

Access Rights Management. Only much Smarter.

Access Rights Management AD Logga Handbuch

Version 9

© 2018 Protected Networks GmbH



1	Security Monitoring	. 4
1.1	8MATE AD Logga	. 5
2	Systemvoraussetzungen	. 7
2.1	Die 8MAN Architektur	. 7
2.2	AD Logga Voraussetzungen	. 8
2.3	Netzwerkanforderungen und Firewall-Einstellungen	. 9
	2.3.1 Die Windows Firewall für den AD Logga einrichten	. 9
3	Scans und Logga konfigurieren	10
3.1	Active Directory (AD) Logga konfigurieren	10
	3.1.1 Überwachung für den AD Logga aktivieren	10
	3.1.1.1 Überwachungsrichtlinien für die Domänencontroller (DC) konfigurieren	10
	3.1.1.1.1 Überwachungsrichtlinien für DCs in Server 2008 konfigurieren	10
	3.1.1.1.2 Überwachungsrichtlinien für DCs ab Server 2008 R2 konfigurieren	11
	3.1.1.1.3 Den AD Logga Speicherplatzbedarf konfigurieren	14
	3.1.1.1.4 Die Ausführung der Überwachungsrichtlinien überprüfen	14
	3.1.1.2 Größe des Windows Security Logs festlegen	15
	3.1.1.3 Die Überwachungsrechte in den AD-Objekt-SACLs einrichten	15
	3.1.2 Die Produktlizenz laden	18
	3.1.3 Eine AD Logga Konfiguration hinzufügen	20
	3.1.4 Den AD Logga aktivieren/deaktivieren	21
	3.1.5 Eine AD Logga Konfiguration anpassen	21
	3.1.5.1 AD Logga Ereignisse filtern	22
	3.1.5.1.1 Die Filterprinzipien verstehen	22
	3.1.5.1.2 Die Ereignisfilter konfigurieren	23
	3.1.6 Eine AD Logga Konfiguration löschen	26
4	Server	27
4.1	Die Anzeigedauer für Kommentarsymbole einstellen	28
4.2	Vorhaltedauer für AD Logga Daten konfigurieren	29
5	AD Logga Daten auswerten	30
5.1	Änderungen im Active Directory überwachen	30
5.2	Temporäre Gruppenmitgliedschaften erkennen	33
5.3	Gesperrte Benutzerkonten identifizieren	35
5.4	Kennwortzurücksetzungen überwachen	36
5.5	AD Logga Ereignisse mit dem Logbuch auswerten	38
5.6	Die letzten Aktionen an einem Nutzerkonto oder einer AD Gruppe identifizieren	40
6	Alarme konfigurieren	42

6.1	AD-Logga Alarmsensoren aktivieren/deaktivieren	. 43
6.2	Alarme für Gruppen anlegen	. 44
6.3	Alarme für Nutzerkonten anlegen	. 46
6.4	Alarme verwalten	. 48
7	Den 8MAN Support kontaktieren	49
8	Haftungsausschluss	50
9	Software-Lizenzvereinbarungen	51

1 Security Monitoring



Sowohl im Active Directory als auch auf dem Fileserver führen eine Reihe von Mitarbeitern Änderungen aus. Ohne ein vollumfängliches Monitoring entstehen Sicherheitsrisiken. Mit dem 8MATE AD Logga (für Active Directory) und dem 8MATE FS Logga (für Fileserver), erfassen Sie alle sicherheitsrelevanten Aktivitäten in Ihrem Firmennetzwerk. Damit können Sie nachvollziehen, wer was wann im Netzwerk gemacht hat und bei Problemen die Ursachen aufklären. Auf Prozessebene erlangen Sie vollständige Transparenz über die Access Rights Aktivitäten. Selbst außerhalb von 8MAN vorgenommene Änderungen werden erfasst. Auf Basis der gewonnenen Informationen lässt sich Ihr Access Rights Management Prozess optimieren. Mit den enthaltenen Alerts werden Sie bei kritischen

Ereignissen in Echtzeit, proaktiv informiert.

Das Security Monitoring ist mit jeder Basisversion kombinierbar. Es basiert auf drei kostenpflichtigen Add-Ons:

Active Directory

8MATE AD Logga

Fileserver

8MATE FS Logga

1.1 8MATE AD Logga



Problem

Auf dem AD führen eine Reihe von Mitarbeitern Änderungen aus. Ohne ein vollumfängliches Monitoring entstehen Sicherheitsrisiken und Unstimmigkeiten in den Prozessen.

Sicherheitsrisiken

Sicherheitsrisiken entstehen, wenn temporäre Gruppenmitgliedschaften unautorisierten Mitarbeitern Zugriff auf vertrauliche Dokumente geben. Werden die Gruppenmitgliedschaften anschließend wieder entzogen, bleibt der Sicherheitsvorfall unerkannt.

Unklare Prozesse

Unklare Prozesse können nur verbessert werden, wenn die Ist-Prozesse analysierbar sind. Wer gibt wem Mitgliedschaften und setzt Passwörter zurück? Wo entstehen Probleme und sind Absprachen nötig? Durch die Analyse von Fehlern, lässt sich ein individuelles Gruppenvergabekonzept erstellen.

Lösung

Der 8MAN schafft Klarheit über die Berechtigungssituation im Active Directory. Der AD Logga erweitert diese Transparenz auf die gesamte Änderungshistorie im System. Dabei werden auch außerhalb vom 8MAN vorgenommene Aktivitäten erfasst. Sicherheitsrelevante temporäre Gruppenmitgliedschaften und daraus resultierende unkontrollierte Berechtigungsvergaben sind damit sofort nachvollziehbar.

Anhand konfigurierbarer Reporte lassen sich Aktivitäten im Hinblick auf Konten, Objekten, Gruppen und Attribute lückenlos aufdecken.

Das erreichen Sie mit dem AD Logga

- Administratoren erhalten ein vollständiges Bild über die Aktivitäten im AD. Prozesse können so optimiert werden.
- Auditoren erkennen Sicherheitsvorfälle und die involvierten Akteure. Maßnahmen können so ergriffen werden.
- Die Geschäftsführung hat die Gewissheit: Der AD Logga stellt mit seinem Monitoring die Daten für interne Sicherheit und Prozessverbesserungen bereit.

Mit dem 8MATE AD Logga überwachen Sie permanent Änderungen am AD. Der AD Logga erfasst auch Änderungen, die nicht mit 8MAN ausgeführt wurden.

Die folgenden Änderungen werden vom AD Logga überwacht:

- AD Objekt erzeugt / gelöscht
- AD Objekt verschoben
- Gruppe, Benutzer- oder Computerkonto erstellt / gelöscht
- Gruppenmitgliedschaft geändert
- Konto aktiviert / deaktiviert
- Kennwort zurückgesetzt
- Konto gesperrt / entsperrt
- Attribut-Änderungen von AD Objekten (z. B. Gruppentyp, Distinguished Name, Department ...)

Erfasste Änderungen werden in der 8MAN Datenbank abgelegt und sind über das 8MAN Logbuch und Reporte kategorisiert abrufbar.

Der 8MAN AD Logga arbeitet agentenlos. Sie müssen also keine extra Software auf den Domänencontrollern installieren. Unterstützte Server Versionen sind in den <u>Systemvoraussetzungen</u> beschrieben.

Die vom 8MATE AD Logga verwendete Technologie stellt sicher, dass alle Ereignisse lückenlos aufgezeichnet werden. Kurzfristige Ausfälle des 8MAN Kollektors, z.B. wegen Wartung, führen nicht zu fehlenden Ereignissen im 8MAN Logbuch.

2 Systemvoraussetzungen

2.1 Die 8MAN Architektur



Die 8MAN Suite gliedert sich in drei Komponenten:

- 8MAN Server für die Verarbeitung der neuen Daten sowie der Anfragen von der grafischen 8MAN Benutzeroberfläche
- Kollektoren zur Anbindung der Ressourcensysteme und Datenverarbeitung
- 8MAN Benutzeroberflächen (Anwendungs- und Konfigurationsoberfläche, Weboberfläche)

Das Komponentenmodell der 8MAN Suite erlaubt es, Remote-Ressourcen durch verteilte Installationen optimal zu unterstützen. Alle Komponenten sind untereinander über netzwerkfähige Schnittstellen verbunden. Es können auch mehrere Komponenten auf dem gleichen Computer betrieben werden.



2.2 AD Logga Voraussetzungen

Der 8MATE AD Logga unterstützt Domänen Controller (DCs), die unter folgenden Server Versionen laufen:

• Microsoft Windows Server 2008 (32-bit und 64-bit), 2008 R2, 2012, 2012 R2 und 2016

Für den 8MATE AD Logga ist kein dedizierter Kollektor erforderlich. Der 8MAN Server selbst kann z. B. als Kollektor verwendet werden.

2.3 Netzwerkanforderungen und Firewall-Einstellungen

2.3.1 Die Windows Firewall für den AD Logga einrichten

@	Window	vs-Firev	wall mit erweiter	rter Sicherł	neit					_ D ×
Datei Aktion Ansicht ?										
♦ ♦ 2										
Windows-Firewall mit enveitert	Eingehende Regeln								Akt	tionen
🔣 Eingehende Regeln	Name		Gruppe ^		Profil	Aktiviert	Aktion	Außer Kra ^	Fir	ngehende Regeln
Ausgehende Regeln	Wetzwerkerkennung (WSD EventsSecure eingeh)	end)	Netzwerkerkennur	ng	Öffen	Ja	Zulassen	Nein		Naus Pagel
Verbindungssicherheitsrege	Netzwerkerkennung (WSD-Ereignisse eingehen	d)	Netzwerkerkennur	ng	Domä	Nein	Zulassen	Nein		Neue Negel
Derwachung	🖉 Netzwerkerkennung (WSD-Ereignisse eingehen	d)	Netzwerkerkennur	ng	Öffen	Ja	Zulassen	Nein	▼	Nach Profil filtern
	Remotedesktop - Benutzermodus (TCP eingehe	end)	Remotedesktop		Alle	Nein	Zulassen	Nein	8	Nach Status filtern
	Remotedesktop - Benutzermodus (UDP eingehe	end)	Remotedesktop		Alle	Nein	Zulassen	Nein		Nach Gruppe filtern
	Remotedesktop - Schatten (TCP eingehend)		Remotedesktop		Alle	Nein	Zulassen	Nein	1 -	
	Remotedienstverwaltung (NP eingehend)		Remotedienstverv	valtung	Alle	Nein	Zulassen	Nein	- I	Ansicht
	Remotedienstverwaltung (RPC)		Remotedienstverv	valtung	Alle	Nein	Zulassen	Nein	Q	Aktualisieren
	Remotedienstverwaltung (RPC-EPMAP)		Remotedienstverv	valtung	Alle	Nein	Zulassen	Nein		Liste exportieren
	Remote-Ereianisprotokollverwaltung (NP einge	hend)	Remote-Ereignisp	rotokollve	Alle	Nein	Zulassen	Nein	2	Hilfe
	Remote-Ereignisprotokollverwaltung (RPC)		Remote-Freignisp	rotokollve	Alle	Nein	Zulassen	Nein		Thine
	Remote-Ereignisprotokollverwaltung (RPC	Regel al	ktivieren p	rotokollve	Alle	Nein	Zulassen	Nein	Re	mote-Ereignispro 4
	Remoteereignisüberwachung (RPC)	Ausschr	neiden b	erwachung	Alle	Nein	Zulassen	Nein	0	Regel aktivieren
	Remoteereignisüberwachung (RPC-EPMA	Koniere		erwachung	Alle	Nein	Zulassen	Nein	-	Assessmentation
	🜑 Eingehende Regel für Remoteherunterfahı	Lynches	a	ihren	Alle	Nein	Zulassen	Nein	4	Ausschneiden
	🔘 Eingehende Regel für Remoteherunterfahr	Loscher	n fa	ihren	Alle	Nein	Zulassen	Nein	19	Kopieren
	🔘 Remoteverwaltung geplanter Aufgaben (F	Eigensc	haften n	g geplante	Alle	Nein	Zulassen	Nein	×	Löschen
	Remoteverwaltung geplanter Aufgaben (F	Hilfe	n	g geplante	Alle	Nein	Zulassen	Nein		Figenschaften
	Remotevolumeverwaltung - Dienst für virturen	Dutentin	nemotevolumevel	rwaltung	Alle	Nein	Zulassen	Nein		
	Remotevolumeverwaltung - Ladeprogramm de	s Diens	Remotevolumeve	nvaltung	Alle	Nein	Zulassen	Nein _		Hilfe
	Remotevolumeverwaltung (RPC-EPMAP)		Remotevolumeve	rwaltung	Alle	Nein	Zulassen	Nein =		
	Routing und Remotezugriff (GRE eingehend)		Routing und RAS		Alle	Nein	Zulassen	Nein		
	Routing und Remotezugriff (L2TP eingehend)		Routing und RAS		Alle	Nein	Zulassen	Nein		
	Routing und Remotezugriff (PPTP eingehend)		Routing und RAS		Alle	Nein	Zulassen	Nein		
	Schlüsselverwaltungsdienst (TCP eingehend)		Schlüsselverwaltur	ngsdienst	Alle	Nein	Zulassen	Nein		
	🖤 Secure Socket Tunneling-Protokoll (SSTP einge	hend)	Secure Socket Tur	nneling-Pr	Alle	Nein	Zulassen	Nein		
	🥑 WWW-Dienste (Eingehender HTTPS-Datenverk	ehr)	Sichere WWW-Die	enste (HTT	Alle	Ja	Zulassen	Nein 🗸		
< III >		n	Children T			AL	7.	>		
Regel aktivieren										

Ist die Windows Firewall auf dem zu überwachenden DC eingeschaltet, müssen Sie die von Microsoft vordefinierte Regel "Remote-

Ereignisprotokollverwaltung (RPC)" aktivieren.

