8MATE FS Logga Handbuch

Version 8.0

Haftungsausschluss

Die in diesem Dokument gemachten Angaben können sich jederzeit ohne vorherige Ankündigung ändern und gelten als nicht rechtsverbindlich.

Die beschriebene Software 8MAN wird von Protected Networks im Rahmen einer Nutzungsvereinbarung zur Verfügung gestellt und darf nur in Übereinstimmung mit dieser Vereinbarung eingesetzt werden.

Dieses Dokument darf ohne die vorherige schriftliche Erlaubnis von Protected Networks weder ganz noch teilweise in irgendeiner Form reproduziert, übermittelt oder übersetzt werden, sei es elektronisch, mechanisch, manuell oder optisch.

Dieses Dokument ist in einer Einheit zu denen auf der Website von Protected Networks veröffentlichten rechtlichen Hinweisen AGB, EULA und der Datenschutzerklärung zu sehen.

Urheberrecht

Protected Networks GmbH
Alt-Moabit 73
10555 Berlin

+49 30 390 63 45 - 0
www.protected-networks.com

Support

+49 30 390 63 45 – 99
helpdesk@8man.com
https://susi.8man.com

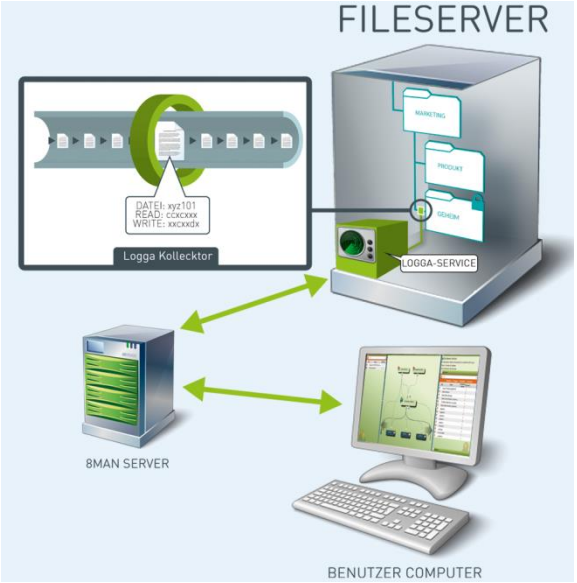
8MATE FS Logga - Überwachung von Fileservern

Mit dem FS Logga können Sie Verzeichnis- und Dateiaktionen auf Windows, NetApp und EMC Fileservern überwachen. (Es werden nicht alle Betriebssystemversionen und Produktvarianten unterstützt. Die konkreten Einschränkungen finden Sie im Dokument „8MAN Systemanforderungen“.)

Folgende Aktionen können mit dem Zeitpunkt der Aktion, dem Typ der Aktion und dem Benutzer, der die Aktion vorgenommen hat, aufgezeichnet werden:

- Datei gelesen
- Datei geschrieben
- Datei oder Verzeichnis erzeugt
- Datei oder Verzeichnis gelöscht
- Datei/Verzeichnis verschoben oder umbenannt
- ACL geändert
- ACL gelesen (standardmäßig ausgeschaltet [Aktivierung in der **pnTracer.config.xml**-Datei möglich] und für NetApp sowie EMC Fileserver nicht verfügbar)

Die aufgezeichneten Daten werden in die Datenbank des 8MAN Servers übertragen und können als Report im CSV oder XPS-Format ausgegeben werden.



1 Installation und Konfiguration der Kollektoren

Für den FS Logga müssen Kollektoren installiert werden. Kollektoren-für-den-FS-Logga-für-Windows-Fileserver haben zusätzliche Einschränkungen. Bitte überprüfen Sie diese im Dokument „8MAN Systemanforderungen“, bevor Sie die Kollektoren für den FS Logga für Windows-Fileserver installieren.

1.1 FS Logga für Windows-Fileserver

Der Kollektor für den FS Logga für Windows-Fileserver muss auf dem zu überwachenden Fileserver installiert werden (weitere Informationen im Dokument „8MAN Installation und Konfiguration“). Dafür müssen Sie bei der Installation den FS Logga für Windows File Server wählen:

Wenn der Kollektor **ohne** FS Logga für Windows File Server installiert wurde und dann **nachträglich** der FS Logga für Windows File Server installiert wird, dann muß der 8MAN Service auf dem Kollektor neu gestartet werden.

Sollen Fileserver auf **Windows Failover Clustern** überwacht werden, dann muss auf allen Nodes des Clusters der Kollektor mit FS Logga für Windows File Server installiert werden.

Wartung bei überwachten Windows Fileservern:
Beim Austausch von Festplatten oder beim Einbinden anderer Festplatten (Einrichten von Volume Mount Points) auf zu überwachende Festplattenbereiche muss der FS-Logga ausgeschaltet werden (ON/OFF-Button in der 8MAN Scan-Konfiguration) und nach der Änderung wieder eingeschaltet werden.

1.2 FS Logga für NetApp-Fileserver

Der Kollektor für den FS Logga für NetApp-Fileserver kann nicht auf den zu überwachenden NetApp Fileserver installiert werden. Er muss auf einem Windows Server installiert werden. NetApp empfiehlt dringend einen Server aus demselben Netzsegment zu wählen, da es sonst zu Performance- und Routingproblemen kommen kann.
Der FS Logga für NetApp Fileserver benötigt keinen Treiber (Gegensatz: der FS Logga für Windows Fileserver benötigt einen Treiber). Daher müssen Sie nur einen 8MAN Kollektor installieren (Ist bereits ein 8MAN Kollektor oder ein Kollektor-für-den-FS-Logga-für-Windows-Fileserver installiert, dann ist auch der Kollektor-für-den-FS-Logga-für-NetApp-Fileserver installiert):

Bei der Anmeldung eines NetApp Fileservers im Active Directory wird als eine Eigenschaft auch das Betriebssystem eingetragen. Dieses wird vom Kollektor verwendet, um Fileserver vom Type NetApp zu erkennen und entsprechend bei der Einrichtung eines FS Logga als solchen zu kennzeichnen. In der Kollektor Konfigurations-Datei ist standardmäßig der Type „OnTap“ und „NetApp“ konfiguriert. Wenn in Ihrem System die NetApp Fileserver andere Werte für das Attribut "operatingSystem" haben, können Sie die Kollektor-Suchwerte anpassen. Dazu öffnen Sie auf dem Server, auf dem der Kollektor installiert ist, die **pnCollector.config.xml**-Datei unter C:\ProgramData\protected-networks.com\8MAN\cfg (wenn nicht vorhanden aus C:\Programme \protected-networks.com\8MAN\etc kopieren, den Inhalt löschen und die folgenden Zeilen einfügen):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <netapp>
     <NetappOperatingSystems>OnTap,NetApp</NetappOperatingSystems>
    </netapp>
  </tracer>
</config>
```

Wenn mehrere Werte für das Attribut "operatingSystem" vorhanden sind, tragen Sie diese einfach mit Komma getrennt ein. Haben nicht alle oder gar kein Fileserver einen Wert für das Attribut „operatingSystem“, so lassen Sie diesen Eintrag leer:

```
<NetappOperatingSystems></NetappOperatingSystems>
```

Bei einem leeren Eintrag werden sämtliche mit der verwendeten Active Directory Anmeldung 'sichtbaren' Fileserver aufgelistet.

1.2.1 NetApp 7-Mode

Für den Kollektor-für-den-FS-Logga-für-NetApp-Fileserver für NetApp 7-Mode sind zusätzliche Einstellungen notwendig, um die Kommunikation zwischen NetApp und Kollektor zu gewährleisten.
Folgende lokale Computer-Richtlinien des Computers, auf dem der Kollektor-für-den-FS-Logga-für-NetApp-Fileserver läuft, sind notwendig (unter Richtlinien für Lokaler Computer\Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen):

Richtlinie	Einstellung
Netzwerkzugriff: Die Verwendung von „Jeder"-Berechtigungen für anonyme Benutzer ermöglichen	Aktiviert
Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann	ntapfprq_<netapp name> (<netapp name> ist der Name des NetApp Fileservers)

Hinweis:
Auf einem 8MAN-Kollektor kann jeweils nur eine 7-Mode NetApp konfiguriert werden. Für jede 7-Mode NetApp wird ein eigener Kollektor benötigt.

1.2.2 NetApp Clustered Data ONTAP

Für den Kollektor-für-den-FS-Logga-für-NetApp-Fileserver für NetApp Clustered Data ONTAP sind keine weiteren Einstellungen notwendig, wenn die Datenübertragung zwischen Kollektor und NetApp unverschlüsselt erfolgen soll.

Haben Sie jedoch verschlüsselte Übertragung konfiguriert (siehe Kapitel 2.2.2.1.2 „Erstellen der External Engine Konfiguration") so muss auf dem Kollektor die pnTracer.config.xml Konfigurationsdatei angepasst werden. Für jeden Fileserver (CIFS-Server der NetApp) der auf diesem Kollektor überwacht werden soll, ist folgender Eintrag unter <tracer><netapp><ssl><cifsServers> hinzuzufügen:

<**name of cifs server**>
    <switchOn type="System.Boolean">**true**</switchOn>
    <protocol type="System.Int32">5</protocol>
    <serverCertificateName>**name of certificate from certificate store to use**</serverCertificateName>
</**name of cifs server**>

Das Zertifikat wird dann im dem Zertifikatsspeicher des Computers gesucht.

Für <protocol> sind folgende Werte möglich: TLS = 1, TLS1.1 = 2, TLS1.2 = 3, SSL2 = 4, SSL3 = 5. Default is SSL3 (5). Wählen Sie ein Protokoll, welches sowohl auf dem Kollektor als auch auf der NetApp verfügbar ist.

1.3 FS Logga für EMC-Fileserver

Der Kollektor für den FS Logga für EMC-Fileserver kann nicht auf dem zu überwachenden EMC Fileserver installiert werden. Er muss auf einem Windows Server installiert werden, bevorzugt auf jenem, auf dem auch der EMC Common Event Enabler (CEE) installiert ist (zu CEE siehe Kapitel 2.3.12.3.1). EMC empfiehlt dringend einen Server aus demselben Netzsegment zu wählen, da es sonst zu Performance- und Routingproblemen kommen kann.
Der FS Logga für EMC Fileserver benötigt keine Treiber oder Agents auf dem EMC-Fileserver selbst. Daher müssen Sie nur einen 8MAN Kollektor installieren:

Bei der Anmeldung eines EMC Fileservers im Active Directory wird als eine Eigenschaft auch das Betriebssystem eingetragen. Dieses wird vom Kollektor verwendet, um Fileserver vom Type EMC zu erkennen und entsprechend bei der Einrichtung eines FS Logga als solchen zu kennzeichnen. In der Kollektor Konfigurations-Datei sind standardmäßig zwei Typen von EMC Fileserver Betriebssystemen gesetzt: „EMC File Server“ und „EMC Celerra File Server“.
Wenn in Ihrem System die EMC Fileserver andere Werte für das Attribut "operatingSystem" haben, können Sie die Kollektor-Suchwerte anpassen. Dazu öffnen Sie auf dem Fileserver mit dem installierten Kollektor die **pnCollector.config.xml**-Datei unter C:\ProgramData\protected-networks.com\8MAN\cfg (wenn nicht vorhanden aus C:\Programme \protected-networks.com\8MAN\etc kopieren, den Inhalt löschen und die folgenden Zeilen einfügen):

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <emc>
      <EmcOperatingSystems>EMC File Server,EMC Celerra File Server</EmcOperatingSystems>
    </emc>
  </tracer>
</config>
```

