

GFI ClearView- Verwaltungshandbuch

Erfahren Sie, wie Sie GFI ClearView in verschiedenen Umgebungen einrichten und konfigurieren und wie Sie erweiterte Funktionen anpassen können.





Die Informationen und Inhalte in diesem Dokument werden ausschließlich zu Informationszwecken und ohne ausdrückliche oder stillschweigende Gewährleistung bereitgestellt, einschließlich und ohne Einschränkung Gewährleistung der Marktgängigkeit, der Eignung für einen bestimmten Zweck und der Nichtverletzung von Rechten Dritter. GFI Software lehnt jegliche Haftung für Verluste oder Schäden jeglicher Art ab, einschließlich Folge- oder Nebenschäden im Zusammenhang mit der Bereitstellung, Leistung oder Verwendung dieses Dokuments. Die Informationen stammen aus öffentlich zugänglichen Quellen. Obwohl angemessene Anstrengungen unternommen wurden, um die Richtigkeit der bereitgestellten Daten zu gewährleisten, gibt GFI keine Garantie, Zusage oder Gewährleistung für die Vollständigkeit, Richtigkeit, Aktualität oder Angemessenheit der in diesem Dokument enthaltenen Informationen und ist nicht für Druckfehler, veraltete Informationen oder Irrtümer verantwortlich. GFI behält sich das Recht vor, seine Produkte, Software oder Dokumentation ohne vorherige Ankündigung zu überarbeiten oder zu aktualisieren. Sie tragen die volle Verantwortung für die Nutzung und Anwendung der Produkte und Dienstleistungen von GFI. Kein Teil dieser Dokumentation darf ohne vorherige schriftliche Genehmigung von GFI Software in irgendeiner Form vervielfältigt werden.

Wenn Sie glauben, dass dieses Dokument sachliche Fehler enthält, setzen Sie sich bitte mit uns in Verbindung, und wir werden Ihr Anliegen so schnell wie möglich prüfen.

GFI und GFI ClearView sind Marken oder eingetragene Marken von GFI Software oder seinen Tochtergesellschaften in USA und anderen Ländern. Alle anderen hierin enthaltenen Marken sind das Eigentum der jeweiligen Inhaber.

GFI ClearView ist eine urheberrechtlich geschützte Software von GFI Software. Alle Rechte vorbehalten. Dokument Version: 1.0

Letzte Aktualisierung (Monat/Tag/Jahr): 30/09/2023

Inhalt

1. Einführung	13
1.1 ClearView-Systemkomponenten	13
1.1.1 ClearView-Anwendung	13
1.1.2 ClearView Web UI	13
1.1.3 ClearView Lösungszentrum	13
1.2 Die ClearView-Produktlinie	13
1.2.1 ClearView virtuelle Anwendungen	13
2. ClearView Handbuch für den Einsatz	14
2.1 Optionen für den Einsatz	14
2.1.1 Voraussetzungen:	14
2.1.2 Diagramm der Netzwerkarchitektur	14
2.1.3 Wie man sie einsetzt:	15
2.2.1 Wie man konfiguriert:	15
2.2.2 Verwandte Themen	16
2.2.3 Verwandte Themen	17
Anpassen der Anzahl für virtuelle Maschine verfügbaren CPUs	17
Anpassen des für die virtuelle Maschine verfügbaren RAMs	17
Anpassen der für die virtuelle Maschine verfügbaren NICs	18
Hinzufügen von Speicher zu einer virtuellen VMware-Maschine	19
Starten der virtuellen VMware-Appliance	22
2.2.4 Verwandte Themen	22
Ausführung unter Microsoft Hyper-V	23
Installation der virtuellen Maschine auf Hyper-V	23
2.2.5 Verwandte Themen	23
Anpassen der Anzahl der für die virtuelle Maschine verfügbaren CPUs	23
2.2.6 Verwandte Themen	24
Anpassen des für die virtuelle Maschine verfügbaren RAM	24
2.2.7 Verwandte Themen	25
Erhöhen Sie den Speicherplatz durch Hinzufügen neuer virtueller Laufwerke	25
2.2.8 Verwandte Themen	31
Anpassen einer virtuellen Hyper-V-Maschine	31
2.2.9 Erstellen einer ersten Konfiguration mit dem Basis-Assistenten	32
3 Verwendung von	35
3.1 Definieren einer Netzwerkumgebung	35
3.1.1 Hinzufügen von Netzwerkobjekten	35
Hinzufügen von Netzwerkobjekten in der GFI ClearView Web UI	36
Wo man es konfiguriert	36
So erstellen Sie ein neues Netzwerkobjekt	36
Beispiele für Netzobjektdefinitionen	37
Wie lässt sich feststellen, ob ein Netzobjekt mit dem Standort "inherit" zu einem internen oder externen Standort aufgelöst wurde?	38
Erstellen von Netzwerkobjekten basierend auf FQDN?	38
3.1.2 Arbeiten mit Benutzern und Gruppen als Objekte	38
Definieren von Netzwerkbenutzerobjekten	39
Definieren und Entfernen von Benutzern als dynamische Netzwerkobjekte	39
Konfigurieren von Netzwerkbenutzergruppenobjekten	40
Definieren und Entfernen von Benutzergruppen als dynamische Netzwerkobjekte	40
3.1.3 Konfigurieren von VLAN-Objekten	41
Konfigurieren von VLAN-Objekten in der GFI ClearView Web UI	41

3.1.4	Hinzufügen von Protokollobjekten.....	41
3.1.5	Hinzufügen von Anwendungsobjekten.....	42
	Hinzufügen von Anwendungsobjekten in der GFI ClearView Web UI.....	44
3.1.6	Hinzufügen und Aktualisieren von Anwendungsgruppenobjekten.....	44
	Hinzufügen von Anwendungsgruppenobjekten in der GFI ClearView Web UI.....	45
	So fügen Sie eine neue Anwendungsgruppe hinzu.....	45
	So aktualisieren Sie eine Anwendungsgruppe.....	45
	Welche Anwendungsgruppen sind vordefiniert?.....	45
3.1.7	Konfigurieren der Erkennung und Überwachung eines anonymen Proxys.....	45
	Wo man es konfiguriert.....	46
	So aktivieren Sie die Klassifizierung des anonymen Proxy-Verkehrs.....	46
	So sehen Sie, wann die Appliance die anonymen Proxy-Definitionen zuletzt aktualisiert hat.....	47
	So erzwingen Sie eine Überprüfung der anonymen Proxy-Definitionen.....	47
	So deaktivieren Sie die Klassifizierung des anonymen Proxy-Verkehrs.....	47
3.1.8	Konfigurieren von Service Level Agreement-Objekten.....	47
	Konfigurieren von Service Level Agreement-Objekten in der GFI ClearView Web UI.....	47
3.1.9	Konfigurieren von Objekten zur Bewertung der Anwendungsleistung.....	49
	Erstellen eines Objekts zur Bewertung der Anwendungsleistung.....	51
	Erstellen eines Objekts zur Bewertung der Anwendungsleistung in GFI ClearView Web UI.....	51
	Wie die Schwellenwerte für die Leistungskennzahlen berechnet werden.....	52
	APS-Schwellenwerte manuell konfigurieren.....	52
	Konfigurieren der automatischen APS-Schwellenwertberechnung.....	53
	Prüfen, ob die Basisberechnung im Gange ist.....	54
3.1.10	Konfigurieren eines Anwendungsleistungsmetrikobjekts.....	54
	Bevor Sie beginnen.....	55
	So erstellen Sie ein APM-Objekt.....	55
	1. Gehen Sie zu Konfiguration > Objekte> Service Levels> Application Performance Metric.....	55
3.2	Überwachung Ihres Netzwerks.....	56
3.2.1	Dashboards.....	56
	System-Dashboard.....	57
	Vorteile Dashboard.....	57
	GFI ClearView empfiehlt.....	58
	Sichtbarkeit.....	58
	Freizeitsport.....	58
3.2.2	Überwachung des Netzwerkverkehrs in Echtzeit.....	59
	Überwachung von Netzwerkanwendungen in Echtzeit.....	59
	Überwachung von Hosts und Benutzern in Echtzeit.....	60
	Überwachung von Gesprächen in Echtzeit.....	61
	Überwachung der Anwendungsreaktion in Echtzeit.....	62
	Überwachung der Anwendungsreaktionen in Echtzeit.....	63
	Anzeige des Berichts in der GFI ClearView Web UI.....	63
	Anzeigen des Berichts in GFI ClearView CLI.....	63
	Überwachung des Hostzustands in Echtzeit.....	64
	Anzeigen des Berichts in der GFI ClearView Web UI.....	65
	Anzeigen des Berichts in GFI ClearView CLI.....	65
3.2.3	Überwachung des Netzwerkdurchsatzes	67
	Wo kann ich diesen Bericht finden?.....	67
	Um die richtige Größe Ihres Netzes zu bestimmen (d. h. Elemente aus der Tabelle zu entfernen).....	68
	Ermittlung des Durchsatzes, der über einem bestimmten Perzentil liegt.....	68
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?.....	68
3.2.4	Überwachung des Dienstleistungsniveaus.....	69
	Überwachung der Leistungswerte von Anwendungen.....	69
	Erzeugen eines PDF-Berichts der APS-Ergebnisse.....	71

Berechnung der Leistungsbewertung einer Anwendung.....	73
Überwachung der Netzreaktion SLA.....	73
Wo kann ich diesen Bericht finden?.....	75
So fügen Sie eine SLA-Site hinzu.....	75
So zeigen Sie das Diagramm für eine andere SLA-Site an.....	75
Wie interagiere ich mit den interaktiven Flash-Zeitdiagrammen?.....	75
Überwachung der TCP-Effizienz.....	75
Wo kann ich diesen Bericht finden?.....	77
Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?.....	78
Überwachung des TCP-Zustands.....	78
Wo kann ich diesen Bericht finden?.....	80
Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?.....	80
3.2.5 Überwachung von Anwendungen.....	80
Überwachung der Anwendungsleistung im Netzwerk.....	80
Überwachung des Datenverkehrs von Anwendungsgruppen.....	81
Anzeigen einer Netzwerkübersicht der Anwendungsgruppen.....	83
Anzeigen des Datenverkehrsvolumens von Anwendungen.....	83
Wo kann ich diesen Bericht finden?.....	84
So filtern Sie die Berichtsdaten.....	85
Ein- oder Ausschalten der Kategorie "übriger Verkehr".....	85
Ändern des Durchsatzdiagramms in gestapelte Flächen- oder Liniendiagramme.....	85
Feststellen, ob eine oder mehrere Anwendungen den anderen Anwendungsverkehr drosseln können.....	85
Feststellen, ob eine der Top-Anwendungen begrenzt zu sein scheint.....	86
Charting einer einzelnen Anwendung.....	86
So zeigen Sie mehr oder weniger Anwendungen im Diagramm der Top-Anwendungen und im Durchsatzdiagramm an.....	86
Wie kann ich mit den neuen Zeitreihen- und Balkendiagrammberichten arbeiten?.....	86
Überwachung der besuchten URLs.....	87
Drilling in Anwendungsdaten.....	89
Deaktivieren von Berechnungen der Leistungskennzahlen von Anwendungen.....	90
3.2.6 Überwachung der Netzwerkbenutzer.....	92
Einstellen des Zeitraums für einen Bericht.....	93
3.2.7 Überwachung des Verkehrsaufkommens der Hosts.....	94
Was sind Wirte?.....	95
Wo kann ich diesen Bericht finden?.....	96
So filtern Sie die Berichtsdaten.....	96
Aufschlüsselung der Berichtsdaten.....	97
Suche nach einem bestimmten Host.....	98
Wie kann ich mit den neuen Zeitreihen- und Balkendiagrammberichten interagieren?.....	98
3.2.9 Überwachung von Netzwerkgesprächen.....	98
Für den Zugang zu diesem Bericht:.....	99
3.2.9 Überwachung von Teilnetzen.....	101
Wo kann ich diesen Bericht finden?.....	102
So konfigurieren Sie ein Subnetz für die Überwachung.....	102
Ich kann meine Subnetzdaten nicht sehen.....	102
Um das Durchsatzdiagramm in ein gestapeltes Flächendiagramm oder ein Liniendiagramm zu ändern.....	103
So zeigen Sie das Datenvolumen der Subnetze in einem Tortendiagramm an.....	103
Um mehr oder weniger Subnetze in der Tabelle der Top-Subnetze und in der Durchsatztabelle anzuzeigen.....	103
Sollten die Summen der Subnetze mit den Summen der virtuellen Verbindungen übereinstimmen, wenn die virtuelle Verbindung und das Subnetz auf demselben Netzwerkobjekt basieren?.....	103
Kann ich die wichtigsten internen oder externen Hosts pro Subnetz in diesem Bericht anzeigen?.....	103
Wie kann ich in diesem Bericht eine Aufschlüsselung vornehmen?.....	104
Wie interagiere ich mit den neuen Zeitserien- und Balkendiagrammberichten?.....	104

	Erstellen eines detaillierten Subnetz-Aktivitätsberichts.....	104
3.2.11	Überwachung der Systemleistung von GFI ClearView Appliance	105
	Überwachung von Verbindungen zu einer GFI ClearView Appliance.....	105
	Wo kann ich diesen Bericht finden?	105
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?	105
	Überwachung der CPU-Auslastung von GFI ClearView Appliance.....	106
	Wo kann ich diesen Bericht finden?	106
	Wo finde ich die anderen Berichte, um den Grund für die hohe CPU-Auslastung zu diagnostizieren?	107
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?	107
	Überwachung der CPU-Temperatur der GFI ClearView Appliance	107
	Wo kann ich diesen Bericht finden?	108
	Wo finde ich den CPU-Nutzungsbericht?.....	108
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?	108
	Überwachung der RAM-Auslastung von GFI ClearView Appliance	108
	Wo kann ich diesen Bericht finden?	109
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?	109
	Überwachung von GFI ClearView Appliance Disk IO.....	109
	Wo kann ich diesen Bericht finden?.....	110
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?.....	110
	Überwachung des Auslagerungsspeichers von GFI ClearView Appliance	111
	Wo kann ich diesen Bericht finden?	111
	Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?.....	111
3.2.12	Anzeigen von Überwachungsstatistiken	111
	Verstehen der Beziehungen zwischen Diagrammen und Daten.	112
	Vergößern eines Zeitintervalls in den Zeitdiagrammen	113
	Einstellen von Zeitbereichen für Diagramme und Kurven.....	114
	Vertiefung der Diagrammdatei	114
	Interaktive Zeitdiagramme verwenden.....	115
	Exportieren, Drucken und Planen von Berichten	116
	Erzeugen von PDF-Berichten.....	116
	So planen Sie einen PDF-Bericht von einem Monitorbildschirm aus.....	117
	So planen Sie einen neuen PDF-Bericht auf der Seite Berichte	118
	So zeigen Sie einen geplanten Bericht bei Bedarf an oder bearbeiten oder löschen einen Bericht.....	119
	So fügen Sie ein benutzerdefiniertes Logo auf dem Deckblatt der geplanten Berichte ein.....	119
	CSV-Berichterstattung	120
3.3	Überwachung von Anwendungen mit dem ClearView Solution Center	121
3.3.1	Wie Leistungsberichte funktionieren	122
3.3.2	Berichte zur Anwendungsleistung verwenden.....	122
	Ausführen eines Anwendungsleistungsberichts	123
	Verstehen der Daten, die in einem Anwendungsleistungsbericht angezeigt werden.....	123
3.3.3	Bandbreitennutzung	124
3.3.4	Verwendung des Berichts Application Performance Monitor VoIP	125
	Ausführen des Berichts Anwendungsleistung VoIP	125
	Verstehen der Daten, die in einem Anwendungsperformance-VoIP-Bericht angezeigt werden.....	125
	Was ist MOS?	126
	Was ist rFactor?	126
3.3.5	Freizeitverkehr.....	126
	Wie kann ich diesen Bericht einrichten?.....	126
3.3.6	Verwendung von Netzwerk-Governance-Berichten	127
	Verstehen der im Bericht Freizeitverkehr angezeigten Daten.....	127
	Ausführen des Berichts Freizeitverkehr	127
3.3.7	Antworten auf häufig gestellte Fragen zur Solution Center-Anwendungsleistung	128
	Welche Art von Daten sind in einem Anwendungsleistungsbericht verfügbar?	128

Was ist der Anwendungsleistungsbericht Baselineing?.....	128
Was ist, wenn das Solution Center anzeigt, dass es keine Lösungen gibt?	129
Was ist, wenn eine Lösung eine höhere GFI ClearView OS-Version erfordert?	129
Kann ich eine Lösung mehr als einmal ausführen?	129
3.3.8 Hinzufügen und Löschen von Lösungen	129
So fügen Sie eine Lösung hinzu	129
So löschen Sie eine Lösung	130
3.3.9 Eine neue Ausgangsbasis schaffen	130
3.3.10 Arbeiten mit Diagrammen zur Anwendungsleistung	130
Ermittlung von Durchsatzwerten für bestimmte Zeitpunkte in der Durchsatztabelle.....	131
3.3.11 Untersuchen einer schlechten Anwendungsleistungsbewertung (APS)	131
3.3.12 Untersuchung von ungewöhnlichen Leistungen	131
3.3.13 Löschen eines Anwendungsleistungsberichts	132
4 Einstellungen	132
4.1 Netzwerk-Einstellungen	132
4.1.1 NIC-Konfiguration	132
Einstellungen der Schnittstelle	132
Wo kann ich diese Konfiguration finden?	133
So konfigurieren Sie die NIC-Schnittstellen	133
4.1.2 Konfiguration der IP-Adresse	133
Wo kann ich diese Konfiguration finden?	134
So konfigurieren Sie eine Schnittstellenadresse und Netzmaske automatisch	134
So konfigurieren Sie eine statische Adresse	134
So konfigurieren Sie die Einstellungen des Gateways	134
4.1.3 Konfiguration der Routen	135
4.1.4 Konfiguration von DNS und Domännennamen	136
Wo kann ich diese Konfiguration finden?	137
So konfigurieren Sie den Hostnamen der Appliance	137
Wie kann man feststellen, ob der DNS vom DHCP-Server konfiguriert wurde?	137
So konfigurieren Sie den Standort der DNS-Server	137
So fügen Sie einen Domännennamen hinzu	137
So entfernen Sie einen Domännennamen	137
4.1.5 HTTP-Proxy-Konfiguration	138
Wo kann ich diese Konfiguration finden?	138
So konfigurieren Sie den Zugriff auf den Server von GFI ClearView über einen HTTP-Proxy	138
4.1.6 E-Mail-Konfiguration	138
Konfigurieren der SMTP-Server-Einstellungen	139
Testen der SMTP-Konfiguration	139
Hinzufügen von E-Mail-Empfängern für Benachrichtigungen	140
Entfernen von E-Mail-Empfängern für Benachrichtigungen	140
4.1.7 SNMP-Konfiguration	141
SNMP konfigurieren	141
Entfernen einer unerwünschten SNMP-Community	142
Herunterladen der SNMP-MIB-Datei	143
Ändern der SNMP-Authentifizierung für den Benutzer Admin	143
Vorübergehendes Anhalten des Versands von SNMP-Traps	144
Entfernen von Siphon-Sink-Servern	144
Definieren von SNMP-Trap-Zielen	144
4.1.8 Integrieren mit Active Directory	145
Wie die Active Directory-Integration funktioniert	145
Installieren Sie den GFI ClearView AD Connector	147
Bereitstellen der erforderlichen Berechtigungen für den GFI ClearView AD-Dienst	147
Installieren des GFI ClearView AD Connector	149

Hinzufügen der GFI ClearView Appliances zum GFI ClearView AD Connector	150
Die Port-Nummer von GFI ClearView AD Connector	151
Ändern der Portnummer von GFI ClearView AD Connector	151
Wählen Sie die Informationen aus, die zwischen der GFI ClearView-Appliance und dem Active Directory-Server übertragen werden. 151	
Identifizieren des Active Directory-Servers	153
Überprüfen der Kommunikation zwischen dem Active Directory Server und der ClearView Appliance	153
Anforderung aktualisierter Benutzer- und Gruppeninformationen vom Active Directory-Server	154
Ändern des Status von GFI ClearView AD Connector	154
Bestimmte Benutzernamen von Berichten ausschließen	155
Adaptive Response mit Active Directory verwenden	155
Identifizierung der Nutzer	156
Installieren Sie das GFI ClearView Citrix XenApp Plugin	157
Fügen Sie den GFI ClearView AD Connector zum GFI ClearView Citrix XenApp Plugin hinzu	157
Aufzeichnung der GFI ClearView Citrix XenApp Plugin-Aktivität in einer Protokolldatei	158
Ändern Sie die Port-Nummer des GFI ClearView Citrix XenApp Plugin	158
Abfrage aktualisierter Benutzerinformationen über das GFI ClearView Citrix XenApp-Plugin	158
Hinzufügen einer neuen Anwendung	159
Welche Möglichkeiten der L7-Signatur gibt es?	159
Beispiel: So erstellen Sie eine benutzerdefinierte Anwendung auf der Grundlage des HTTPS-Protokolls	163
Wichtigste interne und externe Benutzer im Netzwerk	163
4.2 System einrichten	164
4.2.1 Konfiguration von Datum und Uhrzeit	164
Wo kann ich diese Konfiguration finden?	165
So stellen Sie Datum und Uhrzeit über einen NTP-Server ein	165
So stellen Sie Datum und Uhrzeit manuell ein	166
Zum Erzwingen einer Zeitrückstellung, wenn die Zeit erheblich aus der Synchronisation geraten ist	166
4.2.2 Konfiguration des UI-Zugriffs	167
So konfigurieren Sie die Web-Benutzeroberfläche so, dass sie sich nach einer bestimmten Leerlaufzeit automatisch abmeldet	167
So aktivieren Sie den HTTP- oder HTTPS-Webzugriff	168
So deaktivieren Sie die Web-UI	168
Um die Web-UI wieder zu aktivieren	168
So konfigurieren Sie die CLI für den Zugriff über Telnet oder SSH	168
So konfigurieren Sie die CLI so, dass sie sich nach einer bestimmten Leerlaufzeit automatisch abmeldet	168
4.2.3 SQL-Zugriff konfigurieren	168
Den ODBC-Treiber herunterladen	168
Remote-SQL-Optionen einstellen	169
Anzeigen von SQL Access-Daten in Microsoft Excel	175
SQL-Schema	178
fließt Tabelle	178
4.2.4 Überwachung der Konfiguration	182
So konfigurieren Sie die Anzeigoptionen für Überwachungsdiagramme	183
So konfigurieren Sie, wie der Datenverkehr überwacht wird	183
So aktivieren oder deaktivieren Sie anwendungsspezifische Analysemodule (ASAM)	184
So steuern Sie die Reihenfolge der Auflösungsmethoden, die bei der Auflösung von IP-Adressen in Hostnamen verwendet werden	185
So aktivieren oder deaktivieren Sie die Erfassung von Überwachungsdaten	185
So löschen Sie gesammelte Überwachungsdaten	186
4.2.5 Netflow-Konfiguration	187
4.2.6 Geplanten Auftrag erstellen	190
Wo kann ich diese Konfiguration finden?	190
So planen Sie einen Auftrag	190

4.2.7	Ausschreibungen	191
	Festgelegte Schwellenwerte wurden überschritten	192
	Probleme mit Haushaltsgeräten	193
	Aktivieren von Systemwarnungen	193
4.2.8	Diskstorage erklärt	193
	Die Festplattenspeicherkarte	194
	Ändern der Größe des Festplattenspeichers für einen Dienst	195
	Löschen aller für einen Dienst gespeicherten Daten	195
4.3	Authentifizierung	195
4.3.1	Liste der aktiven Benutzer anzeigen	196
4.3.2	Lokale Benutzerkonten	196
4.3.3	AAA	197
4.3.4	LDAP-Authentifizierung	198
4.3.5	Radius-Authentifizierung	198
4.3.6	TACACS+-Authentifizierung	199
4.4	Wartung des Systems	199
4.4.1	Verwalten der Systemkonfiguration	199
	Wie Sie Ihre Appliance-Einstellungen sichern	200
	Systemkonfiguration importieren	201
4.4.2	Werkseinstellungen	202
4.4.3	Neustart/Herunterfahren	202
	Neustart der GFI ClearView Appliance	202
	Automatischer Neustart der GFI ClearView Appliance	203
	Herunterfahren der GFI ClearView-Appliance	203
4.5	System-Werkzeuge	204
4.5.1	Ping	204
4.5.2	Traceroute	204
4.5.3	DNS-Suche	205
4.5.4	Abfrage einer entfernten IPMI GFI ClearView-Appliance	205
4.5.5	iPerf-Kunde	207
4.5.6	iPerf-Server	208
	Optionen nur für Server	209
	Optionen nur für Kunden	209
	Verschiedene Optionen	209
5	Fehlersuche	210
5.1	Diagnostik	210
5.1.1	Diagnosedateien	210
5.1.2	Bildschirm	211
5.1.3	NIC-Diagnose	211
5.1.4	RAID-Diagnose	212
5.1.5	TCP-Dump	213
	Ausführen eines TCP-Dumps von GFI ClearView-Appliance	213
	Allgemeine Anwendungsfälle	214
	Senden Sie einen TCP-Dump an GFI ClearView TAC	215
5.1.6	Anzeigen des Status einer Ausschreibung	215
5.1.7	Eröffnen Sie einen Fall mit ClearView Support Services	216
5.2	Log-Dateien	216
5.2.1	Live-Logbuch	216
5.2.2	Schwanz Log	216
5.2.3	Konfiguration der Systemprotokollierung	217
	Konfigurieren Sie die Appliance-Protokolldateien	217
	Hinzufügen eines entfernten Syslog-Servers	218
	Entfernen eines entfernten Syslog-Servers	218

Entfernen von Ereignissen aus dem Appliance-Systemprotokoll.....	218
5.3 Behebung von Problemen mit der Active Directory-Konfiguration.....	218
5.3.1 GFI ClearView Appliance wird jede Nacht neu gestartet.....	219
Problem	219
Lösung.....	219
5.3.2 WMI-Dienst wird nicht ausgeführt.....	219
Problem	219
Lösung.....	219
5.3.3 Anzeige des Systemkontos in Verkehrsberichten.....	219
Problem	219
Lösung.....	219
5.3.4 Keine Kommunikation zwischen dem GFI ClearView AD Connector und der GFI ClearView Appliance.....	220
Problem	220
Auflösung.....	220
5.3.5 GFI ClearView AD Connector wird nicht mehr ausgeführt.....	220
Problem	220
Lösung.....	220
5.3.6 Ausgeschlossene Benutzer werden weiterhin auf GFI ClearView-Appliance angezeigt.....	220
Problem	220
Lösung.....	221
5.3.7 Änderungen am GFI ClearView Active Directory Controller haben keine Auswirkungen.....	221
Problem	221
Lösung.....	221
5.3.8 Die IP-Adressen werden nicht den AD-Benutzern und -Gruppen zugewiesen.....	221
Problem	221
Lösung.....	221
6 ClearView Befehlszeilenschnittstelle (CLI).....	222
6.1 Verwenden der Befehlszeilenschnittstelle.....	223
6.1.1 Zugriff auf die Befehlszeilenschnittstelle.....	223
6.1.2 Sprungbrett zur CLI-Konfiguration.....	224
6.1.3 Konfigurieren von Befehlszeilenoptionen.....	225
7 Urheberrecht.....	225
7.1 GFI ClearView Endbenutzer-Lizenzvertrag (EULA).....	226
7.2 GNU General Public License (GPL).....	227
7.2.1 Präambel.....	227
7.2.1 BEDINGUNGEN UND KONDITIONEN.....	228
Definitionen.....	228
1. Quellcode.....	229
2. Grundlegende Berechtigungen.....	229
3. Schutz der Rechte von Nutzern vor dem Gesetz zur Bekämpfung von Umgehungen.....	230
4. Übermittlung von wortgetreuen Kopien.....	230
5. Übermittlung von geänderten Quellversionen.....	230
6. Übermittlung von Nicht-Quellformularen.....	231
7. Zusätzliche Begriffe.....	232
8. Beendigung.....	233
9. Annahme nicht erforderlich, um Kopien zu haben.....	233
10. Automatische Lizenzierung von nachgeschalteten Empfängern.....	233
11. Patente.....	234
12. Kein Verzicht auf die Freiheit der anderen.....	235
13. Verwendung unter der GNU Affero General Public License.....	235
14. Überarbeitete Fassungen dieser Lizenz.....	235
15. Gewährleistungsausschluss.....	235
16. Beschränkung der Haftung.....	235

17. Auslegung der Abschnitte 15 und 16.....	236
7.3 BSD 2.0.....	236

1. Einführung

Täglich konkurrieren geschäftskritischer Netzwerkverkehr und Datenverkehr aus dem Freizeitbereich um die Bandbreite überlasteter Netzwerke. GFI ClearView inspiziert, überwacht und verwaltet den Netzwerkverkehr und maximiert so die Geschwindigkeit und Effizienz des Datenflusses, wobei geschäftskritischen Anwendungen in LANs und WANs Vorrang eingeräumt wird.

1.1 ClearView-System Komponenten

ClearView umfasst eine Reihe von erforderlichen und optionalen Komponenten, die in der Infrastruktur Ihres Unternehmens installiert werden können.

1.1.1 ClearView Gerät

Die ClearView-Produktlinie umfasst eine Reihe virtueller Netzwerk-Appliances, die sich mit minimalem Aufwand direkt in Ihre Umgebung integrieren lassen. Die Appliances sind in verschiedenen Größen erhältlich, um jedes Netzwerkszenario und jede Größe abzudecken, von kleinen Büros mit Dutzenden von Benutzern bis hin zu sehr großen Rechenzentren, die Hunderttausende unterstützen.

[Weitere Informationen finden Sie unter Die ClearView-Produktlinie.](#)

1.1.2 ClearView Web UI

GFI ClearView bietet Anwendern und Administratoren eine Web-Benutzeroberfläche, über die sich Richtlinien konfigurieren und die Leistung der Appliances mit Hilfe einer Vielzahl von Dashboards und Berichten überwachen lässt.

1.1.3 ClearView Lösung Zentrum

Das ClearView Solution Center bietet eine Reihe von vordefinierten Monitoren, die Sie ausführen können, um Berichte zur Netzwerkleistung für Anwendungen wie FTP, SSH, Salesforce.com, Microsoft Office365, VoIP und viele andere zu erstellen.

[Weitere Informationen finden Sie unter Überwachung von Anwendungen mit dem ClearView Solution Center.](#)

1.2 Die ClearView-Produktlinie

Die ClearView-Produktlinie umfasst eine Reihe von Hardware- und virtuellen Netzwerk-Appliances, die sich mit minimalem Aufwand direkt in Ihre Umgebung einfügen lassen. Die Appliances sind in verschiedenen Größen erhältlich, um jedes Netzwerkszenario und jede Größe abzudecken, von kleinen Büros mit Dutzenden von Benutzern bis hin zu sehr großen Rechenzentren, die Hunderttausende unterstützen.

1.2.1 ClearView virtuelle Geräte

ClearView bietet dieselben Überwachungs-, Berichts- und Steuerungsfunktionen. Die Kapazität wird durch eine Kombination aus Lizenzierung und zugrunde liegender Hardware bestimmt.

ClearView läuft auf einem Host-Rechner unter einem Hypervisor, der dedizierte Ressourcen verwendet. Die Mindestanforderungen an dedizierte Hypervisor-Hardware sind in der nachstehenden Tabelle aufgeführt:

Specification	Small 1 to 250 devices	Medium 251 to 500 devices	Large 500+ devices
CPU	4 cores	8 cores	8+ cores
Storage	250 GB	750 GB	1.5 TB
Memory (RAM)	8 GB	12 GB	16 GB+

Anforderungen:

- Intel Xeon-Klasse, 64-Bit-CPU mit VT
- Aktiviert Festplattenspeicher auf einer einzelnen Festplatte

NOTE

Disk extending techniques are not supported on virtual appliances. Adding additional storage requires a hard disk.

2. Leitfaden für die ClearView-Bereitstellung

Dieser Leitfaden für die ersten Schritte führt Sie durch den grundlegenden Prozess der Installation, Konfiguration und Verwendung Ihres ClearView.

2.1 Einsatz Optionen

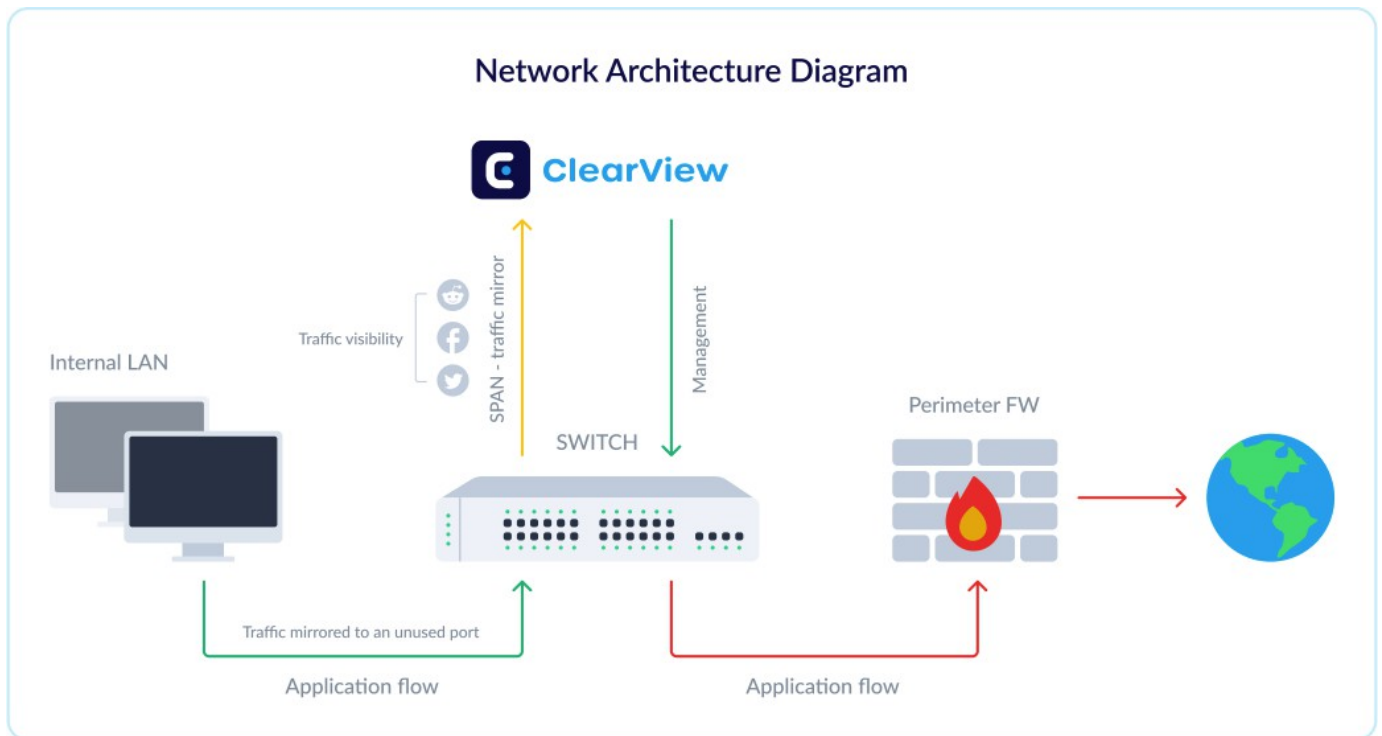
Die GFI ClearView Appliance kann fast überall in Ihrer Netzwerkumgebung eingesetzt werden. Generell gilt: Überall dort, wo Netzwerkpakete von einem Gerät zu einem anderen übertragen werden, sei es über physische Kabel oder durch Virtualisierung, können Sie eine GFI ClearView Appliance anschließen.

In diesem Abschnitt des Handbuchs werden die gängigsten Implementierungen der GFI ClearView Appliance erläutert.

2.1.1 Voraussetzungen: :

- Hypervisor
 - VMware|[OVA-Datei](#)|[Installationsanleitung Video](#)
 - HyperV|[ISO-Datei](#) |[Installationsanleitung Video](#) |[HyperV Port Mirroring Einstellungsanleitung](#)
 - VirtualBox|[OVA-Datei](#)|[Installationsanleitung Video](#)
- Port Mirroring / SPAN-Port Konfiguration
[\[Beispiel\] Videoanleitung](#)

2.1.2 Netzwerkarchitektur Diagramm:



2.1.3 Wie man einsetzt:

1. Laden Sie das Installer-Image herunter
2. Laden Sie das Image in den Hypervisor. Passen Sie die Hardwarespezifikationen entsprechend Ihren Anforderungen und dem Einsatzszenario an.
3. Schalten Sie das Gerät ein.
4. Melden Sie sich bei GFI ClearView mit username=admin und password=exinda an.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
6. Führen Sie die Schritte des Jumpstart-Assistenten aus.
7. Über die der Verwaltungsschnittstelle (eth0) zugewiesene IP können Sie auf die webbasierte Benutzeroberfläche zugreifen, indem Sie zu **https://<IP-Adresse>** navigieren.

Hinweis: Sie können die den Schnittstellen zugewiesenen IPs mit dem folgenden Befehl überprüfen: **show interfaces summary**

8. Öffnen Sie die Web-UI. Navigieren Sie zur Registerkarte **Dashboard> System**, suchen Sie die **Host-ID**, und senden Sie diese an Ihren GFI-Partner.
9. Sobald Sie den Schlüssel von Ihrem Partner erhalten haben, führen Sie bitte die folgenden Schritte aus.
 - a. Navigieren Sie zur GFI ClearView Web UI.
 - b. Um den Status Ihrer Lizenz anzuzeigen, wählen Sie System> Setup und wechseln Sie zur Registerkarte Lizenz.
 - c. Klicken Sie auf "Online auf Lizenz prüfen". Akzeptieren Sie den angezeigten Lizenzschlüssel und speichern Sie die Änderungen.