Wiederholen Sie den Vorgang für jeden zu überwachenden DC.

3 Scans und Logga konfigurieren

BMAN Konfiguration V	ersion:				_ □ ×	8MAN scannt in konfigurierbaren
	Serverstatus Lizenzinformationen		Jobs Übersicht	Kollekta Konfigur	ren Ition	Intervallen Berechtigungsstrukturen von
	Angemeldete Benutzer: 1	24 Scans 17 Reporte	15 Änderungen 36 Weitere	1 Verbunden 1 Insgesamt konfiguriert		verschiedenen Ressourcen-
	Lizenziert	4 Geplant 85 Erfolgreich	0 Ausführung 3 Fehlgeschlagen	Alle Kollektoren sind betriebsbereit		Systemen. Die Scan-Ergebnisse
	🕰 Filter				12	speichert 8MAN in einer SQL-
	Scans Ressourcerkonfigurationen, Leons Elennong CV Lennet	Open Order Open Order-	Benutzerverwaltun Benutzerverwaltun	ung Data Owner g. Organisationskategorien, Data		Datenbank. Benutzer sehen in der Benutzeroberfläche sehr schnell die Ergebnisse, weil diese aus der
	Logge, rieselver Cov import	sourcenseschleisungen	Kollennen walkong	Group Wizard Einstellungen		Datenbank abgerufen werden.
	Lizenz Lizenz Lizentinformationen, Joi	Jobübersicht bstatus, Jobkategorien	Kollektoren 8MAN Kollektorenübersi -konfiguration	Alarmkonfiguration Aktivierte Alarm Sensoren		Ereignisse, die zwischen den Scans passieren, erfassen die 8MATES AD
	Qo	lant -	O.			Add-Ons zu den Basisversionen von
	Ändern-Konfiguration An Algemeine Ansi Änderungseinstellungen, fü Technologiespezifische Å	sichten & Reporte hten & Reporte, Blacklist r Ansichten & Reporte	Server GrantMA, Kommentare, Datenstandspeichen, Server-Gesundheitschen	Basiskonfiguration E-Mail, BMAN-Server, SQL-Server, Ing, Status der Konfiguration ik, Se		8MAN und benötigen eine entsprechende Lizenz.
Bereit				(demosdmin © localhost 🕣 🏄	Klicken Sie auf "Scans", um
						<i>Ressourcen-Scans und die Logga zu konfigurieren.</i>

3.1 Active Directory (AD) Logga konfigurieren

3.1.1 Überwachung für den AD Logga aktivieren

3.1.1.1 Überwachungsrichtlinien für die Domänencontroller (DC) konfigurieren

Für die AD Logga Funktionalität müssen Sie spezielle Überwachungsrichtlinien (Audit Policies) aktivieren. Um Überwachungsrichtlinien auf DCs ändern zu können, müssen Sie Mitglied der entsprechenden Domänen-Admins Gruppe oder der Gruppe der Organisations-Admins sein.

3.1.1.1.1 Überwachungsrichtlinien für DCs in Server 2008 konfigurieren

Führen Sie vor dem Setzen der Überwachungsrichtlinien eine <u>Prüfung</u> aus - ggf. sind ja bereits alle erforderlichen Kategorien aktiviert.

Für die Aktivierung der erforderlichen Überwachungsrichtlinien führen Sie folgende Kommandos auf jedem DC mit Administratorrechten aus:

Für "Richtlinienänderungen überwachen":

auditpol /set /subcategory:{0CCE922F-69AE-11D9-BED3-505054503030} /success:enable

Für "Verzeichnisdienständerungen":

auditpol /set /subcategory:{0CCE923C-69AE-11D9-BED3-505054503030} /success:enable

Für "Benutzerkontenverwaltung", "Computerkontoverwaltung", "Sicherheitsgruppenverwaltung", "Verteilergruppenverwaltung", "Anwendungsgruppenverwaltung" und "Andere Kontoverwaltungsereignisse":

```
auditpol /set /subcategory:{0CCE9235-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9236-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9237-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9239-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
auditpol /set /subcategory:{0CCE9238-69AE-11D9-BED3-505054503030} /success:enable
```



Wiederholen Sie den Vorgang für jeden DC!

3.1.1.1.2 Überwachungsrichtlinien für DCs ab Server 2008 R2 konfigurieren

Ab Server 2008 R2 können Sie den Gruppenrichtlinien-Editor zur Einrichtung der Überwachung benutzen. Damit müssen Sie die Einrichtung nur einmal vornehmen und nicht mehr auf jedem DC wiederholen. Beachten Sie dabei, dass sich die Aktivierung der Überwachungsrichtlinien je nach Replikationsintervall zwischen den Domänencontrollern (DCs) verzögert.

Nachdem Sie die folgenden Einstellungen vorgenommen haben:

- führen Sie ein manuelles Richtlinienupdate mit dem Kommando "gpupdate /force" aus,
- prüfen Sie die Ausführung der Überwachungsrichtlinien.

	Ausführen	Starten Sie die Gruppenrichtlinienverwaltuna, z. B.
Ö <u>f</u> fnen:	Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an. gpmc.msc v	mit: gpmc.msc
	OK Abbrechen <u>D</u> urchsuchen	

Erstellen Sie eine neue Gruppenrichtlinie. Wählen Sie die OU, in der die DC Computerkonten sind, standardmäßig ist das die OU "Domain Controllers".

Stellen Sie sicher, dass die neu erstellte Richtline für die DCs wirksam ist (Hierarchie, Abarbeitungsreihenfolge).



Die Reihenfolge, in der Sie die Optionen setzen, beeinflusst die Wirksamkeit der Richtlinie. Halten Sie die hier vorgegebene Reihenfolge ein!

Wählen Sie die neu erstellte Gruppenrichtlinie mit Rechtsklick und dann "Bearbeiten".





Navigieren Sie zu "Sicherheitsoptionen". Wählen Sie die Richtlinie "Überwachung: Unterkategorie...". Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Sicherheitsrichtlinie wie gezeigt.



Die Reihenfolge, in der Sie die Optionen setzen, beeinflusst die Wirksamkeit der Richtlinie. Halten Sie die hier vorgegebene Reihenfolge ein! Datei Aktion Ansicht ?

wareeinstellungen dows-Einstellungen Namensauflösungsri Skripts (Start/Herunt

l okale Richtlin

Detei Atton Ansicht ? Detei Atton Ansicht ?		
Bechtlinien Bechtlini		
Beginning Beginning	en, konfigurieren:	

Navigieren Sie zu Kontenverwaltung. Nutzen Sie die Mehrfachauswahl und markieren alle Unterkategorien. Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Überwachung bei Erfolg wie gezeigt.

Navigieren Sie zu "DS-Zugriff". Wählen Sie die Unterkategorie "Verzeichnisdienständerungen überwachen".

_ 🗆 X

Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Überwachung bei Erfolg wie gezeigt.



Erklärung



Navigieren Sie zu "Richtlinienänderung". Wählen Sie die Unterkategorie "Überwachungsrichtlinienänderun g überwachen". Mit Rechtsklick und "Bearbeiten" aktivieren Sie die Überwachung bei Erfolg wie gezeigt. Nachdem Sie die Einstellungen vorgenommen haben:

- führen Sie ein manuelles Richtlinienupdate mit dem Kommando gpupdate /force aus,
- prüfen Sie die Ausführung der Überwachungsrichtlinien.

3.1.1.1.3 Den AD Logga Speicherplatzbedarf konfigurieren

Für 1.000 Ereignisse werden ca. 0,57 MB Speicherplatz in der Datenbank benötigt.

Die Vorhaltedauer für AD Logga Einträge beträgt standardmäßig 30 Tage und kann unter Server -> Datenstandspeicherung geändert werden.

3.1.1.1.4 Die Ausführung der Überwachungsrichtlinien überprüfen

Um die Ausführung der Überwachungsrichtlinie zu überprüfen, starten Sie eine Eingabeaufforderung mit Administratorrechten und führen folgendes Kommando aus:

auditpol /get /category:"Richtlinienänderung,Kontenverwaltung,DS-Zugriff"

alternativ für alle Kategorien oder andere Sprachen:

auditpol /get /category:*

C3.5	Administrator: Eingabeaufforderung	×
C:\Vindows\system32>auditpol /get /categor Systemübervachungsrichtlinie Kategorie/Interkategorie Richtlinienänderung Authentifizierungsrichtlinienänderung Autorisierungsrichtlinienänderung MPSSUC-Richtlinienänderung Efiterplattform-Richtlinienänderung	ry:"Richtlinienänderung,Kontenverwaltung,DS-Zugriff" Einstellung Keine Überwachung Rekine Überwachung Rekine Überwachung Keine Überwachung	
Richtlinienänderungen überwachen Kontenverwaltung Benutzerkontoerwaltung Sicherheitsgruppenverwaltung Uerteilergruppenverwaltung Andere Kontoverwaltungsereignisse BS-Zugriff Verzeichnisdienständerungen	Erfolg Erfolg Erfolg Erfolg Erfolg Erfolg Erfolg	
Detaillierte Verzeichnisdienstreplikatie Verzeichnisdienstzugriff	nceine auchwachung Neine Überwachung Keine Überwachung	
C:\Windows\system32>_		~
< III	>	. Hi

Die markierten Unterkategorien müssen auf "Erfolg" eingestellt sein.

3.1.1.2 Größe des Windows Security Logs festlegen

Um keine Ereignisse zu "verlieren", muss je nach Ereignisaufkommen die maximale Größe für das Security Event Log eingestellt werden. Für die betreffenden Überwachungseinstellungen belegt ein Ereignis im Durchschnitt etwa 1 KB.

Beispiel:

Für eine Serverausfall- bzw. Wartungszeit (des als AD Logga Kollektor gewählten Servers) von z.B. einer Stunde bei 1.000 Ereignissen pro Stunde läge das absolute Minimum der Security Event Log Größe also bei 1 MB. In Anbetracht dieser geringen Speicheranforderung für 1.000 Ereignisse, der Unbestimmtheit von Ausfallzeiten, sowie der Relevanz von Security Ereignissen, empfehlen wir, hier reichlich zu dimensionieren.

Wie Sie die Größe einstellen, finden Sie bei Microsoft.

3.1.1.3 Die Überwachungsrechte in den AD-Objekt-SACLs einrichten

Nachdem Sie die Überwachungsrichtlinien aktiviert haben, müssen Sie die Überwachungsrechte für die AD-Objekte (SACL) entsprechend konfigurieren.

Für die Konfiguration der SACL ist das User Recht "Manage Auditing and Security Log" notwendig (was dem Privileg "SeSecurityPrivilege" entspricht). Dazu müssen Sie Mitglied der Gruppe "Ereignisprotokollleser" oder "Domänen-Admins" sein.

Die Einrichtung der SACL ist nur auf einem der zur überwachenden Domäne gehörenden DC notwendig. Die anderen DCs erhalten diese dann über die Replikation.

	Ausführen	Starten Sie die Verwaltung der Active Directory-Benutzer und -
	Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.	Computer auf einem DC, z.B. mit dem Kommando
Ö <u>f</u> fnen:	dsa.msc 🗸	dsa.msc
	OK Abbrechen <u>D</u> urchsuchen	

ktivieren Sie die Option "Ansicht > rweiterte Features".

