Unterrichtseinheit 8

Überwachen von Ereignisprotokollen:

Ereignisse werden überwacht, um Sicherheitsereignisse, die Ressourcenverwaltung oder System- und Anwendungsfehler identifizieren und nachverfolgen zu können. Systemereignisse werden von Windows 2000 automatisch konfiguriert und im Systemprotokoll aufgezeichnet, wohingegen Anwenderereignisse vom Anwendungsentwickler bestimmt und im Anwendungsprotokoll aufgezeichnet werden.

Start → Programme → Verwaltung → Ereignisanzeige

Einführung in Ereignisprotokolle

Ereignisprotokolle ermöglichen die Überwachung von Hard- und Software, Systemproblemen und Sicherheit.
Es existieren drei Arten von Protokollen:

- **Systemprotokoll** enthält die von Windows 2000 vorherbestimmten protokollierten Ereignistypen der Systemkomponenten.
- **Anwendungsprotokoll** enthält von Anwendungen oder Programmen protokollierte Ereignisse. Der Programmentwickler entscheidet, welche Ereignisse aufgezeichnet werden.
- **Sicherheitsprotokoll** Sicherheitsereignisse werden im Zusammenhang mit Anmeldeversuchen und der Ressourcenverwendung aufgezeichnet. Welche Ereignisse im Sicherheitsprotokoll aufgezeichnet werden sollen, legt der Administrator fest.

Achtung:	Anwendungs- und Systemprotokolle können von allen Benutzern angezeigt werden, während auf Sicherheitsprotokolle nur Systemadministratoren zugreifen können.

Arten von System- und Anwendungsereignissen

Es gibt drei Arten von System- und Anwendungsereignissen:

- **Information** Die erfolgreiche Ausführung einer Anwendung, eines Treibers oder eines Dienstes
- **Warnung** Ein Ereignis, das nicht notwendigerweise bedeutsam ist, aber möglicherweise auf ein zukünftiges Problem bei Systemvorgängen hinweist.
- **Fehler** Ein bedeutsames Problem bei Systemvorgängen, wie z.B. ein Daten- oder Funktionalitätsverlust.

Anzeigen von Ereignisprotokollen

System- und Anwendungsereignisse werden in den zugeordneten Protokolldateien sequenziell protokolliert.

Zusätzlich zum Anzeigen eines lokalen Protokolls, kann auch ein Protokoll für einen Remotecomputer angezeigt werden. (In der **Ereignisanzeige** mit der rechten Maustaste klicken und **Verbindung zu anderem Computer herstellen** auswählen)

Achtung:	Ein Domänencontroller verfügt über mehr als diese drei Protokolle!

Man kann auch nach bestimmten Ereignissen, bzw. nach einer Gruppe von Ereignissen suchen (*Start → Programme → Verwaltung → Ereignisanzeige → Ansicht → Suchen*).
Um die Filterfunktion zum Suchen zu aktivieren, muss man mit der rechten Maustaste auf **Sicherheits-**, **System-** oder **Anwendungsprotokoll**, dann auf **Ansicht** und anschließend auf **Filter** klicken.

Beschränkung von Protokolldateigrößen

Ereignisprotokolle können, um Speicherplatzproblemen auf der Festplatte vorzubeugen, durch überschreiben älterer Ereignisprotokolle beschränkt werden.
Um Protokolldateien zu konfigurieren, muss man das entsprechende Protokoll in der Ereignisanzeige auswählen. Hier stehen folgende Optionen zur Verfügung:

- **Ereignisse nach Bedarf überschreiben**
  diese Einstellung erfordert keine Verwaltung und kann bei niedriger Sicherheit gewählt werden – Überprüfung täglich
- **Ereignisse überschreiben die älter als x Tage sind**
  diese Einstellung sollte man wählen, wenn die Überprüfung alle drei bis fünf Tage erfolgt
- **Ereignisse nie überschreiben [Protokoll manuell löschen]**
  hier muss das Löschen des Protokolls manuell erfolgen. Wenn dieses voll ist, zeichnet W2k keine weiteren Ereignisse mehr auf. Diese Einstellung sollte bei sehr hoher Sicherheit ausgewählt werden. W2k kann auch so konfiguriert werden, dass ein volles Sicherheitsprotokoll zum Herunterfahren des Systems führt.

