Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe oder Vervielfältigung.

15 Fehlersuche und Problembehebung

In diesem Kapitel geht es um folgende Themen:

- **Fehler bei der Richtlinienverarbeitung ermitteln und beseitigen**
- **Wie gehe ich mit den Tools Gruppenrichtlinienergebnisse, Gruppenrichtlinienmodellierung und GPResult.exe um?**

15.1 Einführung

Wenn es bei der Gruppenrichtlinienverarbeitung zu Fehlern kommt, stehen Ihnen unterschiedliche Werkzeuge zur Verfügung, um die Fehlerdetails zu ermitteln. Bevor Sie allerdings mit der komplizierten Detailsuche in Protokolldateien beginnen, überprüfen Sie Ihr System auf die in Tabelle 15.1 aufgelisteten Standardfehler.

Tabelle 15.1 Häufige Ursachen für Fehler in der Gruppenrichtlinienanwendung

Ursache	Erläuterung
DNS-Fehler	Wenn in der Namensauflösung Fehler auftreten, wirken sich diese stets auch auf die Gruppenrichtlinienverarbeitung aus. Überprüfen Sie mit `nslookup.exe`, ob eine saubere Auflösung von Namen und Diensteinträgen für den Rechner funktioniert.
Speicherort von Objekten	Damit eine Gruppenrichtlinie für ein Objekt wirkt, muss sich das Objekt am korrekten Speicherort befinden. Häufig ist z. B. der Rechner in der OU, im Gruppenrichtlinienobjekt ist aber der Bereich Benutzerkonfiguration ausgewählt.
Neustart/ Anmeldung ausstehend	Manche Gruppenrichtlinieneinstellungen (z. B. Softwareverteilung) werden vom System nur bei einem Neustart oder einer neuerlichen Anmeldung ausgeführt. Im Zweifelsfall sollten Sie den Client nach dem Ausführen von `gpupdate.exe` neu starten.

(Fortsetzung nächste Seite)

Lizenziert für jonas@aeschlimann.cc
© 2015 Pearson Deutschland GmbH. Alle Rechte vorbehalten, insbesondere die unerlaubte Weitergabe oder Vervielfältigung.

Tabelle 15.1 Häufige Ursachen für Fehler in der Gruppenrichtlinienanwendung *(Fortsetzung)*

Ursache	Erläuterung
Berechtigungen	Überprüfen Sie, ob der Computer oder der Benutzer auch die Berechtigung hat, Richtlinieneinstellungen zu lesen und zu übernehmen.
Vererbung deaktiviert	Wenn auf einer Organisationseinheit die Vererbung deaktiviert ist, dann **erbt** die Organisationseinheit keine Einstellungen von übergeordneten GPOs. Sie **vererbt** weiterhin Einstellungen an untergeordnete OUs!
Bereiche von GPO deaktiviert	Sie können Bereiche von GPOs deaktivieren, die ganze GPO deaktivieren oder eine Verknüpfung deaktivieren. Dies bewirkt, dass die Einstellungen auch nicht mehr angewendet werden.
Erzwungen	Wenn eine Einstellung an höherer Stelle erzwungen wird, kann sie nicht überschrieben werden.
WMI-Filter	WMI-Filter können verhindern, dass bestimmte Rechner oder Benutzer von einem GPO oder (über Zielgruppenadressierung auf Elementebene) einer Einstellung betroffen sind.
Richtlinieneinstellungen für anderes Betriebssystem	Nicht jede Einstellung kann für jedes Betriebssystem verwendet werden. Überprüfen Sie in den Erläuterungen der Einstellung, für welche Betriebssysteme diese angewendet werden kann.

In diesem Kapitel finden Sie teilweise Screenshots von Windows Server 2008 R2 und teils von Windows Server 2012. Die Darstellungen unterscheiden sich teilweise, und da z. B. das Erweitern bestimmter Ansichten nicht unter beiden Systemen möglich oder nötig ist, wurden stets die Darstellungen mit der größtmöglichen Aussagekraft gewählt.

15.2 Gruppenrichtlinienergebnisse

Eines der Werkzeuge, das zum Überprüfen von Gruppenrichtlinienverarbeitung angewendet werden kann, ist „Gruppenrichtlinienergebnisse“ der Gruppenrichtlinienverwaltung.

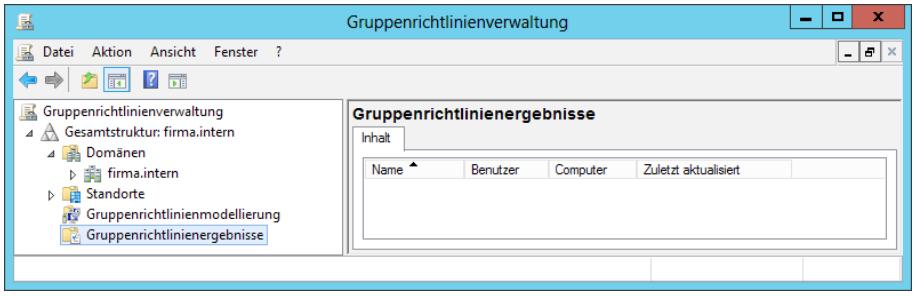

Bild 15.1 Gruppenrichtlinienergebnisse öffnen

Mit den Gruppenrichtlinienergebnissen werden Verarbeitungsinformationen der letzten Anmeldung der letzten bis zu zehn Benutzer abgerufen, die sich schon einmal an einem

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

bestimmten Computer angemeldet haben. Verwenden Sie zum Abrufen der Gruppenrichtlinie am besten Windows 8/Windows Server 2012 oder höher, da Microsoft die Reporting-Funktionalität hier verbessert hat und u. a. Slow Links, Vererbungsblockierung und Loopbackverarbeitung auswertet und im Report anzeigt.

15.2.1 Gruppenrichtlinienergebnis-Assistent

Um Gruppenrichtlinienergebnisse zu verwenden, gehen Sie wie folgt vor:

- Navigieren Sie in der Konsolenstruktur von Gruppenrichtlinienverwaltung zu Gruppenrichtlinienergebnisse und rufen Sie im Kontextmenü Gruppenrichtlinienergebnis-Assistent auf.
- Klicken Sie bei Willkommen auf Weiter, und markieren Sie in der Computerauswahl entweder Dieser Computer oder Anderer Computer und Durchsuchen, um dann wie gewohnt einen Computer auszuwählen.
- Wenn Sie nur den Bereich Benutzerkonfiguration analysieren möchten, können Sie Keine Richtlinieneinstellungen für den ausgewählten Computer im Ergebnis anzeigen (nur Benutzerrichtlinieneinstellungen) aktivieren.
- Klicken Sie anschließend Weiter.

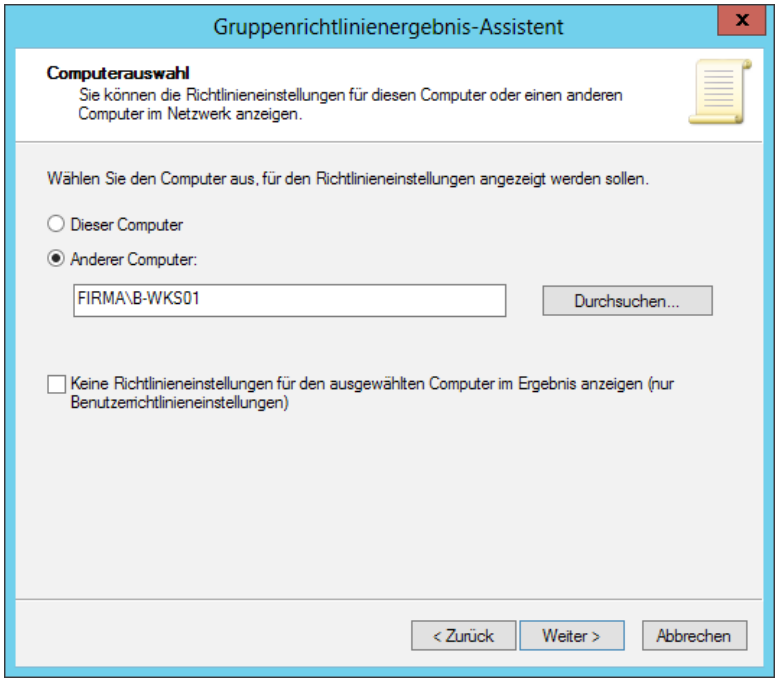

Bild 15.2 Computer für Gruppenrichtlinienergebnisse auswählen

Lizenziert für jonas@aeschlimann.cc
© 2016 Pearson Deutschland GmbH. Alle Rechte vorbehalten, insbesondere die unerlaubte Weitergabe oder Vervielfältigung.

Sie erhalten nun im Fenster Benutzerauswahl die Benutzer angezeigt, die sich bisher auf dem Rechner angemeldet hatten. Nur für diese sind Informationen zur Gruppenrichtlinienverarbeitung gespeichert und können ausgewertet werden.

- Klicken Sie entweder auf AKTUELLEN BENUTZER oder aktivieren Sie BESTIMMTEN BENUTZER AUSWÄHLEN und markieren den entsprechenden Benutzer. Wenn Sie keine Benutzerrichtlinienverarbeitung prüfen möchten, können Sie stattdessen KEINE BENUTZERRICHTLINIENEINSTELLUNGEN IM ERGEBNIS ANZEIGEN (NUR COMPUTERRICHTLINIENEINSTELLUNGEN) aktivieren.
- Klicken Sie auf WEITER.