3	Active Director	y-Benutzer und -Computer		_ _ ×
Datei Aktion Ansicht ?				
Þ 🔿 🙍 💀 Spalten hinzufügen/ent	:fernen			
Große Symbole	-	Typ	Reschreibung	
Gespeich Kleine Symbole		Organisationseinheit	beschiebung	
b 🗿 8man-de Liste		Organisationseinheit		
Details		builtinDomain		
	10 1 0 11	Organisationseinheit		
Benutzer, Kontakte, Gru	ppen und Computer als Container	Container	Default container for up	
Enweiterte Features		Organisationseinheit		
Filteroptionen		Organisationseinheit	Default container for do	
Anpassen	5	Container	Default container for sec	
	@ mnastructure	infrastructureUpdate		=
	CostAndFound	lostAndFound	Default container for or	
	Managed Service Accounts	Container	Default container for ma	
	Microsoft Exchange Security	Gr Organisationseinheit		
	iii Microsoft Exchange System G	Obj msExchSystemObjectsCont	t	
	mtDS Quotas	msDS-QuotaContainer	Quota specifications co	
	🚞 Program Data	Container	Default location for stor	
	📓 Quarantäne	Organisationseinheit		
	Serviceaccounts	Organisationseinheit		
	System	Container	Builtin system settings	
	TestGroups	Organisationseinheit		
	TestUsers	Organisationseinheit		
	TPM Devices	msTPM-InformationOhied	•	Ľ
Andert die Optionen für die Ansicht.				

		Act	tive Directory-Be	enutzer und -Computer		_ 🗆 🗙
Datei Aktion Ansicht	?					
🗢 🔿 🖄 📰 📋 🖾	0 🗟 🛛 🖬 🔧 🐿	7 🗾 🐍				
Active Directory-Benutze	r und -Computer [sv-8man.8ma n Objektvervaltung zuweisen Suchen Domänencontroller ändern Domänencontroller ändern Domänencontroller ändern Domänencontroller ändern Neu Alle Aufgaben Ansicht Aktualisieren	Name SMAN Redin ufstufen	Ces Ilers Principals re Accounts ange System Obj	Typ Organisationseinheit Organisationseinheit BuiltinDomain Organisationseinheit Organisationseinheit Organisationseinheit Organisationseinheit IostAndFound Container Organisationseinheit Organisationseinheit Organisationseinheit	Beschreibung Default container for up Default container for do Default container for do Default container for or Default container for or Queta specifications co	A B
	Eigenschaften Hilfe	TestGroups	5	Organisationseinheit Organisationseinheit Container Organisationseinheit Organisationseinheit	Builtin system settings	
< 111	>	TPM Devices		msTPM-Information∩hiect		~

Active Directory-Benutzer und -Computer

Allgemein Verwattet von Objekt Sicherheit Attribut-Editor

Berechtigungen für "Jeder"

Ale untergeordneten Objekte erstellen Ale untergeordneten Objekte löschen Klicken Sie auf "Erweitet", um spezielle Berechtigungen anzuzeigen.

Vollzugriff Lesen Schreiben

Algemein Verwatet von Objekt Gruppen-oder Benutzemanen: Statuest Statue

OK Abbrechen Übernehmen Hiffe

Eigenschaften von 8man-demo.local ? ×

ung

ntainer for up.. ntainer for do.

ntainer for sec.

tainer for or...

ntainer for ma..

ecifications co... cation for stor...

m settings

^ ≡

Hinzufügen... Entfemen

Zulassen Verweigem

Erweitert

Wählen Sie die zu überwachende Domäne mit Rechtsklick und dann "Eigenschaften".

Wählen Sie im Eigenschaftenfenster den Reiter "Sicherheit" und dann die Schaltfläche "Erweitert".

_ 🗆 X

8MAN

Datei Aktion Ansicht ?

🗢 🔿 📶 📋 🖾 🔂 🖬 🐮 🐮

Active Directory-Benutzer und -Computer [srv-8man.8ma
 Bespeicherte Abfragen
 Fill 8man-demo.local

rechti oppell ndern, berwa	gungen Überwachung Effektiver dicken Sie auf einen Überwachungsein wählen Sie den Eintrag aus, und klicke chungseinträge:	Zugriff trag, um zusätzliche Inform n Sie auf "Bearbeiten" (sow	ationen zu erhalten. U eit vorhanden).	Jm einen Überwachungseintrag zu
Ty	p Prinzipal	Zugriff	Geerbt von	Anwenden auf
🔏 Erf	ol Jeder		Keine	Speziell
Erf	ol Jeder		Keine	Speziell
📕 Erf	ol Domänen-Benutzer (8MAN-D	Alle erweiterten Rechte	Keine	, Nur dieses Objekt
Erf	ol Administratoren (8MAN-DEM	Alle enweiterten Rechte	Keine	Nur dieses Objekt
Erf	ol Jeder	Vollzugriff	Keine	Dieses und alle untergeordnet

Wählen Sie den Reiter "Überwachung". Analysieren Sie die bereits vergebenen Überwachungsrechte. Vielleicht sind ja schon ausreichende Rechte vergeben? Erweitern Sie ggf. die Berechtigungen eines vorhandenen "Jeder"- Prinzipals oder fügen Sie einen Eintrag hinzu.

Überwachı	ungseintrag für "8man-demo"
Prinzipal: Jeder Prinzipal auswählen Typ: Erfolgreich Anwenden auf: Dieses und alle untergeordneten Objekte	▼ ▼
Rejectionnee:	
Vollzugriff	✓ "msExchOmaCarrier"-Objekte löschen
🗌 Inhalt auflisten	"msExchOmaConfigurationContainer"-Objekte erstellen
Alle Eigenschaften lesen	"msExchOmaConfigurationContainer"-Objekte löschen
✓ Alle Eigenschaften schreiben	"msExchOmaContainer"-Objekte erstellen
✓ Löschen	"msExchOmaContainer"-Objekte löschen
☑ Unterstruktur löschen	"msExchOmaDataSource"-Objekte erstellen
Berechtigungen lesen	"msExchOmaDataSource"-Objekte löschen
✓ Berechtigungen ändern	"msExchOmaDeliveryProvider"-Objekte erstellen
Besitzer ändern	"msExchOmaDeliveryProvider"-Objekte löschen
Alle bestätigten Schreibvorgänge	"msExchOmaDeviceCapability"-Objekte erstellen
Alle erweiterten Rechte	"msExchOmaDeviceCapability"-Objekte löschen
☑ Alle untergeordneten Objekte erstellen	"msExchOmaDeviceType"-Objekte erstellen
☑ Alle untergeordneten Objekte löschen	"msExchOmaDeviceType"-Objekte löschen
	OK Abbrechen

Benötigt wird mindestens: Prinzipal: "Jeder" Typ: "Erfolgreich" Anwenden auf: "Dieses und alle untergeordneten Objekte"

Berechtigungen:

- Alle Eigenschaften schreiben
- Löschen
- Unterstruktur löschen
- Berechtigungen ändern
- Alle untergeordneten Objekte erstellen
- Alle untergeordneten Objekte löschen

3.1.2 Die Produktlizenz laden

8MAN Kon	figuration		_	Klicken Sie in der 8MAN
- Lizenzin	formation und Serverstatus			Konfiguration im Menü
	Lizenzinformation	Serverstatus Laufzeit: 2 Stunden Version: 90.118.0 Angemeldete Benutzer: 1 Name Domäne Host BMAN Komponente demoadmin BMAN-DEMO svo-Bman Konfiguration		Serverstatus auf Lizenz laden.
Bereit		c	lemoadmin @ localhost 🗲	
				~
8	Bitte wähler	n Sie die Lizenzdatei	x	Wählen Sie den Pfad zu Ihrer
€ ⊚ - ↑	膭 « Lokaler Datenträger (C:) 🕨 ProgramData 🕨 protected-r	networks.com > 8MAN > licenses > C "licenses" durchs	uchen 🔎	Lizenzdatei.
Organisieren 👻	Neuer Ordner	8	•	QNAAN Lizonzdataion baban dia
🚖 Favoriten 🔳 Desktop	Name Ār	nderungsdatum Typ Größe		Endung ".license".
Downloads		a warden keine odenergebnisse gerunden.		

Nach dem Klick auf Öffnen wird die Lizenzdatei nach

%ProgramData%protectednetworks.com\8MAN\licenses kopiert.

Alle lizenzierten Features werden sofort aktiviert.

💹 Zuletzt besucht

💻 Dieser PC

📔 Desktop

Musik
 Videos
 Lokaler Datenträg

👝 FS (D:)

Dateiname: 8MAN.license

Dokumente
Downloads

✓ Lizenzdatei (*.license)

Öffnen Abbrechen

¥



© 2018 Protected Networks GmbH

3.1.3 Eine AD Logga Konfiguration hinzufügen

tive Directory Ressource	Easy Connect - CSV Ressource	Easy Connect - SQL Ressource	Exchange Ressource	Fileserver Ressource	
gga - Active Directory perwachen eines Active Directory	Logga - File Server Überwachen eines Fileservers	Lokale Accounts	SharePoint ☆ Sharepoint Ressource (Farm Based)	SharePoint SharePoint Webseitensammlung	
arePoint Online arePoint Online Webseitensammlung	VMware vSphere Ressource				
▲ Filter				11]
& ► ► Ø	8man-demo.local			×	
Die Domäne <u>8man-demo.loca</u>	al wird wöchentlich, Samstag, 21:00 []	(Mehr »)			
Ressource ist dieser Do	mane zugeordnet. Kessourcen-koning	uration hinzurugen *		×	
Der vSphere <u>srv-vcenter01</u> wi	rd Auf Anfrage [] Mehr »			, And	
ON 8man-demo.l	ocal (8man-demo.local)			×	
Die Domäne 8man-demo.local Es sind <u>folgende Filter</u> gesetzt. Die Daten werden alle	l wird überwacht auf SRV-8MAN, mit d Überwachung ist <u>aktiviert</u> . Minuten aktualisiert.	er Anmeldung <u>8man-demo\administrat</u>	<u>or</u> .		
B 📐 🕅 🗤	cchange13.8man-demo.local			×	
Der Exchange snv-exchange13	3.8man-demo.local wird Auf Anfrage [.] (Mehr »)			
				×	

Wählen Sie auf der Startseite der Konfiguration "Scans".

Wählen Sie "Logga - Active Directory".



- 1. Geben Sie gültige Anmeldeinformationen für die Domäne an, die überwacht werden soll.
- 2. Nutzen Sie den Filter, um die gewünschte Domäne zu finden.
- 3. Selektieren Sie eine Domäne. Child-Domänen werden nicht mit überwacht. Jede Domäne muss separat konfiguriert werden.
- 4. Wählen Sie einen Kollektor-Server. Sie können nur einen Kollektor pro Domäne wählen.

Wenn Sie eine AD Logga Konfiguration hinzugefügt haben, ist der Logga zunächst deaktiviert.

Sie müssen <u>den AD Logga aktivieren</u>, um Ereignisse aufzuzeichnen.

BMAN Konfigura

P

3.1.4 Den AD Logga aktivieren/deaktivieren



Wählen Sie auf der Startseite der Konfiguration "Scans".

Klicken Sie in der gewünschten AD Logga Konfiguration auf den Schalter oder den Link, um den AD Logga zu aktivieren.

AD Logga Ereignisse werden standardmäßig 30 Tage gespeichert. Siehe Vorhaltedauer für Datenstände konfigurieren

Sie müssen einen Kommentar eingeben.

Gehen Sie für das Deaktivieren analog vor.



Logga einschalten

Bitte bestätigen Sie das **Einschalten** des Active Directory Logga mit einem Kon Das Start-Event wird im 8MAN Logbuch



Wählen Sie auf der Startseite der Konfiguration "Scans".

- 1. Geben Sie der Konfiguration einen anderen Namen.
- 2. Hinterlegen Sie die Anmeldung, mit welcher der AD Logga die Ereignisse von den DCs liest. Das Konto muss Mitglied in der Gruppe "Ereignisprotokollleser" oder "Domänen-Admins" sein. Sie können die Anmeldung nur ändern, wenn der Logga ausgeschaltet ist.
- 3. Legen Sie fest, in welchem Intervall die Logga Daten aktualisiert werden. Ereignisse werden vom Kollektor zwischengespeichert und in dem eingestellten Intervall über den 8MAN Server in die Datenbank geschrieben. Standardeinstellung: 10 min,

Mögliche Werte 1 bis 60 Minuten.

