

praxisnah
& kompetent

Das KOCHBUCH

Microsoft

Windows Server 2019

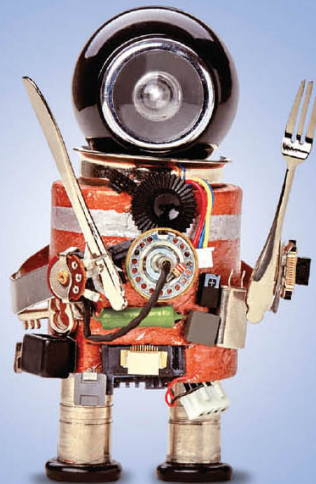
Automatisierung mit

PowerShell

Praxiserprobte Rezepte zur
Automatisierung und Verwaltung
von Administrationsaufgaben



Thomas Lee



O'REILLY®

Inhalt

Cover

Titel

Impressum

Inhaltsverzeichnis

Über den Autor

Danksagungen

Über den Fachlektor der Originalausgabe

Vorwort

Einleitung

In diesem Buch

Was brauchen Sie für dieses Buch?

Für wen ist dieses Buch?

Das Buch optimal nutzen

Konventionen in diesem Buch

Abschnitte und Aufbau der Rezepte

Überschriften der Kapitel und der Rezepte

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Die Begleitdateien

Support und Feedback

1 PowerShell-Umgebung für die Systemverwaltung einrichten

Einführung

Remoteserver-Verwaltungstools auf Windows 10 und Windows Server 2019 installieren

- Vorbereitungen

- So wird's gemacht

- So funktioniert's

- Weitere Informationen

Paketverwaltung kennenlernen

- Vorbereitungen

- So wird's gemacht

- So funktioniert's

- Weitere Informationen

PowerShellGet und den PowerShell-Katalog kennenlernen

- Vorbereitungen

- So wird's gemacht

- So funktioniert's

- Weitere Informationen

- Siehe auch ...

Ein internes PowerShell-Repository erstellen

- Vorbereitungen

- So wird's gemacht

- So funktioniert's

- Weitere Informationen

Eine Umgebung für die Codesignierung einrichten

- Vorbereitungen

- So wird's gemacht

- So funktioniert's

- Weitere Informationen

Just Enough Administration implementieren

Vorbereitungen
So wird's gemacht
So funktioniert's
Weitere Informationen
Siehe auch ...

2 Windows-Netzwerke verwalten

Einführung

Neue Wege, um Altbekanntes zu tun

Vorbereitungen
So wird's gemacht
So funktioniert's
Weitere Informationen

IP-Adressen konfigurieren

Vorbereitungen
So wird's gemacht
So funktioniert's
Weitere Informationen

Einen DHCP-Server installieren und autorisieren

Vorbereitungen
So wird's gemacht
So funktioniert's
Weitere Informationen

DHCP-Bereiche konfigurieren

Vorbereitungen
So wird's gemacht
So funktioniert's
Weitere Informationen

Statt statischer IP-Adresse DHCP verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

DHCP-Failover und Lastenausgleich konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

DNS-Server, Zonen und Ressourceneinträge konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

3 Windows Active Directory verwalten

Einführung

Active Directory mit DNS installieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

AD-Benutzer, Gruppen und Computer erstellen und verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Benutzer aus einer CSV-Datei in AD importieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Ein Gruppenrichtlinienobjekt erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Berichte zu AD-Benutzern

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Inaktive Computer und Benutzer im AD finden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

4 Windows-Speichertechnologien verwalten

Einführung

Physikalische Datenträger und logische Laufwerke verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

NTFS-Berechtigungen verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Speicherreplikate verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Kontingente für Dateiserver verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Speicherberichte verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

5 Freigegebene Daten verwalten

Einführung

Einen SMB-Dateiserver einrichten und absichern

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

SMB-Freigaben erstellen und absichern

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Auf Daten auf SMB-Freigaben zugreifen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Ein iSCSI-Ziel erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Ein iSCSI-Ziel verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Einen DFS-Namespace konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

DFS-Replikation konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

6 Windows Update verwalten

Einführung

Windows Server Update Services installieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

WSUS-Update-Synchronisierung konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Den Windows Update-Client konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Computer-Zielgruppen erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Automatische Genehmigungen für WSUS konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

WSUS-Updates verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

7 Windows-Druckumgebung verwalten

Einführung

Drucker installieren und freigeben

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Einen Drucker veröffentlichen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Spoolerverzeichnis ändern

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Druckertreiber ändern

Vorbereitungen

So wird's gemacht

So funktioniert's

Eine Testseite drucken

Vorbereitungen

So wird's gemacht

So funktioniert's

Druckerberechtigungen verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Einen Druckerpool einrichten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

8 Einführung in Container

Einführung

Einen Container-Host konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Eine Hello World-Beispielanwendung bereitstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

IIS in einem Container bereitstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Ein Dockerfile verwenden, um einen Container zu erstellen und zu verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

9 Internetinformationsdienste verwalten

Einführung

IIS installieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

IIS für SSL konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

TLS-Verschlüsselungssuites verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Einen zentralen Zertifikatsspeicher konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

IIS-Bindungen konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

IIS-Protokollierung und Protokolldateien verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

IIS-Anwendungen und Anwendungspools verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

IIS-Protokolldateien analysieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Netzwerklastenausgleich verwalten und überwachen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

10 Desired State Configuration verwalten

Einführung

DSC und integrierte Ressourcen verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

DSC-Konfiguration mit Parametern versehen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

DSC-Ressourcen finden und installieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

DSC mit Ressourcen aus der PowerShell-Gallery nutzen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Den lokalen DSC-Konfigurations-Manager konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Einen DSC-SMB-Pullserver implementieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Einen DSC-HTTP-Pullserver implementieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

DSC-Teilkonfigurationen verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

11 Hyper-V verwalten

Einführung

Hyper-V installieren und konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Eine VM erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

PowerShell Direct verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

VM-Gruppen verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

VM-Hardware konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Netzwerke in Hyper-V konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Verschachtelte Hyper-V-Virtualisierung implementieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

VM-Status verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

VMs und VM-Datenträger verschieben

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

VM-Replikation konfigurieren

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

VM-Prüfpunkte verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

12 Azure verwalten

Einführung

PowerShell mit Azure verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Azure-Kernressourcen erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Erforschen Sie Ihr Speicherkonto

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Erstellen einer SMB-Dateifreigabe in Azure Files

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Eine Azure-Website erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

Eine Azure-VM erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Siehe auch ...

13 Leistung und Nutzung überwachen

Einführung

Leistungsindikatoren mit Get-Counter abrufen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Leistungsindikatoren mit WMI abrufen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

PLA-Datensammlersätze erstellen und verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Berichte mit den Leistungsdaten erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Die Leistungsüberwachung als Diagramm darstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Den Systemdiagnosebericht erstellen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Bericht zur Druckernutzung

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Hyper-V-Nutzung und Performance überwachen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

14 Probleme mit Windows Server lösen

Einführung

Netzwerkonnektivität überprüfen

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Den Best Practices Analyzer verwenden

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Ereignisprotokolle verwalten

Vorbereitungen

So wird's gemacht

So funktioniert's

Weitere Informationen

Index

Kapitel 4

Windows-Speichertechnologien verwalten

In diesem Kapitel werden die folgenden Rezepte vorgestellt:

- **Physikalische Datenträger und Volumes verwalten**
- **NTFS-Berechtigungen verwalten**
- **Speicherreplikate verwalten**
- **Kontingente für Dateiserver verwalten**
- **Speicherberichte verwenden**

Einführung

Windows Server 2019 stellt einen ganzen Satz von Features zur Verfügung, die es erlauben, unterschiedliche Speicherarten und Storage-Technologien zu verwenden. Windows unterstützt die klassischen Festplatten, USB-Speichersticks und SSD-Datenträger (einschließlich NVMe SSD).

Bevor ein Datenträger verwendet werden kann, müssen Sie auf dem Gerät Partitionen oder Volumes (logische Laufwerke) erstellen und anschließend das Volume formatieren. Wenn Sie einen Datenträger initialisieren, müssen Sie festlegen, welches Partitionsschema verwendet werden soll. Sie haben zwei Optionen: **Master Boot Record (MBR)** oder **GUID-Partitionstabelle (GPT)**. Eine gute Erörterung der Unterschiede zwischen diesen beiden Mechanismen finden Sie hier:

<https://www.howtogeek.com/193669/whats-the-difference-between-gptand-mbr-when-partitioning-a->

drive.

Nachdem das logische Laufwerk erstellt ist, können Sie den Datenträger formatieren. Windows unterstützt fünf wesentliche Dateisysteme, die Sie verwenden können: ReFS, NTFS, exFAT, UDF und FAT32. Details zu den vier letztgenannten finden Sie unter: <https://docs.microsoft.com/en-us/windows/desktop/fileio/filesystem-functionality-comparison>. Das ReFS-Dateisystem ist neuer, basiert auf NTFS, jedoch stellt es einige Features nicht zur Verfügung, die ein Dateiserver möglicherweise benötigt (ReFS unterstützt keine verschlüsselten Dateien). Einen Vergleich der Dateisysteme ReFS und NTFS finden Sie unter <https://www.iperiusbackup.net/de/10148>. Sie werden im Rezept »Physikalische Datenträger und logische Laufwerke verwalten« auf Seite 118 das Partitionieren und das Formatieren von Volumes untersuchen.

NTFS- (und ReFS)-Volumes erlauben das Erstellen von **Zugriffssteuerungslisten (access control lists, ACLs)**, die den Zugriff auf die Dateien und Ordner steuern, die sich in Windows-Volumes befinden. Die Verwaltung der Zugriffssteuerungslisten ist ein wenig schwierig und die Unterstützung von PowerShell ist in diesem Bereich nur rudimentär. Um die ACLs auf Windows-Datenträgern zu verwalten, können Sie, wie Sie im Rezept »NTFS-Berechtigungen verwalten« auf Seite 123 sehen werden, NTFSSecurity herunterladen, ein Modul eines Drittanbieters.

Das Feature **Ressourcen-Manager für Dateiserver (File Server Resource Manager, FSRM)** in Windows Server 2019 hilft Ihnen dabei, Ressourcen zu verwalten, auf denen Dateien gespeichert werden. Mit FSRM können Sie Kontingente für das Speichern von Dateien erstellen. Bei weichen Kontingenten können Benutzer das Kontingent überschreiten und die Administratoren werden benachrichtigt, wenn dies passiert. Bei harten Kontingenten können die Benutzer keine Dateien mehr abspeichern, wenn sie den zugeteilten Speicherplatz komplett verbraucht haben. Sie werden die Verwaltung von Kontingenten im Rezept »Kontingente für Dateiserver verwalten« auf Seite 133 kennenlernen.

FSRM unterstützt außerdem das Erstellen von Berichten über Dateiserver, was Sie im Rezept »Speicherberichte verwenden« auf Seite 141 untersuchen werden. Diese Berichte und die hierbei erstellten XML-Dateien können bei der Verwaltung und der Überwachung von Dateiservern hilfreich sein.

Dieses Kapitel und insbesondere das Rezept »Kontingente für Dateiserver verwalten« auf Seite 133 verwendet ein kostenloses E-Mail-Konto von [Sendgrid.com](https://sendgrid.com). Dies erlaubt Ihnen, den Windows SMTP-Server so zu konfigurieren, dass er Mails an SendGrid weiterleitet, von wo aus die E-Mails an ihre Empfänger verschickt werden. Dies kann ein guter Weg sein, um die Berichterstellung zu testen und um Probleme mit internen SMTP-Servern zu vermeiden.

Physikalische Datenträger und logische Laufwerke verwalten

Windows Server 2019 setzt einen Computer mit mindestens einem Laufwerk voraus (das Laufwerk C:\). Die Datenträger können über verschiedene Bussysteme wie beispielsweise IDE, SATA, SAS oder USB angeschlossen sein. Bevor Sie in Windows einen Datenträger verwenden können, müssen Sie ihn initialisieren und Partitionen oder logische Laufwerke erstellen.

Es gibt zwei Partitionsschemata, die Sie verwenden können. Das ältere Master Boot Record-Format (MBR) und die neue GUID-Partitionstabelle (GPT). Das MBR-Schema, das erstmalig mit PC DOS 2 im Jahre 1983 eingeführt wurde, weist eine Reihe von Einschränkungen auf. So unterstützt MBR nur Partitionen, die maximal 2 TB groß sein können. Wenn Sie mehr als vier Partitionen erstellen wollen, müssen Sie zuerst eine erweiterte Partition erstellen und dann innerhalb der erweiterten Partition weitere Partitionen erstellen. Das GPT-Schema unterstützt hingegen viel größere Laufwerke (die maximale Partitionsgröße hängt vom Betriebssystem ab) sowie bis zu 128 Partitionen je Datenträger.

In diesem Rezept erweitern Sie Server SRV1 um zwei weitere Datenträger und erstellen anschließend auf den neuen Datenträgern Volumes und Partitionen.

