die Webproxyprotokollierung angezeigt werden. Sie können die derzeit im Protokollrepository gespeicherten Onlineprotokollierungen anzeigen oder das Repository abfragen, um frühere Protokollierungen abzurufen. In beiden Modi können Sie Filter definieren, um die angezeigte Datenmenge zu begrenzen und übersichtlichere Auswertungen definieren zu können.

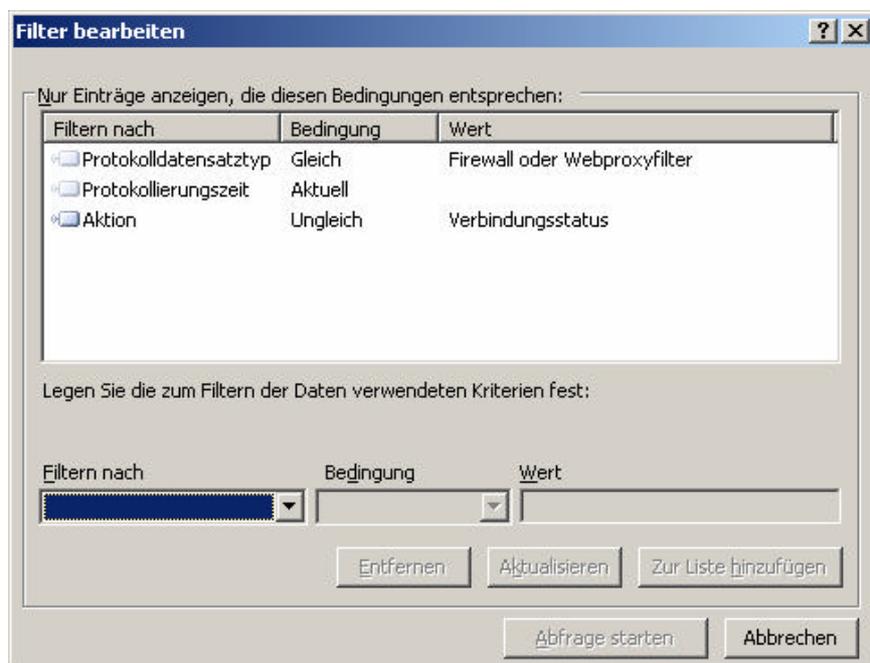


The screenshot shows the Microsoft Internet Security & Acceleration Server 2004 management console. The window title is "Microsoft Internet Security & Acceleration Server 2004". The interface includes a menu bar with "Datei", "Aktion", and "Ansicht". Below the menu is a navigation pane on the left showing a tree view with "proxy-hv-01" expanded, containing "Überwachung", "Firewallrichtlinie", "Virtuelle private Netzwerke (VPN)", and "Konfiguration". The main area displays the "Protokollierung" (Logging) configuration page. The page has a header with "Microsoft Internet Security & Acceleration Server 2004 Standard Edition" and "Überwachung von [redacted]". Below the header are tabs for "Übersicht", "Alarme", "Sitzungen", "Dienste", "Berichte", "Konnektivität", and "Protokollierung". The "Protokollierung" tab is active, showing a table with columns "Filtern nach", "Bedingung", and "Wert". The table contains three rows of filter rules:

Filtern nach	Bedingung	Wert
Protokolldatensat...	Gleich	Firewall oder We...
Protokollierungszeit	Aktuell	
Aktion	Ungleich	Verbindungsstatus