Hinweis: Vergewissern Sie sich, dass die Verwaltungsschnittstelle (eth0) Zugang zum Internet hat.
 - d. Alternativ können Sie auch den in der E-Mail angegebenen Lizenzschlüssel einfügen.
 - e. Klicken Sie auf Lizenz hinzufügen.

2.2.1 Wie Sie konfigurieren:

Damit GFI ClearView den Netzwerkverkehr erkennen kann, müssen Sie die Spiegelung auf dem Switch und ClearView-Appliance aktivieren:

- Aktivieren Sie die Mirror/SPAN-Port-Spiegelung vom Switch auf einen unbenutzten Port. Verbinden Sie diesen Port mit der GFI ClearView-Appliance. In diesem Beispiel wird der Datenverkehr an Port 2 und 4 auf Port 3 gespiegelt. In diesem Beispiel wäre Port 3 mit der GFI ClearView-Appliance verbunden:

Port	Mirroring Port	Mirrored Port
1	<input type="radio"/>	<input type="checkbox"/>
2	<input type="radio"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="radio"/>	<input type="checkbox"/>
4	<input type="radio"/>	<input checked="" type="checkbox"/>
5	<input type="radio"/>	<input type="checkbox"/>

- Aktivieren Sie die Spiegelungsoption auf der GFI ClearView-Schnittstelle, um den Datenverkehr zu überwachen. Über die Web-Benutzeroberfläche:
 - Klicken Sie auf System> Netzwerk> IP-Adresse.
 - Um eine Schnittstelle als Mirror-Port zu verwenden, aktivieren Sie das Kontrollkästchen Mirror.

- Klicken Sie auf "Änderungen übernehmen".

2.2.2 Verwandte Themen

Lesen Sie nach Abschluss der VM-Bereitstellung die folgenden Themen:

- [Anpassen des für die virtuelle Maschine verfügbaren RAM](#)
- [Anpassen der für die virtuelle Maschine verfügbaren NICs](#)
- [Hinzufügen von Speicher zur virtuellen VMware-Maschine](#)

Um die Leistung der virtuellen Appliance zu verbessern, ändern Sie die Anzahl der CPUs, den RAM, das Netzwerk und den Speicher, die der virtuellen Maschine zugewiesen sind.

NOTE

You will need to shut the virtual appliance down before you can modify its configuration.

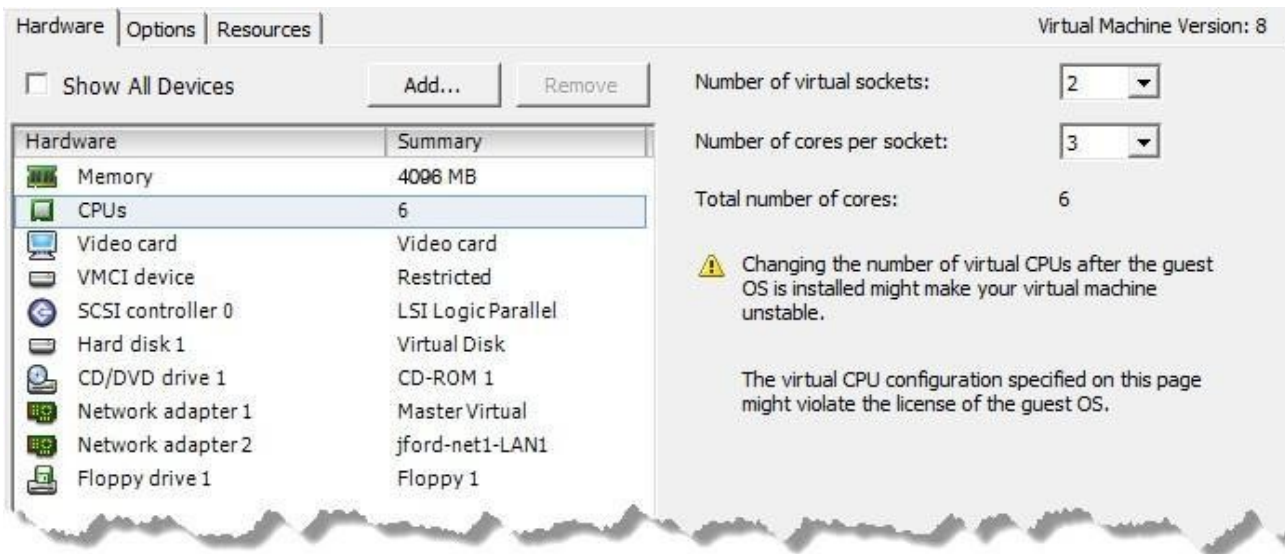
2.2.3 Verwandte Themen

- [Anpassen der Anzahl für virtuelle Maschine verfügbaren CPUs](#)
- [Anpassen des für die virtuelle Maschine verfügbaren RAM](#)
- [Anpassen der für die virtuelle Maschine verfügbaren NICs](#)
- [Hinzufügen von Speicher zur virtuellen VMware-Maschine](#)

Anpassen der Anzahl der für die virtuelle Maschine verfügbaren CPUs

Standardmäßig werden alle virtuellen Appliances mit zwei virtuellen CPUs konfiguriert. Erhöhen Sie die Anzahl der CPUs entsprechend Ihren Anforderungen.

1. Öffnen Sie den VMware vSphere-Client.
2. Klicken Sie mit der rechten Maustaste auf die GFI ClearView Virtual Appliance, und wählen Sie Einstellungen bearbeiten.
3. Wählen Sie auf der Registerkarte Hardware die Option CPUs.
4. Wählen Sie die Anzahl der virtuellen Steckdosen.
5. Wählen Sie die Anzahl der Kerne pro Sockel. Die resultierende Gesamtzahl der Kerne ist gleich oder kleiner als die Anzahl der logischen CPUs auf dem Host. Wenn zum Beispiel die Anzahl der virtuellen Sockel 2 und die Anzahl der Kerne pro Sockel 3 ist, ist die Gesamtzahl der Kerne
6. Bild anzeigen...



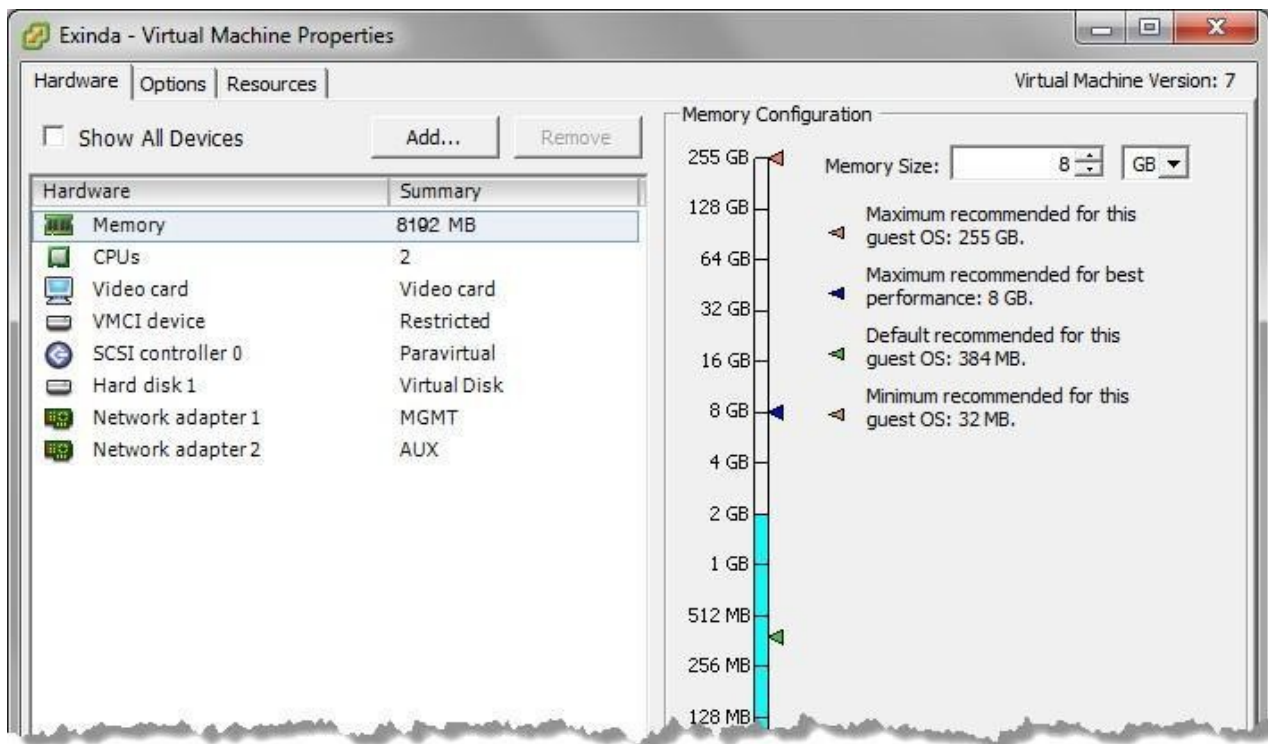
7. Klicken Sie auf OK.

Anpassen des für die virtuelle Maschine verfügbaren Arbeitsspeichers

Standardmäßig werden alle virtuellen Appliances mit 4 GB RAM konfiguriert. Erhöhen Sie die Menge an RAM Ihren Anforderungen.

1. Öffnen Sie den VMware vSphere-Client.

2. Klicken Sie mit der rechten Maustaste auf die GFI ClearView Virtual Appliance, und wählen Sie Einstellungen bearbeiten.
3. Wählen Sie auf der Registerkarte Hardware die Option Speicher.
4. Klicken Sie auf OK.
5. Wählen Sie die gewünschte Speichergröße

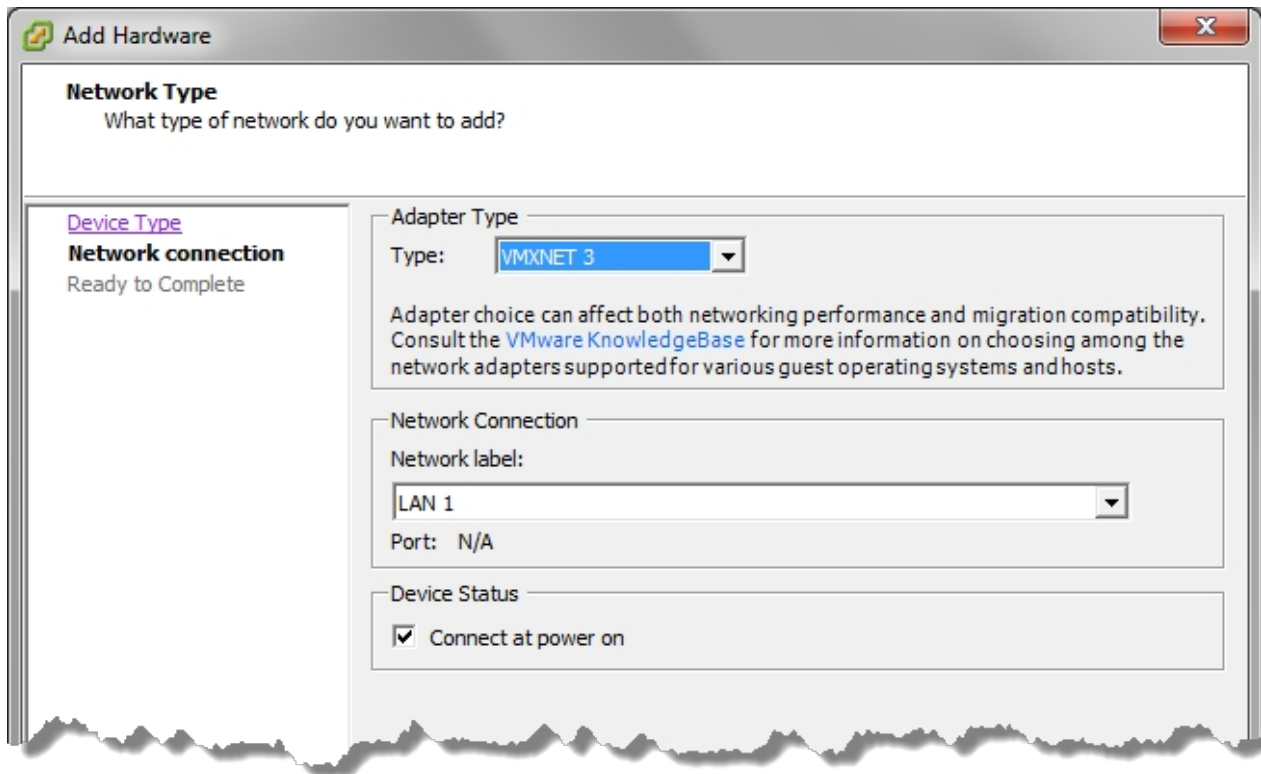


Anpassen der für die virtuelle Maschine verfügbaren NICs

Standardmäßig sind alle GFI ClearView Virtual Appliances mit zwei Netzwerkkarten ausgestattet. Die erste NIC ist die Verwaltungsschnittstelle (für die Verwaltung der virtuellen Appliance), die zweite NIC ist die Hilfsschnittstelle (für HA-Topologien, Clustering und Out-of-Path-Implementierungen) und wird hauptsächlich für die Verbindung mit der Schnittstelle des Host-Rechners verwendet, die gespiegelten Datenverkehr vom Switch empfängt.

Wenn Sie weitere NICs hinzufügen müssen, können Sie dies mit den folgenden Schritten tun:

1. Öffnen Sie den VMware vSphere-Client.
2. Klicken Sie mit der rechten Maustaste auf die GFI ClearView Virtual Appliance, und wählen Sie Eigenschaften.
3. Wechseln Sie zur Registerkarte Hardware.
4. Klicken Sie auf Hinzufügen.
5. Wählen Sie in der Liste Gerätetyp die Option Ethernet-Adapter und klicken Sie auf Weiter.
6. Wählen Sie in der Liste Adaptertyp die Option VMXNET 3.
7. Wählen Sie das Netzwerk aus, dem die Netzwerkkarte zugeordnet werden soll.

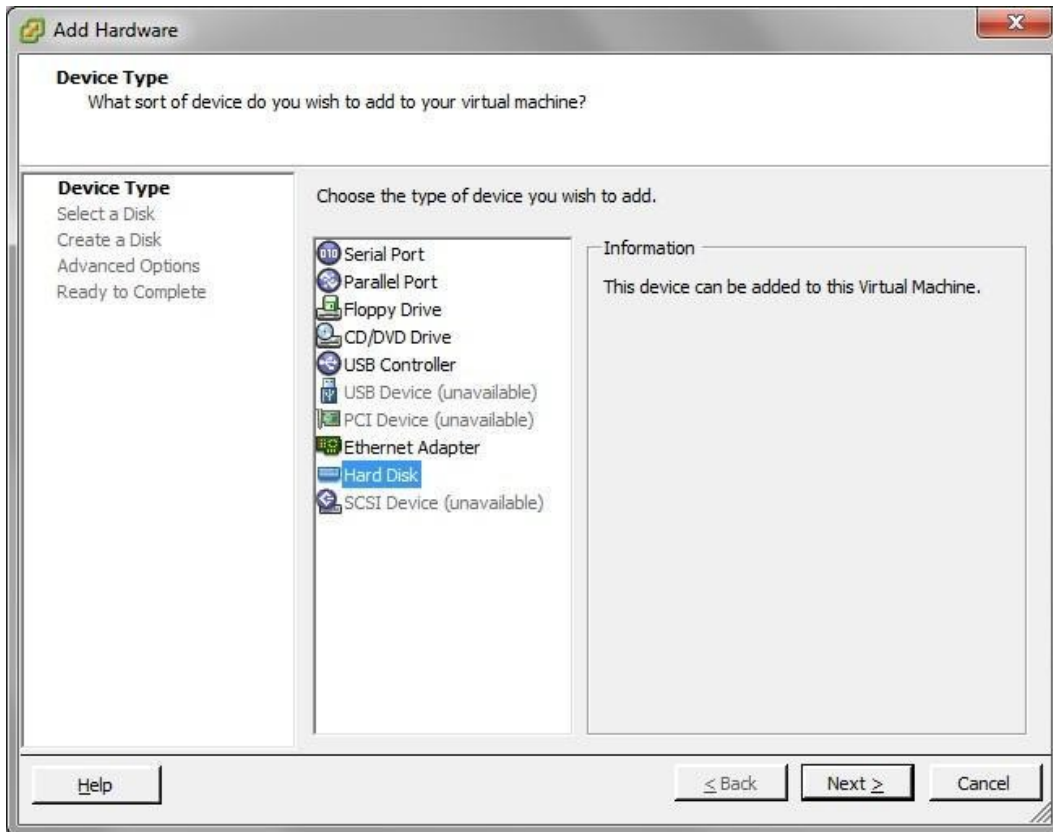


8. Klicken Sie auf Weiter.
9. Überprüfen Sie die Informationen und klicken Sie auf Fertig stellen, um die NIC hinzuzufügen.
10. Starten Sie die virtuelle Appliance neu. Die neuen NICs werden automatisch erkannt.

Hinzufügen von Speicher zur virtuellen VMware-Maschine

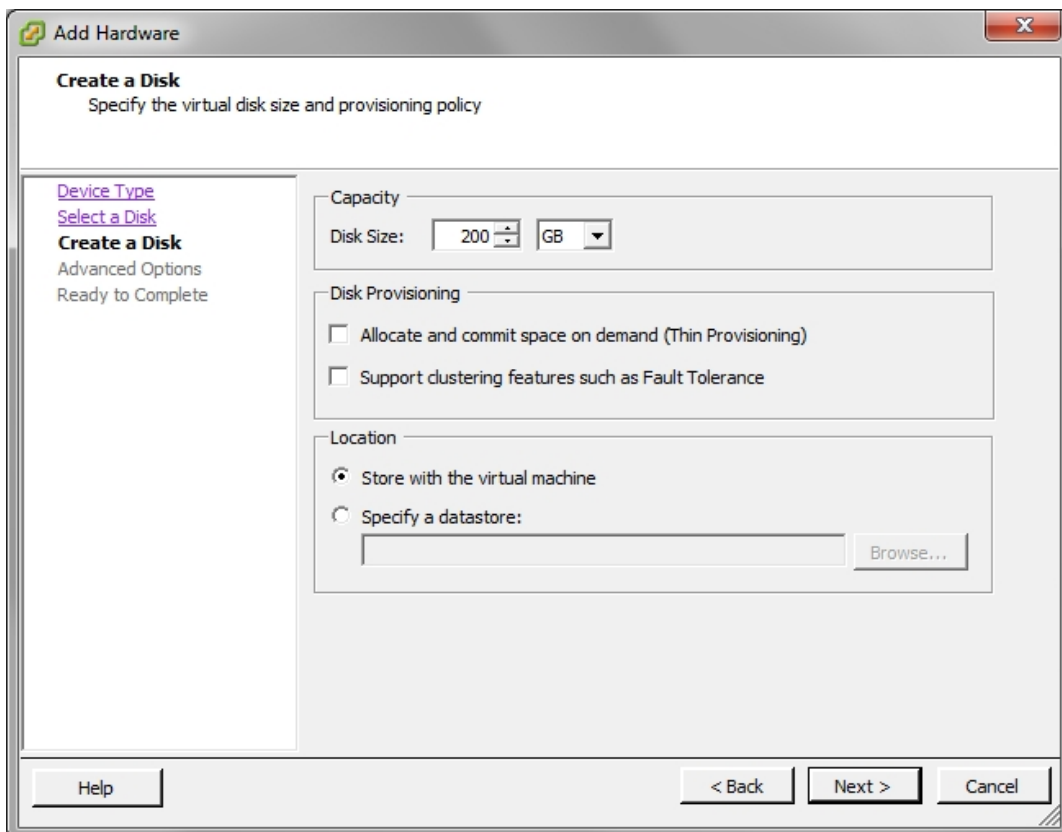
Standardmäßig werden alle virtuellen GFI ClearView-Appliances mit einer einzigen Festplatte von 50 GB (feste Größe) ausgeliefert. Je nach Ihren Anforderungen an die Berichterstellung können Sie weitere Festplatten hinzufügen, indem Sie das folgende Verfahren befolgen:

1. Öffnen Sie den VMware vSphere-Client.
2. Klicken Sie auf der Registerkarte Hardware Bildschirms Eigenschaften der virtuellen GFI ClearView-Apliance auf Hinzufügen.

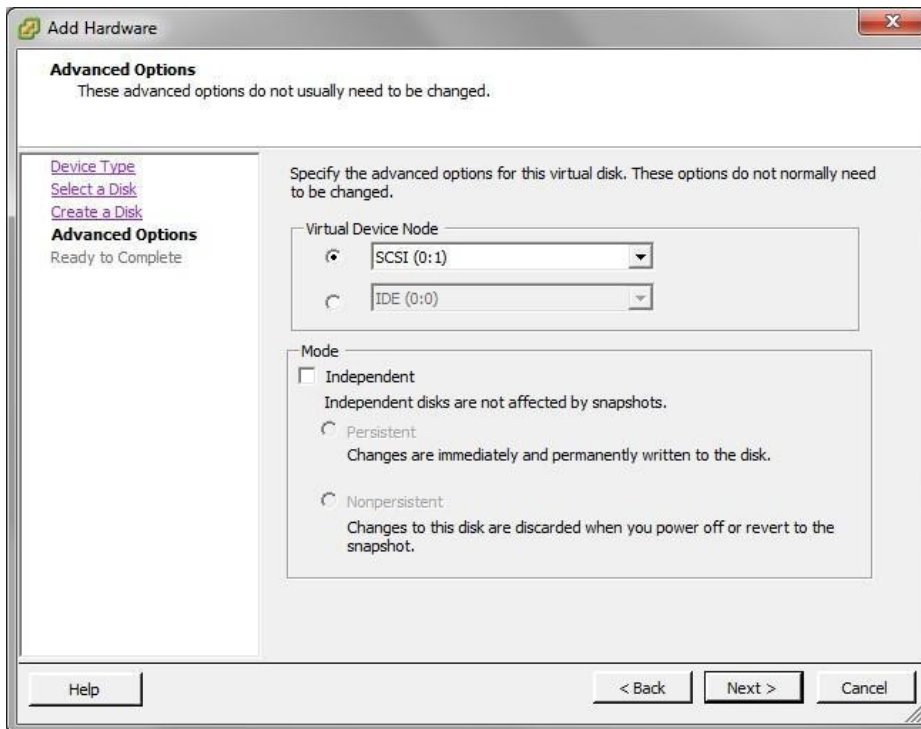


3. Wählen Sie Festplatte und klicken Sie dann auf Weiter.

4. Geben Sie die Größe der zu erstellenden zusätzlichen Festplatte an. Dieser Speicherplatz wird zu den standardmäßigen 50 GB hinzugefügt, die mit der virtuellen Appliance geliefert werden. Wenn Sie hier also einen 200 GB großen Datenträger hinzufügen, beträgt der Gesamtspeicherplatz für die virtuelle Appliance 250 GB.



- Klicken Sie auf Weiter.
- Schließen Sie die neue Festplatte an den nächsten verfügbaren SCSI-Knoten an, um die beste Leistung zu erzielen.



- Klicken Sie auf Weiter.
- Überprüfen Sie die Informationen und klicken Sie auf Fertig stellen, um den Datenträger hinzuzufügen.
- Wenn die Virtual Appliance das nächste Mal gebootet wird, können Sie die Speicherbefehle in der CLI verwenden, um den neuen Speicher bereitzustellen. Der Befehl `show storage` listet die aktuellen Speicherzuweisungen sowie die Festplatten der Virtual Appliance auf.

```
(config) # show storage
Services:
 cifs: available - 3743.46M free of 3876M total
 edge-cache: available - 3723.53M free of 3872M
 total monitor: available - 9882.83M free of 10G
 total users: available - 974.62M free of 1024M
 total
 wan-memory: available - 17.21G free of 17.65G total

Disks:
 sda10(internal): in use - 36.22 GB
 sdb: not in use - 214.7 GB

Total: 36.22
Unallocated: 0
```

- Die Ausgabe zeigt, dass unsere neue 200G-Platte 'sdb' heißt und derzeit nicht verwendet wird. Die Der Befehl `storage disk add` wird zur Bereitstellung der neuen Festplatte verwendet.

```
(config) # storage disk add sdb
This will erase all data on the disk. Do you really want to do this (Y/N)?
[N] Y
```

11. Nachdem dieser Befehl ausgeführt wurde, zeigt ein weiterer Blick auf `show storage`, dass die neue Festplatte nun in Gebrauch ist und unsere 200G bereit für die Zuweisung sind.

```
(config) # show storage
Services:
  cifs: available - 3743.46M free of 3876M total
  edge-cache: available - 3723.53M free of 3872M
  total monitor: available - 9882.83M free of 10G
  total users: available - 974.62M free of 1024M
  total
  wan-memory: available - 17.21G free of 17.65G total

Disks:
  sda10(internal): in use - 36.22 GB
  sdb: in use - 200.00 GB

Total: 236.21G
Unallocated: 200G
```

Starten der VMware Virtual Appliance

Wenn Sie bereit sind, die virtuelle Appliance zum ersten Mal zu starten, schalten Sie sie ein. Die virtuelle Appliance startet und zeigt eine Anmeldeaufforderung auf der VMware-Konsole an. Zu diesem Zeitpunkt können Sie sich mit dem Standardbenutzernamen `admin` und dem Passwort `exinda` anmelden.

Wenn die erste Netzwerkkarte mit einem Netzwerk verbunden ist, das Adressen über DHCP bereitstellt, sollte die virtuelle Appliance eine IP-Adresse abgerufen haben. Auf dem Übersichtsbildschirm der virtuellen Appliance sollten die VMware-Tools die IP-Adresse anzeigen, die die virtuelle Appliance erhalten hat.

```
VMware Tools:    Unmanaged
IP Addresses:    192.168.0.221
DNS Name:        exinda-aab541
```

Wenn die erste Netzwerkkarte keine Adresse über DHCP beziehen kann, müssen Sie über die VMware-Konsole die folgenden CLI-Befehle eingeben, um eine statische IP-Adresse festzulegen.

```
> en
# conf t
(config) # interface eth0 ip address <ip> <netmask>
(config) # ip default-gateway <default gateway>
(config) # ip name-server <dns server>
```

Sobald Sie die IP-Adresse bestimmt oder eine statische IP-Adresse festgelegt haben, können Sie auf die webbasierte Benutzeroberfläche zugreifen, indem Sie zu `https://<IP-Adresse>` navigieren.

2.2.4 Verwandte Themen

Zu diesem Zeitpunkt sollten die folgenden Aufgaben abgeschlossen sein, bevor Sie die virtuelle Appliance verwenden:

- Fügen Sie zusätzliche [NICs](#) hinzu (falls erforderlich) und stellen Sie die virtuelle Appliance entweder in-line oder out-of-path bereit.

- Hinzufügen und Bereitstellen von zusätzlichem [Speicher](#) (falls erforderlich).
- Erwerben Sie eine Lizenz für diese Virtual Appliance.

Ausführung auf Microsoft Hyper- V

In den folgenden Abschnitten wird beschrieben, wie Sie die GFI ClearView Virtual Appliance bereitstellen und die virtuelle Hardware an Ihre Anforderungen anpassen können.

Die GFI ClearView Virtual Appliance ist für Microsoft Hyper-V-Hypervisoren verfügbar.

Installieren Sie die virtuelle Maschine auf Hyper- V

Die virtuellen GFI ClearView-Appliances wurden für den Einsatz in verschiedenen virtuellen Umgebungen entwickelt. Hyper-V bietet Unterstützung für das Hosting der virtuellen GFI ClearView Appliances in Microsoft Server 2012 (R2) und höher. Die detaillierten Installationsschritte finden Sie im [Video Installationsanleitung](#) zusammen mit der [Anleitung für die HyperV Port-Spiegelung](#). Zur Installation der Appliance benötigen Sie außerdem die [ISO-Datei](#).

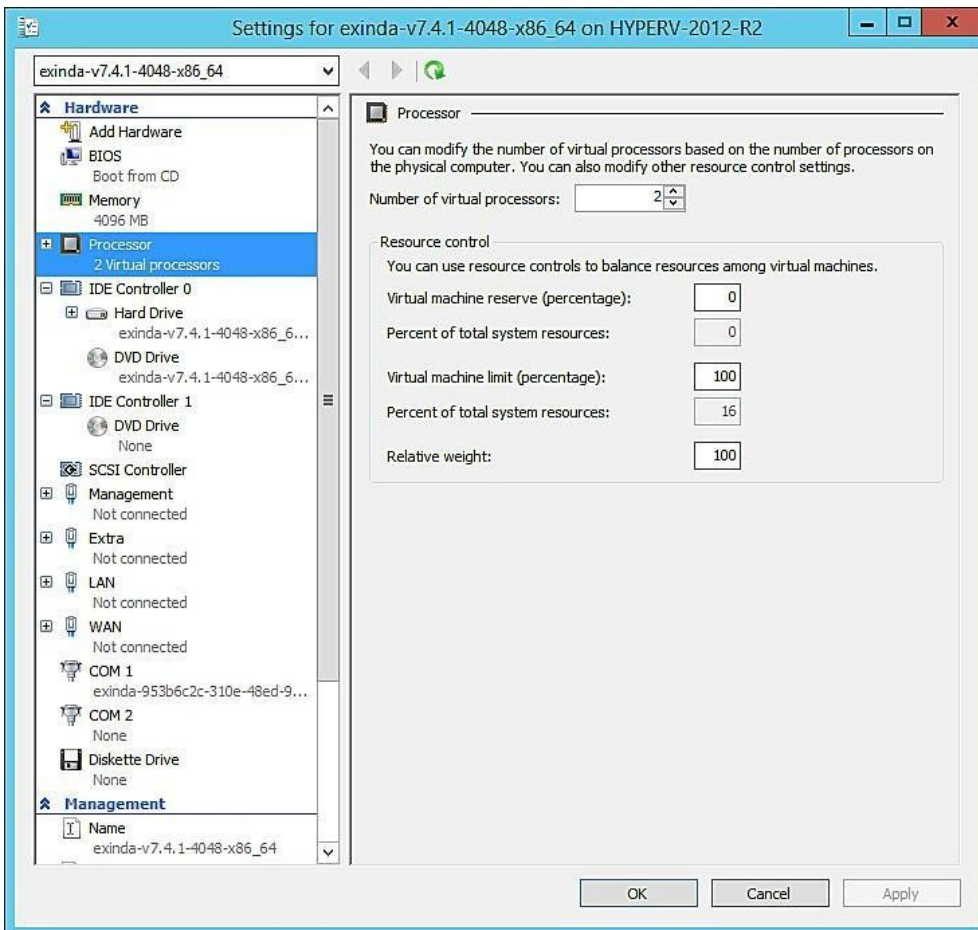
Die von GFI gelieferte virtuelle Maschine verfügt möglicherweise nicht über alle Konfigurationsoptionen, die Sie wünschen. So ist beispielsweise der Festplattenspeicher auf 50 GB beschränkt, was für Ihre Anforderungen wahrscheinlich nicht ausreicht. Bei der Vorbereitung der ISO-Datei Virtual Appliance für den Download ist es nicht möglich zu wissen, welche Hardware auf dem Host-Rechner vorhanden ist. Nachdem Sie die virtuelle Maschine installiert haben, müssen Sie einige Anpassungen an der Konfiguration mit Hilfe der Steuerelemente im Hyper-V-Manager vornehmen. Siehe die folgenden zugehörigen Aufgaben.

2.2.5 Verwandte Themen

Anpassen der Anzahl der für die virtuelle Maschine verfügbaren CPUs

Nach der Installation der virtuellen Maschine müssen Sie möglicherweise die Anzahl der CPUs anpassen, die GFI ClearView Virtual Appliance zur Verfügung stehen. Die Grundkonfiguration der virtuellen Maschine umfasst eine minimale Anzahl von CPUs. Wenn Sie jedoch über freie CPUs auf dem Host-Rechner verfügen, können Sie diese für die virtuelle Maschine verfügbar machen. Sie können die Anzahl der CPUs im Hyper-V Manager anpassen.

1. Öffnen Sie den Hyper-V-Manager.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf die virtuelle Maschine, die Sie bearbeiten möchten, und wählen Sie **Einstellungen**. Das Dialogfeld Einstellungen für die virtuelle Maschine wird geöffnet.
3. Wählen Sie im linken Fensterbereich unter **Hardware** den Eintrag **Prozessor**. Die Prozesseureinstellungen werden im rechten Fensterbereich geöffnet.



4. Klicken Sie in der Spinbox **Anzahl der virtuellen Prozessoren** auf die Pfeile nach oben oder unten, um die Anzahl der CPUs anzupassen.

NOTE

In this pane you can also adjust several other settings to balance resources among any other virtual machines. Consult the Hyper-V documentation for more information on these settings.

5. Klicken Sie auf **OK**. Die Anzahl der für die virtuelle Maschine verfügbaren CPUs wird sofort angepasst.

NOTE

These instructions also apply to changing the configuration after the virtual appliance has entered service.

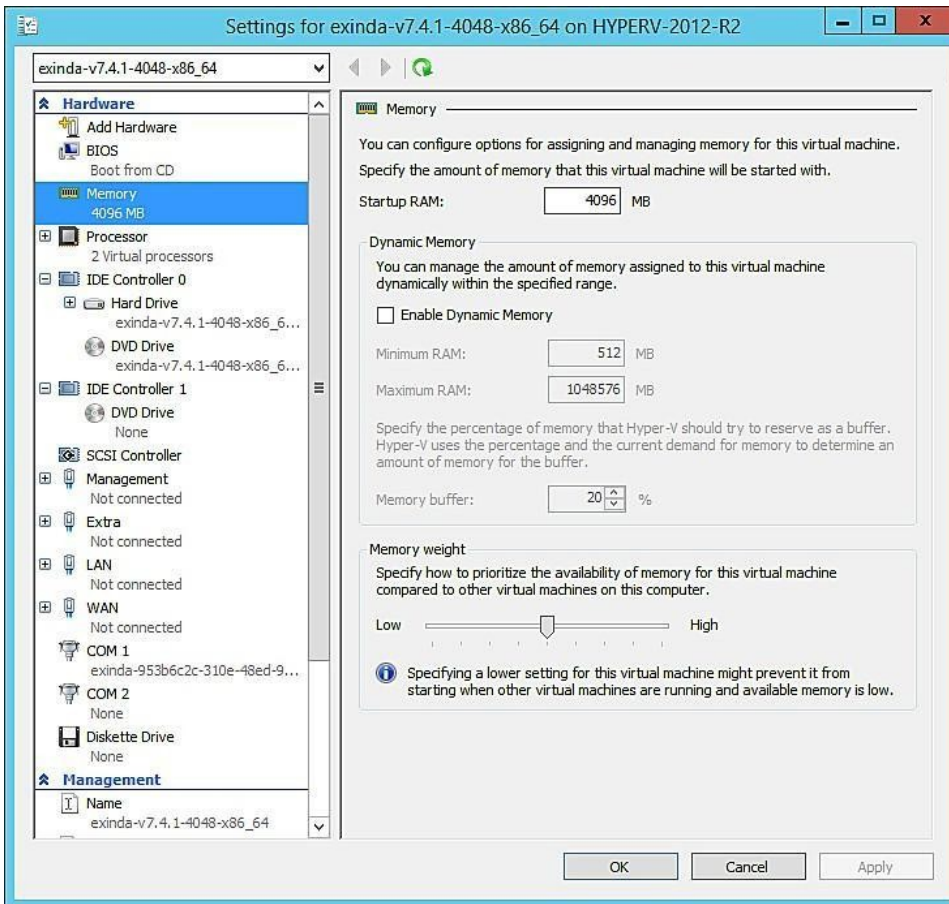
2.2.6 Verwandte Themen

Anpassen des für die virtuelle Maschine verfügbaren Arbeitsspeichers

Nach der Installation der virtuellen Maschine müssen Sie möglicherweise den für die GFI ClearView Virtual Appliance verfügbaren RAM-Speicher anpassen. Die GFI ClearView Virtual Appliance verfügt über eine Grundmenge an Arbeitsspeicher. Wenn Sie jedoch über zusätzlichen Arbeitsspeicher auf dem Host-Rechner verfügen, sollten Sie diesen für die virtuelle Maschine verfügbar machen. Sie können die Größe des Arbeitsspeichers im Hyper-V Manager anpassen.

1. Öffnen Sie den Hyper-V-Manager.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf die virtuelle Maschine, die Sie bearbeiten möchten, und wählen Sie **Einstellungen**. Das Dialogfeld Einstellungen für die virtuelle Maschine wird geöffnet.

3. Wählen Sie im linken Fensterbereich unter **Hardware** den Eintrag **Speicher**. Die Speichereinstellungen werden im rechten



Fensterbereich geöffnet.

4. Geben Sie in das Feld **Startup-RAM** einen neuen Wert für Menge des Arbeitsspeichers ein.

NOTE

These instructions also apply to changing the configuration after the virtual appliance has entered service.

