# ASA 8.2: Konfigurieren von Syslog mithilfe von ASDM

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Grundlegende Syslog-Konfiguration mithilfe von ASDM Protokollierung aktivieren Protokollierung deaktivieren Anmelden bei einer E-Mail Anmeldung bei einem Syslog-Server Erweiterte Syslog-Konfiguration mit ASDM Arbeiten mit Ereignislisten Arbeiten mit Protokollierungsfiltern Übertragungsratenlimit Protokollieren der Hits einer Zugriffsregel Konfigurieren Konfigurationen Überprüfen Fehlerbehebung Problem: Verbindung unterbrochen — Syslog-Verbindung beendet — Lösung Echtzeitprotokolle auf Cisco ASDM können nicht angezeigt werden. Lösung Zugehörige Informationen

# **Einführung**

Dieses Dokument enthält Informationen zum Konfigurieren von Syslog auf der Cisco Adaptive Security Appliance (ASA) 8.x mithilfe der ASDM-GUI (Adaptive Security Device Manager). Systemprotokollmeldungen sind Meldungen, die von der Cisco ASA generiert werden, um den Administrator über Änderungen an der Konfiguration, Änderungen in der Netzwerkeinrichtung oder Änderungen an der Geräteleistung zu informieren. Durch die Analyse der Systemprotokollmeldungen kann ein Administrator den Fehler problemlos beheben, indem er eine Ursachenanalyse durchführt.

Syslog-Meldungen werden hauptsächlich anhand ihres Schweregrads differenziert.

- 1. Schweregrad 0 Notrufe Ressource ist nicht verwendbar
- 2. Schweregrad 1 Warnmeldungen Sofortige Maßnahmen sind erforderlich
- 3. Schweregrad 2 Kritische Nachrichten Kritische Bedingungen
- 4. Schweregrad 3 Fehlermeldungen Fehlerbedingungen
- 5. Schweregrad 4 Warnmeldungen Warnbedingungen
- 6. Schweregrad 5 Benachrichtigungsmeldungen Normale, aber wesentliche Bedingungen
- 7. Schweregrad 6 Informationsmeldungen Nur Informationsmeldungen
- 8. Schweregrad 7 Debugging-Meldungen Nur Debugging-Meldungen**Hinweis:** Der höchste Schweregrad ist ein Notfall, der niedrigste Schweregrad ist das Debuggen.

Hier sehen Sie Beispiele für Syslog-Meldungen, die von der Cisco ASA generiert wurden:

- %ASA-6-106012: IP-Adressen von IP\_Adresse zu IP\_Adresse verweigern, IP-Optionen Hexadezimalziffer
- %ASA-3-211001: Speicherzuweisungsfehler
- %ASA-5-335003: Anwendung der NAC-Standardzugriffskontrollliste, ACL:ACL-Name -Hostadresse

Der in "%ASA-X-YYYYYY:" angegebene numerische Wert X gibt den Schweregrad der Nachricht an. Beispiel: "%ASA-6-106012" ist eine Informationsmeldung und "%ASA-5-335003" ist eine Fehlermeldung.

## Voraussetzungen

#### <u>Anforderungen</u>

Für dieses Dokument bestehen keine speziellen Anforderungen.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA Version 8.2
- Cisco ASDM Version 6.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

## Grundlegende Syslog-Konfiguration mithilfe von ASDM

## Protokollierung aktivieren

1. Wählen Sie *Configuration > Device Management > Logging > Logging Setup* aus, und markieren Sie die Option *Enable* 

ging.	
isco ASDM 6.2 for ASA - 10.78.177.11	
View Tools Wizards Window Help	۶ 
Home 🖧 Configuration 🕢 Monitorine	2 🔚 Save 💽 Refresh 💽 Back 🔘 Forward 🧳 Help
Device Management 🗗 🖗 🗡	Configuration > Device Management > Logging > Logging Setup
Management Access     Licensing     Logping     L	Enable logging <ul> <li>Enable logging on the failover standby unit</li> <li>Send debug messages as syslogs</li> <li>Send syslogs in EMBLEM format</li> </ul> <li>Logging to Internal Buffer         <ul> <li>Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.</li> <li>Buffer Size:                 <ul> <li>1096</li> <li>bytes</li> <li>You can choose to save the buffer contents before the buffer is overwritten.</li> <li>Save Buffer To:</li> <li>FTP Server</li> <li>Configure FTP Settings</li> <li>Flash</li> <li>Configure Flash Usage</li> </ul> </li> </ul> </li> <li>ASDM Logging         <ul> <li>Specify the size of the queue for syslogs intended for viewing in ASDM.</li> <li>Queue Size:</li></ul></li>
	So ASDM 6.2 for ASA - 10.78.177.11 View Tools Wizards Window Help Home Configuration Monitoring Device Management Access Management Access System Image/Configuration Coging Configuration Coging Setup Configuration Coging Filters Rate Limit Systog Servers Systog Servers Sy

2. Sie können die Syslog-Meldungen in einem internen Puffer speichern, indem Sie die Puffergröße angeben. Sie können den Pufferinhalt auch in Flash-Speicher speichern, indem Sie auf *Flash Usage* konfigurieren und die Flash-Einstellungen