Vorbereitungen

Sie führen dieses Rezept auf SRV1 aus. Um das Rezept nutzen zu können, benötigt SRV1 zwei weitere Datenträger. Falls Sie eine Hyper-V-VM verwenden, um das Rezept zu testen, können Sie das folgende Skript verwenden, um die erforderlichen Datenträger zu erstellen. Führen Sie dieses Skript auf dem Hyper-V-Host aus, der die VM SRV1 hostet:

```
# Auf SRV1 virtuelle Datenträger erstellen, die in die VM
eingehängt werden
```

```
New-VHD -Path D:\v6\SRV1\SRV1-F.vhdx -SizeBytes 20gb -Dynamic
```

```
New-VHD -Path D:\v6\SRV1\SRV1-G.vhdx -SizeBytes 20gb -Dynamic
```

```
# Datenträger in die VM einhängen
```

```
$HDHT1 = @{
```

```
    VMName = 'SRV1'
```

```
    Path = 'D:\v6\SRV1\SRV1-F.vhdx'
```

```
    controllerType = 'SCSI'
```

```
    controllerNumber = 0
```

```
}
```

```
Add-VMHardDiskDrive @HDHT1
```

```
$HDHT2 = @{
```

```
    VMName = 'SRV1'
```

```
    Path = 'D:\v6\SRV1\SRV1-G.vhdx'
```

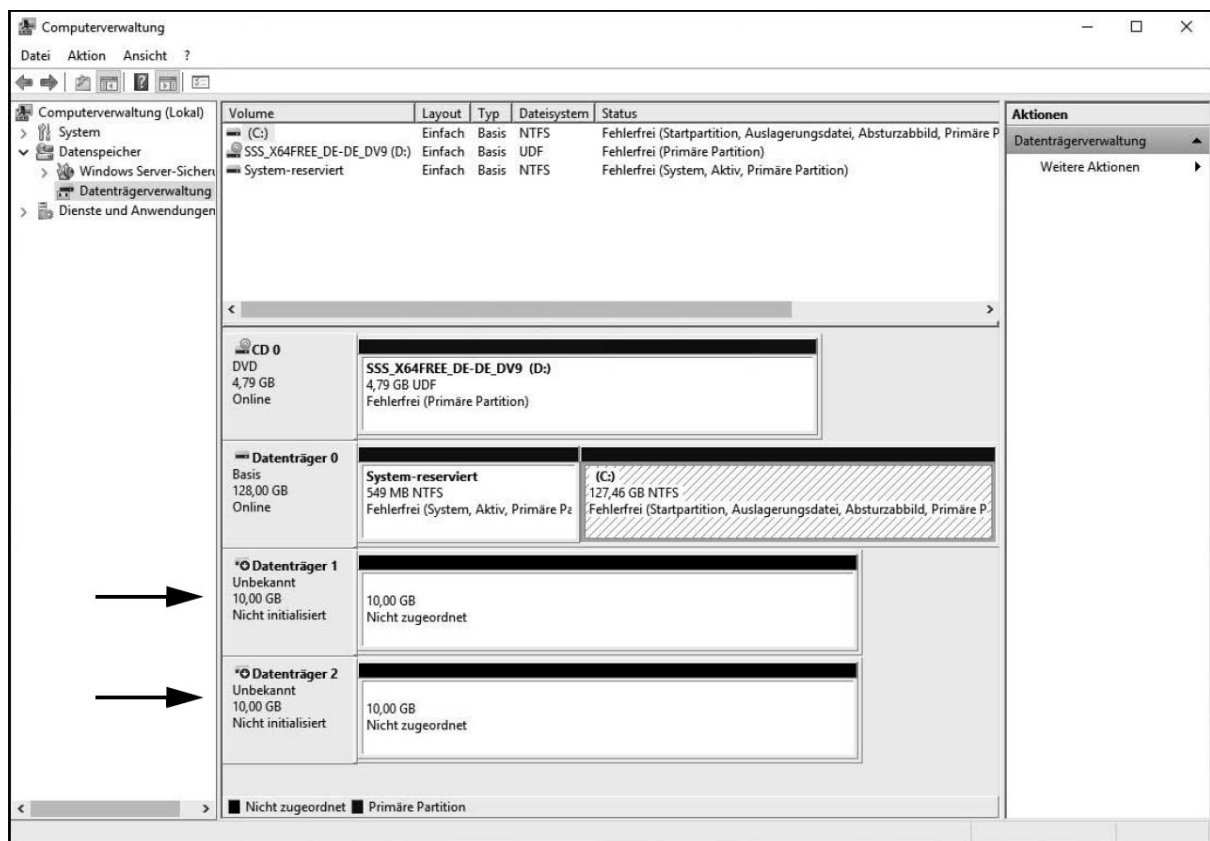
```
    controllerType = 'SCSI'
```

```
    controllerNumber = 0
```

```
}
```

Add-VMHardDiskDrive @HDHT2

In den Begleitdateien für dieses Buch (siehe Einleitung) befindet sich ein Skript, Add-Disksto-Srv1+2.ps1, das die Datenträger, die in diesem und anderen Rezepten dieses Kapitels verwendet werden, erstellt. Nachdem Sie die virtuellen Datenträger zum Server SRV1 hinzugefügt haben, können Sie die **Datenträgerverwaltung**, ein MMC-Snap-In, verwenden, und sich die Ausgangskonfiguration für dieses Rezept ansehen:



So wird's gemacht

1. Rufen Sie die für das System sichtbaren Datenträger auf:

Get-Disk |

Format-Table -AutoSize

2. Initialisieren Sie, falls erforderlich, die Datenträger mit dem GPT-Schema:

```
Get-Disk |  
  
Where PartitionStyle -eq Raw |  
  
Initialize-Disk -PartitionStyle GPT
```

3. Zeigen Sie die Datenträger erneut an:

```
Get-Disk |  
  
Format-Table -AutoSize
```

4. Erstellen Sie auf Datenträger 1 das logische Laufwerk F :

```
$NVHT1 = @{  
  
    DiskNumber    = 1  
  
    FriendlyName  = 'Storage(F)'  
  
    FileSystem    = 'NTFS'  
  
    DriveLetter   = 'F'  
  
}  
  
New-Volume @NVHT1
```

5. Erstellen Sie auf Datenträger 2 zwei logische Laufwerke; zuerst wird das Laufwerk G: erstellt:

```
New-Partition -DiskNumber 2 -DriveLetter G -Size 4gb
```

6. Erstellen Sie eine zweite Partition H::

```
New-Partition -DiskNumber 2 -DriveLetter H -UseMaximumSize
```

7. Formatieren Sie die Laufwerke G: und H::

```
$NVHT1 = @{
```

```
    DriveLetter      = 'G'
```

```
    FileSystem       = 'NTFS'
```

```
    NewFileSystemLabel = 'Log'}
```

```
Format-Volume @NVHT1
```

```
$NVHT2 = @{
```

```
    DriveLetter      = 'H'
```

```
    FileSystem       = 'NTFS'
```

```
    NewFileSystemLabel = 'GDShow'}
```

```
Format-Volume @NVHT2
```

8. Rufen Sie die auf dem System vorhandenen Partitionen ab:

```
Get-Partition |
```

```
Sort-Object -Property DriveLetter |
```

```
Format-Table -Property DriveLetter, Size, Type
```

9. Rufen Sie die Volumes auf SRV1 ab:

```
Get-Volume |
```

```
Sort-Object -Property DriveLetter
```

So funktioniert's

In *Schritt 1* sehen Sie sich die auf SRV1 verfügbaren Datenträger an und erkennen die beiden neuen Datenträger:

```
PS C:\foo> Get-Disk | Format-Table -AutoSize
```

Number	Friendly Name	Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
0	Virtual HD		Healthy	Online	128 GB	MBR
1	Msft Virtual Disk		Healthy	Online	10 GB	RAW
2	Msft Virtual Disk		Healthy	Online	10 GB	RAW

In *Schritt 2* initialisieren Sie die beiden neuen Datenträger; dieser Schritt erzeugt keine Ausgabe. In *Schritt 3* zeigen Sie die Datenträger erneut an und erhalten diese Ausgabe:

```
PS C:\foo> Get-Disk | Format-Table -AutoSize
```

Number	Friendly Name	Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
0	Virtual HD		Healthy	Online	128 GB	MBR
1	Msft Virtual Disk		Healthy	Online	10 GB	GPT
2	Msft Virtual Disk		Healthy	Online	10 GB	GPT

In *Schritt 4* verwenden Sie das Cmdlet `New-Volume`, um ein logisches Laufwerk zu erstellen und zu partitionieren, und zwar auf dem ersten neuen

Datenträger. Sie erhalten diese Ausgabe:

```
PS C:\foo> $NVHT1 = @{
    DiskNumber = 1
    FriendlyName = 'Storage(F)'
    FileSystem = 'NTFS'
    DriveLetter = 'F'
}
PS C:\foo> New-Volume @NVHT1
```

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
F	Storage(F)	NTFS	Fixed	Healthy	OK	9.94 GB	9.98 GB

In *Schritt 5* erstellen Sie die erste von zwei Partitionen auf dem zweiten Datenträger, der zu SRV1 hinzugefügt wurde. Dieser Schritt sieht wie folgt aus:

```
PS C:\foo> New-Partition -DiskNumber 2 -DriveLetter G -Size 4gb
```

```
DiskId      : \\?\ide#diskvirtual_hd_____1.1.1_#5&cfb56de&0&1.1.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
DiskNumber  : 2
DriveLetter : G
Offset      : 16777216
OperationalStatus : Online
PartitionNumber : 2
Size        : 4294967296
Type        : Basic
DiskPath    : \\?\ide#diskvirtual_hd_____1.1.1_#5&cfb56de&0&1.1.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
(... Ausgabe etwas gekürzt)
```

In *Schritt 6* erstellen Sie eine zweite Partition auf dem zweiten Datenträger; dies wird Laufwerk H: . Dieser Schritt sieht wie folgt aus:

```
PS C:\foo> New-Partition -DiskNumber 2 -DriveLetter H -UseMaximumSize
```

```
DiskId      : \\?\ide#diskvirtual_hd_____1.1.1_#5&cfb56de&0&1.1.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
DiskNumber  : 2
DriveLetter : H
Offset      : 4311744512
OperationalStatus : Online
PartitionNumber : 3
Size        : 6424625152
Type        : Basic
DiskPath    : \\?\ide#diskvirtual_hd_____1.1.1_#5&cfb56de&0&1.1.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
(... Ausgabe etwas gekürzt)
```

In *Schritt 7* formatieren Sie die beiden Partitionen, die Sie soeben erstellt haben, was wie folgt aussieht:

```
PS C:\foo> $NVHT1 = @{
    DriveLetter = 'G'
    FileSystem = 'NTFS'
    NewFileSystemLabel = 'Log'
}
PS C:\foo> Format-Volume @NVHT1
PS C:\foo> $NVHT2 = @{
    DriveLetter = 'H'
    FileSystem = 'NTFS'
    NewFileSystemLabel = 'GDShow'
}
PS C:\foo> Format-Volume @NVHT2
```

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
G	Log	NTFS	Fixed	Healthy	OK	3.97 GB	4 GB
H	GDShow	NTFS	Fixed	Healthy	OK	5.95 GB	5.98 GB

In *Schritt 8* verwenden Sie das Cmdlet `Get-Partition`, um die Partitionen auf Server SRV1 abzurufen, und erhalten diese Ausgabe:

```
PS C:\foo> Get-Partition |
Sort-Object -Property DriveLetter |
Format-Table -Property DriveLetter, Size, Type
```

DriveLetter	Size	Type
	575668224	IFS
	16759808	Reserved
	16759808	Reserved
C	136861188096	IFS
F	10719592448	Basic
G	4294967296	Basic
H	6424625152	Basic

In *Schritt 9* verwenden Sie das Cmdlet `Get-Volume`, um eine Liste der logischen Laufwerke auf Server SRV1 abzurufen, was wie folgt aussieht:

```
PS C:\foo> Get-Volume |
Sort-Object -Property DriveLetter
```

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
	System-reserviert	NTFS	Fixed	Healthy	OK	108.3 MB	549 MB
A		Unknown	Removable	Healthy	Unknown	0 B	0 B
C		NTFS	Fixed	Healthy	OK	117.52 GB	127.46 GB
D	SSS_X64FREE_DE-DE_DV9	Unknown	CD-ROM	Healthy	OK	0 B	4.79 GB
F	Storage(F)	NTFS	Fixed	Healthy	OK	9.94 GB	9.98 GB
G	Log	NTFS	Fixed	Healthy	OK	3.97 GB	4 GB
H	GDSHOW	NTFS	Fixed	Healthy	OK	5.95 GB	5.98 GB

Weitere Informationen

Im Abschnitt »Vorbereitungen« dieses Rezepts haben Sie zwei neue Datenträger zu SRV1 hinzugefügt. Diese neuen Datenträger sind nicht initialisiert. Daher ist das Erste, was Sie in *Schritt 1* getan haben, diese Datenträger zu initialisieren.

In *Schritt 4* erstellen Sie ein neues Laufwerk auf Datenträger 1. Hierdurch wird das Laufwerk partitioniert und formatiert. In *Schritt 5* und *Schritt 6* erstellen Sie auf Datenträger 2 zwei neue Partitionen, die Sie in *Schritt 7* formatieren. Sie haben so zwei Methoden kennengelernt, um auf einem Datenträger Laufwerke zu erstellen.

In *Schritt 8* und *Schritt 9* verwenden Sie verschiedene Cmdlets, um die im Prinzip gleichen Objekte zurückzugeben: die Laufwerke/Partitionen auf SRV1.

NTFS-Berechtigungen verwalten

Jede Datei und jeder Ordner im NTFS-Dateisystem besitzt eine **Zugriffssteuerungsliste (Access Control List, ACL)**. Jede ACL wiederum enthält einen Satz von **Zugriffssteuerungseinträgen (Access Control Entries, ACEs)**.

Jeder Zugriffssteuerungseintrag definiert für ein Konto die Berechtigungen für eine Datei oder einen Ordner. So könnte beispielsweise der globalen AD-Gruppe SaLes Vollzugriff auf eine Datei erteilt werden.

Berechtigungen können auch von übergeordneten Ordnern geerbt werden. Wenn Sie einen neuen Ordner und dann in diesem neuen Ordner eine Datei erstellen, erbt die neue Datei standardmäßig die Berechtigungen vom übergeordneten Ordner und des übergeordneten Ordners dieses Ordners. Sie können die Zugriffssteuerungsliste bearbeiten, Berechtigungen hinzufügen oder entfernen sowie die Vererbungseinstellungen anpassen.

Die Unterstützung von PowerShell für die Verwaltung der NTFS-Berechtigungen ist begrenzt. Zwar kennt PowerShell die Cmdlets `Get-ACL` und `Set-ACL`, jedoch müssen Sie für das Erstellen von individuellen Zugriffssteuerungseinträgen standardmäßig auf das .NET Framework zurückgreifen. Ein einfacherer Ansatz besteht darin, ein Modul eines Drittanbieters zu verwenden, in diesem Fall `NTFSSecurity`, mit dem die Verwaltung von ACEs und ACLs, einschließlich der Vererbungseinstellungen, erheblich einfacher ist.