5. Klicken Sie auf **OK**. Die Menge des für die virtuelle Maschine verfügbaren Arbeitsspeichers wird sofort angepasst.

2.2.7 Verwandte Themen

Erhöhen Sie den Speicherplatz durch Hinzufügen neuer virtueller Laufwerke

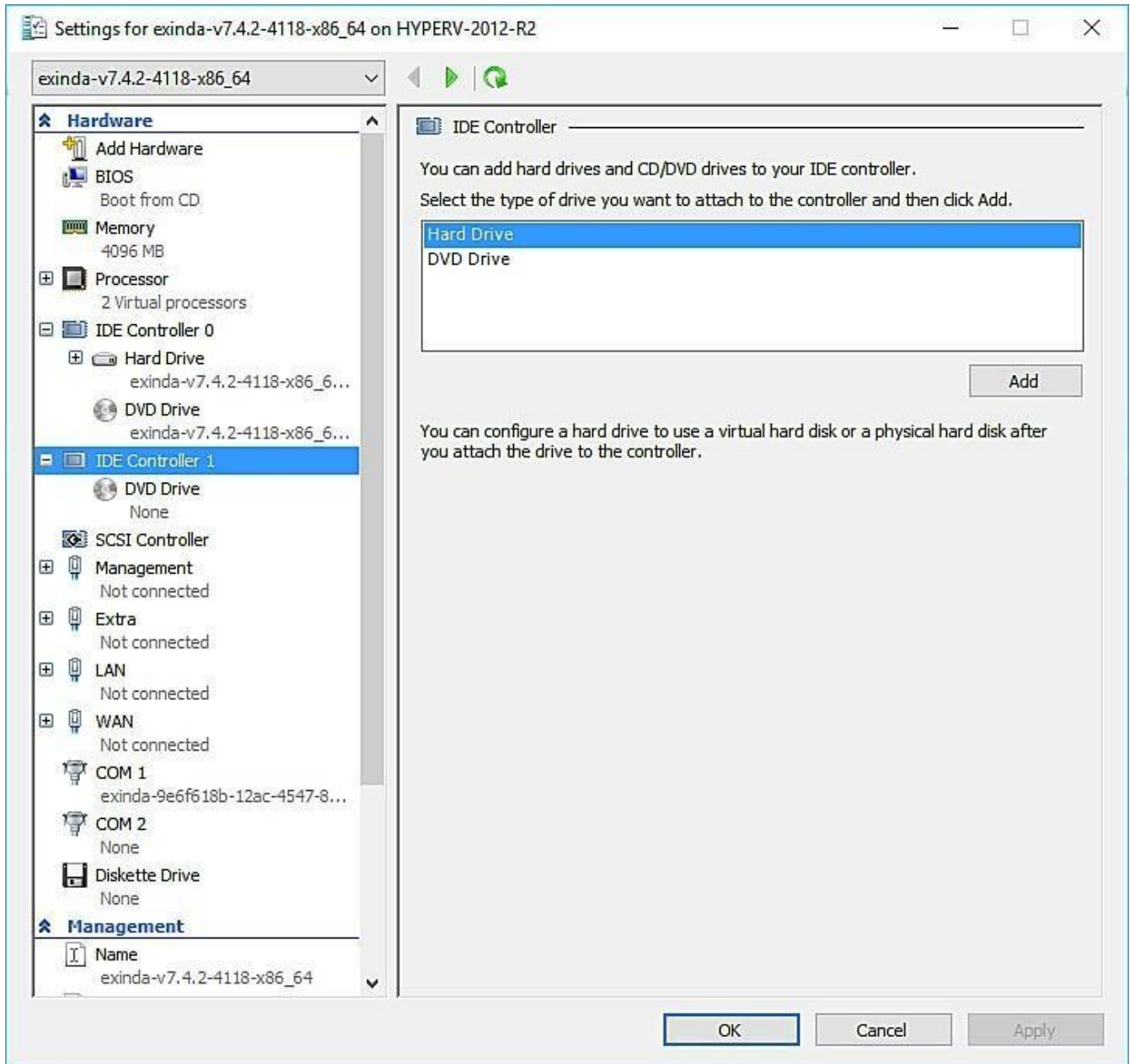
Während der Installation der virtuellen Maschine mussten Sie die virtuelle Festplatte (VHD) mit der GFI ClearView Virtual Appliance verbinden. Bevor Sie die virtuelle Maschine zum ersten einschalten, Sie wahrscheinlich die Größe der VHD erhöhen. Sie können diese Anpassung auch vornehmen, nachdem Sie die GFI ClearView Virtual Appliance in Betrieb genommen haben. Sie können die Größe der VHD im Hyper-V Manager anpassen, indem Sie der VM zusätzliche Festplatten hinzufügen.

Voraussetzungen

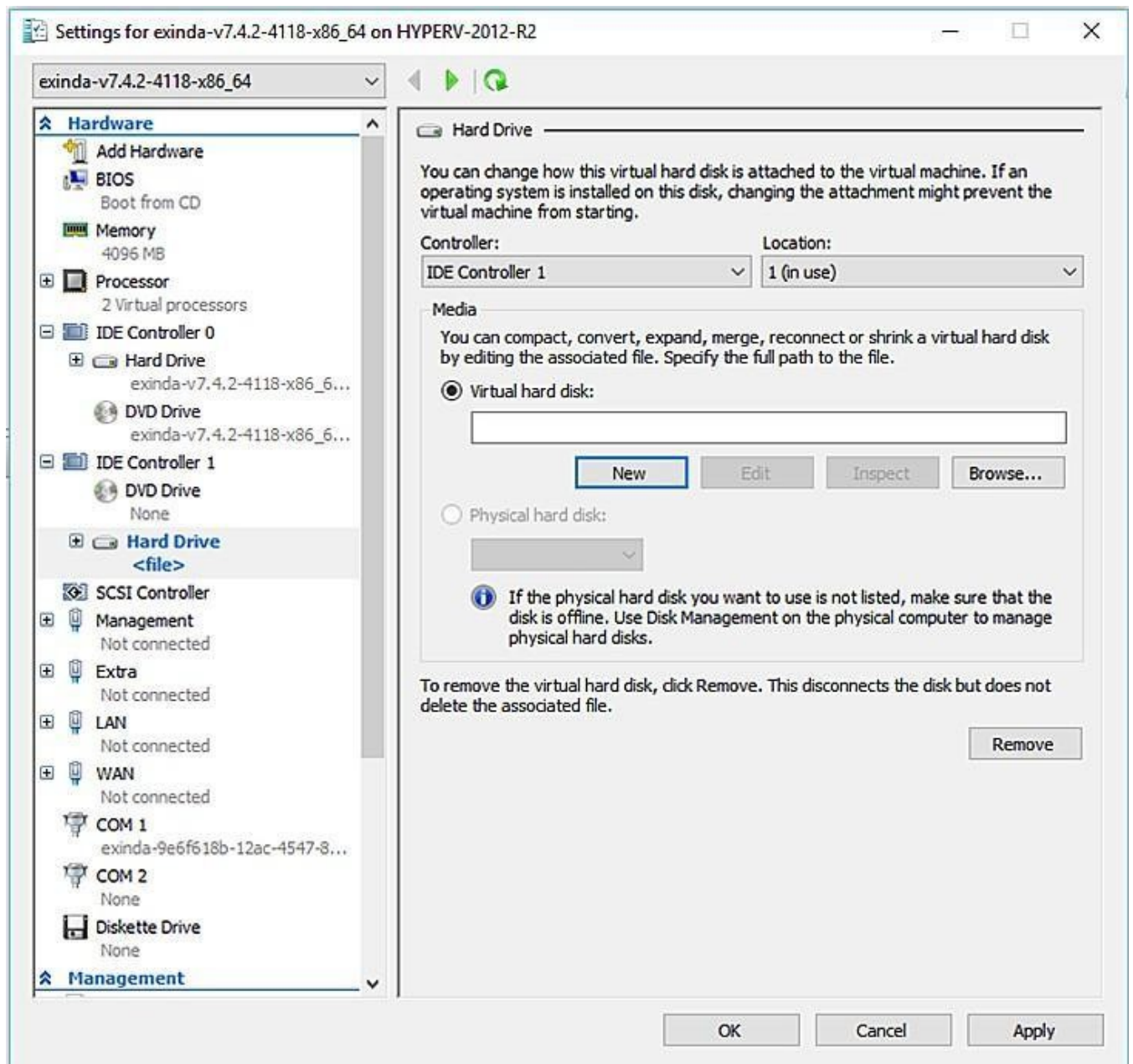
Vergewissern Sie sich vor dem Start dieser Aufgabe, dass die virtuelle Maschine ausgeschaltet ist.

Verfahren

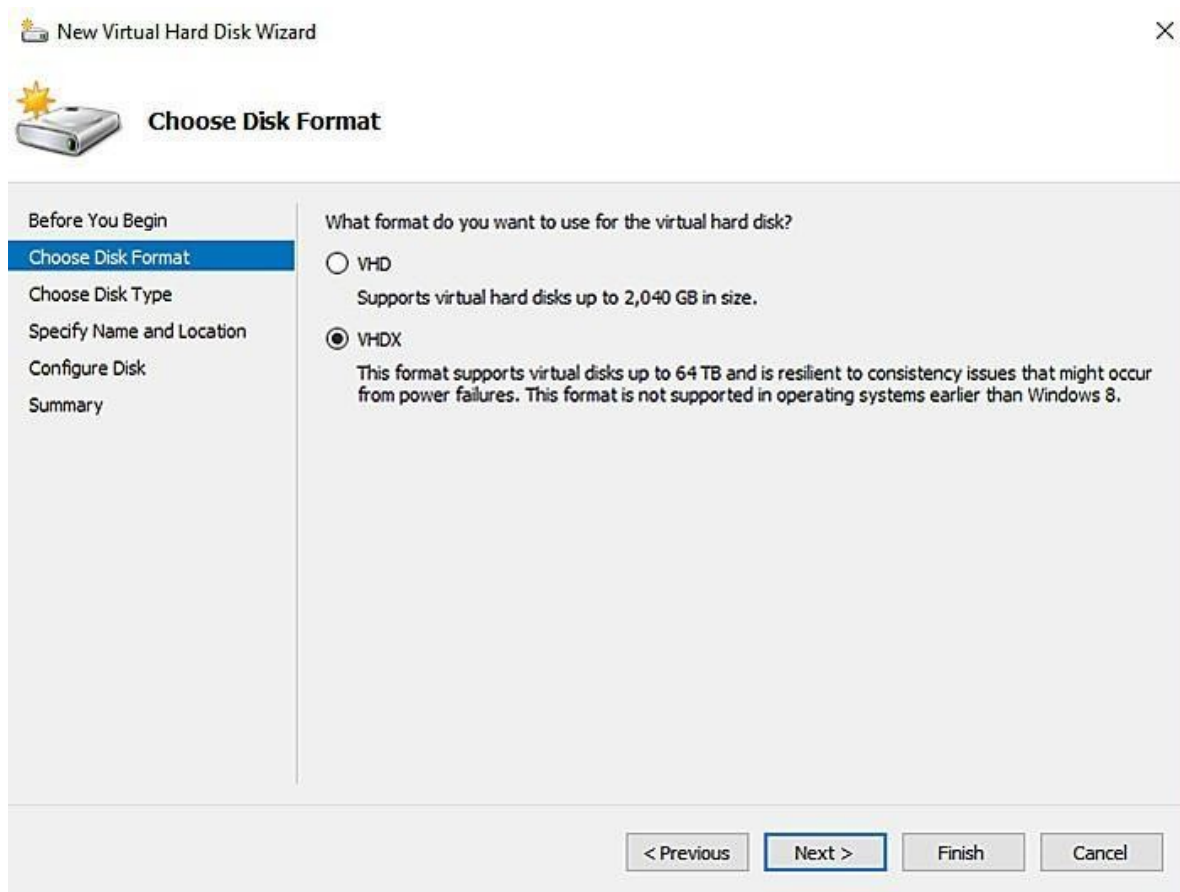
1. Öffnen Sie den Hyper-V Manager, klicken Sie im linken Fenster mit der rechten Maustaste auf die virtuelle Maschine, die Sie bearbeiten möchten, und wählen Sie **Einstellungen**. Das Dialogfeld Einstellungen für die virtuelle Maschine wird geöffnet.
2. Wählen Sie im linken Fensterbereich unter **Hardware** einen beliebigen IDE-Controller aus. Die Festplatteneinstellungen werden im rechten Fensterbereich geöffnet.
3. Wählen Sie im rechten Fenster die Option **Festplatte** und klicken Sie auf **Hinzufügen**.



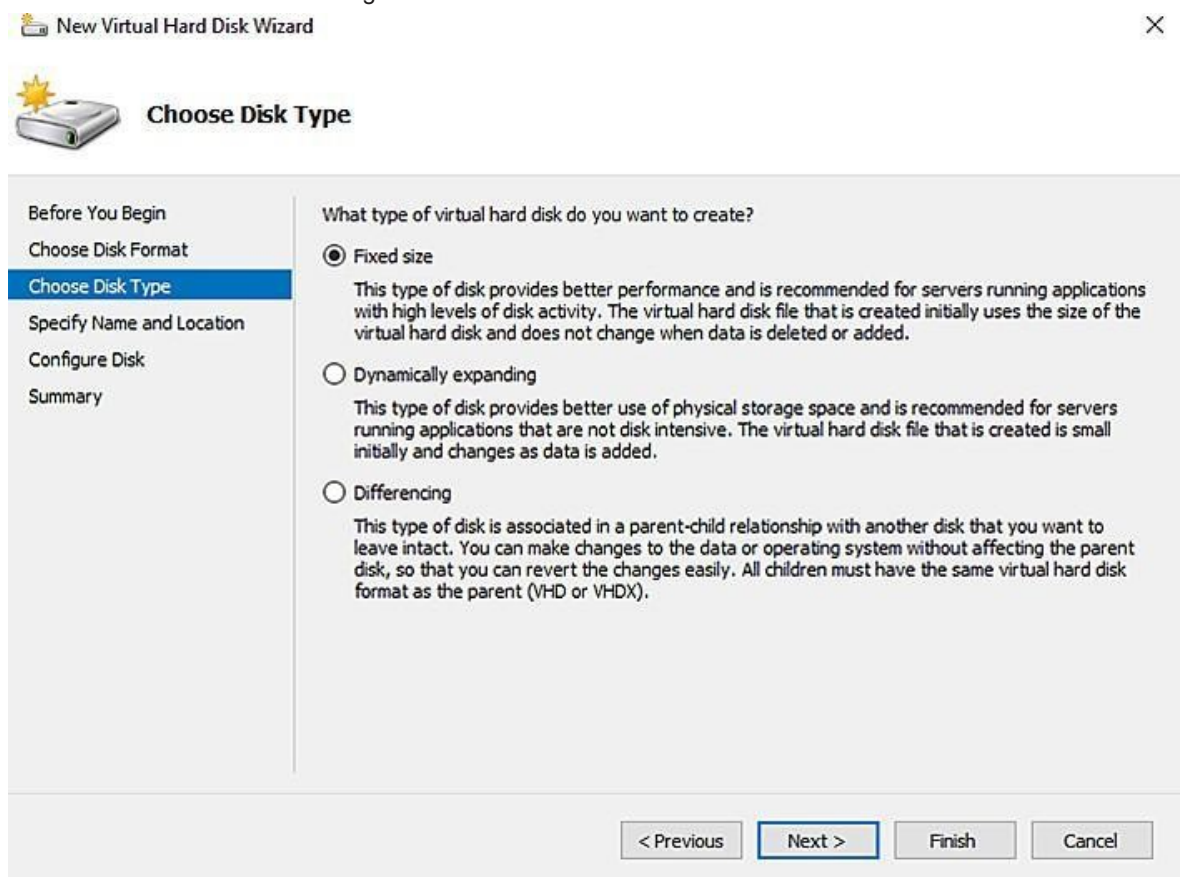
4. Wählen Sie im Abschnitt "Festplatte" als Controller "IDE Controller 1" und als Speicherort "1 (in Gebrauch)". Standardmäßig ist dies der einzige verfügbare Steckplatz in der virtuellen Maschine, in den Sie eine neue virtuelle Festplatte einfügen können. Wenn jedoch in Zukunft mehr Festplatten benötigt werden, können Sie die standardmäßig vorhandenen DVD-Laufwerke entfernen, da diese in der nicht benötigt werden. In diesem Fall sind Controller 0: Speicherplatz 1 und Controller 1: Speicherplatz 0 ebenfalls für die weitere Verwendung verfügbar.



5. Klicken Sie auf **Neu**. Der Assistent für neue virtuelle Festplatten wird geöffnet.



6. Wählen Sie VHDX als Datenträgerformat und klicken Sie auf **Weiter**.



7. Wählen Sie im Abschnitt **Datenträgertyp auswählen** die Option **Feste Größe** und klicken Sie auf **Weiter**.



Specify Name and Location

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

Specify the name and location of the virtual hard disk file.

Name:

Location:

< Previous

8. Geben Sie einen **Namen** und einen **Speicherort** für die virtuelle Festplatte an, und klicken Sie auf **Weiter**.



Configure Disk

Before You Begin

Choose Disk Format

Choose Disk Type

Specify Name and Location

Configure Disk

Summary

You can create a blank virtual hard disk or copy the contents of an existing physical disk.

Create a new blank virtual hard disk

Size: GB (Maximum: 64 TB)

Copy the contents of the specified physical disk:

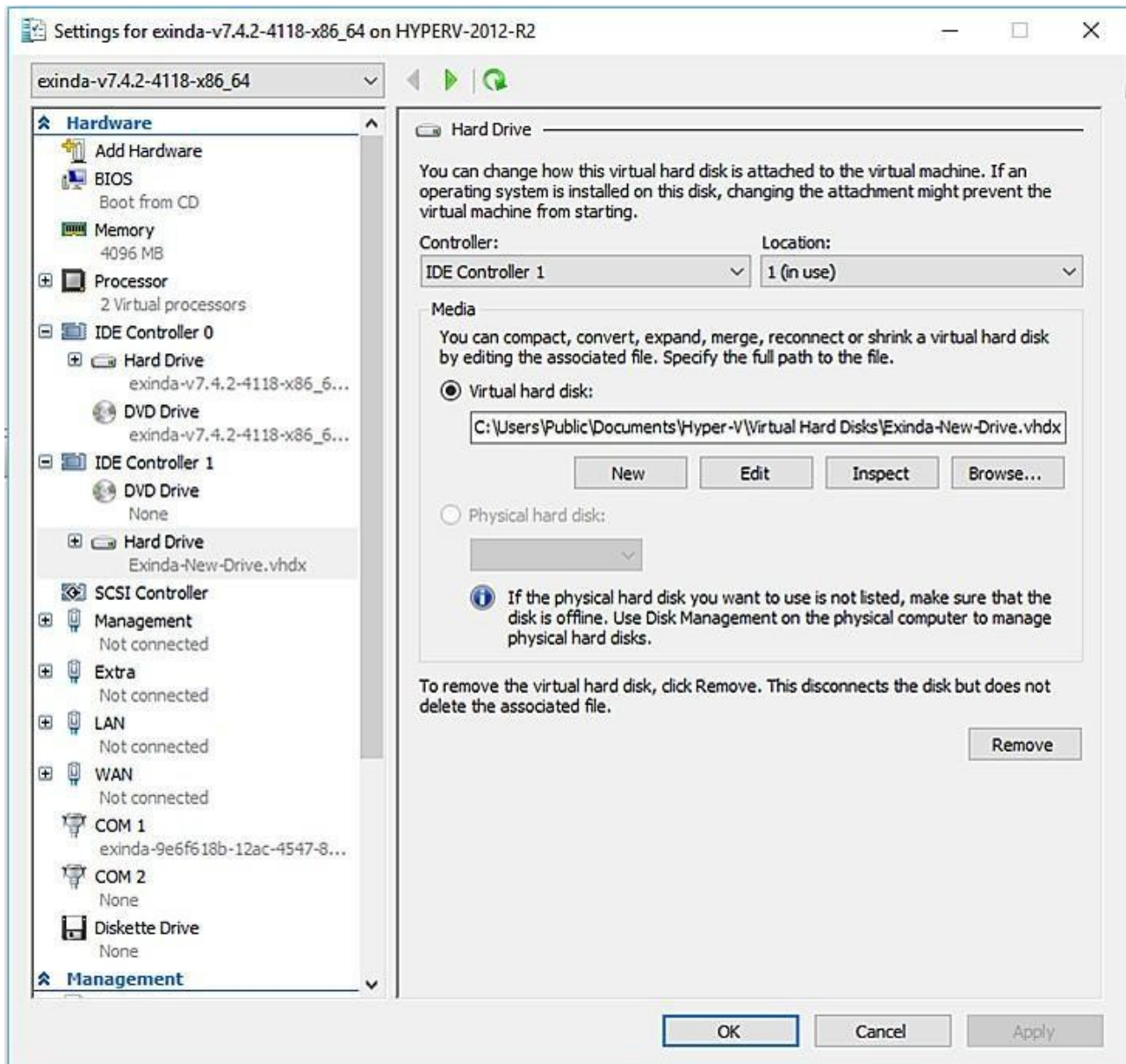
Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	930 GB

Copy the contents of the specified virtual hard disk

Path:

< Previous

9. Legen Sie die **Festplattengröße** fest und klicken Sie auf **Weiter**.
10. Klicken Sie auf **Fertig stellen**, um das zu erstellen. Dies kann ein paar Minuten dauern.



11. Wenn die Seite mit den Festplatteneinstellungen für das neu erstellte Laufwerk geöffnet wird, klicken Sie auf **OK**.
12. Starten Sie die virtuelle Maschine. Wenn die virtuelle Maschine startet, wird das neue Laufwerk automatisch erkannt, aber der neue Speicher muss der virtuellen Appliance manuell hinzugefügt werden.

NOTE

Before connecting, the management interface must already have been configured with an IP address or will obtain an IP address using DHCP. You need to make sure that the Management Interface is connected to the proper Virtual Switch in your Hyper-V environment.

13. Suchen Sie die IP-Adresse, die der Verwaltungsschnittstelle zugewiesen ist, indem Sie mit der rechten Maustaste auf die VM klicken und die Option **Verbinden** wählen. Dies ermöglicht den Zugriff auf die Konsole.
14. Melden Sie sich bei der Appliance mit den Standard-Anmeldeinformationen an (Benutzername: admin, Passwort: exinda). Bevor Sie fortfahren, müssen Sie möglicherweise die EULA akzeptieren.
15. Wenden Sie die folgenden Befehle an. Die Ausgabe enthält die IP-Adresse, die Sie für den Zugriff auf die Web-Benutzeroberfläche der Appliance benötigen.

```
exinda> de
exinda># show int eth0
```

16. Stellen Sie mit einem Browser über HTTPS eine Verbindung zur GFI ClearView-Appliance her.
17. Wenn Sie angemeldet, klicken Sie auf **Konfiguration> System> Setup> Storage**.
18. Fügen Sie das neue Laufwerk hinzu.

NOTE

The following screenshot assumes that the chosen controller was **1**, and the location was **0**, so the new drive is **sdd**.

Configuration

- Traffic Policies
- Optimizer
- Objects
 - Network
 - Users & Groups
 - VLANs
 - Protocols
 - Applications
 - Schedules
 - Adaptive Response
 - Service Levels
 - HTML Response
- System
 - Basic Install Wizard
 - Network
 - Setup
 - Optimization
 - Certificates
 - Authentication
 - Logging
 - Diagnostics
 - Maintenance
 - Tools

System Setup

Date and Time | Access | SDP | SQL Access | Monitoring | Netflow | Scheduled Jobs | Alerts | License | Control | **Storage**

Modify Exinda appliance disk storage settings.
 Before changing the size of a partition, you must remove the encryption on the partition and put the appliance into [Bypass mode](#).

Disk Storage Map.

Service	Status	Free	Size	Minimum	Encrypted	Operation
cifs	available	5117.65M 96%	5340.00M	1024.00M	✗	Resize Format Encrypt
edge-cache	available	2184.37M 95%	2304.00M	1024.00M	✗	Resize Format Encrypt
monitor	available	9657.20M 94%	10.00G	10.00G		Resize Format
users	available	974.62M 95%	1024.00M	512.00M		Resize Format
wan-memory	available	8168.84M 97%	8448.00M	5120.00M	✗	Resize Format Encrypt
unallocated storage			200.00G			
Total Available Storage:			228.71G			

Disk	Status	Size	Operation
sda	in-use		
sdb	unused	214.7 GB	Add
sdc10	in-use	28.72 GiB	Remove
sdd	in-use	200.00 GiB	Add

Refresh Disk Information

Der neue Speicherplatz erscheint als "nicht zugewiesener Speicher" im Abschnitt "Speicherkonfiguration".

19. Weisen Sie den Speicherplatz entsprechend zu.

2.2.8 Verwandte Themen

Anpassen einer virtuellen Hyper-V-Maschine

Die mitgelieferten GFI ClearView Virtual Appliances erfordern einige Konfigurationsänderungen, bevor Sie sie in Ihrem Netzwerk einsetzen können. So sind beispielsweise die virtuellen Festplatten auf 50 GB begrenzt, was für Ihre Anforderungen wahrscheinlich nicht ausreicht. Die Größe der verfügbaren virtuellen Maschinen wird mit minimaler Konfiguration festgelegt, da es nicht möglich ist, genau zu wissen, welche Hardware auf einer Host-Maschine verfügbar ist. Um die Konfiguration zu bearbeiten, müssen Sie die Einstellungen für die virtuelle Maschine im Hyper-V Manager öffnen.

Für die Konfiguration der GFI ClearView Virtual Appliance beschränken sich diese Anweisungen auf das, was notwendig ist, um die Appliance in einen betriebsbereiten Zustand zu versetzen. Wenn Sie weitere Informationen benötigen, lesen Sie bitte die Dokumentation zu Hyper-V. Dieses Thema befasst sich mit Änderungen an der Konfiguration im Zusammenhang mit der

Anzahl der CPUs, des verfügbaren RAMs, der NICs und der Anpassung des Speichers für die virtuelle Maschine.

Die Konfigurationsänderungen sind vor der ersten Verwendung der virtuellen Maschine erforderlich. Sie können auch zu jedem späteren Zeitpunkt weitere Änderungen an Ihrer virtuellen Maschine vornehmen. Wenn Sie im Laufe der Zeit mehr Ressourcen für die virtuelle Maschine benötigen, können Sie sie dem Gast zur Verfügung stellen, sofern diese Ressourcen auf dem Host verfügbar sind.

2.2.9 Erstellen einer ersten Konfiguration mit dem Basis-Assistenten

Der Assistent für die Erstkonfiguration führt Sie schrittweise durch die Konfiguration der Schnittstellen der Appliance, der IP-Einstellungen, der HTTP-Proxy-Einstellungen, der grundlegenden Systeminformationen, der Lizenzinformationen und des Speichervolumens. Er bietet auch die Möglichkeit, die Firmware zu aktualisieren und den ersten Satz von Verkehrsrichtlinien zu erstellen.

1. Die GFI ClearView-Appliance bezieht standardmäßig eine IP-Adresse über DHCP. Die IP-Adresse ist auf der Verwaltungsoberfläche verfügbar.

Hinweis: Wenn keine DHCP-Adresse ausgewählt wird, verwendet die GFI ClearView-Appliance standardmäßig die IP-Adresse 172.14.1.57. Öffnen Sie einen Webbrowser, und stellen Sie eine Verbindung mit der Web-Benutzeroberfläche her, indem Sie <https://172.14.1.57> in das Adressfeld eingeben. Konfigurieren Sie die IP-Adresse Ihres PCs auf dasselbe Subnetz wie die GFI ClearView Appliance, um eine Verbindung herzustellen. Legen Sie Ihre IP-Adresse beispielsweise auf 172.14.1.58 fest, Netzmaske 255.255.255.0.

2. Rufen Sie über einen Webbrowser die folgende Website auf: <http://findmy.exinda.com/>. Daraufhin wird ein Applet heruntergeladen, das automatisch das kürzlich installierte GFI ClearView findet.

Hinweis: Das Applet auf findmyexinda.com verwendet ein Multicast-Paket, um lokale GFI ClearView Appliances zu finden. Der PC, auf dem das Applet ausgeführt wird, muss sich im selben physischen LAN befinden, damit das Applet funktioniert.

3. Klicken Sie auf die gefundene GFI ClearView-Appliance.

4. Melden Sie sich mit **username=admin** und **password=exinda** an.

5. Wählen Sie **Konfiguration > Basisinstallationsassistent**, um den Konfigurationsassistenten zu starten.

- **Basisassistent Schritt 1 - Schnittstellen:** Auf diesem Bildschirm werden alle Systemschnittstellen aufgelistet und eventuelle Probleme mit den Schnittstellen gemeldet. Auf diesem Bildschirm können Sie die Schnittstellengeschwindigkeit und die Duplex-Einstellungen festlegen.

Step 1: Interfaces

Interface	Speed	Duplex	Link Status
eth0	Auto	Auto	✓
eth1	Auto	Auto	✓
eth2	Auto	Auto	✓
eth3	Auto	Auto	✓

[eth0] [eth1] [eth2] LAN [eth3] WAN

Back Next

Basis-Assistent Schritt 2 - IPEinstellungen: Auf diesem Bildschirm können Sie grundlegende Einstellungen für die Netzwerkkonnektivität konfigurieren. Sie können diese Einstellungen entweder manuell festlegen oder **Autoconf** wählen, um diese Einstellungen automatisch zu übernehmen. Die gewählte Art der automatischen Konfiguration hängt von Ihrem Netzwerk ab. Für IPv4-Netzwerke wählen Sie **DHCP**, für IPv6 verwenden Sie **SLAAC**.

Step 2: IP Settings

Static
 Autoconf

* Address (eth0) /

Default IPv4 Gateway

Default IPv6 Gateway

* Host Name

Primary DNS

Secondary DNS

[eth0] [eth1] [eth2] LAN [eth3] WAN

* Required field

Back Next

- Basisassistent Schritt 3 - HTTPProxy-Einstellungen:** Um der Appliance den Zugriff auf den HTTP-Server von GFI ClearView für Firmware-Updates, Lizenz-Updates und Meldungen zu ermöglichen, geben Sie einen HTTP-Proxy an. Wenn Sie SDP aktiviert haben, stellen Sie sicher, dass Ihr Proxy HTTPS unterstützt.

Step 3: HTTP Proxy Settings

Specify a HTTP proxy so the appliance can access Exinda's HTTP server for firmware updates, license updates and messages. If you have SDP enabled, please ensure your proxy supports HTTPS.

HTTP(S) Proxy Address	<input type="text" value="lab-services.wat.exinda.com"/>	HTTP(S) Proxy Authentication	<input type="text" value="None"/>
HTTP(S) Proxy Port	<input type="text" value="3128"/>	HTTP(S) Proxy Username	<input type="text"/>
		HTTP(S) Proxy Password	<input type="password" value="*****"/>
		Do not verify SSL certificates	<input checked="" type="checkbox"/>

- **Basis-Assistent Schritt 4 - System:** Auf diesem Bildschirm können Sie grundlegende Systemeinstellungen vornehmen.

Step 4: System

Domain Name	<input type="text" value="exinda.com"/>	New admin Password	<input type="password"/>
SMTP Server Name	<input type="text" value="smtp.gmail.com"/>	Confirm Password	<input type="password"/>
Time Zone	<input type="text" value="UTC"/>		

- **Basis-Assistent Schritt 5 - Lizenzierung:** Auf diesem Bildschirm können Sie die Lizenz des Systems konfigurieren. Wenn Sie den Bildschirm aufrufen, versucht die GFI ClearView-Appliance, den GFI ClearView-Lizenzserver im zu kontaktieren. Wenn die Appliance über eine Internetverbindung verfügt und eine neue oder aktualisierte Lizenz gefunden wird, wird diese im Textfeld am unteren Rand des Bildschirms angezeigt. Sie können diese Lizenz dem System hinzufügen, indem Sie auf die Schaltfläche **Lizenz hinzufügen** klicken.

Step 5: Licensing

Bandwidth	102400 kbps	Monitor	<input checked="" type="checkbox"/>
Software Subscription Expiry	Dec 31, 2016 (45d)	Optimize	<input checked="" type="checkbox"/>
License Expiry	No license expiry date	Accelerate	<input checked="" type="checkbox"/>
Host ID	0010f305cd54		

License(s) Installed:
 LK2-EXINDA-45A0-023R-GBKA-L5W3-E8H5-J434-005L-115M-05N4-BP00-5P23-45Q0-5R1L-5T24-N5U1-L5V2-G086-GT40-CB58-5KNX-KK0H-CBAY-GT38-X00K

Looking for a license online ...

Connection completed successfully. No new license found.

- **Basis-Assistent Schritt 6 - Speicher:** Dieser Bildschirm zeigt die verfügbaren Festplatten an, die der Volume-Gruppe hinzugefügt werden können.

Step 6: Storage

Do you want to add the following disks to volume group when this wizard is completed?
Note that this will delete all existing data on the disk

Volume: sdb
Model: Virtual disk
Size: 17.1 GB

Yes No

Back Next

- **Basis-Assistent Schritt 7 - Firmware:** Dieser Bildschirm zeigt den Status der auf der GFI ClearView-Applikation laufenden Firmware an. Wenn die Appliance über eine Internet-Verbindung verfügt, prüft das System, ob eine neuere Firmware verfügbar ist. Wenn ein neueres Firmware-Image verfügbar ist, werden Sie gefragt, ob Sie es herunterladen und installieren möchten.

3 Verwendung von

Dieses Thema befasst sich mit der täglichen Arbeit mit der GFI ClearView Appliance, z. B. dem Einrichten von Warnmeldungen, der Leistungsüberwachung, der Überwachung des Datenverkehrs sowie dem Verständnis von Lösungen und Empfehlungen.

3.1 Definieren einer Netzwerkumgebung

Nachdem Sie GFI ClearView mit Ihrem Netzwerk verbunden haben, müssen Sie zunächst festlegen, wie GFI ClearView Ihr Netzwerk und seine Komponenten sieht.

Stellen Sie sich vor, Sie gehen durch Ihr Büro oder Rechenzentrum und kleben Haftnotizen auf alle Server, Kabel und Racks, um sie zu identifizieren und ihre Funktionen zu notieren. Genau das tun Sie, wenn Sie in GFI ClearView Objekte definieren.

Es gibt eine Vielzahl von Objekttypen, die fast alle physischen, virtuellen und logischen Netzwerkkomponenten in Ihrer Umgebung repräsentieren.

3.1.1 Hinzufügen von Netzobjekten

Netzwerkobjekte repräsentieren Hosts in einem Netzwerk und können Subnetze, einzelne Hosts oder Gruppen von beidem umfassen. Einmal definiert, kann ein Netzwerkobjekt in der gesamten GFI ClearView Appliance zu Überwachungszwecken verwendet werden.

Netzwerkobjekte befinden sich in den Konfigurationen anderer Objekte, wie z. B. Anwendungen, Regeln für adaptive Reaktionen, Objekte für Anwendungsleistungsbewertungen und Objekte für Anwendungsleistungsmetriken.

Netzwerkobjekte werden auch verwendet, um zu bestimmen, welcher Verkehr als in Ihr Netzwerk eingehend und welcher als ausgehend betrachtet wird.

Der Standort eines Netzobjekts bestimmt die Richtung des Datenverkehrs. Wenn ein Ende des Gesprächs in einem externen Netzwerkobjekt und das andere Ende in einem internen Netzwerkobjekt definiert ist, dann wird der Verkehr von einem externen Netzwerkobjekt zu einem internen Netzwerkobjekt als eingehender Verkehr betrachtet.

Umgekehrt gilt der Verkehr von einem internen Netzobjekt zu einem externen Netzobjekt als ausgehender Verkehr.

Sie können angeben, ob Sie den Verkehr in Bezug auf das Netzobjekt, d. . den Verkehr in und aus einem bestimmten Netzobjekt, aufzeichnen möchten.

Hinzufügen von Netzwerkobjekten in der Benutzeroberfläche von GFI ClearView Web

Wenn Sie das Kontrollkästchen Subnetzbericht aktivieren, werden die Daten für das Netzwerkobjekt auf der Subnetzmonitorseite angezeigt. Diese Einstellung wirkt sich nur auf die Anzeige der Daten aus. Die Daten werden unabhängig von dieser Einstellung erfasst.

Einige Netzwerkobjekte werden von der Appliance automatisch erstellt: **ALL**, **privates Netz** und **lokales Netz**

» **Alle**- Stellt den gesamten Verkehr im Netzwerk dar. Dieses Netzwerkobjekt ist nicht bearbeitbar und kann nicht gelöscht werden.

» **privates Netz**- Repräsentiert alle möglichen nicht routbaren, privaten IP-Adressen.

» **lokal** - Wird erstellt, wenn einer oder mehreren Brückenschnittstellen eine IP-Adresse zugewiesen wird.

The screenshot shows a web form titled "Add New Network Object". It contains the following elements:

- Name:** A text input field.
- Location:** A dropdown menu currently showing "Inherit".
- Subnet Report:** An unchecked checkbox.
- Subnets:** A table with the header "IP Network Address / Mask Length". It contains four rows, each with two input fields separated by a slash (/).

Add New Network Object

Screenshot 49: Hinzufügen eines neuen Netzwerkobjekts.

Wo kann man it konfigurieren?

Gehen Sie zu **Konfiguration > Objekte > Netzwerkobjekt > Netzwerkobjekte**.

So erstellen Sie ein neues Netzwerkobjekt

1. Geben Sie einen Namen für das Netzwerkobjekt an.

2. Wählen Sie den Standort des Netzwerkobjekts - intern, extern oder geerbt Pakete werden einem Netzwerkobjekt zugeordnet, und das nächstgelegene Teilnetz innerhalb dieses Netzwerkobjekts bestimmt den Standort. Siehe Beispiele unten.

- **Intern** - Alle durch das Netzwerkobjekt definierten Subnetze und Hosts werden auf LAN-Seite der Appliance berücksichtigt.
- **Extern** - Alle durch das Netzwerkobjekt definierten Subnetze und Hosts werden auf der WAN-Seite der Appliance befindlich betrachtet.
- **Vererben** - Die Standorte der durch das Netzwerkobjekt definierten Subnetze und Hosts werden durch die engste Übereinstimmung mit anderen Netzwerkobjekten bestimmt oder vererbt.
 - Wenn alle Teilnetze dieses Netzobjekts in anderen Netzobjekten enthalten sind, die intern sind, erbt der Standort dieses Netzobjekts den internen Standort.
 - Wenn alle Teilnetze in diesem Netzobjekt in anderen Netzobjekten enthalten sind, die extern sind, erbt der Standort dieses Netzobjekts den externen Standort.
 - Wenn einige Teilnetze in diesem Netzobjekt in anderen internen Netzobjekten und einige in anderen externen Netzobjekten enthalten sind, dann wird der Standort dieses Netzobjekts gemischt.