	Configuration > Device Management	nt > Logging > Logging Setup
	🖓 Enable logging	F Enable logging on the failover standby unit
	F Send debug messages as syslogs	Send syslogs in EMBLEM format
	Logging to Internal Buffer Specify the size of the internal buffer Buffer Size:	er to which syslogs will be saved. When the buffer fills up, it will be overwritten. bytes
	You can choose to save the buffer of	contents before the buffer is overwritten.
	Save Buffer To: 🔽 FTP Server	Configure FTP Settings
	( Flash	Configure Flash Usage
	ASDM Logging	
	Specify the size of the queue for sy	sinos intended for viewon in ASDM.
	Queue Size: 100	tonligure Logging Flash Usage
		Specify the maximum space that logging can use on the flash.
		Maximum Flash to Be Used by Logging: 1024 KB
		Specify the minimum free space that logging will preserve on the flash.
		Minimum Free Space to Be Preserved: 3076 KB
		OK Carcel Help
definieren.		

3. Pufferte Protokollmeldungen können an einen FTP-Server gesendet werden, bevor sie überschrieben werden. Klicken Sie auf *FTP-Einstellungen konfigurieren*, und geben Sie die FTP-Serverdetails an, wie hier

I✓ Enable logging		Enable logging on the failover standby unit
🔲 Send debug me	ssages as syslogs	Send syslogs in EMBLEM format
Logging to Internal Bu	,ffer	
Specify the size (	of the internal buffe	r to which syslogs will be saved. When the buffer fills up, it will be overwr
Buffer Size:	4096 b	bytes
You can choose t	o save the buffer o	optents before the tuffer is overwritten
Shup Differ Tou	E ETD Convert	Configure STD Sattings
Save Burrer 10:	P FIF Server	Consigure PTP Seconds
	l Flash	Configure Flash Usage
ASDM Logging		
Specify the size of	of the queue for s	te Configure FTP Settings
Queue Size: 100	Die de la companya de	🔽 Enable FTP client
		Server IP Address: 172.16.18.10
		Path:
		Licensmet Party ser
		e d Assesse
		Password:

#### Protokollierung deaktivieren

Sie können bestimmte Syslog-IDs je nach Ihren Anforderungen deaktivieren.

**Hinweis:** Durch Aktivieren des Kontrollkästchens für die Option *Zeitstempel in Syslogs einschließen* können Sie den Syslogs das Datum und die Uhrzeit hinzufügen, zu dem sie als Feld generiert wurden.

1. Wählen Sie die zu deaktivierenden Syslogs aus, und klicken Sie auf

Bearbeiten.				
Configuration > Device Management > Logging > Sysleg Setup				
Syslog Format Facility Code to Indude in Syslogs: 0.0CAL4(20)  Facility Code to Indude in Syslogs Folde IIP Setup				
Show: - All sysing IDs -	*			
Systog ID	Logging Level	Disabled		Edit
216001	Critical	No	-	·
218002	Critical	No		Restore Defaults
218003	Critical	No.		
218004	Critical	No.		
219002	Errors	No		
302003	Informational	No		
302004	Informational	No	-	
302009	Informational	No.		
302010	Informational	No .		
302012	Informational	No		
302013	Informational	No.		
302014	Informational	No		
302005	Informational	No <sup>1</sup>		
302016	Informational	No		
302017	Informational	No		
302018	Informational	No		

2. Aktivieren Sie im Fenster *Edit Syslog ID Settings (Syslog-ID-Einstellungen bearbeiten*) die Option *Disable messages (Nachrichten deaktivieren)*, und klicken Sie auf

	902015 302016	
Syslog IDs:		
🔽 þísable r	nessages	
Logging Leve	el: Informational	*

3. Die deaktivierten Syslogs können auf einer separaten Registerkarte angezeigt werden, indem Sie im Dropdown-Menü *Syslog-IDs* im *Syslog ID Setup*-Dropdown-Menü die Option *Disabled Syslog IDs* 

Configuration > Device Management > Logging > Syslog Setup			
Syslog Format			
Facility Code to Include in Syslogs: LOCAL4(20)			
Include timestamp in syslogs			
Triclude timestamp in syslogs			
Sysing ID Setup			
F Include timestamp in syslogs Syslog ID Setup Show: Disabled syslog IDs			
Drokude timestamp in syslogs  Syslog ID Setup Show: Disabled syslog IDs  Syslog ID	Lagging Level	Disabled	
Drokude timestamp in syslogs  Syslog ID Setup  Show: Disabled syslog IDs  Syslog ID  302015	Logging Level Enformational	Disabled Yes	1

## Anmelden bei einer E-Mail

Gehen Sie wie folgt vor, um die Syslogs mithilfe von ASDM an eine E-Mail zu senden:

 Wählen Sie Konfiguration > Gerätemanagement > Protokollierung > E-Mail-Einrichtung aus. Das Feld Quell-E-Mail-Adresse ist hilfreich, um eine E-Mail-ID als Quelle für die Syslogs zuzuweisen. Geben Sie die E-Mail-Quelladresse an. Klicken Sie jetzt auf Hinzufügen, um die E-Mail-Empfänger

nliguration > Device Management > Logging > E-Mail Setup		
Enter the e-mail address that will be used as the source address when syslogs are sent as e-mails.		
Source F-Mail Address: ) test 12 Mexanole.com		
and the state of t		
Nel Records		
tal Recipients	Syslog Severity	bba T
tal Recipients Destination E-Nail Address	Syslog Severity	Add
Mail Recipients Destination E-Mail Address	Syslog Severity	Add Ldr.