3.1.5.1 AD Logga Ereignisse filtern

Filtern Sie uninteressante Ereignisse heraus, um nur relevante Einträge aufzuzeichnen. Filtern bedeutet hier, dass herausgefilterte Ereignisse nicht aufgezeichnet werden.

Sie erhöhen damit deutlich den Überblick und reduzieren Datenvolumen. Ein typisches Beispiel sind die häufigen Attributänderungen des Exchange-Servers.

Sie können einen Filter nur konfigurieren, wenn ein AD-Scan vorhanden ist.

3.1.5.1.1 Die Filterprinzipien verstehen

Der AD Logga Filter ist als Blacklist-Filter konzipiert. Blacklist bedeutet hier: Der AD Logga zeichnet mit maximalem Umfang auf. Sie legen fest, welche Ereignisse nicht aufgezeichnet - also verworfen - werden. Standardmäßig ist ein Filter auf die zwei Objektklassen "Service-Connection-Point" und "Print-Queue" gesetzt.

Die Filter-Kriterien arbeiten additiv. Ein Ereignis wird verworfen, wenn Kriterium 1 oder Kriterium 2 oder Kriterium 3 zutrifft, oder auch mehrere Kriterien gleichzeitig.

Die Filter-Kriterien stehen in keiner Korrelation zueinander. Die Ereignisse werden vom AD Logga nacheinander bezüglich der Kriterien bewertet. Bei einem Treffer wird das Ereignis sofort verworfen und nicht weiter überprüft, unabhängig davon, ob ein anderes Kriterium schon bewertet wurde oder nicht.

Beispiele:

- Ist Benutzer A als Filter konfiguriert, dann werden alle von ihm im AD vorgenommen Änderungen verworfen, auch wenn die von ihm geänderte Objektklasse oder das geänderte Attribut nicht als Filter konfiguriert sind. Änderungen, die Benutzer A selbst betreffen, werden weiterhin aufgezeichnet.
- Ist Objektklasse X als Filter konfiguriert, dann werden alle Ereignisse, die explizit diese Objektklasse enthalten, verworfen, auch wenn der Ereignis-Autor oder das geänderte Attribut nicht als Filter konfiguriert sind. Analog gilt dies auch für den Attribut-Filter.

Hinweis:

Nicht alle Security-Log Ereignisse enthalten die betroffene Objektklasse oder das betroffene Attribut. So werden z.B. Mitgliedschaftsänderungen nicht verworfen, selbst wenn die Objektklassen "User" und "Group" und das Attribut "Member" als Filter konfiguriert sind.

3.1.5.1.2 Die Ereignisfilter konfigurieren





- 1. Filtern Sie Ereignisse von Benutzern heraus.
- 2. Nutzen Sie den Filter, um die gewünschten Benutzer zu finden. Sie können nach Anzeigename (Display Name) oder CommonName suchen.
- 3. Selektieren Sie einen Benutzer und ziehen diesen per Drag&Drop in die rechte Spalte.

8MAN Konfigura

- 1. Sie können Gruppen als Ereignis-Autoren herausfiltern. Die Filterstufe wird angezeigt, wenn Sie
- 2. die Option aktivieren. Ziehen Sie Gruppen per Drag&Drop in die rechte Spalte, werden die Ereignisse aller Mitglieder direkte und indirekte herausgefiltert.
- 3. Klicken Sie auf "erweiterte Einstellungen".





Legen Sie fest, nach welchem Modus der Filter die Gruppenmitgliedschaften aktualisiert. Beachten Sie die Hinweise im angezeigten Dialog.

Verwenden Sie "Ereignis-basiert" nur, wenn sich die Mitgliedschaften in den herauszufilternden Gruppen selten ändern.

Das Aktualisierungsintervall für die Option "Zeit-basiert" kann auf Werte zwischen 10 und 1440 min (24h) eingestellt werden. Je kürzer das Intervall, desto höher die Last auf dem AD.



Filtern Sie Ereignisse von einzelnen oder allen Computer-Konten heraus.



Filtern Sie Ereignisse bestimmter Objektklassen heraus.

Standardmäßig werden die Ereignisse der zwei markierten Objektklassen herausgefiltert.

Das erstmalige Laden der Objektklassen aus dem AD kann etwas Zeit in Anspruch nehmen. Danach werden die Objektklassen aus der Datenbank geladen. Klicken Sie auf "Auslesen", um die Objektklassen, z. B. nach einer Schema-Änderung zu aktualisieren.

A Filter	Setzen Sie verschiedene Filter	kriterien, um die vom Active Directory Logga	gesammelten Daten einzuschränken.	11
Die Deserveren G		Auswahl der Attribute	Ausgefilterte Attribute	^
Die Ressource 5	Antius Disentena Fasianian		Filter 2411	
0	Active Directory Ereignisse	ms-Exch-2003-Url (msExch2003Url)	 ms-Exch-2003-Url (msExch2003Url) 	
	+++++	ms-Exch-Accepted-Domain-BL (msExchAcceptedDomainB	ms+Exch+Accepted-Domain+BL (msExchAcceptedDomainE	×
	Benutzer Ereignis-Autoren	ms-Exch-Accepted-Domain-Flags (msExchAcceptedDomai	ms-Exch-Accepted-Domain-Flags (msExchAcceptedDoma	
Die Persource h		ms-Exch-Accepted-Domain-Name (msExchAcceptedDoma	ms-Exch-Accepted-Domain-Name (msExchAcceptedDom-	
Die Ressource I.	+++++	ms-Exch-Access-Control-Map (msExchAccessControlMap)	ms-Exch-Access-Control-Map (msExchAccessControlMap)	
	Gruppen Ereignis-Autoren	ms-Exch-Access-Flags (msExchAccessFlags)	ms-Exch-Access-Flags (msExchAccessFlags)	
i) 🔊		ms-Exch-Access-SSL-Flags (msExchAccessSSLFlags)	ms-Exch-Access-SSL-Flags (msExchAccessSSLFlags)	×
	+++++	ms-Exch-Account-Forest-BL (msExchAccountForestBL)	ms-Exch-Account-Forest-BL (msExchAccountForestBL)	
0.0	Computer Ereignis-Autoren	ms-Exch-Account-Forest-Link (msExchAccountForestLink)	ms-Exch-Account-Forest-Link (msExchAccountForestLink)	
Die Ressource h		ms-Exch-Activation-Config (msExchActivationConfig)	ms-Exch-Activation-Config (msExchActivationConfig)	
	+++++	ms-Exch-Activation-Preference (msExchActivationPreferen	ms-Exch-Activation-Preference (msExchActivationPreferen	
	Objektklassen	ms-Exch-Activation-Schedule (activationSchedule)	ms-Exch-Activation-Schedule (activationSchedule)	×
	₹2	ms-Exch-Activation-Style (activationStyle)	ms-Exch-Activation-Style (activationStyle)	
		ms-Exch-Active-Instance-Sleep-Interval (msExchActiveInsta	ms-Exch-Active-Instance-Sleep-Interval (msExchActiveInst	
Der Exchange 8		ms-Exch-ActiveSync-Device-AutoBlock-Duration (msExchA	ms-Exch-ActiveSync-Device-AutoBlock-Duration (msExch/	
	Attribute	ms-Exch-ActiveSync-Device-Autoblock-Threshold-Incidence	ms-Exch-ActiveSync-Device-Autoblock-Threshold-Inciden	
1		ms-Exch-ActiveSync-Device-Autoblock-Threshold-Incidence	ms-Exch-ActiveSync-Device-Autoblock-Threshold-Inciden	×
	¥ 2411	ms-Exch-ActiveSync-Device-Autoblock-Threshold-Type (m	ms+Exch+ActiveSync+Device-Autoblock-Threshold-Type (n	
	++++	ms+Exch-Activity-Based-Authentication-Timeout-Interval (ms+Exch+Activity-Based+Authentication+Timeout-Interval I*	
Die Ressource h		Aktualisieren der Attribute und Objektklassen durc	ch erneutes Auslesen des Active Directory.	
	Logga Autzeichnung			
				~
100 A				~
On On				
Die Domäne Sm	Bitte einen Kommentar eintragen		Anwenden	

Filtern Sie Ereignisse zu gewählten Attributen heraus.

Beispiel:

Alle Ereignisse zu den Attributen, die "ms-exch" enthalten, werden herausgefiltert, also nicht aufgezeichnet.

Zurück	Filterkonfiguration für de	en Active Directory Logga		X Weitere Systeme
Fibre Die Ressource 5 Die Ressource 1 Die Ressource	Setzen Sie verschiedene Filter	kriterien, um die vom Active Directory Logga ge Auswah der Attribute Auswah der Attribute Auswah der Attribute Auswah der Attribute Auswah der Attribute Attribute Auswah der Attribute Auswah der Attribute Access Control-Map (mSchAccepteDomain m-Eich-Access-Staf-Rag (mSichAccessFagne) m-Eich-Access-Staf-Rag (mSichAccessFagne) m-Eich-Access-Staf-Rag (mSichAccessFagne) m-Eich-Access-Staf-Rag (mSichAccessFagne) m-Eich-Access-Staf-Rag (mSichAccessFagne) m-Eich-Access-Staf-Rag (mSichAccessFagne) m-Eich-Access-Fagn (mSichAccessFagne) m-Eich-Access-Fagne (mSichAccessFagne) m-Eich-Active-Terest-Bi (mSichAccessFagne) m-Eich-Active-Terest-Bi (mSichAccessFagne) m-Eich-Active-Terest-Bi (mSichAccessFagne) m-Eich-Active-Signe-Device-AutoBlock-Duration (mEichA m-Eich-Active)m-Device-AutoBlock-Threnhold-Incelere M-Eich-Active)m-Device-AutoBlock-Threnhold-Incelere M-Eich-Active)m-Device-AutoBlock-Threnhold-Inceler	sammelten Daten einzuschränken. Ausgefilterte Attnbute	
Die Domäne 8m. Es sind	Attribute "ms-exch" herasgefiltert für De	emozwecke.	Anwenden Abbrechen	

Sie müssen einen Kommentar eingeben, um die geänderten Filtereinstellungen anzuwenden.

3.1.6 Eine AD Logga Konfiguration löschen



Wählen Sie auf der Startseite der Konfiguration "Scans". Wählen Sie die gewünschte AD Logga Konfiguration. Klicken Sie auf das rote "X".



Entscheiden Sie, ob Sie vorhandene Logga-Daten behalten oder löschen wollen.

Das Löschen ist nur möglich, wenn alle weiteren Benutzeroberflächen geschlossen sind.

Im Menü Server-Status können Sie angemeldete Benutzer identifizieren.

4 Server

8MAN Konfiguration Version:	_ 🗆 ×	Klicken Sie au
Serverstatus Jobs Kollektoren Lizenzinformationen Übersicht Konflauzion		Einstellunger
Angemeldete Benutzer: 2 17 Reporte 33 Weitere 1 1 Irregerant konfiguriert		Gesundheits
Lizenbert 4 Geplant 0 Ausführung 84 Erfolgreich 3 Fehlgeschlagen Alle Kollektoren sind betriebsbereit		die Ereignis-I
A Filter 12		vorzunehme
Scans Open Order Benutzerverwaltung Data Owner Ressoucentionfigurationen, Löggs, Fieserver CSV Import Open Order- Ressoucenbeschreibungen Benutzerverwaltung, Bolenverwaltung Data Owner Owner Group Wizard Einstelungen Ressourcenbeschreibungen Bolenverwaltung, Group Wizard Einstelungen Owner Ressourcen- Group Wizard Einstelungen		
Lizenz Jobübersicht Kollektoren Alarmkonfiguration		
Lizenzinformationen, Jobatatus, J		
Andern-Konfiguration Ansichten & Reporte Server Basikonfiguration Alternoire Ansichten & Reporte GrandMA Kommentare E-Mail BMA/Songer 501-Server		
Anderungienettellungen, Eir Ansichten & Reporte Datenstandspeicherung, Satus der Konfiguration Technologiespealfische A		
Bereit demoad	min © localhost 🗲 🏼 📥	

Klicken Sie auf "Server" um Einstellungen für Kommentare, E-Mail, Datenstandspeicherung, Gesundheits-Check, GrantMA und die Ereignis-Protokollierung vorzunehmen.