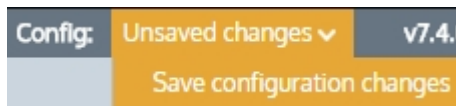
Wenn keine Netzwerkobjekte übereinstimmen, wird der Standort standardmäßig auf extern gesetzt.

NOTE

When creating network objects that have location set to "inherit", you can use the CLI command `show network-object <name>` to show the location.

3. Wählen Sie, ob der Datenverkehr für dieses Netzwerkobjekt in den Subnetzberichten angezeigt werden soll. Weitere Informationen finden Sie unter [Überwachung von Subnetzen](#).
4. Geben Sie die Netzwerk-IP-Adresse und die Länge der Netzmaske des Teilnetzes an. Es werden IPv4- und IPv6-Adressen akzeptiert. Obwohl für ein neues Objekt nur vier Zeilen für IP-Adressen angezeigt werden, können Sie weitere IP-Adressen hinzufügen, indem Sie das Netzwerkobjekt speichern und auf **Bearbeiten** klicken, um weitere vier Zeilen .
5. Klicken Sie auf **Neues Netzwerkobjekt hinzufügen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.



Beispiele für Netzwerkobjekte Definitionen

EXAMPLE – Network object defining two internal proxy servers

Create a network object that defines two internal proxy servers, 192.168.1.10 and 192.168.1.11:

```
Name: Web Proxies
Location: Internal
Subnets: 192.168.1.10 /32
Subnets: 192.168.1.11 /32
```

EXAMPLE – Head office defining a network object for a remote branch

Create a network object that defines the Head Office location, that has a subnet 10.0.100.0/24, where this Exinda appliance is NOT deployed:

```
Name: Head Office
Location: External
Subnets: 10.0.100.0 /24
```

EXAMPLE – Network object defining an internal IPv6 server

Create a network object that defines the internal IPv6 server at 2001:db8::1234:5678

```
Name: FileServer6
Location: Internal
Subnets: 2001:db8::1234:5678 /128
```

EXAMPLE - Network object with inherited location

Define three network objects as follows:

```
Name: HQ Subnets: 10.0.0.0/8 Location: External
```

```
Name: Office-A Subnets: 10.0.1.0/24 Location:
```

```
Internal Name: Server-1 Subnets: 10.0.1.200/32
```

```
Location: Inherit
```

Subnets are matched by decreasing netmask length. The Server-1 network object 10.0.1.200 will be internal, as it most closely matches the Office-A Network Object which is internal. Since the Server-1 Network Object contains a single subnet that can be matched to Office-A, its location is shown as internal.

Was ist mit dem Verkehr von intern zu intern oder von extern zu extern?

Wenn auf der Konfigurationsseite von Monitoring die Option **Ignorieren von intern zu intern** aktiviert ist, wird der gesamte Datenverkehr zwischen als intern gekennzeichneten Netzwerkobjekten ignoriert und unbeeinflusst durch die GFI ClearView-Appliance geleitet. Weitere Informationen finden Sie unter [Monitoring-Konfiguration](#).

Wie lässt sich feststellen, ob ein Netzwerkobjekt mit dem Standort "inherit" zu einem internen oder externen Standort aufgelöst wurde?

Sie können den CLI-Befehl verwenden, um zu sehen, an welchem Ort das Netzwerkobjekt aufgelöst wurde:

```
Netzwerk-Objekt <Name> anzeigen
```

Erstellen von Netzwerkobjekten basierend auf FQDN?

Es ist möglich, Netzwerkobjekte mit vollqualifizierten Domännennamen anstelle von IP-Adressen zu konfigurieren. Sollten zu einem späteren Zeitpunkt Netzwerkeinstellungen auf Anwendungsservern geändert werden müssen, kann die GFI ClearView-Appliance diese Änderung automatisch über DNS erkennen.

Um ein Netzwerkobjekt auf der Grundlage eines voll qualifizierten Domännennamens zu konfigurieren, verwenden Sie die folgenden Befehle:

```
>de #conf t(config) # network-object <NAME> fqdn <voll qualifizierter  
Domänenname>
```

Eine GFI ClearView-Appliance muss mit einem DNS-Server konfiguriert werden, wenn sie eine Namensauflösung über FQDN durchführen soll. Jeder abgerufene Datensatz hat einen Lebenszyklus, der für einen solchen definierten TTL (Time to live) entspricht. Wenn die TTL überschritten wird, aktualisiert GFI ClearView den Datensatz automatisch, um zu überprüfen, ob sich die IP-Adresse nicht geändert hat. Bei einem Neustart der Appliance oder bei Änderungen der DNS-Konfiguration, der Schnittstellenkonfigurationen oder des Verbindungsstatus auf einer Schnittstelle wird das Netzwerkobjekt automatisch aktualisiert. Sollten Sie eine Aktualisierung durchführen müssen, können Sie den folgenden Befehl verwenden:

```
(config) # network-object <NAME> refresh
```

Ist die TTL niedriger als 5 Minuten, wartet GFI ClearView die vollen fünf Minuten, bevor eine Aktualisierung versucht wird, um DNS-Flooding zu vermeiden.

3.1.2 Arbeiten mit Benutzern und Gruppen als Objekte

Benutzer- und Gruppenobjekte werden verwendet, um vorausgefüllte Benutzer und Gruppen zu definieren, die für die Überwachung und Optimierung verwendet werden können.

Es zwei Möglichkeiten, wie die GFI ClearView Appliance Informationen über Benutzer und Gruppen erhalten kann:

1. **Active Directory:** Die GFI ClearView Appliance kann Benutzer- und Gruppeninformationen über den GFI ClearView Active Directory Server empfangen, der auf Active Directory-Servern installiert ist.

2. Statische Benutzer und Gruppen: Statische Benutzer- und Gruppeninformationen können nur über den CLI-Befehl "network user" eingegeben werden.

Sobald die Appliance die Benutzer und Gruppen kennt, können Sie auf den Seiten für Benutzer und Gruppen festlegen, welche Benutzer und Gruppen als **dynamische Netzwerkobjekte** für Überwachung und Optimierung verwendet werden sollen.

» Um Benutzer als dynamische Netzwerkobjekte zu definieren, siehe [Erstellen von Netzwerkbenutzerobjekten](#).

» Um Gruppen als dynamische Netzwerkobjekte zu definieren, siehe [Erstellen von Netzwerkgruppenobjekten](#).

Definition von Netzwerkbenutzern Objekte

Auf der Seite Network Users (Netzwerkbenutzer) wird eine vorausgefüllte Liste von Benutzern (und den zugehörigen IP-Adressen) angezeigt, die entweder vom GFI ClearView AD Connector oder von statischen Benutzern stammen, die über die CLI eingegeben wurden. Wählen Sie die einzelnen Benutzer aus, die Sie als dynamische Netzwerkobjekte definieren möchten.

<input type="checkbox"/>	User (Domain)	IP	Network Object
<input type="checkbox"/>	james	192.168.47.12	<input type="checkbox"/>
<input type="checkbox"/>	joe	192.168.47.13	<input type="checkbox"/>
<input type="checkbox"/>	junaid	192.168.8.13	<input type="checkbox"/>
<input type="checkbox"/>	Junaid.gfi (ALP)		<input type="checkbox"/>
<input type="checkbox"/>	junaid_khalid	192.168.8.14	<input type="checkbox"/>
<input type="checkbox"/>	junaid_mac	65.109.95.28	<input type="checkbox"/>
<input type="checkbox"/>	junaid_pc	65.109.95.6	<input type="checkbox"/>

Screenshot 56: Eine Liste der Netzwerkbenutzer, die auf der Seite Netzwerkbenutzer angezeigt wird.

Definieren und Entfernen von Benutzern als dynamische Netzwerkobjekte

Verwenden Sie die folgenden Anweisungen, um Benutzer als dynamische Netzwerkobjekte zu definieren und deren Identifizierung bei zu beenden. Die Anweisungen konzentrieren sich auf einen Benutzer, aber Sie können mehrere Benutzer definieren oder entfernen, indem Sie mehrere Kontrollkästchen aktivieren.

1. Gehen Sie zu Konfiguration > Objekte > Benutzer und Gruppen > Netzwerkbenutzer.
2. Suchen Sie den Benutzer in der Liste.

TIP

If you have many users, use the links at the top of the page to help find the user.


3. Aktivieren Sie das Kontrollkästchen für den Benutzer.
4. Klicken Sie unten auf der Seite auf **Netzwerkobjekt hinzufügen**. Das Symbol für den Netzwerkstatus Benutzers ändert sich in und zeigt an, dass es sich um ein Netzwerkobjekt handelt.

So beenden Sie die Identifizierung (Entfernung) eines Benutzers als dynamisches Netzwerkobjekt

1. Gehen Sie zu Konfiguration > Objekte > Benutzer und Gruppen > Netzwerkbenutzer.
2. Suchen Sie den Benutzer in der Liste.

TIP

If you have many users, use the links at the top of the page to help find the user.

3. Aktivieren Sie das Kontrollkästchen für den Benutzer.
4. Klicken Sie unten auf der Seite auf **Netzwerkobjekt entfernen**. Das Symbol für den Netzwerkstatus Benutzers ändert sich in  und zeigt an, dass es sich nicht mehr um ein Netzwerkobjekt handelt.


Konfigurieren von Netzwerkbenutzergruppen Objekte

Auf der Seite Netzwerkgruppen wird eine vorausgefüllte Liste von Gruppen angezeigt, die entweder vom GFI ClearView AD Connector oder von statischen Gruppen stammen, die über die Befehlszeilenschnittstelle eingegeben wurden. Auf dieser Seite können Sie auswählen, welche Gruppen Sie als dynamische Netzwerkobjekte definieren möchten.


Definieren und Entfernen von Benutzergruppen als dynamische Netzwerkobjekte

So definieren Sie eine Gruppe als dynamisches Netzobjekt

Verwenden Sie die folgenden Anweisungen, um ein Benutzergruppenobjekt zu definieren.

1. Gehen Sie zu Konfiguration > Objekte > Benutzer und Gruppen > Netzwerkgruppen
2. Suchen Sie die Gruppe in der Liste, und klicken Sie auf **Bearbeiten**.
3. Um alle Benutzer innerhalb der ausgewählten Netzwerkgruppe dem Netzwerkobjekt zuzuordnen, wählen Sie **Auf Netzwerkobjekt zuordnen**.
4. Wählen Sie **Domäne ignorieren**, um das Domänenpräfix auszuschließen.
5. Klicken Sie auf **Anwenden**. Das Symbol für den Netzwerkstatus der Gruppe ändert sich zu , was bedeutet, dass es sich nun um ein Netzwerkobjekt handelt. Wenn das dynamische Netzwerkobjekt aus mehreren Gruppen erstellt wurde, werden die Gruppen in einem einzigen Eintrag zusammengefasst und jede Domäne wird nach dem Gruppennamen angegeben.

So entfernen Sie eine Gruppe als dynamisches Netzwerkobjekt

1. Gehen Sie zu Konfiguration > Objekte > Benutzer und Gruppen > Netzwerkgruppen
2. Suchen Sie die Gruppe in der Liste, und klicken Sie auf **Bearbeiten**.
3. Deaktivieren Sie das Kontrollkästchen **Auf Netzwerkobjekt abbilden**.
4. Klicken Sie auf **Übernehmen**. Das Symbol für den Netzwerkstatus der Benutzergruppe ändert sich in  und zeigt damit an, dass es sich nicht mehr um ein Netzwerkobjekt handelt.

NOTE

If the dynamic network object was created from multiple groups, each group is again listed individually in the list.

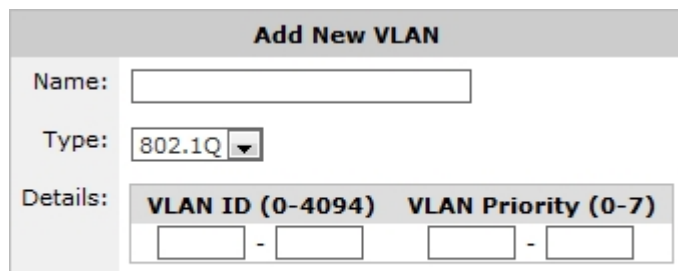
3.1.3 Konfigurieren von VLAN Objekten

Virtuelle LAN-Objekte (VLAN) werden verwendet, um Hosts (oder Gruppen von Hosts) auf einer funktionalen Basis und nicht auf einer physischen Basis logisch zu trennen.

Konfigurieren von VLAN-Objekten in der Benutzeroberfläche von GFI ClearView Web

Standardmäßig ist auf der GFI ClearView Appliance ein einziges VLAN mit der Bezeichnung "ALL" definiert, das den gesamten Datenverkehr erfasst (unabhängig davon, ob er zu einem VLAN gehört oder nicht). Weitere VLAN-Objekte können leicht hinzugefügt werden.

Alle definierten VLAN-Objekte werden in der Tabelle angezeigt. Jedes VLAN-Objekt kann bearbeitet oder gelöscht werden, indem Sie auf die entsprechende Schaltfläche in der Tabelle klicken. Das Objekt **ALL** VLAN ist geschützt und kann nicht bearbeitet oder gelöscht werden.



Add New VLAN

Screenshot 57: Hinzufügen eines neuen VLANs.

So fügen Sie ein neues VLAN-Objekt hinzu:

1. Gehen Sie zu Konfiguration > Objekte > VLANs.
2. Geben Sie einen aussagekräftigen Namen für das VLAN-Objekt ein.
3. Geben Sie den Typ des zu definierenden VLANs an. Derzeit sind nur 802.1Q-VLANs verfügbar.
4. Geben Sie den Bereich der zu definierenden VLAN-IDs an. Um alle VLAN-IDs zu definieren, lassen Sie dieses Feld leer oder geben Sie 0 - 4094 ein. Sie können eine einzige VLAN-ID definieren, indem Sie in beiden Feldern denselben Wert eingeben.
5. Geben Sie den zu definierenden VLAN-Prioritätsbereich an. Um alle VLAN-Prioritäten zu definieren, lassen Sie dieses Feld leer oder geben Sie 0 - 7 ein. Sie können eine einzige VLAN-Priorität definieren, indem Sie denselben Wert in beide Felder eingeben.
6. Klicken Sie auf die Schaltfläche **Neues VLAN hinzufügen**. Das VLAN wird der Liste der VLANs in der Tabelle hinzugefügt.

3.1.4 Hinzufügen von Protokollobjekten

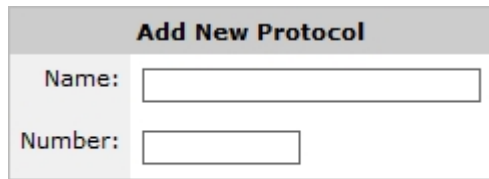
Protokollobjekte dienen zur Definition von IPv4-Protokollnummern, die dann zur Definition von Anwendungsobjekten verwendet werden können. In der Werkseinstellung der Appliance sind alle wichtigen Protokolle des Internetprotokolls (IPv4) enthalten, darunter ICMP (Internet Control Message Protocol), TCP (Transmission Control Protocol) und UDP (User Datagram Protocol). Zusätzliche IPv4-Protokolle können einfach durch Angabe der IPv4-Protokollnummer hinzugefügt werden.

NOTE

Protocol numbers are unique and can only be defined once.

In der Tabelle werden alle definierten Protokollobjekte angezeigt. Jedes Protokollobjekt kann durch Anklicken der entsprechenden Schaltfläche in der Tabelle bearbeitet oder gelöscht werden. Einige Protokolle sind geschützt und können nicht bearbeitet oder gelöscht werden.

gelöscht.



Add New Protocol

Name:

Number:

Add New Protocol

Screenshot 58: Hinzufügen eines neuen Protokolls.

Um Protokollobjekte zu konfigurieren:

1. Gehen Sie zu Konfiguration > Objekte> Protokolle.
2. Geben Sie einen aussagekräftigen Namen für das Protokoll ein.
3. Geben Sie im Feld **Nummer** die Nummer des IPv4-Protokolls an.
4. Klicken Sie auf die Schaltfläche **Neues Protokoll hinzufügen**. Das Protokoll wird der Liste der Protokolle in der Tabelle hinzugefügt.

EXAMPLE

Consider where SCTP (Stream Control Transport Protocol) is undefined by default and need to be defined.

Name: SCTP

Number:

132

3.1.5 Hinzufügen von Anwendungsobjekten

Anwendungsobjekte werden zur Klassifizierung des Datenverkehrs im Netz verwendet und bestehen aus Schicht-7-Signaturen oder TCP/UDP-Portnummern und Portbereichen. Die Anwendungsklassifizierung kann zur Überwachung des Datenverkehrs oder zur Erstellung anwendungsspezifischer Richtlinien verwendet werden. Auf der Appliance gibt es viele vordefinierte Anwendungen. Sie können beliebige Anwendungen hinzufügen, die noch nicht in der Liste enthalten sind.

Anwendungen können aus verschiedenen Kombinationen von L7-Signaturen, TCP/UDP-Portnummern oder -bereichen und Netzwerkobjekt erstellt werden. Die folgenden Kombinationen sind gültig.

- » Anwendungen auf der Grundlage von L7-Signaturen. Sie können zum Beispiel eine Anwendung für eine bestimmte Website erstellen, indem Sie http, host auswählen und die Domain der Website eingeben.
 - » Anwendungen auf der Grundlage von L7-Signaturen und TCP/UDP-Portnummern oder -bereichen, die mit ODER verknüpft werden. Sie können z. B. HTTP auf der Grundlage von TCP-Port 80 ODER der L7-Signatur "http" definieren.
 - » Anwendungen auf der Grundlage von Netzwerkobjekten und TCP/UDP-Portnummern oder -bereichen, die werden. Sie können zum Beispiel eine Anwendung auf der Grundlage einer bestimmten Portnummer auf einem bestimmten Server (angegeben durch das Netzwerkobjekt) definieren.
- » Anwendungen, die nur auf einem Netzwerkobjekt basieren. Sie können zum Beispiel eine Anwendung definieren, die auf einem bestimmten Anwendungsserver basiert (angegeben durch das Netzwerkobjekt).
- » Anwendungen, die nur auf TCP/UDP-Portnummern oder -bereichen basieren. Sie können zum Beispiel eine Anwendung für einen bestimmten Port erstellen.

Netzobjekte können nicht in Verbindung mit einer Schicht-7-Signatur verwendet werden.

Add New Application			
Name:	<input type="text" value="Exinda Website"/>		
Network Object:	<input type="text" value=""/>		
L7 Signature:	<input type="text" value="http --->"/>	<input type="text" value="host"/>	<input type="text" value="exinda.com"/>
Ports/Protocols:	<input type="text" value="TCP Port/Range"/>	<input type="text" value=""/>	eg. 80,8080,3127-3128
Show a List of Common Port Numbers			

Screenshot 59: Hinzufügen eines neuen Anwendungsobjekts.

NOTE

When creating applications based on ports, any given port number can only be defined once for TCP and once for UDP. The same port number can be defined for TCP and UDP. For example, if you define an application object with a port range TCP 500-510, you cannot then define another application object on TCP port 505. However, you can define another application object with UDP port 505.

You can define duplicate ports/port ranges if a network object is also specified.

Viele der L7-Signaturen verfügen über Subtyp-Klassifizierungen, wodurch die Sichtbarkeit der Schicht 7 viel granularer wird. So können die meisten Anbieter beispielsweise nur den Datenverkehr von Port 80 erfassen, um Berichte über bestimmte Web-Anwendungen zu erstellen. GFI ClearView ermöglicht einen tieferen Einblick in Layer-7-Anwendungen. Ein Beispiel aus dem Vergleich:

» Layer-4-Berichtstools berichten über Webanwendungen »

als: Port 80 oder HTTP Layer-7-Berichtstools berichten

auf Webanwendungen wie: Yahoo oder Skype

» Schicht 7 mit Subtyp-Klassifizierungsbericht über Webanwendungen als: Yahoo Video, Yahoo Voice oder Yahoo Webchat.

Dadurch können Sie die Überwachung auf einer viel feineren Ebene durchführen.

Hinzufügen von Anwendungsobjekten in der Benutzeroberfläche von GFI ClearView Web

Add New Application

Name:

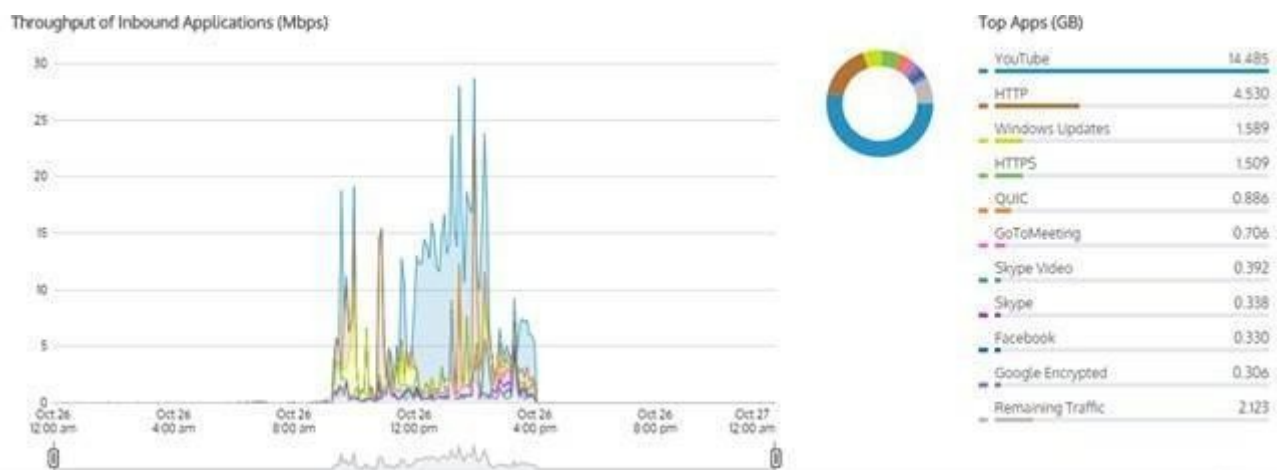
Network Object:

L7 Signatures:

Ports/Protocols:

[Show a List of Common](#)

- file-transfer
- unknown
- video
- voice**
- webchat



Screenshot 60: Diagramm zur Anzeige des Bandbreitendurchsatzes für Anwendungen.

3.1.6 Hinzufügen und Aktualisieren von Objekten der Anwendungsgruppe

Die richtige Klassifizierung von Anwendungen in Ihrem Netzwerk ist wichtig, um zu verstehen, was passiert und um eine bestimmte Art von Datenverkehr zu kontrollieren oder zu schützen.

Die GFI ClearView Appliance verfügt über eine lange Liste vordefinierter Anwendungen zur Klassifizierung des Netzwerkverkehrs. Wenn Sie jedoch Ihre eigene Anwendung erstellen möchten, können Sie neue Anwendungen auf Basis von L7-Signaturen, TCP/UDP-Portnummern und -Portbereichen oder Netzwerkobjekten erstellen.

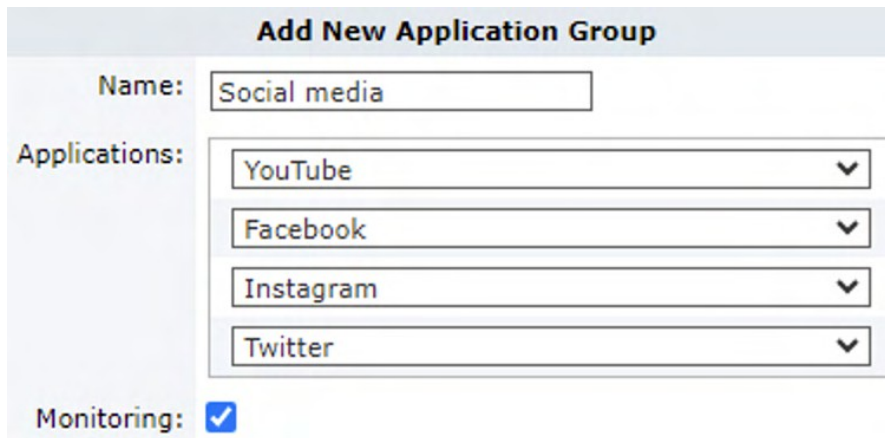
Möglicherweise möchten Sie Ihren Datenverkehr auch überwachen, kontrollieren oder schützen, indem Sie eine Gruppe von Anwendungen zusammenfassen. Die Kontrolle von Social-Networking-Anwendungen in einer Gruppe bietet in den meisten Fällen eine ausreichende Granularität. Die GFI ClearView Appliance wird mit einer Reihe von Standard-Anwendungsgruppen geliefert. Sie können neue Anwendungen zu diesen Gruppen hinzufügen, neue Gruppen erstellen oder bestehende Gruppen löschen.

Es gibt mehrere vordefinierte Anwendungsgruppen, z. B. Mail, P2P, Sprache usw. Sie können bestehende Anwendungsgruppen bearbeiten oder neue Gruppen erstellen.

NOTE

A given application can exist in multiple application groups. However, monitored groups must not contain applications which are already a member of another group being monitored. Any given application can only be monitored within a single application group.

Hinzufügen von Anwendungsgruppenobjekten in der Benutzeroberfläche von GFI ClearView Web



Add New Application Group

Name:

Applications:

- ▼
- ▼
- ▼
- ▼

Monitoring:

Screenshot 61: Hinzufügen einer neuen Anwendungsgruppe.

So fügen Sie eine neue Anwendungsgruppe hinzu

1. Gehen Sie zu Konfiguration > Objekte> Anwendungen> Anwendungsgruppen.
2. Geben Sie im Bereich **Neue Anwendungsgruppe hinzufügen** einen Namen für die neue Gruppe ein.
3. Wählen Sie die Anwendungen aus, die in die neue Gruppe gehören. Standardmäßig gibt es vier Dropdown-Listen zum Hinzufügen von Anwendungsobjekten zur Verfügung. Wenn Sie weitere hinzufügen möchten, speichern Sie das Objekt der Anwendungsgruppe und wählen Sie dann die Schaltfläche **Bearbeiten** neben der neu erstellten Anwendungsgruppe. Es werden vier weitere Dropdowns angezeigt, über die Sie weitere Anwendungen hinzufügen können.
4. Wenn Sie möchten, dass diese Anwendungsgruppe im Anwendungsgruppenbericht überwacht wird, wählen Sie das Feld Kontrollkästchen **Überwachung**.
5. Klicken Sie auf **Neue Anwendungsgruppe hinzufügen**.

So aktualisieren Sie eine Anwendungsgruppe

1. Gehen Sie zu Konfiguration > Objekte> Anwendungen> Anwendungsgruppen.
2. Suchen Sie die Gruppe, aus der Sie Anwendungen hinzufügen oder löschen möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie eine neue Anwendung aus einer leeren Dropdown-Liste aus. Oder um eine Anwendung zu entfernen, öffnen Sie die Dropdown-Liste mit der zu entfernenden Anwendung und wählen Sie die leere Zeile oben aus.
4. Klicken Sie auf **Änderungen übernehmen**.

Welche Anwendungsgruppen sind vordefiniert?

Weitere Informationen finden Sie unter [Vordefinierte Anwendungsgruppen](#).

3.1.7 Konfigurieren der Erkennung anonymer Proxys und der Überwachung von

Anonyme Proxys werden in der Regel verwendet, um Sicherheitsrichtlinien zu umgehen und Benutzern den Zugang zu verbotenen Freizeit-, Erwachsenen- oder anderen nicht geschäftlichen Websites zu ermöglichen, indem dieser Datenverkehr über eine reguläre oder verschlüsselte HTTP-Sitzung getunnelt wird. Anonyme Proxys bieten auch Anonymität; Benutzer, die über einen anonymen Proxy auf Websites zugreifen, können nicht ohne weiteres zu ihrer ursprünglichen IP-Adresse zurückverfolgt werden.

GFI ClearView Appliances bieten eine integrierte Unterstützung für die Erkennung anonymer Proxys. Die GFI

ClearView Appliance erhält täglich Updates mit aktualisierten anonymen Proxy-Definitionen, ähnlich wie Antiviren-Anwendungen tägliche Updates zu Bedrohungen erhalten.

Die anonyme Proxy-Anwendung ist ein spezielles Anwendungsobjekt, das dazu dient, anonyme Proxy-Websites und -Dienste zu erkennen. Der anonyme Proxy-Dienst ist jedoch standardmäßig deaktiviert.

Wenn der anonyme Proxy-Dienst aktiviert ist, holt die GFI ClearView-Appliance täglich eine Liste mit anonymen Proxy-Definitionen von den GFI-Webservern ab.

Es wird automatisch ein Anwendungsobjekt mit der Bezeichnung "Anonymer Proxy" erstellt. Die Anwendung "Anonymer Proxy" verfolgt den gesamten Datenverkehr, der über einen der anonymen Proxys in der Liste gesendet wird. Dieses Anwendungsobjekt wird in den Überwachungsberichten wie jedes andere Anwendungsobjekt angezeigt.

NOTE

» Anonymous Proxy classification only occurs if the Anonymous Proxy ASAM module is enabled on the **Configuration > System > Setup > Monitoring** page.

» In order to receive daily Anonymous Proxy definition updates, the GFI ClearView appliance must be able to contact the GFI web servers and the appliance must also have a valid software subscription.

Anonymous Proxy Options

Auto Update Service Enable

Apply changes

Settings

URL	http://updates.exinda.com/aplist/alist.gz
Last Check	2023/09/19 10:17:21
Last Update	2023/04/19 00:05:55
Status	Ok

The **renumerate** button refreshes the Anonymous Proxy list immediately

Renumerate

Screenshot 62: Das Formular zur Aktivierung des Dienstes Anonymer Proxy, um eine Liste der anonymen Proxy-Sites zu führen.

ASAM	
Anonymous Proxy	<input checked="" type="checkbox"/> Enable

Screenshot 63: Das Formular zum Aktivieren/Deaktivieren des für die Klassifizierung erforderlichen anonymen Proxy-ASAM.

Wo kann man it konfigurieren?

» Um den anonymen Proxy-Dienst zu aktivieren, gehen Sie zu **Konfiguration > Objekte >**

Anwendungen >> **Anonymer Proxy**. Um die Klassifizierung des anonymen Proxy-Verkehrs zu aktivieren, gehen Sie zu

Konfiguration > System > Einrichtung > Überwachung.

So aktivieren Sie die Klassifizierung des anonymen Proxy-Verkehrs

1. Aktivieren Sie das Kontrollkästchen Auto Update Service **Enable**. Die Appliance kommuniziert täglich mit den GFI-Webservern und holt alle neuen anonymen Proxy-Definitionen ab.

2. Vergewissern Sie sich, dass das ASAM-Modul Anonymer Proxy aktiviert ist, indem Sie die Seite **Konfiguration > System > Setup > Überwachung** aufrufen und sicherstellen, dass das Kontrollkästchen **Anonymer Proxy** im Abschnitt **ASAM** aktiviert ist. Das ASAM-Modul Anonymer Proxy ist standardmäßig aktiviert. Die Appliance klassifiziert den Datenverkehr, indem sie ihn mit der Liste der anonymen Proxys abgleicht.

So sehen Sie, wann die Appliance die Definitionen des anonymen Proxys zuletzt aktualisiert hat

1. Sehen Sie sich den Abschnitt **Einstellungen** an.
2. Das Feld **Letzte Prüfung** gibt an, wann die Appliance das letzte Mal den GFI-Dienst auf neue anonyme Proxy-Definitionen überprüft hat.
3. Das Feld **Letzte Aktualisierung** zeigt an, wann zuletzt neue anonyme Proxy-Definitionen gefunden und aktualisiert wurden.

So erzwingen Sie eine Überprüfung der Definitionen des anonymen Proxys

Klicken Sie auf die Schaltfläche **Renumerate**. Die Appliance überprüft die GFI-Webserver sofort auf neue anonyme Proxy-Informationen.

So deaktivieren Sie die Klassifizierung des anonymen Proxy-Verkehrs

1. Deaktivieren Sie das Kontrollkästchen Automatischer Aktualisierungsdienst **deaktivieren**.
2. Deaktivieren Sie den ASAM für anonymen Proxy, indem Sie auf der Seite **Konfiguration > System > Einrichtung > Überwachung** das Kontrollkästchen **Anonymer Proxy** im Abschnitt **ASAM** deaktivieren und auf die Schaltfläche **Änderungen übernehmen** klicken. Durch die Deaktivierung des ASAM werden die vorhandenen anonymen Proxy-Definitionen gelöscht.

3.1.8 Konfigurieren von Service Level Agreement Objekten

Die Service Level Agreement (SLA)-Objekte werden zur Überwachung der Verfügbarkeit eines bestimmten IP-Standorts verwendet. Durch die Erstellung eines SLA-Objekts geben Sie an, welcher IP-Standort überwacht werden soll. Die GFI ClearView-Appliance sendet alle 10 Sekunden einen ICMP-Ping an die IP-Adresse. Sie können die Größe der zu verwendenden Ping-Pakete festlegen. Sie können auch festlegen, wann eine Warnung ausgelöst wird, indem Sie den Schwellenwert für die Ping-Latenzzeit und die Dauer der Überschreitung des Schwellenwerts angeben. Ein Alarm wird ausgelöst, wenn die Latenz der SLA-Site den Latenzschwellenwert länger als die angegebene Dauer überschreitet.

Konfigurieren von Service Level Agreement-Objekten in der GFI ClearView Web UI

Add New SLA Site	
Name:	<input type="text"/>
Type:	<input type="text" value="IP address"/> <input type="text" value="0.0.0.0"/>
Latency Threshold (ms):	<input type="text" value="500"/>
Ping Size:	<input type="text" value="64"/>
Duration: (Duration for which the threshold is exceeded)	<input type="text" value="1 hour"/>
Enable:	<input type="checkbox"/>

Screenshot 64: Hinzufügen einer SLA-Site.

Um auf diese Konfiguration zuzugreifen, gehen Sie zu **Konfiguration > Objekte > Service Levels > Service**

Level-Vereinbarungen. So erstellen Sie ein Service Level Agreement (SLA)-Objekt:

1. Klicken Sie auf die Schaltfläche **Neues SLA-Objekt hinzufügen**.
2. Geben Sie einen Namen für das SLA-Objekt ein.
3. Geben Sie in das Feld **Ziel-IP** eine IP-Adresse ein, die angepingt werden soll.
4. Geben Sie den **Schwellenwert für die Latenzzeit** (in ms) ein, über den Sie benachrichtigt werden möchten, wenn dieser Schwellenwert dauerhaft überschritten wird. Der Standardwert ist 500 Millisekunden.
5. Geben Sie in das Feld **Ping-Größe** die Größe des Ping-Pakets (in Byte) ein, die verwendet werden soll. 64 Byte ist der Standardwert.
6. Wählen Sie die Dauer aus, d. h. die Zeitspanne, die der Latenzschwellenwert überschritten werden muss, bevor die Warnung gesendet wird. Die Optionen sind:
 - 30 Sekunden
 - 60 Sekunden
 - 5 Minuten
 - 30 Minuten
 - 1 Stunde (Standard)
 - 0 - (Deaktivieren), wodurch der Alarm deaktiviert wird.
7. Aktivieren Sie das Kontrollkästchen **Aktivieren**, damit das SLA-Objekt mit dem Pinggen der IP-Site beginnen kann.
8. Klicken Sie auf die Schaltfläche **Änderungen übernehmen**. Das Objekt wird der Liste der konfigurierten SLA-Objekte hinzugefügt.

NOTE

Ensure that the Send Email alert is enabled for this on the Configuration > System > Setup > Alerts page.

Valid SMTP and email settings are required for email alerts. To configure, see For more information, refer to [SNMP configuration](#) (page 498). and For more information, refer to [Email configuration](#) (page 495)..

3.1.9 Konfigurieren der Anwendungsleistungsbewertung Objekte

Das Application Performance Score (APS)-Objekt wird verwendet, um zu bewerten, wie die Netzwerkbenutzer die Netzwerkleistung von geschäftskritischen Anwendungen erleben. Der Wert, der zwischen 0 und 10 liegt, wobei 0 schlecht und 10 ausgezeichnet ist, zeigt an, ob die Anwendung die erwartete Leistung erbringt oder ob sie schlecht ist. Bei der Erstellung eines APS-Objekts geben Sie eine zu überwachende Anwendung an.

Optional können Sie auch ein Netzwerkobjekt angeben, so dass die Anwendung nur überwacht wird, wenn sie in diesem Teil des Netzwerks beobachtet wird. Sie legen Schwellenwerte für eine oder mehrere Netzwerkmetriken fest. Später wird der Verkehr für diese Anwendung anhand dieser Schwellenwerte bewertet, um festzustellen, wie gut die Anwendung arbeitet.

Die geeigneten Schwellenwerte für eine Anwendung sind für jede Netzwerkumgebung einzigartig. Sie können die Schwellenwerte für die Netzwerkmetriken manuell festlegen oder das System automatisch Schwellenwerte erstellen lassen, indem es den Datenverkehr beobachtet, um angemessene Basiswerte zu ermitteln. Zu den Metriken gehören Netzwerkverzögerung, Serververzögerung, Round Trip Time, Jitter und Netzwerkverlust. Beachten Sie, dass Sie die Metrik für den Netzwerkverlust manuell einstellen können, sie wird jedoch nicht automatisch während der Baseline-Analyse berechnet. Sie können eine oder mehrere dieser Metriken in Ihrem APS-Objekt verwenden. Die meisten Anwendungen verwenden transaktionale Protokolle. Anwendungen wie Citrix XenApp Server oder Microsoft Remote Desktop verwenden nicht-transaktionale Protokolle, die Informationen zwischen Client und Server zu beliebigen Zeiten senden. Bei diesen Anwendungstypen führt die Standardmethode zur Berechnung der Netzwerk- und Serververzögerungen nicht zu einer genauen Metrik. Wenn die Anwendung ein nicht-transaktionales Protokoll verwendet, müssen Sie dies bei der Erstellung des APS-Objekts angeben.