2. Geben Sie die *E-Mail-Zieladresse* an, und wählen Sie den *Schweregrad aus*. Je nach Schweregrad können Sie verschiedene E-Mail-Empfänger definieren. Klicken Sie auf *OK*, um zum Bereich *E-Mail-Setup* 

	(D		
	Destination E-Mail Add	ress: monitorsyslog@example.com	
	Filter the syslogs sent severity filter used for severity selected below recipients in Configura Filters.	to this recipient by severity. The syslog this recipient will be the higher of the w and the global filter set for all e-mail tion>Properties>Logging>Logging	
	Syslog Severity:	Errors	
		Emergencies	
	OK	Alerts	
		Errors	
		Warnings	
		Notifications	
		Informational	
rückzukehren.		Debugging	Daraus ergibt sich
gende			
onfiguration:			
infiguration > Device	Management > Logging > E	-Mail Setup	
Enter the e-mail address	that will be used as the source a	address when syslogs are sent as e-mails.	
Source E-Mail Address:	test123@example.com		
-Mail Recipients			
	Destination E-Mail A	address	Syslog Severity
monitorsyslog@example	com		Errors

3. Wählen Sie *Configuration > Device Setup > Logging > SMTP* aus, und geben Sie den SMTP-Server

an.		
Configuration > Device Manage	ement > Logging >	> <u>SMTP</u>
Configure the remote SMTP serve	er IP address for send	ding email alerts and notifications in response to select events.
Demote CMTD Conver		
Remote SMTP Server	·	
Primary Server IP Address:	172.18.10.20	
Secondary Server IP Address:		(Optional)

## Anmeldung bei einem Syslog-Server

Sie können alle Syslog-Meldungen an einen dedizierten Syslog-Server senden. Führen Sie diese Schritte mit ASDM durch:

1. Wählen Sie *Konfiguration > Gerätemanagement > Protokollierung > Syslog-Server* aus, und klicken Sie auf *Hinzufügen*, um einen Syslog-Server hinzuzufügen.

Configur	ation > Device Managemen	t > Logging > Syslog Servers				
Specify	up to 16 syslog servers. Make :	sure logging is enabled in Configuration	> Device Management > Logging > Loggin	p Setup.		
		and the second				
	Interface	(P Address	Protocol/Port	EMOLEM	Secure	Add
						Edit
						Pullitur
						Contract.

Das Fenster Syslog-Server hinzufügen wird angezeigt.

2. Geben Sie die Schnittstelle an, der der Server zugeordnet ist, sowie die IP-Adresse. Geben Sie die *Protokoll-* und *Port-*Details je nach Netzwerkeinrichtung an. Klicken Sie anschließend auf *OK*.**Hinweis:** Stellen Sie sicher, dass Sie über die Cisco ASA auf den Syslog-Server

nicen ace:	linside	<u> </u>
P Address:	172.16.11.10	00
Protocol:	C TCP	O UDP
Port:	514	_
Log mes	sages in Cisco	EMBLEM format (UDP

zugreifen können.

3. Der konfigurierte Syslog-Server wird wie hier gezeigt angezeigt. Änderungen können durchgeführt werden, wenn Sie diesen Server auswählen und dann auf *Bearbeiten* klicken.

6.11.100	UDP/514	No	No	_
				_
				100
				De
wed to be queued when a syslog	server is busy. Use 0 to indicate unimited of	sueue size.		
time on the descent success of and	and the or entry there is no it in the second to second the	for the second		
wed to be queued when a syslog	server is busy. Use 0 to indicate unlimited of	queue size.		
	wed to be surved when a svisiog	wed to be queued when a syslog server is busy. Use 0 to indicate unlimited	wed to be queued when a systog server is busy. Use 0 to indicate unimited queue size,	wed to be queued when a systog server is busy. Use 0 to indicate unimited queue size.

**Hinweis:** Aktivieren Sie die Option *Benutzerdatenverkehr zum Weiterleiten zulassen, wenn der TCP-Syslog-Server ausgefallen ist.* Andernfalls werden die neuen Benutzersitzungen über die ASA abgelehnt. Dies gilt nur, wenn das Transportprotokoll zwischen ASA und dem Syslog-Server TCP ist. Standardmäßig werden neue Netzwerkzugriffssitzungen von der Cisco ASA verweigert, wenn ein Syslog-Server aus irgendeinem Grund ausfällt.Informationen zum Definieren des Typs von Syslog-Meldungen, die an den Syslog-Server gesendet werden sollen, finden Sie im Abschnitt <u>Protokollierungsfilter</u>.