4.1 Die Anzeigedauer für Kommentarsymbole einstellen

Zurück * Kommentare Image: Anzahl der Tage, für die Kommentarzettel an Accounts und Ressourcen angezeigt werden sollen. Image: Diese Einstellung betrifft lediglich das Symbol an den betroffenen Accounts und Ressourcen. Das komplette Logbuch kann zu jedem Zeitpunkt über das Kontextmenü erreicht werden.
 Kommentare Anzahl der Tage, für die Kommentarzettel an Accounts und Ressourcen angezeigt werden sollen. Anzehl der Tage zur Geschlung betrifft lediglich das Symbol an den betroffenen Accounts und Ressourcen. Das komplette Logbuch kann zu jedem Zeitpunkt über das Kontextmenü erreicht werden.
90 100 Anzahl der Tage, für die Kommentarzettel an Accounts und Ressourcen angezeigt werden sollen.
✓ E-Mail
✓ Datenstandspeicherung
✓ Server Gesundheits-Check
✓ Server Ereignis Protokollierung

8MAN zeigt in der Benutzeroberfläche ein Notizzettel-Symbol für hinterlegte Kommentare oder AD Logga Informationen an. Je länger Sie 8MAN betreiben, desto mehr Notizzettel sehen Sie. Reduzieren Sie die Anzeigedauer,

wenn Sie in der Benutzeroberfläche zu viele Notizzettel-Symbole sehen.

4.2 Vorhaltedauer für AD Logga Daten konfigurieren

BMAN Konfiguration			×
Zurück			
← Kommentare			
✓ E-Mail			
^ Datenstandspeicherung			
Scan-Archiv aktivieren, um alte und bereits in der Datenbank gelöschte Datenstände zu laden.			
Der 8MAN Server speichert das Scan-Archiv unter dem Pfad C <u>\ProgramData\protected-networks.com\8MAN\data\ScanArchive</u>			
Wenn nicht mehr genügend Speicherplatz im Archiv verfügbar ist lösche die ältesten Archive			
☑ Automatisches Löschen alter Datenstände in der Datenbank aktivieren.			
Tägliche Active Directory Datenstände in der Datenbank speichern für < 180 🕨 Tag(e). 🗱 Monatliche Datenstände beibehalten für 🤇 60 🕨 Monat(e).			
 Tägliche Datenstände in der Datenbank speichern für (21) Tag(e). Monatliche Datenstände beibehalten für (3) Monat(e). 			
Aufgezeichnete AD Logga Daten werden gelöscht, wenn sie älter sind als (999) Tag(e).			
Aufgezeichnete FS Logga Daten werden gelöscht, wenn sie älter sind als 💽 999 🕥 Tag(e).			
✓ Server Gesundheits-Check			
← Server Ereignis Protokollierung			
Bereit	📥 cradmin @ localhost 🗲	Version: 1	7

In der Datenstandspeicherung legen Sie fest, wie lange Scan- und Logga-Daten vorgehalten werden. Sie beeinflussen damit die Größe der Datenbank und den verwendeten Speicherplatz.

Beachten Sie die Hinweise zur Verwendung von SQL Express.

81	1AN Konfiguration	_ □	×
•	Server		
	✓ GrantMA		
	✓ Kommentare		
	✓ E-Mail		
\land	* Datenstandspeicherung		
	Stan-Archiv äktivieren, um alte und bereits in der Datenbank gelöschte Datenstande zu luden. Der BMAN Server speichert das Scan-Archiv unter dem Pfad CJProgram Data/protected-networks.com/BMAN/data/ScanArchive Wenn nicht mehr genügend Speicherplatz im Archiv verfügbar ist überspringe das Archivieren Mutomatisches Löschen alter Datenstände in der Datenbank skriveren. Monatische Datenstände in der Datenbank speicherm für Monatische Datenstände in der Datenbank speicherm für Monatische Datenstände in der Datenbank speicherm für Monatische Datenstände beibehalten für		
	 Server-Gesundheitscheck 		
	✓ Server-Ereignisprotokollierung		
Bereit	demoadmin û	localhost	€ -

Legen Sie fest, wie lange 8MAN Logga Daten vorhält. Die Ereignisse verbrauchen folgenden Speicherplatz: FS Logga: ca. 50 Byte AD Logga: ca. 600 Byte

5.1 Änderungen im Active Directory überwachen

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga überwachen Sie die Ist-Prozesse in ihrem Active Directory. Das Besondere: Auch mit Bordmitteln durchgeführte, temporäre Änderungen werden erfasst. Aus sicherheitskritischer Sicht sind insbesondere Veränderungen an Ereignistypen und Ereignisautoren wichtig:

Überwachung von Ereignistypen

Änderungen an:

- Attributen
- Benutzern
- Computern
- Gruppen
- Kennwörtern
- Konten

BSI

• Mitgliedern

Überwachung von Ereignisautoren

- Benutzer
- Gruppen
- Computer

Zusätzlich können Sie noch nach Objekt Klassen und Attributen filtern. Dabei handelt es sich jedoch um Experteneinstellungen. Filtern Sie nach einem seltenen Attribut, kann dies die gesamte Suche verfremden.

Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen <u>M</u> 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie <u>M 4.312 Überwachung von</u> <u>Verzeichnisdiensten</u>.

Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten Alarme für Gruppen anlegen Alarme für Nutzerkonten anlegen

Report".

Der Prozess in einzelnen Schritten



- × 1. Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.
 - 2. Legen Sie den Zeitraum für den Report fest.
 - 3. Wählen Sie die Domänenobjekte, deren Ereignisse im Report enthalten sein sollen.

AD Logga Report

keport-koniiguration	AD Logga Report
Titel	Bitte Ressource(n) auswählen
Commentar Kommentar	Bessourcen
Reportzeitraum <u>Fester Zeitraum 19.12.2017 17:02 - 21.12.2017 17:02</u>	2 Sman-demo.local
Dbjekte	
8man-demo local	⇒ ···· → Berlin
unan demonocar	3 Builtin
	• • • • • • • • • • • • • • • • • • •
	• • • • • • • • • • • • • • • • • • •
reignistyp	••• • • • • • • • • • • • • • • • • •
Bitte wählen Sie einen oder mehrere Ereignistypen.	🕀 🛑 😉 Critical Ressources
Soll nach allen Ereignistypen gesucht werden, lassen Sie die Auswahl frei.	→ … 🗉 🔿 😉 Program Data
	····
reignis-Autor	···· 🕀 🔘 😣 Managed Service Accounts
5	🕀 🌒 🙂 Domain Controllers
Bitte wählen Sie einen oder mehrere Benutzer.	···⊞ 🛑 😉 Serviceaccounts
Sollen Ereignisse aller Benutzer gesucht werden, lassen Sie die Auswahl frei.	🕀 🌒 Quarantäne
	→ ··· 🕀 🔿 😗 System
Objekt Klasse	· · · · · · · · · · · · · · · · · · ·
Finstellungen	🕀 🌒 TestGroups
Ellistellungen	🕀 🌒 😗 vSphere-Roles
Das Ausgabeformat ist XLS ~	😳 🕀 🌒 🚺 TestUsers
Erzeuge den Report <u>für alle Konten zusammengefasst in einem</u> Dokument.	
Reportausführung wird manuell gestartet	
Benutzerdefinierter Speicherpfad ist nicht konfiguriert	
E-Mail Versenden ist <u>deaktiviert</u>	 1 Vorlage verfügbar





Definieren Sie den Umfang des Reports, in dem Sie die folgenden Filter setzen. Für alle Filter gilt: Sollen alle aufgezeichneten Ereignisse im Report enthalten sein, lassen Sie die Auswahl frei.

- 1. Fügen Sie die Typen von Ereignissen hinzu.
- 2. Fügen Sie die Autoren von Ereignissen hinzu.
- 3. Fügen Sie die Objektklassen hinzu.
- 4. Fügen Sie die Attribute von Ereignissen hinzu.

8MAN Report-Konfiguration AD Logga Report nete Active Directory Ereign Report über aufgezei 1 Vorlage verfügba Ereignistyp ---Be 0 Erzeugt am 🔻 Autor Ereignis-Autor 30.09.2014 16:16 8 Ber Objekt Klasse Speichern der Vorlag Attribut 🕞 🔚 Überschreiber Einstellungen Nei Das Ausgabeformat ist <u>XLS</u> ~ Reportausführung <u>wird manuell gestarte</u> Speichern ist <u>deaktiviert</u> E-Mail Versenden ist <u>deaktiviert</u> 0

Sie können AD Logga Reportkonfigurationen als Vorlagen speichern. Erleichtern Sie sich so die Wiederverwendung von komplexen Reportkonfigurationen.

- 1. Wählen Sie eine vorhandene Vorlage.
- 2. Speichern Sie die aktuelle Konfiguration als Vorlage.

- 1. Legen Sie verschiedene Ausgabeoptionen fest.
- 2. Starten Sie die Erstellung des Reports.



8MAN

5.2 Temporäre Gruppenmitgliedschaften erkennen

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga schliessen Sie eine zentrale Sicherheitslücke: Temporäre Gruppenmitgliedschaften. Innentäter berechtigen sich auf geheime Verzeichnisse, kopieren Daten und stellen den Ursprungszustand der Berechtigungssituation wieder her. Ohne AD Logga bleiben Aktionen wie diese unter dem Radar.



Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahme <u>M</u> <u>4.312 Überwachung von Verzeichnisdiensten</u>.

Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten Alarme für Gruppen anlegen Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Start".
- 2. Klicken Sie auf "AD Logga Report".

- 1. Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.
- 2. Legen Sie den Umfang des Reports fest. Wählen Sie bei Ereignistyp "Mitglied entfernt" und "Mitglied hinzugefügt".
- 3. Legen Sie Ausgabeoptionen fest.
- 4. Starten Sie die Erstellung des Reports.

SIVIA IN Ver	sion: 7.			
	Suche			
YY	AD Logga Report		×	
	Report-Konfiguration	AD Logga Report		
Bere	Titel Titel	Ereignistyp	×	
	Kommentar Kommentar	A Filter	18	
	Reportzeitraum Fester Zeitraum 08.11.2016 12:47 - 10.11.2016 12:47			
	Domänen	Attribut entfernt		
	8man-demo.local	Attribut geändert	lun lun	
		Reputzer erstellt	100	
🕖 🛛 Beny		Benutzer gelöscht		
	Ereignistyp	Computer erstellt		
o≃o Ac	Manufact analysis Manufact Manufact	Computer gelöscht		
• E	Witglied entremt, Witglied Ninzugerügt	Gruppe erstellt	enu	
G		Gruppe gelöscht		
	Ereignis-Autor	Kennwort zurücksetzen	nist	
E		Konto deaktiviert	Bor	
	Bitte wählen Sie einen oder mehrere Benutzer. Sollen Ereignisse aller Regulter gesucht werden Jassen Sie die Auswahl frei	Konto entsperrt	0.1	
	Solien creignisse aller benutzer gesucht werden, lassen sie die Auswahl nei.	Konto gesperrt	gen	
C ¹ 1	Objekt Klasse	Mitglied entfernt	Rep	
Sich		Mitglied hinzugefügt		
1	Bias and the Construction October	Sonstige Objekte erstellt		
	 Einstellungen 	Sonstige Objekte geloscht		
	Das Ausnaheformat ist XIS Y		inse	
20 L Fi	Reportausführung wird manuell gestartet		arve	
	Speichern ist <u>deaktiviert</u>			
	E-Mail Versenden ist <u>deaktiviert</u>	✓ 1 Vorlage verfügbar		
		Start	Verwerfen	
4 • •				
5				
• W				
		8MAN-DEMO.LOCAL ~ (🕒 📑 📀 <neuester sca<="" td=""><td>n> ′ 🛈</td></neuester>	n> ′ 🛈

5.3 Gesperrte Benutzerkonten identifizieren

Hintergrund / Mehrwert

Der versuchte Login mit einem fremden Konto endet im besten Fall mit einem gesperrten Nutzerkonto. Der AD Logga zeigt Ihnen, von welchem Computer der Angriff kam.

Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten Alarme für Gruppen anlegen Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Start".
- 2. Klicken Sie auf "AD Logga Report".

- 8MAN 0 AD Logga Report rt-Konfigurati AD Logga Report Ereignistyp A Filter zeitraum Fester Zeitraum 08.11.2016 12:47 10.11.2016 12:47 Attribut entfernt Attribut geänder omäner 춫 ribut hinzugefüg nutzer erstellt Bei Benutzer gelöscht Computer erstellt Ereignistyp * Computer gelö Gruppe erstellt Konto gesperrt Gruppe gelösch Kennwort zurüc Konto aktiviert Konto deaktivie Ereignis-Autor onto entsperit onto entsperit conto gesperit "~d entfernt Objekt Klasse Einstellunger rmat ist XLS führung <u>wird manue</u> ist <u>deaktiviert</u>
- 1. Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.
- 2. Legen Sie den Umfang des Reports fest. Wählen Sie bei Ereignistyp "Konto gesperrt".
- 3. Legen Sie Ausgabeoptionen fest.
- 4. Starten Sie die Erstellung des Reports.