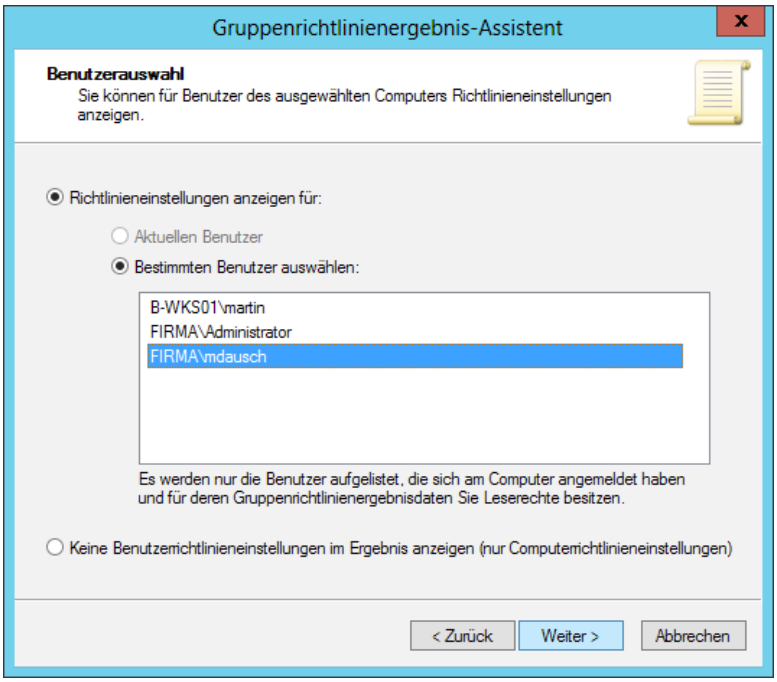

Bild 15.3 Benutzer wählen

- Lesen Sie die Zusammenfassung der Einstellungen und bestätigen Sie diese mit WEITER.
- Beenden Sie den Assistenten mit FERTIG STELLEN.

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

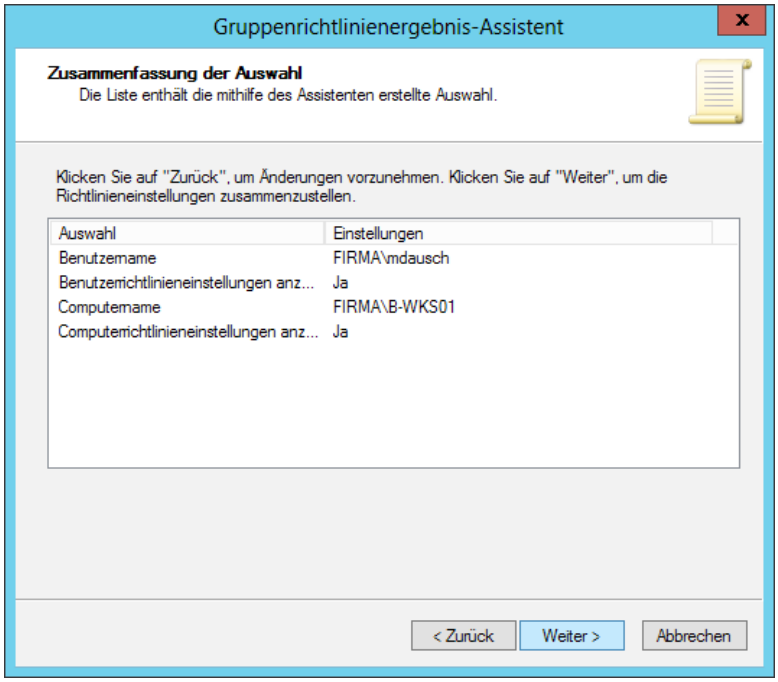

Bild 15.4 Zusammenfassung kontrollieren

15.2.2 Gruppenrichtlinienergebnis untersuchen

Wenn Sie im Knoten „Gruppenrichtlinienergebnisse“ die Ansicht erweitern, erhalten Sie eine Übersicht aller Gruppenrichtlinienergebnisse, die Sie bisher abgerufen haben. Sie können eine Auswertung auch erneut starten, indem Sie das Kontextmenü eines Ergebnissatzes aufrufen und „Abfrage erneut ausführen“ auswählen.

Die folgenden Ausführungen beziehen sich auf Windows Server 2008 R2, weiter unten finden Sie die Änderungen in Windows Server 2012.

- Markieren Sie das Ergebnis, das Sie mit dem Assistenten erzeugt haben, und kontrollieren Sie im Register ZUSAMMENFASSUNG, ob der Komponentenstatus mit einem roten Kreis mit weißem Kreuz markiert ist. Unter Komponenten werden hier die Gruppenrichtlinienerweiterungen (GPEs) verstanden, die für die Verarbeitung der Einstellungen zuständig sind. In diesem Fall konnten die Ergebnisse nicht sauber verarbeitet werden.

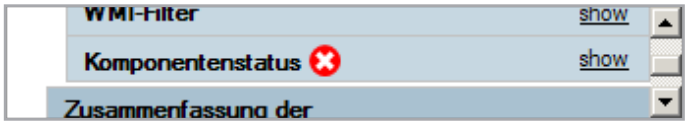

Bild 15.5 Fehler im Komponentenstatus

Lizenziert für jonas@aeschlimann.cc
© 2011 Addison-Wesley Verlag. Alle Rechte vorbehalten, auch die unerlaubte Weitergabe oder Vervielfältigung.

Wenn Komponenten teilweise nicht verarbeitet werden konnten, erhalten Sie in der Ansicht ein gelbes Warndreieck.

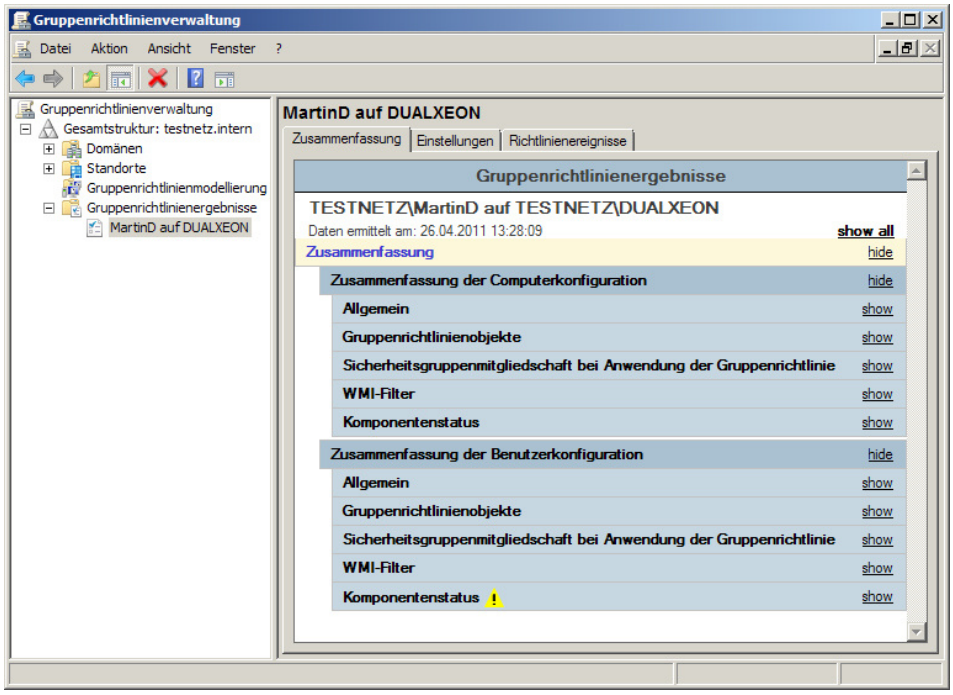

Bild 15.6 Gruppenrichtlinienergebnis anzeigen

- Klicken Sie unter Allgemein auf SHOW.

Sie erhalten eine Auflistung des Computernamens, der Domäne, des Standorts und des letzten Zeitpunktes der Gruppenrichtlinienverarbeitung.

- Klicken Sie unter Gruppenrichtlinienobjekte auf SHOW und erweitern Sie anschließend die Ansicht unter ANGEWENDETE GRUPPENRICHTLINIENOBJEKTE und ABGELEHNTE GRUPPENRICHTLINIENOBJEKTE.

Hier finden Sie die Auflistung der einzelnen GPOs mit den Informationen zum Verknüpfungsstandort und der Version. Bei den abgelehnten GPOs ist angegeben, warum sie abgelehnt wurden.

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

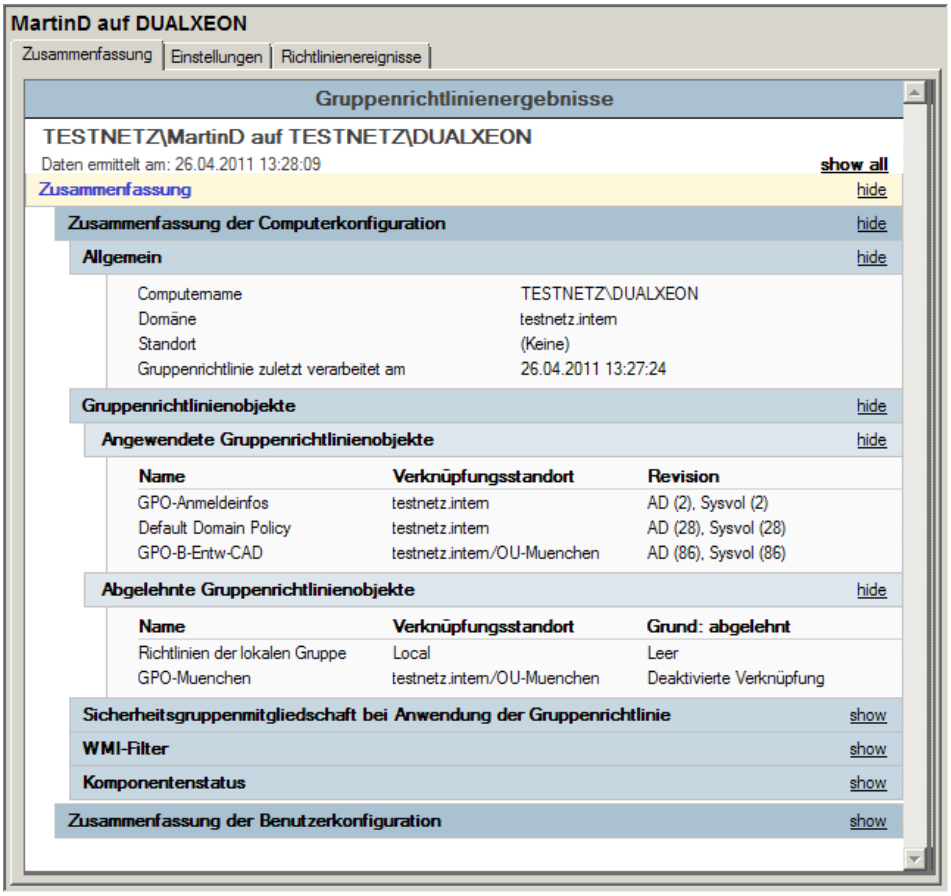

Bild 15.7 Allgemeine Informationen und GPOs

- Klicken Sie nun unter „Sicherheitsgruppenmitgliedschaft bei Anwendung der Gruppenrichtlinie“ auf SHOW.

