

VARONIS LEISTUNGSKATALOG

ZU DEN PRODUKTEN DATADVANTAGE UND DATAPRIVILEGE

Inhaltsverzeichnis

Einleitung	02
Grundsatzhandbuch des BSI	03
Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie	05
varonis© datadvantage©	05
Feature 1: Bidirektionale Sicht	06
Feature 2: Berechtigungsvorschläge	07
Feature 3: Audit Trail	08
Feature 4: Berechtigungsmodellierung	09
Feature 5: Reports	10
varonis© dataprivilege©	11
Feature 1: Webbasierte Berechtigungsanfrage	11
Feature 2: Webbasierte Gruppenmitgliedschaftsanfrage	12
Feature 3: Webbasierte Berechtigungs- und Gruppenmitgliedschaftserteilung	13
Feature 4: Entitlement Review	14
Zusammenfassung	15
Unterstützte Plattformen	16
Event Übersicht	166
Anforderungen an eine Testinstallation	17

EINLEITUNG

Unstrukturierte Daten wachsen exponentiell. Unternehmen aller Größenordnungen sehen sich einer zunehmenden Datenflut ausgesetzt, die verfügbar gehalten werden muss. In einem typischen Fortune 1000-Unternehmen wachsen unstrukturierte Daten jährlich mit ca. 30% (vgl. Gartner). Ein Großteil der Daten können als unternehmenskritisch eingeschätzt werden, da sie entweder personenbezogenen Inhalt haben oder als vertrauliche Daten gelten. Dieses rasante Wachstum führt dazu, dass sicherheitsrelevante Fragen immer schwerer beantwortet werden können:

- Wer hat welche Berechtigungen?
- Wer hat auf welche Daten tatsächlich zugegriffen?
- Wer sollte auf welche Daten zugreifen können?
- Wer ist der „Data Owner“?

Der erhebliche Kostendruck in der Administration und die dadurch reduzierten Mittel zur Überprüfung der Berechtigungen führen zu einem Aufweichen der Sicherheitsregeln. Dies bedeutet: Unternehmen setzen Berechtigungen in vielen Fällen so, dass unternehmenskritische Daten im Zugriff zu vieler Mitarbeiter sind. Dies stellt nicht nur ein finanzielles wie auch ein Sicherheitsrisiko dar sondern auch einen rechtlichen Verstoß. So gibt es mehrere rechtliche Regularien, die eindeutig vorgeben, wie Berechtigungen auf personenbezogene als auch auf unternehmenskritische Daten zu regeln sind. Der folgende Text zeigt auf, welche regulatorischen Maßgaben existieren und wie adäquat auf diese Herausforderung reagiert werden kann.

BERECHTIGUNGEN UND BERECHTIGUNGSMANAGEMENT

Wenn im Folgenden von Berechtigungen bzw. deren Management gesprochen wird, dann ist damit der Blick auf Benutzer oder Gruppen und Ressourcen gemeint. Die Grundfrage, die sich stellt ist: Wer (Benutzer oder Gruppen) darf auf welche Ressourcen (Systeme, Anwendungen, Dienste etc.) zugreifen und was (lesen, schreiben, ausführen, ändern, löschen) damit tun?

RECHTLICHE ANFORDERUNGEN UND BERECHTIGUNGSMANAGEMENT

Grundschutzhandbuch des BSI

Das Grundschutzhandbuch des BSI macht klare Vorgaben, wie Berechtigungen und damit Zugriffe auf Ressourcen zu handhaben sind. Darüber hinaus wird im Grundschutzhandbuch klar darauf verwiesen, dass das Managen von Berechtigungen aufwändig ist und oft nicht mit der nötigen Sorgfalt erledigt wird.

Folgende Maßnahmen aus dem IT-Grundschutzhandbuch enthalten die Kernanweisungen für ein Berechtigungsmanagement-Konzept.

M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme:

- Wird sichergestellt, dass nur autorisierte Personen IT-Systeme benutzen können (Zugangskontrolle)?
- Wird sichergestellt, dass Benutzer nur auf die Daten zugreifen können, die sie zur Aufgabenerfüllung benötigen?
- Sind Unregelmäßigkeiten und Manipulationsversuche erkennbar?
- Sind Daten gegen zufällige Zerstörung oder Verlust geschützt (Verfügbarkeitskontrolle)?

M 2.8 Vergabe von Zugriffsrechten

- Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?
- Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?
- Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?
- Existiert ein geregelter Verfahren für den Entzug von Zugriffsrechten?

M 4.149 Datei- und Freigabeberechtigungen unter Windows

- Wurde ein bedarfsgerechtes Berechtigungs- und Zugriffskonzept entworfen?
- Sind im Berechtigungs- und Zugriffskonzept auch organisatorische und geschäftliche Anforderungen berücksichtigt worden?

M 2.370 Administration der Berechtigungen unter Windows Server 2003

- Werden vorsorglich Simulationswerkzeuge bei der Modellierung von Berechtigungen und bei der Administration im laufenden Betrieb benutzt?

M 4.53 Vergabe von Zugriffsrechten:

- Wird die Attributvergabe bei Systemdateien und der Registrierung regelmäßig überprüft?
- Werden die Einstellungen der Benutzerprofile regelmäßig überprüft?
- Gibt es Listen, anhand derer diese Überprüfungen durchgeführt werden?

Zusammenfassend lässt sich aus diesen Anforderungen ableiten, dass bezüglich eines Berechtigungsmanagements für unstrukturierte Daten die folgende Punkte sicher gestellt sein müssen.

1. Need-to-Know Prinzip: Jeder Benutzer (und auch jeder Administrator) sollte nur auf jene Datenbestände zugreifen dürfen, die er für seine tägliche Arbeit auch wirklich benötigt.
Dem läuft entgegen, dass Mitarbeiter durch das Vergessen von globalen Gruppen auf Ordnern Zugriff auf Daten erlangen. Das Auditieren von Berechtigungen der globalen Gruppen ist nur mit großem Aufwand möglich. Desweiteren besteht das Problem, dass Mitarbeiter generell an zu vielen Ordnern berechtigt sind, da z.B. vergessen wurde, bei Abteilungswechsel die alte Berechtigung zu entziehen (Azubi Effekt).
2. Kontinuierliche Überprüfung von Berechtigungen. In der Praxis werden Berechtigungen in der Regel nur einmalig überprüft und das ist bei der initialen Einrichtung. Danach werden Berechtigungen jedoch nur sehr selten auf Richtigkeit überprüft bzw. an neue organisatorische Erfordernisse angepasst. Dies führt dazu, dass Überberechtigungen entstehen.
3. Fachverantwortliche (DataOwner) sind in den Berechtigungsmanagement-Prozess zu involvieren. Um Berechtigungen akkurat zu halten, ist es wichtig, Fachverantwortliche zu involvieren, da nur diese wissen können, wer mit den Daten arbeiten muss. Dem läuft in der Praxis entgegen, dass die Fachverantwortlichen für einen Großteil der Daten gar nicht bekannt sind.
4. Unberechtigter Zugriff auf Daten ist zu erkennen. Unberechtigte administrative Zugriffe auf Daten (z.B. Personaldaten) sind schwer bis gar nicht zu erkennen. Dies führt dazu, dass Administratoren unter Generalverdacht stehen.

Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie

Informationssysteme spielen im Rahmen der Abschlussprüfung und der Buchführung im allgemeinen eine immer größer werdende Rolle. Aus diesem Grund werden Systeme der elektronischen Datenverarbeitung zunehmend Gegenstand der Prüfung durch Wirtschaftsprüfer. Grundsätzlich sind die folgenden Papiere Grundlage der Audits durch den Wirtschaftsprüfer:

- Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1 vom 24.09.2002) (Quelle: WPg 2002, S. 1157 ff., Heft-Nr. 21/2002)
- IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330 vom 24.09.2002) (Quelle: WPg 2002, S. 1167 ff., Heft-Nr. 21/2002)

Kernaussagen der Arbeitspapiere sind, dass Voraussetzung für die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung neben der Gesetzesentsprechung des Rechnungslegungssystems die Sicherheit der verarbeiteten Daten ist. Dies bedeutet, dass über den Zugriffsschutz auch ein organisatorischer Prozess aufgesetzt sein muss, der Berechtigungen und deren Vergabe regelt. Zitat: In organisatorischen Grundsätzen sind die Einrichtung und Entziehung von Berechtigungen, die Protokollierung aller Aktivitäten im Bereich der Berechtigungsverwaltung, ... festzulegen. “ (vgl: Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie 2001)

Des weitern wird klar auf das „Need to Know Prinzip “ verwiesen, d.h. „Mitarbeitern sind nur die Berechtigungen zu erteilen, die zur Wahrnehmung ihrer Aufgaben erforderlich sind “ (vgl: Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie 2001)

VARONIS© DATADVANTAGE©

Varonis DatAdvantage ist eine Lösung zur Optimierung von Daten- und Berechtigungsmanagement auf Windows und Unix File Servern, NAS-Devices, Exchange und Microsoft Share Point. Über standardisierte Workflows und eine zentrale administrative Oberfläche bietet Varonis die optimalen Voraussetzung, um Daten zu analysieren, zu reporten und Filesysteme zentral unter Kontrolle zu halten und so rechtlichen Regularien zu entsprechen.

Feature 1: Bidirektionale Sicht

Diese Funktion ermöglicht einem Administrator, ohne Aufwand eine zentrale Übersicht über die gesamten Filesystemberechtigungsstrukturen zu erhalten. Dies wird von Varonis DatAdvantage durch das Auslesen/Scannen der Benutzer und Gruppen aus dem Active Directory, der ACLs und der Ordnerstruktur möglich. Die Kombination ermöglicht eine zentrale und visuelle Wiedergabe. Es ist zu ersehen, wer an welchem Ordner welche Rechte hat und warum. Ungeachtet von Verschachtelung oder von direkten Berechtigungen.

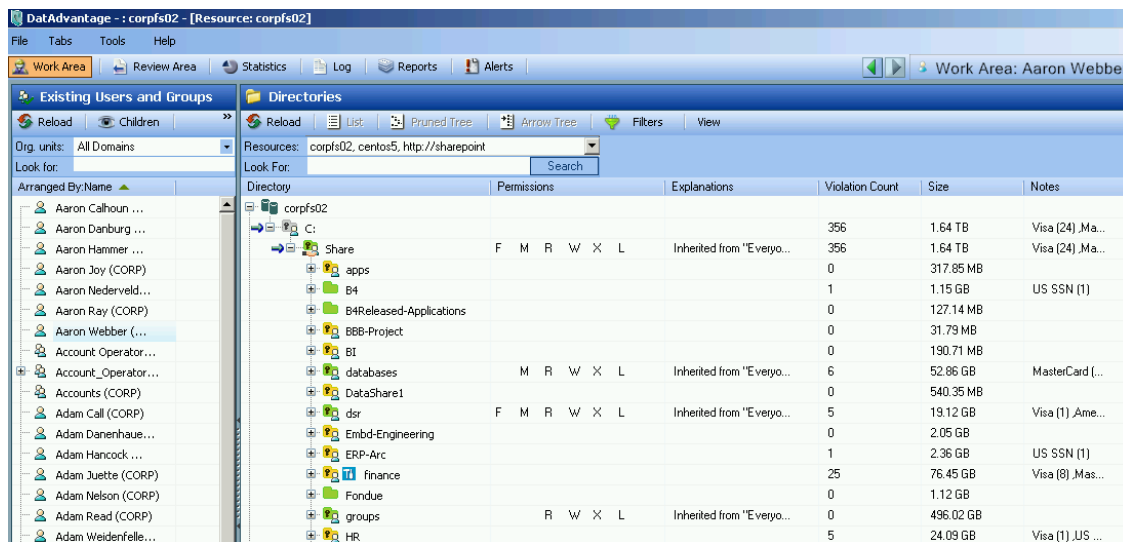
Dies liefert die Grundlage, um Berechtigungskonzepte zu prüfen, zu überarbeiten, aufzuräumen oder auch Filesysteme zu migrieren. Desweiteren kann direkt aus der zentralen administrativen Oberfläche eine Berechtigungsänderung/-säuberung durchgeführt werden. Alle Berichte sind auch per Report darstellbar. Die Reports können per Mail in verschiedensten Formaten versendet werden.

Durch diese Funktionalität können Fragen beantwortet werden wie z.B.:

An welchen Ordnern haben globale Gruppen (z.B. Jeder) Zugriffsrechte?

An welchen Ordner hat eine gewisser User Zugriffsrechte?

Welche Personen und Gruppen haben auf einen Ordner Zugriffsrechte?