# **Erweiterte Syslog-Konfiguration mit ASDM**

## Arbeiten mit Ereignislisten

Mit Ereignislisten können wir benutzerdefinierte Listen erstellen, die die Gruppe von Syslog-Meldungen enthalten, die an ein Ziel gesendet werden sollen. Ereignislisten können auf drei verschiedene Arten erstellt werden:

- Nachrichten-ID oder Bereich der Nachrichten-IDs
- Schweregrad der Nachricht
- Message-Klasse

#### Nachrichten-ID oder Bereich der Nachrichten-IDs

Gehen Sie wie folgt vor:

 Wählen Sie Configuration > Device Management > Logging > Event Lists (Konfiguration > Gerätemanagement > Protokollierung > Ereignislisten) aus, und klicken Sie auf Add, um eine neue Ereignisliste zu

erstellen.			
Configuration > Device Management > Log	aina > Event Lists		0
Use event lists to define a particular set of sysk	ogs that you are interested in. The event list can be used to filter syslogs sent	to a logging destination.	
Name	Event Class / Severity	Message IDs	Add
			Edit
			Delete

2. Geben Sie im Feld *Name* einen Namen an. Klicken Sie im Bereich "*Nachrichten-ID-Filter" auf Hinzufügen*, um eine neue Ereignisliste zu

lass/Severity Filters			
indesty be reme; rincers		Message ID Filters	
vent Class Severity	Add	Message IDs	Add
	Edt		Edit
	Delete		Delete

3. Geben Sie den Bereich der Syslog-Nachrichten-IDs an. Hier sind beispielsweise die TCP-Syslog-Meldungen enthalten. Klicken Sie zum Abschließen auf

to the specified lev	el. Add Syslog Message ID Filter
Event Class/Severi	Enter the syslog message ID. Use hyphen to specify a range
Liferic Gidss	or systog IDs, for example, 101001-101010.
	Message IDs: 302013-302018
	OK Cancel Help

4. Klicken Sie erneut auf OK, um zum Fenster Ereignislisten

figuration > Device Management > Logging > Ev	int Lists	
se event lists to define a particular set of suslans that up	are interested in. The event list can be used to filter systems sent t	o a looping destination.
se orene is to corrie a particular sec or systems for	are not along in the event is carried area to the sprange serve	
Nane	Event Class / Severity	Message IDs

#### Schweregrad der Nachricht

1. Ereignislisten können auch anhand des Schweregrads der Nachricht definiert werden. Klicken Sie auf *Hinzufügen*, um eine separate Ereignisliste zu

auration > Device Management > Logging > Eve	ntLists		
e event lists to define a particular set of sysiogs that you	are interested in. The event list can be used to filter syslogs sent to	a logging destination.	
Name	Event Class / Severity	Message IDs	Add
p-conn-syslog		302013-302018	
			Ed
			m.L.L.

2. Geben Sie den Namen an, und klicken Sie auf

	🚰 Add Event List			×
	Name: syslog-sev-error Specify filters for the event list. You can filter represents the maximum level for logging me to the specified level.	r syslogs by their clas ssages. The ASA will f	s and severity, or by their IDs ilter system log messages with	. The severity level severity levels up
	Event Class/Severity Filters	Mess	age ID Filters	1 1
	Event Class Severity	-	Message IDs	Add
	Ec	5t		Ed‡
	Del	ete		Delete
Hinzufügen	OK	Cancel	Help s and Severity Filter All All Event Classes	
		Severity:	Errors	<b>Ξ</b>
		OK	Emergencies	
		UK	Critical	
			Errors Warnings Notifications Informational	
	dan Oaburana madala Esti	ОК	Debugging	

- 3. Wählen Sie den Schweregrad als Fehler aus.
- 4. Klicken Sie auf

epresents the max o the specified leve ivent Class/Severit	imum level for log sl. y Filters	iging messages. The ASA	will filter system log messages wi Message ID Filters	th severity le
Event Class	Severity	Add	Message IDs	Add
All	Errors	Edit		Edit
		Delete		Deeb

#### Message-Klasse

Ereignislisten werden auch basierend auf der Message Class konfiguriert. Eine Nachrichtenklasse

ist eine Gruppe von Syslog-Meldungen, die sich auf eine Sicherheitsanwendungsfunktion beziehen, mit der Sie eine ganze Nachrichtenklasse angeben können, anstatt für jede Nachricht einzeln eine Klasse anzugeben. Verwenden Sie z. B. die auth-Klasse, um alle Syslog-Meldungen auszuwählen, die mit der Benutzerauthentifizierung zusammenhängen. Einige verfügbare Nachrichtenklassen sind hier aufgeführt:

- Alle Alle Ereignisklassen
- auth Benutzerauthentifizierung
- Bridge Transparente Firewall
- ca PKI-Zertifizierungsstelle
- config Befehlsschnittstelle
- ha Failover
- ips Intrusion Protection Service
- IP IP-Stack
- np Netzwerkprozessor
- ospf OSPF-Routing
- RIP RIP-Routing
- Sitzung Benutzersitzung

Führen Sie diese Schritte aus, um eine Ereignisklasse zu erstellen, die auf der *vpnclient-errors*-Nachrichtenklasse basiert. Die Nachrichtenklasse *vpnc* kann alle Syslog-Meldungen kategorisieren, die sich auf den vpnclient beziehen. Der Schweregrad für diese Nachrichtenklasse wird als "Fehler" ausgewählt.