Für die Baseline-Analyse wird der Verkehr während des angegebenen Zeitraums analysiert und eine Reihe von Schwellenwerten für die Metrik erstellt. Die Schwellenwertempfehlungen zielen auf einen APS von 8,5 ab. Wenn die Anwendung einen APS-Wert unter 8,5 meldet, ist die Leistung der Anwendung schlechter als die der Baseline. Wenn während des Baseline-Zeitraums kein Datenverkehr beobachtet wird, beginnt die Appliance automatisch mit einer weiteren Baseline-Analyse für den nächstgrößeren Zeitraum. Für jede fehlgeschlagene Baseline-Analyse wird eine E-Mail versandt.

NOTE

It is a best practice to start the baseline analysis during a time period when you would expect traffic for the application is typical. This will ensure that the baseline values accurately reflect the typical usage of the application. This means that if network conditions changes, it is recommended that the thresholds are re-evaluated.

NOTE

APS is not supported for small-packet applications like Citrix and RDP. The metrics are normalized as if the application runs with larger packet sizes, leading to larger values.

Sie können auch Warnungen einstellen, so dass Sie benachrichtigt werden, wenn die Punktzahl unter einen bestimmten Schwellenwert fällt. Es gibt eine Einstellung für die Verzögerung der Alarmauslösung, die voraussetzt, dass der Wert eine bestimmte Zeit lang unter dem Schwellenwert bleibt, bevor der Alarm ausgelöst wird. Dadurch wird verhindert, dass kurzzeitige schlechte Werte wie ein Notfall wirken.

Add New APS Object	
APS Name:	<input type="text"/>
Application:	<input type="text" value="Zoom"/>
Network Object - Internal:	<input type="text" value="private net"/>
Network Object - External:	<input type="text" value="ALL"/>
Alert Enable:	<input type="checkbox"/>
Alert Threshold:	<input type="text" value="0.0"/>
Alert Trigger Delay:	<input type="text" value="5 minutes"/>
Auto Baseline	<input checked="" type="checkbox"/>
Auto Baseline Period:	<input type="text" value="Current Hour"/>
Non-Transactional Protocol	<input type="checkbox"/>

Screenshot 69: Das Formular zum Hinzufügen eines neuen APS-Objekts.

Bei der Bearbeitung des APS-Objekts können Sie die Alarmkonfiguration ändern, den Baseline-Vorgang neu starten und die ändern. Wenn Sie die Einstellungen des Netzwerkobjekts ändern, empfiehlt es sich, die Schwellenwerte der Metrik neu zu bewerten und möglicherweise eine Baseline neu zu starten.

Edit APS Object		Baseline Info	
APS Name:	<input type="text" value="Zoom"/>	Status:	Stopped
Application:	<input type="text" value="Zoom"/>	Average Packet Size (bytes):	144
Network Object - Internal:	<input type="text" value="ALL"/>	Traffic Seen (KB):	3628
Network Object - External:	<input type="text" value="ALL"/>	Start Date:	Wed Dec 07 11:00:00 UTC 2022
Alert Enable:	<input checked="" type="checkbox"/>	End Date:	Wed Dec 07 12:00:00 UTC 2022
Alert Threshold:	<input type="text" value="8.0"/>	Auto Baseline Period:	<input type="text" value="Current Hour"/>
Alert Trigger Delay:	<input type="text" value="60 seconds"/>		
Non-Transactional Protocol	<input type="checkbox"/>		
Scoring Metrics			
Metric	Config	Baseline	
Normalized Network Delay (ms/kb):	<input type="text" value="217"/>	217	
Normalized Server Delay (ms/kb):	<input type="text" value="102"/>	102	
Network Delay (ms):	<input type="text" value="394"/>	394	
Server Delay (ms):	<input type="text" value="257"/>	257	
Network Jitter (ms):	<input type="text" value="367"/>	367	
Round Trip Time (ms):	<input type="text" value="159"/>	159	
Network Loss (%):	<input type="text"/>	-	

Screenshot 70: Bearbeitung eines APS-Objekts.

Erstellen eines Objekts zur Bewertung der Anwendungsleistung

Verwenden Sie die folgenden Anweisungen, um ein neues APS-Objekt zu erstellen. Während dieser Einrichtung können Sie einen Bereich für den Überwachungsprozess festlegen. Die Bewertungen können sich auf bestimmte interne und/oder externe Netzwerkobjekte oder auf ALLE in einer oder beiden Kategorien konzentrieren.

Bevor Sie beginnen...

» Wenn Sie Warnmeldungen aktivieren müssen, stellen Sie sicher, dass Sie E-Mail unter **Konfiguration > System > Setup** > Seite mit **den Warnungen**.

Weitere Informationen finden Sie in der Hilfe zu GFI ClearView Web UI.

» Außerdem müssen Sie SNMP auf der Seite **Konfiguration > System > Netzwerk > SNMP** einrichten. Weitere Informationen finden Sie in der Hilfe zu GFI ClearView Web UI.

Erstellen eines Objekts zur Bewertung der Anwendungsleistung in der Benutzeroberfläche von GFI ClearView Web

Um das Objekt zu erstellen:

1. Gehen Sie zu Konfiguration > Objekte > Service Levels > Application Performance Score.
2. Klicken Sie auf die Schaltfläche **Neues APS-Objekt hinzufügen**.
3. Geben Sie in das Feld **APS-Name** einen Namen für die Bewertung ein.
4. Wählen Sie in der Liste **Anwendung** den zu überwachenden Anwendungsverkehr aus.
5. Öffnen Sie die Dropdown-Liste **Netzwerkobjekt - Intern** und wählen Sie entweder ein bestimmtes Netzwerkobjekt oder ALLE aus.
6. Öffnen Sie die Dropdown-Liste **Netzwerkobjekt - Extern** und wählen Sie entweder ein bestimmtes Netzwerkobjekt oder ALLE aus.

NOTE

By specifying both an internal and external network object, only the application conversations between the specified network objects is tracked.

7. Wenn Sie eine Warnung erhalten möchten, wenn der Leistungswert der Anwendung unter einen bestimmten Schwellenwert fällt, legen Sie die folgenden Warneinstellungen fest:
 - a. Vergewissern Sie sich, dass das Kontrollkästchen **Warnung aktivieren** aktiviert ist.
 - b. Legen Sie im Feld **APS-Schwellenwert** einen Schwellenwert zwischen 0 und 10 fest.
 - c. Geben Sie im Feld **Alarmauslöseverzögerung** an, wie viele Minuten der APS-Wert unter dem Schwellenwert liegen muss, bevor die Benachrichtigung gesendet wird.

EXAMPLE

If the alert threshold is set to 7.0 and the alert trigger delay is set to 5 minutes, then the alert needs to be below 7.0 for 5 minutes before the alert is triggered.

8. Wenn das Baselineing sofort beginnen soll, aktivieren Sie das Kontrollkästchen **Automatische Baseline** und wählen Sie den **Zeitraum für die automatische Baseline**.
9. Wenn die Anwendung ein nicht-transaktionales Protokoll für den Datenverkehr zwischen Client und Server verwendet, wie z. B. Citrix XenApp Server oder Microsoft Remote Desktop, wählen Sie die Option Kontrollkästchen **Nicht-transaktionales Protokoll**.
10. Klicken Sie auf **Neues APS-Objekt hinzufügen**. Das Objekt wird der Liste der konfigurierten APS-Objekte hinzugefügt.

Wie die Schwellenwerte für Leistungskennzahlen berechnet werden

Die Netzleistungskennzahlen werden auf der Grundlage des beobachteten Datenverkehrs berechnet. Jeder Schwellenwert wird so berechnet, dass er um 0,85 Standardabweichungen über der durchschnittlichen Beobachtung für diese Kennzahl liegt. Dadurch wird sichergestellt, dass der berechnete Schwellenwert einen APS von 9,0 anstrebt. Wenn die Anwendung einen APS-Wert unter 9,0 meldet, ist die Leistung der Anwendung schlechter als die des Basiswerts.

APS-Schwellenwerte manuell konfigurieren

Metrische Schwellenwerte können bei der erstmaligen Erstellung des APS-Objekts oder bei der Bearbeitung eines APS-Objekts manuell festgelegt werden, auch wenn sie automatisch durch den Baselineing-Vorgang bestimmt wurden. Wenn beispielsweise der Baselineing-Vorgang alle Schwellenwerte festgelegt hat und Sie sich nur für die Round Trip Time, die normalisierte Serververzögerung und die normalisierte Netzwerkverzögerung interessieren, können Sie die Schwellenwerteinstellungen für die anderen Metriken entfernen.

1. Gehen Sie zu Konfiguration > Objekte > Service Levels > Application Performance Score.
2. Deaktivieren Sie im Formular **Neues APS-Objekt hinzufügen** das Kontrollkästchen **Auto Baseline**. Wenn eine Basislinienanalyse läuft, müssen Sie auf die Schaltfläche **Basislinie anhalten** klicken. Die Schwellenwerte können nur bearbeitet werden, wenn keine Baseline läuft. Die Messwerte werden auf dem Bildschirm angezeigt. Sie können auch das APS-Objekt in der Liste bearbeiten und dann im Formular **APS-Objekt bearbeiten** die **Bewertungsmetriken** am unteren Rand des Formulars anzeigen.
3. Geben Sie die Werte für die Metriken ein, für die Sie Schwellenwerte festlegen möchten, oder ändern Sie sie. Beachten Sie, dass alle Metriken, für die kein Schwellenwert festgelegt wurde, bei der Berechnung des APS-Scores nicht analysiert werden.

Netzwerkverzögerung - die Zeit, die Daten benötigen, um das Netzwerk (auf der Leitung) in einer Richtung vom Client über die GFI ClearView-Appliance zum Server (oder in der entgegengesetzten Richtung) zu durchlaufen, in ms

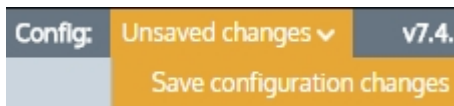
- Serververzögerung - die Zeit, die ein Server benötigt, um auf die Anfrage zu antworten, in ms
- Normalisierte Netzwerkverzögerung - die Zeit, die Daten benötigen, um das Netzwerk in eine Richtung zu durchqueren, wobei die Verzögerung unabhängig von der Transaktionsgröße gemessen wird, indem eine normalisierte Paketgröße von 1024 Byte angenommen wird
- Normalisierte Serververzögerung - die Zeit, die ein Server benötigt, um auf die Anfrage zu antworten, wobei die Verzögerung unabhängig von der Transaktionsgröße gemessen wird, indem eine normalisierte Paketgröße von 1024 Byte angenommen wird
- Round-Trip-Time - die Zeit, die ein Paket benötigt, um von einem Client über die GFI ClearView-Appliance zum Server und zurück zu gelangen
- Jitter - das Maß für die Variabilität der Netzverzögerung, definiert als eine Standardabweichung der normalisierten Netzverzögerung
- Eingehender Verlust - der Prozentsatz der Paketverluste

bei • eingehendem Verkehr Ausgehender Verlust - der
Prozentsatz der

Paketverlust bei ausgehendem Verkehr

4. Klicken Sie auf **Änderungen übernehmen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.



Konfigurieren der automatischen APS-Schwellenwertberechnung

Der Baselining-Prozess kann bei der erstmaligen Erstellung des APS-Objekts oder bei der Bearbeitung eines APS-Objekts gestartet werden. Sie können den Baselining-Prozess jederzeit neu starten, wenn Sie möchten, dass das System die Schwellenwerte neu berechnet.

1. Gehen Sie zu Konfiguration > Objekte > Service Levels > Application Performance Score.
2. Stellen Sie im Formular **Neues APS-Objekt hinzufügen** sicher, dass das Kontrollkästchen **Auto Baseline** aktiviert ist, und legen Sie in der Dropdown-Liste **Auto Baseline Zeitraum** fest, wie lange das System den Datenverkehr bei der Berechnung der Schwellenwerte beobachten soll. Wählen Sie den Zeitraum für die Baseline auf der Grundlage der Popularität der Anwendung. Wenn beispielsweise viel HTTP-Verkehr im Netzwerk stattfindet, ist der Zeitraum von 1 Stunde lang genug, um den Verkehr zu analysieren und eine genaue Basislinie zu erstellen. Für eine Anwendung, die nicht sehr häufig genutzt wird, verwenden Sie den Zeitraum von 1 Woche für die Baseline, um sicherzustellen, dass genügend Datenverkehr analysiert wird, um Baseline-Empfehlungen zu erstellen.
3. Oder legen Sie im Formular **APS-Objekt bearbeiten** den **Zeitraum für die automatische Basislinie** fest und klicken Sie auf **Basislinie starten**.

NOTE

The Network Loss metric is not calculated during the baseline analysis.

NOTE

If no traffic matching this APS object is observed during the baseline period, the appliance restarts the baseline analysis for the next larger time period. For example, if no traffic observed during the one hour period, the traffic continues to be analyzed for one day. If no traffic is observed during the one day period, then the traffic is analyzed for a week. If the traffic is analyzed for one week and no traffic has been transferred, the auto baseline analysis stops.

Each time the system unsuccessfully baselines the traffic (that is, when no traffic is observed during the auto baseline period), an email notification is sent to the users configured on the **Configuration > System > Network > Email** page.

Prüfen, ob die Basisberechnung im Gange ist

Auf der Konfigurationsregisterkarte **Application Performance Score** wird die Liste der APS-Objekte angezeigt. Wenn die APS derzeit den Datenverkehr der Anwendung ermittelt, ist ein grünes Häkchen in der Spalte "**Auto Baseline**" zu sehen.

Drücken Sie die Schaltfläche **Bearbeiten** für das APS-Objekt. Der Abschnitt **Baseline-Info** gibt den Status (läuft oder gestoppt) sowie Start- und Enddatum und -uhrzeit der Baseline-Periode an. Beachten Sie, dass hier auch die durchschnittliche Paketgröße und die Menge des beobachteten Datenverkehrs angezeigt werden.

3.1.10 Konfigurieren einer Anwendungsleistungsmetrik Objekt

Die Application Performance Metric (APM)-Objekte werden zur Überwachung bestimmter Anwendungsleistungsmetriken verwendet. Wenn Sie ein APM-Objekt erstellen, geben Sie an, welche Anwendung überwacht werden soll. Optional können Sie auch ein Netzwerkobjekt angeben, so dass die Anwendung nur überwacht wird, wenn sie in diesem Teil des Netzwerks beobachtet wird. Sie legen einen Schwellenwert für eine einzelne Netzwerkmetrik fest. Später wird der Datenverkehr für diese Anwendung anhand dieses Schwellenwerts bewertet, um festzustellen, wie gut die Anwendung arbeitet. Ein Alarm wird ausgelöst, wenn der Schwellenwert über einen bestimmten Zeitraum hinweg überschritten wird.

Die folgenden Metriken sind verfügbar:

- verlorene Bytes
- Netzwerkverzögerung
- Server-Verzögerung
- Transaktionsverzögerung
- normalisierte Netzverzögerung
- normalisierte Server-Verzögerung
- normalisierte Transaktionsverzögerung
- Rundreisezeit
- tcp-Verbindungen abgebrochen
- tcp-Verbindungen werden ignoriert
- tcp-Verbindungen abgelehnt

- tcp verbunden gestartet.

Add New APM Object

APM Name:

Metric:

Application:

Network Object - Internal:

Network Object - External:

APM Threshold:

Alert Trigger Delay:

Alert Enable:

Add New APM Object

Cancel

Screenshot 79: Hinzufügen eines neuen APM-Objekts.

NOTE

APM values are not shown on any report; they are used solely to generate alerts.

Verwenden Sie die folgenden Anweisungen, um ein APM-Objekt zu erstellen.

Bevor Sie beginnen...

» Wenn Sie Warnmeldungen aktivieren müssen, stellen Sie sicher, dass Sie E-Mail unter **Konfiguration > System > Setup > Seite mit den Warnungen**.

Weitere Informationen finden Sie in der Hilfe zu GFI ClearView Web UI.

» Außerdem müssen Sie SNMP auf der Seite **Konfiguration> System> Netzwerk> SNMP** einrichten. Weitere Informationen finden Sie in der Hilfe zu GFI ClearView Web UI.

So erstellen Sie ein APM Objekt

1. Gehen Sie zu **Konfiguration> Objekte> Service Levels> Application Performance Metric**.
2. Klicken Sie auf die Schaltfläche **Neues APM-Objekt hinzufügen**.
3. Geben Sie einen Namen für das APM-Objekt ein.
4. Wählen Sie die Metrik aus, die Sie überwachen möchten. Die folgenden Metriken sind verfügbar:
 - **bytes-lost** - Durch erneute Übertragungen verlorene Bytes.
 - **network-delay** - Die Zeit, die die Daten benötigen, um das Netzwerk zu durchlaufen.
 - **server-delay** - Die Zeit, die ein Server benötigt, um auf eine Anfrage zu antworten.
 - **transaction-delay** - Die Gesamtzeit für eine Transaktion (Netzwerkverzögerung+ Serververzögerung)
 - **normalized-network-delay** - Die Zeit, die Daten brauchen, um das Netzwerk zu durchqueren, wenn die Paketgröße auf 1024 Bytes normiert ist.
 - **normalized-server-delay** - Das normalisierte Maß für die Zeit, die ein Server benötigt, um

auf eine Transaktionsanfrage antworten.

- **normalized-transaction-delay** - Das normalisierte Maß für die Zeit, die eine Client-Anfrage braucht, um an einen Server gesendet zu werden, und die Antwort des Servers, um vom Client empfangen zu werden.
- **Round-Trip-Time** - Die Zeit, die ein Paket benötigt, um von einem Gerät über ein Netzwerk zu gelangen und wieder zurückzukehren.
- **tcp-connections-aborted** - Die Anzahl der TCP-Verbindungen, die nach dem Verbindungsaufbau zurückgesetzt wurden. (RST vom Client oder Server)
- **tcp-connections-ignored** - Die Anzahl der TCP-Verbindungen, die im Zustand SYN-SENT ablaufen. Es wird keine Antwort vom Server empfangen.
- **tcp-connections-refused** - Die Anzahl der TCP-Verbindungen, die zurückgesetzt werden, bevor die Verbindung aufgebaut wird. (RST im Zustand SYN-SENT)
- **tcp-connections-started** - Die Anzahl der initiierten TCP-Verbindungen.

5. Wählen Sie in der Liste **Anwendung** den zu überwachenden Anwendungsverkehr aus.

6. Wenn Sie die Anwendung nur für ein bestimmtes internes Netzwerkobjekt überwachen wollen, geben Sie das gewünschte interne Netzwerkobjekt an; andernfalls wählen Sie ALLE.

7. Wenn Sie die Anwendung nur für ein bestimmtes externes Netzwerkobjekt überwachen möchten, geben Sie das gewünschte externe Netzwerkobjekt an; andernfalls wählen Sie ALLE. Wenn Sie sowohl das interne als auch das externe Netzwerkobjekt angeben, werden nur die Verbindungen der Anwendung zwischen den angegebenen Netzwerkobjekten überwacht.

8. Aktivieren Sie das Kontrollkästchen "**Alarm aktivieren**".

9. Geben Sie in das Feld **APM-Schwellenwert** den Schwellenwert ein, der eine Warnung auslöst, wenn der Wert unter diesen Wert fällt.

10. Wählen Sie in der Liste **Alarmauslöseverzögerung** aus, wie lange die Metrik unter dem Schwellenwert bleiben muss, bevor der Alarm gesendet wird. Wenn der Alarm beispielsweise die Anzahl der verlorenen Bytes überwacht, der Schwellenwert auf 100 und die Verzögerung für den Alarmauslöser auf 5 Minuten eingestellt ist, muss die Anzahl der verlorenen Bytes 5 Minuten lang über 100 liegen, bevor der Alarm ausgelöst wird.

11. Legen Sie den Schwellenwert für die APM-Metrik fest. Die Einheiten des Schwellenwerts sind relativ zu der Metrik. Das heißt, Verzögerungen und Round Trip Time werden in Millisekunden gemessen, TCP-Verbindungen und verlorene Bytes werden gezählt.

12. Klicken Sie auf **Neues APM-Objekt hinzufügen**. Das Objekt wird der Liste der konfigurierten APM-Objekte hinzugefügt.

3.2 Überwachung Ihres Netzwerks

Nach der Installation und Konfiguration der GFI ClearView Appliance können Sie Ihr Netzwerk überwachen und erhalten einen umfassenden Überblick über die Anwendungen, auf die Benutzer zugreifen, sowie über den eingehenden und ausgehenden Datenverkehr und den Netzwerkdurchsatz.

3.2.1 Dashboards

Die GFI ClearView Web UI bietet Dashboards, mit denen Sie den Betrieb einer ClearView Appliance überwachen können. Ein Dashboard zeigt den Systemzustand und Statusinformationen zur GFI ClearView Appliance an. Das andere Dashboard liefert statistische Daten, die den Nutzen und die Auswirkungen der GFI ClearView Appliance in Ihrem Netzwerk aufzeigen.

System Dashboard

Das System-Dashboard zeigt Systeminformationen, den Status von Systemalarmen sowie eine Übersicht über andere GFI ClearView-Appliances und deren jeweilige Reduktionsstatistiken an. Das Dashboard beantwortet Fragen wie "Gibt es Probleme mit den Netzwerkkarten, der CPU-Auslastung usw.? Für was ist diese Appliance lizenziert? Wie lautet die Host-ID der Appliance?"

Hostname: exinda-22061		Alarm	Status	Last Triggered	Count
Hardware Series:	2061	CPU Utilization	OK		
Licensed Model:	Exinda 2861 (1.000/0.020Gbps - HP)	System Disk Full	OK		
SS Expiry Date:	Aug 31, 2018	Memory Paging	OK		
Host ID:	00900b2e7a32	Bridge Link	OK		
Timezone:	Etc/UTC	Bridge Direction	OK		
System Uptime:	6d 20h 55m 26.592s	Link Negotiation	OK		
Scheduled Jobs:	No scheduled jobs.	NIC Problems	OK		
Memory Usage:	86.29% of 3816MB	NIC Collisions	OK		
CPU Usage:	7%	NIC Dropped Packets	OK		
Database Status:	Running	SMB Signed Connections	OK		
		Redundant Power	Not Available		
		Redundant Storage	Not Available		
		Max Accelerated Connections Exceeded	DISABLED		
		Asymmetric Route Detection	OK		
		MAPI Encrypted Connections	OK		

Screenshot 80: Das System-Dashboard zeigt Informationen zu einer GFI ClearView-Appliance an.

Der Status der Appliance-Datenbank wird als **Datenbankstatus** angezeigt. Zu den möglichen Status»

gehören: **Start** - Die Datenbank wird initialisiert und wartet auf eine Antwort von der

» System auf verfügbarem Speicher. **Läuft** - Die Datenbank ist in Betrieb.

» **Aktualisierung** - Die Datenbank ist gestartet, wird aber aktualisiert.

» **Herabstufung**: Die Datenbank wurde gestartet, wird aber gerade aktualisiert.

» **Gestoppt** - Die Datenbank ist gestoppt.

» **Fehler** - Auf die Datenbank kann nicht zugegriffen werden. Dies wird normalerweise angezeigt, wenn ein Problem mit Upgrade oder Downgrade der Datenbank auftritt.

» **Unbekannt** - Der Zustand der Datenbank ist unbekannt.

Vorteile Dashboard

Das Benefits Dashboard bietet eine Reihe von Widgets, die auf einem Dashboard angeordnet sind, das Informationen über Ihren Netzwerkverkehr auf hoher Ebene anzeigt. Das Dashboard gibt Antworten auf Fragen wie "Welches sind die dominierenden Anwendungsgruppen in meinem Netzwerk? Beanspruchen Freizeitanwendungen einen großen Teil meiner Bandbreite? Ist meine Verbindung ausgelastet?" Das Dashboard kann auch eine Empfehlung aussprechen. Die GFI ClearView Appliance analysiert den Netzwerkverkehr und spricht auf der Grundlage der gewonnenen Erkenntnisse Empfehlungen aus.

Widgets können ausgeblendet werden, um das Dashboard so anzupassen, dass es nur die für relevanten Widgets enthält. Um ein ausgeblendetes Widget hinzuzufügen, klicken Sie auf den Link "**Mehr hinzufügen**" oben rechts auf dem Dashboard. Wenn der Link "**Weitere hinzufügen**" nicht sichtbar ist, werden alle verfügbaren Widgets angezeigt. Die Widget-Einstellungen und -Layouts werden zwischen den Anmeldungen beibehalten.

Das Dashboard kann erfasst und in eine PDF-Datei umgewandelt werden, indem Sie auf das PDF-Symbol oben rechts auf der Benutzeroberfläche klicken.

GFI ClearView empfiehlt

Jede Nacht nach Mitternacht analysiert die GFI ClearView Appliance den des vorangegangenen Tages. Wenn etwas Auffälliges oder Ungewöhnliches festgestellt wird, gibt sie eine Empfehlung ab, die auf dem Dashboard angezeigt und an die im **Netzwerk-Setup** konfigurierten E-Mail-Adressen gesendet wird.

> **E-Mail.**

Jede Empfehlung enthält das Datum der Verkehrsdaten. Verwerfen Sie die Empfehlung, indem Sie auf die Schaltfläche "Schließen" klicken. Um die letzten drei Empfehlungen anzuzeigen, doppelklicken Sie auf das GFI ClearView-Logo in der Kopfleiste des Dashboards.



Exinda Recommends

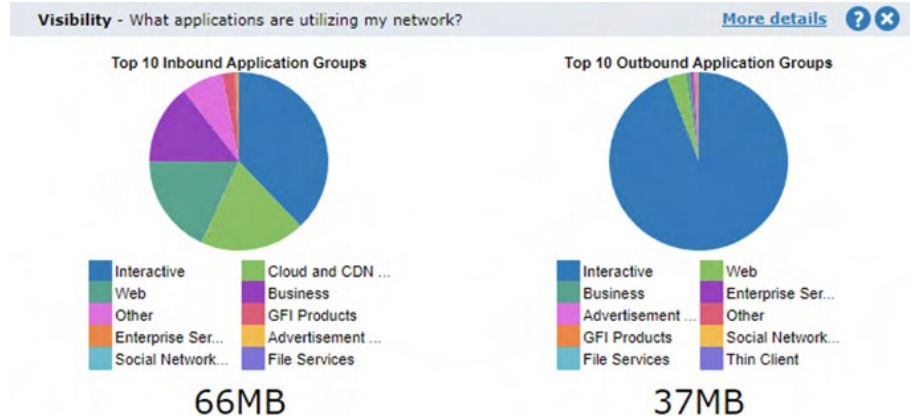
- The applications - BitTorrent, Flash - are appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you verify that you have an appropriate policy to control or protect this traffic. (Dec 22, 2015)
- The application - Skinnv - is appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you verify that you have an appropriate policy to control or protect this traffic. (Dec 17, 2015)
- The application - Print - is appearing in the top 10 for the first time in the preceding seven days. Exinda recommends that you verify that you have an appropriate policy to control or protect this traffic. (Dec 15, 2015)

Screenshot 81: Beispiel Empfehlungsmeldungen von GFI ClearView im Dashboard

Sichtbarkeit

Die Sichtbarkeit gibt Ihnen Einblick in den Datenverkehr in Ihrem Netzwerk, so dass Sie es effektiv kontrollieren oder schützen können. Die Sichtbarkeitsdiagramme zeigen die Anwendungsgruppen, die das Netzwerk nutzen. Diese Diagramme geben Antworten auf Fragen wie: "Überlasten Streaming-Anwendungen für Musik und Videos das Netzwerk? Überlasten Datensicherungen das Netzwerk?"

Klicken Sie auf den Drilldown-Link, um zu sehen, welche Anwendungen sich in einer Anwendungsgruppe befinden.



Freizeitgestaltung

Die Einsicht in wichtige Freizeit Anwendungen ist der erste Schritt, um sie zu verwalten. Diese Anwendungen sind in der Regel unerwünscht, da sie die Leistung wichtiger Geschäftsanwendungen beeinträchtigen, das Kundenerlebnis negativ beeinflussen, die Produktivität verringern, Viren in das Netzwerk einschleusen und das Herunterladen von illegalem oder urheberrechtlich geschütztem Material ermöglichen können.

Recreational - How much recreational usage is there? More details ? X			
Application	Hosts	Time	Data
	3	5m 30s	3MB
Games	1	20s	0MB
Instant Messaging	0	0s	0MB
P2P	0	0s	0MB
Social Networking	2	1m 50s	1MB
Streaming	2	3m 20s	2MB

3.2.2 Überwachung des Netzwerkverkehrs in Echtzeit

Dieser Abschnitt beschreibt die Echtzeit-Berichterstellung mit der GFI ClearView Web UI. Die Echtzeit-Monitore zeigen Informationen zum Datenverkehr an, der über überwachte Links mit einer von bis zu 1 Sekunde geleitet wurde.

Es gibt mehrere Ansichten, die Ihnen helfen, den Echtzeit-Netzwerkverkehr zu verstehen. Dazu gehören der Datenverkehr nach Anwendungen, nach Hosts (und Benutzern), nach Konversationen und nach Reduzierung pro Anwendung. Normalerweise sind Konversationen in Echtzeit die wertvollste Ansicht, da jede Konversation separat angezeigt wird und nicht über eine Anwendung oder einen Host kollabiert. In der Konversationsansicht können Sie die Ansicht auch nach IP-Adresse oder Subnetz filtern.

Bei der Untersuchung eines aktuellen Problems können Sie mit den Echtzeit-Monitoren Fragen wie diese beantworten:

- Meine Verbindung ist überlastet. Welche Gespräche, Anwendungen oder Hosts können zu der Überlastung beitragen?
- Ich weiß, dass ich ein Problem mit einem bestimmten Host oder Subnetz habe; welchen Datenverkehr verarbeitet dieser Host?

Überwachung von Netzwerkanwendungen in Echtzeit

Der Monitor "Anwendungen in Echtzeit" zeigt die wichtigsten Anwendungen nach Durchsatz, die in den letzten 1 Sekunde bis 1 Minute beobachtet wurden. Dieser Bericht beantwortet Fragen wie:

- Meine Verbindung ist überlastet; welche Anwendungen befinden sich gerade in meinem Netz?
- Wie viel Bandbreite verbraucht BitTorrent im ?

Der Monitor "Anwendungen in Echtzeit" zeigt den eingehenden Anwendungsverkehr getrennt vom ausgehenden Anwendungsverkehr an. Der Verkehr wird nach Übertragungsrate sortiert. Die Paketrage und die Anzahl der Datenflüsse für jede Anwendung in diesem Zeitraum werden ebenfalls angezeigt. Der Verteilungsprozentsatz zeigt den Anteil des Bandbreitenverbrauchs jeder Anwendung im Verhältnis zu allen Anwendungen.

Sie können das Diagramm so einstellen, dass es häufig, selten oder nicht aktualisiert wird. Bei jeder Aktualisierung werden die Daten für den ausgewählten Zeitbereich angezeigt.

Inbound Applications				
Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	202.846	119	183	
HTTP	146.626	38	73	
HTTPS	30.860	30	18	
SMTP	18.102	42	15	
ICMP	3.216	5	36	
Skype	1.846	3	26	
Twitter	1.645	1	1	
Unclassified	0.204	0	9	
IKE	0.163	0	1	
ExindaCom	0.104	0	3	
IMAP-SSL	0.080	0	1	

Screenshot 82: Der Monitor Eingehende Anwendungen

Outbound Applications				
Application Name	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	824.998	146	185	
HTTPS	486.747	52	18	
SMTP	217.695	32	15	
HTTP	109.099	47	73	
ICMP	4.987	8	36	
Skype	3.326	4	26	
Twitter	1.301	1	1	
Unclassified	0.885	1	9	
IKE	0.375	0	1	
ExindaCom	0.198	0	3	
Print	0.150	0	1	
Other	0.236	0	2	

Screenshot 83: Der Monitor für ausgehende Anwendungen

So finden Sie diesen Bericht:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Echtzeit> Anwendungen.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Überwachung von Hosts und Benutzern in Echtzeit

Die Widgets Hosts/Users im Realtime Monitor zeigen die internen Hosts mit dem höchsten Bandbreitenverbrauch im ausgewählten Zeitraum (1 Sekunde bis zu 60 Sekunden). Die angezeigten Daten beantworten Fragen wie:

Meine Verbindung ist überlastet. Welche Hosts befinden sich gerade in meinem Netzwerk?

»

Der Realtime Monitor trennt den eingehenden und ausgehenden Host-/Benutzerverkehr. Der Verkehr wird nach Übertragungsrate sortiert. Es werden die Paketrate und die Anzahl der Flows im vorangegangenen Zeitraum angezeigt. Falls konfiguriert, wird auch der Benutzername des internen Hosts angezeigt.

Der Verteilungsprozentsatz zeigt den Anteil des Bandbreitenverbrauchs jedes Hosts im Verhältnis zu allen Hosts für den betreffenden Zeitraum. Sie können das Diagramm so einstellen, dass es häufig, selten oder gar nicht aktualisiert wird.

Inbound Hosts/Users				
IP Address (User)	Transfer Rate (kbps)	Packet Rate (pps)	Flows	Distribution (%)
Total	138.037	46	117	
172.16.0.246 (Ksiakou)	105.324	10	5	
172.16.0.134 (Pforto)	13.909	3	4	
172.16.1.70 (Selfservice)	6.639	18	3	
172.16.1.240	3.771	6	34	
172.16.0.211	3.554	3	12	
172.16.0.244 (Cniko)	1.295	2	15	
172.16.0.127 (Sshannon)	1.060	2	20	
172.16.1.74	0.684	0	1	
172.16.0.239 (Jbothe)	0.593	1	5	
172.16.0.63 (Lenehan)	0.493	0	1	
Other	0.715	2	9	

Screenshot 84: Bericht zur Überwachung eingehender Hosts/Benutzer

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Echtzeit> Hosts/Benutzer.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Um die mit den internen Hosts verbundenen Benutzer anzuzeigen, aktivieren Sie das Kontrollkästchen **Benutzer anzeigen**.

NOTE

Active Directory must be configured on the GFI ClearView Appliances before usernames can be displayed in reports. See

For more information, refer to [Integrate with Active Directory](#) (page 503).

Überwachung von Gesprächen in Echtzeit

Der Realtime Conversations Monitor zeigt die wichtigsten Konversationen nach Durchsatz an, die von

der GFI ClearView Appliance während des ausgewählten Zeitraums (1 Sekunde bis zu 60 Sekunden). Dieser Bericht beantwortet Fragen wie:

- Meine Verbindung ist überlastet; wer macht gerade was in meinem Netz?
- Ich glaube, ich habe ein Problem mit einem bestimmten Host oder Subnetz; was macht dieser Host oder dieses Subnetz gerade?

Eingehender und ausgehender Gesprächsverkehr wird getrennt angezeigt. Konversationen werden durch externe IP-Adresse, interne IP-Adresse und Anwendung dargestellt. Bei einigen Verkehrsarten werden zusätzliche Informationen (wie die URL) in eckigen Klammern nach der Anwendung angezeigt.

Der Verkehr wird nach Übertragungsratesortiert. Die Paketrate und die Anzahl der Datenflüsse für jede Konversation vorangegangenen (ausgewählten) Zeitraum werden angezeigt. Sie können das Diagramm so einstellen, dass es häufig, selten oder gar nicht aktualisiert wird.

Der Realtime Conversations Monitor hilft Ihnen bei der Diagnose von Problemen:

- Filtern der Gespräche nach IP-Adresse oder Subnetz
- Anzeige des mit der internen IP-Adresse verbundenen Benutzernamens
- Verbindungen innerhalb eines Flusses können entweder einzeln angezeigt oder gruppiert werden
- Hervorhebung von beschleunigten Gesprächen in gelber Farbe und Angabe der verwendeten Beschleunigungstechnik
- Hervorhebung der vom Edge-Cache verarbeiteten Konversationen (in blau)
- Angabe, wie die Konversationen durch den Hochverfügbarkeitscluster fließen
- Anzeige von asymmetrischem Verkehr

Überwachung der Anwendungsreaktion in Echtzeit

Der Realtime Application Response Monitor zeigt die langsamsten Anwendungen nach Roundtrip-Zeit an, die von der GFI ClearView Appliance während des ausgewählten Zeitraums beobachtet wurden.

Dieser Bericht kann Fragen wie diese beantworten:

1. Bei welchen Anwendungen können Probleme auftreten?
2. Was sind meine leistungsschwächsten Anwendungen?
3. Warum funktioniert die Anwendung schlecht? Könnte es an einer Netzwerk- oder Serververzögerung liegen?

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Real Time> Application Response.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Der Monitor zeigt die Antwortmetriken der Anwendung an, wie z. B. Round-Trip-Time (RTT), normalisierte Netzwerkverzögerung, normalisierte Serververzögerung, normalisierte Gesamtverzögerung, Netzwerkverzögerung, Serververzögerung, Transaktionsverzögerung, Transaktionsanzahl und Flussanzahl nach Anwendung. Der Verkehr wird nach Round-Trip-Zeit sortiert.

Sie können das Diagramm so einstellen, dass es häufig, selten oder nicht aktualisiert wird.