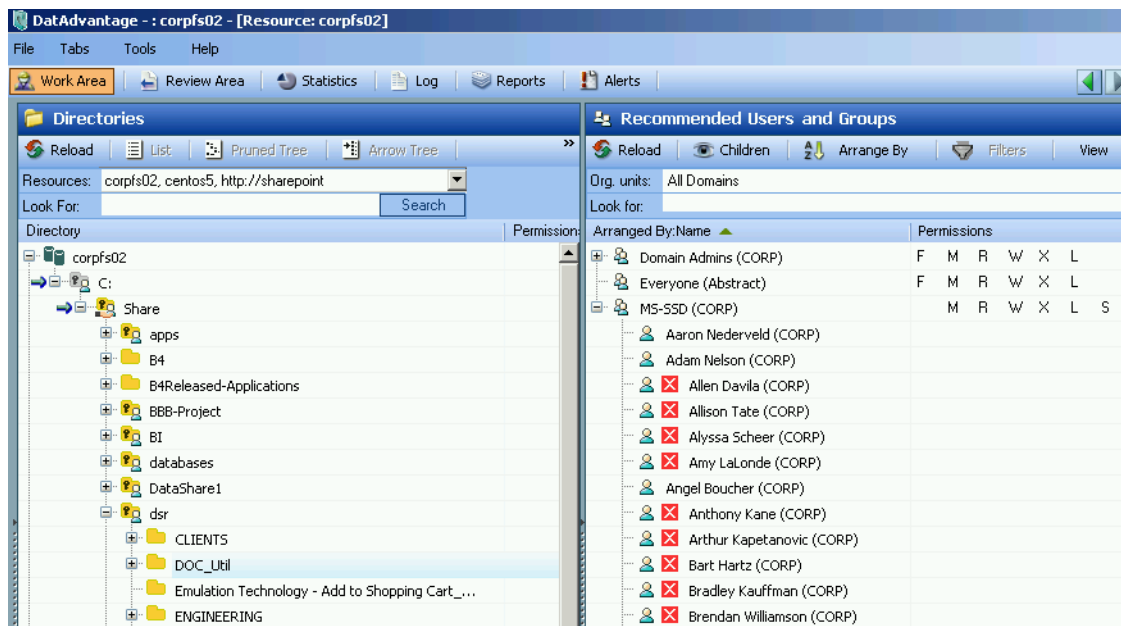


The screenshot shows the Varonis DatAdvantage interface. On the left, there is a tree view of 'Existing Users and Groups' with a list of users and groups. On the right, there is a 'Directories' pane showing a tree view of the file system structure. Below the tree view, there is a table with columns: Directory, Permissions, Explanations, Violation Count, Size, and Notes.

Directory	Permissions	Explanations	Violation Count	Size	Notes
corpfs02					
Share	F M R W X L	Inherited from "Everyo...	356	1.64 TB	Visa (24) ,Ma...
apps			0	317.85 MB	Visa (24) ,Ma...
B4			1	1.15 GB	US SSN (1)
B4Released-Applications			0	127.14 MB	
BBB-Project			0	31.79 MB	
BT			0	190.71 MB	
databases	M R W X L	Inherited from "Everyo...	6	52.86 GB	MasterCard (...)
DataShare1			0	540.35 MB	
dsv	F M R W X L	Inherited from "Everyo...	5	19.12 GB	Visa (1) ,Ame...
Embd-Engineering			0	2.05 GB	
ERP-Arc			1	2.36 GB	US SSN (1)
finance			25	76.45 GB	Visa (8) ,Mas...
Fondue			0	1.12 GB	
groups	R W X L	Inherited from "Everyo...	0	496.02 GB	
HR			5	24.09 GB	Visa (1) ,JUS ...

Feature 2: Berechtigungsvorschläge

Mit der Berechtigungsvorschläge-Funktion bietet Varonis DatAdvantage einen einzigartigen Prozess zum Aufzeigen und Eliminieren von Überberechtigungen. So kann sicher gestellt werden, dass Mitarbeiter nur die Berechtigungen an Daten haben, die Sie auch wirklich zum täglichen Arbeiten benötigen. Überberechtigungen können vielfältige Gründe haben, so z.B. Abteilungswechsel oder Mitarbeit in Projekten. Varonis erkennt Berechtigungen, die Benutzer zu Unrecht führen und macht konkrete Vorschläge, diese zu beseitigen. Darüber hinaus können in diesen Prozess Data-Owner (Fachverantwortliche) involviert werden.



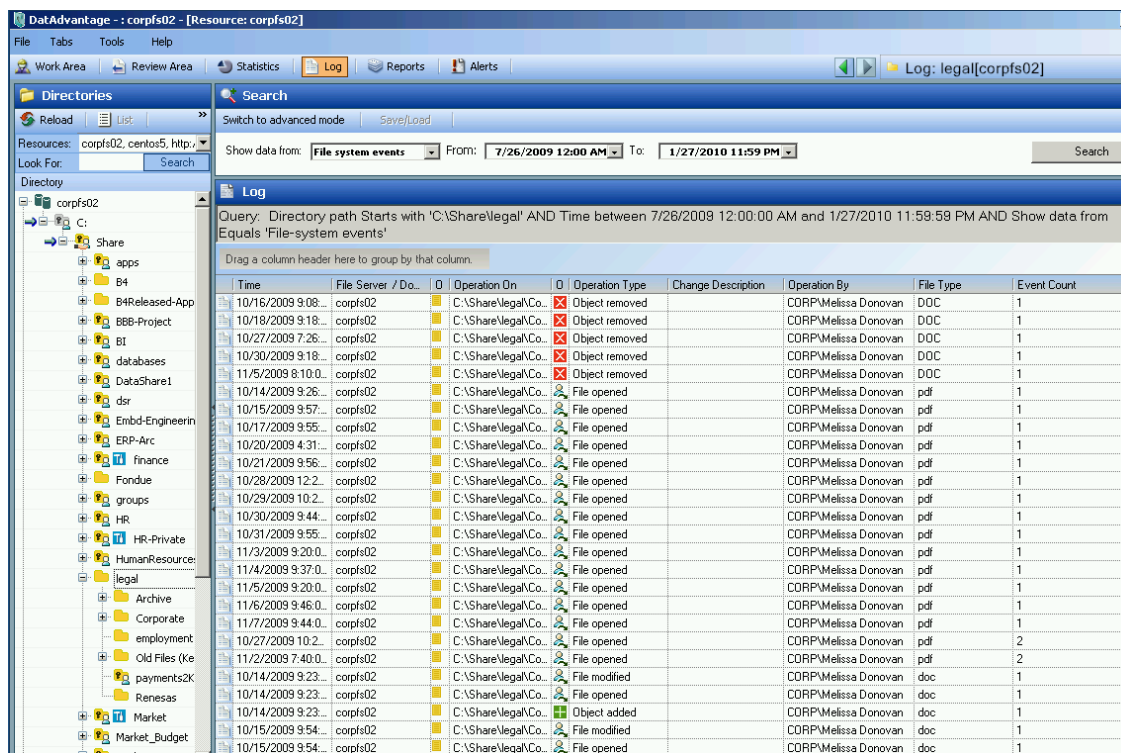
The screenshot displays the Varonis DatAdvantage interface for a resource named 'corpfs02'. The interface is divided into two main panes:

- Directories Pane (Left):** Shows a tree view of the file system. The root is 'corpfs02', which contains a 'Share' folder. Under 'Share', there are several subfolders: 'apps', 'B4', 'B4Released-Applications', 'BBB-Project', 'BI', 'databases', 'DataShare1', 'dsr', 'CLIENTS', 'DOC_Util', 'Emulation Technology - Add to Shopping Cart_...', and 'ENGINEERING'.
- Recommended Users and Groups Pane (Right):** Displays a list of users and groups with their permissions. The list is arranged by name and includes the following entries:

Entity	Permissions
Domain Admins (CORP)	F M R W X L
Everyone (Abstract)	F M R W X L
MS-SSD (CORP)	M R W X L S
Aaron Nederveld (CORP)	
Adam Nelson (CORP)	
Allen Davila (CORP)	
Allison Tate (CORP)	
Alyssa Scheer (CORP)	
Amy LaLonde (CORP)	
Angel Boucher (CORP)	
Anthony Kane (CORP)	
Arthur Kapetanovic (CORP)	
Bart Hartz (CORP)	
Bradley Kauffman (CORP)	
Brendan Williamson (CORP)	

Feature 3: Audit Trail

Mit dem Audit-Trail bietet Varonis DatAdvantage eine 100%ige Nachvollziehbarkeit zur Frage der Datenverwendung in Unternehmen. Varonis loggt die Filesystem- Events (CIFS, NFS). Konkret kann nachvollzogen werden, ob eine Datei geöffnet, erstellt, gelöscht, umbenannt, verschoben oder verändert wurde. Diese Events werden in einer zentralen Datenbank abgelegt und können durchsucht, sortiert und gruppiert werden. Events werden nicht nur für Benutzer, sondern auch für lokale Administratoren erstellt. Die Filesystem-Events werden über Standardschnittstellen geloggt- ohne das Aktivieren der Microsoft Auditing-Funktion.

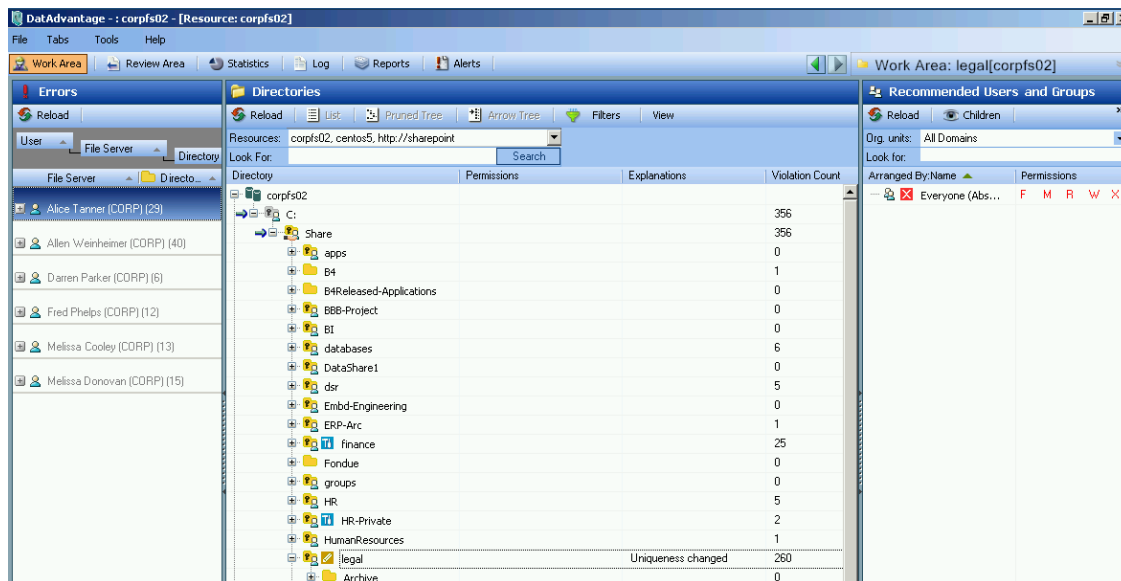


The screenshot shows the Varonis DatAdvantage interface. The search criteria are set to 'File system events' from '7/26/2009 12:00 AM' to '1/27/2010 11:59 PM'. The log query is: 'Directory path Starts with 'C:\Share\legal' AND Time between 7/26/2009 12:00:00 AM and 1/27/2010 11:59:59 PM AND Show data from Equals 'File-system events''.

Time	File Server / Do...	Operation On	Operation Type	Change Description	Operation By	File Type	Event Count
10/16/2009 9:08...	corps02	C:\Share\legal\Co...	Object removed		CORPMelissa Donovan	DOC	1
10/18/2009 9:18...	corps02	C:\Share\legal\Co...	Object removed		CORPMelissa Donovan	DOC	1
10/27/2009 7:26...	corps02	C:\Share\legal\Co...	Object removed		CORPMelissa Donovan	DOC	1
10/30/2009 9:18...	corps02	C:\Share\legal\Co...	Object removed		CORPMelissa Donovan	DOC	1
11/5/2009 8:10:0...	corps02	C:\Share\legal\Co...	Object removed		CORPMelissa Donovan	DOC	1
10/14/2009 9:26...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/15/2009 9:57...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/17/2009 9:55...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/20/2009 4:31...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/21/2009 9:56...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/28/2009 12:2...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/29/2009 10:2...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/30/2009 9:44...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/31/2009 9:55...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
11/3/2009 9:20:0...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
11/4/2009 9:37:0...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
11/5/2009 9:20:0...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
11/6/2009 9:46:0...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
11/7/2009 9:44:0...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	1
10/27/2009 10:2...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	2
11/2/2009 7:40:0...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	pdf	2
10/14/2009 9:23...	corps02	C:\Share\legal\Co...	File modified		CORPMelissa Donovan	doc	1
10/14/2009 9:23...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	doc	1
10/14/2009 9:23...	corps02	C:\Share\legal\Co...	Object added		CORPMelissa Donovan	doc	1
10/15/2009 9:54...	corps02	C:\Share\legal\Co...	File modified		CORPMelissa Donovan	doc	1
10/15/2009 9:54...	corps02	C:\Share\legal\Co...	File opened		CORPMelissa Donovan	doc	1

Feature 4: Berechtigungsmodellierung

Die Funktion der Berechtigungsmodellierung bietet die Möglichkeit, geplante Berechtigungsstrukturänderungen im Vorfeld auf der Datenbank zu simulieren, so dass bei der Umsetzung das Fehlerpotential minimiert wird. Dies erspart wertvolle Support- und Nacharbeitungszeit. So ist es z.B. möglich zu simulieren, welche Effekte das Löschen einer Gruppe von einem Laufwerk hat. Über eine Fehlerfunktion wird Ihnen in einem Report Tree ausgegeben, welche Benutzer Berechtigungen zu unrecht verlieren würden. Auch bei einer Filesystem-Migration ist diese Funktion äußerst nützlich, um den IST- mit dem SOLL- Zustand abzugleichen.