Hier sind alle Gruppen aufgelistet, in denen der Computer oder, wenn Sie die Zusammenfassung der Benutzerkonfiguration prüfen, der Benutzer Mitglied war, als die Richtlinienverarbeitung stattfand.

Lizenziert für jonas@aeschlimann.cc
© 2011 Microsoft Press. Alle Rechte vorbehalten. Unerlaubte Weitergabe oder Vervielfältigung.

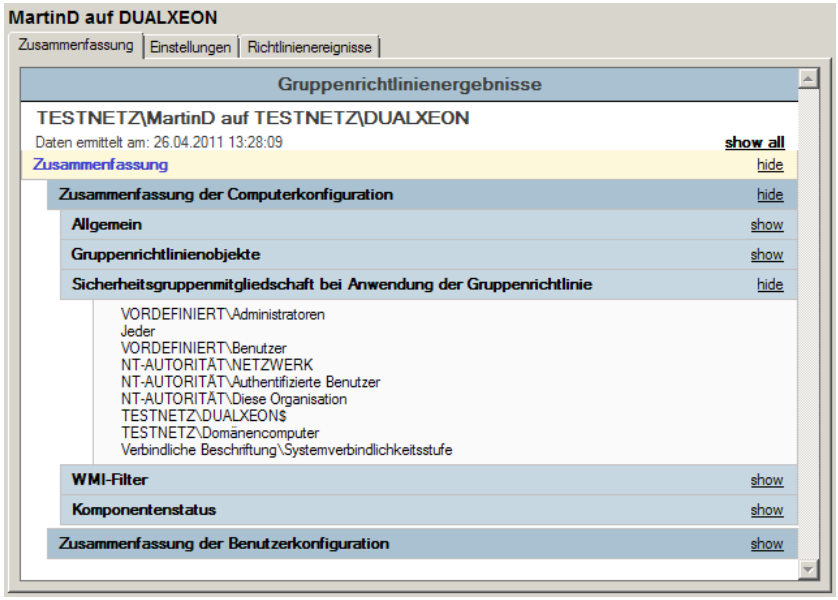

Bild 15.8 Sicherheitsgruppenmitgliedschaften

- Klicken Sie unter Komponentenstatus auf SHOW.

Der Verarbeitungsstatus der einzelnen Betriebssystemkomponenten für die Gruppenrichtlinienverarbeitung wird hier differenziert aufgelistet. Ab Windows Server 2012 wird auch die Zeit angegeben, die jede einzelne Komponente für die Verarbeitung benötigt hat. Das kann sehr hilfreich sein, um die Ursache für langsame Anmeldevorgänge zu ermitteln.

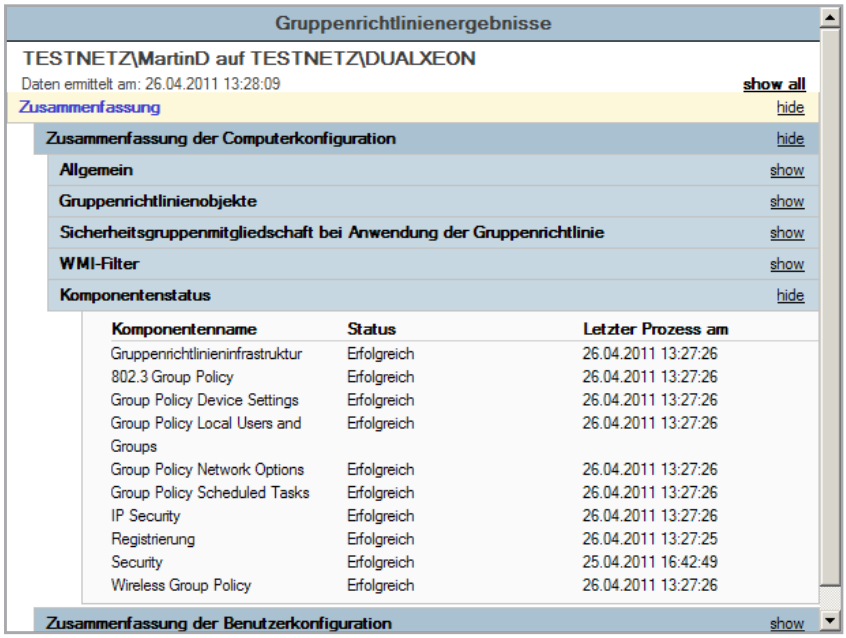

Bild 15.9 Komponentenstatus überprüfen

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

Wenn Probleme zu einem bestimmten Zeitpunkt in der Komponentenverarbeitung auftraten, können Sie sich die Problembeschreibung anzeigen lassen.

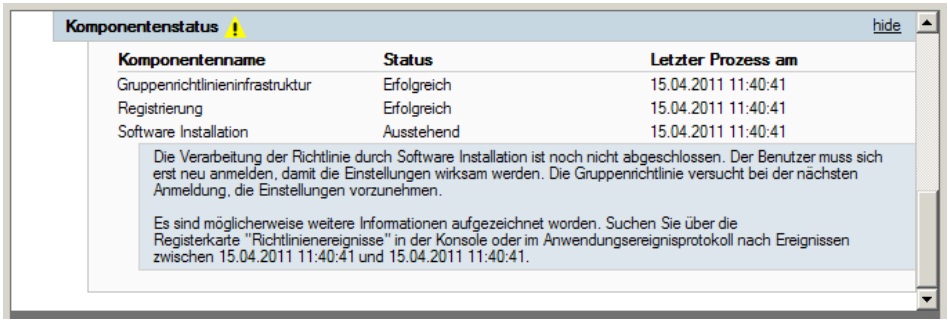

Bild 15.10 Problembeschreibung

Unter Windows Server 2012 R2 werden in der Zusammenfassung nur rudimentäre Ergebnisse festgehalten.

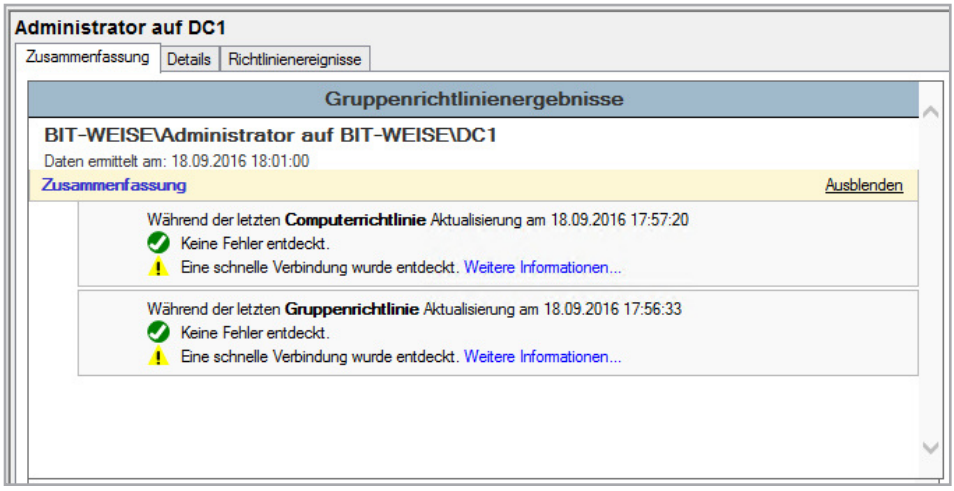

Bild 15.11 Zusammenfassung unter Windows Server 2012 R2

Die Informationen, die Windows Server 2008 R2 noch unter ZUSAMMENFASSUNG angezeigt hat, finden Sie jetzt unter DETAILS. Hier finden Sie außerdem die Einstellungen, die tatsächlich auf den Computer und den Benutzer angewendet wurden. Die Details entsprechen des Weiteren dem Register Einstellungen unter Windows Server 2008 R2.

Lizenziert für jonas@aeschlimann.cc
© 2013 Addison-Wesley Verlag. Alle Rechte vorbehalten, auch die unerlaubte Weitergabe oder Vervielfältigung.

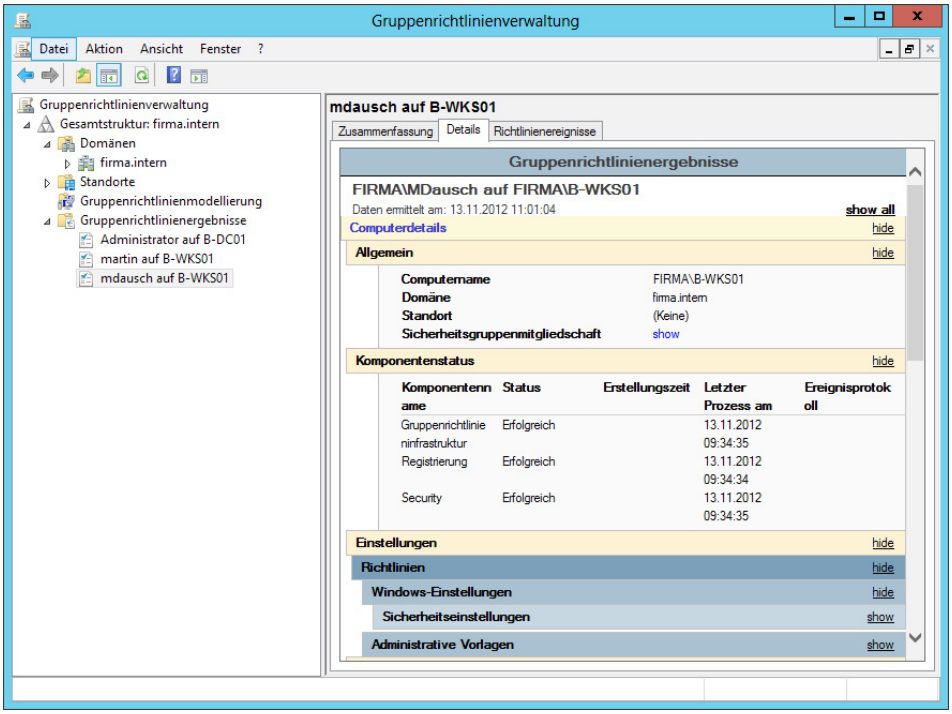

Bild 15.12 Details im Gruppenrichtlinienergebnis unter Windows Server 2012

Betrachten Sie im Vergleich die Gruppenrichtlinienergebnisse unter Windows Server 2008 R2.