.OCAL \vee 这 📑 🥝 <Neuester Scan> 🗠

5.4 Kennwortzurücksetzungen überwachen

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga überwachen Sie den Prozess des Kennwortrücksetzens. Diesem ist ein Sicherheitsrisiko inhärent. Setzt beispielsweise ein Helpdesk-Mitarbeiter heimlich das Kennwort einer Führungskraft zurück, kann er mit dem Übergangspasswort sich anmelden und geheime Daten einsehen. Die betroffene Führungskraft würde den Vorfall wahrscheinlich nicht merken und sich nur über das nicht mehr gültige Kennwort wundern, den Support kontaktieren und ein neues Kennwort erhalten.



Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen <u>M</u> 2.11 Regelung des Passwortgebrauchs, <u>M 4.48 Passwortschutz unter Windows-Systemen</u> sowie <u>M 4.312</u> Überwachung von Verzeichnisdiensten.

Weiterführende Services

AD Logga Ereignisse mit dem Logbuch auswerten Alarme für Gruppen anlegen Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



\varTheta St

8MAN

- Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.
- 2. Legen Sie den Umfang des Reports fest. Wählen Sie bei Ereignistyp "Kennwort zurücksetzen".
- 3. Legen Sie Ausgabeoptionen fest.
- 4. Starten Sie die Erstellung des Reports.

Bor	Titel Titel	A	
Dere		Ereignistyp	×
	Kommentar Kommentar	A filter	18
	Reportzeitraum Fester Zeitraum 01.02.2014 13:30 - 10.11.2016 13:30	-	
	Dawland	Attribut entfernt	
	Domanen	Attribut geändert	
	8man-demo.local	Attribut hinzugefügt	Import-
Ren		Benutzer erstellt	
Беп		Benutzer gelöscht	
	Ereignistyp	Computer erstellt	
0≏o A		Computer gelöscht	
	Kennwort zurücksetzen	Gruppe erstellt	enutzer'
		Gruppe gelöscht	
		Kennwort zurücksetzen	pistrator
	Ereignis-Autor	Konto aktiviert	
	Bitte wählen Sie einen oder mehrere Benutzer.	Konto deaktiviert	Benutzer
	Sollen Ereignisse aller Benutzer gesucht werden, lassen Sie die Auswahl frei.	Konto entsperrt	ach
		Konto gesperrt	
Ciak	Objekt Klasse	Mitglied entfernt	Report
Sich		Mitglied hinzugefügt	
	Bas webs Contraction Objection	Sonstige Objekte erstellt	
	 Einstellungen 	Sonstige Objekte geloscht	
			inex
35 📃 📮 Fi	3 Das Ausgabetormat ist XLS *		rver)?
	Speichern ist deaktiviert		
	E-Mail Versenden ist <u>deaktiviert</u>	Vorlage verfügbar	
		Start Verwe	rfen
4			
		MAN-DEMOLOCAL X D	Contractor Server V
		SIMAIN-DEMOLEOCAL · O ES	Viveuester acan> •

ਜ਼ ਙਾਟਾ ਦ						gga Report_8N	MAN-DEMO_cradmin_20161110133143.XLS -	Excel		
Datei	Start	Einfügen	Seitenlayout	Formeln	Daten Überprüfen		Q Was möchten Sie tun?		Jörg Bran	idt 🛛 🤱 Freigeber
A389	Ŧ	: × v	fx							
4	А			в			С	D	E	F
Zeit		Autor			C	bjekt		Objektklasse	Ereignis	Attribut Name A
2	6.02.2014	16:56 cradmir	i (8man-demo\o	cradmin)	B	no, Al (8man	-demo\Al.Bino)	User(user)	Kennwort zurücksetzen	
28.02	2.2014 15:4	0:35 cradmir	(8man-demo\d	cradmin)	Z	fer, Lou (8ma	n-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
11.03	3.2014 09:1	15:01 Admini:	strator (8man-d	emo\Administ	trator) Z	fer, Lou (8ma	n-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
13.03	3.2014 14:5	0:42 Admini	strator (8man-d	emo\Administ	trator) Z	fer, Lou (8ma	n-demo\Lou.Zifer)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 11:4	19:04 neadmi	n (8man-demo\	neadmin)	B	org, Inge (8m	an-demo\inge.Borg)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 12:3	1:32 neadmi	n (8man-demo\	neadmin)	B	org, Inge (8m	an-demo\lnge.Borg)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 15:	12:28 Admini	strator (8man-d	emo\Administ	trator) K	rise, Christiar	ne (8man-demo\Christiane.Krise)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 15:4	7:05 Admini	strator (8man-d	emo\Administ	trator) A	nder, Ole (8m	nan-demo\Ole Ander)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:	0:09 neadmi	n (8man-demo\	neadmin)	A	ber, Mark (8n	nan-demo\Mark Aber)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:	0:09 neadmi	n (8man-demo\	neadmin)	A	ien, Arnold (3man-demo\Arnold Alien)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:5	0:09 neadmi	n (8man-demo\	neadmin)	A	loe. Vera (8m	an-demo\Vera Aloe)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:	0:09 neadmi	n (8man-demo)	neadmin)	A	nder. Ole (8m	nan-demo\Ole Ander)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:	0:09 neadmi	n (8man-demo\	neadmin)	A	nder, Cori (8r	nan-demo\Cori Ander)	User(user)	Kennwort zurücksetzen	
10.03	3 2015 16	0.09 neadmi	n (8man-demo)	neadmin)	A	ner Dominik	(8man-demo\Dominik Aner)	User(user)	Kennwort zurücksetzen	
10.03	3 2015 16	0.09 neadmi	n (8man-demo)	neadmin)	A	ngebrandt A	ngie (8man-demo\Angie Angebrandt)	User(user)	Kennwort zurücksetzen	
10.03	3 2015 16	0.09 neadmi	n (8man-demo)	neadmin)	A	ofel Adam (8	man-demo\Adam Apfel)	User(user)	Kennwort zurücksetzen	
10.03	3 2015 164	0:09 neadmi	n (8man-demo)	neadmin)	A	rheit Andi (8	man-demo\Andi Arbeit)	User(user)	Kennwort zurücksetzen	
10.03	3 2015 16-	0:09 neadmi	n (8man-demo)	neadmin)	Δ	m Armin (8r	man-demo\Armin Arm)	Liser(user)	Kennwort zurücksetzen	
10.03	3 2015 16-	0:09 neadmi	n (8man-demo)	neadmin)	Δ	oni Mark (8	man-demo/Mark Aroni)	User(user)	Kennwort zurücksetzen	
10.03	3 2015 16-	0:09 noadmi	n (8man domo)	noadmin)	A	sil. Claire (8a	an domo)Clairo Asil)	User(user)	Konnwort zurücksetzen	
10.00	3 2015 16.	0:09 neadmi	n (8man-demo)	neadmin)	~	uor Karl (8m	an domo/Kad Auor)	User(user)	Kennwort zurücksetzen	
10.00	2 2015 16.	0:00 neadmi	n (Oman-demo)	neadmin)	~	where Arra (011	man demoltan Aukeo)	User(user)	Kennuert zurücksetzen	
10.03	2 2015 10.5	0:09 neadmi	n (oman-demo)	neadmin)	A	utoob Anko	(Sman demo)Anko Autooh)	User(user)	Kennwolt zurücksetzen	
10.00	3.2015 10.3	0.09 neadmi	n (oman-demo)	neaumin)		utsch, Anker	(ornan-demovarike Adusch)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 10.3	0.09 neadmi	n (oman-demo)	neadmin)	~	ZUDI, Aridy (d	man-demovandy Azubi)	User(user)	Kennwolt zurücksetzen	
10.03	3.2015 10.3	0.09 neadmi	n (oman-demo)	neadmin)		aba, Ali (oma	n-demoval Baba)	User(user)	Kennwolt zurücksetzen	
10.03	3.2015 16.5	0.09 headmi	n (oman-demo)	neadmin)		acri, Kiara (o	(Ordernovkiara bach)	User(user)	Kennwolt zurücksetzen	
10.03	3.2015 103	o.us neadmi	(oman-demo)	neaumin)		aer, Jonannes	s (oman-demo Jonannes Baer)	User(user)	Kennword Zurücksetzen	
10.03	3.2015 163	0.09 neadmi	n (oman-demo\	neadmin)	8	aer, Roy (8m	an-demokoy baerj	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:	ou.ug neadmi	n (oman-demo\	neadmin)	8	aem, Al (8ma	in-demoval Baem)	User(user)	Kennwort zurucksetzen	
10.03	3.2015 16:	0:09 neadmi	n (oman-demo)	neadmin)	8	aiken, Don R	(8man-demo\Don R. Balken)	User(user)	Kennwort zurücksetzen	
10.03	3.2015 16:	0:09 neadmi	n (oman-demo)	neadmin)	B	ecner, Joe Ki	urt (sman-demouoe Kurt Becher)	User(user)	Kennwort zurücksetzen	
5 10.03	3.2015 16:	0:09 neadmi	n (8man-demo)	neadmin)	B	erter, Walter	(8man-demo\Walter Beiter)	User(user)	Kennwort zurücksetzen	<u> </u>
	F 1	Configuration	Ereignisse	Filter Ko	nfiguration (+)		: ((2

Öffnen Sie den Report in Excel. Auf dem Tabellenblatt "Ereignisse" listet der Report die Passwort-Rücksetzungen auf.

5.5 AD Logga Ereignisse mit dem Logbuch auswerten

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga aufgezeichnete Ereignisse können Sie mit den Reportfunktionen detailliert und wiederkehrend analysieren. Schneller beantworten Sie konkrete Fragen zu AD-Änderungen mit der Logbuchansicht.

Weiterführende Services

Änderungen im Active Directory überwachen Temporäre Gruppenmitgliedschaften erkennen Gesperrte Benutzerkonten identifizieren Kennwortrücksetzungen überwachen Alarme für Gruppen anlegen Alarme für Nutzerkonten anlegen

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Logbuch".
- 2. Legen Sie den Zeitraum für die Logbuch-Analyse fest.
- 3. Über die Filter fokussieren Sie auf die Events, die Sie prüfen möchten.
- 4. Selektieren Sie alle Ereignisse eines Tages (eine Zeile).

- 1. Selektieren Sie eine Zelle (einen Ereignistyp), um Ihre Abfrage weiter einzugrenzen.
- 8MAN zeigt eine Liste aller gewählten Ereignisse. An dem "Fußspuren-Symbol" erkennen Sie vom AD Logga aufgezeichnete Ereignisse. Selektieren Sie ein Ereignis.
- 3. 8MAN zeigt alle Details zum Ereignis.