The screenshot shows the DatAdvantage interface with the following components:

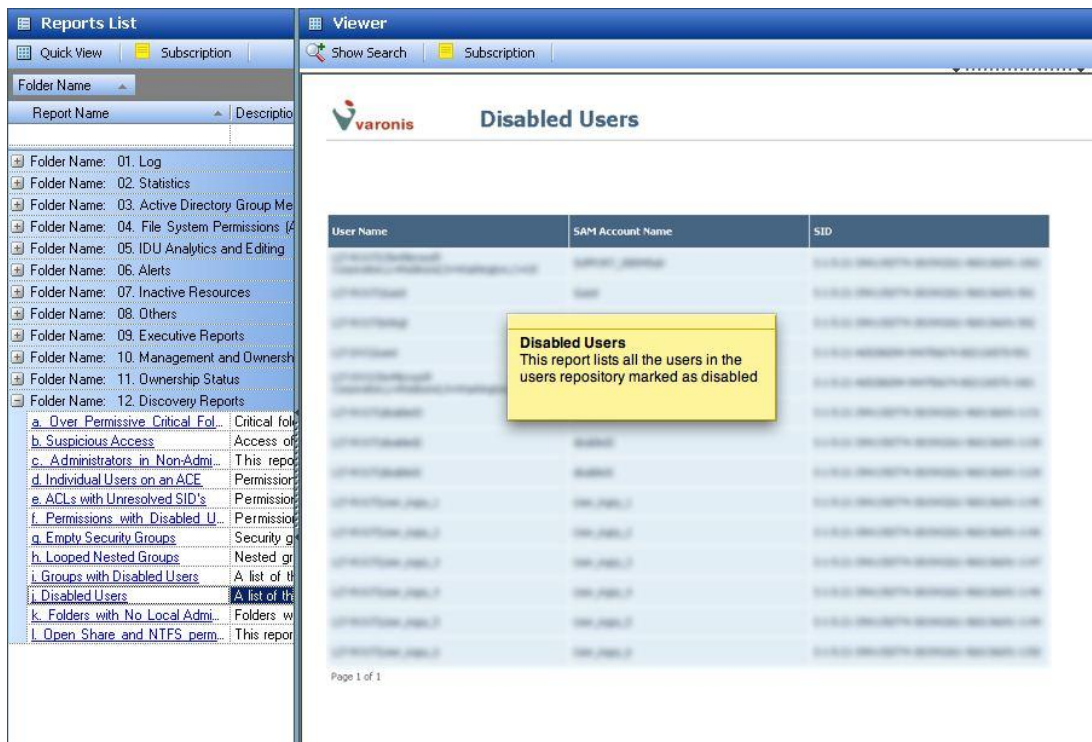
- Errors Panel:** Lists users such as Alice Tanner (CORP) (29), Allen Weinheimer (CORP) (40), Darren Parker (CORP) (6), Fred Phelps (CORP) (12), Melissa Cooley (CORP) (13), and Melissa Donovan (CORP) (15).
- Directories Panel:** Displays a tree view of the file system under 'corpfs02', including folders like 'Share', 'apps', 'B4', 'B4Released-Applications', 'BBB-Project', 'BI', 'databases', 'DataShare1', 'dsr', 'Embd-Engineering', 'ERP-Arc', 'finance', 'Fondue', 'groups', 'HR', 'HR-Private', 'HumanResources', 'legal', and 'Archive'.
- Table:** A table with columns 'Directory', 'Permissions', 'Explanations', and 'Violation Count'. The 'Violation Count' column shows values for each directory, such as 356 for 'Share', 0 for 'apps', 1 for 'B4', 0 for 'B4Released-Applications', 0 for 'BBB-Project', 0 for 'BI', 6 for 'databases', 0 for 'DataShare1', 5 for 'dsr', 0 for 'Embd-Engineering', 1 for 'ERP-Arc', 25 for 'finance', 0 for 'Fondue', 0 for 'groups', 5 for 'HR', 2 for 'HR-Private', 1 for 'HumanResources', 260 for 'legal' (with the explanation 'Uniqueness changed'), and 0 for 'Archive'.
- Recommended Users and Groups Panel:** Shows a list of users and groups with their permissions, including 'Everyone (Abs...)' with permissions F, M, R, W, X.

Feature 5: Reports

Mit der Reportsektion ist es möglich individuelle Berichte zu generieren, die verschiedenste Analysen des Filesystems zulassen so sind unter anderem die folgenden Abfragen mögliche:

- Berechtigungsreports crossplattform (NTFS; Exchange; Unix; SharePoint)
- Reports bezüglich Konfigurationsfehler (Rekursion, tote SIDs etc.)
- Datennutzungsanalysen (None business data, ungenutzte Daten)

Die Reports können in verschiedenen Formaten generiert werden und auch abonniert werden. So ist es z.B. möglich einmal im Monat einen Report in Excel zu versenden der die Personen aufführt die an dem Ordner berechtigt sind.



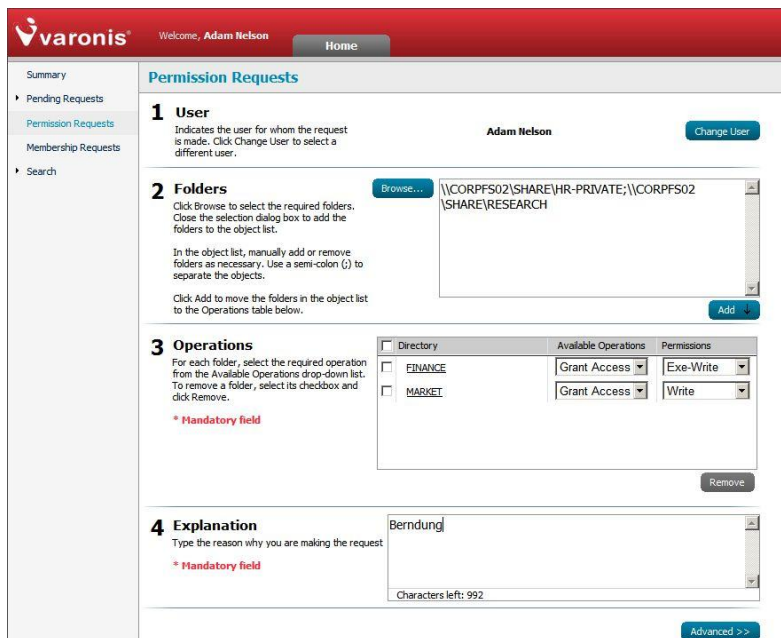
The screenshot shows the 'Reports List' and 'Viewer' sections of the Varonis interface. The 'Reports List' on the left contains a tree view of reports, with '12. Discovery Reports' expanded to show sub-reports like 'i. Groups with Disabled Users'. The 'Viewer' on the right displays the 'Disabled Users' report, which includes a table with columns for 'User Name', 'SAM Account Name', and 'SID'. A yellow tooltip box is overlaid on the table, stating: 'Disabled Users This report lists all the users in the users repository marked as disabled'. The page number 'Page 1 of 1' is visible at the bottom of the viewer.