- Klicken Sie auf das Register EINSTELLUNGEN.

Hier können Sie sich für einzelne Einstellungen anzeigen lassen, wie diese konfiguriert sind und aus welchem GPO die Einstellungen stammen.

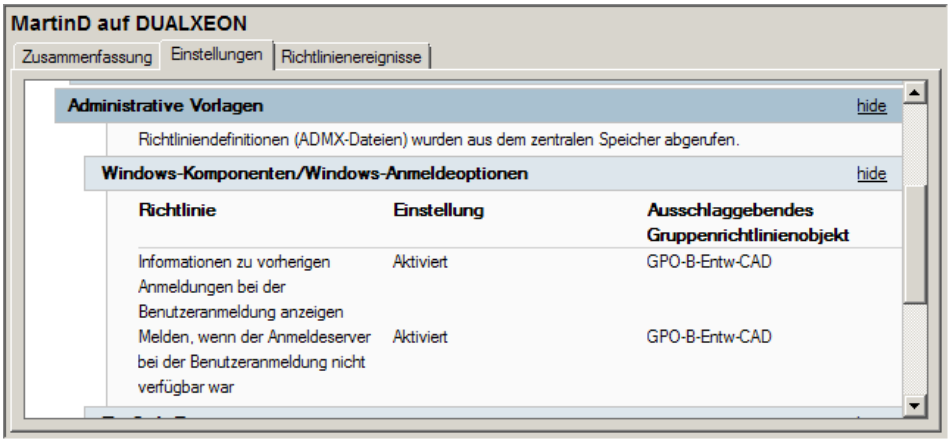

Bild 15.13 Einstellungen prüfen

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

- Klicken Sie auf das Register RICHTLINIENEREIGNISSE.

Sie erhalten die gefilterte Ereignisanzeige der Gruppenrichtlinienverarbeitung.

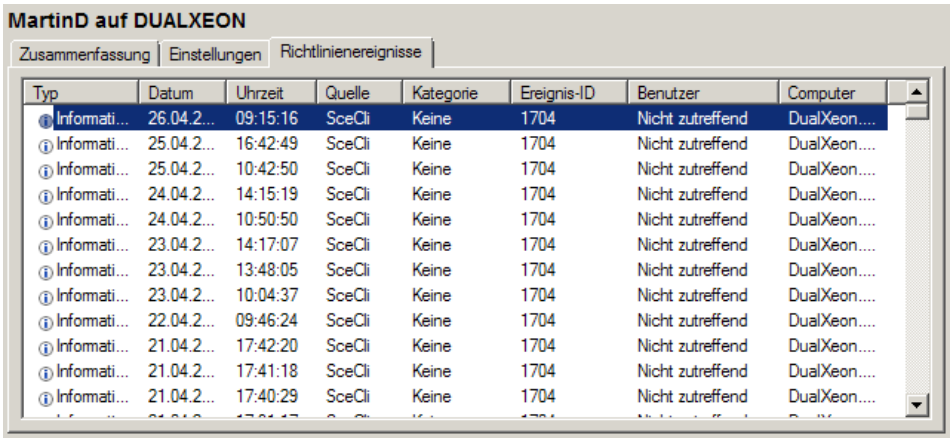

Bild 15.14 Richtlinienereignisse anzeigen

Sie können die Einstellungen eines Gruppenrichtlinienergebnisses auch anzeigen, indem Sie im Kontextmenü des Ergebnisses den Befehl ERWEITERTE ANSICHT ... aufrufen.

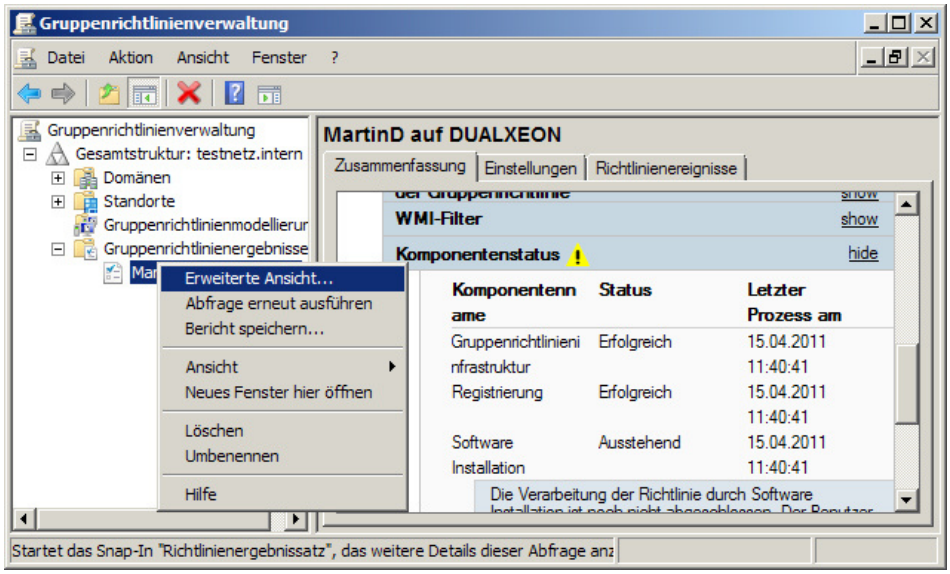

Bild 15.15 Erweiterte Ansicht aufrufen

Dann wird Ihnen der Ergebnissatz im Gruppenrichtlinien-Editor angezeigt. Leere administrative Vorlagen-Einstellungen werden nicht angezeigt. Bereiche, in denen Fehler auftraten, sind mit einem gelben Warndreieck markiert.

Lizenziert für jonas@aeschlimann.cc
© 2010 Pearson Deutschland GmbH. Alle Rechte vorbehalten, insbesondere die unerlaubte Weitergabe oder Vervielfältigung.

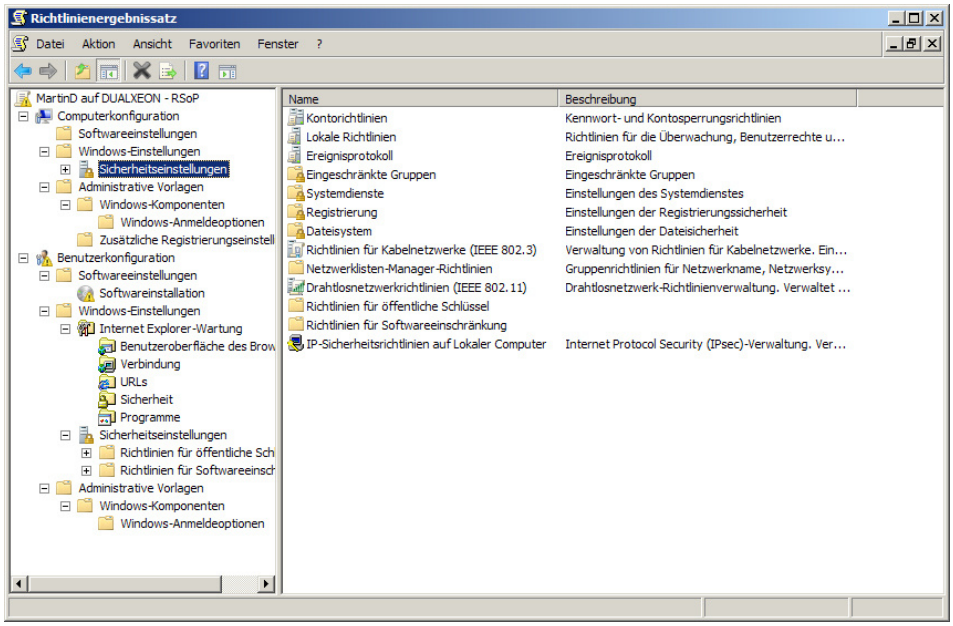

Bild 15.16 Erweiterte Ansicht verwenden

15.3 Gruppenrichtlinienmodellierung

Die Gruppenrichtlinienmodellierung dient der Planung von GPOs. Während beim Gruppenrichtlinienergebnissatz der Client erreichbar sein muss, muss bei der Planung nicht einmal ein echtes Konto angegeben werden.

PRAXISTIPP: Die Erfahrung zeigt, dass die Vorhersagen der Gruppenrichtlinienmodellierung nicht so zuverlässig sind wie ein echter Test mit einer Test-OU, Testrechnern und -benutzern. Für finale Tests verwenden Sie nach Möglichkeit die Testumgebung und Gruppenrichtlinienergebnisse für die Planung.

15.3.1 Gruppenrichtlinienmodellierungs-Assistent

- Klicken Sie in der GPMC auf Gruppenrichtlinienmodellierung, und wählen Sie im Kontextmenü Gruppenrichtlinienmodellierungs-Assistent.
- Klicken Sie im Willkommenfenster auf Weiter. Im Fenster Domänencontrollerwahl können Sie die Domäne auswählen, für die Sie eine Modellierung durchführen möchten. Wählen Sie anschließend entweder Beliebiger verfügbarer Domänencontroller mit

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte W

Windows Server 2003 oder höher oder Dieser Domänencontroller und markieren einen Domänencontroller in der Liste. Klicken Sie anschließend auf Weiter.