Vorbereitungen

Dieses Rezept verwendet `SRV1`, einen universellen Server, der der Domäne beigetreten ist und auf dem Windows Server 2019 ausgeführt wird. Außerdem muss ein Domänencontroller (beispielsweise `DC1`) laufen und erreichbar sein. Die Gruppe `SaLes` sollte im Active Directory vorhanden sein; falls sie noch nicht vorhanden ist, wird sie vom Rezept erstellt. Sie sollten ein Benutzerkonto verwenden, das Mitglied der Gruppe Domänen-Admins ist und das Rezept in einer Konsole mit erhöhten Rechten ausführen. Außerdem sollten auf `SRV1` die AD Remoteserver-Verwaltungstools geladen sein.

So wird's gemacht

1. Laden Sie das Modul `NTFSSecurity` von `PSGallery` herunter und installieren Sie es:

```
Install-Module NTFSSecurity -Force
```

2. Lassen Sie eine Liste aller Befehle dieses Moduls anzeigen:

```
Get-Command -Module NTFSSecurity
```

3. Erstellen Sie einen neuen Ordner und dann eine neue Datei in diesem Ordner:

```
New-Item -Path C:\Secure1 -ItemType Directory |
```

```
Out-Null
```

```
"Secure" | Out-File -FilePath C:\Secure1\Secure.Txt
```

```
Get-ChildItem -Path c:\Secure1
```

4. Lassen Sie die ACL dieses Ordners anzeigen:

```
Get-NTFSAccess -Path C:\Secure1 |
```

```
Format-Table -AutoSize
```

5. Lassen Sie die ACL der Datei anzeigen:

```
Get-NTFSAccess C:\Secure1\Secure.Txt |
```

```
Format-Table -AutoSize
```

6. Erstellen Sie die Gruppe SaLes, falls diese noch nicht existiert:

```
try {
```

```

    Get-ADGroup -Identity 'Sales' -ErrorAction Stop
}

catch {

    New-ADGroup -Name Sales -GroupScope Global |

        Out-Null

}

```

7. Lassen Sie Informationen zu der Gruppe anzeigen:

```
Get-ADGroup -Identity Sales
```

8. Erteilen Sie den Domänen-Admins explizit Vollzugriff auf den Ordner:

```

$AHT1 = @{

    Path          = 'C:\Secure1'

    Account       = 'Reskit\Domänen-Admins'

    AccessRights  = 'FullControl'

}

Add-NTFSAccess @AHT1

```

9. Entfernen Sie die Zugriffsrechte für VORDEFINIERT\Benutzer von der Datei secure.txt:

```
$AHT2 = @{  
  
    Path          = 'C:\Secure1\Secure.Txt'  
  
    Account       = 'VORDEFINIERT\Benutzer'  
  
    AccessRights  = 'FullControl'  
  
}  
  
Remove-NTFSAccess @AHT2
```

10. Entfernen Sie die vererbten Zugriffsrechte von diesem Ordner:

```
$IRHT1 = @{  
  
    Path          = 'C:\Secure1'  
  
    RemoveInheritedAccessRules = $True  
  
}  
  
Disable-NTFSAccessInheritance @IRHT1
```

11. Erteilen Sie der Gruppe Sa les Vollzugriff auf den Ordner:

```
$AHT3 = @{  
  
    Path          = 'C:\Secure1\  

```

```
Account      = 'Reskit\Sales'  
  
AccessRights = 'FullControl'  
  
}  
  
Add-NTFSAccess @AHT3
```

12. Rufen Sie die aktualisierte Zugriffssteuerungsliste des Ordners ab:

```
Get-NTFSAccess -Path C:\Secure1 |  
  
Format-Table -AutoSize
```

13. Rufen Sie die aktualisierte Zugriffssteuerungsliste der Datei ab:

```
Get-NTFSAccess -Path C:\Secure1\Secure.Txt |  
  
Format-Table -AutoSize
```

So funktioniert's

In *Schritt 1* laden Sie das Modul `NTFSSecurity` vom PowerShell-Katalog im Internet herunter und installieren es, was keine Ausgabe erzeugt. In *Schritt 2* verwenden Sie das Cmdlet `Get-Command`, um die Befehle anzuzeigen, die das Modul `NTFSSecurity` enthält, was wie folgt aussieht:

```

PS C:\foo> Get-Command -Module NTFSSecurity

```

CommandType	Name	Version	Source
Cmdlet	Add-NTFSAccess	4.2.6	NTFSSecurity
Cmdlet	Add-NTFSAudit	4.2.6	NTFSSecurity
Cmdlet	Clear-NTFSAccess	4.2.6	NTFSSecurity
Cmdlet	Clear-NTFSAudit	4.2.6	NTFSSecurity
Cmdlet	Copy-Item2	4.2.6	NTFSSecurity
Cmdlet	Disable-NTFSAccessInheritance	4.2.6	NTFSSecurity
Cmdlet	Disable-NTFSAuditInheritance	4.2.6	NTFSSecurity
Cmdlet	Disable-Privileges	4.2.6	NTFSSecurity
Cmdlet	Enable-NTFSAccessInheritance	4.2.6	NTFSSecurity
Cmdlet	Enable-NTFSAuditInheritance	4.2.6	NTFSSecurity
Cmdlet	Enable-Privileges	4.2.6	NTFSSecurity
Cmdlet	Get-ChildItem2	4.2.6	NTFSSecurity
Cmdlet	Get-DiskSpace	4.2.6	NTFSSecurity
Cmdlet	Get-FileHash2	4.2.6	NTFSSecurity
Cmdlet	Get-Item2	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSAccess	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSAudit	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSEffectiveAccess	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSHardLink	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSInheritance	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSOrphanedAccess	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSOrphanedAudit	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSOwner	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSSecurityDescriptor	4.2.6	NTFSSecurity
Cmdlet	Get-NTFSSimpleAccess	4.2.6	NTFSSecurity
Cmdlet	Get-Privileges	4.2.6	NTFSSecurity
Cmdlet	Move-Item2	4.2.6	NTFSSecurity
Cmdlet	New-NTFSHardLink	4.2.6	NTFSSecurity
Cmdlet	New-NTFSSymbolicLink	4.2.6	NTFSSecurity
Cmdlet	Remove-Item2	4.2.6	NTFSSecurity
Cmdlet	Remove-NTFSAccess	4.2.6	NTFSSecurity
Cmdlet	Remove-NTFSAudit	4.2.6	NTFSSecurity
Cmdlet	Set-NTFSInheritance	4.2.6	NTFSSecurity
Cmdlet	Set-NTFSOwner	4.2.6	NTFSSecurity
Cmdlet	Set-NTFSSecurityDescriptor	4.2.6	NTFSSecurity
Cmdlet	Test-Path2	4.2.6	NTFSSecurity

In *Schritt 3* erstellen Sie einen neuen Ordner, C:\Secure1, und eine Datei innerhalb dieses Ordners (C:\Secure1\Secure.Txt), was wie folgt aussieht:

```

PS C:\foo> New-Item -Path C:\Secure1 -ItemType Directory |
Out-Null
PS C:\foo> "Secure" | Out-File -FilePath C:\Secure1\Secure.Txt
PS C:\foo> Get-ChildItem -Path c:\Secure1

```

Verzeichnis: C:\Secure1

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	17.07.2019 09:57	18	Secure.Txt

In *Schritt 4* verwenden Sie das Cmdlet `Get-NTFSAccess`, um sich die ACL des Ordners `C:\Secure1` anzusehen, und erhalten die folgende Ausgabe:

```

PS C:\foo> Get-NTFSAccess -Path C:\Secure1 |
Format-Table -AutoSize

```

Path: C:\Secure1 (Inheritance enabled)

Account	Access Rights	Applies to	Type	IsInherited	InheritedFrom
NT-AUTORITÄT\SYSTEM	FullControl	ThisFolderSubfoldersAndFiles	Allow	True	C:
VORDEFINIERT\Administratoren	FullControl	ThisFolderSubfoldersAndFiles	Allow	True	C:
VORDEFINIERT\Benutzer	ReadAndExecute, Synchronize	ThisFolderSubfoldersAndFiles	Allow	True	C:
VORDEFINIERT\Benutzer	CreateDirectories	ThisFolderAndSubfolders	Allow	True	C:
VORDEFINIERT\Benutzer	CreateFiles	ThisFolderAndSubfolders	Allow	True	C:
ERSTELLER-BESITZER	GenericAll	SubfoldersAndFilesOnly	Allow	True	C:

In *Schritt 5* verwenden Sie das Cmdlet `Get-NTFSAccess`, um sich die ACL der Datei `C:\Secure1\Secure.txt` anzusehen, und erhalten die folgende Ausgabe:

```

PS C:\foo> Get-NTFSAccess C:\Secure1\Secure.Txt |
Format-Table -AutoSize

```

Path: C:\Secure1\Secure.Txt (Inheritance enabled)

Account	Access Rights	Applies to	Type	IsInherited	InheritedFrom
NT-AUTORITÄT\SYSTEM	FullControl	ThisFolderOnly	Allow	True	C:
VORDEFINIERT\Administratoren	FullControl	ThisFolderOnly	Allow	True	C:
VORDEFINIERT\Benutzer	ReadAndExecute, Synchronize	ThisFolderOnly	Allow	True	C:

In *Schritt 6* erstellen Sie in der Domäne `Reskit.Org` eine globale Gruppe (`Sales`), falls die Gruppe nicht bereits existiert. Gleichgültig, ob die globale Gruppe existiert oder nicht, erzeugt dieser Schritt keine Ausgabe. In *Schritt 7* lassen Sie Details zur globalen Gruppe `Sales` anzeigen, was wie folgt aussieht:

```
PS C:\foo> Get-ADGroup -Identity Sales

DistinguishedName : CN=Sales,OU=Sales,DC=Reskit,DC=Org
GroupCategory     : Security
GroupScope       : Global
Name             : Sales
ObjectClass      : group
ObjectGUID       : 21ec38da-af78-4281-bad3-6887a3203850
SamAccountName   : Sales
SID              : S-1-5-21-1666168338-3639645042-4083363113-1127
```

In *Schritt 8* erstellen Sie einen expliziten Zugriffssteuerungseintrag, der den Mitgliedern der Gruppe Domänen-Admins Vollzugriff erteilt. In *Schritt 9* entfernen Sie den ACE für VORDEFINIERT\Benutzer aus der ACL der Datei. Und in *Schritt 10* entfernen Sie die ACE-Einträge von der Datei C:\Secure1\Secure.txt, die ursprünglich vom Ordner C:\Secure1 geerbt wurden. In *Schritt 11* ergänzen Sie eine ACL, die den Mitgliedern der globalen Gruppe Reskit\Sales Vollzugriff erteilt. Diese vier Schritte erzeugen keine Ausgabe.

In *Schritt 12* verwenden Sie das Cmdlet Get-NTFSAccess, um sich die ACL für den Ordner C:\Secure1 anzeigen zu lassen und erhalten die folgende Ausgabe:

```
PS C:\foo> Get-NTFSAccess -Path C:\Secure1 |
Format-Table -AutoSize

Path: C:\Secure1 (Inheritance disabled)

Account                Access Rights Applies to                Type IsInherited InheritedFrom
-----
RESKIT\Domänen-Admins FullControl  ThisFolderSubfoldersAndFiles Allow False
RESKIT\Sales           FullControl  ThisFolderSubfoldersAndFiles Allow False
```

In *Schritt 13* geben Sie die ACL für die Datei C:\Secure1\Secure.txt aus, was wie folgt aussieht:

```
PS C:\foo> Get-NTFSAccess -Path C:\Secure1\Secure.Txt |
Format-Table -AutoSize

Path: C:\Secure1\Secure.Txt (Inheritance enabled)

Account                Access Rights Applies to                Type IsInherited InheritedFrom
-----
RESKIT\Domänen-Admins FullControl  ThisFolderOnly Allow True      C:\Secure1
RESKIT\Sales           FullControl  ThisFolderOnly Allow True      C:\Secure1
```

Weitere Informationen

In *Schritt 3* erstellen Sie einen Ordner (C:\Secure1) und eine Datei (C:\Secure1\Secure.Txt). In den weiteren Schritten passen Sie die ACLs

der Datei und des Ordners an, um die Sicherheitsrichtlinien Ihres Unternehmens umzusetzen.

In *Schritt 6* stellen Sie sicher, dass die globale Gruppe `Sales` im AD existiert, da Sie diese verwenden, um ACLs festzulegen. Wenn die globale Gruppe bereits vorhanden ist (weil Sie beispielsweise andere Rezepte in diesem Buch verwendet haben, die diese Gruppe einsetzen), dann macht dieser Schritt nichts.

In *Schritt 8* erteilen Sie der Gruppe `Reskit\Domänen-Admins` mittels eines ACEs Vollzugriff auf den Ordner. Dies bedeutet, dass Sie, da Sie als Mitglied dieser Gruppe angemeldet sind, auch nach dem Entfernen des Standard-Zugriffssteuerungseintrags für `VORDEFINIERT\Benutzer` in *Schritt 9* weiterhin Zugriff auf den Ordner und die Ordnerinhalte haben und daher die weiteren Schritte des Rezepts durchführen können.

Nachdem Sie die Zugriffssteuerungsliste des Ordners geändert haben, sehen Sie in *Schritt 12* und *Schritt 13*, dass der Ordner `C:\Secure1` nicht mehr länger die ACEs des übergeordneten Ordners erbt. Außerdem können Sie sehen, dass die Zugriffssteuerungsliste der Datei einen Zugriffssteuerungseintrag enthält, der von diesem Ordner geerbt wurde.

In einer Produktivumgebung kann es angebracht sein, die Berechtigungen für das Konto `Domänen-Admins` zu entfernen, nachdem die Anwender in der Lage sind, auf den Ordner zuzugreifen und ihn erfolgreich zu verwenden. Wenn ein Domänen-Administrator die ACL ändern muss, kann er einfach den Besitz des Ordners übernehmen, sich selbst Vollzugriff auf den Ordner gewähren und dann die erforderlichen Verwaltungsaufgaben durchführen. (Der temporäre Zugriff kann wieder entfernt werden, nachdem die administrativen Aufgaben abgeschlossen sind.)

Siehe auch ...