VARONIS® DATAPRIVILEGE®

Varonis DataPrivilege ermöglicht es, die Verantwortung für das Management der Datenzugriffsberechtigung vom IT-Bereich auf die Business Owners ohne Änderungen der Infrastruktur oder Unterbrechungen im Firmengeschäft zu übertragen. DataPrivilege bringt Dateninhaber und Datenbenutzer in einem Forum zur Kommunikation, Autorisierung und Aktivierung von Berechtigungen zusammen. Varonis DataPrivilege erlaubt es, ein geschlossenes Umfeld zur Datenzugriffsberechtigung zu schaffen und dabei die Verantwortlichkeit zu verbessern und Risiken zu verringern.

Feature 1: Webbasierte Berechtigungsanfrage

Mit Varonis DataPrivilege implementieren Sie einen webbasierten Prozess zur Berechtigungsvergabe auf bestehende Ordnerstrukturen: Ein Mitarbeiter erfragt über eine Website Berechtigungen an einem Ordner bzw. mehreren Ordnern. Die Website, über welche die Anfrage gestellt wird, kann in vorhandene Systeme eingebunden werden (z.B. Intranet). Sobald der Mitarbeiter die Anfrage bestätigt, wird diese dokumentiert und aufgezeichnet. Desweiteren wird eine Mail generiert, die an den vorher definierten Business Owner versandt wird. In dem Prozess können mehrere Business Owner definiert werden. Der Mitarbeiter kann zu jedem Zeitpunkt den Bearbeitungsstand über das Webinterface abfragen.



The screenshot shows the 'Permission Requests' web interface. It features a sidebar on the left with navigation links: Summary, Pending Requests, Permission Requests (selected), Membership Requests, and Search. The main content area is titled 'Permission Requests' and contains four numbered sections:

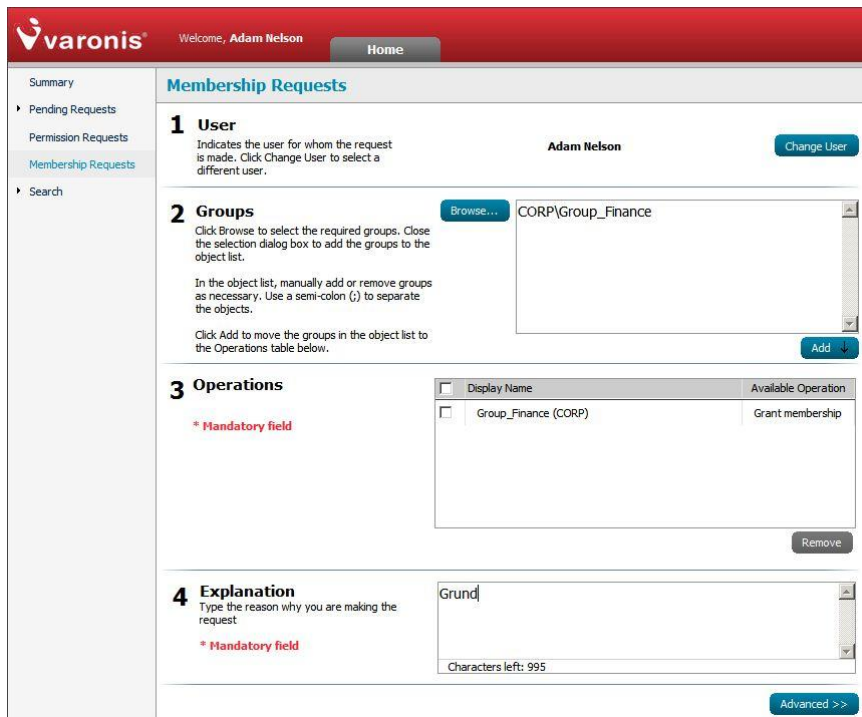
- 1 User:** Indicates the user for whom the request is made. The user is 'Adam Nelson'. A 'Change User' button is present.
- 2 Folders:** Click Browse to select the required folders. A text box contains the path: '\\CORPFS02\SHARE\HR-PRIVATE;\CORPFS02\SHARE\RESEARCH'. An 'Add' button is at the bottom right.
- 3 Operations:** For each folder, select the required operation from the Available Operations drop-down list. A table shows:

Directory	Available Operations	Permissions
<input type="checkbox"/> FINANCE	Grant Access	Exe-Write
<input type="checkbox"/> MARKET	Grant Access	Write

 A 'Remove' button is at the bottom right.
- 4 Explanation:** Type the reason why you are making the request. The text 'Berndung' is entered. A 'Characters left: 992' indicator is at the bottom. An 'Advanced >>' button is at the bottom right.

Feature 2: Webbasierte Gruppenmitgliedschaftsanfrage

Mit Varonis DataPrivilege implementieren Sie einen webbasierten Prozess zur Mitgliedschaftsanfrage auf bestehende Gruppen: Ein Mitarbeiter erfragt über eine Website Gruppenmitgliedschaften an bzw. mehreren Gruppen. Die Website, über welche die Anfrage gestellt wird, kann in vorhandene Systeme eingebunden werden (z.B. Intranet). Sobald der Mitarbeiter die Anfrage bestätigt, wird diese dokumentiert und aufgezeichnet. Desweiteren wird eine Mail generiert, die an den vorher definierten Business Owner versandt wird. In dem Prozess können mehrere Business Owner definiert werden. Der Mitarbeiter kann zu jedem Zeitpunkt den Bearbeitungsstand über das Webinterface abfragen.