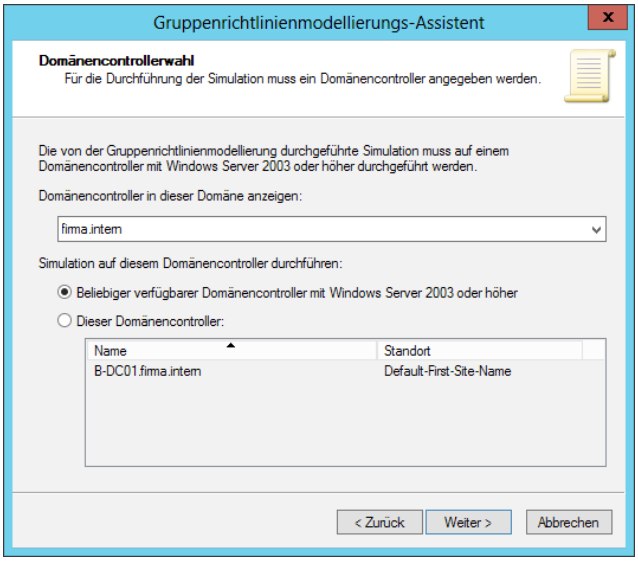

Bild 15.17
Domänencontroller für die Simulation wählen

- Unter Benutzer- und Computerauswahl können Sie entweder Organisationseinheiten für Benutzer und Computer auswählen, oder Sie geben explizit Konten an.

PRAXISTIPP: Wenn Sie genügend Informationen gesammelt haben, können Sie jederzeit mit dem Kontrollkästchen Zur letzten Seite des Assistenten wechseln, ohne weitere Daten zu erfassen.

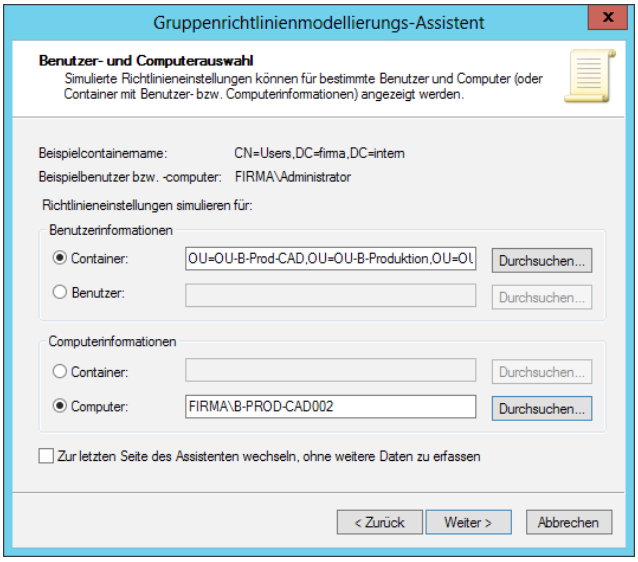

Bild 15.18
Benutzer- und Computerinformationen festlegen

Lizenziert für jonas@aeschlimann.cc
© 2016 Hanser ... unerlaubte Weitergabe oder Vervielfältigung.

- Legen Sie den Standort fest, für den die Simulation durchgeführt werden soll.
- Aktivieren Sie gegebenenfalls LANGSAME NETZWERKVERBINDUNG (z. B. EINWÄHLVERBINDUNG) und LOOPBACKVERARBEITUNG im gewünschten Modus. Klicken Sie anschließend auf WEITER.

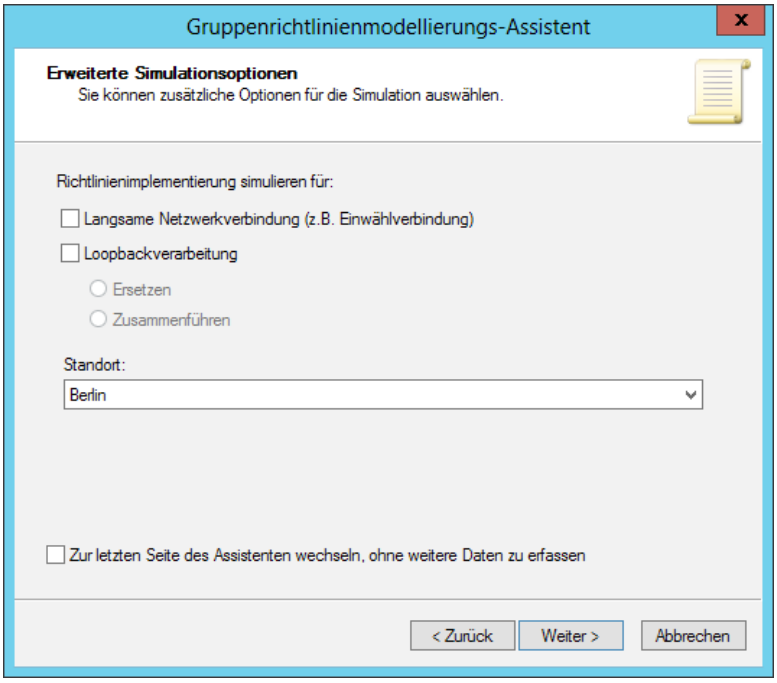

Bild 15.19 Standort und Verbindungseigenschaften definieren

HINWEIS: Das folgende Fenster des Assistenten erscheint nur, wenn Sie im vorletzten Fenster ein vorhandenes Benutzer- oder Computerkonto verwendet haben. Hier können Sie für die Simulation die Konten in andere OUs „verschieben", also quasi eine Was-wäre-wenn-Analyse vornehmen.

- Legen Sie hier fest, ob simuliert werden soll, dass der Computer oder Benutzer die Organisationseinheit wechselt. Wenn Sie versehentlich falsche Pfade verwendet haben, können Sie mit WIEDERHERSTELLEN die Änderungen rückgängig machen. Klicken Sie anschließend auf WEITER.

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

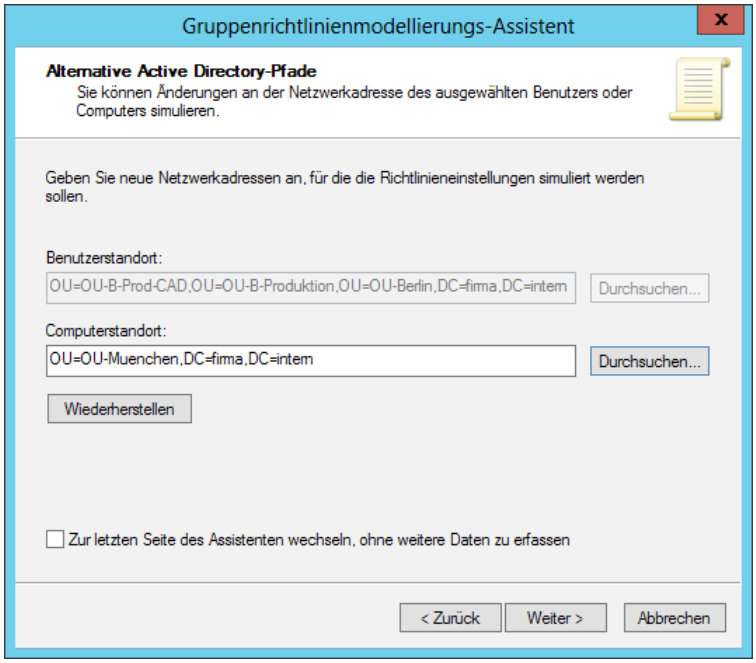

Bild 15.20 Active Directory-Pfade festlegen

- In den nächsten beiden Fenstern können Sie die Sicherheitsgruppenmitgliedschaft des Benutzers und des Computers, den Sie simulieren möchten, anpassen.

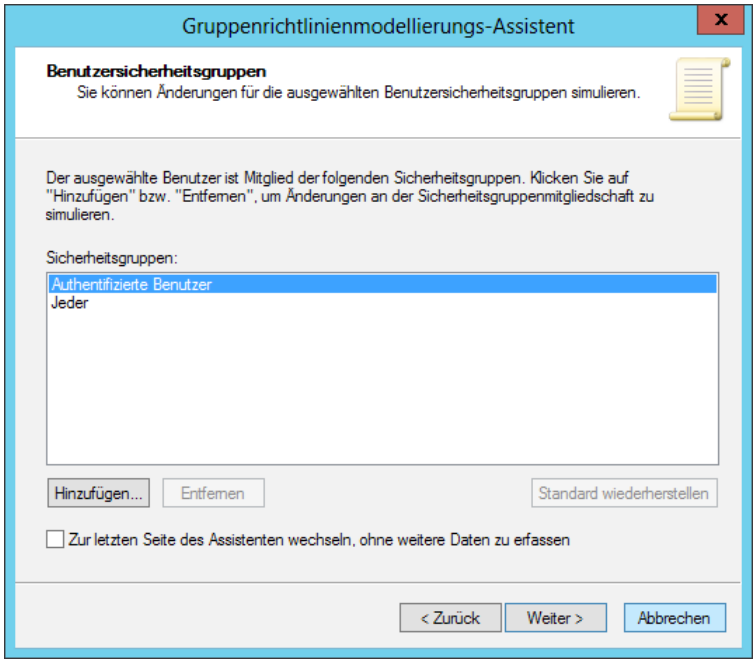

Bild 15.21 Benutzersicherheitsgruppen konfigurieren

Lizenziert für jonas@aeschlimann.cc
© 2015 Hanser ... unerlaubte Weitergabe oder Vervielfältigung.

- Geben Sie in den beiden folgenden Fenstern an, welche WMI-Filter mit dem Benutzer und dem Computer verbunden werden sollen.