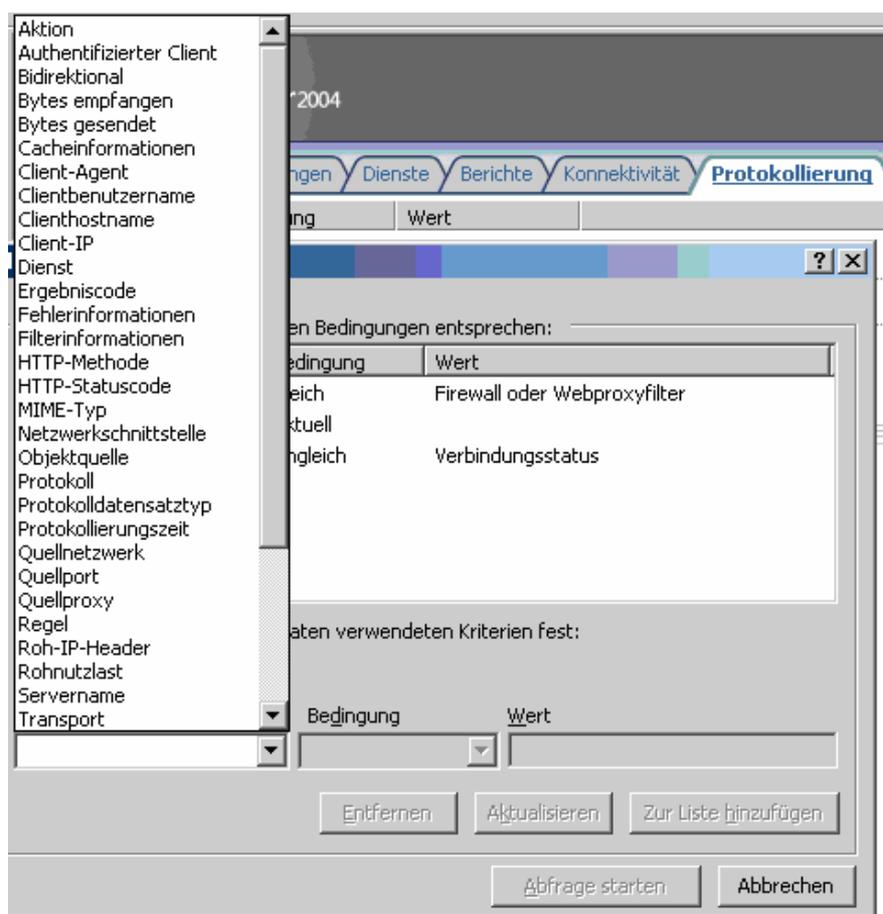
Below the table, there are instructions: "Klicken Sie auf [Abfrage starten](#), um eine neue Abfrage zu starten." and "Klicken Sie auf [Filter bearbeiten](#), um einen Filter zu erstellen und eine neue Abfrage zu starten."

Der Standard Abfrage Filter filtert nach dem Protokoll Datensatztyp = Firewall- oder Webproxyfilter, der Anzeige der Daten in Echtzeit und nach jedem Verbindungsstatus.



Sie können den Filter modifizieren, indem Sie im Standard-Filter unter *Filtern nach* den Filtertyp auswählen und dann anpassen.

Sie können auch einen eigenen Filter erstellen, indem Sie unter Filtern nach einen Filter auswählen. Es stehen zahlreiche Filtermöglichkeiten zur Verfügung. Eine Übersicht über die Filtermöglichkeiten zeigt das nächste Bild.



Nachdem Sie einen Filtertyp ausgewählt haben (in diesem Beispiel Client-IP) können Sie noch eine Bedingung zur Filterung hinzufügen.

Achtung: Die zur Verfügung stehenden Filter Bedingungen sind immer abhängig von der Filterart (Filtern nach). In diesem Beispiel ist die Filterart Client-IP und für diese Filterart stehen die Bedingungen *Gleich*, *Größer oder gleich*, *Kleiner oder gleich* und *Ungleich* zur Verfügung.

The screenshot shows the 'Filter bearbeiten' dialog box. At the top, it says 'Nur Einträge anzeigen, die diesen Bedingungen entsprechen:'. Below this is a table with three columns: 'Filtern nach', 'Bedingung', and 'Wert'. The table contains three rows: 'Protokolldatensatztyp' with 'Gleich' and 'Firewall oder Webproxyfilter', 'Protokollierungszeit' with 'Aktuell', and 'Aktion' with 'Ungleich' and 'Verbindungsstatus'. Below the table, it says 'Legen Sie die zum Filtern der Daten verwendeten Kriterien fest:'. There are three input fields: 'Filtern nach' (set to 'Client-IP'), 'Bedingung' (with a dropdown menu open showing options: 'Gleich', 'Größer oder gleich', 'Kleiner oder gleich', 'Ungleich'), and 'Wert' (empty). There are buttons for 'Aktualisieren', 'Zur Liste hinzufügen', 'Abfrage starten', and 'Abbrechen'.