Wenn mehrere Werte für das Attribut "operatingSystem" vorhanden sind, tragen Sie diese einfach mit Komma getrennt ein. Haben nicht alle oder gar kein Fileserver einen Wert für das Attribut „operatingSystem“, so lassen Sie diesen Eintrag leer:

```
<EmcOperatingSystems></EmcOperatingSystems>
```

Bei einem leeren Eintrag werden sämtliche mit der verwendeten Active Directory Anmeldung 'sichtbaren' Fileserver aufgelistet.

2 Konfiguration der zu überwachenden Fileserver

2.1 Windows-Fileserver

Es ist keine spezielle Konfiguration für den zu überwachen Fileserver notwendig.

2.2 NetApp-Fileserver

Neben der Konfiguration des Kollektors ist auch eine Konfiguration der zu überwachenden NetApp erforderlich, um die Aufzeichnungen zu ermöglichen.

2.2.1 NetApp 7-Mode

2.2.1.1 FPolicy Feature

Der FS-Logga für NetApp Fileserver nutzt das FPolicy Feature der NetApp. Deshalb muss es auf der NetApp aktiviert und passend eingestellt werden.

Aktivierung des FPolicy Features:

```
> options fpolicy.enable on
```

Einrichten der FPolicy:

```
> fpolicy create 8ManLogga screen
> fpolicy enable 8ManLogga
> fpolicy options 8ManLogga cifs_setattr on
```

Der Wert „8ManLogga" der FPolicy muss mit dem Wert in der Konfigurationsdatei **pnTracer.config.xml** auf dem Computer mit dem installierten Kollektor-für-den-FS-Logga-für-NetApp-Fileserver (C:\Programme \protected-networks.com\8MAN\etc) übereinstimmen. „8ManLogga" ist der Default nach der Installation:

```
<?xml version="1.0" encoding="utf-8"?>
<config>
  <tracer>
    <netapp>
      <policy>8ManLogga</policy>
    </netapp>
  </tracer>
</config>
```

2.2.1.2 Domänen-Konten

Zur Registrierung des FS Logga-für-NetApp-Fileserver an dem NetApp Fileserver muss der Logga zu einem Konto gehören, das Mitglied in der Gruppe "Backup Operators" auf dem NetApp Fileserver ist. Da der Logga zu dem Computerkonto des Fileservers gehört, auf dem er gestartet wurde, muss das Computerkonto zu dieser NetApp-Gruppe hinzugefügt werden:

```
>useradmin domainuser add <domain\computer-account> -g "Backup Operators"
```

Um die Freigaben mit den kompletten Pfaden lesen zu können wird ein Benutzerkonto gebraucht, das zur Gruppe "Power Users" auf dem NetApp Fileserver gehört (mit dieser Anmeldung sollte der Logga kinfiguriert sein).

```
>useradmin domainuser add <domain\user> -g "Power Users"
```

2.2.2 NetApp Clustered Data ONTAP

2.2.2.1 FPolicy Feature

Der FS-Logga für NetApp Fileserver nutzt das FPolicy Feature der NetApp. Deshalb muss diese Feature auf der NetApp über die CLI entsprechend konfiguriert und aktiviert werden.
Um diese Konfiguration durchführen zu können, muss die dafür benutzte Anmeldung die Rolle admin oder vsadmin haben.

In allen folgenden CLI Kommandos ist der Parameter „<vserver_name>“ in den Namen der SVM (Storage Virtual Machine) zu ändern, auf der der zu überwachende CIFS-Server konfiguriert ist.

2.2.2.1.1 Erstellen der Event Konfiguration

Mit der Event Konfiguration werden die vom Logga benötigten Ereignisse, die auszufilternden Ereignisse und das Protokoll (der Logga unterstützt nur das CIFS-Protokoll) festgelegt. Bitte ändern Sie im folgenden Kommando nur den Parameter <vserver_name>. Änderungen an den anderen Parametern führen zu fehlenden Ereignissen in den Reporten und/oder zu erhöhter Last von NetApp und Kollektor, weil nicht benötigte Ereigisse verarbeitet werden.

```
> fpolicy policy event create -vserver <vserver_name> -event-name event_8manlogga_cifs -file-
operations create, create_dir, delete, delete_dir, read, write, rename, rename_dir, setattr, open -
protocol cifs -filters first-read, first-write, open-with-delete-intent
```

Mit dem folgenden Kommando können Sie prüfen, ob diese Einstellung übernommen wurde:

```
> fpolicy policy event show
```

2.2.2.1.2 Erstellen der External Engine Konfiguration

Die External Engine Konfiguration legt fest, an welchen Server (definiert über Port und IP-Adresse) die Ereignisse gesendet werden sollen. Hier muss eine IP-Adresse angegeben werden, über die die NetApp den Kollektor erreichen kann, auf dem der Logga laufen soll. Der angegebene Port muss auf dem Kollektor noch frei sein.

```
> fpolicy policy external-engine create -vserver <vserver_name> -engine-name engine_8manlogga -
primary-servers <collector-ip> -port 2002 -extern-engine-type asynchronous -ssl-option <ssl-option>
```

Für <ssl-option> werden die Werte „no-auth“ und „server-auth“ unterstützt, wobei „no-auth“ bedeutet, dass die Ereigisdaten von der NetApp zum Logga unverschlüsselt übertragen werden.
Sollen die Daten verschlüsselt übertragen werden, so wählen Sie „server-auth“. In diesem Fall sind zusätzliche Konfigurationen auf dem Kollektor als auch auf der NetApp notwendig. Diese sind in Kapitel 1.2.2 und 2.2.2.4 beschrieben.

Mit dem folgenden Kommando können Sie prüfen, ob die External Engine Einstellung übernommen wurde:

```
> fpolicy policy external-engine show
```

2.2.2.1.3 Erstellen der FPolicy Konfiguration

Die FPolicy Konfiguration führt die Event- und die External Engine Konfiguration zusammen.

```
> fpolicy policy create -vserver <vserver_name> -policy-name 8manlogga -events event_8manlogga_cifs -
engine engine_8manlogga -is-mandatory false
```

Mit dem folgenden Kommando können Sie prüfen, ob diese Einstellung übernommen wurde:

```
> fpolicy policy show
```

2.2.2.1.4 Erstellen des Scopes für die FPolicy

Der Scope definiert die Volumes und damit die Shares und deren Unterverzeichnisse und enthaltenen Dateien, für die die Ereignisse an den Logga gemeldet werden sollen. Wenn nur bestimmte Shares auf bestimmten Volumes zu überwachen sind, empfehlen wir, statt der Wildcard ("*") eine Komma-separierte Liste dieser Volumes anzugeben, um die Last für den NetApp Fileserver und den Kollektor zu reduzieren.

```
> fpolicy policy scope create -vserver <vserver_name> -policy-name 8manlogga -volumes-to-include "*"
```

Mit dem folgenden Kommando können Sie prüfen, ob der Scope erstellt wurde:

```
> fpolicy policy scope show
```

2.2.2.1.5 FPolicy aktivieren

Wenn alle vorherigen FPolicy Konfigurationen erfolgreich waren, kann die FPolicy aktiviert werden.
Die Sequence-Number muss immer angeben werden (auch wenn es nur eine FPolicy gibt). Sie legt fest, in welcher Reihenfolge die Fpolicies abgearbeitet werden.

```
> fpolicy enable -vserver <vserver_name> -policy-name 8manlogga -sequence-number 1
```

Mit dem folgenden Kommando können Sie prüfen, ob die FPolicy aktiviert wurde:

```
> fpolicy show-enabled
```

2.2.2.2 Domänen-Konten

Um die Freigaben mit den kompletten Pfaden lesen zu können wird ein Benutzerkonto gebraucht, das zur Gruppe "Power Users" auf dem NetApp Fileserver gehört (mit dieser Anmeldung sollte der Logga konfiguriert sein).

```
> vserver cifs users-and-groups local-group add-members -vserver <vserver_name> -group-name
"BUILTIN\Power Users" -member-names <domain\user>
```

Der Logga nutzt das ONTAP API, um FPolicy Daten bei der NetApp auszulesen und sich anzumelden. Dafür nutzt er ein Konto, für das eingeschränkte Berechtigungen eingestellt werden sollten, was über das Einrichten einer Rolle auf der NetApp erfolgt.