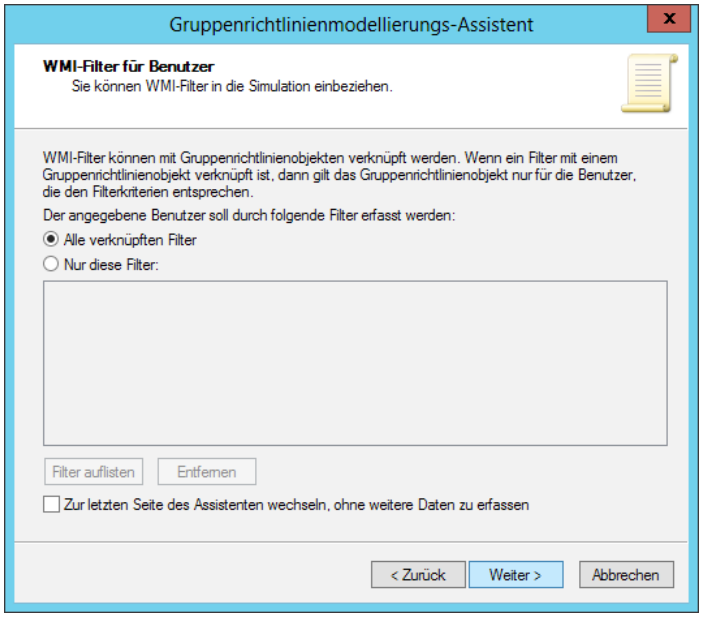

Bild 15.22 WMI-Filter für Benutzer festlegen

- Lesen Sie die abschließende Zusammenfassung und beenden Sie den Assistenten mit WEITER und anschließend FERTIG STELLEN.

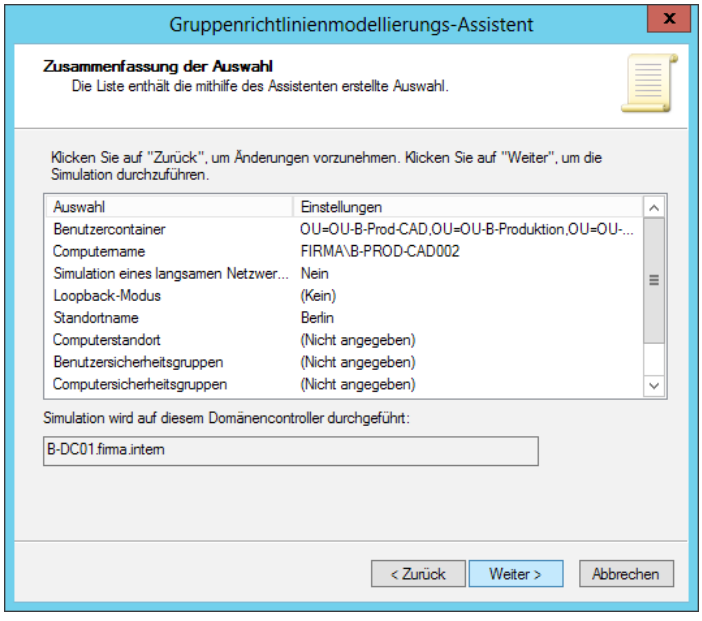

Bild 15.23 Zusammenfassung kontrollieren

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte W

15.3.2 Gruppenrichtlinienmodellierung auswerten

Der Aufbau des Ergebnisses der Gruppenrichtlinienmodellierung entspricht dem eines Gruppenrichtlinienergebnisses. Dies betrifft auch die Unterschiede in der Darstellung zwischen Windows Server 2008 R2 und Windows Server 2012. Im Folgenden habe ich mich auf die Darstellung der Modellierungsergebnisse unter Windows Server 2008 R2 beschränkt, da diese (leider!) etwas ausführlicher sind.

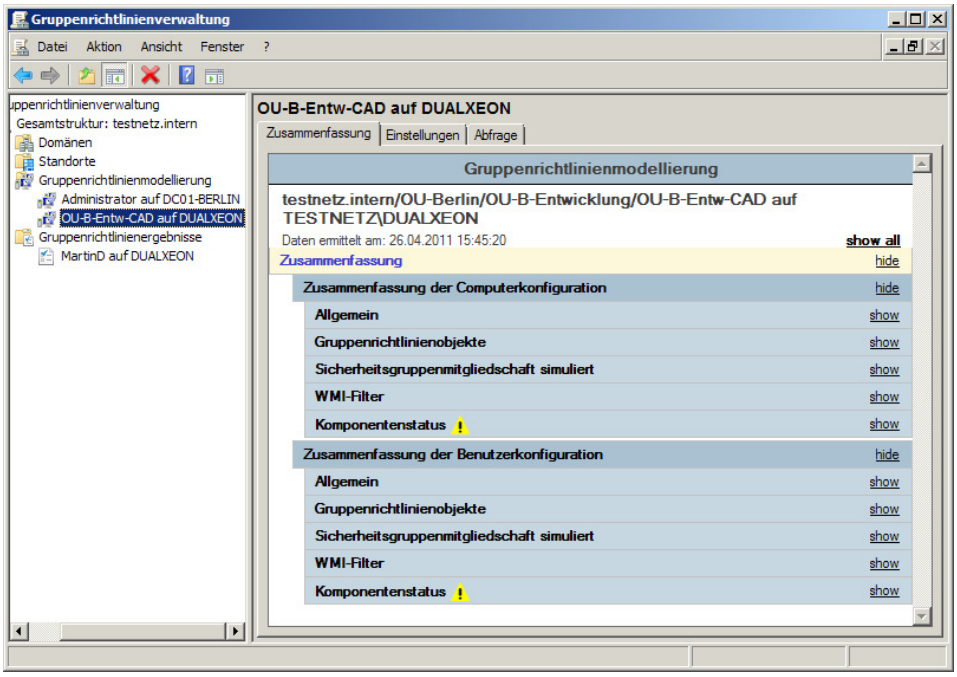

Bild 15.24 Gruppenrichtlinienmodellierung auswerten

Die Warnungen beim Komponentenstatus sind darauf zurückzuführen, dass bei der Modellierung kein Benutzer, sondern nur eine Organisationseinheit ausgewählt wurde. Generell führt der Modellierungs-Assistent aber häufig zu unvollständigen Ergebnissen. In der Ereignisanzeige des Servers finden sich entsprechende Einträge im Anwendungsprotokoll.

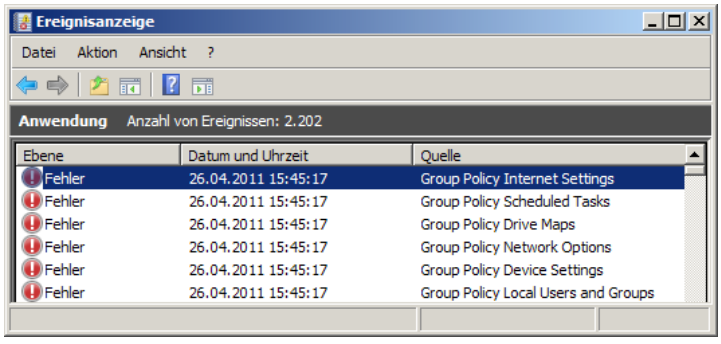

Bild 15.25 Ergebnis einer Gruppenrichtlinienmodellierung

Lizenziert für jonas@aeschlimann.cc
© 2011 Microsoft Press. Alle Rechte vorbehalten. Jede unerlaubte Weitergabe oder Vervielfältigung.

15.4 GPResult

Auf der Kommandozeile können Sie das Tool `gpresult.exe` verwenden, um einen Gruppenrichtlinienergebnissatz zu generieren. Mit Parameter /? rufen Sie die Befehlszeilenreferenz auf.

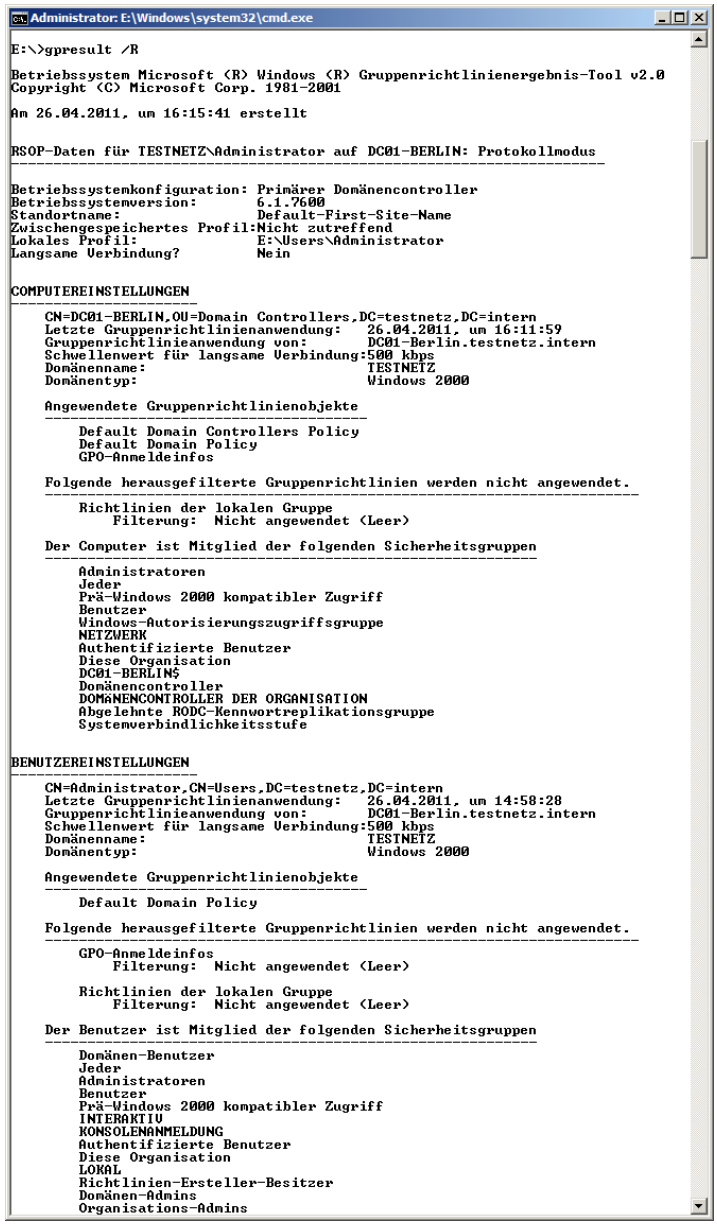

Bild 15.26 Beispielausgabe von `gpresult.exe` in der Eingabeaufforderung

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe.