Filtern nach	Bedingung	Wert
<input type="checkbox"/> Protokolldatensatztyp	Gleich	Firewall oder Webproxyfilter
<input type="checkbox"/> Protokollierungszeit	Aktuell	
<input checked="" type="checkbox"/> Aktion	Ungleich	Verbindungsstatus

Legen Sie die zum Filtern der Daten verwendeten Kriterien fest:

Filtern nach: Client-IP
Bedingung: Gleich
Wert:

Buttons: Aktualisieren, Zur Liste hinzufügen, Abfrage starten, Abbrechen

Als *Wert* wurde in diesem Beispiel die IP-Adresse 192.168.1.111 eingegeben. Zum Abschluss müssen Sie noch auf *Zur Liste hinzufügen* klicken, damit der neue Filter zur Filterbedingung hinzugefügt wird und auf *Abfrage starten* klicken.

The screenshot shows the 'Filter bearbeiten' dialog box after the filter condition has been added. The table now has four rows: 'Protokolldatensatztyp' with 'Gleich' and 'Firewall oder Webproxyfilter', 'Protokollierungszeit' with 'Aktuell', 'Aktion' with 'Ungleich' and 'Verbindungsstatus', and 'Client-IP' with 'Gleich' and '192.168.1.111'. The 'Client-IP' row is highlighted. Below the table, it says 'Legen Sie die zum Filtern der Daten verwendeten Kriterien fest:'. There are three input fields: 'Filtern nach' (set to 'Client-IP'), 'Bedingung' (set to 'Gleich'), and 'Wert' (set to '192 . 168 . 1 . 111'). There are buttons for 'Entfernen', 'Aktualisieren', 'Zur Liste hinzufügen', 'Abfrage starten', and 'Abbrechen'.

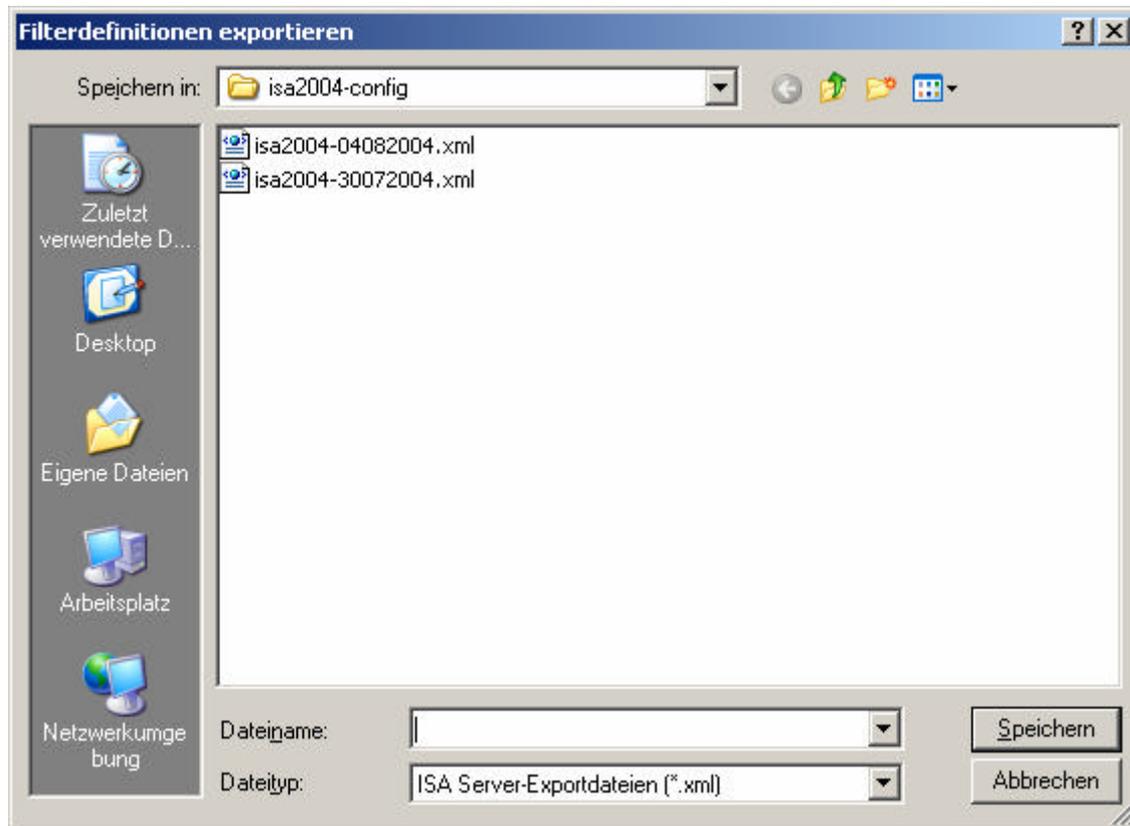
Filtern nach	Bedingung	Wert
<input type="checkbox"/> Protokolldatensatztyp	Gleich	Firewall oder Webproxyfilter
<input type="checkbox"/> Protokollierungszeit	Aktuell	
<input checked="" type="checkbox"/> Aktion	Ungleich	Verbindungsstatus
<input checked="" type="checkbox"/> Client-IP	Gleich	192.168.1.111