1. Klicken Sie auf Hinzufügen, um eine neue Ereignisliste zu

iguration > Device Management > Log	aina > Event Lists		
e event lists to define a particular set of sysk	igs that you are interested in. The event list can be used to filter syslogs sent to	a logging destination.	
Name	Event Cless / Seventy	Message IDs	66A
p-conn-syslog		302013-302018	
vslog-sev-error	All / Errors		Edit

2. Geben Sie den Namen an, der für die von Ihnen erstellte Nachrichtenklasse relevant sein soll, und klicken Sie auf

N	ame: vpnclient-er	rors			
St	pecify filters for the presents the maximum	e event list. Yo mum level for k	u can filter syslogs by their ogging messages. The ASA	r class and severity, or by their II will filter system log messages w	)s. The severity th severity leve
to Ev	the specified leve vent Class/Sevenit	il. y Filters ———		Message ID Filters	
	Event Class	Severky	Add	Message IDs	Add
			Edt		Edt
			Delete		Delete
				-	
				11	

3. Wählen Sie vpnc aus der Dropdown-Liste

specified leve	imum level f	or logging mess	ages. The ASA will filter s	stem log messages	with severity lev
Class/SeverR	y Filters -	Add Class	and Severity Filter		
Event Class	Severi	Event Class:	All		Add
		Description:	ssi	-	Ed?
		Severity:	sys		
		OK	vm updo		Deets
			vpor	-	

aus.\_\_

4. Wählen Sie den Schweregrad als *Fehler aus*. Dieser Schweregrad gilt nur für Nachrichten, die für diese Nachrichtenklasse protokolliert werden. Klicken Sie auf *OK*, um zum Fenster Ereignisliste hinzufügen

ne: vpndient-en	ors			
cify filters for the	event list	. You can filter	syslogs by their class and se sages. The ASA will filter sys	everity, or
the specified leve ant Class/Sevents	Filters -	nd Add Class	and Severity Filter	×
Event Class	Severi	Event Class:	vpnc	*
		Description:	VPN Client	
		Severity:	Errors	*
		-	Emergencies	
		OK	Alerts	
	1.1		Critical	
			Errors	
			Warnings	
			Notifications	
		1	Informational	
		OK	Debugging	

zurückzukehren.

5. Die Ereignisklasse/-schweregrad wird hier angezeigt. Klicken Sie auf *OK*, um die Konfiguration der Ereignisliste "vpnclient-errors"

cify filters for the esents the maxime specified leve nt Class/Severity	e event list. You mum level for lo I. v Filters	can filter syslogs by the gging messages. The AS	er class and severity, or by their ID A will filter system log messages wi Message ID Filters	s. The severity th severity leve
Event Class	Severity	Add	Message IDs	Add
vpnc	Errors	Edit		Edit
		Delete		Delete

abzuschließen.

Im nächsten Screenshot wird auch gezeigt, dass eine neue Ereignisliste, "user-auth-syslog", mit einer Nachrichtenklasse als "auth" und dem Schweregrad für die Syslogs dieser spezifischen Nachrichtenklasse als "Warnungen" erstellt wird. Durch diese Konfiguration gibt die Ereignisliste alle Syslog-Meldungen an, die sich auf die

Authentifizierungsnachrichtenklasse beziehen, mit Schweregraden bis zur Stufe

"Warnungen".**Hinweis:** Hier ist der Begriff "Bis" von Bedeutung. Beachten Sie bei der Angabe des Schweregrads, dass alle Syslog-Meldungen bis zu diesem Level protokolliert

werden.**Hinweis:** Eine Ereignisliste kann mehrere Ereignisklassen enthalten. Die Ereignisliste "vpnclient-errors" wird durch Klicken auf **Bearbeiten** geändert und eine neue Ereignisklasse "ssl/error"

#### definiert.

infiguration > Device Management > Log	ging > Event Lists	
Use event lists to define a particular set of sysi	ogs that you are interested in. The event list can be used to filter sysl	ogs sent to a logging destination.
Name	Event Class / Severity	Message IDs
tcp-conn-syslog		302013-302018
syslog-sev-error	All / Errors	
vpnclient-errors	vpnc./ Errors	
user-auth-syslog	auth / Warnings	

## Arbeiten mit Protokollierungsfiltern

Protokollierungsfilter werden verwendet, um die Syslog-Meldungen an ein bestimmtes Ziel zu senden. Diese Syslog-Meldungen können auf dem Schweregrad oder den Listen "Selbst" basieren.

Diese Filter sind für die Bestimmungsorte geeignet:

- Interner Puffer
- SNMP-Trap
- E-Mail
- Konsole
- Telnet-Sitzungen
- ASDM
- Syslog-Server

Gehen Sie wie folgt vor:

1. Wählen Sie Konfiguration > Gerätemanagement > Protokollierung > Protokollierungsfilter aus, und wählen Sie das Protokollierungsziel aus. Klicken Sie anschließend auf Bearbeiten, um die Einstellungen zu

nfiguration > Device Management > Loggi	ng > Longing Filters		
Configure syslog filters for logging destinations.			
Logging Destination	Systogs From All Event Classes	Syslogs From Specific Event Classes	Edit
Internal Buffer	Disabled		
SNMP Trap	Disabled		
E-14al	Deabled		
Console	Disabled		
Teinet and 55H Sessions	Disabled		
ASOM	Disabled		
Sudan Services	Disabled'		

2. Sie können die Syslog-Meldungen je nach Schweregrad senden. Hier wurde **Notfälle** als Beispiel

nfigure logging filter s nerate system log mes	attings. The seve sages with sever	rity level represent ity levels up to the	s the maximum level fo specified level.	r logging messages. The	ASA will
gging Destination: Int	ernal Buffer				
slogs from All Event Cl	asses				
Filter on severity	Emergencies	*	).		
C Use event list	user-auth-sysic	g 💌 New	1		
C Disable logging fro	m all event classe	s	_		
sloas from Specific Eve	nt Classes				
			Event Class	Severity	
Event Class: auth	*	<u></u>			
Description: User A	uthentication	Add >>			
	encles 💌	Delete			
Severity: Emerg	and the second s				