Verwalten von Ereignisprotokollen

1. Die Ereignisprotokolle sollten für folgende Zwecke archiviert werden:
   - zum Nachverfolgen von Trends, um die Ressourcenverwendung zu bestimmen
   - zum Nachverfolgen nicht autorisierter Ressourcenverwendung
   - zum Aufbewahren von Aufzeichnungen aus rechtlichen Gründen

2. Folgende Dateiformate zum Anzeigen archivierter Protokolle sind möglich:
   1. Protokolldateiformat (EVT)
   2. Textdateiformat (TXT)
   3. Textdateiformat mit Kommas als Trennzeichen (CSV)

3. Löschen der Ereignisprotokolle, wenn diese nicht überschrieben werden sollen

Verwenden des Task-Managers

Der Task-Manager stellt Echtzeitinformationen über derzeit auf dem System ausgeführte Anwendungen, Prozessen und ihrer Speicherverwendung (ein Programm, welches in einem reservierten Arbeitsspeicherbereich ausgeführt wird) oder anderen Prozessdaten, sowie zu Statistiken über die Arbeitsspeicher- und Prozessorleistung bereit.

1. **Überwachen von Programmen**
   Mit der Registerkarte **Anwendungen** kann der Status (**wird ausgeführt** oder **keine Rückmeldung** – kann über **Task beenden** beendet werden) aller ausgeführten Anwendungen überwacht werden.
   Um den zugeordneten Prozess einer Anwendung zu identifizieren, muss man mit der rechten Maustaste erst auf die Anwendung und dann auf **Zum Prozess wechseln** klicken, worauf die Registerkarte **Prozesse** mit dem zugeordneten Prozess angezeigt wird.

2. **Überwachen von Prozessen**
   In der Registerkarte **Prozesse** werden alle ausgeführten Prozesse und Ihre Maße (quantitative Angaben eines Prozesses, wie CPU-Nutzung[%], CPU-Zeit, Speichernutzung, E/A [Lesen], E/A [Schreiben]) angezeigt.
   Zum Anzeigen anderer Eigenschaften muss auf **Ansicht** und anschließend auf **Spalten auswählen** geklickt werden.

3. **Überwachen der Leistung**
   Zum Überwachen der aktuellen (dynamischen prozessor- und speicherverwendenden) Leistungen wird die Registerkarte Systemleistung verwendet.

Verwenden des Systemmonitors zum Überwachen der Systemleistung

Um ausführlichere Details des Computers und dessen Leistung zu erhalten wird der Systemmonitor (*Start → Programme → Verwaltung → Systemmonitor)* verwendet.

- **Objekte:** Im Systemmonitor sind Objekte (Hardware und Software) wichtige Komponenten oder Subsysteme des Computersystems

Achtung:	Systemmonitorobjekte sind nicht das Gleiche wie Objekte von Active Directory und haben nichts mit diesen zu tun!

- **Instanzen**: dies sind mehrere Exemplare desselben Objekttyps
- **Leistungsindikatoren:** sammeln Daten zu verschiedenen Aspekten von Objekten. Im Systemmonitor wird angeben, welche Leistungsindikatoren angezeigt werden sollen.

Anzeigen der Leistungsindikatoren

Die Daten können auf drei Arten in Echtzeit angezeigt werden:

1. **Histogramm** zeigt Daten in einem Balkendiagramm an
2. **Bericht** zeigt numerische Daten in Spalten an (zum weiterverarbeiten in Tabellenkalkulationsprogrammen)
3. **Diagramm** zeigt Daten in einem Kurvendiagramm an

Auch mit dem Tool Leistungsdatenprotokolle können Daten in Echtzeit angezeigt werden. Es gibt dabei zwei Arten von Protokollen:

- **Leistungsindikatorenprotokolle:** (dauernde kontinuierliche Darstellung) zeichnen Daten zu Hardwareressourcen und Systemdiensten auf der Grundlage der Leistung über längere Zeiträume auf
- **Protokolle der Ablaufverfolgung:** (wird erst ab dem Eintreten des Ereignisses aktiv) sammeln Ablaufverfolgungen mit Leistungsstatikmaßen zu Ereignissen, wie z.B. Datenträger- und Datei-E/A-Ereignissen

Verwenden von Warnungen

Warnungen werden zum Benachrichtigen eines Benutzers oder Administrators beim Überschreiten festgelegter Kriterien (bestimmte Leistungsindikatoren, welche nicht aktiv überwacht werden) verwendet.
Man kann Warnungen so konfigurieren, dass diese eine Netzwerkmeldung sendet, ein Programm ausführt oder ein Protokoll startet.
Zum Ausführen des Tools Leistungsdatenprotokolle und Warnungen muss man über Administratorrechte verfügen.