Dieses Rezept zeigt, wie Sie das Modul `NTFSSecurity` verwenden, um verschiedene Aspekte der Zugriffssteuerungslisten von Ordnern und Dateien zu verwalten. Dieses Modul wurde im Jahre 2014 angekündigt und seitdem kontinuierlich verbessert. Weitere Informationen über dieses Modul finden Sie unter

<https://blogs.technet.microsoft.com/fieldcoding/2014/12/05/ntfssecurity-tutorial-1-getting-adding-and-removing-permissions>.

Speicherreplikat verwalten

Speicherreplikat (SR) ist ein Feature von Windows Server 2019, das die Replikation von Volumes zwischen Systemen ermöglicht. Das Feature Speicherreplikat steht für Windows Server 2019 Datacenter Edition und Windows Server 2019 Standard Edition zur Verfügung. In der Standard Edition ist der Funktionsumfang eingeschränkt: Hier repliziert das Speicherreplikat ein einzelnes Volume (anstatt einer unbegrenzten Anzahl). Außerdem ist die Größe der replizierten Volumes auf 2 TB beschränkt.

Vorbereitungen

Dieses Rezept verwendet zusätzliche Datenträger-Volumes auf SRV1 und SRV2. Im Rezept »Physikalische Datenträger und logische Laufwerke verwalten« auf Seite 118 haben Sie SRV1 zwei zusätzliche Datenträger hinzugefügt. In diesem Rezept benötigen Sie auf SRV2 ebenfalls zwei zusätzliche Datenträger, die als Basis für die Speicherreplizierung dienen. Sie können das Skript `Add-DiskstoSrv1+2.ps1` verwenden, um die Datenträger zu erstellen, die in diesem und anderen Rezepten dieses Kapitels verwendet werden. Sie finden das Skript in den Begleitdateien zu diesem Buch und dort im Ordner mit den Skripten dieses Kapitels (siehe Einleitung).

So wird's gemacht

Führen Sie dieses Rezept auf SRV1 aus, wobei SRV2 und DC1 online sein müssen.

1. Erstellen Sie im Laufwerk F : auf dem Server SRV1 ein paar Inhalte:

```
1..100 | ForEach {
```

```
    $NF = "F:\CoolFolder$_"
```

```
    New-Item -Path $NF -ItemType Directory | Out-Null
```

```
1..100 | ForEach {
```

```
    $NF2 = "$NF\CoolFile$_"
```

```
"Cool File" | Out-File -PSPath $NF2  
  
}  
  
}
```

2. Zeigen Sie an, was sich lokal (SRV1) auf Laufwerk F : befindet:

```
Get-ChildItem -Path F:\ -Recurse | Measure-Object
```

3. Lassen Sie die Inhalte des gleichen Laufwerks auf SRV2 remote anzeigen:

```
$SB = {  
  
    Get-ChildItem -Path F:\ -Recurse |  
  
    Measure-Object  
  
}  
  
Invoke-Command -ComputerName SRV2 -ScriptBlock $SB
```

4. Installieren Sie das Feature Speicherreplikat auf SRV1:

```
Add-WindowsFeature -Name Storage-Replica
```

5. Führen Sie auf SRV1 einen Neustart durch, um die Installation abzuschließen:

Restart-Computer

6. Installieren Sie das Feature Speicherreplikat auf SRV2:

```
$SB= {  
  
    Add-WindowsFeature -Name Storage-Replica | Out-Null  
  
}
```

```
Invoke-Command -ComputerName SRV2 -ScriptBlock $SB
```

7. Führen Sie auf SRV2 einen Neustart durch und warten Sie, bis der Neustart erfolgt ist:

```
$RSHT = @{  
  
    ComputerName = 'SRV2'  
  
    Force          = $true  
  
}  
  
Restart-Computer @RSHT -Wait -For PowerShell
```

8. Richten Sie eine Speicherreplikat-Partnerschaft von Laufwerk F : auf SRV1 zu Laufwerk F : auf SRV2 ein:

```
$SRHT = @{  
  
    SourceComputerName      = 'SRV1'
```

```
SourceRGName          = 'SRV1RG'  
  
SourceVolumeName     = 'F:'  
  
SourceLogVolumeName  = 'G:'  
  
DestinationComputerName = 'SRV2'  
  
DestinationRGName    = 'SRV2RG'  
  
DestinationVolumeName = 'F:'  
  
DestinationLogVolumeName = 'G:'  
  
LogSizeInBytes       = 2gb  
  
}
```

```
New-SRPartnership @SRHT -Verbose
```

9. Zeigen Sie Informationen zur Speicherreplikat-Partnerschaft an:

```
Get-SRPartnership
```

10. Lassen Sie Informationen zu den Laufwerken auf SRV2 anzeigen:

```
$SB = {
```

```
Get-Volume |
```

```
Sort-Object -Property DriveLetter |
```

Format-Table

}

Invoke-Command -ComputerName SRV2 -ScriptBlock \$SB

11. Ändern Sie die Replikationsrichtung:

\$SRHT2 = @{

NewSourceComputerName = 'SRV2'

SourceRGName = 'SRV2RG'

DestinationComputerName = 'SRV1'

DestinationRGName = 'SRV1RG'

Confirm = \$false

}

Set-SRPartnership @SRHT2

12. Zeigen Sie Informationen zur Speicherreplikat-Partnerschaft an,
nachdem die Replikationsrichtung geändert wurde:

Get-SRPartnership

13. Untersuchen Sie die gleichen Laufwerke remote auf SRV2:

```
$SB = {
```

```
    Get-ChildItem -Path F:\ -Recurse |
```

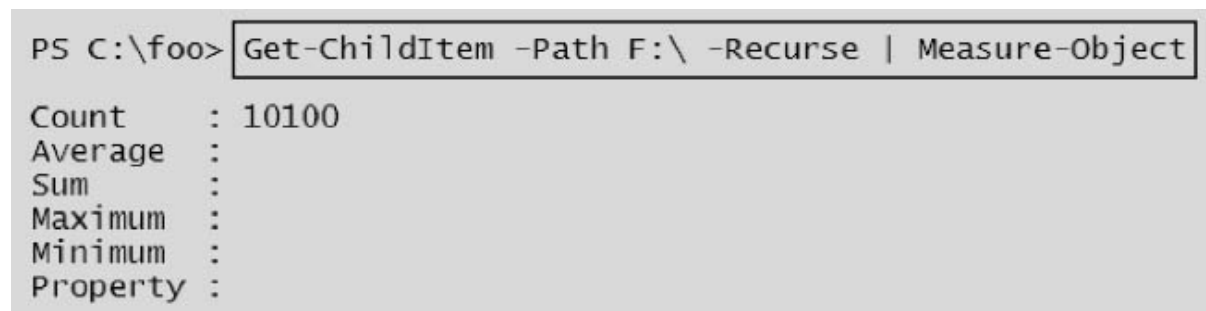
```
        Measure-Object
```

```
}
```

```
Invoke-Command -ComputerName SRV2 -ScriptBlock $SB
```

So funktioniert's

In *Schritt 1* erstellen Sie 100 Ordner im Laufwerk F: auf Server SRV1. Innerhalb jedes Ordners erstellen Sie 100 Dateien, die ein paar Inhalte enthalten. Dieser Schritt erzeugt keine Ausgabe. In *Schritt 2* lassen Sie sich anzeigen, was Sie in *Schritt 1* erstellt haben:



```
PS C:\foo> Get-ChildItem -Path F:\ -Recurse | Measure-Object
Count      : 10100
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :
```

In *Schritt 3* lassen Sie sich Laufwerk F: auf Server SRV2 anzeigen, das noch keine Dateien enthält. Die Ausgabe von *Schritt 3* sieht wie folgt aus:

```

PS C:\foo> $SB = {
    Get-ChildItem -Path F:\ -Recurse |
    Measure-Object
}
PS C:\foo> Invoke-Command -ComputerName SRV2 -ScriptBlock $SB

Count           : 0
Average         :
Sum             :
Maximum         :
Minimum         :
Property        :
PSComputerName  : SRV2

```

In *Schritt 4* installieren Sie das Feature Speicherreplikat auf SRV1, was wie folgt aussieht:

```

PS C:\foo> Add-WindowsFeature -Name Storage-Replica

Success Restart Needed Exit Code      Feature Result
-----
True      Yes           SuccessRest... {Speicherreplikat}
WARNUNG: Sie müssen den Server neu starten, um den Installationsprozess abzuschließen.

```

In *Schritt 5* führen Sie auf SRV1 einen Neustart durch. In *Schritt 6* und *Schritt 7* installieren Sie das Feature Speicherreplikat auf SRV2 und starten dann SRV2 neu. Diese drei Schritte erzeugen keine Ausgabe.

In *Schritt 8* erstellen Sie eine Speicherreplikat-Partnerschaft, die die Inhalte von F: auf SRV1 zu F: auf SRV2 repliziert (wobei das Laufwerk G: auf beiden Servern als Ordner für die Protokolldateien für die Speicherreplizierung verwendet wird). Die Ausgabe dieses Schritts sieht wie folgt aus:

```

PS C:\foo> $SRHT = @{
    SourceComputerName      = 'SRV1'
    SourceRGName            = 'SRV1RG'
    SourceVolumeName       = 'F:'
    SourceLogVolumeName    = 'G:'
    DestinationComputerName = 'SRV2'
    DestinationRGName      = 'SRV2RG'
    DestinationVolumeName  = 'F:'
    DestinationLogVolumeName = 'G:'
    LogSizeInBytes         = 2gb
}
PS C:\foo> New-SRPartnership @SRHT -Verbose

DestinationComputerName : SRV2
DestinationRGName       : SRV2RG
Id                      : 084afd15-3340-4695-9f9a-5fdc666a89c6
SourceComputerName     : SRV1
SourceRGName           : SRV1RG
PSComputerName         :

```

In *Schritt 9* verwenden Sie das Cmdlet `Get-SRPartnership`, um sich die Eigenschaften der Replikationspartnerschaft anzeigen zu lassen, was wie folgt aussieht:

```

PS C:\foo> Get-SRPartnership

DestinationComputerName : SRV2
DestinationRGName       : SRV2RG
Id                      : 084afd15-3340-4695-9f9a-5fdc666a89c6
SourceComputerName     : SRV1
SourceRGName           : SRV1RG
PSComputerName         :

```

In *Schritt 10* untersuchen Sie die logischen Laufwerke, die auf SRV2 verfügbar sind, was so aussieht:

```

PS C:\foo> $SB = {
    Get-Volume |
    Sort-Object -Property DriveLetter |
    Format-Table
}
PS C:\foo> Invoke-Command -ComputerName SRV2 -ScriptBlock $SB

```

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
		FAT32	Fixed	Healthy	OK	70.16 MB	96 MB
		NTFS	Fixed	Healthy	OK	284.93 MB	300 MB
C		NTFS	Fixed	Healthy	OK	245.17 GB	255.48 GB
D		Unknown	CD-ROM	Healthy	Unknown	0 B	0 B
E		Unknown	CD-ROM	Healthy	Unknown	0 B	0 B
F	Volume	NTFS	Fixed	Healthy	OK	9.94 GB	9.98 GB
G	Log	NTFS	Fixed	Healthy	OK	9.91 GB	9.98 GB

Bisher verwenden Sie SRV1 als Quellserver und SRV2 als Zielservers. In *Schritt 11* ändern Sie die Replikationsrichtung, was keine Ausgabe erzeugt. In *Schritt 12* können Sie sehen, dass die Replikationsrichtung geändert wurde und jetzt

Dateien von SRV2 zu SRV1 repliziert werden. Die Ausgabe dieses Schritts sieht wie folgt aus:

```
PS C:\foo> Get-SRPartnership
DestinationComputerName : SRV1
DestinationRGName       : SRV1RG
Id                      : 084afd15-3340-4695-9f9a-5fdc666a89c6
SourceComputerName     : SRV2
SourceRGName           : SRV2RG
PSComputerName         :
```

In *Schritt 13* zählen Sie die Dateien, die jetzt auf SRV2 liegen, und erhalten diese Ausgabe:

```
PS C:\foo> $SB = {
    Get-ChildItem -Path F:\ -Recurse |
    Measure-Object
}
PS C:\foo> Invoke-Command -ComputerName SRV2 -ScriptBlock $SB
Count           : 10100
Average         :
Sum             :
Maximum         :
Minimum         :
Property        :
PSComputerName  : SRV2
```

Weitere Informationen

In diesem Rezept haben Sie auf SRV1 100 Ordner und 10.000 Dateien erstellt, die Sie dann zu SRV2 replizieren. Nachdem die Replikation gestartet ist, können Sie auf SRV2 keine Daten sehen, da das Volume nun von Speicherreplikat verwendet wird. Wie Sie in *Schritt 10* sehen können, sind die replizierten Daten auf SRV2 nicht zu sehen; die Partition, in der Speicherreplikat die Replikation vornimmt, hat anscheinend kein Dateisystem. Nachdem Sie die Replikationsrichtung geändert haben, sind, wie Sie in *Schritt 11* und *Schritt 12* sehen können, nun die Dateien und Ordner auf SRV2 sichtbar und auf SRV1 hingegen nicht mehr. Hierbei handelt es sich um ein Feature von Speicherreplikat das dafür sorgt, dass nicht versehentlich Daten auf dem replizierten Datenträger gespeichert werden.