In allen folgenden CLI Kommandos ist der Parameter „<vserver_name>“ in den Namen der SVM zu ändern, auf der der zu überwachende CIFS-Server konfiguriert ist.

```
> security login role create -role 8manrole -vserver <vserver_name> -cmd "vserver fpolicy"
> security login role create -role 8manrole -vserver <vserver_name> -cmd "volume" -access readonly
> security login role create -role 8manrole -vserver <vserver_name> -cmd "vserver" -access readonly
> security login role create -role 8manrole -vserver <vserver_name> -cmd "version" -access readonly
```

Mit dem folgenden Kommando können Sie prüfen, ob die Rolle entsprechend eingerichtet wurde:

```
> security login role show -role 8manrole
```

Das durch den Logga zu nutzende Konto wird nun der Rolle zugewiesen:

```
> security login create -username <domain\username> -application ontapi -authmethod domain -role
8manrole -vserver <vserver_name>
```

Mit dem folgenden Kommando können Sie prüfen, ob das Konto entsprechend zugewiesen wurde:

```
> security login show
```

2.2.2.3 Firewall Anpassungen

Der Logga nutzt das ONTAP API via https, um das Logging bei der SVM zu starten. Dazu muss auf einem LIF (Logical Interface) der SVM der Service https freigegeben sein. Diese LIF muss vom 8MAN-Kollektor, auf dem der Logga gestartet wird, erreichbar sein.
Welcher Service auf welcher SVM über welche Firewall Policy freigegeben ist, können Sie mit folgendem Kommando prüfen:

```
> system service firewall policy show
```

Die Zuordnung der Firewall Policies zu den LIF’s auf der SVM finden Sie mit diesem Kommando heraus:

```
> network interface show -vserver <vserver_name> -fields firewall-policy
```

Wenn auf einem LIF der SVM bereits eine Firewall Policy mit Service https aktiv ist, müsse Sie gegebenenfalls nur noch die ‘allow-list’ anpassen:

```
> system services firewall policy modify -vserver <vserver_name> -policy <current_firewall_policy> -
service https -allow-list <collector-ip/32>
```

Ist die Änderung der aktiven Firewall Policy nicht erwünscht/sinnvoll, weil es z.B. eine Default Policy ist, dann können Sie diese zuerst kopieren und dann die Änderung an der Kopie vornehmen und dann dem gewünschten LIF zuweisen:

```
> system services firewall policy clone -vserver <vserver_name> -policy <current_firewall_policy> -
destination-policy 8manlogga_fp

> system services firewall policy modify -vserver <vserver_name> -policy 8manlogga_fp -service https
-allow-list <collector-ip/32>

> network interface modify -vserver <vserver_name> -lif <lif> -firewall-policy 8manlogga_fp
```

Wobei <current_firewall_policy> die für das LIF von <vserver_name> aktive Firewall Policy ist und <collector-ip> die schon in Kapitel 2.2.2.1.2 „Erstellen der External Engine Konfiguration“ verwendete IP-Adresse des Kollektors ist.

2.2.2.4 Zertifikate Einstellung für verschlüsselte Ereignisübertragung

Wenn Sie konfiguriert haben, dass die Ereignisübertragung zwischen NetApp und Logga verschlüsselt erfolgen soll (siehe 2.2.2.1.2 „Erstellen der External Engine Konfiguration“) dann muss ein entsprechendes CA Zertifikat auf der NetApp installiert werden, mit dem die NetApp das Server-Zertifikat verifizieren kann (hierbei ist der 8MAN-Kollektor der Server, der sich mit Zertifikat auhentifizieren muss, siehe Kapitel 1.2.2).

```
> security certificate install -vserver <vserver_name> -type client-ca
```

Mit folgendem Kommando können Sie überprüfen, ob das Zertikat installiert wurde:

```
> security certificate show
```

2.3 EMC-Fileserver

Um das Monitoring zu ermöglichen ist neben der Konfiguration der zu überwachenden EMC die Installation der EMC spezifischen Anwendungssoftware “Common Event Enabler” (CEE) für Windows erforderlich.

2.3.1 EMC Common Event Enabler (CEE)

2.3.1.1 Installation des CEE

Die Überwachung von EMC Fileservern benötigt die Installation der EMC spezifischen Anwendungssoftware “Common Event Enabler” (CEE) für Windows. Dieser kann in der jeweilig aktuellen Version von den EMC Support Seiten geladen werden. Die weiteren maschinenspezifischen Installationsschritte können aus den zu Ihrer Version dazugehörigen Anwendungshandbüchern entnommen werden. Diese sind zu finden unter https://community.emc.com.

2.3.1.2 8MAN spezifische Anpassung des CEE

Für die effiziente Verbindung zwischen dem 8MAN Kollektor und dem CEE Framework sollten beide Komponenten auf einem Server laufen.
Die Verbindung von 8MAN Kollektor und CEE wird durch eine Änderung in den CEE Windows Registry Einträgen gesteuert. Unter dem Registrierungspunkt „[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP]“ müssen folgende Einträge angepasst, beziehungsweise erzeugt werden:

[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] Enabled=(REG_DWORD) 0x00000001

Für eine lokale Verarbeitung der Daten wird folgender Endpoint Eintrag vorgenommen:
[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint=(REG_SZ) "pnTracer"

Für Änderungen benötigen Sie Admin-Schreibrechte. Nach erfolgtem Eintrag muss der Service neu gestartet werden um die Änderungen zu übernehmen. Das kann mittels der grafischen Service Management Konsole oder dem Kommandozeilenaufruf „net [start|stop] „emc cava“ erfolgen.

2.3.2 Konfiguration der EMC

Der Common Event Enabler (siehe 2.3.1) muss der EMC bekannt gemacht werden, damit diese die Dateizugriffe an diesen weiterleiten kann. Wir empfehlen, den Common Event Enabler (CEE) zu installieren und zu starten und dann die EMC zu konfigurieren. Dann kann gleich nachgeprüft werden, ob die EMC Verbindung mit dem CEE auch zustande gekommen ist.

2.3.2.1 Erstellen / Editieren der cepp.conf Datei

- Erstellen / editieren Sie die Datei cepp.conf auf der EMC:
  $ vi cepp.conf
- Konfiguration eingeben:
  cifsserver=
  surveytime=10

ft level=0
msrpcuser=<Account unter dem der CEE Service läuft>
pool name=8manpool \
servers=<IP Addresse oder FQDN des Windows Servers auf dem der CEE Service läuft> \
postevents=* \
option=ignore \
reqtimeout=1000 \
retrytimeout=500

- Kopieren Sie diese Datei ins Root-Verzeichnis des Data Movers:
  $ server_file <movername> -put cepp.conf cepp.conf

2.3.2.2 Administration der Rechte des CEE Accounts

Zur Verifikation des CEE Accounts (eingerichtet während der CEE Installation) ist auf der EMC dieser Account entsprechend zu administrieren (Installation des MMC Snap-in ist im EMC Dokument „Installing Management Applications on VNX for File“ beschrieben). Führen Sie folgende Schritte aus (original Text aus dem Dokument https://www.emc.com/collateral/TechnicalDocument/docu48055.pdf):

1. Click Start and select Settings > Control Panel > Administrative Tools > EMC VNX File CIFS Management. The EMC VNX File CIFS Management window appears.
2. Perform one of the following:
   a. If a Data Mover is already selected (name appears after Data Mover Management), go to step 4.
   b. If a Data Mover is not selected:
      – Right-click Data Mover Management and select Connect to Data Mover.
      – In the Select Data Mover dialog box, select a Data Mover by using one of the following methods:
         i. In the Look in: list box, select the domain in which the Data Mover that youwant to manage is located and select the Data Mover from the list.
            Or
         ii. In the Name box, type the computer name, IP address, or the NetBIOS name of the Data Mover.
3. Double-click Data Mover Management, and double-click Data Mover Security Settings.
4. Click User Rights Assignment. The assignable rights appear in the right pane.
5. Double-click EMC Event Notification Bypass. The Security Policy Setting dialog box appears.
6. Click Add. The Select Users or Groups dialog box appears.
7. If necessary, choose the server from the Look in drop-down list. Select the user from the list box.
8. Click Add, and then click OK to close the Select Users or Groups dialog box.
9. Click OK to close the Security Policy Setting dialog box.
10. In the User Rights Assignment list, double-click EMC Virus Checking. The Security Policy Setting dialog box appears.
11. Click Add. The Select Users or Groups window appears.
12. If necessary, choose the server from the Look in drop-down list. Select the user from the list box.
13. Click Add, and then click OK to close the Select Users or Groups dialog box.
14. Click OK to close the Security Policy Setting dialog box.
15. Close the EMC VNX File CIFS Management window.