3. Eine Ereignisliste kann auch ausgewählt werden, um festzulegen, welche Arten von Nachrichten an ein bestimmtes Ziel gesendet werden sollen. Klicken Sie auf

	on: Internal Butter				
Syslogs from All E	vent Classes				
C Filter on se	Emergencies	<u>.</u>			
Use event	list user-auth-sys	log View	1		
Systogs from Spe	onc Event Classes		Event Class	Severity	
Event Class:	auth 💌	Add >>			
Description:	User Authentication				
200000000000000000000000000000000000000		Dade			

4. Überprüfen Sie die

#### Änderung.

nfiguration > Device Management > Loggi	ng > Logging Filters	
Configure syslog filters for logging destinations.		
Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNNP Trap	Disabled	
Internal Buffer	Event List: user-auth-syslog	8.
E-Mail	Disabled	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )
Console	Disabled	
Telnet and SSH Sessions	Disabled	
ASDM	Disabled	
Syslag Servers	Disabled	

Dies sind die Schritte zum Senden einer Gruppe von Nachrichten (abhängig von ihrem Schweregrad) an den E-Mail-Server.

1. Wählen Sie **E-Mail** im Feld Logging Destination (Logging-Ziel) aus. Klicken Sie anschließend auf

#### Bearbeiten.

Configuration > Device Management > Logg	ing > Loaging Filters.		
Configure syslog filters for logging destinations.			
Logging Destination	Syslogs From All Event Classes	Sysiegs Frem Specific Event Classes	Edit
SNMP Trap	Disabled		
Internal Buffer	Event List: user-auth-syslog		
E-Mail	++ Disabled ++		
Cansale	Disabled		2
Telhet and SSH Sessions	Disabled		
ASDM	Disabled		
Syslog Servers	Disabled		

2. Wählen Sie die Option **Nach Schweregrad filtern**, und wählen Sie den gewünschten Schweregrad

aus.

e cuit Lugging ritters				4
Configure logging filter settings. The severity level generate system log messages with severity levels	represents t up to the sp	ne maximum level fo scified level.	r logging messages. The A	SA wil
Logging Destination: E-Mail				
Syslogs from All Event Classes				
( Filter on severity Emergencies 💌				
C Use event list Emergencies	New			
C Disable logging fror Errors				
Syslogs from Specific Eve Notifications	-			
Informational		Event Class	Severity	
Event Class: outh adv	155 1			
Description: User Authentication				
Severity: Emergencies *	lete			
	1 6000	1   Hala	1	
OK	Cance	neib		

#### ier wurde Alerts als Schweregrad

#### ausgewählt.

Configure syslog filters for logging destinations.		
Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	Disabled	
Internal Buffer	Event List: user-auth-syslog	
E-Mail	Severity: Alerts	
Console	Disabled	
Teinet and SSH Sessions	Disabled	
ASDM	Disabled	
Syslog Servers	Disabled	

Sie sehen, dass alle Alert-Syslog-Meldungen an die konfigurierte E-Mail gesendet werden sollen.

anfinute purchas filters for logging destinations	Ing - Konganing Linesitz	
uningure systog nicers for logging descriptions.		
Logging Destination	Sysiags From All Event Classes	Syslogs From Specific Event Classes
Internal Buffer	Event List: user-auth-syslog	
SNMP Trap	Disabled	
E-Mai	Severity: Alerts	
Console	Disabled	П
Telnet and SSH Sessions	Disabled	- U
ASDM	Disabled	
Sysion Servers	Disabled	

## <u>Übertragungsratenlimit</u>

Dieser Parameter gibt die Anzahl der Syslog-Meldungen an, die eine Cisco ASA innerhalb eines festgelegten Zeitraums an ein Ziel sendet. Sie wird in der Regel für den Schweregrad definiert.

1. Wählen Sie Configuration > Device Management > Logging > Rate Limit (Konfiguration >

# Gerätemanagement > Protokollierung > Übertragungsratenlimit) aus, und wählen Sie den gewünschten Schweregrad aus. Klicken Sie anschließend auf

#### Bearbeiten.

bugging trinited  kind unimited  kind unimited  kind unimited  sining unim	Logging Level	No. of Messages	Interval (Seconds)	Edk
uninited       uninited         sergendes       uninited         arrings       uninited         ors       uninited         romational       uninited         sits       uninited	bugging	uninited	2444 - 1446 - 144 - 146	
tical urinited urinit	tifications	uninited		
ergendiss urlinited urlini	tical	unimited		
anings uninted	ergencies	unimited		
ors uninted un	anings	unimited		
ormstonal unimited unimited unimited	ors	uniinited		
with a unimited and a second sec	ormational	unimited		
d olly 8 ate Timbert System Messagies				
	NI3	unimited		

2. Geben Sie die Anzahl der Nachrichten an, die zusammen mit dem Zeitintervall gesendet werden sollen. Klicken Sie auf

Logging Level: Debugging Number of Messages: 600	To allow an unlimited r Number of Messages	number of messages and Time Interval fie	s keep both the alds empty.
Number of Messages: 600	Logging Level:	Debugging	
and the second	Number of Messages:	600	
Time Interval:  86400 second	Time Interval:	86400	second