Legen Sie die zum Filtern der Daten verwendeten Kriterien fest:

Filtern nach: Client-IP
Bedingung: Gleich
Wert: 192 . 168 . 1 . 111

Buttons: Entfernen, Aktualisieren, Zur Liste hinzufügen, Abfrage starten, Abbrechen

Einmal definierte Filteroptionen können exportiert und auch wieder importiert werden. Dieses Feature ist sehr hilfreich, weil sich der Administrator damit eine Sammlung an Filterdefinitionen erstellen kann, welche in einem bestimmten Verzeichnis gespeichert werden und dann bei Bedarf importiert werden können. Somit stehen dem Administrator fertige Vorlagen zur Verfügung mit welchem er die Protokolldaten filtern kann.



Der ISA Server 2004 zeigt jetzt in „Echtzeit“ die Protokoll Daten, basierend auf Ihrer Filterdefinition an.

Übersicht Alarme Sitzungen Dienste Berichte Konnektivität Protokollierung					
Filtern nach	Bedingung	Wert			
Protokolldatensat...	Gleich	Firewall oder We...			
Protokollierungszeit	Aktuell				
Aktion	Ungleich	Verbindungsstatus			

Prot...	Ziel-IP	Zielport	Protokoll	Aktion	Regel
20.08.2004 ...	[redacted]	8080	Nicht identifizierter IP-Datenv...	Getrennte Verbindung	
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	http	Zugelassene Verbindung	IT-Abteilung
20.08.2004 ...	[redacted]	80	HTTP	Getrennte Verbindung	
20.08.2004 ...	[redacted]	8080	Nicht identifizierter IP-Datenv...	Getrennte Verbindung	

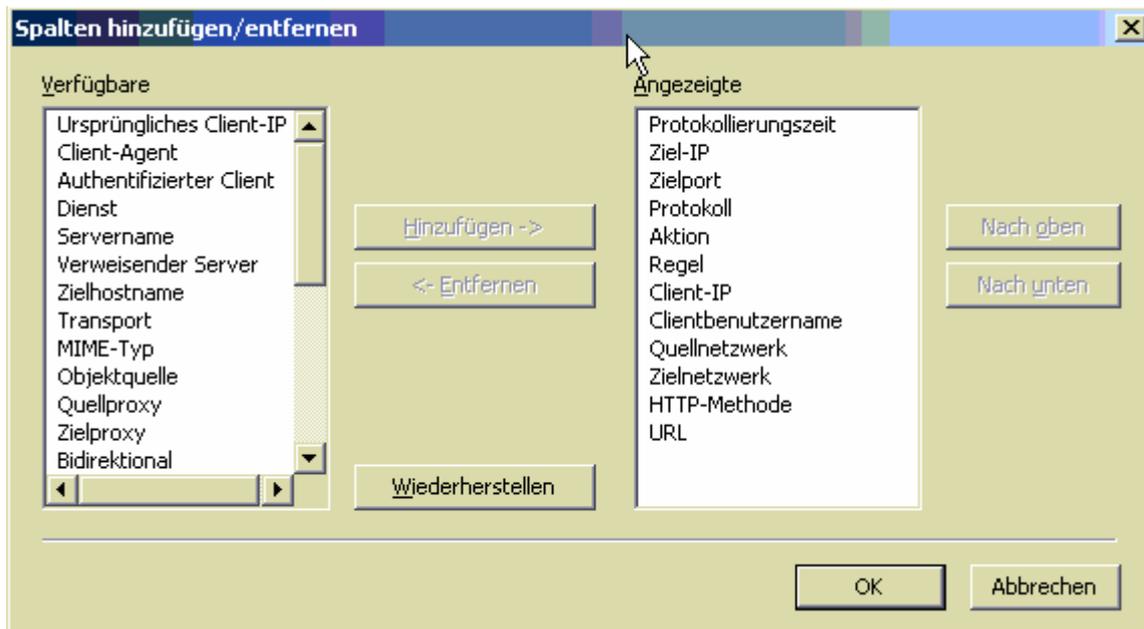
Mit einem Rechtsklick mit der Maus im Protokollfenster können Sie die *aktuelle Abfrage beenden* oder den *Filter bearbeiten*.