2.3.2.3 Starten des Common Event Publishing Agent (CEPA)

Der letzte Schritt ist das Starten des CEPA auf der EMC und die Überprüfung auf korrekte Ausführung:

- Starten
  $ server_cepp <movername> -service –start
  wobei:
  <movername> = Name des Data Mover
  Ergebnis:
  <movername> : done

- CEPA Status prüfen
  $ server_cepp <movername> -service –status
  Ergebnis:
  <movername>: CEPP Started

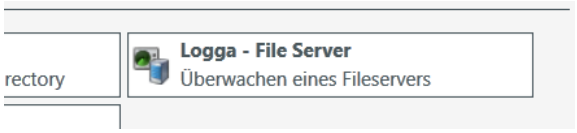
- Detaillierte Info:
  $ server_cepp <movername> -pool –info
  Ergebnis:
  <movername>:
  pool_name = <pool name>
  server_required = no
  access_checks_ignored = 0
  req_timeout = 500 ms
  retry_timeout = 50 ms
  pre_events =
  post_events = CreateFile,DeleteFile, RenameFile, FileRead…..
  post_err_events =
  CEPP Servers:
  *IP = <CEE IP>, state = **ONLINE**, vendor = Unknown*

3 FS Logga Konfiguration

Die Logga Konfiguration ist nur für 8MAN Administratoren nutzbar. Für die Logga Konfiguration ist eine Lizenz notwendig. Ob eine Lizenz vorhanden ist, können Sie in der 8MAN Konfiguration unter „Lizenz“ in den Lizenzinformationen-Bereich überprüfen. Die „Anzahl Fileserver Logga“ definiert wie viele Fileserver (egal ob Windows, EMC oder NetApp) Sie parallel überwachen können:

3.1 Fileserver und Kollektor auswählen

In der 8MAN Konfigurations-Ansicht „Scans“ können Sie über die Schaltfläche „Logga - Fileserver“ den Auswahldialog für den Fileserver und den Kollektor, der diesen Fileserver überwachen soll, öffnen:

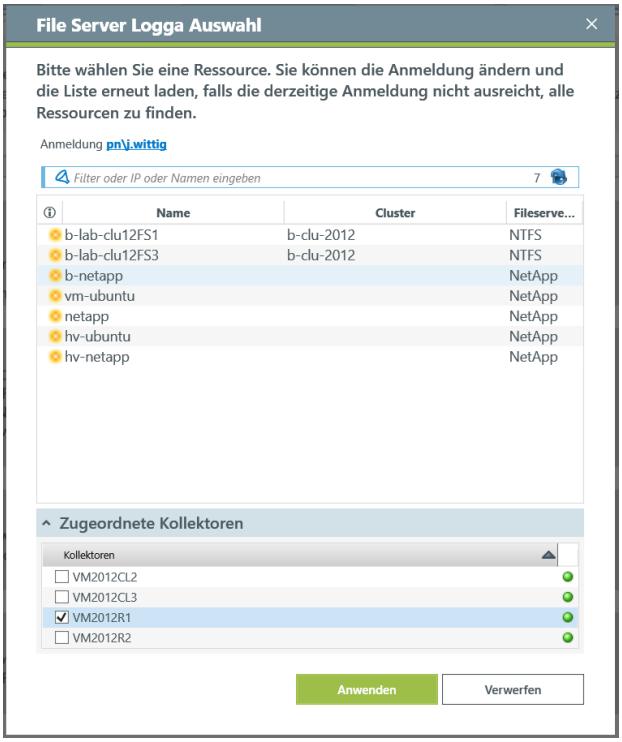


Im Logga-Auswahl-Dialog können Sie folgendes auswählen:

- die für die Fileserversuche zu verwendende Anmeldung (standardmäßig werden zum Lesen des Active Directory die Anmeldedaten aus der Basiskonfiguration übernommen)
- den zu überwachenden Fileserver
- die Kollektoren, die die Überwachung übernehmen sollen

3.1.1 Windows Fileserver, NetApp und EMC

Da die verfügbaren NetApp- und EMC- Fileserver aus dem Active Directory ausgelesen werden, benötigen Sie ein Benutzerkonto, das das entsprechende Active Directory auslesen darf.
Für die Auflistung der Windows Fileserver spielt die Anmeldung keine Rolle. Es werden nur die Windows Fileserver angezeigt, auf denen der FS Logga für Windows Fileserver installiert ist und deren Kollektoren eine aktive Verbindung zum 8MAN Server haben.



Für Windows Fileserver ist nur der Kollektor auf dem ausgewählten Fileserver selbst wählbar (für Windows Failover Cluster siehe 3.1.2).
Da NetApp und EMC Fileserver remote überwacht werden, können Sie, abhängig von Ihrer Installation, zwischen verschiedenen Kollektoren wählen. Pro Kollektor können mehrere NetApp bzw. EMC Fileserver überwacht werden und auch eine zusätzliche Auswahl als FS Logga für Windows Fileserver, AD Logga und als Fileserver- oder AD-Scanner ist möglich (wie viele Logga gleichzeitig auf einem Kollektor aktiv sein können hängt von der Leistungsfähigkeit des Servers ab, auf dem der Kollektor installiert ist und natürlich von dem Datenaufkommen, dass jeder einzelne Logga verarbeiten muss).

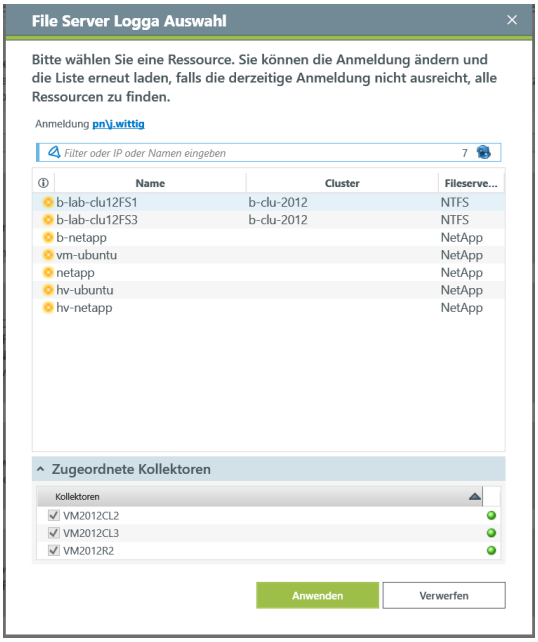
Hinweis:
Die Liste der Fileserver im Logga Auswahl Dialog enthält:

- Windows-Fileserver, auf denen der FS Logga für Windows Fileserver installiert ist und
- Fileserver, bei denen im Active Directory das Attribut "operatingSystem" mit bestimmten Werten gestezt ist. Der voreingestellte Suchwert des Kollektors für "operatingSystem" ist:
    - "OnTap" sowie „NetApp“ für NetApp Fileserver und
    - „EMC File Server“ sowie „EMC Celerra File Server“ für EMC Fileserver

Wenn in Ihrem System andere bzw. zusätzliche Werte für das Attribut "operatingSystem" für EMC oder NetApp Fileserver eingerichtet sind, können sie diese Werte in der **pnCollector.config.xml**-Datei anpassen. Die Anpassung ist beschrieben in den Kapiteln „FS Logga für NetApp-Fileserver“ und „FS Logga für EMC-Fileserver“.

3.1.2 Windows Failover Cluster

Wenn das Windows Failover Cluster Feature auf einem Fileserver aktiv ist, werden in der Auswahl der möglichen zu überwachenden Server statt des Computernamens des Fileservers die aktiven Dienste/Rollen vom Typ Fileserver angezeigt (Dienste in Windows 2008 und Rollen in Windows 2012).



In der Kollektorenübersicht sind alle Nodes des Failover Cluster als Kollektoren vorausgewählt. Diese Auswahl ist nicht änderbar, da für die lückenlose Überwachung einer Cluster-Ressource der Logga auf allen Nodes konfiguriert und aktiv sein muss.

Bitte überprüfen Sie, dass die Kollektoren der Cluster Nodes in der 8MAN Konfiguration über ihren Namen oder FQDN konfiguriert sind und nicht über die IP-Adresse (siehe 8MAN Installation und Konfiguration Handbuch, Kapitel Kollektorverbindung).

Die folgenden Voraussetzungen müssen für eine erfolgreiche Konfiguration der Überwachung von Dienste/Rollen auf Failover Clustern gegeben sein:

- Auf allen Nodes ist der 8MAN Kollektor installiert,
- auf allen Nodes ist der FS Logga für Windows Fileserver installiert,
- die Kollektoren auf diesen Nodes haben eine aktive Verbindung zum 8MAN Server.

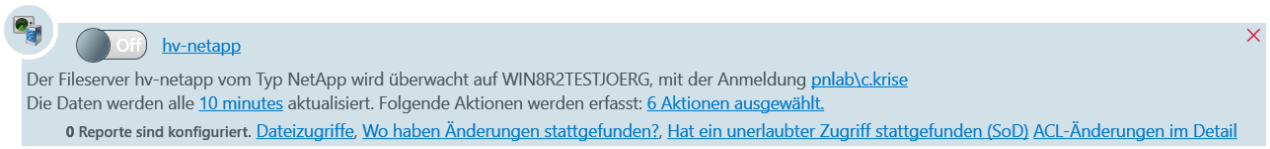
Ist für einen Node des Failover Clusters eine dieser Bedingungen nicht erfüllt, ist dieser Node in der Kollektorübersicht rot gekennzeichnet und die Logga-Konfiguration lässt sich nicht erstellen.

Werden nach bereits erfolgter Logga Konfiguration dem Cluster zusätzliche Nodes hinzugefügt, passt der 8MAN die Logga Konfiguration automatisch an und startet die Überwachung auf den hinzugefügten Nodes. Der automatische Start der Überwachung ist aber nur erfolgreich, wenn die oben schon genannten Voraussetzungen gegeben sind:

- Auf allen hinzugefügten Nodes ist der 8MAN Kollektor installiert,
- auf allen hinzugefügten Nodes ist der FS Logga für Windows Fileserver installiert,
- die Kollektoren auf diesen Nodes haben eine aktive Verbindung zum 8MAN Server.