Application Name	Application Response								Transaction Count	Flows
	RTT (ms)	Normalized Network (ms/kb)	Normalized Server (ms/kb)	Normalized Delay Total (ms/kb)	Network (ms)	Server (ms)	Transaction Delay (ms)			
HTTPS	192.49	1.07	7.88	8.94	1.88	13.90	15.78	1	4	

Screenshot 88: Das Anwendungsantwortmonitoring zeigt die Antwort nach RTT an.

NOTE

These statistics are only available if the Performance Metrics ASAM Module is enabled on the [System > Setup > Monitoring](#) page.

Überwachung der Echtzeit-Anwendung Antwort

Die APM-Werte sind als Echtzeitanzeige verfügbar. Die Echtzeitanzeige zeigt die APM-Werte nach Anwendung für den ausgewählten Zeitraum. Neben den werden auch die Anzahl der Flows und die Anzahl der Transaktionen angezeigt.

Anzeige des Berichts in der Benutzeroberfläche von GFI ClearView Web

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Monitor > Echtzeit** und wechseln Sie in den Bereich Registerkarte **Antwort der Anwendung**. Der folgende Bericht wird geöffnet:

Application Name	Application Response								Transaction Count	Flows
	RTT (ms)	Normalized Network (ms/kb)	Normalized Server (ms/kb)	Normalized Delay Total (ms/kb)	Network (ms)	Server (ms)	Transaction Delay (ms)			
HTTP	3074.50	1.94	0.98	2.92	73.19	2.16	75.36	38	79	
FTP	9.81	0.00	0.00	0.00	0.00	0.00	0.00	0	6	
mDNS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	4	
ICMPV6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	1	
HTTPS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	4	
DNS	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	202	
SMTP	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	2	

6. Um zu ändern, wie oft die Tabelle aktualisiert wird, wählen Sie eine **automatische Aktualisierungsrate** aus der Liste aus.

Anzeige des Berichts in GFI ClearView CLI

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie auf **Konfiguration > System > Tools > Konsole**.
5. Geben Sie den Appliance-Benutzernamen und das Kennwort bei den entsprechenden Aufforderungen ein. Führen Sie einen der folgenden Schritte aus:
 - Um in den privilegierten EXEC-Modus (enable) zu gelangen, führen Sie an der Eingabeaufforderung den Befehl: `hostname> enable`
Es erscheint die Eingabeaufforderung `hostname #`.
 - Um in den Konfigurationsmodus (config) zu gelangen, führen Sie an der Eingabeaufforderung die folgenden Befehle aus: `hostname # configure terminal`

Es erscheint die Eingabeaufforderung `hostname (config)#`.

7. Um APM-Echtzeitdaten über die CLI anzuzeigen, verwenden Sie den folgenden Befehl:

```
(config) # show realtime apm applications
```

Es werden die folgenden Ergebnisse angezeigt:

```
ex-240 (config) # show realtime apm applications
```

Application	RTT (ms)	Network (ms)	Server (ms)	Transaction (ms)	Transactions	Flows
ExindaWM	956.04	77706.24	206863.37	226125.26	48	4
Unclassified	459.74	35040.99	15000.30	37512.24	8	44
Replify	292.75	2660.00	0.00	2655.70	4	1
HTTP	256.16	202.86	147.08	338.41	10	9
HTTPS	217.45	97.34	26.83	124.18	10	6
CIFS	108.53	186.69	89.73	231.30	2	2
SSH	71.48	386.28	0.00	336.24	2	1
ExindaCom	0.00	0.00	0.00	0.00	0	16
mDNS	0.00	0.00	0.00	0.00	0	3
ICMP	0.00	0.00	0.00	0.00	0	7
ssdp	0.00	0.00	0.00	0.00	0	1
IGMP	0.00	0.00	0.00	0.00	0	15
NTP	0.00	0.00	0.00	0.00	0	2
sln	0.00	0.00	0.00	0.00	0	1

```
ex-240 (config) # █
```

Überwachung des Hostzustands in Echtzeit

Der Realtime Host Health Monitor zeigt ungesunde Hosts an, gemessen an der Anzahl der erneut übertragenen Bytes während des ausgewählten Zeitraums (1 Sekunde bis zu 60 Sekunden). Dieser Bericht beantwortet Fragen wie z. B.:

» Welche internen Hosts haben die größten Schwierigkeiten, den Datenverkehr erfolgreich zu übertragen?

Der Monitor trennt interne und externe Hosts und zeigt Metriken wie die Anzahl der erneut übertragenen Bytes, die Anzahl der abgebrochenen Verbindungen, die Anzahl der verweigerten Verbindungen, die Anzahl der ignorierten Verbindungen und die Anzahl der Flows für jeden internen und externen Host an, der während ausgewählten Zeitraums überwacht wird.

Der Verkehr wird nach der Anzahl der erneut übertragenen Bytes sortiert. Sie können das Diagramm so einstellen, dass es häufig, selten oder gar nicht aktualisiert wird.

Health						
Internal IP	Retransmitted (bytes)	Aborted	Refused	Ignored	Flows	
192.168.0.59	0	0	0	0	1	
192.168.0.87	0	0	0	0	1	
192.168.0.1	0	0	0	0	1	
192.168.0.35	0	0	0	0	1	
192.168.0.209	0	0	0	0	1	
192.168.60.59	0	0	0	0	1	
192.168.10.206	0	0	0	0	1	
172.16.0.222	0	0	0	0	1	

Bild 89: Der Bericht Realtime Host Health zeigt die Anzahl der erneut übertragenen Bytes an.

NOTE

These statistics are only available if the Performance Metrics ASAM Module is enabled on the System > Setup > Monitoring page.

Anzeige des Berichts in der Benutzeroberfläche von GFI ClearView Web

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie auf **Monitor>Echtzeit>Host Health**. Die Berichte enthalten den folgenden Status:
5. Um zu ändern, wie oft die Tabelle aktualisiert wird, wählen Sie eine **automatische Aktualisierungsrate** aus der Liste aus.

Connection Status	Description
Aborted Connections	Connections that were unexpectedly aborted by either the client or server sending a TCP reset.
Refused Connections	Connections that were refused by the server (TCP SYN sent, received ICMP refused or TCP reset in response).
Ignored Connections	Connections that were ignored by the server (TCP SYN sent, received nothing in response).

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Anzeige des Berichts in GFI ClearView CLI

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie auf **Konfiguration> System> Tools> Konsole**.
5. Geben Sie den Appliance-Benutzernamen und das Kennwort bei den entsprechenden Aufforderungen ein. Führen Sie einen der folgenden Schritte aus:

- Um in den privilegierten EXEC-Modus (enable) zu gelangen, führen Sie an der Eingabeaufforderung den Befehl: `hostname> enable`

Es erscheint die Eingabeaufforderung `hostname #`.

- Um in den Konfigurationsmodus (config) zu gelangen, führen Sie an der Eingabeaufforderung die folgenden Befehle aus: `hostname # configure terminal`

Es erscheint die Eingabeaufforderung `hostname (config)#`.

6. Um den TCP-Zustand in Echtzeit über die CLI anzuzeigen, verwenden Sie den folgenden Befehl:

```
(config) # show realtime apm hosts
```

Es werden die folgenden Ergebnisse angezeigt:


```
ex-240 (config) # show realtime apm hosts
```

Internal Host	Retransmissions	Aborted	Refused	Ignored	Flows
172.16.1.240	0	0	0	0	13
192.168.0.176	0	0	0	0	1
172.16.0.213	0	0	0	0	1
192.168.50.147	0	0	0	0	1
192.168.0.179	0	0	0	0	1
172.16.0.63	0	0	2	0	3
172.16.1.242	0	0	0	0	1
192.168.40.96	0	0	0	0	1
192.168.0.178	0	0	0	0	6
0.0.0.0	0	0	0	0	1
192.168.0.209	0	0	0	0	1
192.168.50.143	0	0	0	0	1
172.16.0.252	0	0	0	0	1
172.16.0.108	0	0	0	0	3
172.16.1.149	0	0	0	0	3
172.16.0.67	0	0	0	0	5
172.16.0.190	0	1	0	0	4
192.168.0.118	0	0	0	0	1
192.168.0.145	0	0	0	0	1
192.168.0.207	0	0	0	0	1

Screenshot 90: Echtzeit-TCP-Zustand über die CLI.

3.2.3 Überwachung des Netzes Durchsatzes

Der Bericht "Netzwerkübersicht" zeigt den Verkehrsdurchsatz im Zeitverlauf nach Anwendung, Anwendungsgruppen, internen oder externen Hosts, internen oder externen Benutzern, Konversationen oder URLs. Sie können Elemente aus dem Diagramm entfernen, um Verkehrsmuster und Quellen zu isolieren.

Dieser Bericht beantwortet Fragen wie:

» Wie sieht das Muster des Durchsatzes für bestimmte Anwendungen, Anwendungsgruppen, Benutzer, Hosts usw. aus? » Gibt es Spitzen und welche Art von Datenverkehr kann diese Spitzen verursachen?

» Was würde mit dem Durchsatz passieren, wenn ich eine Richtlinie zum Blockieren einer bestimmten Anwendung, Anwendungsgruppe, eines Benutzers oder Hosts erstellen würde?

Die Diagramme helfen Ihnen, Probleme zu diagnostizieren und Was-wäre-wenn-Szenarien durchzuführen, um die richtige Größe Ihres Netzwerks zu bestimmen.

Der Bericht zeigt LAN- und WAN-seitige Diagramme sowohl für eingehenden als auch für ausgehenden Datenverkehr. Das gesamte Datenvolumen, der maximale Durchsatz und der durchschnittliche Durchsatz werden ebenfalls in Tabellen unter jedem Diagramm angezeigt. Die Diagramme fassen Daten außerhalb der Top 10 in einer Kategorie namens "Andere" zusammen.

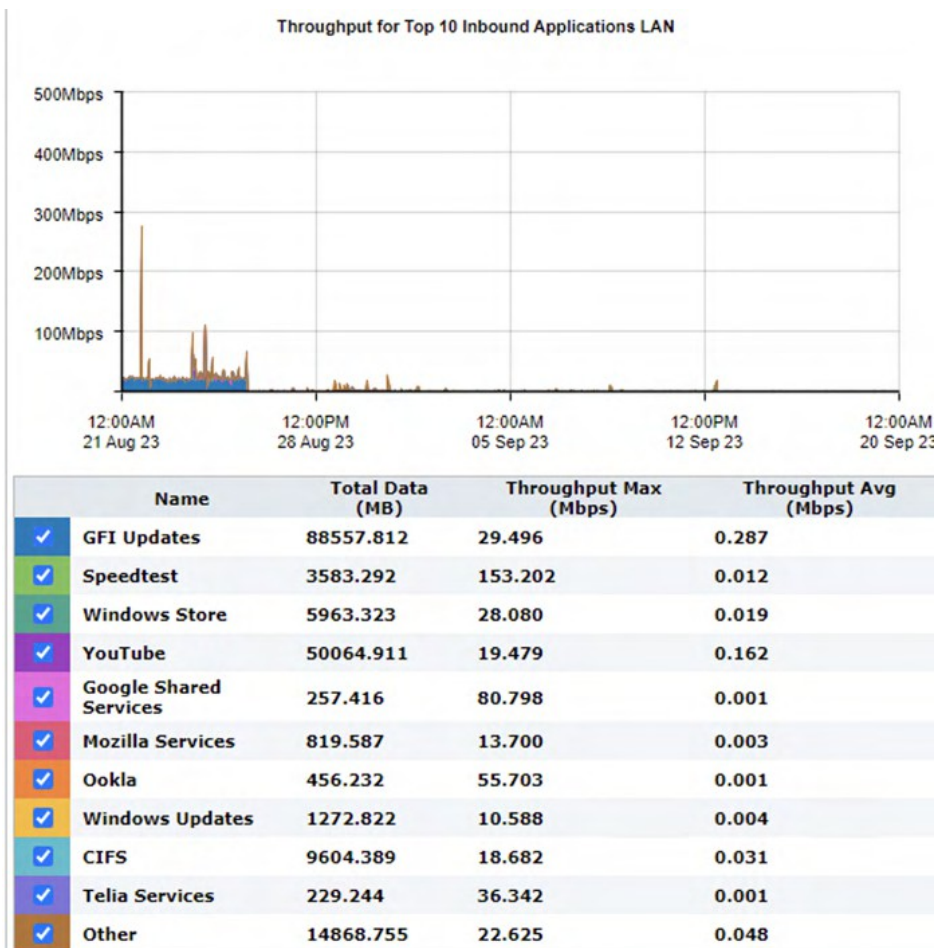


Bild 93: Der Bericht Netzwerkübersicht zeigt das LAN-Verkehrsvolumen für die 10 wichtigsten eingehenden Anwendungen an.

Wo kann ich diesen Bericht finden?

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).

2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor> Netzwerk**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

So bestimmen Sie die richtige Größe Ihres Netzes (d. h. entfernen Sie Elemente aus der Tabelle)

Entfernen Sie bestimmte Arten von Datenverkehr aus dem Diagramm, indem Sie das entsprechende Kontrollkästchen in der Legende unterhalb des deaktivieren. Der verbleibende Verkehr stellt dar, wie Ihr Netzwerkverkehr aussehen würde, wenn Sie diese Art von Verkehr blockieren würden. Sie können dann eine angemessene Menge an benötigter Bandbreite bestimmen.

Ermittlung des Durchsatzes, der über einem bestimmten Perzentil liegt

Wählen Sie die gewünschte Perzentilstufe aus dem Auswahlfeld **Perzentilmarker zur Anzeige auswählen** aus.

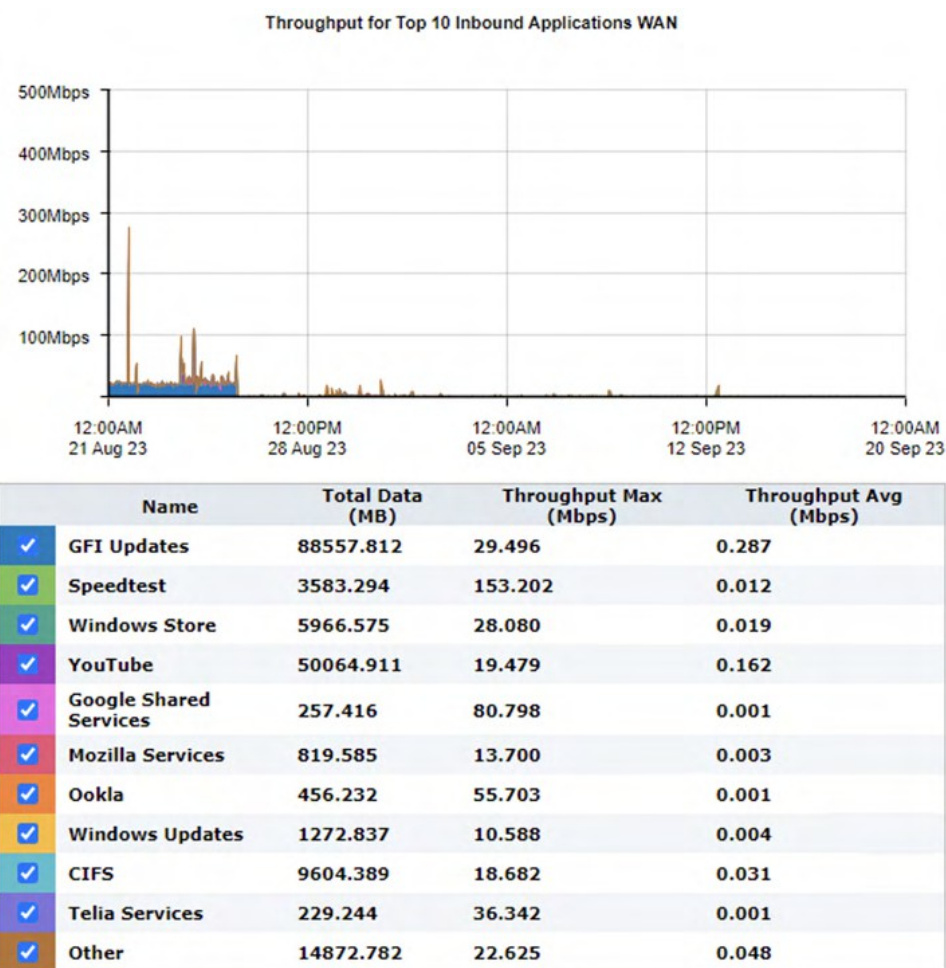


Bild 94: Der Bericht Netzwerkübersicht zeigt das WAN-Verkehrsvolumen für die 10 wichtigsten eingehenden Anwendungen an.

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Interaktive Zeitdiagramme verwenden](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm festlegen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Um zu verstehen, wie Sie den drucken oder planen können, siehe [Drucken und Planen](#)

Berichte.

3.2.4 Überwachung des Dienstes

Erfahren Sie, wie Sie Berichte über die Anwendungsleistung, die Verfügbarkeit Ihres ISP und den Zustand und die Effizienz des TCP-Verkehrs anzeigen können.

Überwachung der Anwendungsleistung scores

Der Application Performance Score (APS)-Bericht zeigt Ergebnisse zur Bewertung der Netzwerkleistung und der Benutzerfreundlichkeit bei der Nutzung geschäftskritischer Anwendungen.

Diese Diagramme können Fragen wie diese beantworten:

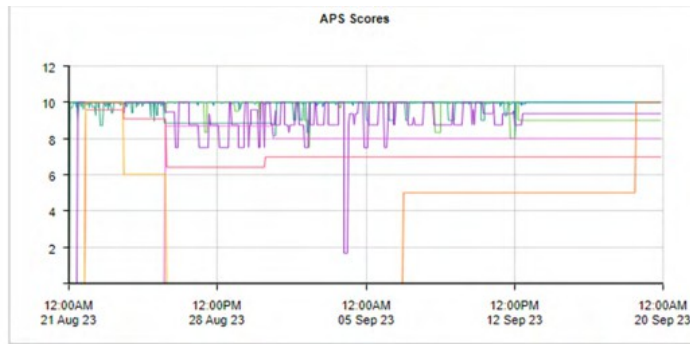
- » Ist die Leistung meiner wichtigen Anwendungen aus der Netzwerkperspektive für die » Netzwerkbenutzer gut? Handelt es sich um ein dauerhaftes Problem oder wird es schlimmer?
- » Wenn eine Anwendung nicht gut funktioniert, was könnte die Ursache für das Problem sein? So rufen Sie den Bericht auf:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Service Levels> Application Performance Score (APS).

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Eine Punktzahl zwischen 0 und 10, wobei 0 für schlecht und 10 für ausgezeichnet steht, zeigt an, ob App gut oder schlecht abschneidet.

Die Ergebnisse werden im Laufe der Zeit grafisch dargestellt, um die Veränderungen und Trends der Ergebnisse aufzuzeigen. Die zugrundeliegenden Metriken und Maßnahmen, die zur Berechnung der Werte verwendet werden, sind in der Tabelle unter dem Diagramm aufgeführt. Sie können die Details der APS durch Anklicken eines Anwendungsnamens aufrufen.



Name	APS Scores								
	Score	Normalized Delays (ms/kb)		Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
		Network	Server	Network	Server		Inbound	Outbound	
Microsoft products	9.97	50.93	3.09	158.34	8.99	16.53	1.30	0.30	111.67
Skype	9.89	102.73	1.35	363.53	6.16	1.13	2.50	6.70	155.50
Office 365 Solution Center (620)	9.83	63.33	0.98	293.56	4.43	13.99	3.10	4.10	105.29
Microsoft Teams Solution Center (8388951)	9.11	22.96	1.39	133.33	8.13	0.22	1.90	1.00	68.26
Zoom Solution Center (8388825)	8.05	107.03	22.35	573.54	107.65	40.12	0.00	0.70	195.39
Speedtest Solution Center (831)	8.01	2244.16	11.73	1011.60	85.40	580.98	0.50	1.40	74.36
CIFS	5.06	27.35	0.77	15.04	0.61	0.00	5.20	0.00	6.12
Salesforce Solution Center (521)	4.00	102.69	0.23	206.27	0.80	50.62	0.00	4.60	81.61

Bild 95: Der Application Performance Score zeigt im Zeitverlauf Werte von 0 bis 10 an.

Eine Bewertung umfasst eine oder mehrere der folgenden Metriken:

- » Netzwerkverzögerung - die Zeit, die die Daten benötigen, um das Netzwerk zu durchqueren » (auf der Leitung) Serververzögerung - die Zeit, die ein Server benötigt, um auf den Antrag zu antworten
- » Normalisierte Netzwerkverzögerung - die Zeit, die die Daten für die Durchquerung des Netzwerks benötigen, wobei die Verzögerung unabhängig von der Transaktionsgröße gemessen wird, indem eine normalisierte Paketgröße von 1024 Byte angenommen wird
- » Normalisierte Server-Verzögerung - die Zeit, die ein Server benötigt, um auf die Anfrage zu antworten, wobei die Verzögerung unabhängig von der Transaktionsgröße gemessen wird, indem eine normalisierte Paketgröße von 1024 Bytes angenommen wird
- » Hin- und Rückreisezeit - die Zeit, die für
- » Jitter - das Maß für die Variabilität der Netzwerkverzögerung, definiert als eine Standardabweichung » der Netzwerkverzögerung
- Eingangungsverlust - der Prozentsatz der Paketverluste auf eingehenden Verkehr
- » Ausgehender Verlust - der Prozentsatz der Paketverluste beim ausgehenden Verkehr

Für jede Metrik, die zur Bewertung beiträgt, ist ein Schwellenwert festgelegt. Der Schwellenwert kann manuell festgelegt oder automatisch von der GFI ClearView Appliance bestimmt worden sein, die den Datenverkehr über einen bestimmten Zeitraum beobachtet hat, um einen Basisschwellenwert zu ermitteln. Die Tabelle unterhalb des Diagramms zeigt die aktuell beobachteten Werte für diese Metriken und gibt an, ob dieser Wert als gut oder schlecht eingestuft wird.

- » Liegt der beobachtete Verkehr innerhalb des Schwellenwerts, gilt er als gut und wird in der APS-Scores-Tabelle grün eingefärbt.
- » Liegt der beobachtete Verkehr über dem Schwellenwert, aber nicht über dem Vierfachen des Schwellenwerts, gilt er als tolerierbar und wird gelb markiert.
- » Liegt der beobachtete Verkehr über dem 4-fachen des Schwellenwerts, gilt er als schlecht und wird rot eingefärbt.
- » Wenn die Tabelle für eine bestimmte Kennzahl keine Farbe enthält, bedeutet dies, dass diese Kennzahl nicht zur Berechnung des APS-Scores beiträgt.

Anhand dieser Informationen können Sie feststellen, welche Metriken zur Leistungsbewertung einer Anwendung beitragen.

Generieren Sie einen PDF-Bericht der APS Ergebnisse

Erstellen Sie einen Bericht, der die APS, den TCP-Zustand und die TCP-Effizienz für eine bestimmte Zeitspanne enthält.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Bericht** und wechseln Sie auf die Registerkarte **PDF-Berichte**.
6. Klicken Sie auf **Neuen PDF-Bericht hinzufügen**.
7. Wählen Sie im Bereich Berichtsauswahl **APS**, **TCPHealth** und **TCPEfficiency**.
8. Geben Sie im Bereich Berichtsdetails einen Namen für den Bericht ein.
9. Geben Sie an, wie oft der Bericht erstellt werden soll.
10. Klicken Sie auf **Neuen Bericht hinzufügen**.
11. Um den Bericht zu erstellen, suchen Sie den Bericht in der Liste und klicken Sie auf **PDF**.

Was zu erwarten ist

Wenn ein APS-Bericht keine Daten anzeigt

Entweder sind für das APS-Objekt keine Schwellenwerte festgelegt, so dass die Punktzahl nicht berechnet werden kann, oder es gibt in dem auf dem Bildschirm angezeigten Zeitraum keinen Verkehr für die angegebene Anwendung im Netz.

Wenn die Schwellenwerte mit Hilfe der Baselineing-Funktion festgelegt wurden

Sie sollten eine Anwendungsleistung von 9,0 erhalten, wenn Sie den gleichen Datenverkehr beobachten würden.

Evaluierung der APS

Wenn die Schwellenwerte mit Hilfe der Baselineing-Funktion festgelegt wurden, gilt eine Punktzahl von 8,5 oder höher als gute Punktzahl. Die Schwellenwerte werden automatisch so festgelegt, dass sie geringfügig über dem Durchschnitt der beobachteten Maßnahmen liegen, so dass ein guter Wert am oberen Ende der Bewertungsspanne liegt.

Wenn Sie die Schwellenwerte manuell so festlegen, dass Ihre Schwellenwerte an der Grenze dessen liegen, was Sie als gut oder nicht gut ansehen, dann sollten Sie APS-Werte über 5,0 als gut betrachten, da Sie statistisch gesehen in der Hälfte der Fälle erwarten würden, dass die beobachteten Werte leicht über Ihrem Schwellenwert liegen und in der anderen Hälfte der Fälle würden die beobachteten Werte leicht unter dem Schwellenwert liegen.

Ein Blick auf die Ergebnisse

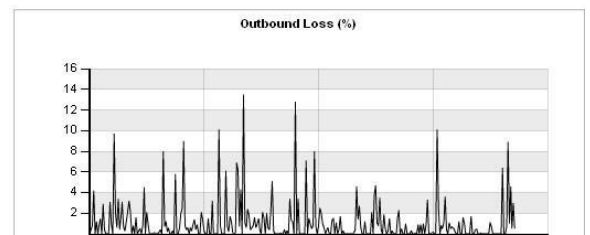
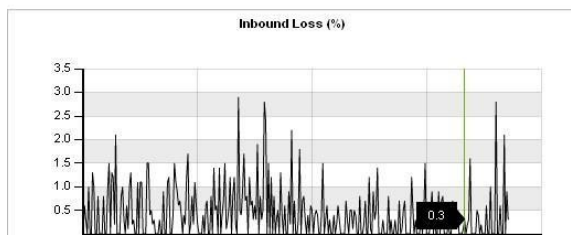
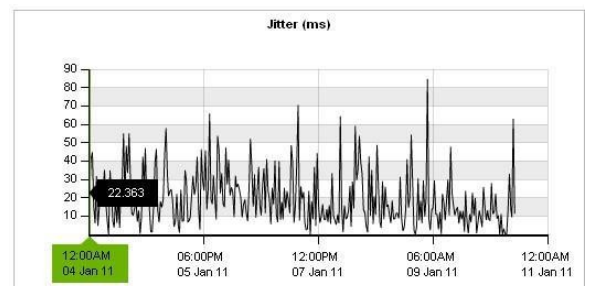
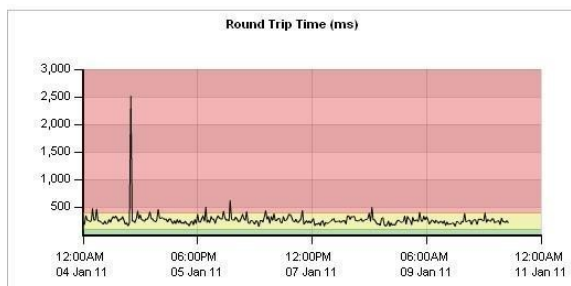
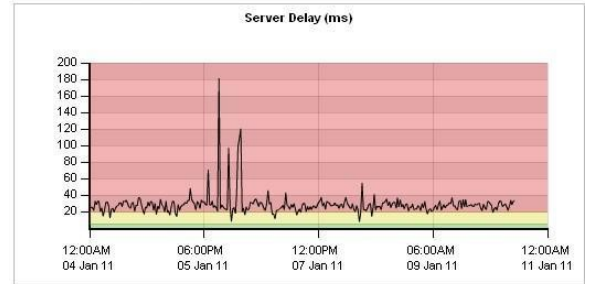
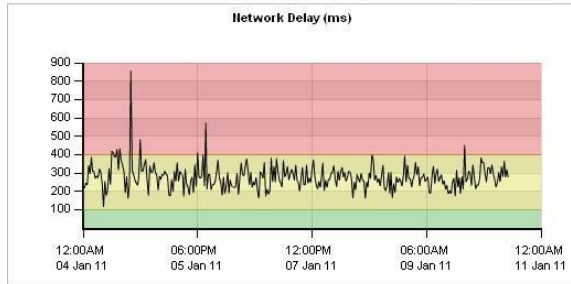
Ermittlung der Ursachen für einen niedrigen APS-Wert

Klicken Sie auf den APS-Namen in der Tabelle. Ein neuer Bildschirm mit Diagrammen für jede zugrunde liegende Kennzahl wird angezeigt. Der Hintergrund jedes Diagramms ist farbig, um den Wert innerhalb des Schwellenwerts, innerhalb des 4fachen Schwellenwerts und darüber darzustellen.

Wenn der Hintergrund des Diagramms nicht eingefärbt ist, trägt diese Kennzahl nicht zur Berechnung des APS-Wertes bei. Sie können in diese Diagramme hineinzoomen, indem Sie innerhalb eines Diagramms klicken und ziehen, um in den Bereich der x-Achse zu zoomen. Alle anderen Diagramme synchronisieren ihre Zoombereiche mit dem angegebenen Zoombereich.

Die Metriken, die schlechte Werte aufweisen, könnten auf ein zu untersuchendes Problem hinweisen. Wenn beispielsweise die Netzwerkverzögerung gut, die Serververzögerung aber schlecht ist, wissen Sie, dass das Netzwerk nicht die Schuld trägt und dass der Serveradministrator sich den Anwendungsserver ansehen sollte.

APS Metrics for License DB					
Transaction Delays (ms)		Jitter (ms)	Loss (%)		RTT (ms)
Network	Server	Inbound	Outbound		
277.85	28.44	19.49	0.40	1.00	265.18



Feststellen, ob ein Problem anhaltend ist

Schauen Sie sich den Zeitplan für den APS-Wert an. Wenn der Wert über einen längeren Zeitraum niedrig war oder wenn es so aussieht, als würde der Wert sinken, wissen Sie, dass es sich um ein anhaltendes Problem handelt, das angegangen werden muss.

Feststellen, ob Sie auf die normalisierten Verzögerungen oder die Transaktionsverzögerungen achten sollten

Im Allgemeinen sollten Sie die Transaktionsverzögerungen verwenden, es sei denn, das zu überwachende Protokoll hat große oder variable Paketgrößen. Das normalisierte Verzögerungsmaß normalisiert die Punktzahl auf eine Paketgröße von 1024 und ermöglicht so einen einfacheren Vergleich der Verzögerungen, wenn die Pakete unterschiedlich groß sind.

Konfigurieren des Systems, um Sie zu benachrichtigen, wenn der APS-Wert zu niedrig ist

Sie können das System so konfigurieren, dass es eine E-Mail sendet, wenn der APS-Wert unter einen von Ihnen festgelegten Wert fällt und für eine bestimmte Dauer unter diesem Wert bleibt. Sie können zum Beispiel festlegen, dass Sie benachrichtigt werden, wenn der Wert unter 7,0 fällt und 5 Minuten lang unter 7,0 bleibt.

Bessere Lesbarkeit der APS-Tabelle durch Entfernen der Bewertungslinien

» Sie können vorübergehend Zeilen aus dem APS-Diagramm entfernen, indem Sie die Kontrollkästchen neben dem APS-Namen in der Tabelle deaktivieren.

» Sie können einen Bereich von Interesse vergrößern, indem Sie in das Diagramm klicken und ziehen, um einen kleineren Zeitbereich auszuwählen. Dies hat oft den Effekt, dass die Linien abgeflacht werden, so dass es weniger unübersichtlich erscheint.

Berechnung der Leistung einer Anwendung

Das Application Performance Score-Objekt definiert den zu überwachenden Anwendungsverkehr und die zu bewertenden Leistungskennzahlen der Anwendung. Es bietet auch Schwellenwerte für die Anwendungsleistung, die bei der Bewertung verwendet werden.

Für jede Metrik wird der beobachtete Verkehr mit dem Schwellenwert verglichen und in eine von drei Kategorien eingestuft:

- » Gut - Die Basislinie für die Anwendung ist gut, was bedeutet, dass die Leistung der Anwendung innerhalb der erwarteten Werte liegt (unterhalb des Schwellenwerts). Die Benutzer sollten mit der Anwendungsleistung zufrieden sein.
- » Toleriert - Die Leistung der Anwendung ist geringer als erwartet, liegt aber immer noch in einem Bereich, den die Benutzer tolerieren sollten (zwischen dem Schwellenwert und dem Vierfachen des Schwellenwerts).
- » Frustriert - Die Anwendung hat eine schlechte Leistung (mehr als das Vierfache des Schwellenwerts). Die Benutzer werden frustriert sein.

Die Anzahl der guten Beobachtungen für alle Metriken mit einem Schwellenwert wird zusammengezählt und erhält eine volle Gewichtung; die Anzahl der tolerierten Beobachtungen für alle Metriken mit einem Schwellenwert wird zusammengezählt und erhält eine halbe Gewichtung; und alle frustrierten Beobachtungen erhalten eine Nullgewichtung. Diese gewichteten Gesamtwerte werden addiert und durch die Gesamtzahl der Beobachtungen geteilt.

$$\text{aps} = 10 * ((1 * \text{Anzahl der zufriedenen Proben}) + (0,5 * \text{Anzahl der tolerierten Proben}) + (0 * \text{Anzahl der frustrierten Proben})) / \text{Proben insgesamt}$$

EXAMPLE

For HTTP, a threshold is configured for Network Delay as $T = 300 \text{ msec}$ and a threshold is configured for round-trip time (RTT) as $T = 40 \text{ msec}$.

In one 10s period, 11 flows are sampled for HTTP with the following results:

- » 2 flow samples have a network delay of $> 1200 \text{ ms}$ (frustrated samples)
- » 3 flow samples have a network delay of $> 300 \text{ ms}$ but $< 1200 \text{ ms}$ (tolerated samples)
- » 6 flow samples have a network delay of $< 300 \text{ ms}$ (satisfied samples)
- » 1 flow sample has a RTT of $> 40 \text{ ms}$ but $< 160 \text{ ms}$ (tolerated samples)
- » 10 flow samples have a RTT of $< 40 \text{ ms}$ (satisfied samples)

The APS score is calculated as follows:

$$\text{aps} = 10 * (1 * (6 + 10) + 0.5 * (3 + 1) + 0 * 2) / 22 = 8.1$$

Festlegung von Schwellenwerten

Welche Schwellenwerte für eine Anwendung geeignet sind, hängt von der jeweiligen Netzwerkumgebung ab. Schwellenwerte können bei der Konfiguration eines APS-Objekts manuell festgelegt werden, oder die GFI ClearView-Appliance kann den Datenverkehr für eine Anwendung für einen Basiszeitraum analysieren und einen empfohlenen Schwellenwertsatz erstellen.

Weitere Informationen finden Sie unter [Konfigurieren von Anwendungsperformance-Score-Objekten](#).

Überwachung der Netzreaktion SLA

Der SLA-Monitor meldet die Leistung Ihres ISP anhand einer Reihe von vordefinierten Kriterien. Der SLA-Monitor sendet alle 10 Sekunden einen 64-Bit langen ICMP-Ping an die . Er meldet die maximale und durchschnittliche Latenzzeit und den prozentualen Verlust der Pings über die Zeit. Dieser Bericht beantwortet Fragen wie:

- » Ist mein ISP immer erreichbar?
- » Wie hoch ist die Latenzzeit meines Internetanbieters?

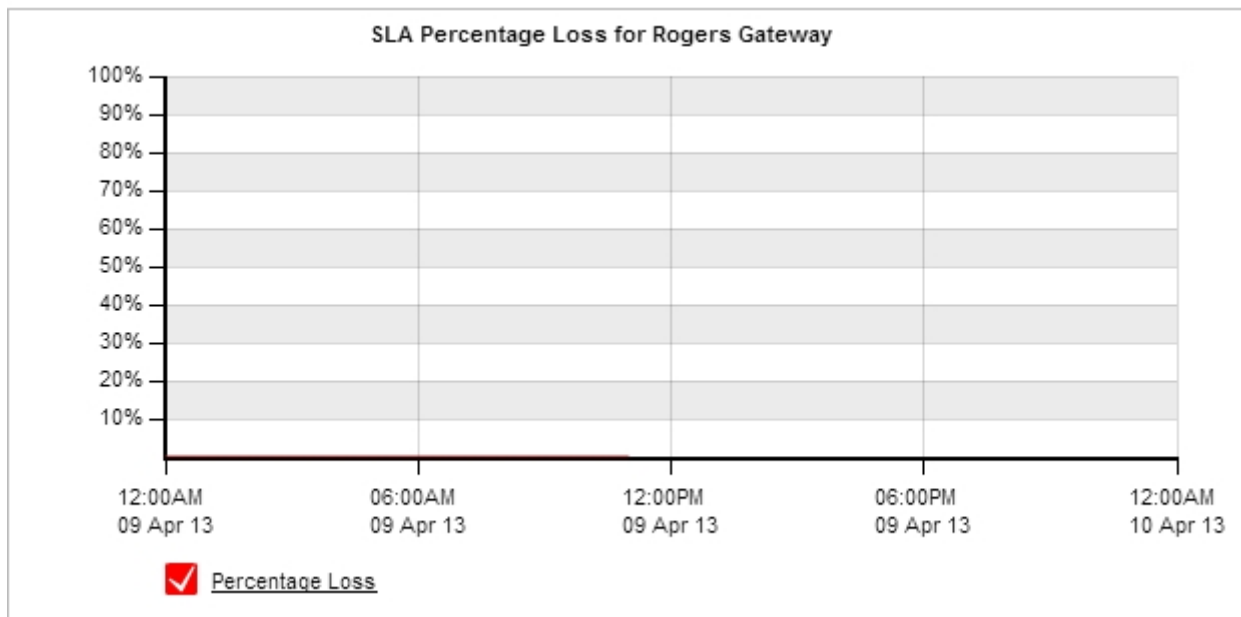
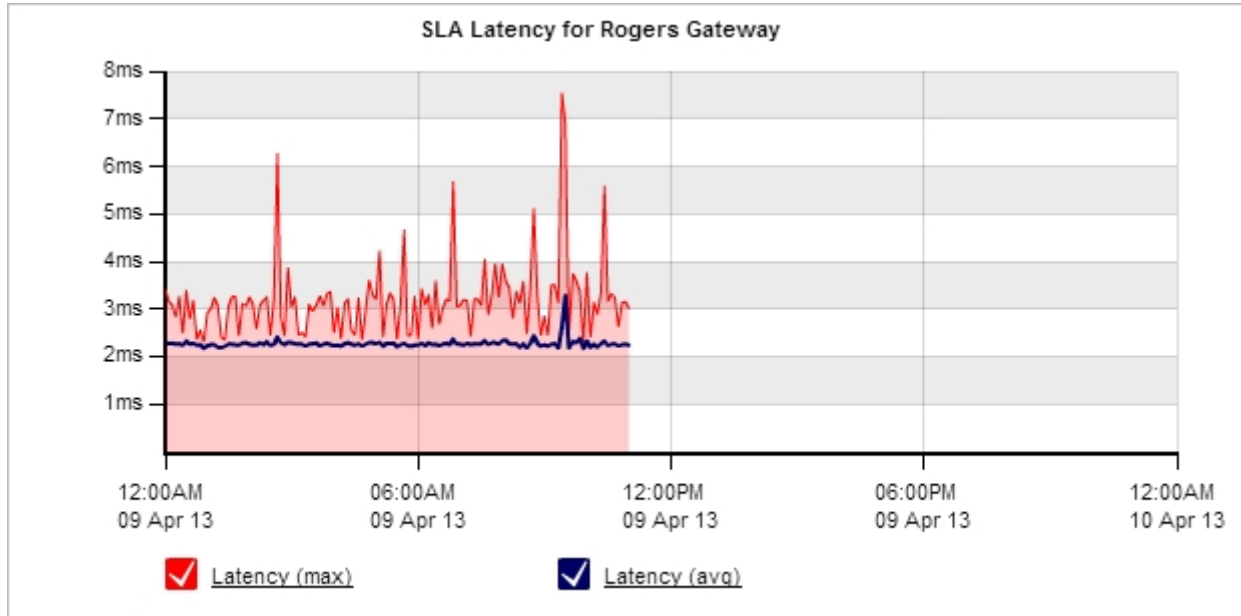


Bild 96: Das SLA-Monitoring erfasst die Latenzzeit und den prozentualen Verlust im Zeitverlauf.