Membership Requests

1 User
Indicates the user for whom the request is made. Click Change User to select a different user.
Adam Nelson [Change User](#)

2 Groups
Click Browse to select the required groups. Close the selection dialog box to add the groups to the object list.
In the object list, manually add or remove groups as necessary. Use a semi-colon (;) to separate the objects.
Click Add to move the groups in the object list to the Operations table below.
[Browse...](#) CORP\Group_Finance [Add](#)

3 Operations
* Mandatory field

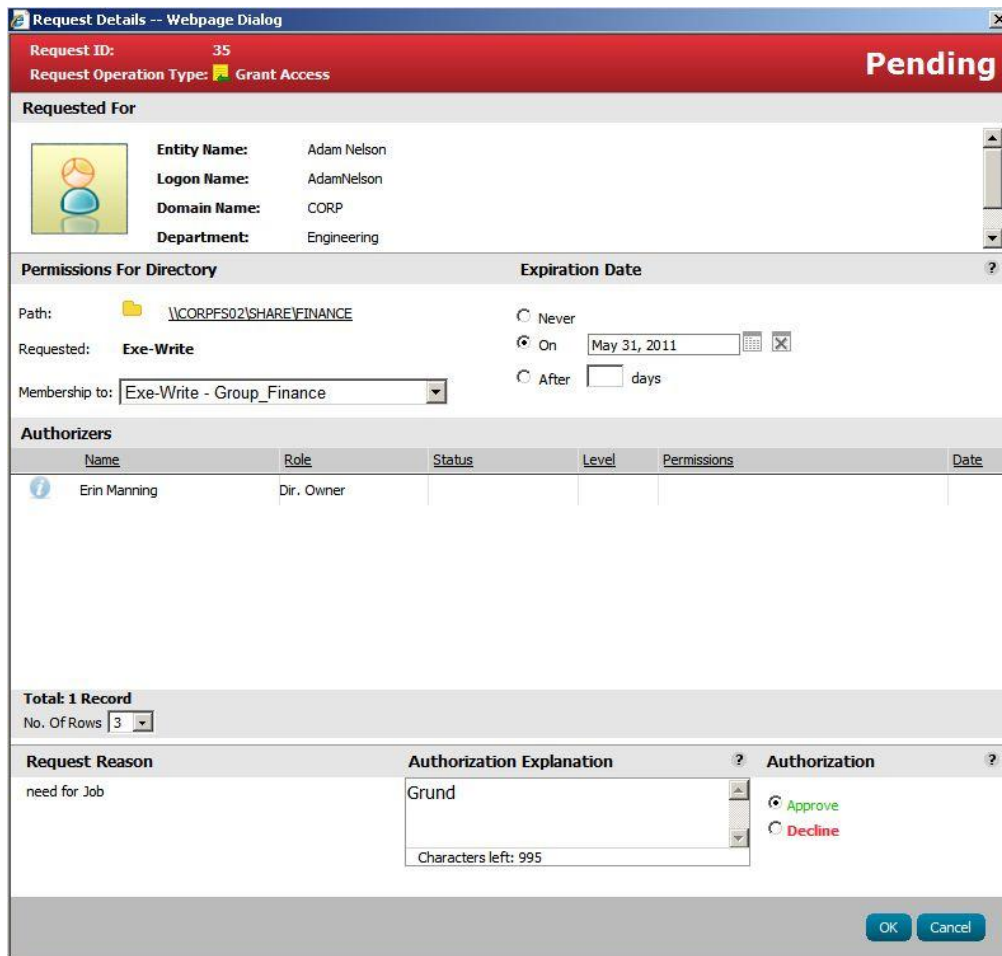
<input type="checkbox"/> Display Name	Available Operation
<input type="checkbox"/> Group_Finance (CORP)	Grant membership

[Remove](#)

4 Explanation
Type the reason why you are making the request
* Mandatory field
Grund
Characters left: 995
[Advanced >>](#)

Feature 3: Webbasierte Berechtigungs- und Gruppenmitgliedschaftserteilung


Sobald ein Benutzer eine Berechtigungs- oder Gruppenmitgliedschaftsanfrage gestellt hat, erhält der Verantwortliche auf der Fachseite eine Benachrichtigung per Mail, dass er diese Anfrage frei geben kann oder muss. Über das Webinterface sieht er die Anfrage und kann diese entsprechend bearbeiten. So ist es ihm möglich, diese Anfrage zu verwerfen, ihr zuzustimmen oder auch nur zeitlich eingeschränkt zu entsprechen. Alle Aktionen werden dokumentiert und lassen sich im Nachgang nachvollziehen.




Request Details -- Webpage Dialog



Request ID: 35
Request Operation Type: Grant Access **Pending**

Requested For


 **Entity Name:** Adam Nelson
Logon Name: AdamNelson
Domain Name: CORP
Department: Engineering

Permissions For Directory **Expiration Date** ?

Path:  \\CORPFS02\SHARE\FINANCE
Requested: **Exe-Write**
Membership to: Exe-Write - Group_Finance

Never
 On  
 After days

Authorizers

Name	Role	Status	Level	Permissions	Date
 Erin Manning	Dir. Owner				

Total: 1 Record
No. Of Rows: 3

Request Reason **Authorization Explanation** ? **Authorization** ?