SUMAN Suba Suba Suba Suba Subaba Mathrachauswald Lagdout Subaba Su						
	8M/	4N		🛇 Suche	🌩 cra-	
Logbuch Von 6.Monate zuor bis Heate Freing. 7. Oktober 2016 Repet 					⑧ Dashboard ☑ Mehrfachauswahl 邱 Logbuch ඟ Scanvergleich	
Image: Control of the second secon	Logbuch	Von <u>6 Monate</u>	zuvor bis <u>Heute</u>	Ø	Freitag, 7. Oktober 2016	Report +
Walk Kommentar uszgén W Alk Kommetar uszgén		4			A Filter 13	von 42
Mile 0.1.2.016 2 <t< th=""><th>۲</th><th>D Anderungen gesamt D Anderungen gesamt D Konto aktiviert D Anthoux geindert D Anthoux geindert D Anthoux geindert D Boultzer entsperit D Anthoux geindert</th><th> Competentiat Competentiat Seechigung painteet Logga Yordiguration Logga Status Medungen Appaintent Antilige Seentiges </th><th>8</th><th>X Alle Kommentare anargen V Alle Kommentare anargen O Zeit[*] Administrator (Rman-demol.Administrator) Administrator (Rman-demol.Administrator) 1312 cradmin (Rman-demol.Administrator) 1242 cradmin (Rman-demol.cradmin) 1240 cradmin (Rman-demol.cradmin)</th><th>tionsproze</th></t<>	۲	D Anderungen gesamt D Anderungen gesamt D Konto aktiviert D Anthoux geindert D Anthoux geindert D Anthoux geindert D Boultzer entsperit D Anthoux geindert	 Competentiat Competentiat Seechigung painteet Logga Yordiguration Logga Status Medungen Appaintent Antilige Seentiges 	8	X Alle Kommentare anargen V Alle Kommentare anargen O Zeit [*] Administrator (Rman-demol.Administrator) Administrator (Rman-demol.Administrator) 1312 cradmin (Rman-demol.Administrator) 1242 cradmin (Rman-demol.cradmin) 1240 cradmin (Rman-demol.cradmin)	tionsproze
W1 W1 <td< td=""><td>Mo 05.12.2016</td><td>2</td><td>2</td><td></td><td>S N 12:40 cradmin (8man-demo\cradmin)</td><td></td></td<>	Mo 05.12.2016	2	2		S N 12:40 cradmin (8man-demo\cradmin)	
com 0.11.2016 3 1 2 1 1 2 1 1 2 1 1 2 1 <td< td=""><td>Pr 02.12.2016</td><td>4</td><td>4</td><td></td><td>Sa 🔊 🕼 12:40 cradmin (8man-demo\cradmin)</td><td></td></td<>	Pr 02.12.2016	4	4		Sa 🔊 🕼 12:40 cradmin (8man-demo\cradmin)	
Bit 2911 2016 3 1 2 1 2 1 2 1 1 2 1 <	Mi 30.11.2016	3	3		Section 22:40 cradmin (8man-demo\cradmin)	
Mile 21.12016 20 4 4 1 12.00 cadmin (Bman-demo)(cadmin) V2.112016 4 4 4 4 4 1 12.00 cadmin (Bman-demo)(cadmin) V2.112016 4 <td>Di 29.11.2016</td> <td>3 1</td> <td>1 2</td> <td></td> <td>readmin (oman-demo)cradmin)</td> <td></td>	Di 29.11.2016	3 1	1 2		readmin (oman-demo)cradmin)	
01 2.1.1 2016 6 2 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	Mi 23.11.2016	20	6 14			
Ma 21.12016 4 S 191.2016 5 S 19 S 10.2016 5 S 1 S 1 S 1 S 1 S 1 S 1 S 1 S 1 S 1 S 1	Di 22.11.2016	6	2 4		aradmin (8man-demo\cradmin)	
Sa 13.12016 6 6 6 14.12016 1 1 6 6 14.12016 1 1 1 6 6 14.12016 1 1 1 1 1 1 11.12016 1 1 1 1 1 1 1 11.12016 1	Mo 21.11.2016	4	4			
fr 18.12016 0	Sa 19.11.2016	6	6		4	
Ma 14.120/6 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	Fr 18.11.2016	10	10			
A D Loga Gri Fman-demolcal A AD Loga Gri Fman-demolcal Andersong durch Administrator (Eman-demolcal) Mil 05102016 0 2 05102016 2 1 05102016 2 2 1 Mil 03802016 7 5 2 1 Mil 03802016 2 2 1 2 Bereich ein- box: ausklappen Bereich ein- box: ausklappen Bereich ein- box: ausklappen C Neuseter Scan> * 0 *	Nio 14.11.2016	8 4	4		😵 Gruppenmitgliedschaft geändert	
Image: Construction And enung durch & deministrator (Bman-demo) & deminist	Mo 10.10.2016	34 22	12	3	AD Logga für 8man-demo.local	
De 06.102016 0 C 2 3 1 1 2 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C 2 C	Fr 07.10.2016	42 3 1 6 1 13 3	3 11 3 1		Änderung durch Administrator (8man-demo\Administrator):	
Mi 05.102.016 0 2 3 3 1 1 3 0 Mi 26.5102.016 7 5 2 2 1 2 0 Mi 27.07.2016 2 2 2 1 2 2 1 0 Di 26.07.2016 3 2 1 2 1 0 Bereich ein- box: ausKappen Bereich ein- box: ausKappen	Do 06.10.2016	8	8		Comparentialitat (Chara Admin (Perce Admin) Chara Admin) in (Demotran Admin) kine and first	
Mi 28.02016 7 5 2 2 4 2 1 5 5 2 2 5 7 7 5 5 2 2 5 7 7 5 5 7 7 5 5 7 7 5 7 7 5 7 7 7 5 7	Mi 05.10.2016	10 2 3	1 1 3		or oppositive second resolution of the second	
Mi 0.0.02016 N2 4 2 1 5 2.707.2016 3 2 1 2 Di 2.607.2016 3 2 1 1 Bereich ein-box, ausklappen Bereit	Mi 28.09.2016	7 5	2			
MI 27.07.2016 2 2 Di 26.07.2016 3 2 1 Bereich ein- box. ausklappen Bereit BMAN-DEMOLOCAL → O B Orleuster Scan → O A	Mi 03.08.2016	12 4 2	1 5			
Bereich ein- bow, ausklappen Bereit BMAN-DEMOLOCAL V O B Orlevester Scan V O 🖄	Mi 27.07.2016	2	2			
	Bereit				Bereich ein- bzw. ausklappen	4
	Bereit				owiaix-DEMOLOCAL V U Bo Vieuester Scan> V U	<u> </u>

5.6 Die letzten Aktionen an einem Nutzerkonto oder einer AD Gruppe identifizieren

Hintergrund / Mehrwert

Nutzerkonten und Gruppen haben eine eigene Historie. Deshalb macht es Sinn, vor der weiteren Bearbeitung zu prüfen, was vorher durchgeführte Aktivitäten waren.

8MAN zeigt in einer Schnellansicht die letzten Aktivitäten oder Sie gelangen direkt in das Logbuch, um eine vollständige Auflistung zu erhalten.

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Accounts".
- Suchen Sie nach dem gewünschten Nutzer oder der gewünschten Gruppe.



An dem Notizzettel-Symbol erkennen Sie, dass Aktivitäten im 8MAN Logbuch aufgezeichnet sind. Fahren Sie mit dem Mauszeiger über das Symbol, um eine Kurzübersicht der letzten Aktivitäten zu erhalten, die an dem Account durchgeführt wurden.



Klicken Sie mit rechts auf das gewünschte Objekt und wählen dann "Öffne Logbuch", um alle aufgezeichneten Informationen zu erhalten.

			Peter (Orean dame)	(
		eter.Sille)	Peter (8man-demo\	Kommentare fur: Sille
		😵 Kennwort zurückgesetzt	37	🕰 Filter
		AD Logga für 8man-demo.local		O Nur meine
		Anderung durch <u>neadmin (8man-demo\neadmin)</u> :		₩ Datum/Uhrzeit▼
		(and the first part of the part of the second s	neadmin (8man-demo\r ^	R 10.03.2015 16:50
		vennwort für benutzer <u>Sille, Peter (oman-demo\PeterSille)</u> ' erfolgreich zurückgesetzt	SRV-EXCHANGE13 (8ma	
			SRV-EXCHANGE13 (8ma	S # 02.10.2014 11:34
			SRV-EXCHANGE13 (8ma	S # 02.10.2014 11:34
md (8man-demo\L_D			SRV-EXCHANGE13 (8ma	S # 02.10.2014 11:34
ertneb_md)			SRV-EXCHANGE13 (8ma	S # 25.09.2014 16:12
6 P (2)			SRV-EXCHANGE13 (8ma	10 25.09.2014 16:12
			SRV-EXCHANGE13 (8ma	16:12
			SRV-EXCHANGE13 (8ma	
			SRV-EXCHANGE13 (8ma	§ Ø 25.09.2014 09:53
			SRV-EXCHANGE13 (8ma	§ Ø 25.09.2014 09:53
			SRV-EXCHANGE13 (8ma	§ Ø 25.09.2014 09:53
			SRV-EXCHANGE13 (8ma	関 💕 25.09.2014 09:53
			SRV-EXCHANGE13 (8ma	関 💕 25.09.2014 09:53
			SRV-EXCHANGE13 (8ma	Image: March 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,
			SRV-EXCHANGE13 (8ma	Image: March 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10
			SRV-EXCHANGE13 (8ma	Image: March 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10
			SRV-EXCHANGE13 (8ma	
			SRV-EXCHANGE13 (8ma	
			SRV-EXCHANGE13 (8ma	
			cradmin >	22 11 2013 15:11
	Hinzufügen		gen	Bitte einen Kommentar eintra
	Abbreaker			

Prüfen Sie die am Objekt bereits durchgeführten Aktivitäten. Sie können einen Kommentar in das Logbuch schreiben. An dem "Fußspuren-Symbol" erkennen Sie, dass die Ereignisse vom AD Logga aufgezeichnet wurden.

8MAN

| 41

6 Alarme konfigurieren

8MAN Konfiguration	Version:				×	In der Kategorie "Alarme"
	Serverstatus Lizenzinformationen Angemeldete Benutzer: 1	48 Scans 2 1 Reporte	Jobs Übersicht 22 Änderungen 31 Weitere	Kollektor Konfigurat 1 Verbunden 1 Insgesamt konfiguriert	en Ion	aktivieren und deaktivieren Sie die Alarm-Sensoren.
	Lizenziert	4 Geplant 58 Erfolgreich 4	0 Ausführung 40 Fehlgeschlagen	Alle Kollektoren sind betriebsbereit		Sie Alarme für <u>Gruppen</u> oder
	A, Filter			1	12	<u>Nutzerkonten</u> anlegen.
	Scans Ressourcerionfigurationen, Logga, Fleserver CSV Import Res	Open Order Open Order- sourcenbeschreibungen	Benutzerverwaltun Rollenverwaltung	ung Data Owner g. Organisationstategorien, Data Owner, Ressourcen, Zustätliche Group Wizard Einstellungen		verwalten Sie angelegte Alarme.
	Lizenz Lizenz Serverstatus	Jobübersicht Isstatus, Jobkategorien	Kollektoren 8MAN Kollektorenübersi -konfiguration	Alarmkonfiguration Activiete Alarm Sensoren		Sie benötigen eine <u>Lizenz</u> für die 8MATEs FS Logga oder AD Logga.
	Ändern-Konfiguration Anni Adgereich Anni Anderurgerintellungen, 10	sichten & Reporte chien & Reporte, Blacklist r Ansichten & Reporte	Server GrantMA, Kommentare, Datenstandspeicher Server-Gesundheitschei	E-Mal, k; Se.		
Bereit					demosdmin @ localhost 🕤 🏄	



6.1 AD-Logga Alarmsensoren aktivieren/deaktivieren



- Aktivieren/Deaktivieren Sie die Alarmsensoren.
 - 2. Sie müssen einen Kommentar angeben.
 - 3. Übernehmen Sie die Einstellungen.

Nur mit aktiven Alarmsensoren sind die Alarmkonfigurationen wirksam.

8MAN

6.2 Alarme für Gruppen anlegen

Hintergrund / Mehrwert

Über Gruppenmitgliedschaften erhalten Mitarbeiter ihre Zugriffsrechte im Firmennetzwerk. Besonders schützenswerte Gruppen verleihen ihren Mitgliedern Rechte auf geheime Ordner und wichtige Ressourcen. Mit dem im 8MATE AD Logga können Sie AD Gruppen aktiv überwachen und sollten neue Mitglieder hinzugefügt werden, einen Alarm auslösen.

Die Gruppenverschachtelungen im Active Directory machen es notwendig, auch Gruppenmitgliedschaften zu überwachen, die sich aus neuen, indirekten Mitgliedschaften ergeben. Ein Beispiel: Die Gruppe "Geschäftsführer" wird überwacht und hat als Mitglied die Gruppe "geheime Daten". 8MATE AD Logga Alarme benachrichtigen Sie jetzt auch, wenn der letztgenannten Gruppe neue Mitglieder oder Gruppen hinzugefügt bzw. entfernt werden.



Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen <u>M</u> <u>2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle</u> sowie <u>M 4.312 Überwachung von</u> <u>Verzeichnisdiensten</u>.

Weiterführende Services

<u>Alarmsensoren aktivieren/deaktivieren</u> <u>Alarme für Nutzerkonten anlegen</u> <u>Alarme verwalten</u>

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Accounts".
- 2. Finden Sie die gewünschte Gruppe mit der Suchfunktion.
- 3. Rechtsklicken Sie die Gruppe und wählen "Alarm anlegen" im Kontextmenü.



- 1. Geben Sie dem Alarm einen Namen.
- 2. Aktivieren Sie die Checkbox, um auch über indirekte Änderungen an den Gruppenmitgliedschaften informiert zu werden.
- 3. Sie können beliebig viele E-Mail-Empfänger hinterlegen. Darüber hinaus kann der Alarm auch in die Windows Ereignisanzeige geschrieben werden.
- 4. Sie müssen einen Kommentar hinterlegen.
- 5. Aktivieren Sie den Alarm.