Für jedes SLA-Objekt erfasst GFI ClearView in der Tabelle unterhalb der Diagramme die IP-Adresse, die prozentuale Verfügbarkeit, die minimale und maximale sowie die durchschnittliche Latenz.

- » Die Verfügbarkeit ist der Prozentsatz der Zeit, in der eine Ressource von der GFI ClearView-Appliance erreicht werden kann.
- » Die Latenz ist die Verzögerung beim Erhalt einer ICMP-Echo-Antwort auf eine von der GFI ClearView-Appliance generierte ICMP-Echo-Anfrage. Sie stellt sowohl die Verzögerung von der lokalen GFI ClearView-Appliance zu einem Remote-Host als auch zurück dar.

SLA Statistics for DNS					
Site Name	IP Address	Availability	Min Latency (ms)	Avg Latency (ms)	Max Latency (ms)
DNS	203.2.192.124	100.00 %	44.34	57.65	113.15

Wo kann ich diesen Bericht finden?

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Service Levels> Network Response (SLA).

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

So fügen Sie eine SLA Site hinzu

Klicken Sie auf den Link **SLA-Site hinzufügen/bearbeiten....** Siehe TO-DO für Details zur Konfiguration eines SLA-Objekts.

So zeigen Sie das Diagramm für eine andere SLA-Site an

Wählen Sie den gewünschten Standort aus der SLA-Standortauswahl.

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Verwendung von interaktiven Zeitdiagrammen](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Überwachung der Effizienz von TCP

Der Bericht zur TCP-Effizienz zeigt die Gesamteffizienz aller TCP-Verbindungen im Zeitverlauf. Die Berichtsdaten können nach Anwendungen, internen Hosts oder externen Hosts kategorisiert werden. Sie können bestimmte Anwendungen oder Hosts aufschlüsseln, um die Effizienz für einen bestimmten Datenverkehr anzuzeigen.

Dieser Bericht beantwortet Fragen wie:

- » Gibt es Netzwerkverzögerungen aufgrund von TCP-Ineffizienzen?
- » Gibt es bei einer bestimmten Anwendung oder einem bestimmten Host Probleme aufgrund von erneuten Übertragungen?

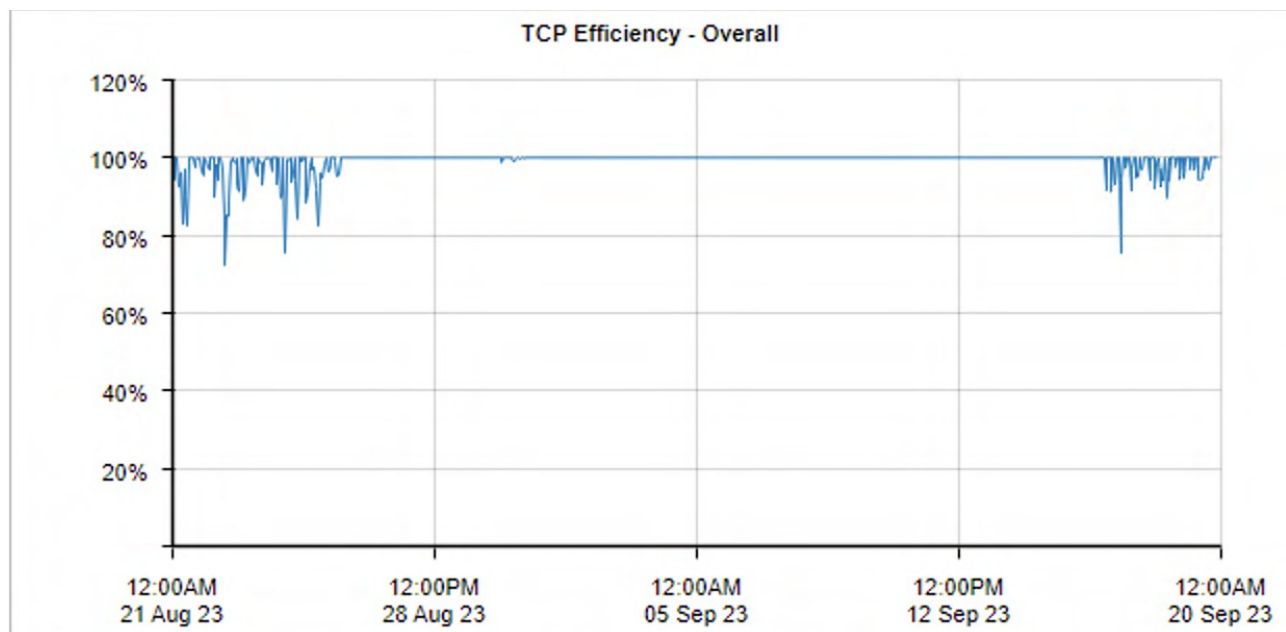


Bild 97: Der Bericht TCP-Effizienz zeigt die Effizienz von TCP-Verbindungen im Zeitverlauf an.

Die TCP-Effizienz wird nach der folgenden Formel berechnet:

$$\text{TCP-Effizienz} = (\text{Gesamte Bytes} - \text{zurückgesendete Bytes}) / \text{Gesamte Bytes}$$

Die nachstehende Tabelle zeigt sowohl neu übertragene Bytes als auch die Effizienz pro Anwendung oder Host. Jedes Element in der Tabelle unten kann aufgeschlüsselt werden, um Details zur TCP-Effizienz und ein Diagramm für dieses Element anzuzeigen.

Top 30 Least Efficient Applications					
	Bytes Inbound (MB)		Bytes Outbound (MB)		Efficiency (%)
	Retransmitted	Total	Retransmitted	Total	
TripleLift	0.004	0.023	0.003	0.010	81.33
Microsoft Outlook	20.862	99.123	0.203	19.795	82.29
IdenTrust	0.001	0.004	0.000	0.003	87.71
Facebook Chat	0.001	0.008	0.001	0.003	87.94
Psiphon	0.005	0.175	0.047	0.280	88.55
Facebook	0.001	0.015	0.002	0.007	88.97
Cloudflare	0.003	0.548	0.266	1.943	89.19
DNA TV	3.461	31.578	0.003	0.492	89.20
Google Play	0.278	5.494	1.016	6.831	89.50
Outbrain	0.000	0.014	0.002	0.010	90.52
OpenX	0.000	0.004	0.001	0.002	90.99
LiveRamp	0.001	0.024	0.002	0.008	91.15
Amazon Cloud	23.731	201.964	0.000	135.182	92.96
Taboola	0.000	0.021	0.002	0.011	93.12
Xandr	0.000	0.033	0.004	0.023	93.18
Telia Services	15.609	229.244	0.010	2.996	93.27
Ada Support	0.000	0.007	0.001	0.002	93.33
Zoom	6.626	100.483	0.005	2.191	93.54
Index Exchange	0.000	0.009	0.001	0.009	93.60
Demandbase	0.000	0.007	0.001	0.003	93.60
Media-net	0.000	0.018	0.002	0.008	93.74
Salesforce	0.000	0.012	0.001	0.006	93.75
Oracle Services	0.000	0.023	0.002	0.012	93.83
CookiePro	0.036	0.605	0.002	0.033	94.07
LinkedIn	0.000	0.019	0.002	0.009	94.14
xbox-live	0.239	4.043	0.003	0.107	94.16
Google Ads	0.079	2.922	0.125	0.601	94.19
Verizon Media Services	0.000	0.006	0.001	0.004	94.49
Microsoft OneNote	0.010	0.344	0.009	0.052	95.18
Microsoft Bing	2.102	39.988	0.053	5.474	95.26

Bild 98: Der Bericht zur TCP-Effizienz zeigt die 50 am wenigsten effizienten Anwendungen an.

Wo kann ich diesen Bericht finden?

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.

4. Gehen Sie zu Monitor> Service Levels> TCP Efficiency.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

» Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Verwendung von interaktiven Zeitdiagrammen](#).

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).

» Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Überwachung des Zustands von TCP

Der TCP-Zustandsbericht zeigt die Anzahl der abgebrochenen, abgelehnten und ignorierten Verbindungen im Zeitverlauf an. Der Bericht kann nach Anwendungen, internen Hosts oder externen Hosts kategorisiert werden. Sie können bestimmte Anwendungen oder Hosts aufschlüsseln, um den Zustand für einen bestimmten Datenverkehr anzuzeigen.

Dieser Bericht kann Fragen wie die folgenden beantworten:

» Warum gibt es so viele Neuübertragungen für eine bestimmte Anwendung oder einen bestimmten Host?"

Die Definitionen für abgebrochene, abgelehnte und ignorierte Verbindungen, die vom TCP Health Report verwendet werden:

» **Abgebrochen** - Verbindungen wurden aufgebaut, aber durch ein RST (Reset) entweder vom Client oder vom Server beendet, anstatt sie sauber zu schließen. Eine hohe Anzahl abgebrochener Verbindungen kann auf Netzwerk- oder Serverprobleme hinweisen.

» **Abgelehnt** - Ein SYN-Paket wurde beobachtet und als Antwort wurde eine RST- oder ICMP-Meldung "Verbindung abgelehnt" empfangen. Dies bedeutet in der Regel, dass der Server aktiv ist, die Anwendung jedoch nicht verfügbar ist oder nicht richtig funktioniert. Es kann auch bedeuten, dass ein TCP-Port-Scan durchgeführt wird.

» **Ignoriert** - Ein SYN-Paket wurde beobachtet, aber es wurde keine SYN-ACK-Antwort empfangen. Dies bedeutet normalerweise, dass der Server nicht antwortet, nicht existiert, nicht erreichbar ist oder die Verbindungsanfrage ignoriert. Es kann auch bedeuten, dass ein TCP-Port-Scan durchgeführt wird.

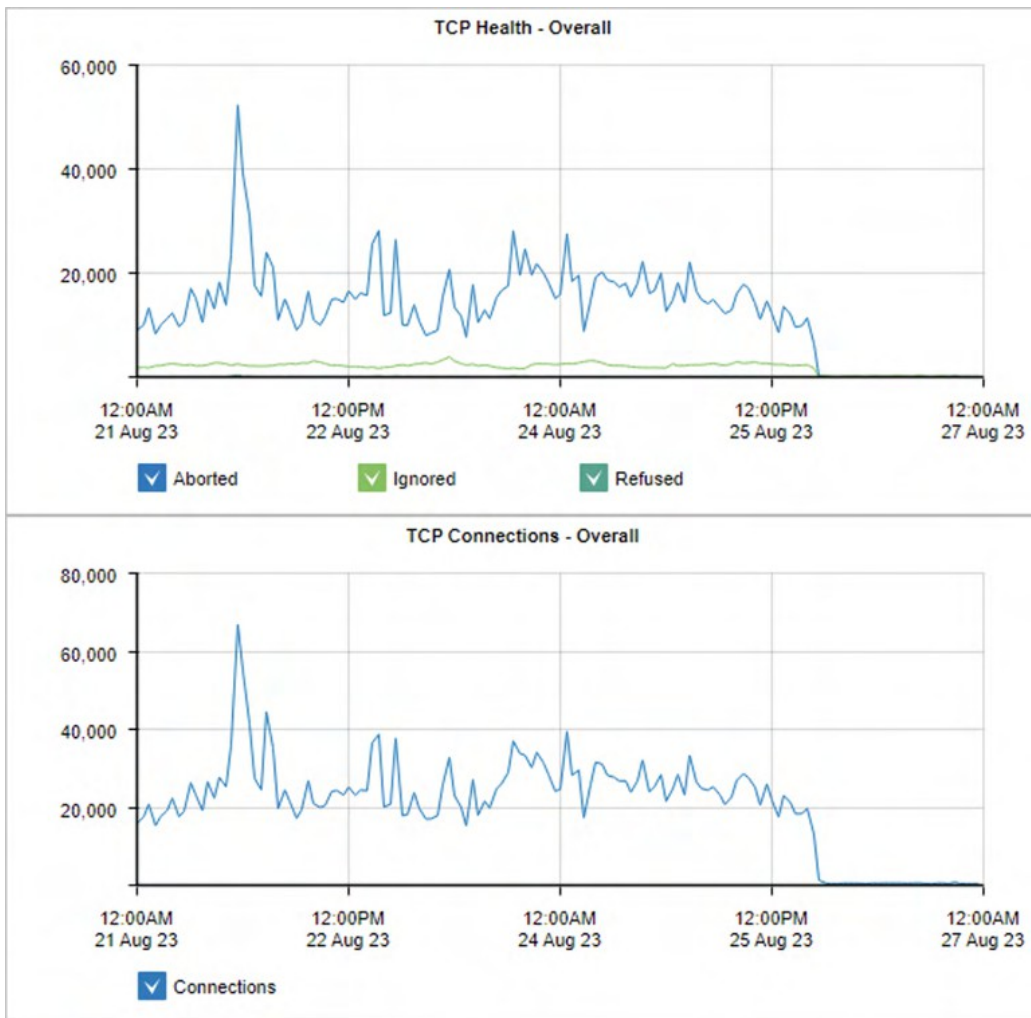


Bild 99: Der TCP-Gesundheitsbericht zeigt Daten über Verbindungen im Zeitverlauf an.

Die ungesündesten Anwendungen oder Hosts sind in der Tabelle unter den Diagrammen aufgeführt. Die Tabelle zeigt die Anzahl der Verbindungen, die Anzahl der abgebrochenen, ignorierten und verweigerten Verbindungen. Sie können auf den Namen der Anwendung oder des Hosts klicken, um die TCP Health-Details und ein Diagramm für dieses Element anzuzeigen.

Top 30 Applications				
	Connections	Aborted	Ignored	Refused
RDP	1745403	1460388	4148	0
CIFS	604672	211716	158285	1601
HTTP	191837	131887	3860	74
SSH	48665	6164	9878	954
HTTPS	167379	10847	1626	0
Telnet	24782	0	11316	4
VNC	13731	5	6031	0
HTTP-ALT	9572	41	5445	0
GFI AppManager	54639	4608	0	0
SMTP	5508	146	1839	5
Microsoft Services	3410	1032	0	0
SSL	6917	775	0	0
Cloudflare	483	415	0	0
Windows Store	1413	325	0	0
Office 365	470	265	0	0
CBT	292	0	250	0
FTP	306	0	242	0
MySQL	282	0	240	0
MS-SQL	249	0	215	0

Bild 100: Der TCP-Gesundheitsbericht zeigt die Anwendungen mit den meisten Verbindungen an.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Service Levels> TCPHealth.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Verwendung von interaktiven Zeitdiagrammen](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

3.2.5 Überwachung von Anwendungen

In diesem Abschnitt finden Sie Informationen zu verschiedenen Berichten, die sich mit der Leistung Ihrer Anwendungsgruppen, einzelnen Anwendungen, nicht klassifizierten Anwendungen und URLs befassen.

Überwachung der Anwendungsleistung im Netz

Die Analyse der Leistung von Netzwerkanwendungen ist eine häufige Aufgabe für Netzwerkadministratoren, da jedes Unternehmen auf diese Anwendungen angewiesen ist, um seine Geschäfte abzuwickeln. Allzu oft werden die Ursachen für eine schlechte Anwendungsleistung missverstanden. Und wenn die Grundursache unbekannt ist oder falsch diagnostiziert wird, beinhalten die Lösungen in der Regel teure Upgrades zur Erhöhung und Verbesserung der Netzwerkkapazität.

Die GFI ClearView Appliance wurde entwickelt, um Netzwerkprobleme zu erkennen, sie anzuzeigen und die Ursachen zu beseitigen. So können Sie die vorhandene Netzwerk-Hardware und -Kapazität voll ausschöpfen und nur bei Bedarf in zusätzliche Hardware investieren.

GFI ClearView Appliances überwacht und sammelt verschiedene Eigenschaften von TCP-Flüssen einer Anwendung und wandelt sie in Metriken um. Diese Metriken werden mit einem festgelegten Schwellenwert verglichen und mit einer Punktzahl zwischen eins und zehn bewertet, die als Application Performance Score (APS) bezeichnet wird. Die Appliance überwacht auch einzelne Metrikerwerte innerhalb von TCP-Flüssen für eine bestimmte Anwendung, die so genannten Application Performance Metrics (APM).

Auf diese Weise können IT-Abteilungen mit Hilfe des Application Performance Score (APS) feststellen, was gut läuft und was nicht. APS und APM haben Schwellenwerte, die akzeptable Leistungsniveaus für die Anwendungen festlegen. Wenn die metrischen Werte den konfigurierten Schwellenwert überschreiten, werden Benachrichtigungen an die entsprechenden Benutzer gesendet, damit diese das Problem überprüfen und die erforderlichen Änderungen vornehmen können, damit die Anwendungen innerhalb des Schwellenwerts arbeiten.

Berichte über die Anwendungsleistung können leicht an die Geschäftsleitung und an die Benutzer weitergegeben werden, um die Leistung der Anwendungen zu erläutern. Die Berichte können auch dazu verwendet werden, Probleme im Netzwerk zu diagnostizieren und zu ermitteln. Für jeden APS-Score können die Ergebnisse für Metriken den spezifischen Bereich innerhalb des Netzwerks identifizieren, der die Leistung der Anwendung beeinträchtigt, z. B. Serververzögerungen, Netzwerkverzögerungen oder Jitter. Dies erleichtert die Behebung von Netzwerkproblemen und die Wiederherstellung der optimalen Leistung der Anwendung.

Überwachung von Anwendungsgruppen Verkehr

Der Bericht Verkehrsanalyse Anwendungsgruppen zeigt die wichtigsten Anwendungsgruppen nach Datenvolumen für einen ausgewählten Zeitraum an. Eingehender und ausgehender Datenverkehr werden separat angezeigt.

Dieser Bericht beantwortet Fragen wie:

- » Welche Anwendungsgruppen können mein Netzwerk überlasten?
- » Entspricht der Anteil des Verkehrs für eine bestimmte Anwendungsgruppe meinen Erwartungen?

Anhand dieser Informationen können Sie feststellen, ob Sie Richtlinien zur Kontrolle oder zum Schutz von Anwendungsgruppen mit hohem Datenvolumen erstellen müssen.

Sie können die Anwendungsgruppe aufschlüsseln, indem Sie in den Tabellen unter den Diagrammen auf den Namen der Anwendungsgruppe klicken. Daraufhin wird der [Hosts-Bericht](#) angezeigt, der die Hosts der ausgewählten Anwendungsgruppe auflistet. Sie können dann eine bestimmte Anwendung aufschlüsseln, um die Hosts zu sehen, die diese Anwendung verwenden.

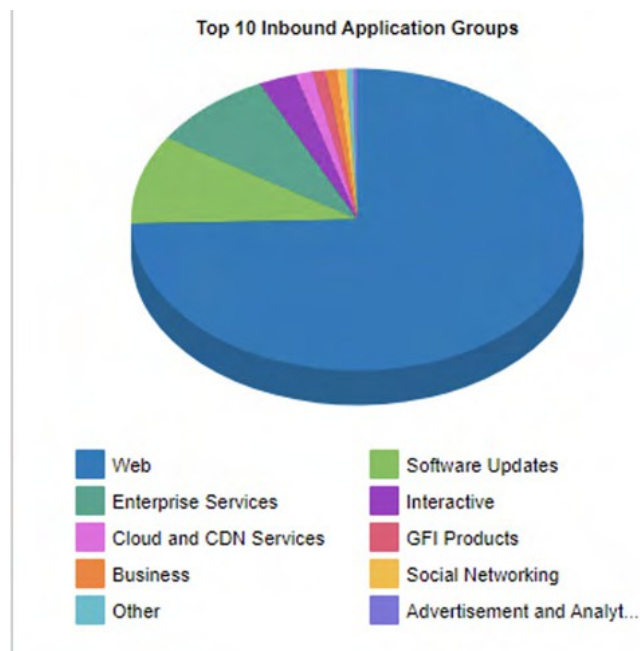


Bild 101: Der Bericht Anwendungsgruppen zeigt die 10 wichtigsten eingehenden Anwendungsgruppen an.

Die Tabellen am unteren Ende des Berichts zeigen für jede der wichtigsten Anwendungsgruppen die Gesamtdatenmenge sowie die maximalen und durchschnittlichen Durchsatzraten, die Anzahl der Pakete und die Anzahl der Flows für den ausgewählten Zeitraum. Weitere Netzwerkmetriken, wie z. B. Round-Trip-Time (RTT), Netzwerk- und Serververzögerungen und TCP-Effizienz, können durch Klicken auf den Link **Details anzeigen** in den Tabellen angezeigt werden.

Top 30 Inbound Application Groups					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
Web	2307969	2800.194	8.85	21119.92	366
Software Updates	269328	357.651	116.60	16796.22	185
Enterprise Services	419497	329.689	6.48	13482.10	473
Interactive	828509	101.830	0.23	3.93	10
Cloud and CDN Services	31258	44.349	516.71	969.05	10
GFI Products	83625	36.067	0.85	8.27	10
Business	36042	30.455	9.57	8049.89	44
Social Networking	119660	24.415	0.80	31.21	21
Other	241656	17.887	0.25	10.31	1900
Advertisement and Analytic Services	78661	12.907	0.53	7.72	27
File Services	16005	4.519	0.31	7.95	7
Games	1802	2.547	356.03	451.32	6
Organizers	5044	2.238	3.15	22.26	2
Conference	1560	0.990	3.58	7.77	17
Voice	1390	0.609	4.02	20.40	12
Device Security	325	0.153	2.07	6.19	13

Bild 102: Der Bericht Anwendungsgruppen zeigt das Verkehrsaufkommen der wichtigsten Anwendungsgruppen an.

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Anwendungen> Anwendungsgruppen.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Sie können die in einer Anwendungsgruppe enthaltenen Anwendungsobjekte anpassen. Weitere Informationen finden Sie unter [Hinzufügen und Aktualisieren von Anwendungsgruppenobjekten](#).

Um mit den tortenbasierten Berichten zu interagieren, können Sie den Mauszeiger über die Tortenscheiben bewegen, um die übertragene Datenmenge sowie den prozentualen Anteil der Torte anzuzeigen. Beachten Sie, dass der Kuchen nur die obersten Elemente anzeigt, so dass der Anteil relativ zu den obersten Elementen ist - nicht relativ zum gesamten Datenverkehr durch die Appliance. Das heißt, wenn ein Keil 50 % des Datenverkehrs anzeigt, bedeutet das, dass es sich um 50 % der Top-Elemente handelt, nicht um 50 % des gesamten Datenverkehrs durch die Appliance.

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).

» Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter

[Aufschlüsseln der Daten](#). » Um zu verstehen, wie man den Bericht druckt oder plant, siehe [Drucken und Planen Berichte](#).

Anzeigen einer Netzwerkzusammenfassung der Anwendungsgruppen

Jede Tabelle zeigt die wichtigsten Anwendungsgruppen zusammen mit der Anzahl der Pakete, der Anzahl der übertragenen Datenströme und der Durchsatzstatistik.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Monitor > Anwendungsgruppen**.
6. Klicken Sie auf **Details anzeigen**, um die Statistiken zu Round Trip Time, Normalized Delays, Transaction Delays und Efficiency für jede Anwendungsgruppe anzuzeigen.

Top 30 Inbound Application Groups													
Name	Packets	Data (MB)	Throughput (kbps)		Flows	RTT (ms)	Normalized Delays (ms/kb)			Transaction Delays (ms)			Efficiency (%)
			Average	Max			Network	Server	Total	Network	Server	Total	
[-] Hide Details													
Web	2307969	2800.194	8.85	21119.92	366	107	45	53	98	119	44	163	99.98
Software Updates	269328	357.651	116.60	16796.22	185	95	71	27	98	199	24	223	99.83
Enterprise Services	419497	329.689	6.48	13482.10	473	137	367	503	870	341	51	392	99.39
Interactive	828509	101.830	0.23	3.93	10	-	-	-	-	-	-	-	100.00
Cloud and CDN Services	31258	44.349	516.71	969.05	10	100	138	39	177	305	51	356	100.00
GFI Products	83625	36.067	0.85	8.27	10	263	214	7270	7484	1145	14363	15508	99.95
Business	36042	30.455	9.57	8049.89	44	92	71	79	150	227	109	336	99.22
Social Networking	119660	24.415	0.80	31.21	21	29	294	1	295	366	2	368	99.98
Other	241656	17.887	0.25	10.31	1900	105	1915	0	1915	582	0	582	100.00
Advertisement and Analytic Services	78661	12.907	0.53	7.72	27	71	109	4	113	242	8	250	99.96
File Services	16005	4.519	0.31	7.95	7	121	3854	0	3854	2288	1	2289	99.96
Games	1802	2.547	356.03	451.32	6	160	125	14	139	555	57	612	93.43
Organizers	5044	2.238	3.15	22.26	2	150	126	0	126	386	0	386	100.00
Conference	1560	0.990	3.58	7.77	17	85	40	0	40	199	3	202	99.90
Voice	1390	0.609	4.02	20.40	12	181	121	6	127	431	24	455	99.50
Device Security	325	0.153	2.07	6.19	13	195	90	4	94	427	30	457	100.00

7. Um die Daten für einzelne Anwendungen innerhalb einer Gruppe anzuzeigen, klicken Sie auf den Namen der Anwendungsgruppe.

Anzeige des Anwendungsverkehrs volume

Der Bericht Anwendungen zeigt die wichtigsten Anwendungen nach Volumen und durchschnittlichem Durchsatz. Volumen- und Durchsatzdaten für einzelne Anwendungen können grafisch dargestellt werden, indem Sie auf das Filtersymbol für die gewünschte Anwendung in der Datentabelle unter den Diagrammen klicken. Eingehender und ausgehender LAN-Anwendungsverkehr wird separat ausgewiesen.

Um den gesamten Anwendungsverkehr anzuzeigen, fügen Sie [eine Kategorie hinzu](#), die den restlichen Anwendungsverkehr in Ihrem Netzwerk darstellt. Auf diese Weise kann der kumulative Stack im Durchsatzdiagramm gesamten Anwendungsverkehr darstellen, der durch die Appliance fließt.

Dies hilft Ihnen, die Bedeutung der wichtigsten Anwendungen im Verhältnis zur Gesamtheit zu verstehen. Zusätzlich zur gestapelten kumulativen Ansicht können Sie den Durchsatz auch als Liniendiagramm anzeigen lassen

mit einer gemeinsamen Null-Basislinie. Sie können die Anwendungsvolumina auch in Form eines Tortendiagramms anzeigen. Diese Diagramme können Fragen beantworten wie:

- Welches sind die wichtigsten Anwendungen in meinem Netzwerk?
- Sind diese Top-Anwendungen im Verhältnis zum gesamten Datenverkehr von Bedeutung?
- Wie viel Bandbreite benötigt meine FTP-Anwendung normalerweise?
- Könnte es sein, dass eine Anwendung den Datenverkehr einer anderen Anwendung drosselt?
- Scheint eine meiner Top-Anwendungen eingeschränkt zu sein?

Anhand dieser Informationen können Sie feststellen, ob Sie Richtlinien für Anwendungen mit hohem Datenvolumen und Anwendungen, die zu großen Datenvolumen-Spitzen neigen, erstellen müssen. Vielleicht möchten Sie Schutzrichtlinien für Ihre geschäftskritischen Anwendungen und Begrenzungsrichtlinien für Anwendungen mit hohem Datenvolumen erstellen nicht geschäftskritische Anwendungen wie Freizeitanwendungen.



Bild 103: Der Bericht "Anwendungen" zeigt das Verkehrsaufkommen im Zeitverlauf an.

NOTE

Average bandwidth is calculated as the total bits observed in the charting interval divided by the number of seconds in that interval. E.g. For a chart with an hour of data, the intervals are five minutes.

Wenn Sie von einem der Diagramme für virtuelle Schaltkreise, Subnetze oder Hosts in das Anwendungsdiagramm geblättert haben, wird der entsprechende virtuelle Schaltkreis, das Subnetz oder der Host in der Filterleiste unterhalb der Schaltflächenleiste angezeigt. Um die Filterung zu deaktivieren, klicken Sie auf das geschlossene "x" im Filter-Tag.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> Anwendungen> Anwendungen.

Überwachungsberichte können als PDF-Dokument exportiert, als zeitgesteuerter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und](#)

[Berichte zur Terminplanung.](#)

So filtern Sie die Daten des Berichts

Verschiedene Komponenten des Bildschirms können durch Anklicken von Schaltflächen oberhalb der Diagramme ein- und ausgeschaltet werden. Beachten Sie, dass bei der Erstellung eines PDF-Berichts über diesen Bildschirm die Umschaltzustände berücksichtigt werden. Das heißt, wenn Sie die Ausgangsdiagramme ausgeschaltet haben, werden sie im PDF-Bericht nicht angezeigt.

» **Host-Typ:** Wenn Sie den Hosts-Bericht zum ersten Mal laden, werden standardmäßig interne Hosts dargestellt. Klicken Sie auf die Schaltfläche Interne Hosts und wählen Sie dann Externe Hosts, um den Typ zu ändern. Beachten Sie, dass Sie nicht gleichzeitig interne und externe Hosts darstellen können.

» **Verkehrsart (eingehend/ausgehend):** Standardmäßig werden sowohl der eingehende als auch der ausgehende Datenverkehr grafisch dargestellt. Klicken Sie entweder auf die Option Eingehend oder Ausgehend, um die Daten auszublenden, einschließlich aller Warenkörbe und der Datentabellen unter den Diagrammen.

» **Diagrammtyp:** Schaltet die Zeitreihendiagramme ein oder aus und ermöglicht die Auswahl einer gestapelten Flächendarstellung gegenüber einer Liniendarstellung.

» **Torte:** Schaltet das farbcodierte Tortendiagramm links neben der Liste der Top-Hörer und Top-Sprecher ein oder aus.

» **Verbleibender Verkehr:** Fügen Sie die Kategorie "Verbleibender Verkehr" unter den Listen "Top-Hörer" und "Top-Sprecher" ein oder blenden Sie sie aus.

Diese Option schaltet das Vorhandensein einer Kategorie für alle verbleibenden Anwendungen zusammengenommen ein oder aus.

» **Daten-Details:** Schaltet die Datentabellen unter den Zeitreihendiagrammen ein oder aus.

» **Mauszeiger:** Bewegen Sie den Mauszeiger über das Diagramm, um den Datendurchsatz zu einem bestimmten Datum und einer bestimmten Uhrzeit anzuzeigen.

Ein- oder Ausschalten der Kategorie Restverkehr

Schalten Sie die Schaltfläche Verbleibender Verkehr in der Schaltflächenleiste ein. Wenn die Schaltfläche aktiviert ist, wird in allen Diagrammen (Durchsatz, Torte, Top-Anwendungen) eine graue Diagrammreihe angezeigt, die alle Anwendungen in Ihrem Netzwerk darstellt, die nicht explizit in den Top-Anwendungen enthalten sind. Wenn die verbleibenden Anwendungen ein wesentlich höheres Datenvolumen aufweisen als die Top-Anwendungen, können die Top-Anwendungen im Verhältnis zur Gesamtzahl unbedeutend erscheinen, so dass Sie die Kategorie "Verbleibender Verkehr" ausschalten müssen, um die relativen Unterschiede und Nutzungsmuster der Top-Anwendungen zu sehen.

Ändern des Durchsatzdiagramms in gestapelte Flächendiagramme oder Liniendiagramme

Klicken Sie auf den Pfeil nach unten neben der Dropdown-Liste oben auf der Seite und wählen Sie aus, welcher Diagrammtyp angezeigt werden soll. Das Liniendiagramm zeigt die Anwendungen im Vergleich zur gemeinsamen Null-Basislinie, so dass sie miteinander verglichen werden können und das Muster einer bestimmten Anwendung deutlicher wird. Sie können nach bestimmten Mustern suchen, z. B. nach Spitzen oder flachen Oberseiten.

Feststellen, ob eine oder mehrere Anwendungen den Datenverkehr einer anderen Anwendung behindern

Sehen Sie sich die Durchsatzdiagramme an, wenn die Kategorie "Verbleibender Verkehr" aktiviert ist. Gibt es Zeiträume, in denen der kumulative Durchsatz besonders hoch ist (im Vergleich zur Größe der von dieser Appliance verwalteten Leitung), gibt es eine oder zwei Anwendungen, die einen erheblichen Teil der Bandbreite verbrauchen. Wenn ja, könnte diese Anwendung andere Anwendungen ausbremsen und wäre ein Kandidat für eine Kontrolle. Bitte beachten Sie, dass Sie möglicherweise die Tabelle der virtuellen Schaltkreise aufrufen und die Anwendungen nach den einzelnen virtuellen Schaltkreisen filtern müssen, um festzustellen, ob eine Anwendung andere drosselt, da sich die virtuellen Schaltkreise die Bandbreite teilen und eine Anwendung möglicherweise einen virtuellen Schaltkreis überlastet, andere jedoch nicht.

Feststellen, ob eine der Top-Anwendungen auf beschränkt zu sein scheint

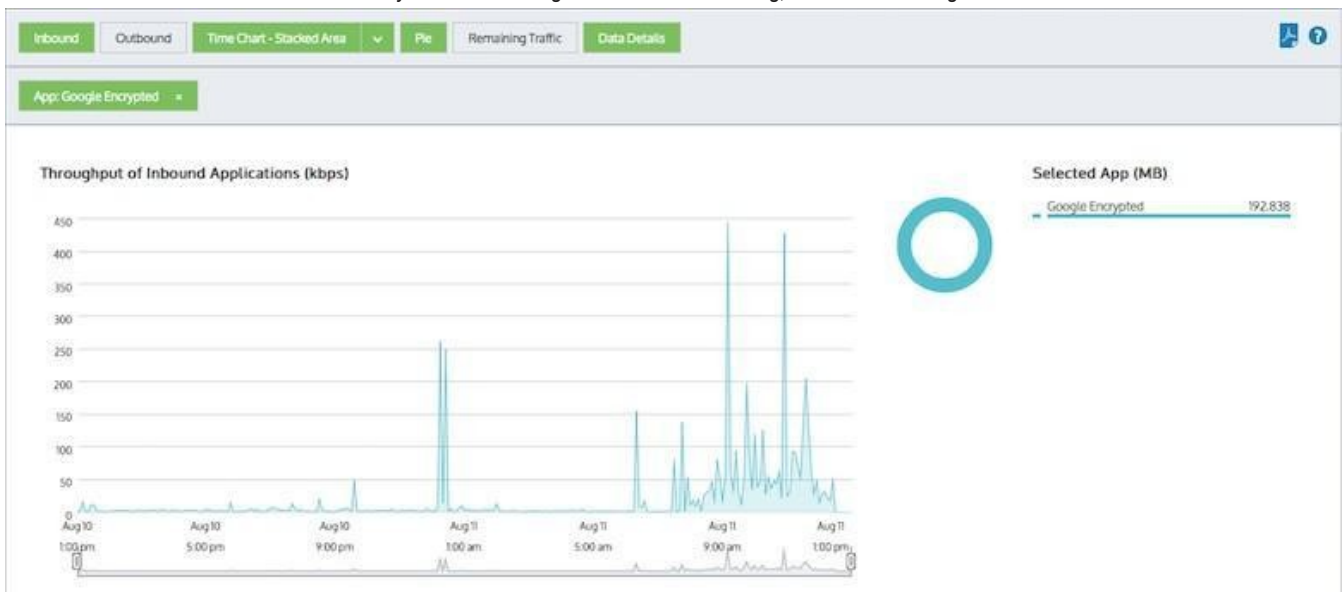
Betrachten Sie die Durchsatzdiagramme als Liniendiagramm, wobei die Kategorie "übriger Verkehr" ausgeschaltet ist. Wenn eine der Linien, die die Anwendungen darstellen, erhöhte flache Spitzen hat, kann dies bedeuten, dass die Anwendung durch die Kapazität Ihrer Leitung begrenzt wird.