Übersicht Alarme Sitzungen Dienste Berichte Konnektivität Protokollierung					
Filtern nach	Bedingung	Wert			
Protokolldatensat...	Gleich	Firewall oder We...			
Protokollierungszeit	Aktuell				
Aktion	Ungleich	Verbindungsstatus			

Prot...	Ziel-IP	Zielport	Protokoll	Aktion
20.08.2004 ...	[redacted]	80	HTTP	Getrennt
20.08.2004 ...	[redacted]	80	HTTP	Initiierte
20.08.2004 ...	[redacted]	80	http	Zugelass
20.08.2004 ...	[redacted]	80	HTTP	Getrennt
20.08.2004 ...	[redacted]	80	HTTP	Initiierte
20.08.2004 ...	192...	80	http	Zugelass
20.08.2004 ...	[redacted]	80		Zugelass
20.08.2004 ...	[redacted]	80	HTTP	Getrennt
20.08.2004 ...	[redacted]	8080	Nicht identifizierter IP-Datenv...	Initiierte
20.08.2004 ...	[redacted]	8080	Nicht identifizierter IP-Datenv...	Initiierte

Filter bearbeiten
Abfrage beenden

Sie können dem Protokollfenster zusätzliche Spalten Hinzufügen/Entfernen, sowie den Ursprungszustand *Wiederherstellen*.

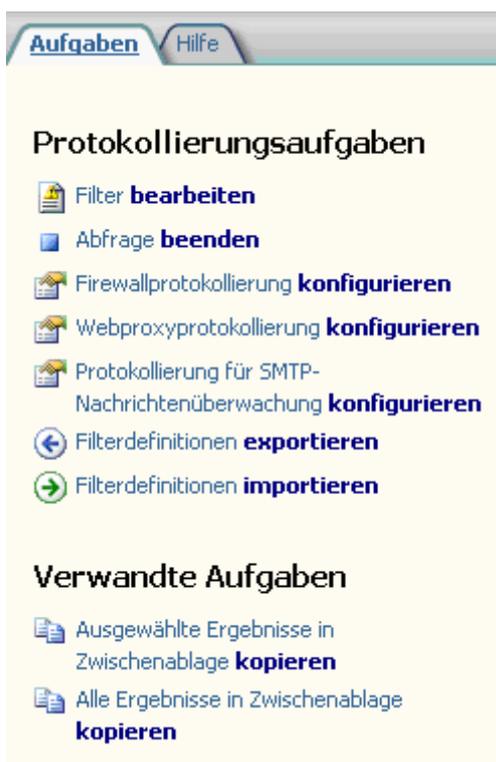


Nachdem wir uns um die Anzeige der Protokolldaten und deren Filterung gekümmert haben, gehen wir jetzt zur Konfiguration der Protokollierung über.

Der ISA Server 2004 bietet die Möglichkeit eine ...

- ? Firewallprotokollierung
- ? Webproxyprotokollierung und
- ? SMTP Nachrichtenüberwachungsprotokollierung

einzurichten.



Folgende Protokollspeicherformate stehen zur Verfügung:

- ? MSDE-Datenbank
- ? Datei
 - W3C-Protokollierungsformat
 - ISA-Server Dateiformat
- ? SQL Datenbank über ODBC

Der Firewall- und Webproxydienst protokollieren die Daten per Default in eine MSDE Datenbank.