Kontingente für Dateiserver verwalten

Das Feature **Ressourcen-Manager für Dateiserver (File Server Resource Manager, FSRM)** ist ein Feature von Windows Server, das Sie bei der Verwaltung Ihrer Dateiserver unterstützt. Der Ressourcen-Manager für Dateiserver besitzt drei zentrale Features:

- **Kontingentverwaltung:** Mit dem Ressourcen-Manager für Dateiserver können Sie für Volumes und Ordner weiche und harte Kontingentgrenzen festlegen. Beim Erreichen einer weichen Kontingentgrenze wird diese nicht erzwungen, jedoch werden alle konfigurierten Benachrichtigungen generiert. Wird die harte Kontingentgrenze erreicht, wird der Benutzer daran gehindert, weitere Dateien zu speichern. Sie können für Kontingente Schwellenwerte sowie Schwellenwertaktionen konfigurieren. Wenn der Benutzer beispielsweise 65 % der Kontingentgrenze erreicht hat, kann der Ressourcen-Manager eine E-Mail senden. Bei 90 % können Sie im Ereignisprotokoll ein Ereignis protokollieren oder ein Programm starten. Für die verschiedenen Schwellenwerte stehen Ihnen verschiedene Aktionen zur Verfügung. Dieses Rezept zeigt, wie Sie Kontingente verwenden.
- **Dateiprüfung:** Sie können einen Dateifilter einrichten und einen Benutzer daran hindern, bestimmte Dateien zu speichern, die durch den Filter gelaufen sind. Sie können beispielsweise auf .MP3- oder FLAC-Dateien prüfen lassen. Wenn der Benutzer versucht, eine Datei zu speichern (beispielsweise `j g75-02-28D1T1 . flac`), weist der Filter diese Anfrage zurück und erlaubt es dem Benutzer nicht, die Datei zu speichern.
- **Speicherberichte:** Der Ressourcen-Manager für Dateiserver hilft Ihnen dabei, ganz unterschiedliche Speicherberichte zu erstellen, die für administrative Aufgaben und Verwaltungszwecke sehr nützlich sein können.

In diesem Rezept installieren Sie das Feature FSRM, nehmen ein paar allgemeine Einstellungen vor und setzen dann weiche und harte Kontingentgrenzen ein.

Vorbereitungen

Dieses Rezept verwendet einen E-Mail-Server, damit der Ressourcen-Manager für Dateiserver E-Mails an den Admin senden kann. Um die E-Mail-bezogenen

Komponenten testen zu können, brauchen Sie einen SMTP-Server oder einen E-Mail-Forwarder. Die E-Mails, die dieses Rezept generiert, wurden an SRV1 gesendet und dann an den kostenlosen E-Mail-Service <https://www.sendgrid.com> weitergeleitet. Wenn Sie ein SendGrid-Konto besitzen, können Sie auf einem Server in Ihrer Umgebung einen SMTP-Dienst einrichten und diesen so konfigurieren, dass er die Mails an SendGrid weiterleitet, von wo aus die Mails dann an den Empfänger geschickt werden.

So wird's gemacht

1. Installieren Sie das Feature Ressourcen-Manager für Dateiserver (FSRM):

```
$IHT = @{
```

```
    Name = 'FS-Resource-Manager'
```

```
    IncludeManagementTools = $True
```

```
}
```

```
Install-WindowsFeature @IHT
```

2. Konfigurieren Sie die SMTP-Einstellungen für FSRM:

```
$MHT = @{
```

```
    SmtpServer = 'SRV1.Reskit.Org' # wurde bereits  
    eingerichtet
```

```
    FromEmailAddress = 'FSRM@Reskit.Org'
```

```
    AdminEmailAddress = 'psrezepte@hits-amsterdam.nl'
```

```
}
```

```
Set-FsrmSetting @MHT
```

3. Senden Sie eine Test-E-Mail, um die Konfiguration zu testen:

```
$MHT = @{
```

```
ToEmailAddress = 'psrezepte@hits-aachen.de'
```

```
Confirm = $false
```

```
}
```

```
Send-FsrmTestEmail @MHT
```

4. Erstellen Sie eine neue Kontingentvorlage für 10 MB:

```
$QHT1 = @{
```

```
Name = '10 MB-Grenze'
```

```
Description = '10 MB Kontingent'
```

```
Size = 10MB
```

```
}
```

```
New-FsrmQuotaTemplate @QHT1
```

5. Erstellen Sie eine weitere Kontingentvorlage mit 5 MB:

```
$QHT2 = @{  
  
    Name          = '5 MB-Grenze Softlimit'  
  
    Description = 'Weiche Kontingentgrenze von 5 MB'  
  
    Size          = 5MB  
  
    SoftLimit    = $True  
  
}
```

```
New-FsrmQuotaTemplate @QHT2
```

6. Lassen Sie die vorhandenen FSRM-Kontingentvorlagen anzeigen:

```
Get-FsrmQuotaTemplate |  
  
Format-Table -Property Name, Description, Size, SoftLimit
```

7. Legen Sie zwei neue Ordner an, denen später Kontingente zugewiesen werden:

```
If (-Not (Test-Path C:\Quota)) {  
  
    New-Item -Path C:\Quota -ItemType Directory |  
  
    Out-Null  
  
}
```

```

If (-Not (Test-Path C:\QuotaS)) {

    New-Item -Path C:\QuotaS -ItemType Directory |

        Out-Null

}

```

8. Erstellen Sie eine FSRM-Aktion, die beim Überschreiten des Schwellenwerts ausgeführt werden soll:

```

$Body = @'

Benutzer [Source Io Owner] hat den Schwellenwert [Quota
Threshold]% für das Kontingent

von [Quota Path] auf Server [Server] überschritten. Die
Kontingentgrenze ist [Quota Limit

MB] MB;

derzeit werden [Quota Used MB] MB verwendet ([Quota Used
Percent]% des Grenzwerts).

'@

$NAHT = @{

    Type      = 'Email'

    MailTo    = 'psrezepte@hits-amsterdam.nl'

    Subject   = 'Kontingentgrenze erreicht [Source Io Owner]'

```

```
Body      = $Body  
  
}
```

```
$Action1 = New-FsrmAction @NAHT
```

9. Erstellen Sie eine weitere FSRM-Aktion für die Überschreitung des weichen Schwellenwerts:

```
$Thresh = New-FsrmQuotaThreshold -Percentage 85 -Action  
$Action1
```

10. Weisen Sie dem Ordner C:\Quotas die weiche Kontingentgrenze von 5 MB und einen Schwellenwert (in *Schritt 9* erstellt) zu:

```
$NQHT1 = @{  
  
    Path      = 'C:\QuotaS'  
  
    Template  = '5 MB-Grenze Softlimit'  
  
    Description = 'Weicher Grenzwert 5 MB'  
  
    Threshold = $Thresh  
  
}
```

```
New-FsrmQuota @NQHT1
```

11. Testen Sie den 85 %-Schwellenwert und die weiche Kontingentgrenze auf C:\QuotaS:

```
Get-ChildItem c:\quotas -Recurse | Remove-Item -Force
```

```
$S = '42'
```

```
1..24 | foreach {$s = $s + $s}
```

```
$S | Out-File -FilePath C:\QuotaS\Demos.txt
```

```
Get-ChildItem -Path C:\QuotaS\Demos.txt
```

12. Prüfen Sie, ob Sie in Outlook oder einem anderen E-Mail-Client eine Benachrichtigung erhalten haben.

13. Erstellen Sie eine zweite Schwellenwertaktion, die das Ereignis im Ereignisprotokoll einträgt:

```
$Action2 = New-FsrmAction -Type Event -EventType Error
```

```
$Action2.Body = $Body
```

14. Erstellen Sie zwei Schwellenwerte für ein neues Kontingent:

```
$Thresh2 = New-FsrmQuotaThreshold -Percentage 65
```

```
$Thresh3 = New-FsrmQuotaThreshold -Percentage 85
```

```
$Thresh2.Action = $Action2
```

```
$Thresh3.Action = $Action2 # gleiche Aktion wie bei $Thresh2
```

15. Erstellen Sie eine harte Kontingentgrenze mit zwei Schwellenwerten und entsprechenden Schwellenwertaktionen auf Basis einer Vorlage:

```

$NQHT = @{

    Path          = 'C:\Quota'

    Template      = '10 MB-Grenze'

    Threshold     = ($Thresh2, $Thresh3)

    Description   = 'Harte Kontingentgrenze mit 2 Aktionen'

}

```

```
New-FsrmQuota @NQHT
```

16. Entfernen Sie die existierenden Dateien, falls vorhanden:

```
Get-ChildItem C:\Quota -Recurse | Remove-Item -Force
```

17. Testen Sie die harte Kontingentgrenze C:\Quota unter einem anderen Benutzerkonto:

```
$URK = "ThomasL@reskit.org"
```

```
$PRK = ConvertTo-SecureString 'Pa$$w0rd' -AsPlainText -Force
```

```
$CredRK = New-Object system.management.automation.PSCredential
$URK,$PRK
```

```
$SB = {
```

```
    $S = '42'
```

```
1..27 | foreach {$s = $s + $s}
```

```
$S | Out-File -FilePath C:\Quota\Demos.Txt -Encoding ascii
```

```
$Len = (Get-ChildItem -Path C:\Quota\Demos.Txt).Length}
```

```
$ICMHT = @{
```

```
    ComputerName = 'SRV1'
```

```
    Credential    = $CredRK
```

```
    ScriptBlock   = $SB}
```

```
Invoke-Command -ComputerName SRV1 -Credential $CredRK -  
ScriptBlock $SB
```

18. Lassen Sie die Einträge in der Ereignisanzeige anzeigen, die durch das Überschreiten der Schwellenwerte erzeugt wurden:

```
Get-EventLog -LogName Application -Source SRMSVC |
```

```
Format-Table -AutoSize -Wrap
```

So funktioniert's

In *Schritt 1* installieren Sie das Feature Ressourcen-Manager für Dateiserver (File Server Resource Manager, FSRM) auf SRV1, was wie folgt aussieht:

```

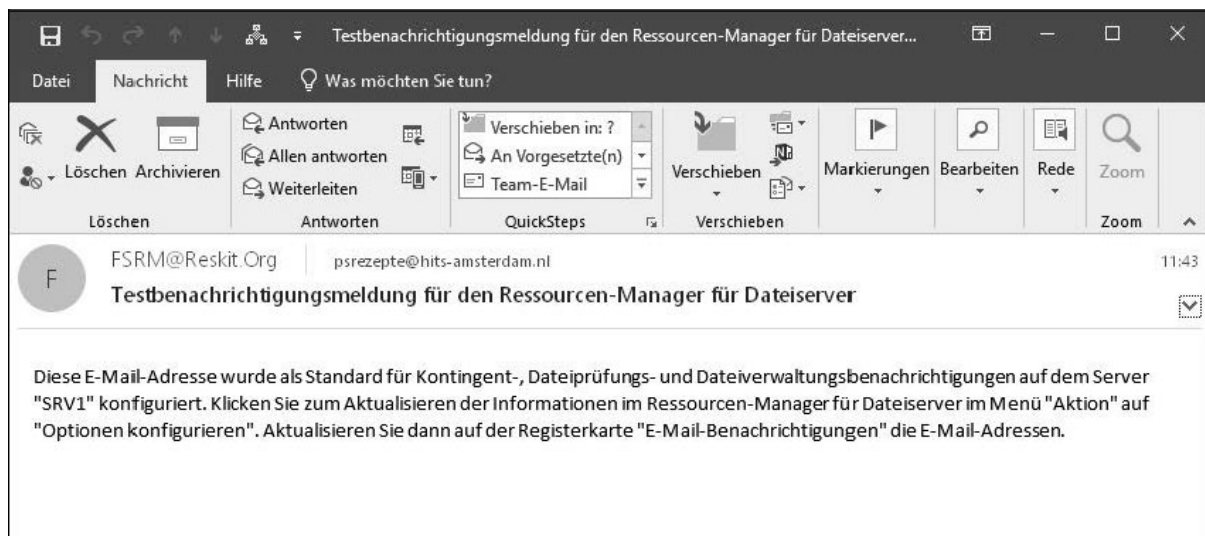
PS C:\foo> $IHT = @{
    Name = 'FS-Resource-Manager'
    IncludeManagementTools = $True
}
PS C:\foo> Install-WindowsFeature @IHT

```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Ressourcen-Manager für Dateiserver, Tools...

In *Schritt 2* konfigurieren Sie die SMTP-Server-Einstellungen für FSRM, was keine Ausgabe erzeugt. Dieser Schritt geht davon aus, dass Sie SRV1 als E-Mail-Forwarder konfiguriert haben, der die Mails an einen anderen Server weiterleitet, der schließlich die Mails an die Empfänger sendet.

In *Schritt 3* testen Sie den SMTP-Dienst, indem Sie das Cmdlet `Send-FsrmTestEmail` verwenden. Dieser Schritt erzeugt keine Ausgabe, jedoch sollte die sich so ergebende E-Mail ungefähr so aussehen:



In *Schritt 4* erstellen Sie eine FSRM-Kontingentvorlage, was wie folgt aussieht:

```

PS C:\foo> $QHT1 = @{
    Name           = '10 MB-Grenze'
    Description    = '10 MB Kontingent'
    Size           = 10MB
}
PS C:\foo> New-FsrmQuotaTemplate @QHT1

Description           : 10 MB Kontingent
Name                  : 10 MB-Grenze
Size                  : 10485760
SoftLimit             : False
Threshold             :
UpdateDerived         : False
UpdateDerivedMatching : False
PSComputerName       :

```

In *Schritt 5* erstellen Sie eine weitere FSRM-Kontingentvorlage, diesmal für 5 MB, was folgendermaßen aussieht:

```

PS C:\foo> $QHT2 = @{
    Name           = '5 MB-Grenze Softlimit'
    Description    = 'Weiche Kontingentgrenze von 5 MB'
    Size           = 5mb
    SoftLimit      = $True
}
PS C:\foo> New-FsrmQuotaTemplate @QHT2

Description           : Weiche Kontingentgrenze von 5 MB
Name                  : 5 MB-Grenze Softlimit
Size                  : 5242880
SoftLimit             : True
Threshold             :
UpdateDerived         : False
UpdateDerivedMatching : False
PSComputerName       :

```

In *Schritt 6* lassen Sie alle FSRM-Kontingentvorlagen anzeigen, die auf SRV1 verfügbar sind. Zu diesen Vorlagen gehören die Standardvorlagen, die zusammen mit dem Feature Ressourcen-Manager für Dateiserver installiert wurden, sowie die eigenen Vorlagen, die Sie in *Schritt 4* und *Schritt 5* erstellt haben. Die Liste der verfügbaren Vorlagen sieht folgendermaßen aus:

```
PS C:\foo> Get-FsrmQuotaTemplate |
Format-Table -Property Name, Description, Size, SoftLimit
```

Name	Description	Size	SoftLimit
100 MB-Grenze		104857600	False
200 MB-Grenze mit Bericht an Benutzer		209715200	False
200 GB-Volumenbelegung überwachen		214748364800	True
500 MB-Freigabe überwachen		524288000	True
200 MB-Grenze mit 50 MB Erweiterung		209715200	False
250 MB erweiterte Grenze		262144000	False
2-GB-Limit		2147483648	False
5-GB-Limit		5368709120	False
10-GB-Limit		10737418240	False
3-TB-Volumenbelegung überwachen		3298534883328	True
5-TB-Volumenbelegung überwachen		5497558138880	True
10-TB-Volumenbelegung überwachen		10995116277760	True
10 MB-Grenze	10 MB Kontingent	10485760	False
5 MB-Grenze Softlimit	Weiche Kontingentgrenze von 5 MB	5242880	True

In *Schritt 7* erstellen Sie auf SRV1 zwei neue Ordner, um die weichen und harten Kontingentgrenzen zu testen. In *Schritt 8* und *Schritt 9* erstellen Sie zwei neue Aktionen, die beim Überschreiten der Kontingente ausgeführt werden sollen. Diese drei Schritte erzeugen keine Ausgabe.