3.2 Überwachte Aktionen und Datenaktualisierungsintervall

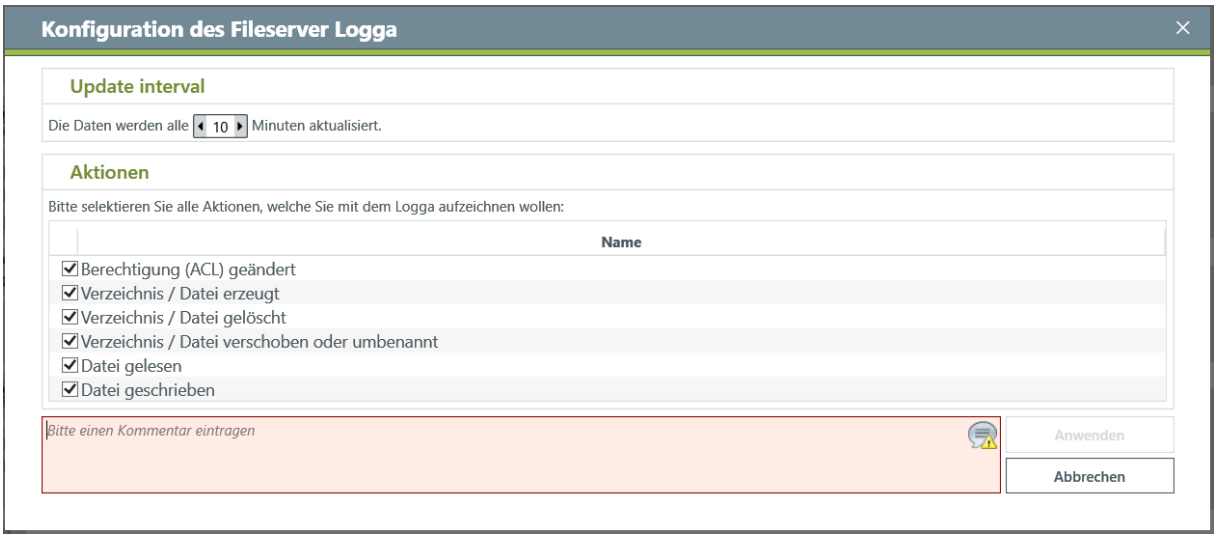
Wenn in der File Server Logga Auswahl ein Fileserver ausgewählt und der Anwenden Button gedrückt wurde, erscheint ein Logga-Konfigurations-Bubble:



Die FS-Logga-Konfigurations-Bubble besteht aus

- Der Aktivierung bzw. Deaktivierung des FS Logga:
  
- Dem (änderbaren) Namen dieser Konfiguration:
  hv-netapp
- Der (änderbaren) Anmeldung, mit der bei NetApp und EMC-Fileservern die Shares mit den zugehörigen lokalen Pfaden ausgelesen werden:
  Anmeldung pnlab\c.krise
  Dieses Konto muss zur Gruppe Power User auf diesem Fileserver gehören (siehe 2.2.1.2 bzw. 2.2.2.2).
- Der Konfiguration des Zeitintervalls, in dem der Logga die gesammelten Daten im 8MAN Server aktualisiert:
  Die Daten werden alle 10 minutes aktualisiert.
- Der Konfiguration der erfassten Aktionen:
  Folgende Aktionen werden erfasst: 6 Aktionen ausgewählt.
- Einer Auflistung der möglichen Reporttypen:
  Dateizugriffe, Wo haben Änderungen stattgefunden?, Hat ein unerlaubter Zugriff stattgefunden (SoD) ACL-Änderungen im Detail

Bei Click auf den Link für die Konfiguration des Datenaktualisierungsintervalls oder den Link für Konfiguration der zu erfassenden Aktionen erscheint folgender Dialog:

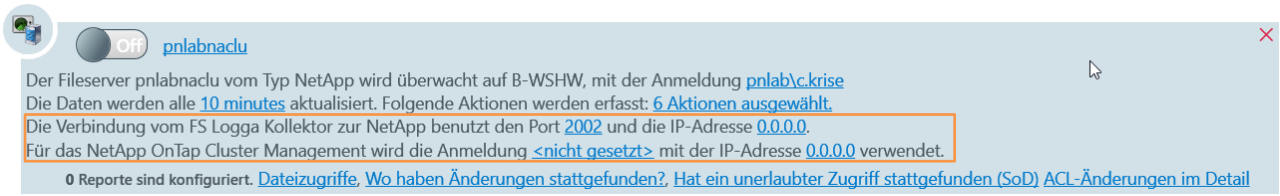


Hier kann das Datenaktualisierungsintervall zwischen 1 und 60 Minuten eingestellt werden und es kann eingestellt werden, welche Aktionen der Logga erfassen soll und welche nicht. Sie können hiermit durch Abwahl für Sie uninteressanter Aktionen den Datenbankspeicherverbrauch reduzieren.
Änderungen sind mit Kommentar zu bestätigen und werden im Logbuch gespeichert.

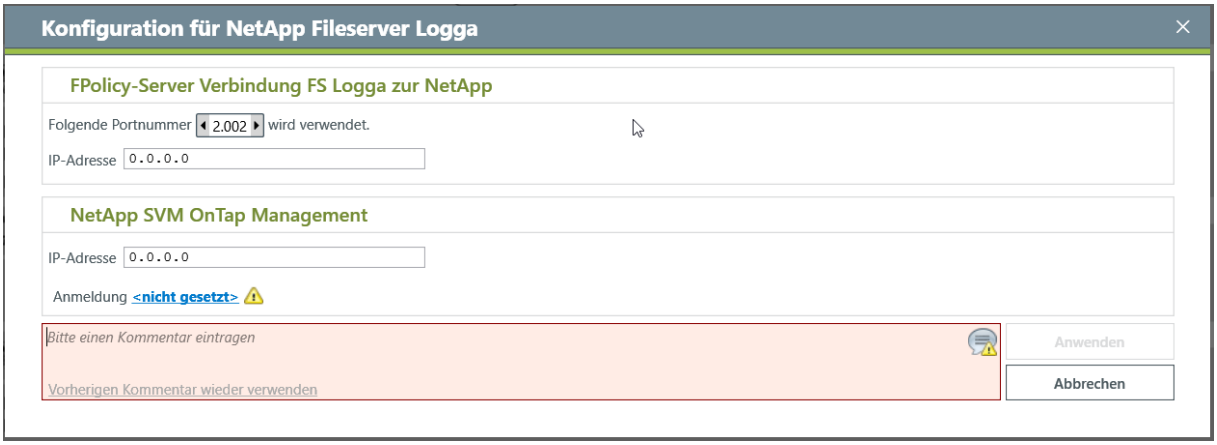
Hinweis:
Die Abwahl von Aktionen hat keinen Einfluss auf die Reporttypen „Wo haben Änderungen stattgefunden“ und „ACL-Änderung im Detail“. Diese Reporttypen erfassen nur dedizierte Aktionen. Haben Sie diese Aktionen abgewählt, wird 8MAN diese automatisch wieder aktivieren, um die Funktionalität der genannten Reporttypen zu sichern.

3.3 NetApp Clustered Data ONTAP Einstellungen

8MAN erkennt automatisch, wenn der ausgewählte Fileserver auf einer NetApp Clustered Data ONTAP läuft und fordert in diesem Falle Zusatzinformationen an.



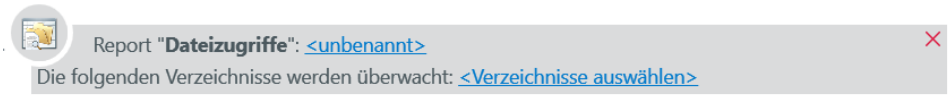
Wenn Sie auf einen dieser Links klicken, können Sie die Werte ändern:



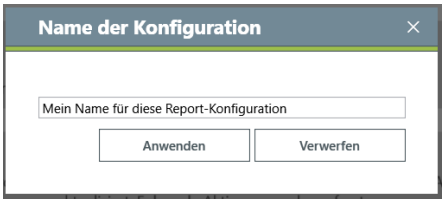
- **Fpolicy-Server Verbindung FS Logga zur NetApp:**
  Das ist eine IP-Adresse des Kollektors. Diese IP-Adresse und der Port müssen identisch sein mit den Werten, die Sie für die Konfiguration der External Engine auf der NetApp (siehe Kapitel 2.2.2.1.2 „Erstellen der External Engine Konfiguration“) verwenden. Auf dem ausgewählten Kollektor muss diese IP-Adressse verfügbar und der Port noch frei sein. Über diese Adresse empfängt der Logga auf dem Kollektor die Monitoring-Daten von der NetApp.
- **NetApp SVM OnTap Management:**
  Tragen Sie hier die IP-Adresse des LIF (Logical Interface) der SVM (Storage Virtual Machine) ein, in der der zu überwachende Fileserver läuft. Das zu wählende LIF muss mit den Einstellungen beschrieben in Kapitel 2.2.2.3 „Firewall Anpassungen“ übereinstimmen.
  Als Anmeldung geben Sie hier das Konto an, dem Sie gemäß Kapitel 2.2.2.2 „Domänen-Konten“ die Rolle „8manrole“ zugewiesen haben.

3.4 Namen und zu überwachende Verzeichnisse für die FS-Logga-Report-Konfigurationen auswählen

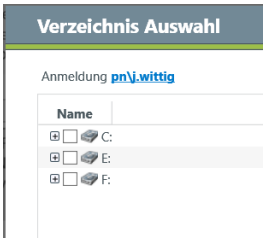
Bei Klick auf einen der Links in der Auflistung der Reporttypen erscheint ein neuer Reportkonfigurations-Bubble:



Für jede Report-Konfiguration können Sie bei Klick auf <unbenannt> einen Namen vergeben:



und bei Klick auf <Verzeichnisse auswählen> die zu überwachenden Verzeichnisse auswählen:



Für die Überwachung von Verzeichnissen auf NetApp Fileservern ist eine spezielle Berechtigung zur Ermittlung der lokalen Pfade notwendig. Ein Benutzerkonto das auf dem ausgewählten Fileserver zur Gruppe "BUILTIN\Power Users" gehört, hat diese Berechtigung (siehe 2.2.2.2 „**Domänen-Konten**“). Daher geben Sie im Verzeichnis-Auswahl-Dialog für NetApp Fileserver die Anmeldedaten eines solchen Benutzerkontos ein.

Sobald mindestens eine Report-Konfiguration mit mindestens einem oder mehreren Verzeichnissen erstellt wurde, kann der FS Logga eingeschaltet werden (siehe Kapitel 3.6).

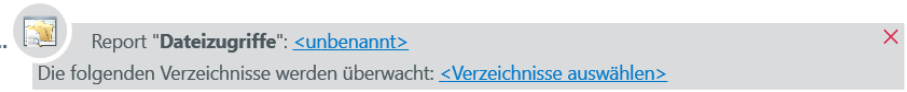
Hinweis:
Die Länge eines ausgewählten Verzeichnispfads darf 1960 Zeichen nicht überschreiten.
Die Summe aller in allen Report-Konfigurationen eines Fileservers ausgewählten Laufwerke/Verzeichnisse darf 512 nicht übersteigen

Die aufgezeichneten Daten werden in der 8MAN Datenbank standardmäßig für 30 Tage gespeichert und können solange für die Erstellung von Reporten verwendet werden. Sie können die Speicherdauer unter 8MAN Konfiguration → Server → Datenstandspeicherung anpassen (siehe Dokument „Installation und Konfiguration“).