Hinweis: Diese Zahlen werden

als Beispiel angegeben. Diese unterscheiden sich je nach Netzwerkumgebung.Geänderte Werte werden hier

#### angezeigt:

Configuration > Device Management > Logging > R	ate Limit	
Assign rate limits for all the syslog messages in a logging l	evel or assign it individually to specific syslog messages.	
Data Linda for Surba Langing Laugh		
Race Limits for sysiog Logging Levels		1
Logging Level	No. of Messages	Interval (Seconds)
Debugging	600	86400
Notifications	unimted	
an and a d		

## Protokollieren der Hits einer Zugriffsregel

Sie können die Zugriffsregelhits mit dem ASDM protokollieren. Das

Standardprotokollierungsverhalten besteht darin, eine Syslog-Meldung für alle abgelehnten Pakete zu senden. Für die zulässigen Pakete wird keine Syslog-Meldung angezeigt, und diese werden nicht protokolliert. Sie können jedoch eine benutzerdefinierte

Protokollierungsschweregrad-Ebene für die Zugriffsregel definieren, um die Anzahl der Pakete zu verfolgen, die diese Zugriffsregel erreicht.

Gehen Sie wie folgt vor:

1. Wählen Sie die gewünschte Zugriffsregel aus, und klicken Sie auf *Bearbeiten*.Das Fenster Zugriffsregel bearbeiten wird

💼 Edit Acce	ss Rule	
Interface: Action:	inside	
Source:	10.10.10	
Destination	20.20.20.200	
Service:	- ·	
Description:		
I⊽ Enable L Logging	ogging Level: Default 💌	
More Opt	Ions Emergencies Alerts Critical OK Cancel Help	
	Warnings Notifications Informational	Hinweis: Ir

angezeigt.

diesem Bild zeigt die *Standard*-Option im Feld *Protokollierungsebene* das Standardprotokollierungsverhalten der Cisco ASA an. Weitere Informationen hierzu finden Sie im Abschnitt <u>"Logging Access List Activity"</u> (Protokollzugriffslistenaktivität).

2. Aktivieren Sie die Option *Protokollierung aktivieren*, und geben Sie den gewünschten Schweregrad an. Klicken Sie anschließend auf

Source:	10.10.10.10		-		
Destination	20.20.20.200		<u></u>		
Service:	ip		-		
Description:					
Constant Consta		$ \rightarrow $			
More Opt	lons				*
More Opt	lons Rule				<u> </u>
More Opt	lons Rule ection: @ In C (	ur.			*
More Opt Enable Traffic Dire Source Se	lons Rule ection: @ In _ C ( vice: _	xn.		- (TCP or UDP serv	vice only)
More Opt Enable Traffic Dire Source Se Logging In	ions Rule ection: @ In @ C vice: terval: 300sec	our.		- (TCP or UDP serv	vice only)

Wenn Sie auf die Dropdown-Registerkarte *More options (Weitere Optionen*) klicken, wird die Option *Logging Interval (Protokollierungsintervall) angezeigt*. Diese Option wird nur hervorgehoben, wenn die Option *Protokollierung aktivieren* aktiviert aktiviert ist. Der Standardwert dieses Timers beträgt 300 Sekunden. Diese Einstellung ist hilfreich, um den Timeoutwert für die zu löschenden Flussstatistiken anzugeben, wenn für diese Zugriffsregel keine Übereinstimmung vorliegt. Bei Treffern wartet ASA bis zum Protokollierungsintervall und sendet diese an das Syslog.

 Die Änderungen werden hier angezeigt. Alternativ können Sie auf das Feld Protokollierung der jeweiligen Zugriffsregel doppelklicken und dort den Schweregrad festlegen

4	Enabled	Source	Destination	Service	Action	Hits	Logging		lime
5th in	side (5 inco	ming rules)			111-001-00				1
1	P	<b>3</b> 10.10.10.10	20.20.20.200	38-10	🥩 Permit	0	Errors		1
2	P	10.10.10.20	any	JP- iD	🖌 Permit	0	n.		1
3		<b>10.20.10.0/24</b>	20.20.20.200	😕 ip	🕲 Deny	0		1	
4		r inside-network/26	🔹 any	ID (0	Permit	0	Default		
5		<ul> <li>any</li> </ul>	any	ai ar	🕴 Deny		Default	*	Implicit rule
pi a	utside (1 im	plicit incoming rules)			- Comp.		Emergencies	1117-	1/2000/10/2010/00/
1	200	anv.	anv 🔅	10 × 10	Deny		Alerts		Implicit rule

**Hinweis:** Diese alternative Methode zur Angabe des *Protokollierungsgrads* im gleichen Bereich *für* Zugriffsregeln durch Doppelklicken funktioniert nur für manuell erstellte Zugriffsregeleinträge, nicht jedoch für implizite Regeln.