In *Schritt 10* weisen Sie C:\QuotaS eine neue weiche Kontingentgrenze zu, was wie folgt aussieht:

```
PS C:\foo> $NQHT1 = @{
    Path      = 'C:\QuotaS'
    Template  = '5 MB-Grenze Softlimit'
    Description = 'Weicher Grenzwert 5 MB'
    Threshold = $Thresh
}
PS C:\foo> New-FsrmQuota @NQHT1
```

```
Description      : Weicher Grenzwert 5 MB
Disabled          : False
MatchesTemplate   : False
Path              : C:\QuotaS
PeakUsage        : 1024
Size              : 5242880
SoftLimit        : True
Template          : 5 MB-Grenze Softlimit
Threshold         : {MSFT_FSRMQuotaThreshold}
Usage            : 1024
PSComputerName   :
```

In *Schritt 11* testen Sie die weiche Kontingentgrenze, indem Sie eine lange Zeichenfolge erstellen und diese Zeichenfolge in eine Datei schreiben, die das weiche Kontingent überschreitet. Die Ausgabe dieses Schritts sieht folgendermaßen aus:

```

PS C:\foo> Get-ChildItem c:\quotas -Recurse | Remove-Item -Force
PS C:\foo> $$ = '42'
PS C:\foo> 1..24 | foreach {$s = $s + $s}
PS C:\foo> $$ | Out-File -FilePath C:\QuotaS\Demos.txt
PS C:\foo> Get-ChildItem -Path C:\QuotaS\Demos.txt

```

Verzeichnis: C:\QuotaS

Mode	LastwriteTime	Length	Name
-a----	17.07.2019 12:20	67108870	Demos.txt

Wenn die weiche Kontingentgrenze überschritten wird, wird eine E-Mail-Nachricht generiert, die wie folgt aussieht:



In *Schritt 13* erzeugen Sie eine zweite Schwellenwertaktion, die das Ereignis im Ereignisprotokoll einträgt. In *Schritt 14* erstellen Sie zwei neue Kontingentschwellenwerte (65 % des Kontingents überschritten, 85 % des Kontingents überschritten). Diese beiden Schritte erzeugen keine Ausgabe.

In *Schritt 15* erstellen Sie eine harte Kontingentgrenze für C:\Quota, mit der zwei Schwellenwertaktionen verknüpft sind, die Sie in den beiden vorigen Schritten erstellt haben. Diese Ausgabe dieses Schritts sieht folgendermaßen aus:

```

PS C:\foo> $NQHT = @{
    Path          = 'C:\Quota'
    Template      = '10 MB-Grenze'
    Threshold     = ($Thresh2, $Thresh3)
    Description   = 'Harte Kontingentgrenze mit 2 Aktionen'
}
PS C:\foo> New-FsrmQuota @NQHT

Description      : Harte Kontingentgrenze mit 2 Aktionen
Disabled         : False
MatchesTemplate  : False
Path             : C:\Quota
PeakUsage        : 1024
Size             : 10485760
SoftLimit        : False
Template         : 10 MB-Grenze
Threshold        : {MSFT_FSRMQuotaThreshold, MSFT_FSRMQuotaThreshold}
Usage            : 1024
PSComputerName   :

```

In *Schritt 16* löschen Sie alle eventuell in C:\Quota vorhandenen Dateien, was keine Ausgabe erzeugt. In *Schritt 17* testen Sie die harte Kontingentgrenze, was wie folgt aussieht:

```

PS C:\foo> $URK = "ThomasL@reskit.org"
PS C:\foo> $PRK = ConvertTo-SecureString 'Pa$w0rd' -AsPlainText -Force
PS C:\foo> $CredRK = New-Object system.management.automation.PSCredential $URK,$PRK
PS C:\foo> $SB = {
    $S = '42'
    1..27 | foreach {$S = $S + $S}
    $S | Out-File -FilePath C:\Quota\Demos.Txt -Encoding ascii
    $Len = (Get-ChildItem -Path C:\Quota\Demos.Txt).Length
}
PS C:\foo> $ICMHT = @{
    ComputerName = 'SRV1'
    Credential   = $CredRK
    ScriptBlock  = $SB
}
PS C:\foo> Invoke-Command -ComputerName SRV1 -Credential $CredRK -ScriptBlock $SB

Es steht nicht genug Speicherplatz auf dem Datenträger zur Verfügung.
+ CategoryInfo          : NotSpecified: (:) [out-lineInfo], IOException
+ FullyQualifiedErrorId : System.IO.IOException,Microsoft.PowerShell.Commands.OutLineOutputCommand
+ PSComputerName        : SRV1

```

In *Schritt 18* schauen Sie sich die Einträge im Ereignisprotokoll Anwendung an, die FSRM erstellt hat, als die beiden Kontingentschwellenwerte überschritten wurden (also als das Kontingent zu 65 % und zu 85 % ausgeschöpft war). Die Ausgabe sieht folgendermaßen aus:

```

PS C:\foo> Get-EventLog -LogName Application -Source SRMSVC |
            Format-Table -AutoSize -Wrap

```

Index	Time	EntryType	Source	InstanceID	Message
406	Jul 17 12:30	Error	SRMSVC	2147758117	Benutzer RESKIT\ThomasL hat den Schwellenwert 85% für das Kontingent von C:\Quota auf Server SRV1 überschritten. Die Kontingentgrenze ist 10,00 MB; derzeit werden 8,50 MB verwendet (85% des Grenzwerts).
405	Jul 17 12:30	Error	SRMSVC	2147758117	Benutzer RESKIT\ThomasL hat den Schwellenwert 65% für das Kontingent von C:\Quota auf Server SRV1 überschritten. Die Kontingentgrenze ist 10,00 MB; derzeit werden 6,50 MB verwendet (65% des Grenzwerts).

Weitere Informationen

In diesem Rezept haben Sie sowohl eine weiche als auch eine harte FSRM-Kontingentgrenze eingerichtet und getestet. Die weiche Kontingentgrenze haben Sie so konfiguriert, dass eine E-Mail gesendet wird, die den Empfänger darüber informiert, dass der Speicherplatz ausgeschöpft ist. Für die harte Kontingentgrenze haben Sie zwei Einträge im Ereignisprotokoll erstellt: einen, wenn das Kontingent zu 65 % ausgeschöpft ist, und den zweiten bei 85 %. Bei einer weichen Kontingentgrenze kann der Benutzer den festgelegten Wert überschreiten; bei einer harten Kontingentgrenze kann der Benutzer nur so lange speichern, bis der maximale Wert erreicht ist. Wie Sie in *Schritt 17* sehen können, war die Größe der Datei, die in C:\Quota gespeichert werden kann, auf nur 10 MB begrenzt.

Die Kontingente, die dieses Rezept verwendet, sind extrem klein und in einer Produktivumgebung vermutlich nicht geeignet. Jedoch lässt sich eine Änderung, beispielsweise von 10 MB in 10 GB, einfach vornehmen. Wenn die weiche Kontingentgrenze überschritten wird, führt dies dazu, dass als Aktion eine E-Mail gesendet wird, während für die harte Kontingentgrenze lediglich Einträge im Ereignisprotokoll erstellt werden. In einer Produktivumgebung würden Sie die E-Mail sowohl an einen Administrator als auch an den Benutzer senden, der den Schwellenwert oder das Kontingent überschritten hat.

In *Schritt 14* haben Sie zwei Kontingentschwellenwerte erstellt (einen, der bei 65 % ausgelöst wird, und den zweiten bei 85 %). Für beide Schwellenwerte haben Sie den gleichen Text festgelegt, der protokolliert wird, falls einer der beiden Schwellenwerte erreicht wird. Sie können die beiden Meldungen in *Schritt 18* sehen.

Speicherberichte verwenden

Ein weiteres Feature der FSRM-Komponente ist die Berichterstellung. FSRM definiert eine Reihe von einfachen Berichtstypen, die Sie anfordern können. Diese Berichte können entweder sofort (also interaktiv) erstellt werden, oder zu einem vorher festgelegten Zeitpunkt. Im letzteren Fall führt das dazu, das FSRM wöchentlich oder monatlich Berichte erstellt.

Vorbereitungen

Führen Sie dieses Rezept auf SRV1 aus, nachdem Sie das Feature Ressourcen-Manager für Dateiserver installiert haben. Dies haben Sie bereits im Rezept »Kontingente für Dateiserver verwalten« auf Seite 133 erledigt. Dieses Rezept hat außerdem zwei große Dateien erstellt. Falls Sie das Rezept nicht verwendet haben, sollten Sie auf SRV1 ein paar große Dateien erstellen, bevor Sie dieses Rezept ausführen.

So wird's gemacht

1. Erstellen Sie einen neuen Speicherbericht für große Dateien auf C:\ auf SRV1:

```
$NRHT = @{  
  
    Name                = 'Große Dateien auf SRV1'  
  
    NameSpace           = 'C:\'  
  
    ReportType          = 'LargeFiles'  
  
    LargeFileMinimum    = 10MB  
  
    Interactive          = $true  
  
}
```

```
New-FsrmStorageReport @NRHT
```

2. Rufen Sie die aktuell verfügbaren Berichtstypen ab:

```
Get-FsrmStorageReport *
```

3. Nachdem der Speicherbericht ausgeführt wurde, sehen Sie sich die erzeugten Berichte im Dateisystem an:

```
$Path = 'C:\StorageReports\Interactive'
```

```
Get-ChildItem -Path $Path
```

4. Sehen Sie sich den HTML-Bericht an:

```
$Rep = Get-ChildItem -Path $Path\*.html
```

```
Invoke-item -Path $Rep
```

5. Rufen Sie die Schlüsselinformationen aus dem XML ab:

```
$XF = Get-ChildItem -Path $Path\*.xml
```

```
$XML = [XML] (Get-Content -Path $XF)
```

```
$Files = $XML.StorageReport.ReportData.Item
```

```
$Files | Where-Object Path -NotMatch  
'^Windows|^Program|^Users' |
```

```
Format-Table -Property name, path,
```

```
@{ name = 'Sizemb'
```

```
expression = {((([int]$_size)/1mb).tostring('N2'))},
```

```
DaysSinceLastAccessed -AutoSize
```

6. Erstellen Sie eine monatliche FSRM-Aufgabe in der Aufgabenplanung:

```
$Date = Get-Date '04:00'
```

```
$NTHT = @{
```

```
Time = $Date
```

```
Monthly = 1
```

```
}
```

```
$Task = New-FsrmScheduledTask @NTHT
```

```
$NRHT = @{
```

```
Name = 'Monatsbericht Dateien nach Dateityp'
```

```
Namespace = 'C:\'
```

```
Schedule = $Task
```

```
ReportType = 'FilesbyFileGroup'
```

```
FileGroupInclude = 'Textdateien'
```

```
LargeFileMinimum = 25MB  
  
}  
  
New-FsrmStorageReport @NRHT | Out-Null
```

7. Rufen Sie Details der geplanten Aufgabe ab:

```
Get-ScheduledTask |  
  
Where-Object taskname -Match 'Monatsbericht' |  
  
Format-Table -AutoSize
```

8. Starten Sie die Aufgabe jetzt:

```
Get-ScheduledTask -TaskName '*Monatsbericht*' |  
  
Start-ScheduledTask  
  
Get-ScheduledTask -TaskName '*Monatsbericht*'
```

9. Sehen Sie sich den von der Aufgabe erstellten Bericht an:

```
$Path = 'C:\StorageReports\Interactive'  
  
$Rep = Get-ChildItem -Path $path\*.html  
  
Invoke-item -Path $Rep
```

So funktioniert's

In *Schritt 1* verwenden Sie das Cmdlet `New-FsrmStorageReport` um einen neuen Bericht zu erstellen, der alle Dateien auf `C:\` ausgibt, die größer als 10 MB sind. Sie erhalten die folgende Ausgabe:

```
PS C:\foo> $NRHT = @{
    Name           = 'Große Dateien auf SRV1'
    Namespace      = 'C:\'
    ReportType     = 'LargeFiles'
    LargeFileMinimum = 10MB
    Interactive     = $true
}
PS C:\foo> New-FsrmStorageReport @NRHT

FileGroupIncluded      :
FileOwnerFilePattern   :
FileOwnerUser          :
FileScreenAuditDaysSince : 0
FileScreenAuditUser    :
FolderPropertyName     :
Interactive             : True
LargeFileMinimum       : 10485760
LargeFilePattern       :
LastError              :
LastReportPath         :
LastRun                :
LeastAccessedFilePattern :
LeastAccessedMinimum   : 0
MailTo                 :
MostAccessedFilePattern :
MostAccessedMaximum    : 0
Name                   : Große Dateien auf SRV1
Namespace              : {C:\}
PropertyFilePattern    :
PropertyName           :
QuotaMinimumUsage      : 0
ReportFormat           : {Dhtml, XML}
ReportType             : LargeFiles
Schedule               :
Status                 : Queued
PSComputerName         :
```

In *Schritt 2* sehen Sie sich die vorhandenen FSRM-Berichte an, was wie folgt aussieht:

```

PS C:\foo> Get-FsrmStorageReport *
FileGroupIncluded      :
FileOwnerFilePattern  :
FileOwnerUser         :
FileScreenAuditDaysSince : 0
FileScreenAuditUser   :
FolderPropertyName    :
Interactive            : True
LargeFileMinimum      : 10485760
LargeFilePattern      :
LastError             :
LastReportPath        :
LastRun               :
LeastAccessedFilePattern :
LeastAccessedMinimum  : 0
MailTo                :
MostAccessedFilePattern :
MostAccessedMaximum   : 0
Name                  : Große Dateien auf SRV1
Namespace             : {C:\}
PropertyFilePattern   :
PropertyName          :
QuotaMinimumUsage     : 0
ReportFormat          : {Dhtml, XML}
ReportType            : LargeFiles
Schedule              :
Status                : Running
PSComputerName        :

```

Nachdem der Speicherbericht zu großen Dateien gelaufen ist, schauen Sie sich in *Schritt 3* die Ergebnisse im Dateisystem an, was wie folgt aussieht:

```

PS C:\foo> $Path = 'C:\StorageReports\Interactive'
PS C:\foo> Get-ChildItem -Path $Path

```

Verzeichnis: C:\StorageReports\Interactive

Mode	LastWriteTime		Length	Name
d-----	17.07.2019	12:39		GroßeDateien2_2019-07-17_12-39-02_files
-a----	17.07.2019	12:39	191540	GroßeDateien2_2019-07-17_12-39-02.html
-a----	17.07.2019	12:39	422144	GroßeDateien2_2019-07-17_12-39-02.xml

In *Schritt 4* öffnen Sie den HTML-Bericht, der so aussieht:

Browser window showing a report titled "Bericht für große Dateien".