Bei der MSDE (Microsoft SQL Server Desktop Engine) handelt es sich um eine kostenlose, funktionsreduzierte Datenbank aus dem Hause Microsoft. Für mehr Informationen über die MSDE sei auf folgende Webseite verwiesen:

<http://www.microsoft.com/sql/msde/>

Bemerkung: Während der Installation des ISA Server 2004 wird eine MSDE Datenbank installiert.

Die SMTP Nachrichtenüberwachungsprotokollierung erfolgt per Default im erweiterten W3C Nachrichtenformat.

Im folgenden Bild sehen Sie die Möglichkeit das Protokollspeicherformat auszuwählen.

Eigenschaften von Firewallprotokollierung

Protokollierung | Felder

Protokollspeicherformat auswählen:

MSDE-Datenbank

Namensformat: ISALOG_yyyymmdd_FWS_nnn.mdf

Datei

Namensformat: ISALOG_yyyymmdd_FWS_nnn.w3c

Format:

SQL-Datenbank

ODBC-Datenquellennamen (DSN):

Tabellenname:

Dieses Konto verwenden:

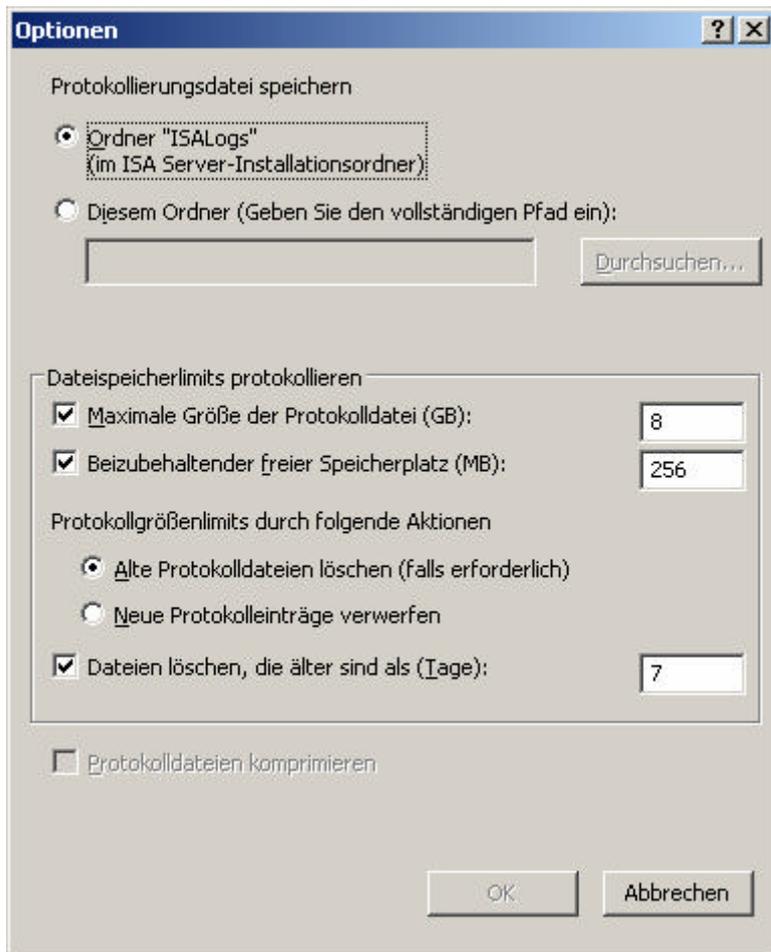
Protokollierung für diesen Dienst aktivieren

Aktivieren Sie im Systemrichtlinien-Editor die entsprechenden Remoteprotokollierungs-Konfigurationsgruppen, um ein Protokoll remote in einer Datei oder SQL-Datenbank zu erstellen.

Achten Sie darauf, dass der Haken bei *Protokollierung für diesen Dienst aktivieren* aktiv ist. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden keine Ereignisse protokolliert.