## **Konfigurieren**

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## **Konfigurationen**

In diesem Dokument werden folgende Konfigurationen verwendet:

CiscoASA
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0

```
shutdown
no nameif
no security-level
no ip address
interface Ethernet0/1
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.0
interface Ethernet0/2
nameif inside
security-level 100
ip address 10.78.177.11 255.255.255.192
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors
access-list inside_access_in extended permit ip host
10.10.10.20 any
access-list inside_access_in extended deny ip 10.20.10.0
255.255.255.0 host 20.20.20.200
access-list inside_access_in extended permit ip
10.78.177.0 255.255.255.192 any log emergencies
pager lines 24
logging enable
logging list user-auth-syslog level warnings class auth
logging list TCP-conn-syslog message 302013-302018
logging list syslog-sev-error level errors
logging list vpnclient-errors level errors class vpnc
logging list vpnclient-errors level errors class ssl
logging buffered user-auth-syslog
logging mail alerts
logging from-address test123@example.com
logging recipient-address monitorsyslog@example.com
level errors
logging queue 1024
logging host inside 172.16.11.100
logging ftp-bufferwrap
logging ftp-server 172.16.18.10 syslog testuser ****
logging permit-hostdown
no logging message 302015
no logging message 302016
logging rate-limit 600 86400 level 7
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-623.bin
asdm history enable
arp timeout 14400
!!--- Output Suppressed ! timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute timeout TCP-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy ! !---
Output Suppressed ! ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list no threat-detection
statistics TCP-intercept ! !--- Output Suppressed !
username test password /FzQ9W6s1KjC0YQ7 encrypted
privilege 15 ! ! class-map inspection_default match
```

default-inspection-traffic ! ! policy-map type inspect							
dns preset_dns_map parameters message-length maximum 512							
policy-map global_policy class inspection_default							
<pre>inspect dns preset_dns_map inspect ftp inspect h323 h225</pre>							
inspect h323 ras inspect netbios inspect rsh inspect							
rtsp inspect skinny inspect esmtp inspect sqlnet inspect							
sunrpc inspect tftp inspect sip inspect xdmcp ! service-							
policy global_policy global <b>smtp-server 172.18.10.20</b>							
prompt hostname context							
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4							
: end							

# <u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

• Sie können die Syslogs im ASDM anzeigen. Wählen Sie **Monitoring > Logging > Real Time** Log Viewer aus. Hier wird eine Beispielausgabe

toring > Logging > Real-Time Log Viewer									
-Time Log	Time Log Viewer								
🕵 Real-T	lime Log Vier	wer - 10.7	8.177.11		11	International Contents		=03	
File Too	ols Window	Help							
00 Page	e Ma Copy	Save 1	Cear	Color Settings	Create Ru	le 📰 Show Rule	Show Details	🥐 Help	
Г	1997 - The Control of C				les et l				
Hiter By:			· ·	r. 個 Show All	Find:		<i>a</i> ,		
Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port		
6 🔔	May 31 2011	10:24:38	606003	10.78.153.167				ASDM logging session number 0 from 10	
1.6	May 31 2011	10:24:38	605005	10.78,153.167	4009	10.78.177.11	https	Login permitted from 10.78.153.167/40	
<u>2</u> 6	May 31 2011	10:24:38	725002	10.78.153.167	4009			Device completed SSL handshake with o	
<u>i</u> 6	May 31 2011	10:24:38	725003	10.78.153.167	4009			SSL client inside: 10.78.153.167/4009 re	
6 🌲	May 31 2011	10:24:38	725001	10.78.153.167	4009			Starting 55L handshake with client inside	
<u>    6                                </u>	May 31 2011	10:24:38	302013	10.78.153.167	4009	10.78,177.11	443	Built inbound TCP connection 136 for inc	
<u>i</u> 6	May 31 2011	10:24:31	725007	10.78.153.167	4008			SSL session with client inside: 10.78.153	
£ 6	May 31 2011	10:24:31	106015	10.78.153.167	4008	10.78.177.11	443	Deny TCP (no connection) from 10.78.1	
4.6	May 31 2011	10:24:31	302014	10.78.153.167	4008	10.78.177.11	443	Teardown TCP connection 135 for inside	
<u>£</u> 5	May 31 2011	10:24:31	111008					User 'test' executed the 'logging asdm a	
								Syslog Connection Lost	

# **Fehlerbehebung**

## Problem: Verbindung unterbrochen — Syslog-Verbindung beendet —

Dieser Fehler tritt auf, wenn versucht wird, die ASDM-Protokollierung für einen der Kontexte im Geräte-Dashboard zu aktivieren.

"Verbindung unterbrochen - Syslog-Verbindung beendet -"

Wenn ASDM für die direkte Verbindung mit dem Admin-Kontext verwendet wird und dort die ADSM-Protokollierung deaktiviert ist, wechseln Sie zu einem Subkontext, und aktivieren Sie die ASDM-Protokollierung. Die Fehler werden empfangen, aber die Syslog-Meldungen erreichen den Syslog-Server gut.

## **Lösung**

Dies ist ein bekanntes Verhalten von Cisco ASDM, das in der Cisco Bug ID <u>CSCsd10699</u> dokumentiert ist (nur <u>registrierte</u> Kunden). Aktivieren Sie als Problemumgehung die ASDM-Protokollierung, wenn Sie sich im Admin-Kontext anmelden.

### Echtzeitprotokolle auf Cisco ASDM können nicht angezeigt werden.

Ein Problem besteht darin, dass die Echtzeitprotokolle nicht auf dem ASDM angezeigt werden können. Wie wird diese konfiguriert?

## **Lösung**

Konfigurieren Sie Folgendes auf der Cisco ASA:

```
ciscoasa(config)#logging monitor 6
ciscoasa(config)#terminal monitor
ciscoasa(config)#logging on
ciscoasa(config)#logging trap 6
```

# Zugehörige Informationen

- <u>Unterstützung von Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>