URL: C:\StorageReports\Interactive\GroßeDateien2_2019-07-17_12-39-02.html

Report Title: Bericht für große Dateien
Generiert um: 17.07.2019 12:39:02

Berichtsbeschreibung: Führt Dateien auf, die einer angegebenen Mindestgröße entsprechen. Diesen Bericht können Sie verwenden, um schnell diejenigen Dateien zu bestimmen, die den meisten Speicherplatz auf dem Server belegen und dadurch schnell große Mengen an Speicherplatz wieder verwenden.

Computer: SRV1
Berichtsordner: 'C:\'
Parameter: Mindestdateigröße: 10,00 MB

Bericht für große Dateien Inhaltsverzeichnis

- Bericht insgesamt
- Größe nach Besitzer
- Größe nach Dateigruppe
- Berichtsstatistik

Bericht insgesamt			
Im Bericht angezeigte Dateien		Alle den Berichtskriterien entsprechenden Dateien	
Dateien	Gesamtgröße auf Datenträger	Dateien	Gesamtgröße auf Datenträger
200	18.631 MB	200	18.631 MB

Zum Anfang des aktuellen Berichts

Größe nach Besitzer

- VORDEFINIERT\Administratoren; 14.999 MB; (80,50 %)
- NT SERVICE\TrustedInstaller; 2.480 MB; (13,31 %)
- NT-AUTORITÄT\SYSTEM; 1.096 MB; (5,88 %)
- Andere; 56,5 MB; (0,30 %)

Größe nach Besitzer		
Besitzer	Gesamtgröße auf Datenträger	Dateien
VORDEFINIERT\Administratoren	14.999 MB	19
NT SERVICE\TrustedInstaller	2.480 MB	122
NT-AUTORITÄT\SYSTEM	1.096 MB	56
NT-AUTORITÄT\Lokaler Dienst	31,0 MB	2
SRV1\rainerghaseller	25,5 MB	1

In *Schritt 5* extrahieren Sie Informationen aus der XML-Version des interaktiven FSRM-Berichts zu großen Dateien und erhalten diese Ausgabe:

```
PS C:\foo> $XF = Get-ChildItem -Path $Path\*.xml
PS C:\foo> $XML = [XML] (Get-Content -Path $XF)
PS C:\foo> $Files = $XML.StorageReport.ReportData.Item
PS C:\foo> $Files | Where-Object Path -NotMatch '^Windows|^Program|^Users'|
    Format-Table -Property name, path,
    @{ name = 'Sizemb'
      expression = {((([int]$_.size)/1mb).tostring('N2'))},
      DaysSinceLastAccessed -AutoSize
```

Name	Path	Sizemb	DaysSinceLastAccessed
1{3808876b-c176-4e48-b7ae-04046e6cc752}	System Volume Information		0
pagefile.sys		1.751,55	0
Demos.txt	Quota\$	64,00	0
Demos.Txt	Quota	10,00	0

In *Schritt 6* erstellen Sie eine Aufgabe für einen geplanten Bericht, was keine Ausgabe erzeugt. In *Schritt 7* schauen Sie sich die Details der geplanten Aufgabe an:

```
PS C:\foo> Get-ScheduledTask |
  Where-Object taskname -Match 'Monatsbericht' |
  Format-Table -AutoSize
```

TaskPath	TaskName	State
\Microsoft\Windows\File Server Resource Manager\	StorageReport-Monatsbericht Dateien nach Dateityp	Ready

In *Schritt 8* starten Sie die in *Schritt 7* definierte Aufgabe und sehen, dass der Bericht ausgeführt wird, was wie folgt aussieht:

```
PS C:\foo> Get-ScheduledTask -TaskName '*Monatsbericht*' |
  Start-ScheduledTask
PS C:\foo> Get-ScheduledTask -TaskName '*Monatsbericht*'

TaskPath
```

TaskPath	TaskName	State
\Microsoft\Windows\File Server Resource Man...	StorageReport-Monatsbericht Da...	Running

In *Schritt 9* sehen Sie sich den Bericht nach Dateitypen an, der wie folgt aussieht:

The screenshot shows a web browser window displaying an interactive storage report. At the top, there is a table showing storage usage for different file types:

SRV1\rainerghaseller	2,12 MB	24
NT-AUTORITÄT\Netzwerkdienst	0,10 MB	1
NT-AUTORITÄT\SYSTEM	0,00 MB	1

Below this table, there is a section titled 'Größe nach Dateigruppe' (Size by file group). It features a pie chart and a legend indicating that 'Textdateien' (Text files) account for 91,8 MB (100,00 %). An arrow points from the legend to the pie chart.

Below the pie chart, there is a table summarizing the data:

Dateigruppe	Gesamtgröße auf Datenträger	Dateien
Textdateien	91,8 MB	176

At the bottom, there is a detailed table titled 'Statistik für Dateien in Dateigruppe: 'Textdateien'' (Statistics for files in file group: 'Text files'). This table lists individual files, their locations, sizes, and owners.

Dateiname	Ordner		
	Größe auf Datenträger	Größe	Besitzer
Demos.bt	C:\QuotaS	64,0 MB	VORDEFINIERT\Administratoren
Demos.Txt	C:\Quota	10,0 MB	VORDEFINIERT\Administratoren
TableTextServiceArray.bt	C:\Program Files (x86)\windows nt\tabletextservice	1,22 MB	NT SERVICE\TrustedInstaller
TableTextServiceArray.bt	C:\Program Files\windows nt\tabletextservice	1,22 MB	NT SERVICE\TrustedInstaller
TableTextServiceArray.bt	C:\Windows\WinSxS\amd64_microsoft-windows-t..._31bf3856ad364e35_10.0.17763.1_none_559fb825ba17cec8	1,22 MB	NT SERVICE\TrustedInstaller
TableTextServiceArray.bt	C:\Windows\WinSxS\wow64_microsoft-windows-t..._31bf3856ad364e35_10.0.17763.1_none_5ff46277ee7890c3	1,22 MB	NT SERVICE\TrustedInstaller
TableTextServiceDaVi.bt	C:\Program Files (x86)\windows nt\tabletextservice	0,94 MB	NT SERVICE\TrustedInstaller
	C:\Program Files\windows nt\tabletextservice		

Weitere Informationen

In *Schritt 2* lassen Sie die vorhandenen FSRM-Berichte anzeigen und verwenden hierfür das Cmdlet `Get-FsrmStorageReport`. Sie sehen dann alle aktiven FSRM-Berichte (geplant und interaktiv), obwohl FSRM, nachdem ein interaktiver Bericht erstellt wurde, diesen mit `Get-FsrmStorageReport` nicht mehr anzeigt.

In *Schritt 3* sehen Sie sich die Ausgabe an, die FSRM für den interaktiven Speicherbericht generiert hat. Wie Sie sehen können, wird der Bericht sowohl im HTML- als auch im XML-Format erzeugt. Die HTML-Ausgabe sieht gut aus (wie Sie in *Schritt 4* sehen können), jedoch kann das Format nicht angepasst werden. Sie erhalten jedoch im XML alle Informationen, die auch im HTML-Bericht enthalten sind. Sie können das XML verwenden, um die Ergebnisse wie gewünscht zu formatieren. Die XML-Dateistruktur ist recht einfach und Sie können die

grundlegenden Informationen aus dem XML extrahieren, um die Details zu sehen, an denen Sie interessiert sind (siehe *Schritt 5*).

In *Schritt 9* sehen Sie sich den zweiten Bericht an, einen Bericht, der nach den Dateitypen organisiert ist. In diesem Beispiel werden lediglich Textdateien angezeigt. Gäbe es andere Dateien, die zu anderen Dateitypen gehörten, dann wären diese ebenfalls im Bericht enthalten. Bitte beachten Sie, dass sich die Berichte, die von geplanten Aufgaben erstellt werden, im Ordner `C:\StorageReports\Scheduled` befinden. Da die Erstellung des zweiten Berichtes jedoch in *Schritt 8* manuell gestartet wurde, finden Sie ihn im Ordner `C:\StorageReports\Interactive`.

Index

3DES 258

A

Abgelaufene Computerkonten finden 113

Access Control Lists (ACLs) 118

Active Directory

 Autorisierung von DHCP-Server 76

 Azure 386

 Benutzerkonten aus CSV-Datei erstellen 103

 Benutzerkonten entfernen 99

 Benutzerkonten erstellen 99

 Berichte zu Benutzern erstellen 109

 Computerkonten erstellen 100

 DNS 84

 Domänendienste installieren 92

 Drucker veröffentlichen 215

 Gruppe erstellen 100

 Gruppenrichtlinienobjekte erstellen 105

 Gruppenrichtlinienobjekte mit OU verknüpfen 106

 inaktive Benutzerkonten 113

 inaktive Computerkonten 113

 mit DNS installieren 92

 Organisationseinheit erstellen 98

 Ports 95

 Vertrauensstellung für Delegierungszwecke 371

Anfügeblobs 395

Anschlüsse für Druckerpools 227

Anwendungspools 272

- Neustart 273
- Anzahl virtueller Prozessoren in VM 352
- APIPA 359
- App Service-Plan 406
- Arbeitsprozesse 272
- Arbeitsspeichergröße einer VM 352
- Aufzählungsmodus 154
- Ausführungsrichtlinie 30
- Automatic Private IP Address 359
- Autorisierung von DHCP-Server 76
- Azure
 - App Service-Plan erstellen 406
 - Blobcontainer erstellen 398
 - Blobs 395
 - Cmdlets für Azure Active Directory 386
 - Files 396
 - Kosten 385
 - PowerShell-Modul installieren 386
 - Regionen 387
 - Ressourcengruppe 390
 - SMB-Freigabe erstellen 402
 - SMB-Port 445 403
 - Speicherkonto 391, 395
 - Table Storage 395
 - Testabonnement 385
 - Umgebungen 387
 - und Powershell 385
 - VM erstellen 411
 - Warteschlange 395
 - Web-App erstellen 406

B

- Background Intelligent Transfer Service (BITS) 35
- Basis-Betriebssystemimages 230

Benutzer *siehe* Benutzerkonten

Benutzerkonten

- anzeigen 99

- aus CSV-Datei in AD importieren 103

- erstellen 98

- inaktive 113

- löschen 99

- verschieben 100

Benutzerkonten im AD erstellen 99

Berichte

- Druckernutzung 437

- Hyper-V-Nutzung und Performance 439

- Systemdiagnosebericht 436

Best Practices Analyzer

- Modul Webserver ausführen 448

- Module anzeigen 448

- remote verwenden 450

Bindungen 266

BIOS, Virtualisierungsfunktionen 341

BITS (Background Intelligent Transfer Service) 35

Blobs 395

Blockblobs 395

C

Central Certificate Store (CCS) 261

Certificate Authority (CA) 255

Challenge Handshake Authentication Protocol (CHAP) 165

Chocolatey *siehe* DSC-Ressourcen

Cipher Suites verwalten 258

Cluster 149

- IIS-Webserver 280

Cluster Shared Volume 162

cmdkey.exe 405

Codesignierung 51

Computer anpingen 67

Computerkonten

- abgelaufene finden 113

- erstellen 100

- inaktive 113

Computer-Zielgruppen

- Regel für automatische Genehmigung 203

- Windows Update 200

Container

- Hello World-Beispielanwendung bereitstellen 234

- Host konfigurieren 231

- IIS bereitstellen 240

- mit Hyper-V-Isolierung ausführen 240

- neues Image erstellen 243

- Portweiterleitung 241, 243

CSV-Datei

- Benutzerkonten importieren 103

- Leistungsdaten 430

D

Dateifilter 133

Dateiprüfung 133

Datenträger

- anzeigen 120

- GUID-Partitionstabelle 118

- initialisieren 120

- Laufwerke anzeigen 120

- Master Boot Record (MBR) 118

- Partitionen anzeigen 120

Datenträgerverwaltung, MMC-Snap-In 119

Desired State Configuration (DSC)

- DSC-Ressourcen suchen und installieren 299

- Ereignisprotokollierung 319

- HTTP-Pullserver implementieren 319

- integrierte Ressourcen verwenden 289
- Konfiguration mit Parametern versehen 296
- lokalen Konfigurations-Manager konfigurieren 309
- Metakonfiguration 309
- Pullmodell 309
- Pushmodell 309
- Ressourcen aus der PowerShell-Gallery nutzen 304
- SMB-Pullserver implementieren 312
- Teilkonfiguration verwenden 327
- Überblick 287
- DFS (Distributed File System) 150
- DFS-Namespaces
 - Feature installieren 170
 - neuen Stamm erstellen 171
 - Ordnerziele hinzufügen 172
 - RSAT-Tools installieren 170
- DFS-Replikation
 - Cmdlets anzeigen 176
 - Feature installieren 175
 - Mitgliedschaftseinstellungen festlegen 177
 - Replikationsgruppe 174
 - Replikationsgruppen anzeigen 176
 - Topologie 175
- DHCP
 - aktivieren 79
 - Bereiche konfigurieren 77
 - Failover konfigurieren 81
 - Lastenausgleich konfigurieren 81
 - Server installieren und autorisieren 75
- Differenzierende Festplatte 376
- Digicert, Link 52
- Distributed File System (DFS) 150
- DNS
 - Abfrage durchführen 68