Bitte beachten Sie, dass eine längere Speicherdauer einen größeren Speicherbedarf auf der 8MAN Datenbank bedeutet. Je aufgezeichneter Aktion werden 43 Byte benötigt.

3.5 Reporttypen

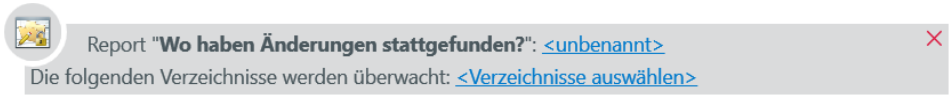
3.5.1 Dateizugriffe



Für die gewählten Verzeichnisse, Unterverzeichnisse und den dort enthaltenen Dateien werden folgende Aktionen aufgezeichnet:

- Datei gelesen
- Datei geschrieben
- Verzeichnis / Datei erzeugt
- Verzeichnis / Datei gelöscht
- Verzeichnis / Datei verschoben bzw. umbenannt
- ACL geändert
- ACL gelesen (standardmäßig ausgeschaltet [Aktivierung in der pnTracer.config.xml-Datei möglich] und für NetApp und EMC Fileserver nicht verfügbar)

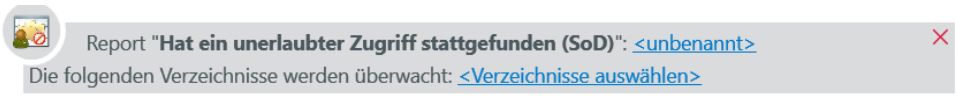
3.5.2 Wo haben Änderungen stattgefunden?



Für die gewählten Verzeichnisse, Unterverzeichnisse und den dort enthaltenen Dateien werden folgende Aktionen aufgezeichnet:

- Datei geschrieben
- ACL geändert

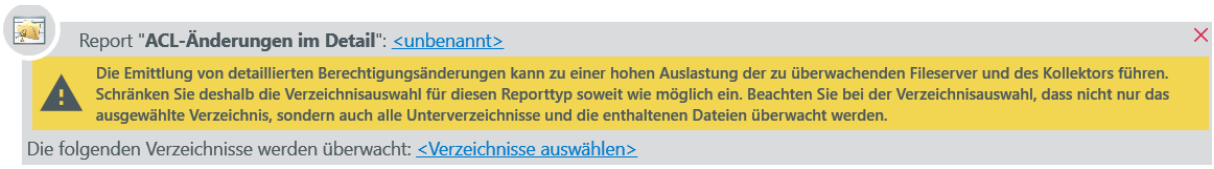
3.5.3 Hat ein unerlaubter Zugriff stattgefunden - Segregation of Duty (SoD)



Für die gewählten Verzeichnisse, Unterverzeichnisse und den dort enthaltenen Dateien werden folgende Aktionen aufgezeichnet (die Auswahl der erlaubten Benutzer und Gruppen erfolgt bei der Reporterstellung):

- Datei gelesen
- Datei geschrieben
- Verzeichnis / Datei erzeugt
- Verzeichnis /Datei gelöscht
- Verzeichnis / Datei verschoben bzw. umbenannt
- ACL geändert
- ACL gelesen (standardmäßig ausgeschaltet [Aktivierung in der pnTracer.config.xml-Datei möglich] und für NetApp und EMC Fileserver nicht verfügbar)

3.5.4 ACL-Änderung im Detail



Für die gewählten Verzeichnisse, Unterverzeichnisse und die dort enthaltenen Dateien wird die Aktion ACL geändert aufgezeichnet. Wobei hier, im Unterschied zu den drei oben beschriebenen Reports, nicht nur der Aktionstyp (hier ACL geändert) sondern auch die vorgenommenen Änderungen selbst (z.B. Lese-Berechtigung für Benutzer X hinzugefügt) aufgezeichnet werden.

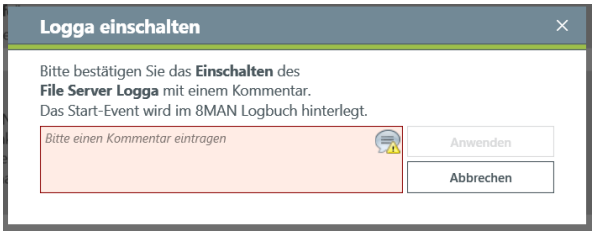
Dieser Reporttyp ist nicht für Windows Failover Cluster verfügbar.

Hinweis:
Die Ermittlung der detaillierten Berechtigungs-Änderungen erfordert eine aufwendige Prozedur, die nicht nur den FS Logga, sondern auch die überwachten Fileserver belastet. Wählen Sie diesen Reporttyp möglichst nur, wenn die Information, dass die Berechtigung auf einem Verzeichnis/einer Datei geändert wurde und wer diese Änderung gemacht hat, nicht ausreichen ist, wenn Sie also unbedingt die ACL-Änderungen im Detail benötigen.
Schränken Sie die Verzeichnisauswahl für diesen Reporttyp soweit wie möglich ein. Beachten Sie dabei, dass (wie auch bei den anderen Reporttypen) nicht nur das ausgewählte Verzeichnis, sondern auch alle Unterverzeichnisse und die enthaltenen Dateien überwacht werden.

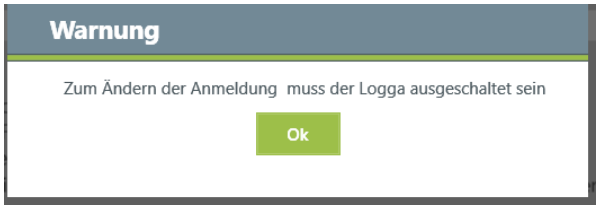
3.6 FS Logga aktivieren bzw. deaktivieren

Durch klicken auf 

können Sie den FS Logga aktivieren bzw. deaktivieren. Sie werden dann dazu aufgefordert, einen Kommentar einzugeben. Im 8MAN Logbuch wird diese Konfigurationsänderung mit Ihrem Kommentar abgelegt.



Solange der FS Logga eingeschaltet ist, ist es nicht möglich die Anmeldedaten zu ändern (nur bei NetApp und EMC Fileservern):



Bitte prüfen Sie nach Aktivieren des Logga, ob im 8MAN-Logbuch in der Spalte „Logga Status-Meldungen“ die Meldung des Kollektors über den Start des Logga zu finden ist.

3.7 FS Logga Einstellungen in der Konfigurationsdatei pnTracer.config.xml

3.7.1 Filtern von redundanten Ereignissen (Datenmenge wird reduziert)

Pro Verzeichnis/Datei-Aktion werden 43 Byte Datenbankspeicher verbraucht. Bei 1 Million Aktionen sind das schon 41 MB. Hier kann es sinnvoll sein, durch Einschränkung der zu überwachenden Aktionen die gesammelte Datenmenge zu reduzieren.

Bei vielen Benutzer-Aktionen wie z.B. bei einer Verzeichnisauflistung oder beim einfachen Öffnen oder Speichern einer Datei werden von der verwendeten Applikation oft mehrere Lese- bzw. Schreibvorgänge durchgeführt. Diese redundanten Ereignisse werden vom FS Logga verworfen, wenn sie innerhalb eines konfigurierbaren Zeitraums erfolgen.
Sie können konfigurieren:

- ob der FS Logga redundante Ereignisse (getrennt für Lese- und Schreibereignisse) verwerfen soll oder nicht
- den relevanten Zeitraum, innerhalb dessen diese Ereignisse als redundant gewertet werden

Default mäßig ist das Verwerfen redundanter Lese- und Schreibereignisse eingeschaltet und der Zeitraum, innerhalb dessen Lese- und Schreibereignisse als redundante Ereignisse gewertet werden, beträgt 10 Sekunden.
Sie können diese Einstellungen ändern. Auf dem Fileserver mit installiertem FS Logga öffnen Sie die **pnTracer.config.xml**-Datei unter **C:\ProgramData\protected-networks.com\8MAN\cfg** (wenn nicht vorhanden aus **C:\Programme \protected-networks.com\8MAN\etc** kopieren, den Inhalt löschen und die folgenden Zeilen einfügen):

```
<?xml version="1.0" encoding="utf-8"?>
<config>

    <tracer>
    <fileserver>
      <redundantEntriesHandling>
        <removeRead type="System.Boolean">true</removeRead>
        <removeWrite type="System.Boolean">true</removeWrite>
        <!-- maximum time-diff in seconds to ignore read or write, default 10 -->
        <maxTimeDiffForReads type="System.Int32">10</maxTimeDiffForReads>
        <maxTimeDiffForWrites type="System.Int32">10</maxTimeDiffForWrites>
      </redundantEntriesHandling>
    </fileserver>
  </tracer>

</config>
```

In den Zeilen für „removeRead“ bzw. „removeWrite“ können Sie das Verwerfen von redundanten Lese- bzw. Schreibereignissen ausschalten, indem Sie von „true“ auf „false“ ändern. Den relevanten Zeitraum ändern Sie in den Zeilen für „maxTimeDiffForReads“ bzw. „maxTimeDiffForWrites“. Hier ist der minimalen Wert 1 (1 Sekunde) und der maximale Wert 60 (60 Sekunden = 1 Minute).

Nach dem Speichern der pnTracer.config.xml-Datei muss der FS Logga aus- und wieder eingeschaltet werden, damit die Änderungen wirksam werden.