need for Job

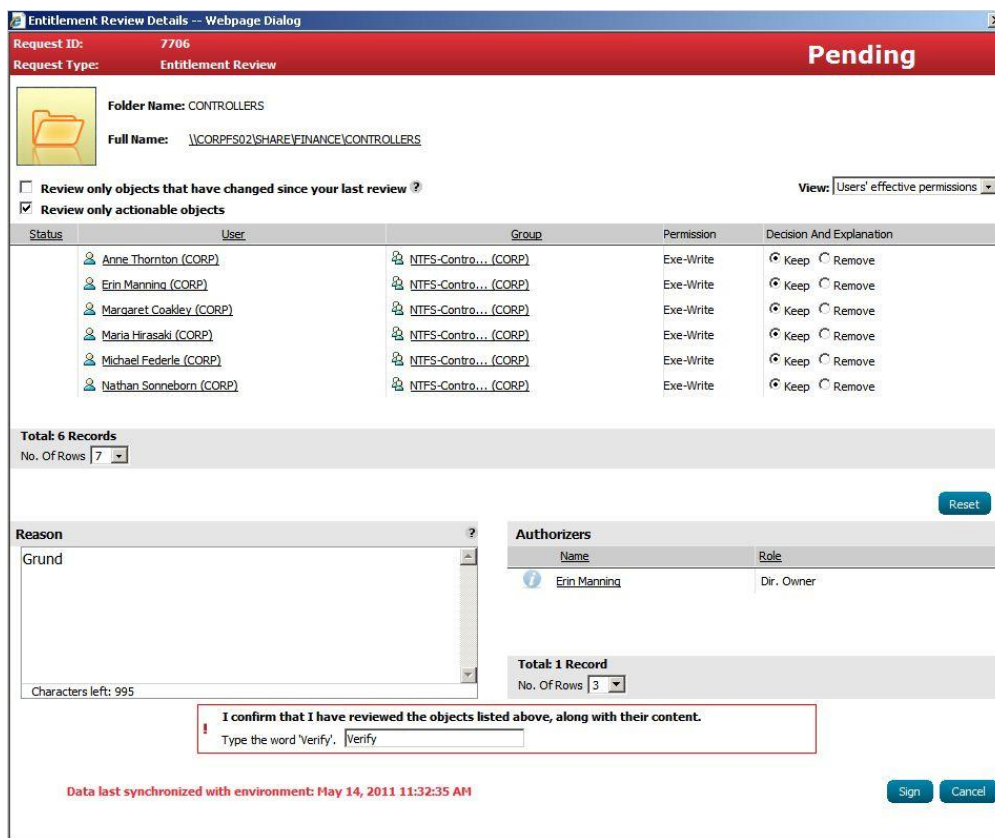
Grund

Characters left: 995

Approve
 Decline

Feature 4: Entitlement Review

Das regelmäßige Überprüfen von gewährten Berechtigungen ist extrem wichtig, da nur so Überberechtigungen auf Dauer verhindert werden können. Berechtigungen müssen an geänderte Strukturen fortlaufend angepasst werden. Hierzu gibt es den Prozess des Entitlement Reviews. Hier wird dem Data Owner in einem festgesetzten Intervall (z.B. einmal im Quartal) eine Mail gesendet mit der Bitte über das Webinterface Berechtigungen zu überprüfen und gegebenenfalls diese zu entziehen. Über den Workflow kann gesteuert werden was passieren soll wenn der Data Owner seiner Aufgabe nicht nachkommt. Eine Möglichkeit wäre eine Erinnerung zu schreiben oder den Vorgang an eine andere Person weiterzuleiten.



Request ID: 7706
Request Type: Entitlement Review

Pending

Folder Name: CONTROLLERS
Full Name: \\CORPFS02\SHARE\FINANCE\CONTROLLERS

Review only objects that have changed since your last review ?
 Review only actionable objects

View: Users' effective permissions

Status	User	Group	Permission	Decision And Explanation
	Anne Thornton (CORP)	NTFS-Contro... (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Erin Manning (CORP)	NTFS-Contro... (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Marqaret Coakley (CORP)	NTFS-Contro... (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Maria Hirasaki (CORP)	NTFS-Contro... (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Michael Federle (CORP)	NTFS-Contro... (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	Nathan Sonneborn (CORP)	NTFS-Contro... (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove

Total: 6 Records
No. Of Rows: 7

Reason: Grund

Authorizers:

Name	Role
Erin Manning	Dir. Owner

Total: 1 Record
No. Of Rows: 3

I confirm that I have reviewed the objects listed above, along with their content.
Type the word 'Verify'. | Verify

Data last synchronized with environment: May 14, 2011 11:32:35 AM

Sign Cancel

Zusammenfassung

Bei der heutigen Wirtschaftslage sind die Daten eines Unternehmens das Kapital. Mit den wachsenden IT-Prozessen im Bereich Datenverwaltung wurde es meistens versäumt, die Gegebenheiten den dynamisch wachsenden Daten anzugleichen. Die aktuell genutzten Verfahren und Prozesse sind Zeit raubend und unproduktiv. Eine Momentaufnahme ist oft schon nach wenigen Stunden hinfällig, da es bereits in diesem Zeitraum zu Änderungen kommen kann.

Varonis DatAdvantage bietet innovative Ansätze und neue Wege, um diese Aufgaben erfolgreich lösen zu können. Durch die Verbindung von Benutzerverwaltung (Benutzer & Gruppen) und den File-Systemen einer Organisation in einer zentralen Management-Konsole erfolgt ein erheblicher Mehrwert in Bezug auf Daten- und Berechtigungsmanagement.

Nicht zuletzt sind Transparenz und Nachvollziehbarkeit unerlässliche Bedingungen/ Anforderungen in den heutigen Unternehmen.

Fragen wie:

- Wer hat Zugriff auf welche Daten?
- Wer greift auf welche Daten zu?
- Wer sollte wo Zugriff haben?
- Wer hat Daten gelöscht/verschoben/umbenannt?

werden einfach und schnell beantwortet. Die IT Abteilungen bekommen und behalten den Überblick über die Daten- und Berechtigungsstrukturen und somit wird die Sicherheit von Unternehmensdaten drastisch erhöht.

Unterstützte Plattformen

Plattform	DATADVANTAGE	DATAPRIVILEGE	Protokolle
Windows Server	X	X	NTFS
SharePoint Server	X		SharePoint Datenbank
Exchange Server	X		Exchange Datenbank
Unix Server	X		NFS
IBM AIX	X		NFS
NetApp	X	X (NTFS)	NTFS & NFS
EMC	X	X (NTFS)	NTFS & NFS
BlueArc	X	X (NTFS)	NTFS & NFS

Event Übersicht

EVENTS File Systeme & SharePoint

object open	files
object created	file, folder
object modified	file, folder
object renamed	file, folder
object deleted	file, folder
object permission changed	file, folder, site

EVENTS Exchange

object open	messages, public folders
object create	messages, public folders
object delete	messages, public folders
object rename/move/copy	messages, public folders
object set security/add delegate	public folders
object modify	messages
object send / receive	messages
object send as	messages
object send on behalf	messages
object mark read/unread	messages
object set properties	messages
object attachment open/delete	messages

Anforderungen an eine Testinstallation

- VMWare oder Hardware mit mindestens 100 GB HDD (20 GB C / 80 GB D)
- 6-8 GB Arbeitsspeicher
- Windows 2003 Server SP2 (IIS & ASP.net installiert) **ODER** Windows 2008 Server [auch R2] / aktuell gepatcht
- .net 2.0, 3.0 und 3.5 SP1 Framework installiert / aktuell gepatcht
- Microsoft SQL2005 SP3 / Microsoft SQL 2008 [auch R2] / **STANDART oder ENTERPRISE / KEINE EXPRESS** / aktuell gepatcht – **Der SQL Server muss auf dem Applikationsserver installiert sein (hierzu gibt es eine Installationsanleitung unter folgendem Link als Download <https://varonis.box.net/shared/a4mpvok8zk>)**
- Der Server benötigt einmalig Internetzugriff bezüglich der Lizenz Registrierung
- DCOM Service muss aktiv sein
- Windows Firewall muss aus sein
- Erweiterte IE Sicherheitseinstellungen müssen deaktiviert sein
- Benutzerkontensteuerung abschalten
- Muss ein Domain Member Server sein
- NetBIOS muss aktiv sein
- Server darf nicht VARONIS heissen

Weitere wichtige Informationen:

- Domänen Account mit lokalen administrativen Rechten für den Filern muss bereitgehalten werden
- LDAP Account zur LDAP Abfrage am Active Directory

- Wenn Sie EMC oder NetApp im Einsatz haben, dann melden Sie sich bitte vorab, damit die verschiedenen Anbindungsmöglichkeiten durchgesprochen werden können.