- Auflösungscache anzeigen 67
- Auflösungscache leeren 68
- Autoregistrierung 84
- mit Active Directory installieren 92
- primäre Forward-Lookup-Zone 85
- primäre Reverse-Lookup-Domäne 85
- Ressourceneinträge erstellen 85
- Ressourceneinträge konfigurieren 84
- Server konfigurieren 84
- Serveradresse festlegen 74
- Server-Dienst installieren 84
- SPF-Ressourceneinträge 90
- Zonen konfigurieren 84

Docker

- Infos zur Version anzeigen 232
- Konfigurationsinformationen anzeigen 232
- Provider installieren 231
- Status des Dienstes anzeigen 232

Docker *siehe auch* Container

Docker Swarm 230

Dockerfile 230, 243

- erstellen 245

Domänendienste installieren 92

Drucker

- Berechtigungen verwalten 222
- Druckerpool einrichten 227
- Druckserver installieren 212
- freigeben 213
- IP-Anschluss hinzufügen 213
- Testseite drucken 221
- Treiber ändern 220
- veröffentlichen 215
- Veröffentlichungsstatus 215

Druckernutzung 437

Druckertreiber

ändern 220

installieren 213

Druckserver

installieren 212

Spoolerverzeichnis ändern 217

DSC *siehe* Desired State Configuration

DSC-Ressourcen 299

aus der PowerShell-Gallery nutzen 304

Begriff 287

integrierte verwenden 289

E

Enterprise Certificate Authority (CA) 335

Ereignisprotokolle 452

Anwendungs- und Dienstprotokolle 452

Desired State Configuration (DSC) 319

Ereignisquellen 453

löschen 453

Namen der Protokolle abrufen 453

Windows Update-Client 453

Windows-Protokolle 452

Ereignisprotokolleinträge, Link 64

exFAT 117

F

Failover für DHCP konfigurieren 81

Failover-Test 373

FAT32 117

Fibre Channel SAN 162

File Server Resource Manager *siehe* Ressourcen-Manager für Dateiserver

File, DSC-Ressource 300

Format der Protokolldateien in IIS 269

FSRM *siehe* Ressourcen-Manager für Dateiserver

G

Get-Counter 419

GPT, GUID-Partitionstabelle 118

Große Dateien, Speicherbericht 141

Gruppenrichtlinienobjekte

- Bericht erstellen 107

- erstellen 105

- mit OU verknüpfen 106

GUID-Partitionstabelle 118

H

Hello World-Beispielanwendung bereitstellen 234

HTTP-Pullserver für DSC einrichten 319

Hyper-V

- Container mit Isolierung ausführen 240

- Datenträger verschieben 366

- differenzierende Festplatte 376

- erweiterter Sitzungsmodus 339

- Feature installieren 338

- Netzwerke konfigurieren 355

- NUMA 339

- NUMA, Link 341

- Nutzung 439

- Performance 439

- PowerShell Direct 345

- Prüfpunkte 376

- Ressourcenmessung 341

- Standardpfad für virtuelle Datenträger 339

- Standardpfad für virtuellen Computer 339

- verschachtelte Virtualisierung 360

- virtuellen Switch erstellen 356

- VM erstellen 342

- VM verschieben 366

- VM-Gruppen 347

VM-Hardware konfigurieren 351

VM-Replikation 371

VM-Status verwalten 363

I

IIS

Anwendungspools 272

Arbeitsprozesse 272

Bindungen konfigurieren 266

Central Certificate Store 261

Cipher Suites verwalten 258

Format der Protokolldateien 269

Hostname 266

IISAdministration, Modul 250

installieren 250

Netzwerklastenausgleich 280

Protokolldateien 276

Protokollierung 268

Server Name Indication, SNI 267

Speicherort der Protokolldateien 269

SSL konfigurieren 255

Verschlüsselungssuites verwalten 258

Verwaltungstools 254

WebAdministration, Modul 250

zentraler Zertifikatsspeicher 260

Inaktive Benutzerkonten finden 113

Internet Information Services *siehe* IIS

Internetinformationsdienste

 BPA-Modul Webserver 449

 in Container bereitstellen 240

Internetinformationsdienste *siehe* IIS

IP-Adresse statisch festlegen 74

IP-Adressen

 dynamische statt statische verwenden 79

- konfigurieren 73
- IP-Adress-Konfiguration abrufen 67
- IP-basierter Druckeranschluss 213
- IPC\$ 158
- Ipconfig 68
- iSCSI
 - Feature Zielsever installieren 163
 - Target einrichten 163
 - virtuellen Datenträger erstellen 163
 - Ziel erstellen 162
 - Ziel verwenden 165

J

- JEA-Dokumentation, Link 64
- Just Enough Administration
 - implementieren 57
 - Objekte 57

K

- Kontingentverwaltung 133
- Kontingentvorlagen erstellen 134

L

- Lastenausgleich für DHCP konfigurieren 81
- Laufwerke
 - anzeigen 120
 - formatieren 120
- LCM (Local Configuration Manager) 309
- LDAP-Verbindung testen 444
- Leistungsindikatoren
 - als Diagramm darstellen 433
 - Datensammlersätze erstellen 427
 - einzelne Instanz 421
 - mehrere Instanz 421
 - mit Get-Counter abrufen 419

- mit WMI abrufen 424
- Logische Laufwerke verwalten 118
- Lokale Sicherheitsgruppe 101
- Lokaler Konfigurations-Manager (LCM) 309

M

- Mail-Exchanger 88
- Managed Object Format (MOF) 288
- Master Boot Record (MBR) 118
- MBR (Master Boot Record) 118
- Metakonfiguration, DSC 309
- Microsoft Lan Manager 149
- MOF-Dokument 288

N

- Nested Virtualization 337
- net share 67
- Network Load Balancing (NLB) 280
- Netzwerke
 - Computer anpingen 67
 - DHCP aktivieren 79
 - DHCP-Bereiche konfigurieren 77
 - DHCP-Lastenausgleich konfigurieren 81
 - DHCP-Server installieren und autorisieren 75
 - DNS-Abfrage durchführen 68
 - DNS-Auflösungscache anzeigen 67
 - DNS-Auflösungscache leeren 68
 - DNS-Server 84
 - DNS-Serveradresse festlegen 74
 - freigegebenen Ordner verwenden 67
 - IP-Adresse statisch festlegen 74
 - IP-Adress-Konfiguration abrufen 67
 - Ordner freigeben 67
- Netzwerke *siehe auch* DHCP
- Netzwerke *siehe auch* DNS

Netzwerkonnektivität

LDAP-Verbindung testen 444

SMB-Verbindung testen 444

überprüfen 444

Netzwerklastenausgleich (NLB) 280

NLB (Netzwerklastenausgleich) 280

NLB-Cluster 285

Non-Uniform Memory Access 339–340

NTFS 117

NTFS-Berechtigungen verwalten 123

NTFSSecurity, Modul 123

Null-Session-Verbindung 158

NUMA 339–340

O

Ordner

ACL anzeigen 124

freigeben 67

freigegebenen verwenden 67

Ordnerziele, DFS 172

Organisationseinheit erstellen 98

P

Packet InterNetwork Groper 73

Paketverwaltung 38

Parametrierung, DSC-Konfiguration 296

Partitionen anzeigen 120

Performance Logs and Alerts (PLA) 416

Datensammlersätze 427

Leistungsüberwachung 416

Task-Manager 416

Performance Monitor 415

PFX-Datei 262, 264

Physikalische Datenträger verwalten 118

Ping 73

- Ping.exe 67
- PLA (Performance Logs and Alerts) 416
- PLA-Datensammlersätze
 - Ergebnisse auswerten 430
 - erstellen 427
- Ports für Active Directory 95
- Portweiterleitung, Container 241, 243
- PowerShell Direct 345
- PowerShellGet erforschen 41
- PowerShell-Katalog 41
- Prestaging eines Computerkontos 103
- Primäre Forward-Lookup-Zone 85
- Primäre Reverse-Lookup-Domäne 85
- PrintManagement 223
- PrintUI.DLL 214
- ProGet, internes Repository 48
- Protokollierung, IIS 268
- PSGallery 41
- Pullmodell, DSC 309
- Pullserver für DSC einrichten
 - HTTP 319
 - SMB 312
- Pullserver, DSC 289
- Pushmodell, DSC 309

R

- ReFS 117
- Remote Server Administration Tools (RSAT) 30
- Remoteserver-Verwaltungstools 30
- Replikationsgruppen (DFS-Replikation) 174
 - anzeigen 176
 - erstellen 176
 - Mitgliedschaftseinstellungen 177
- Replikationsrichtung, Speicherreplikat 129

- Replikationsserver, VM 371
- Repository 41
 - internes erstellen 48
- Ressourcen-Designer 304
- Ressourceneinträge erstellen 85
- Ressourcengruppe, Azure 390
 - erstellen 391
- Ressourcen-Manager für Dateiserver 133
 - installieren 133
 - Kontingentvorlage erstellen 134
 - Kontingentvorlagen anzeigen 134
 - SMTP-Einstellungen 134
 - Speicherberichte 141
- Root Directory Server Agent Service Entry 97

S

- SAN (Storage Area Networking) 150
- Scale-Out File-Server (SOFS) 150, 370
- SCSI-Controller in VM 352
- Secure Socket Layer (SSL) 255
- Seitenblobs 395
- Selbstsigniertes Zertifikat 256
- Sender Protected Framework 90
- Server Message Block (SMB) 149
- Server Name Indication (SNI) 267
- Serverankündigungen 153
- Signierung, SMB-Pakete 159
- SMB (Server Message Block) 149
- SMB-Dateifreigabe, Azure 401
- SMB-Dateiserver
 - einrichten 150
 - Einstellungen abrufen 151
 - Features installieren 151
 - SMB1-Protokoll deaktivieren 151

- SMB-Signierung und Verschlüsselung aktivieren 151
- SMB-Freigaben
 - Aufzählungsmodus 154
 - erstellen 154
 - Signierung aktivieren 159
 - Verschlüsselung aktivieren 154
 - vorhandene abrufen 154
 - zentraler Zertifikatsspeicher 261
 - Zugriff auf 158
 - Zugriffssteuerungsliste anzeigen 156
- SMB-Pullserver für DSC einrichten 312
- SMB-Verbindung testen 444
- SMTP-Einstellungen für FSRM 134
- Snapshots, VM 376
- SOFS (Scale-Out File-Server) 150
- Speicherberichte 133, 141
 - erstellen 141
- Speicherkonto, Azure 391
 - erstellen 392
 - primäre Endpunkte 392
- Speicherreplikat
 - Feature installieren 129
 - Partnerschaft anzeigen 129
 - Partnerschaft erstellen 129
 - Replikationsrichtung ändern 129
- Speicherschlüssel 401
- SPF-Ressourceneinträge 90
- Spooler-Dienst neu starten 218
- Spoolerverzeichnis ändern 217
- SSL-Protokoll 255
- Stammzertifikatsspeicher 262
- Startreihenfolge im BIOS 352
- Storage Area Networking, SAN 150
- SWEET32 Birthday Attacks 260

Systemdiagnosebericht 436

T

Table Storage 395

TCPing (Anwendung), Downloadlink 73

Teilkonfigurationen, DSC 327

Testseite drucken 221

Transport Layer Security (TLS) 255

U

UDF 117

Unternehmenszertifizierungsstelle 335

Updateklassifizierungen 192

in Regel für automatische Genehmigung 203

V

Veröffentlichungsprofil, Azure Web-App 407

Verschachtelte Hyper-V-Virtualisierung 360

Verschachtelte Virtualisierung 337

Verschlüsselung

SMB-Dateiserver 151

SMB-Freigaben 154

Verschlüsselungssuites 258

VHDX-Datei erstellen 352

Virtualisierung *siehe* Hyper-V

Virtueller Switch 356

VM

Anzahl der virtuellen Prozessoren 352

Bericht erstellen über 440

COM-Ports 355

Datenträger verschieben 366

erstellen 342–343

Failover-Test 373

herunterfahren 352

in Azure erstellen 411

- Netzwerke konfigurieren 355
- neue VHDX-Datei erstellen 352
- Prüfpunkte 376
- Replikation konfigurieren 371
- SCSI-Controller hinzufügen 352
- starten 343, 352
- Startreihenfolge im BIOS 352
- Status verwalten 363
- verschieben 366
- virtuelle Festplatte erstellen 343
- virtuelles Diskettenlaufwerk 355
- VMConnect 375
- VM-Hardware konfigurieren 351
- Volume Shadow Copy Service (VSS) 376
- Volumeschattenkopie 376

W

- Webserver installieren 250
- Windows Assessment and Deployment Kit 342
- Windows Defender und Docker 232
- Windows Server Update Services *siehe* Windows Update
- Windows Update
 - automatische Genehmigungen 202
 - automatische Synchronisierung 193
 - Client konfigurieren 196
 - Computer-Zielgruppen 200
 - Ereignisprotokoll 453
 - Feature installieren 184
 - Produktkategorien 185
 - Synchronisierung konfigurieren 191
 - Synchronisierungsstatus 195
 - Updateklassifizierungen 192
 - vollständige Synchronisierung 189
- WinRM 424

WMI, Leistungsindikatoren abrufen mit 424

WSUS *siehe* Windows Update

Z

Zertifikate als PFX-Datei exportieren 262

Zertifikatsspeicher, zentraler 260

Zertifizierungsstelle 255

Zugriffssteuerungseinträge 123

Zugriffssteuerungslisten 118, 123

- anzeigen 124

- Drucker 222

- SMB-Freigaben 156

- vererbte Rechte 124