3.7.2 Die standardmäßige Nicht-Aufzeichnung von Aktionen für bestimmte Sicherheits-IDs (SIDs) ausschalten (nur FS Logga für Windows Fileserver)

Die standardmäßige Nicht-Aufzeichnung von Aktionen für folgende Sicherheits-IDs (SIDs) dient der Reduzierung der aufgezeichneten Datenmenge:

```
S-1-5-18  NT-AUTORITÄT\SYSTEM
S-1-5-19  NT-AUTORITÄT\LOKALER DIENST
S-1-5-20  NT-AUTORITÄT\NETZWERDIENST
```

Sie können die Aktionen auch dieser Accounts aufzeichnen. Dazu öffnen Sie auf dem Fileserver mit installiertem FS Logga die **pnTracer.config.xml**-Datei unter C:\ProgramData\protected-networks.com\8MAN\cfg (wenn nicht vorhanden aus C:\Programme \protected-networks.com\8MAN\etc kopieren, den Inhalt löschen und die folgenden Zeilen einfügen):

```
<?xml version="1.0" encoding="utf-8"?>

<config>
   <tracer>
    <windows>
      <suspendfilter type="System.Boolean">true</suspendfilter>
    </windows>
  </tracer>
</config>
```

Wenn Sie den Wert für „suspendfilter“ auf <false> setzen, werden Aktionen für alle oben genannten SIDs aufgezeichnet. Die Nicht-Aufzeichnung von Aktionen für einzelne SIDs ist nicht möglich.

Nach dem Speichern der pnTracer.config.xml-Datei muss der FS Logga aus- und wieder eingeschaltet werden, damit die Änderungen wirksam werden.

3.7.3 Verzeichnis für die Ablage temporärer Dateien ändern

Standardmäßig werden die temporären Dateien im Verzeichnis **C:\ProgramData\protected-networks.com\8MAN\data** abgelegt. Diese Einstellung können Sie ändern in der pnTracer.config.xml Datei. Auf dem Fileserver mit installiertem FS Logga öffnen Sie die **pnTracer.config.xml**-Datei unter **C:\ProgramData\protected-networks.com\8MAN\cfg** (wenn nicht vorhanden aus **C:\Programme \protected-networks.com\8MAN\etc** kopieren, den Inhalt löschen und die folgenden Zeilen einfügen):

```
<?xml version="1.0" encoding="utf-8"?>

<config>
  <tracer>
      <localStoragePath>E:\anderes\Verzeichnis</localStoragePath>
  </tracer>
</config>
```

Nach dem Speichern der pnTracer.config.xml-Datei muss der FS Logga aus- und wieder eingeschaltet werden, damit die Änderung wirksam wird.

4 FS Logga Reporte erstellen

Sie können aus den aufgezeichneten FS Logga Daten die Reporte:

- „Dateizugriffe“
- „Wo haben Änderungen stattgefunden?“
- „Hat ein unerlaubter Zugriff stattgefunden(SoD)“

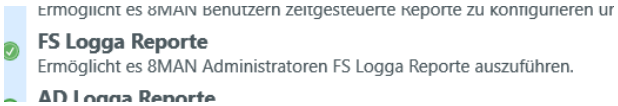
im CSV- oder XPS-Format erstellen und den Report

- „FS Logga Berechtigungsverlauf“

Im XLS-Format erstellen.

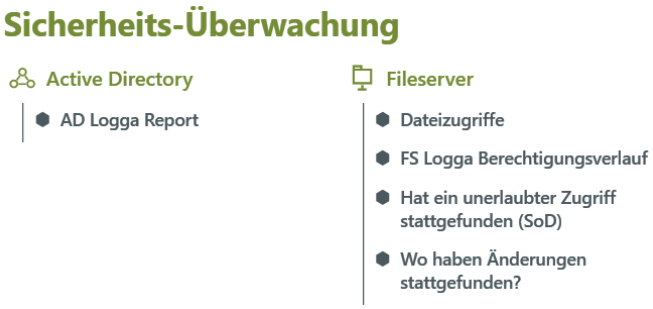
Voraussetzungen

- FS Logga Lizenz
- Domänenscan vorhanden
- Scan des Fileservers mit installiertem FS Logga vorhanden
- FS Logga ist für den Fileserver konfiguriert und zeichnet Daten auf
- eingeschaltete FS-Logga-Report-Funktion (8MAN Konfiguration → Benutzerverwaltung → Erweiterte Benutzerverwaltung):



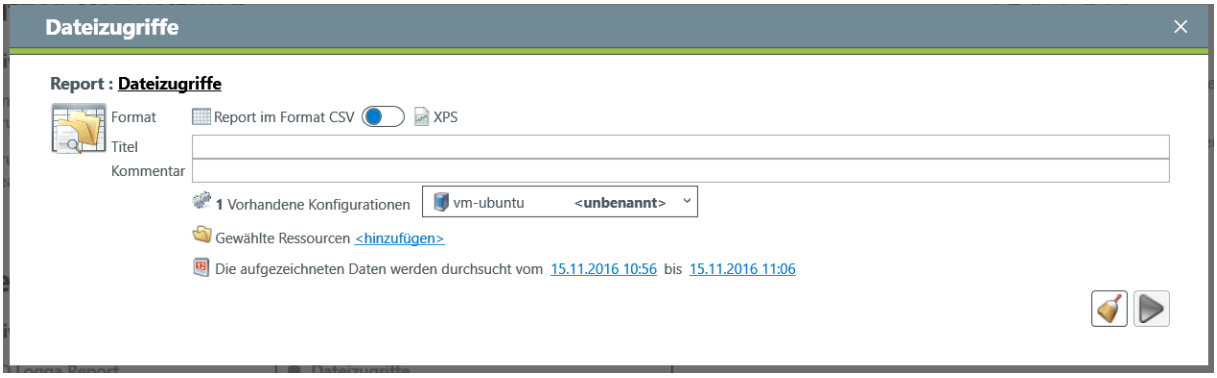
Aufruf

- 8MAN Startseite (Die jeweiligen Schaltflächen erscheinen nur, wenn mindestens eine Konfiguration für den entsprechenden Reporttyp existiert):



4.1 Reporte „Dateizugriffe“, „Wo haben Änderungen stattgefunden?“ und „Hat ein unerlaubter Zugriff stattgefunden(SoD)“

Dialog (am Beispiel Report „Dateizugriffe“; zusätzliche Parameter für die anderen 2 Reporten in Tabelle aufgeführt)



Parameter	Beschreibung
Report im Format CSV XPS	Wählbare Report Formate: CSV und XPS.
Titel	Sie können einen Titel des FS Logga Reports eintragen um z.B. die erstellten Reports zu ordnen.
Kommentar	Sie können z. B. den Anlass oder Auftraggeber benennen.
1 Vorhandene Konfigurationen vm-ubuntu <unbenannt>	Sie können eine in der 8MAN Konfiguration erstellte Konfiguration auswählen. Aus dieser Konfiguration wird dann ein Report erstellt.
Gewählte Ressourcen <hinzufügen>	Im erscheinenden Dialog können Sie die Verzeichnisse für den Report auswählen.
Die aufgezeichneten Daten werden durchsucht vom	Im erscheinenden Dialog können Sie den Zeitraum der aufgezeichneten FS Logga Daten für den Report auswählen.
Nur für „Wo haben Änderungen stattgefunden?“: Ändern des Filters für erfasste Aktionen	Im erscheinenden Dialog können Sie Aktionen für den Report auswählen.
Nur für „Hat ein unerlaubter Zugriff stattgefunden (SoD)“: Der Zugriff ist nur für diese Benutzer/Gruppen erlaubt <hinzufügen>	Im erscheinenden Dialog können Sie durch Doppelklick oder das Kontextmenü die erlaubten Benutzer und Gruppen für den Report auswählen.

Wenn Sie auf  klicken, wird ein Report im CSV- oder XPS-Format erstellt. Sie können den Report dann speichern, anzeigen oder per E-Mail senden (Voraussetzung E-Mail: 8MAN Konfiguration → Server → E-Mail → Option „Senden von E-Mails“ aktiviert):

Es ist auch möglich den Report später in der Report Übersicht zu öffnen.

Wenn im Report SIDs statt Benutzernamen angezeigt werden, müssen Sie einen erneuten Domänenscan und Scan des Fileservers mit installiertem FS Logga durchführen (siehe Voraussetzungen), um die SIDs aufzulösen.

4.2 Report “FS Logga Berechtigungsverlauf”

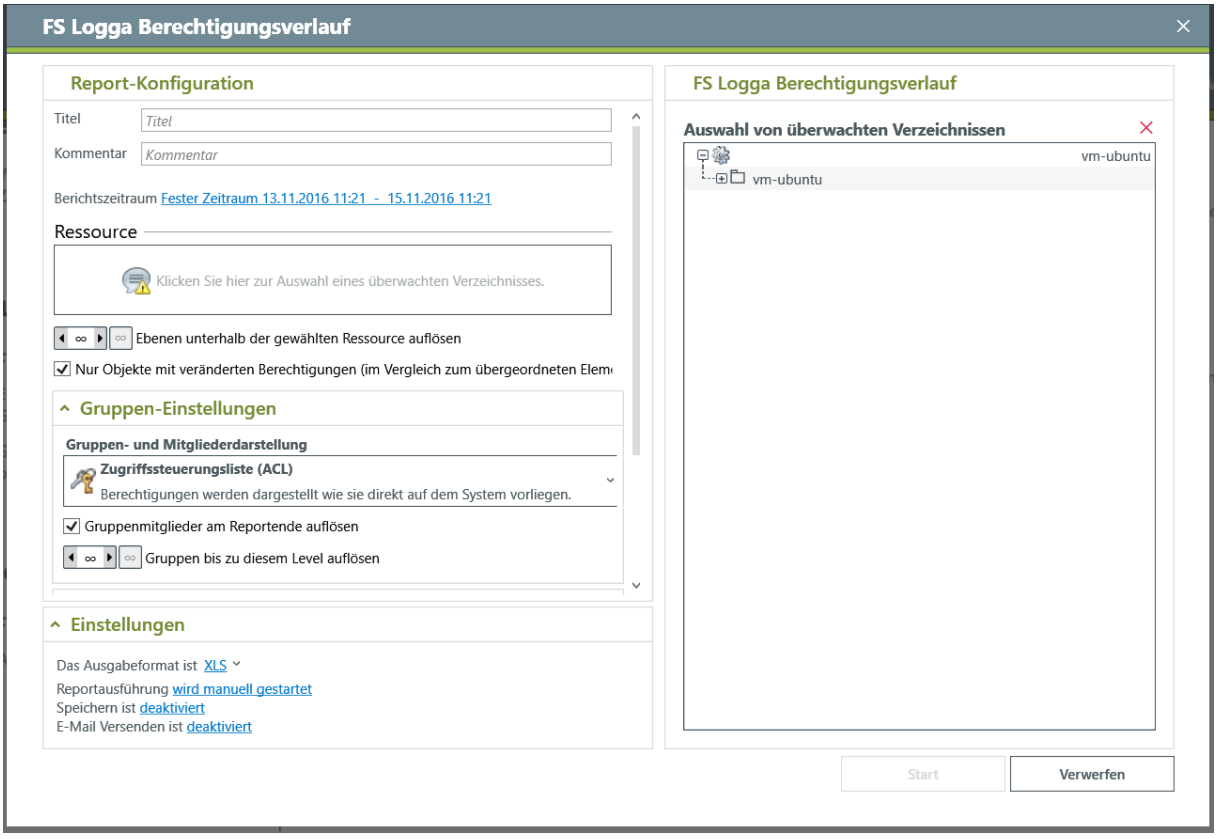
Dieser Report liefert basierend auf den Daten, die mit dem 8MATE FS Logga aufgezeichnet wurden, eine Übersicht über die Änderungen der Berechtigungslage in einem auszuwählenden Zeitraum. Weiterhin beinhaltet der Report die Darstellung der Berechtigungen zur Anfangs- und Endzeit basierend auf den jeweils passenden Scan-Daten.