6.3 Alarme für Nutzerkonten anlegen

Hintergrund / Mehrwert

Mit dem 8MATE AD Logga überwachen Sie den Prozess des Kennwortrücksetzens. Diesem ist ein Sicherheitsrisiko inhärent. Setzt beispielsweise ein Helpdesk-Mitarbeiter heimlich das Passwort einer Führungskraft zurück, kann er mit dem Übergangspasswort sich anmelden und geheime Daten einsehen. In diesem Fall sind bei aktivierter Alerts Funktion die kontrollierenden Instanzen informiert.



Dieser Service ist BSI-relevant. Beachten Sie die Anforderungen und Prüffragen der Maßnahmen <u>M</u> 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle sowie <u>M 4.312 Überwachung von</u> <u>Verzeichnisdiensten</u>.

Weiterführende Services

Alarmsensoren aktivieren/deaktivieren Alarme für Gruppen anlegen

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Accounts".
- 2. Finden Sie den gewünschten Benutzer mit der Suchfunktion.
- 3. Rechtsklicken Sie den Benutzer und wählen "Alarm anlegen" im Kontextmenü.

- EMAN

 Statt

 Statt

 Statt

 Statt

 Statt

 </table
- 1. Geben Sie dem Alarm einen Namen.
- 2. Wählen Sie ein Ereignis, über das Sie informiert werden.
- 3. Sie können beliebig viele E-Mail-Empfänger hinterlegen. Darüber hinaus kann der Alarm auch in die Windows Ereignisanzeige geschrieben werden.
- 4. Sie müssen einen Kommentar hinterlegen.
- 5. Aktivieren Sie den Alarm.

6.4 Alarme verwalten

Hintergrund / Mehrwert

Sie können gesetzte Alarme jederzeit anpassen. Die Verwaltung erfolgt auf der 8MAN Startseite.

Weiterführende Services

Alarmsensoren aktivieren/deaktivieren

Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Start".
- 2. Wählen Sie "Alarme verwalten".

						7
tatus	Name 🔺	Ressource		Ereignis	Schwellenwert	Aktion
~	"C-Level" Gruppenmitgliedschaften geändert (8man- demo\C-Level)	C-Level (8man-demo\C-Level)	ጼ	Gruppenmitgliedschaften geändert		E-Mail senden Schreiben in die Windows B
	"Domänen-Admins" Gruppenmitgliedsch. geändert	Domänen-Admins (8man-demo\Domänen-Admins)	ஃ	Gruppenmitgliedschaften geändert		E-Mail senden Skript ausführen
~	Berechtigungsänderungen am Verzeichnis für Vertrieb	\\srv-8man\Vertrieb		Änderungen im Verzeichnis		E-Mail senden
~	Kennwort zurückgesetzt für Krise, Christiane	Krise, Christiane (8man-d\Christiane.Krise)	ሔ	Kennwort zurückgesetzt		E-Mail senden Schreiben in die Windows I
~	Konto gesperrt für Krise, Christiane (8man-demo \Christiane.Krise)	Krise, Christiane (8man-d\Christiane.Krise)	為	Konto gesperrt		E-Mail senden Schreiben in die Windows I
~	Mögliche Virusattacke auf dem Fileserver für srv-8man	\\srv-8man		Änderungen auf dem Fileserver	1000x / 20s	E-Mail senden Skript ausführen
~	Möglicher Datendiebstahl auf dem Fileserver für srv-8man	\\srv-8man Aktivieren		Änderungen auf dem Fileserver	5000x / 5m	E-Mail senden
t		atus Name V Level ² Gruppenmitgliedschaften geändert (Bman- demol/c-Level) "Domänen-Admins" Gruppenmitgliedsch: geändert Berechtigungsänderungen am Verzeichnis für Vertrieb Kennwort zurückgesetzt für Krise, Christiane Konto gespert für Krise, Christiane (Bman-demo /Christiane.Krise) Mögliche Virusattacke auf dem Fileserver für srv-Bman / Mögliche Datendiebstahl auf dem Fileserver für srv-Bman	atus Name Ressource 'Clevel' Gruppenmitgliedschaften geändert (Bman- demol/C-Level) C-Level (Bman-demol/C-Level) 'Domänen-Admins' Gruppenmitgliedsch. geändert Domänen-Admins (Bman-demol/C-Level) 'Berechtigungsänderungen am Verzeichnis für Vertrieb Nanv-Bman/Vertrieb Kennwort zurückgesetzt für Krise, Christiane Krise, Christiane (Bman-d/Christiane-Krise) Konto gespert für Krise, Christiane (Bman-demolychristiane-Krise) Krise, Christiane (Bman-d/Christiane-Krise) Mögliche Virusattacke auf dem Fileserver für srv-8man Varv-8man Mögliche Totendiebstahl auf dem Fileserver für srv-8man Varv-8man	atus Name Ressource ''Level' Gruppenmitgliedschaften geändert (Bman- demol/C-Level) A ''Domänen-Admins' Gruppenmitgliedsch. geändert Domänen-Admins (Bman-demol/Domänen-Admins) Berechtigungsänderungen am Verzeichnis für Vertrieb Visrv-Bman/Vertrieb Kennvort zurückgesetzt für Krise, Christiane Krise, Christiane (Bman-d./Christiane.Krise) Konto gespert für Krise, Christiane (Bman-demo Christane.Krise) Megliche Virusattacke auf dem Fileserver für srv-Bman Mögliche Varusattacke auf dem Fileserver für srv-Bman Visrv-Bman	atus Name Ressource Ereignis ''Leverl' Gruppenmitgliedschaften geändert (Bman- demol/C-Level) A Gruppenmitgliedschaften geändert ''Domänen-Admins' Gruppenmitgliedsch geändert Domänen-Admins' Gruppenmitgliedschaften geändert Scruppenmitgliedschaften geändert Berechtigungsänderungen am Verzeichnis für Vertieb Visn-®man/Vertieb Image: Administration of the component of	Attus Name Ressource Ereignis Schwellenwert V:Clevell Gruppenmitgliedschaften geändert (Bman- demolC-Level) Gruppenmitgliedschaften geändert C-Level (Bman-demolC-Level) Gruppenmitgliedschaften geändert Domänen-Admins' Gruppenmitgliedschaften geändert V:Domänen-Admins' Gruppenmitgliedschaften geändert Domänen-Admins (Bman-demolDomänen-Admins) A Gruppenmitgliedschaften geändert V:Domänen-Admins' Gruppenmitgliedschaften geändert Domänen-Admins (Bman-demolDomänen-Admins) A Gruppenmitgliedschaften geändert V:Sonwort zurückgesett für Krise, Christiane Krise, Christiane (Bman-d)./Christiane.Krise) A Kennwort zurückgesetzt V:Mogliche Virusattacke auf dem Fileserver für sn-8man Krise, Christiane (Bman-d)./Christiane.Krise) A Konto gesperrt V:Mogliche Virusattacke auf dem Fileserver für sn-8man Virus-8man Adtriveren Anderungen auf dem Fileserver 1000x / 20s Mögliche Virusattacke auf dem Fileserver für sn-8man Virus-8man Anterungen auf dem Fileserver 5000x / 5m

× 8MAN zeigt Ihnen alle Alarmkonfigurationen.

- 1. Suchen Sie nach einer Alarmkonfiguration.
- 2. Schalten Sie Alarme ein oder aus.
- 3. Mit Rechtsklick oder den Links löschen, bearbeiten oder aktivieren/deaktivieren Sie die selektierte Alarmkonfiguration.

7 Den 8MAN Support kontaktieren

Sie erreichen unseren Support

per Telefon +49 30 390 6345-99 Montag bis Freitag von 9.00 bis 17.00 Uhr.

per E-Mail support@8man.com

per Website

https://susi.8man.com

Sie starten auf der Website mit einer Selbstregistrierung. Nach Abschluss können Sie die öffentlich zugänglichen Inhalte sehen.

Nach der Registrierung werden Sie durch unseren Support einer Berechtigungsebene zugeordnet. Erst dann können Sie nicht-öffentliche Inhalte sehen und das Ticketsystem nutzen.

Dieser Vorgang kann etwas Zeit in Anspruch nehmen.

8MAN

8 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

8MAN ist eine geschützte Bezeichnung für ein Programm und die entsprechenden Dokumente, dessen Urheberrechte bei Protected Networks GmbH liegen.

Marken und geschäftliche Bezeichnungen sind – auch ohne besondere Kennzeichnung – Eigentum des jeweiligen Markeninhabers.

Protected Networks GmbH Alt-Moabit 73 10555 Berlin

+49 30 390 63 45 - 0 www.protected-networks.com www.8man.com

9 Software-Lizenzvereinbarungen

- Json.net, © 2006-2014 Microsoft, <u>https://json.codeplex.com/license</u>
- JSON.NET Copyright (c) 2007 James Newton-King <u>https://github.com/JamesNK/Newtonsoft.Json/blob/master/LICENSE.md</u>
- Irony Copyright (c) 2011 Roman Ivantsov http://irony.codeplex.com/license
- Jint Copyright (c) 2011 Sebastien Ros http://jint.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, installed on the computer on which the FS Logga for Windows file servers is installed: C:\Program Files\protected-networks.com\8MAN\driver (Usage only for FS Logga for Windows file server)
- NetApp Manageability SDK, © 2013 NetApp, <u>https://communities.netapp.com/docs/DOC-1152</u> (Usage only for FS Logga for NetApp Fileserver)
- WPF Shell Integration Library 3.0.50506.1, © 2008 Microsoft Corporation , <u>http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx</u>
- WPF Toolkit Library 3.5.50211.1, © Microsoft 2006-2013, <u>http://wpf.codeplex.com/license</u>
- WpfAnimatedGif, © Copyright 2012-2017 Thomas Levesque, <u>https://github.com/XamlAnimatedGif/WpfAnimatedGif/blob/master/LICENSE.txt</u>
- Bootstrap, © 2011-2016 Twitter, Inc, <u>https://github.com/twbs/bootstrap/blob/master/LICENSE</u>
- jQuery, © 2016 The jQuery Foundation, <u>https://jquery.org/license</u>
- jquery.cookie, © 2014 Klaus Hartl, <u>https://github.com/carhartl/jquery-cookie/blob/master/MIT-LICENSE.txt</u>
- jquery-tablesort, © 2013 Kyle Fox, https://github.com/kylefox/jquery-tablesort/blob/master/LICENSE
- LoadingDots, © 2011 John Nelson, <u>http://johncoder.com</u>
- easyModal.js, © 2012 Flavius Matis, https://github.com/flaviusmatis/easyModal.js/blob/master/LICENSE.txt
- jsTimezoneDetect, © 2012 Jon Nylander
 <u>https://bitbucket.org/pellepim/jstimezonedetect/src/f9e3e30e1e1f53dd27cd0f73eb51a7e7caf7b378/LICENCE.txt?</u>
 <u>at=defaultjquery-tablesort</u>
- Sammy.js, © 2008 Aaron Quint, Quirkey NYC, LLC <u>https://raw.githubusercontent.com/quirkey/sammy/master/LICENSE</u>
- Mustache.js, © 2009 Chris Wanstrath (Ruby), © 2010-2014 Jan Lehnardt (JavaScript) and © 2010-2015 The mustache.js community <u>https://github.com/janl/mustache.js/blob/master/LICENSE</u>
- Metro UI CSS 2.0, © 2012-2013 Sergey Pimenov, https://github.com/olton/Metro-UI-CSS/blob/master/LICENSE
- Underscore.js, © 2009-2016 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors <u>https://github.com/jashkenas/underscore/blob/master/LICENSE</u>
- Ractive.js, © 2012-15 Rich Harris and contributors, https://github.com/ractivejs/ractive/blob/dev/LICENSE.md
- RequireJS, © 2010-2015, The Dojo Foundation, https://github.com/jrburke/requirejs/blob/master/LICENSE
- typeahead.js, © 2013-2014 Twitter, Inc, <u>https://github.com/twitter/typeahead.js/blob/master/LICENSE</u>
- Select2, © 2012-2015 Kevin Brown, Igor Vaynberg, and Select2 contributors <u>https://github.com/select2/select2/blob/master/LICENSE.md</u>
- bootstrap-datepicker, © Copyright 2013 eternicode <u>https://github.com/eternicode/bootstrap-datepicker/blob/master/LICENSE</u>
- RabbitMQ, © Copyright 2007-2013 GoPivotal, https://www.rabbitmq.com/mpl.html

• EPPlus, JanKallman, <u>https://github.com/JanKallman/EPPlus/blob/master/LICENSE</u>