Warnungen werden wie folgt festgelegt:
*Start → Programme → Verwaltung → Systemmonitor → **Leistungsdatenprotokolle und Warnungen** → Warnungen → rechte Maustaste auf **Neue Warnungseinstellungen** → Namen vergeben → auf der Registerkarte **Allgemein** einen Kommentar mit einer Kurzbeschreibung vergeben → Hinzufügen → hier die entsprechenden Leistungsindikatoren auswählen und auf der Registerkarte **Allgemein** die Eigenschaften für das Abtastintervall und den Warnschwellenwert festlegen → Auf der Registerkarte **Vorgang** das Kontrollkästchen **Einen Eintrag im Ereignisprotokoll der Anwendungen protokollieren** aktivieren → auf der Registerkarte **Zeitplan** unter **Suche starten** und **Suche beenden** die Parameter festlegen → **OK***

Optimieren der Leistung

Um das Betriebssystem und die Anwendungen die Systemressourcen effizienter verwenden zu können, sollte die Leistung (Basislinie) des Computers optimiert werden.
Zu den wichtigsten Ressourcen, welche überwacht werden sollten, um die Basislinie beizubehalten, gehören folgende:

- Arbeitsspeicher
- Prozessor
- Datenträgeraktivität
- Netzwerkaktivität

Prozess der Leistungsoptimierung

Durch die Optimierungsprozesse kann bestimmt werden, welche Aktionen zum Verbessern der Systemleistung – entsprechend der Anforderungen an das System - ausgeführt werden sollten. Dieser Prozess umfasst folgende Aufgaben:

- Analysieren von Überwachungsdaten durch:
    - das Analysieren von Prozessen (Programme und Threads)
    - Informationen, ob die übermäßige Verwendung Hardwareressource die Systemleistung verringert
    - Informationen, ob es Auswirkungen von Engpässen oder aus sonstigen Gründen nicht hinreichend ausgelastete Hardwareressourcen gibt (z.B. Arbeitsspeicher, Festplattenspeicher...)
- Identifizieren von Bereichen mit inakzeptabler Leistung. Bei dieser Analyse kann möglicherweise festgestellt werden, dass die Systemleistung nicht jederzeit, abhängig von der Benutzerumgebung, ausreicht.
- Ausführen von korrigierenden Aktionen. Abhängig von den Gründen und dem Ausmaß der festgelegten Abweichungen, können korrigierende Aktionen durchgeführt werden.

Untersuchen der Arbeitsspeicherleistung

Schlechte Arbeitsspeicherbedingungen können die Ausführung von Anwendungen und Diensten auf dem Computer verlangsamen und sich auf die Leistung anderer Systemressourcen auswirken.
Zum Einrichten einer Basislinie (Werte, in dem die Verwendung des physischen Arbeitsspeichers liegen kann) für die Verwendung des physischen Arbeitsspeichers, wird dieser bei Normalauslastung untersucht.
Die gesamte auf einem System ausgeführte Verarbeitung findet im Arbeitsspeicher statt, dabei muss sichergestellt werden, dass von diesem genügend zur Verfügung steht.

Folgende Leistungsindikatoren sind zum Untersuchen des **Speicher**-Objekts nützlich:

- **Seiten/s** zeigt die Anzahl von angeforderten Seiten an, die nicht sofort im RAM verfügbar waren
- **Verfügbare Bytes** zeigt an, wie viel physischer Arbeitsspeicher noch übrig ist

Untersuchen von Auslagerungsdateien

Ein Mangel an Arbeitsspeicher wird durch ein häufiges Auslagern von Daten auf die Festplatte festgestellt. Die Auslagerung ist der Prozess, bei dem virtueller Arbeitsspeicher zwischen dem physischen Arbeitsspeicher und den Datenträger hin- und herverschoben wird. Das Überprüfen der Auslagerungsdateigröße (empfohlen: verfügbares RAM * 1,5) ist wichtig, um festzustellen ob sich eine Auslagerungsdatei im oberen Bereich des Grenzwertes befindet.
Folgende Leistungsindikatoren werden zum Überwachen der Größe von **Pagefile.sys** (Auslagerungsdatei) des **Auslagerungsdatei**-Objekts verwendet:

- **Auslagerungsdatei\Belegung (%)** dieser Wert liegt nah bei der Einstellung für die maximale Auslagerungsdateigröße
- **Auslagerungsdatei\Max.Belegung (%)** dieser Wert liegt nah bei 100%

Untersuchen der Prozessorleistung

Zum Untersuchen der Prozessorleistung muss die Rolle des Computers und die Art der ausgeführten Arbeit berücksichtigt werden.
Es gibt folgende nützliche Leistungsindikatoren:

- Prozessor **Prozessorzeit(%)** zeigt den Prozentsatz der vergangenen Zeit an, während dessen ein Prozessor einen Tread ausführt. (Ein Wert von über 80% kann auf einen Engpass hinweisen)
- System **Prozessor-Warteschlangenlänge** zeigt die Anzahl von derzeit in der Prozessorwarteschlange befindlichen Thread an. (Eine Warteschlange mit zwei oder mehr Elementen kann bei einem Einprozessorsystem auf einen Engpass hinweisen)

Hohe Verwendungswerte können bei Arbeitsstationen auf eine effiziente Bearbeitung hinweisen. Beim Start eines neuen Prozesses kann die Prozessorzeit möglicherweise bis zu 100% ausgelastet sein (bei kurzeitiger Auslastung normal, bei langzeitiger Auslastung kritisch !).

Eine Prozessorauslastung von 100% auf einem Server, auf dem viele Clientanforderungen ausgeführt werden, weist auf einen Engpass hin und ist völlig inakzeptabel.

Untersuchen der Datenträgerleistung

Das **Physikalischer Datenträger**-Objekt stellt Leistungsindikatoren für die Aktivität physischer Datenträger bereit, wohingegen das **Logischer Datenträger**-Objekt für Statistiken zu logischen Datenträgern und Speicherdatenträgern verantwortlich ist.
Folgende Leistungsindikatoren sind zum Untersuchen der Datenträgerleistung nützlich:

- **Freier Speicherplatz** — zeigt den Prozentsatz an nicht reserviertem Speicherplatz in Bezug auf den gesamten verwendbaren Speicherplatz auf dem logischen Datenträger an
- **Mittlere Bytes/Übertragung** — ermittelt die Größe der Datenmengen bei E/A-Operationen
- **Mittlere Sek./Übertragung** — zeigt an, wie schnell Daten verschoben werden (ein hoher Wert kann bedeuten, dass das System Anforderungen wegen langer Warteschlangen, oder aufgrund von Datenträgerfehlern wiederholt lesen muss)
- **Bytes/s** — zeigt die Übertragungsrate für Bytes an und ist das primäre Maß für den Datenträgerdurchsatz
- **Übertragungen/s** — zeigt die Anzahl von pro Sekunde ausgeführten Lese- und Schreibvorgängen an (übersteigt der Wert 50 [beim Stripeset 50 pro physischem Datenträger], entsteht möglicherweise ein Engpass)

Untersuchen der Netzwerkleistung

Der Systemmonitor (Leistungsaspekt) ermöglicht es, die Leistung der Netzwerkobjekte auf einem Server zu überwachen.
Folgende Leistungsindikatoren sind zum Untersuchen der Netzwerkaktivität nützlich:

- Netzwerkschnittstelle
  - **Ausgabewarteschlangenlänge** — zeigt die Ausgabewarteschlange für Pakete an
  - **Ausgehende Pakete, verworfen** — hiermit kann bestimmt werden, ob das Netzwerk ‚gesättigt' ist
  - **Gesamtzahl Bytes/s** — zum Überwachen der Netzwerkkartenleistung
- Transmission Control Protocol (TCP)
  - **Segmente empfangen/s**
  - **Erneut übertragene Segmente/s**
  - **Segmente/s**
  - **Segmente gesendet/s**

  Überwachen die Aktivität der Transportschicht

- Internet Protocol (IP)

    - **Weitergeleitete Datagramme/s**
    - **Datagramme empfangen/s**
    - **Datagramme/s**
    - **Datagramme gesendet/s**

    Überwachen die Aktivität der Netzwerkschicht

Der Netzwerkmonitor (Detailaspekt) kann zum Überwachen des Datenstromes im Netzwerk verwendet werden.