GPResult kann sehr hilfreich sein, wenn Sie direkt auf dem Client, auf dem der Fehler aufgetreten ist, eine Gruppenrichtlinien-Auswertung durchführen wollen oder wenn Ihnen gerade keine GPMC zur Verfügung steht. Verwenden Sie dafür folgende Parameter:

- Erstellen eines Reports für das aktuelle System und den angemeldeten Benutzer:
  `gpresult Gpresult /H c:\temp\report.html`
- Erstellen eines Reports für ein Remotesystem
  `gpresult /S Client2 /U Bit-Weise\Hwurst /H C:\temp\client2hwurst.html`
- Auswertung der angewendeten Richtlinien ohne Report der Einstellungen
  `GPResult /R`
- Alternativ können Sie das PowerShell-Cmdlet `Get-GPResultantSetOfPolicy` verwenden, das allerdings nur mit der GPMC zusammen installiert wird.

15.5 Gruppenrichtlinien-Eventlog

Der Gruppenrichtlinienclient führt eine sehr intensive Protokollierung im Windows-Ereignisprotokoll durch, und das an verschiedenen Stellen. Es gibt drei Ereignisprotokolle, die Sie zur Fehleranalyse verwenden können.

Das Anwendungsprotokoll: Im Anwendungsprotokoll schreiben vor allem CSEs Status- und Fehlermeldungen. So warnt hier z. B. die Ordnerumleitung, dass sie die Verarbeitung von Richtlinien erst beim nächsten Start verarbeiten kann.

Bild 15.27 Die Ordnerumleitung warnt vor verzögerter Verarbeitung.

Das Systemprotokoll: Im Systemprotokoll speichert der Gruppenrichtlinienclient allgemeine Informationen über erfolgreiche und fehlgeschlagene Verarbeitungszyklen.

Lizenziert für jonas@aeschlimann.cc
© 2016 Jonas Aeschlimann. Alle Rechte vorbehalten. Jede unerlaubte Weitergabe oder Vervielfältigung.

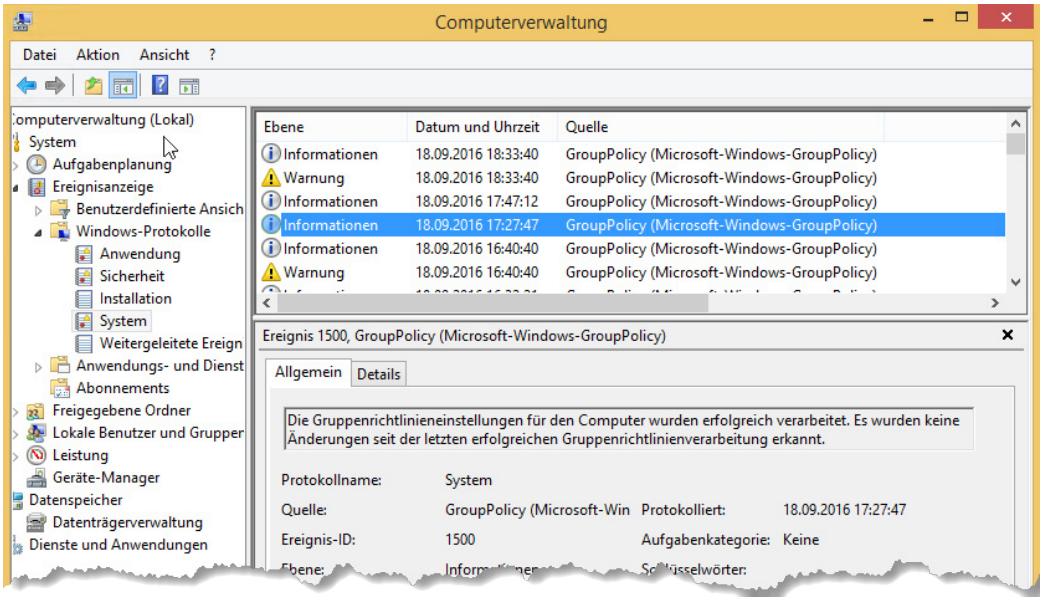

Bild 15.28 Das Systemlog speichert vor allem allgemeine Informationen.

Das GroupPolicy Operational Log[1]: Hier finden Sie die tatsächlich interessanten Informationen, denn hier legt der Gruppenrichtlinienclient sein detailliertes Log an. Diese Informationen werden zum Teil auch vom Gruppenrichtlinienergebnissatz angezeigt (siehe Bild 15.28).

Sie finden es unter den Anwendungsprotokollen. Öffnen Sie hierzu die Ereignisanzeige, und navigieren Sie zu `Anwendungs-und Dienstprotokolle > Microsoft > Windows > Group Policy`.

Hier finden Sie tatsächlich einen ganzen Sack voll von Ereignissen pro Gruppenrichtlinienverarbeitung. Der Gruppenrichtlinienclient protokolliert hier akribisch jede Client Side Extension mit ihrer Verarbeitungszeit. Er trägt hier auch ein, ob er einen Slow Link gefunden hat, ob der Loopbackmodus aktiviert war usw. Im Prinzip können Sie dem Client hier bei der Arbeit zusehen.

Damit Sie nachvollziehen können, welche Ereignisse zu welchem Durchlauf gehören, schreibt der Gruppenrichtlinienclient in jedes Event eine Correlation-ID. Man kann sie anzeigen, indem man das Event öffnet und unter DETAILS ein wenig nach unten scrollt. Die Correlation-ID ist einfach eine ID, die den Verarbeitungsdurchlauf identifiziert. Alle Events des gleichen Verarbeitungsdurchlaufs haben die gleiche Correlation-ID. Mithilfe von Filtern oder mithilfe von PowerShell können Sie die Correlation-ID nutzen, um sich nur die Ereignisse eines spezifischen Durchlaufs anzusehen. Hierzu können Sie auch die Funktion `Get-GPEvent` aus dem PowerShell-Modul zum Buch verwenden, die ich Ihnen zur Verfügung stelle.

[1] Der englische Name ist „Operational“, was im Deutschen mit „Betriebsbereit“ übersetzt wurde …

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe oder Vervielfältigung.

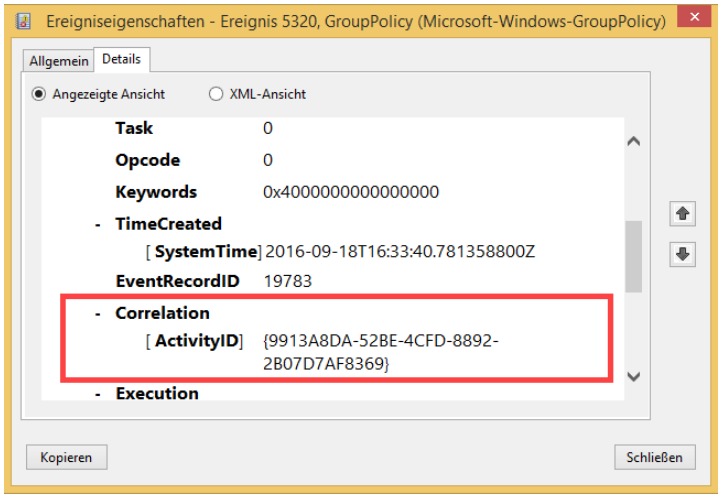

Bild 15.29 Die Correlation-ID identifiziert zusammenhängende Ereignisse.

Die wichtigsten Event-IDs sind:

ID	Bedeutung
4016	Start der Gruppenrichtlinienverarbeitung
5016	Ende der Gruppenrichtlinienverarbeitung
5312	Gruppenrichtlinien, die angewendet werden
5317	Gruppenrichtlinien, die abgelehnt wurden
8000, 8001	Verarbeitungszeit für Computer- und Benutzerrichtlinie beim Starten bzw. Anmelden
8006,8007	Verarbeitungszeit für Computer- und Benutzerrichtlinie während der Hintergrundaktualisierung

Eine Auflistung aller Event-IDs und ihrer Bedeutung finden Sie bei Microsoft unter *https://technet.microsoft.com/en-us/library/cc749336(v=ws.10).aspx*.

Ein hilfreiches Kommandozeilen-Tool, das Ihnen alle relevanten Einträge aus dem Eventlog zur besseren Analyse in ein Textfile (HTML, XML, TXT) exportieren kann, ist gplogview, das Sie bei Microsoft unter *https://www.microsoft.com/en-us/download/details.aspx?id=11147* beziehen können.

15.6 Debug-Logging

Wenn Ihnen die Informationen nicht ausreichen, die Ihnen das Eventlog zur Verfügung stellt, können Sie auch noch ein erweitertes Debug-Logging aktivieren. Das Debug-Logging erzeugt eine Textdatei namens GPSvc.Log im Ordner %windir%\debug\usermode. Hier folgt ein kleiner Ausschnitt aus der Datei.

Lizenziert für jonas@aeschlimann.cc.
© 2015 Microsoft Press. Alle Rechte vorbehalten. Jede unerlaubte Weitergabe oder Vervielfältigung.