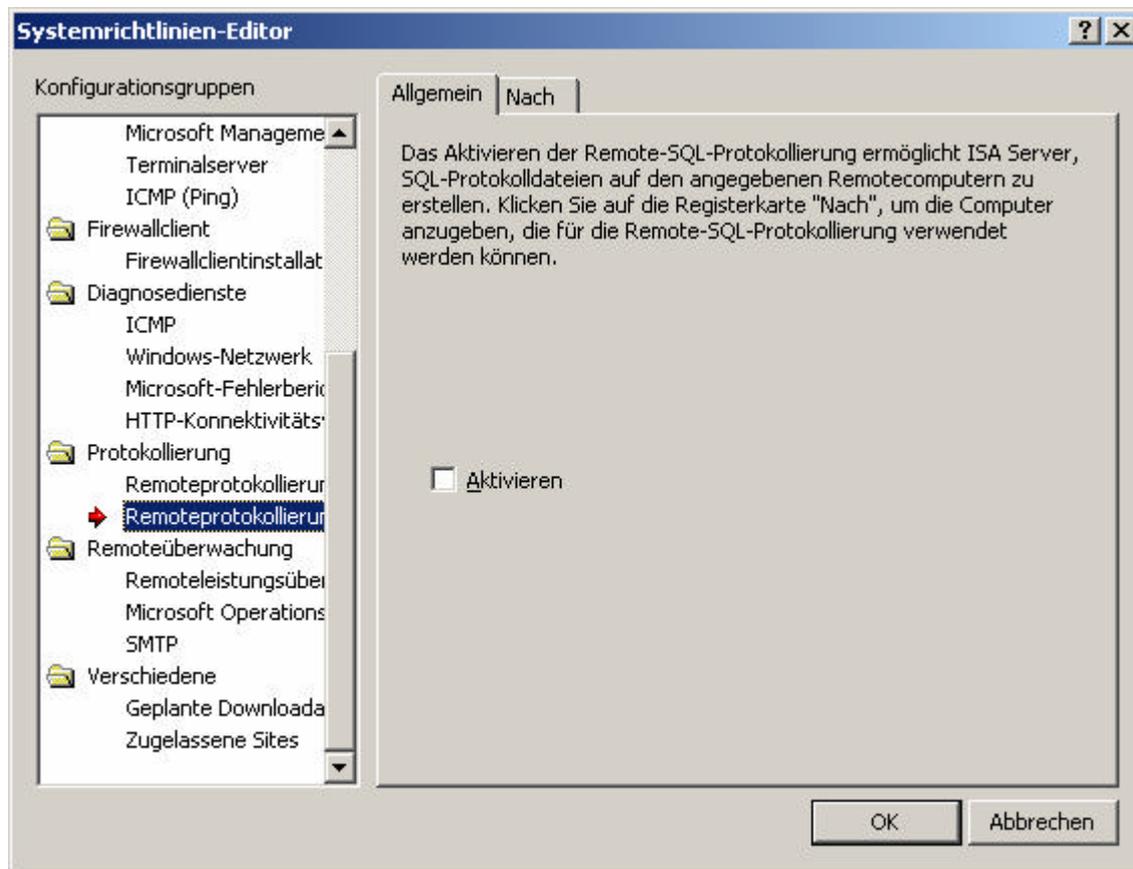
Sie können für die MSDE-Datenbank diverse Optionen konfigurieren. Es besteht die Möglichkeit, den Ort der Protokolldatei anzugeben, Dateispeicherlimits festzulegen und eine Aktion zu definieren, welche Aktion beim Erreichen des Protokollgrößenlimits durchgeführt werden soll.

Die maximale Protokolldateigröße bei der Verwendung der MSDE beträgt 8 GB. Insider sehen hier schon, dass es sich nicht um die Standard MSDE handelt, deren Größe auf maximal 2 GB limitiert ist, sondern um die erweiterte MSDE.



Die Protokolldateien können zur Reduzierung des Platzbedarfs komprimiert werden. Dieses Feature steht jedoch nur auf Partitionen mit dem NTFS Dateisystem zur Verfügung.

Wenn Sie eine Protokollierung in eine SQL Datenbank AUSSERHALB des ISA Server 2004 planen, müssen Sie mit Hilfe des Systemrichtlinien-Editor die *Remoteprotokollierung für SQL* Aktivieren und im Reiter *Nach* das Netzwerk angeben, welches den Remote SQL Server beinhaltet.



Stand: 21.08.2004/MG. <http://www.it-training-grote.de>