Voraussetzungen (8MAN Konfiguration):

- Für 8MATE FS Logga muss der neue Reportyp “ACL-Änderungen im Detail” aktiviert und vollständig konfiguriert sein
- FS-Scans für den gleichen Server, der die überwachten Verzeichnisse beinhaltet müssen existieren, damit Start- und Endsituation dargestellt werden können

Neben der Möglichkeit den Report direkt auszuführen ist es auch möglich eine Ausführung zu planen. In diesem Fall wird empfohlen für den Report nicht ein fixes Anfangs- und Enddatum auszuwählen, sondern einen sich automatisch anpassenden Zeitraum.

Der Report erlaubt (wie auch der Berechtigungsreport „Wer hat wo Zugriff?“) die Festlegung der Gruppen-/Nutzerdarstellung sowie das zusätzliche Ausgeben von AD-Attributen.



Der Report kann folgende Tabellenblätter beinhalten:

- Konfiguration: Zusammenfassung der verwendeten Einstellungen
- Logga Konfigurationsänderungen: Übersicht über die Einstellungen des FS Logga, die während des Berichtszeitraums geändert wurden (sofern Änderungen vorgenommen wurden)

- Start-Situation: Berechtigungslage zum Beginn des Berichtszeitraums für Ordner
- Logga-Aufzeichnungen: Übersicht über alle Berechtigungsänderungsereignisse
- Details: Details zu den einzelnen Änderungsereignissen inkl. Wer? Wann? Was? Wo?
- 8MAN-Änderungen: Auflistung der Änderungen die mit 8MAN durchgeführt wurden, inkl. Kommentar des 8MAN-Benutzers
- Ist-Situation: Berechtigungslage zum Ende des Berichtszeitraums für Ordner

Hinweis:
Das Ermitteln der notwendigen Daten für diesen Report, also der Details der Berechtigungsänderungen, erhöht, je nach Größe (Anzahl Unterverzeichnisse und Dateien) der zu überwachenden Verzeichnisse, den Speicher- und Performance-Bedarf des Kollektors und in geringerem Maße auch den des zu überwachenden Fileservers. In der FS-Logga Konfiguration sollte deshalb die Verzeichnisauswahl für den Reportyp “ACL-Änderungen im Detail” auf die unbedingt notwendigen Verzeichnisse eingeschränkt werden.

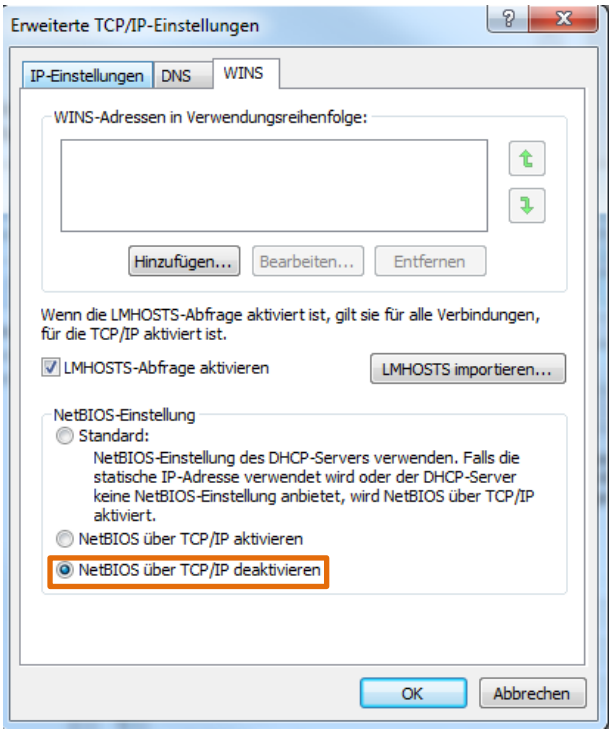
Anhang

Anhang I: Hilfe im Problemfall

Verbindungsprobleme zwischen Logga und NetApp

Die Einstellung NetBIOS über TCP/IP deaktivieren:

Eine mögliche Lösung für Netzwerkverbindungsprobleme ist die NetBIOS über TCP/IP-Einstellung zu deaktivierten. Um NetBIOS über TCP/IP zu deaktivieren gehen Sie auf dem Computer mit installiertem Kollektor-für-den-FS-Logga-für-NetApp-Fileserver zu folgendem Dialog Start → Systemsteuerung (Anzeige: Kategorie) → Netzwerk und Internet → Netzwerk- und Freigabecenter → Adaptereinstellungen ändern → LAN-Verbindung Eigenschaften → Internetprotokoll Version 4 (TCP/IPv4) → Eigenschaften → Erweitert → WINS und wählen die Einstellung NetBIOS über TCP/IP deaktivieren aus:



Leerer Report bei Windows Failover Cluster Logga

Beim Verschieben von Fileserver Ressourcen von einem Node zu einem anderen Node wegen Stoppen des Cluster Services auf dem Node oder durch Neustart des Nodes reagiert der übernehmende Node in seltenen Fällen nicht richtig beim Verbindungsaufbau zum Logga-Treiber, so dass der Treiber keine Information über das zum Node gewechselte Laufwerk bekommen kann. Dies führt dazu, dass der Logga keine Ereignisse über Datei-Aktionen für diese Laufwerk erhält.

Schalten Sie in diesem Falle den Logga, der die Verzeichnisse überwacht, für die der Report keine Aktionen anzeigt, aus und nach etwa 10 Sekunden wieder ein. Dies führt zu einem erneuten Verbindungsversuch zwischen Logga-Treiber und dem Node, was dann wegen des zu diesem Zeitpunkt stabilen Zustandes der Laufwerkskonfiguration des Nodes erfolgreich sein wird.

Anhang II: Software-Lizenzvereinbarungen

- Json.net, © 2006-2014 Microsoft, https://json.codeplex.com/license
- #ziplib 0.85.5.452, © 2001-2012 IC#Code, http://www.icsharpcode.net/opensource/sharpziplib/
- PDFsharp 1.33.2882.0, © 2005-2012 empira Software GmbH, Troisdorf (Germany), http://www.pdfsharp.net/PDFsharp_License.ashx
- JetBrains Annotations, ©2007-2012 JetBrains, http://www.apache.org/licenses/LICENSE-2.0
- Microsoft Windows Driver Development Kit, © Microsoft, EULA auf dem Computer auf dem der FS Logga für Windows Fileserver installiert ist unter: C:\Program Files\protected-networks.com\8MAN\driver (Verwendung nur für FS Logga für Windows Fileserver)
- NetApp Manageability SDK, © 2013 NetApp, https://communities.netapp.com/docs/DOC-1152 (Verwendung nur für FS Logga für NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation ,

  http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx

  MSDN CODE GALLERY BINARY LICENSE

  You are free to install, use, copy and distribute any number of copies of the software, in object code form, provided that you retain:

  • all copyright, patent, trademark, and attribution notices that are present in the software,

  • this list of conditions, and

  • the following disclaimer in the documentation and/or other materials provided with the software.

  The software is licensed “as-is.” You bear the risk of using it. No express warranties, guarantees or conditions are provided. To the extent permitted under your local laws, the implied warranties of merchantability, fitness for a particular purpose and non-infringement are excluded. This license does not grant you any rights to use any other party’s name, logo, or trademarks. All rights not specifically granted herein are reserved.

  v061708
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, http://wpf.codeplex.com/license
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC; https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE
- Mustache.js, © 2009 Chris Wanstrath (Ruby) and © 2010-2014 Jan Lehnardt (JavaScript), https://github.com/janl/mustache.js/blob/master/LICENSE
- jQuery, © 2014 The jQuery Foundation, https://jquery.org/license/
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE
- LoadingDots, © 2011 John Nelson, http://www.johncoder.com

- Underscore.js, © 2009-2014 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors https://github.com/jashkenas/underscore/blob/master/LICENSE
- easyModal.js, © 2013 Flavius Matis, https://github.com/flaviusmatis/easyModal.js
- jsTimezoneDetect, © 2012 Jon Nylander, project maintained at https://bitbucket.org/pellepim/jstimezonedetect; https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENCE.txt?at=defaultjquery-tablesort
- jquery-tablesort, © 2013 Kyle Fox, https://github.com/kylefox/jquery-tablesort