Listing 15.1 Die GPSvc.Log protokolliert sehr ausführlich.

```
GPSVC(fcc.e18) 15:32:57:336 GroupPolicyClientServiceMain
GPSVC(fcc.e18) 15:32:57:351 CGPService::Start with flags = 0x0.
GPSVC(fcc.e18) 15:32:57:351 CGPService::Start: InstantiateGPEngine
GPSVC(fcc.e18) 15:32:57:351 CGPService::Start: GetAOACConfig
GPSVC(fcc.e18) 15:32:57:351 GetAOACConfig: dwAOACConfig was 0, setting to 600.
GPSVC(fcc.e18) 15:32:57:351 CGPService::Start: RegisterServiceCtrlHandlerEx
GPSVC(fcc.e18) 15:32:57:351 CGPService::Start: InitializeGPSubSystem
GPSVC(fcc.e18) 15:32:57:351 bMachine = 1
GPSVC(fcc.e18) 15:32:57:351 GPEventSubSystem::GPRegisterForWinLogonEventNotificati
                            on::++
GPSVC(fcc.e18) 15:32:57:367 GPEventSubSystem::GPRegisterForWinLogonEventNotificati
                            on::--
GPSVC(fcc.e18) 15:32:57:367 CGPService::InitializeRPCServer starting RPCServer.
GPSVC(fcc.e18) 15:32:57:367 Creating a New Instance of CGPRPCService
GPSVC(fcc.e18) 15:32:57:367 Created a New Instance of CGPRPCServerBase
GPSVC(fcc.e18) 15:32:57:367 Setting Singleton Instance of CGPRPCServerBase
GPSVC(fcc.e18) 15:32:57:367 CGPService::InitializeRPCServer finished starting
                            RPCServer. status 0x0
GPSVC(fcc.e18) 15:32:57:367 CGPService::Start: CreateGPSessions
GPSVC(fcc.e18) 15:32:57:367 Detected that the service has been restarted after
                            machine startup
```

Sie können das Debug-Logging über die Registry aktivieren:

Schlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics`

Wert: `"GPSvcDebugLevel"`

Eintrag: `dword:00030002`

Alternativ können Sie den Wert auch über die PowerShell-Funktion `Enable-GPSvcDebugLogging` aus dem PowerShell-Modul zum Buch aktivieren und deaktivieren.

Die Daten aus dem Debug-Log zu interpretieren ist schon aufgrund der schieren Größe gar nicht so leicht. Ein hilfreiches Werkzeug ist hier der kostenlose Policy Reporter, der die Daten strukturiert darstellt und gruppiert. Sie können ihn unter *http://www.sysprosoft.com/policyreporter.shtml* herunterladen.

Lizenziert für jonas@aeschlimann.cc.
© 2016 Carl Hanser Fachbuchverlag. Alle Rechte vorbehalten. Keine unerlaubte Weitergabe oder Vervielfältigung.

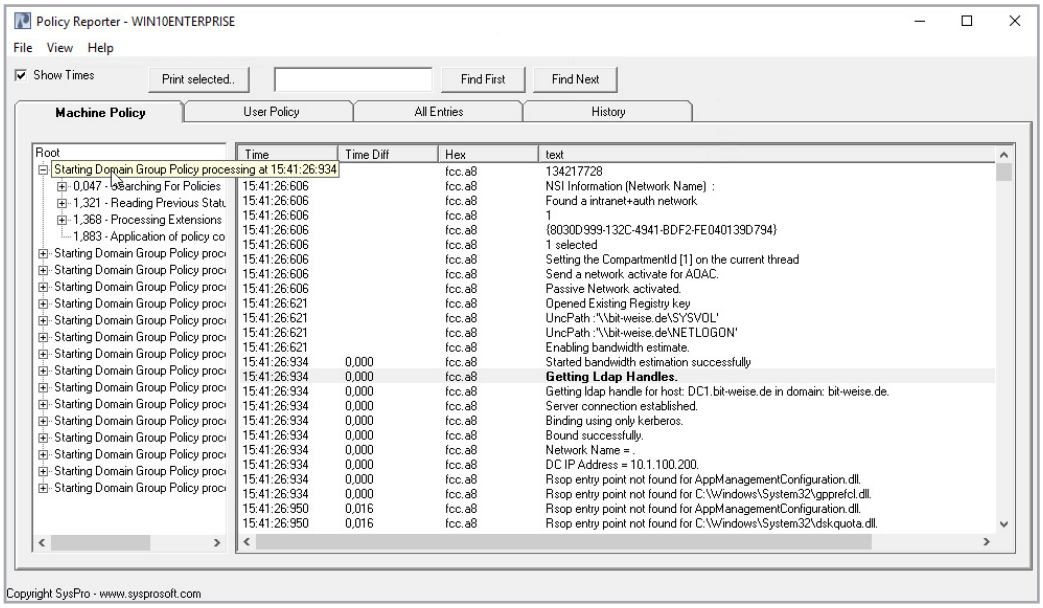

Bild 15.30 Der Policy Reporter erleichtert die Auswertung des GPSvc.Log.

Einen sehr guten, mehrteiligen Blog, der erklärt, wie man das GPSvc.Log liest, finden Sie unter *https://blogs.technet.microsoft.com/askds/2008/11/11/understanding-how-to-read-a-userenv-log-part-1/*.

15.7 Performanceanalyse

Wenn Ihre Anmelde- und Startprozesse langsam sind, könnte das an der Gruppenrichtlinienverarbeitung liegen. Allerdings ist es gar nicht so einfach, den Startprozess zu überwachen. Ich biete Ihnen hier drei mögliche Lösungswege an.

Zum einen können Sie das Group Policy Operational Log (s. Abschnitt 15.5) nutzen, um die Startzeit und die Endzeit der Gruppenrichtlinienverarbeitung zu ermitteln. Dabei helfen Ihnen die Events mit der EventID 4016 und 5016, die den Startzeitpunkt und den Endzeitpunkt der Verarbeitung markieren. Zusätzlich hilft Ihnen die Correlation-ID, die zur Verarbeitung gehörenden Event-Einträge zu finden.

Alternativ können Sie das Kommandozeilentool gptime.exe vom GPO-Guy verwenden, das Sie nach einer Registrierung kostenlos herunterladen können. Es macht nichts anderes, als die Eventlogs abzufragen, aber Sie müssen die Daten nicht mehr manuell suchen.

Lizenziert für jonas@aeschlimann.cc
© 2016 Hanser ... unerlaubte Weitergabe oder Vervielfältigung.

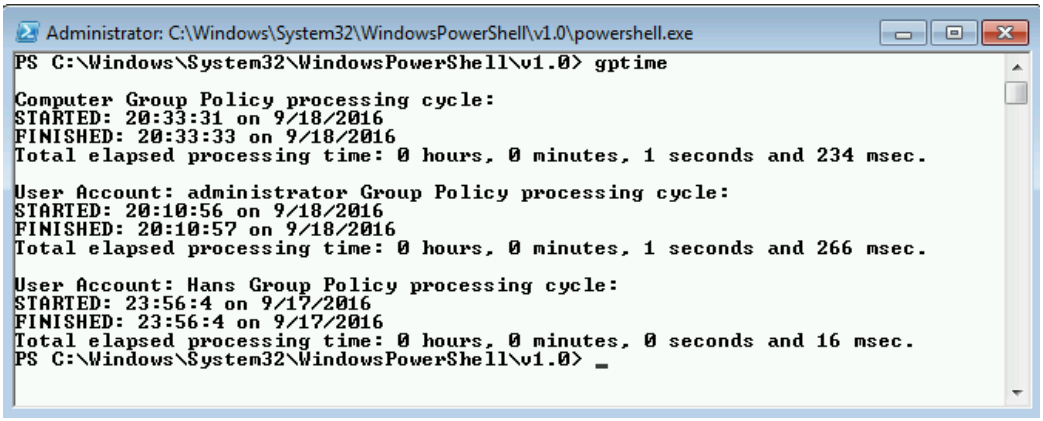

Bild 15.31 gptime gibt die Laufzeiten der Richtlinienverarbeitung aus.

Wenn Sie auf diesem Weg nicht weiter kommen, gibt es weitere Möglichkeiten, den Startvorgang zu überwachen. Ein äußerst nützliches Tool zum Überwachen des Startvorgangs ist das Sysinternals-Tool Procmon, das sämtliche Zugriffe auf Registry, Dateisystem, Netzwerk und Prozessaktivitäten protokollieren und anzeigen kann. Procmon läuft normalerweise interaktiv und zeigt die laufenden Systemzugriffe, aber man kann auch eine Bootprotokollierung aktivieren, die dann alle Zugriffe während des Startvorgangs protokolliert. Sie können das Programm direkt bei Microsoft unter *https://technet.microsoft.com/de-de/sysinternals/processmonitor.aspx* herunterladen.

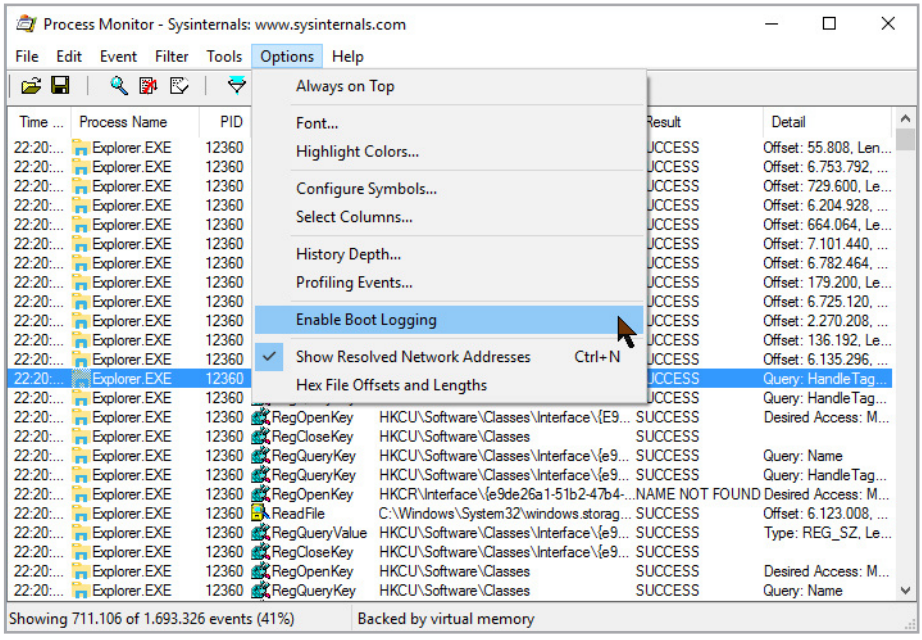

Bild 15.32 Procmon – Enable Boot Logging