Charting einer einzelnen Anwendung

In der Datentabelle hat jede Anwendung ein Filtersymbol auf der rechten Seite der Zeile. Wenn Sie auf das Filtersymbol klicken, wie unten für Google Encrypted gezeigt, wird nur die ausgewählte Anwendung in der Tabelle angezeigt.

Grooveshark	0.379 GB	0.036 Mbps	▼
Google Encrypted	0.194 GB	0.018 Mbps	▼
DropBox	0.142 GB	0.013 Mbps	▼
MPEG	0.098 GB	0.009 Mbps	▼

Screenshot 104: Klicken Sie auf das Filtersymbol neben der gewünschten Anwendung, um diese anzuzeigen.



Screenshot 105: Die Anwendungen werden so gefiltert, dass nur "Google Encrypted" angezeigt wird.

Im Filtermodus kann jedes andere Anwendungsfiltersymbol angeklickt werden, um zu ändern, welche Anwendung dargestellt werden soll.

Um diesen Filter zu entfernen und zum oberen Anwendungssatz zurückzukehren, klicken Sie auf das "x" auf dem grünen "App: Google Verschlüsselt".

So zeigen Sie mehr oder weniger Anwendungen im Diagramm der Top-Anwendungen und im Diagramm des Durchsatzes an

Die Anzahl der angezeigten Anwendungen kann über die Einstellung **Chart Items** auf der **Configuration > System > Setup > Monitoring** konfiguriert werden. Bitte beachten Sie, dass diese Konfiguration für alle Diagramme auf der Appliance gilt. Siehe [Konfiguration der Überwachung](#).

Wie interagiere ich mit den neuen Zeitreihen- und Balkendiagrammberichten ?

- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Um zu verstehen, wie die Diagramme interagieren und was die Schaltflächen bewirken, lesen Sie den Abschnitt [Beziehung zwischen Diagrammen verstehen](#).
- » Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter [Aufschlüsseln der Daten](#).
- » Um den Unterschied zwischen eingehendem und ausgehendem Datenverkehr zu verstehen, lesen Sie bitte den Abschnitt [Verkehrsrichtung verstehen](#).
- » Um zu verstehen, wie viele Datenpunkte für jede Zeitperiode angezeigt werden, lesen Sie bitte den Abschnitt [Verkehrsgranularität verstehen](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

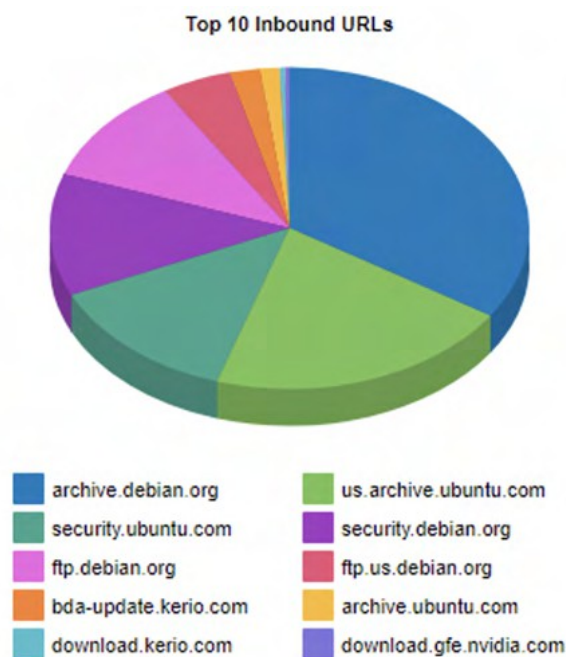
Überwachung der besuchten URLs

Der URLs-Bericht zeigt die am häufigsten besuchten URLs nach Datenvolumen für den ausgewählten Zeitraum. Der URLs-Bericht zeigt den eingehenden Verkehr getrennt vom ausgehenden Verkehr. Dieser Bericht beantwortet Fragen wie:

- » Welche Websites erzeugen den meisten Verkehr?

Anhand dieser Informationen können Sie feststellen, ob Sie Anwendungen auf der Grundlage von URLs erstellen und Richtlinien zur Kontrolle oder zum Schutz von URLs mit hohem Datenvolumen erstellen müssen.

Die URL-Namen werden als Domänen-/Hostnamen dargestellt. Klicken Sie auf den URL-Namen in den Tabellen unter den Diagrammen, um die URLs zu untersuchen. Dadurch wird der [Hosts-Bericht](#) angezeigt, der die Aufzüge auflistet, die die URL besucht haben.



Die Tabellen am unteren Ende des Berichts zeigen die Gesamtdatenmenge sowie die maximalen und durchschnittlichen Durchsatzraten, die Anzahl der Pakete und die Anzahl der Datenflüsse für den ausgewählten Zeitraum für die wichtigsten URLs. Weitere Netzwerkmetriken wie Round-Trip-Time (RTT), Netzwerk- und Serververzögerungen und TCP-Effizienz können durch Klicken auf den Link **Details anzeigen** in den Tabellen angezeigt werden.

Top 30 Inbound URLs					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
archive.debian.org	519681	726.703	999.35	2453.88	19
us.archive.ubuntu.com	307623	439.852	7530.10	26907.05	5
security.ubuntu.com	195836	282.724	5155.78	10854.01	15
security.debian.org	186271	260.657	401.20	1339.66	20
ftp.debian.org	175555	230.037	340.93	15691.08	7
ftp.us.debian.org	83036	99.271	1365.16	3134.89	16
bda-update.kerio.com	34608	43.632	620.36	3605.57	10
archive.ubuntu.com	19120	27.620	4633.90	3995.14	2
download.kerio.com	6193	7.630	77.11	1262.30	9
download.gfe.nvidia.com	5014	7.069	1976.59	1976.59	1
updates.gfi.com	44366	5.933	0.31	25.98	10
173.255.253.150	3720	4.897	73.36	1468.71	4
th.archive.ubuntu.com	3560	4.684	357.19	294.47	1
65.109.95.28:5985	18439	3.111	1.60	19.70	8
ciscobinary.openh264.org	1665	2.351	73.05	377.37	5
mirror.aarnet.edu.au	6832	1.409	10.11	8.89	3
192.168.47.2:3128	12175	1.058	0.46	0.42	3
65.109.95.28	3215	0.502	6.58	42.06	25
btensai.com	1762	0.472	12.00	45.51	11

Bild 106: Der Bericht URLs zeigt das Verkehrsaufkommen nach eingehenden URLs an.

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.

3. Klicken Sie auf **Anmelden**.

Gehen Sie zu **Monitor > Anwendungen > URLs**.

Um mit den tortenbasierten Berichten zu interagieren, können Sie den Mauszeiger über die Tortenscheiben bewegen, um die übertragene Datenmenge sowie den prozentualen Anteil der Torte anzuzeigen. Beachten Sie, dass der Kuchen nur die obersten Elemente anzeigt, so dass der Anteil relativ zu den obersten Elementen ist - nicht relativ zum gesamten Datenverkehr durch die Appliance. Das heißt, wenn ein Keil 50 % des Datenverkehrs anzeigt, bedeutet das, dass es sich um 50 % der Top-Elemente handelt, nicht um 50 % des gesamten Datenverkehrs durch die Appliance.

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).

» Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter

[Aufschlüsseln der Daten](#). » Um zu verstehen, wie man den Bericht druckt oder plant, siehe [Drucken und Planen Berichte](#).

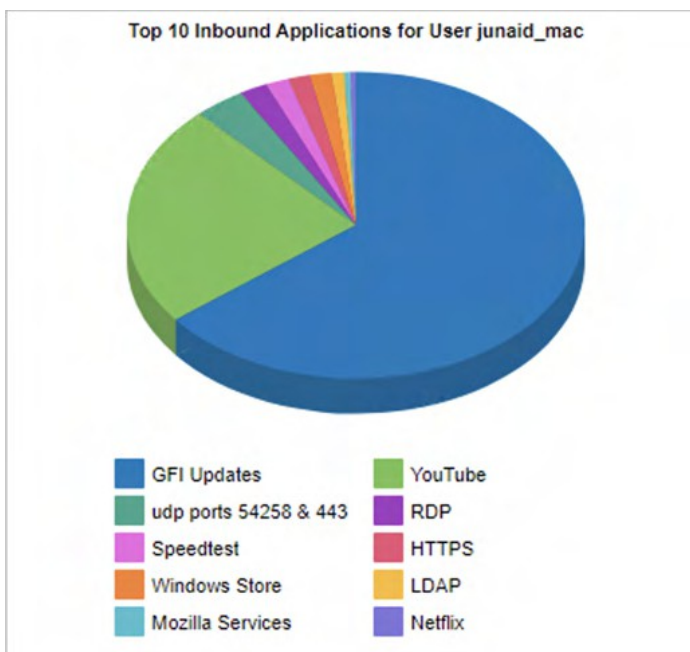
Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Aufschlüsselung der Daten der Anwendung

Der Anwendungs-Drill-in-Bericht zeigt das anwendungsspezifische Verkehrsvolumen für einen ausgewählten Zeitraum. Eingehender und ausgehender Datenverkehr werden getrennt ausgewiesen. Dieser Bericht beantwortet Fragen wie:

- » Welche Anwendungen gehören zu der Anwendungsgruppe, auf die ich geklickt habe?
- » Welche Anwendungen hat ein bestimmter Benutzer oder Host verwendet?

Sie können die Anwendung genauer untersuchen, indem Sie in den Tabellen unter den Diagrammen auf den Anwendungsnamen klicken. Daraufhin wird der [Hosts-Bericht](#) angezeigt, der die Hosts auflistet, die die



Anwendung verwendet haben.

Bild 107: Der Bericht "Anwendungen" zeigt ein Diagramm des Verkehrsaufkommens nach Anwendungen.

Die Tabellen am Ende des Berichts zeigen die Gesamtdatenmenge, die maximalen und durchschnittlichen Durchsatzraten, die Anzahl der Pakete und die Anzahl der Datenflüsse nach Anwendung für die ausgewählten

Zeitspanne. Klicken Sie auf den Link "Details anzeigen" in der Spalte "Name", um weitere Metriken wie Round-Trip-Time (RTT), Netzwerk- und Serververzögerungen und TCP-Effizienz anzuzeigen.

Name [+] Show Details	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
GFI Updates	50836419	73387.975	19769.52	287930.14	75
YouTube	21837579	26856.404	9143.18	23352.10	16
udp ports 54258 & 443	3354475	4124.434	18601.22	19430.63	1
RDP	14242685	2242.832	3.60	223.83	183
Speedtest	1608623	1846.479	12491.44	43763.08	4
HTTPS	1386843	1792.587	25.20	80946.15	14
Windows Store	1225794	1755.201	1890.08	37255.53	25
LDAP	10616942	983.243	13.29	1908.33	163
Mozilla Services	366134	512.770	18701.86	26505.08	1
Netflix	361494	445.716	1059.19	4065.24	8
Windows Updates	261051	365.015	816.53	19597.84	12
HTTP-ALT	349859	334.656	16513.53	26027.03	1
Ookla	178325	256.999	13474.14	19874.31	1
IPSEC	471441	229.887	368.72	2387.64	1
Amazon Cloud	213977	145.997	11.19	15043.25	56
Google Shared Services	95830	135.906	1781.35	80797.53	1
Telia Services	69083	99.252	2448.79	3040.53	1
Microsoft Services	60193	84.041	417.15	12199.73	9

Greifen Sie auf diesen Bericht zu, indem Sie von anderen Berichten aus einen Drill-in vornehmen, z. B. Anwendungsgruppe, Hosts, Benutzer, Konversationen, Subnetze.

Um mit den tortenbasierten Berichten zu interagieren, können Sie den Mauszeiger über die Tortenscheiben bewegen, um die übertragene Datenmenge sowie den prozentualen Anteil der Torte anzuzeigen. Beachten Sie, dass der Kuchen nur die obersten Elemente anzeigt, so dass der Anteil relativ zu den obersten Elementen ist - nicht relativ zum gesamten Datenverkehr durch die Appliance. Das heißt, wenn ein Keil 50 % des Datenverkehrs anzeigt, bedeutet das, dass es sich um 50 % der Top-Elemente handelt, nicht um 50 % des gesamten Datenverkehrs durch die Appliance.

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).

» Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter

[Aufschlüsseln der Daten](#). » Um zu verstehen, wie man den Bericht druckt oder plant, siehe [Drucken und Planen Berichte](#).

Deaktivieren von Berechnungen der Anwendungsleistung metrics

Stoppen Sie die Berechnung der Round Trip Time (RTT), der Netzwerk- und Server-Verzögerung, der Verluste und der Effizienz sowie des TCP-Zustands durch die GFI ClearView Appliance.

IMPORTANT

Application performance metrics must be enabled to calculate Application Performance Scores.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration > System > Setup** und wechseln Sie auf die Registerkarte **Überwachung**.
6. Deaktivieren Sie im Abschnitt ASAM das Kontrollkästchen **Performance Metrics**.

7. Klicken Sie auf **Änderungen übernehmen**.

8. Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf die Schaltfläche **Ungespeicherte Änderungen** und wählen Sie **Konfigurationsänderungen speichern**.

3.2.6 Überwachung des Netzes Benutzer

Der Bericht "Benutzer" zeigt die wichtigsten Benutzer nach Datenvolumen für einen ausgewählten Zeitraum. Eingehender und ausgehender Datenverkehr werden getrennt ausgewiesen. Sie können in dem Bericht interne und externe Benutzer anzeigen und Fragen beantworten wie:

- » Welche internen Nutzer sind die Top-Gesprächspartner und Top-Zuhörer? » Welche externen Nutzer sind die Top-Talker?
- » Welche externen Benutzer sind die besten Zuhörer? » Wird das Netzwerk durch einen einzelnen Benutzer blockiert?

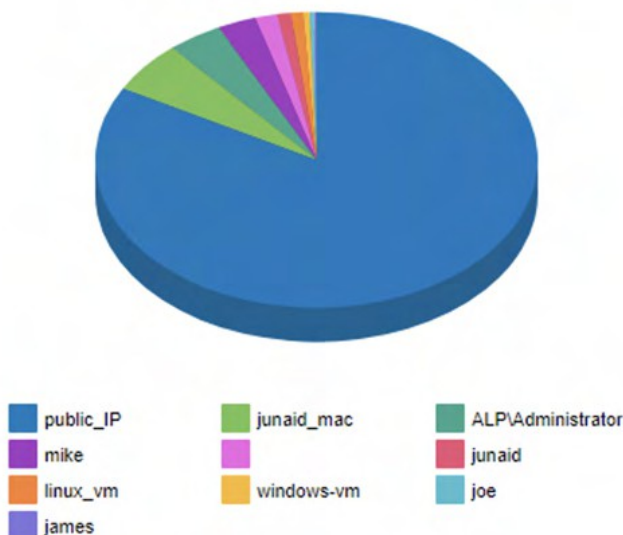
Anhand dieser Informationen können Sie feststellen, ob Sie Richtlinien für diese Benutzer mit hohem Datenaufkommen erstellen müssen. Vielleicht möchten Sie Schutzrichtlinien für Ihre wichtigen Benutzer, wie z. B. den Geschäftsführer oder die Finanzabteilung, erstellen oder Kontrollrichtlinien erstellen, um Benutzer, die das Netzwerk missbrauchen, einzuschränken.

In diesem Bericht werden die Benutzer mit IP-Adressen verknüpft. Der Netzwerkverkehr fließt von einem Host zu einem anderen, und in der Regel gilt ein Host als intern in Ihrem Netzwerk, während der andere als extern betrachtet wird.

Hosts, die in ein als intern definiertes Netzwerkobjekt fallen, gelten als intern in Ihrem Netzwerk. Hosts, die in ein als extern definiertes Netzwerkobjekt fallen, werden als extern zu Ihrem Netzwerk betrachtet. Beachten Sie, dass sich der eingehende und ausgehende Datenverkehr auf Ihr LAN bezieht - nicht auf den Host oder den Benutzer. Eingehender Datenverkehr für einen externen Benutzer bedeutet, dass ein Benutzer Daten in Ihr Netzwerk gesendet hat.

Sie können den Benutzer aufschlüsseln, indem Sie in den Tabellen unter den Diagrammen auf den Benutzernamen klicken. Dadurch wird der [Anwendungsbericht](#) für den Benutzer angezeigt, den Sie aufgeschlüsselt haben. Sie können dann den Selektor auf der Seite des Anwendungsberichts verwenden, um

Top 10 Internal Users Receiving Inbound Traffic



URLs, Konversationen oder Hosts anzuzeigen, an denen der Benutzer beteiligt war.

Bild 108: Der Bericht "Benutzer" zeigt das Verkehrsaufkommen nach Benutzern an.

Die Tabellen am unteren Ende des Berichts zeigen für jeden der Top-Benutzer die Gesamtdatenmenge sowie die maximalen und durchschnittlichen Durchsatzraten, die Anzahl der Pakete und die Anzahl der Flows für den ausgewählten Zeitraum. Weitere Netzwerkmetriken, wie z. B. Round-Trip-Time (RTT), Netzwerk- und Serververzögerungen und TCP-Effizienz, können durch Klicken auf den Link **Details anzeigen** in den Tabellen angezeigt werden.

Top 30 Internal Users Receiving Inbound Traffic					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
public IP	1830936464	1708785.866	61.16	614040.34	22993
junaid mac	108989536	116001.683	109.32	287930.14	707
ALP\Administrator	66348219	82916.300	162.48	444933.21	388
mike	47410250	58261.610	576.55	23600.24	244
'junaid khalid'	27139213	32805.959	521.63	23111.49	106
junaid	16466584	20933.012	779.30	75097.68	171
linux vm	14159570	18539.019	629.98	52805.40	908
windows-vm	8610644	9412.580	53.21	59206.54	1112
joe	5384832	6944.409	289.42	21798.73	81
james	3478144	3864.610	13.07	37407.64	648
junaid khalid	1402708	1718.210	989.93	2733.02	12
mat	1315280	1692.036	33.56	27054.58	559
rose	610331	105.613	0.25	704.59	50
junaid pc	132811	10.766	51.61	75.58	2

Bild 109: Die Tabelle im Bericht "Benutzer" zeigt die nach Benutzern aufgeschlüsselten Daten zum Verkehrsaufkommen.

Um auf diesen Bericht zuzugreifen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor> Benutzer**.

Wenn Sie nur interne oder nur externe anzeigen möchten, verwenden Sie die Option "**Zu zeigende Benutzer auswählen**" oben auf der Seite.

Um mit den tortenbasierten Berichten zu interagieren, können Sie den Mauszeiger über die Tortenscheiben bewegen, um die übertragene Datenmenge sowie den prozentualen Anteil der Torte anzuzeigen. Beachten Sie, dass der Kuchen nur die obersten Elemente anzeigt, so dass der Anteil relativ zu den obersten Elementen ist - nicht relativ zum gesamten Datenverkehr durch die Appliance. Das heißt, wenn ein Keil 50 % des Datenverkehrs anzeigt, bedeutet das, dass es sich um 50 % der Top-Elemente handelt, nicht um 50 % des gesamten Datenverkehrs durch die Appliance.

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).

» Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter

[Aufschlüsseln der Daten](#). » Um zu verstehen, wie man den Bericht druckt oder plant, siehe [Drucken und Planen Berichte](#).

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Einstellen des Zeitraums für einen Bericht

Um Berichtsdaten auf bestimmte Zeiträume zu beschränken, legen Sie den Datumsbereich fest. Die Anzeige von Berichten nach Datumsbereich ist für alle Berichte mit Ausnahme von Echtzeitberichten verfügbar.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Wählen Sie einen Bericht aus der Liste Monitor aus.
6. Wählen Sie neben dem Titel des Berichts den gewünschten Datumsbereich aus der Dropdown-Liste aus.

Range: 20/Sep/2023 12:00AM - 21/Sep/2023 12:00AM

7. Um einen benutzerdefinierten Datumsbereich anzugeben, wählen Sie in der Dropdown-Liste **Benutzerdefiniert**. Wählen Sie das Start- und Enddatum und die Uhrzeit, die in den Bericht aufgenommen werden sollen. Nachdem der Datumsbereich ausgewählt wurde, werden die

Range: -

Diagramme und Tabellen sofort aktualisiert.

[Zeitliche Granularität der gespeicherten Daten](#)

Die GFI ClearView Appliance speichert Daten für die folgenden Zeitintervalle: » 2

Jahre Daten - dieses Jahr, letztes Jahr und die letzten 12 Monate

» Daten für 2 Monate - diesen Monat, den Vormonat und die letzten 30

Tage » Daten für 2 Wochen - diese Woche, die Vorwoche und die letzten 7

Tage

» Daten von 2 Tagen - heute, gestern und die letzten 24 Stunden

» Daten von 1 Tag - diese Stunde, letzte Stunde und letzte 60 Minuten, letzte 5 Minuten

Für die Berichte "Anwendungen", "URLs", "Benutzer", "Hosts", "Konversationen" und "Subnets" die Daten unter folgender Adresse gespeichert:

» Stündliche Granularität für bis zu 2 Tage (heute, gestern, diese Stunde, vorherige Stunde)

» Tägliche Granularität für bis zu 2 Monate (diese Woche, letzte Woche, dieser Monat und letzter

Monat) » Monatliche Granularität für bis zu 2 Jahre (dieses Jahr, letztes Jahr)

Für die Schnittstelle, das Netzwerk, die Serviceebenen und das System werden die Daten gespeichert: » 10 Sekunden Granularität für 1 Tag (außer Netzwerk)

»

5-Minuten-Granularität für 2 Wochen

» 30-Minuten-Granularität für 2 Monate

» 60-Minuten-Granularität für 6 Monate

» 24-Stunden-Granularität für 2 Jahre

3.2.7 Überwachung des Host-Verkehrs volume

Der Bericht Hosts zeigt die wichtigsten Hosts nach Datenvolumen für den ausgewählten Zeitraum an. Für

Weitere Informationen finden Sie unter [Festlegen des Zeitraums für einen Bericht](#).

Der in Ihr LAN eingehende Verkehr wird getrennt vom ausgehenden Verkehr erfasst. Sie können interne und externe Hosts anzeigen, und die Daten werden für Top Listeners und Top Talkers getrennt dargestellt. Dies ermöglicht Unternehmen mit mehreren Standorten die Überwachung von Unternehmenssystemen unter Ausschluss von Internetservern.

Dieser Bericht beantwortet Fragen wie:

» Welche internen Moderatoren sind die besten Redner und die besten Zuhörer?

» Welche externen Hosts sind die Top-Talker, von denen interne Hosts Informationen abrufen? » Welche

externen Hosts sind die wichtigsten Zuhörer, an die interne Hosts Informationen senden? » Könnte ein Host

mein Netzwerk lahmlegen?

Anhand dieser Informationen können Sie feststellen, ob Sie Richtlinien für diese Hosts mit hohem Datenvolumen erstellen müssen. Vielleicht möchten Sie Schutzrichtlinien für Ihre geschäftskritischen Server erstellen oder Kontrollrichtlinien erstellen, um Hosts einzuschränken, die das Netzwerk missbrauchen.

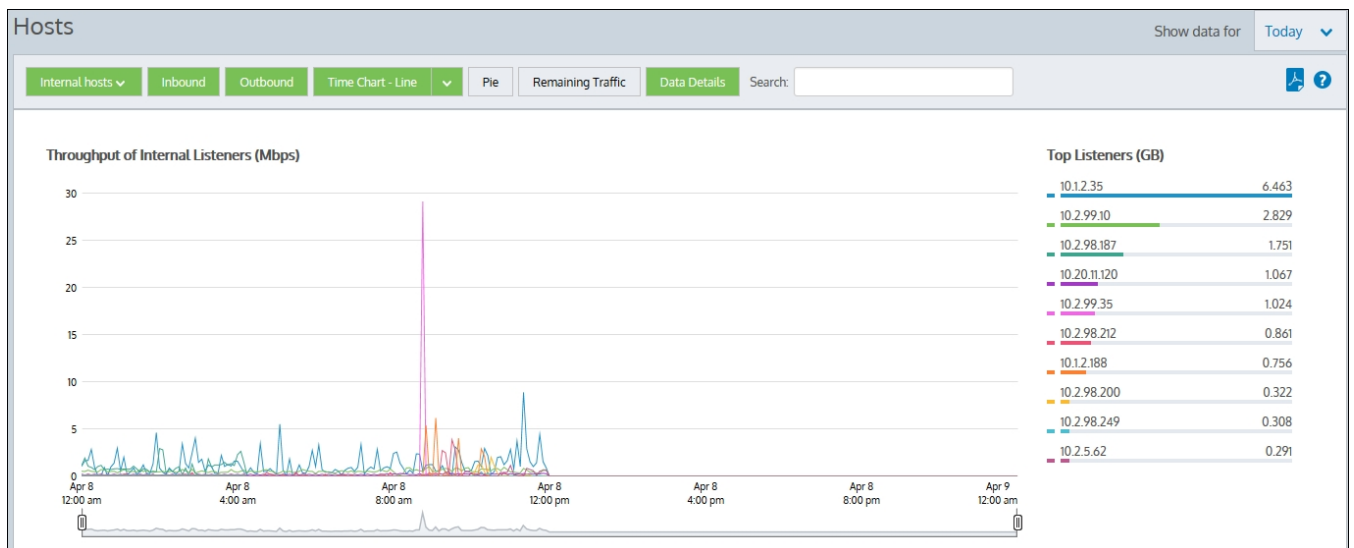


Bild 110: Der Hosts-Bericht zeigt das Verkehrsaufkommen im Zeitverlauf und die wichtigsten Hörer an.

AVERAGE BANDWIDTH

Average bandwidth is calculated as the total bits observed in the charting interval divided by the number of seconds in that interval. E.g. For a chart with an hour of data, the intervals are five minutes.

Was sind Hosts?

Hosts sind Endpunkte mit IP-Adressen in IP-Transaktionen und sind normalerweise Client-PCs oder Server. Während eines Datenflusses fließt der Verkehr von einem Host zu einem anderen. In der Regel gilt ein Host als intern in Ihrem Netz, der andere als extern:

» Hosts, die zu einem Netzwerkobjekt gehören, das als intern definiert wurde, werden als intern in Ihrem Netzwerk betrachtet.

» Hosts, die zu einem Netzwerkobjekt gehören, das als extern definiert wurde, werden als extern zu Ihrem Netzwerk betrachtet.

Eingehender und ausgehender Datenverkehr bezieht sich auf Ihr LAN, nicht auf den Host. Eingehender Datenverkehr für einen externen Host bedeutet daher, dass dieser Host Daten in Ihr Netzwerk gesendet hat.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor> Hosts**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

So filtern Sie die Daten des Berichts

Schalten Sie verschiedene Diagrammelemente ein und aus, indem Sie auf die Schaltflächen über den Diagrammen klicken. Beachten Sie, dass bei der Erstellung eines PDF-Berichts von diesem Bildschirm die Umschaltzustände berücksichtigt werden. Das heißt, wenn Sie die Ausgangsdiagramme ausgeschaltet haben, werden sie nicht in der PDF-Datei erscheinen.

» **Host-Typ:** Wenn Sie den Hosts-Bericht zum ersten Mal laden, werden standardmäßig interne Hosts dargestellt. Klicken Sie auf die Schaltfläche Interne Hosts und wählen Sie dann Externe Hosts, um den Typ zu ändern. Beachten Sie, dass Sie nicht gleichzeitig interne und externe Hosts darstellen können.

» **Verkehrsart (eingehend/ausgehend):** Standardmäßig werden sowohl der eingehende als auch der ausgehende Datenverkehr dargestellt. Klicken Sie entweder auf die Option Eingehend oder Ausgehend, um die Daten auszublenden. Bei der Anzeige von internen Hosts werden durch das Ausblenden der eingehenden Daten die Top-Listener-Daten aus den Diagrammen ausgeblendet, während durch das Ausblenden der ausgehenden Daten die Top-Talker-Daten ausgeblendet werden. Bei der Anzeige von externen Hosts ist das Gegenteil der Fall.

» **Diagrammtyp:** Das Diagramm wird zunächst als gestapelte Fläche abgebildet, aber Sie können das Format bei Bedarf in ein Liniendiagramm ändern.

» **Torte:** Schaltet das farbcodierte Tortendiagramm links neben der Liste der Top-Hörer und Top-Sprecher ein oder aus.

» **Verbleibender Verkehr:** Fügen Sie die Daten zum verbleibenden Datenverkehr unterhalb der Listen Top Listeners und Top Talkers ein oder blenden Sie sie aus. Der verbleibende Verkehr stellt den verbleibenden Anwendungsverkehr in Ihrem Netzwerk dar, und der kumulative Stapel im Durchsatzdiagramm stellt alle Hosts dar, die über Appliance kommunizieren. Wenn der verbleibende Datenverkehr ein wesentlich höheres Datenvolumen aufweist als die Top-Hosts, können die Top-Hosts im Verhältnis zur Gesamtzahl unbedeutend erscheinen, so dass Sie die Kategorie des verbleibenden Datenverkehrs ausschalten müssen, um die relativen Unterschiede und Nutzungsmuster der Top-Hosts zu sehen.

NOTE

If there are more than 100,000 hosts to display, it may take several minutes to render the screen when Remaining Traffic is enabled.

» **Daten-Details:** Schaltet die Datentabellen unter den Zeitreihendiagrammen ein oder aus.

» **Mauszeiger:** Bewegen Sie den Mauszeiger über das Diagramm, um den Datendurchsatz zu einem bestimmten Datum und einer bestimmten Uhrzeit anzuzeigen. Weitere Informationen finden Sie unter Diagramminteraktionen - Drill in & Data brush in der [WUI Guided Tour](#).

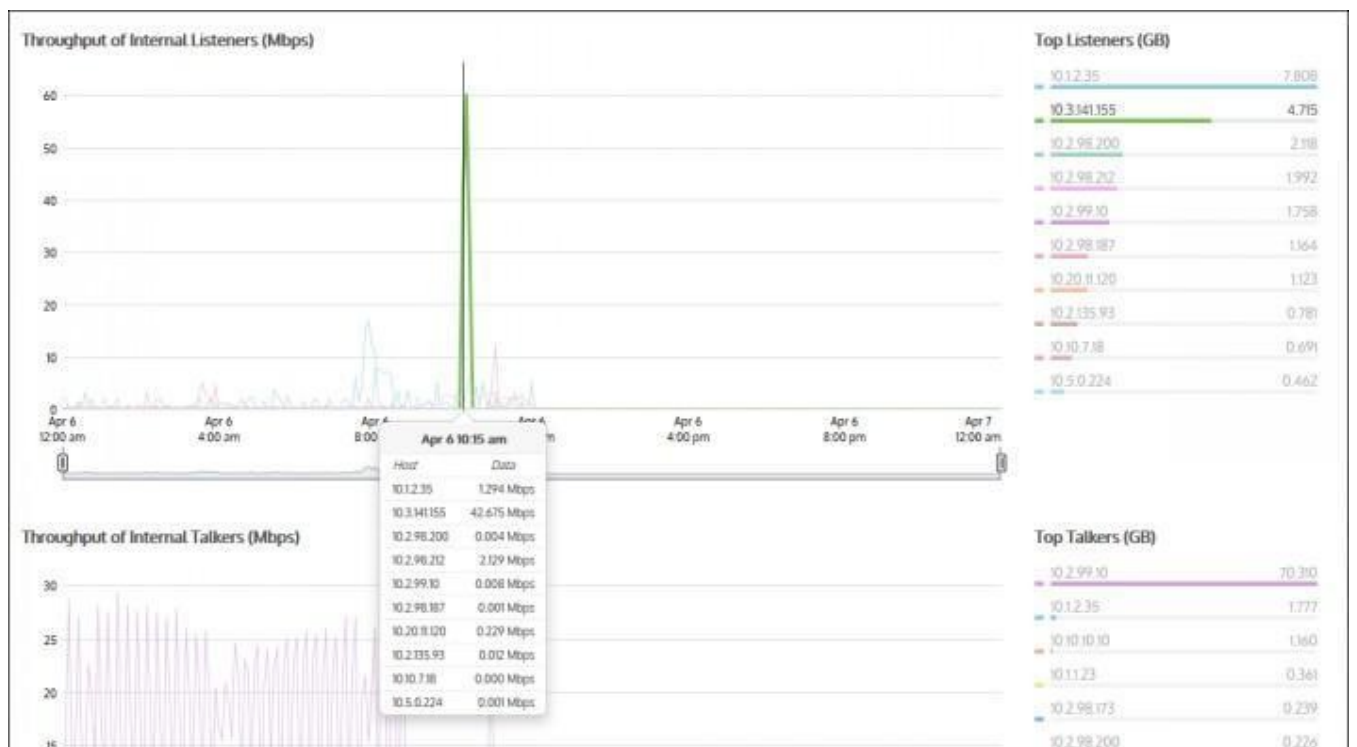


Bild 111: Der Bericht "Hosts" zeigt den Durchsatz der internen Hörer im Zeitverlauf, aufgeschlüsselt nach Top-Hörern und Sprechern.

Aufschlüsselung der Daten im Bericht

Klicken Sie auf einen Host in der Liste "Top Listeners" oder "Top Talkers" (rechts neben den Diagrammen), um die Hostdaten zu analysieren. Klicken Sie auf einen bestimmten Host, um den [Anwendungsbericht](#) für ausgewählten Host anzuzeigen. Sie können dann den Selektor auf der Seite Anwendungsbericht verwenden, um URLs oder Konversationen anzuzeigen, an denen der Host beteiligt ist.

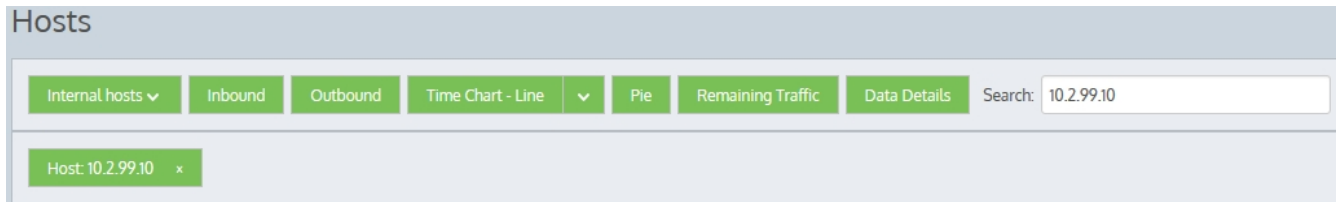
Die Tabellen am unteren Ende des Hosts-Berichts enthalten Informationen zu den wichtigsten Hörern und Sprechern sowie die IP-Adresse, das Gesamtdatenvolumen und die durchschnittlichen Durchsatzraten. Klicken Sie auf einen beliebigen Eintrag in der Tabelle, um den Anwendungsbericht für diesen speziellen Host zu öffnen.

Internal Listeners			Internal Talkers		
Name	Total Volume	Avg Throughput	Name	Total Volume	Avg Throughput
10.12.35	9.266 GB	0.921 Mbps	10.2.99.10	73.596 GB	7.317 Mbps
10.3.141.155	4.715 GB	0.469 Mbps	10.3.139.172	7.328 GB	0.729 Mbps
10.2.98.200	2.318 GB	0.230 Mbps	10.12.35	1.918 GB	0.191 Mbps
10.2.98.212	2.228 GB	0.222 Mbps	10.10.10.10	1.423 GB	0.141 Mbps
10.2.99.10	1.863 GB	0.185 Mbps	10.11.23	0.438 GB	0.044 Mbps
10.2.135.93	1.451 GB	0.144 Mbps	10.10.7.77	0.321 GB	0.032 Mbps
10.20.11.120	1.379 GB	0.137 Mbps	10.2.98.173	0.285 GB	0.028 Mbps
10.2.98.187	1.174 GB	0.117 Mbps	10.2.98.200	0.241 GB	0.024 Mbps

Bild 112: Aufschlüsselung der Hostdaten.

Suche nach einem bestimmten Host

Wenn der von Ihnen gesuchte Host nicht in der Liste der Top-Hosts aufgeführt ist, können Sie die Suchfunktion verwenden, um Daten für einen einzelnen Host finden. Geben Sie eine einzelne IP-Adresse in das Suchfeld ein, um Daten für einen bestimmten Host zu finden. Wenn Sie einen IPv6-Host eingeben, verwenden Sie nur die vollständige IPv6-Adresse. Wenn die Daten abgerufen werden, wird der einzelne Host in der Filterleiste unterhalb der Schaltflächenleiste angezeigt. Um die Filterung zu deaktivieren, klicken Sie auf das geschlossene 'x' im Filter-Tag.



Wie interagiere ich mit den neuen Zeitreihen- und Balkendiagrammberichten ?

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#). » Um zu verstehen, wie die Diagramme interagieren und was die Umschalttasten bewirken, siehe » [Zusammenhänge zwischen Diagrammen](#). Um zu verstehen, wie man in die Daten eindringt, um bestimmte gefilterte Daten zu finden,

siehe [Drilling into the Data](#).

» Um den Unterschied zwischen eingehendem und ausgehendem Datenverkehr zu verstehen, siehe » [Verkehrsrichtung verstehen](#). Um zu verstehen, wie viele Datenpunkte für jeden Zeitraum angezeigt werden, siehe » unter [Verständnis der Verkehrsgranularität](#). Um zu verstehen, wie man den Bericht druckt oder

den Bericht zu planen, siehe [Drucken und Planen von Berichten](#).

3.2.9 Überwachung von Gesprächen im Netz

Der Bericht "Konversationen" zeigt die wichtigsten Konversationen nach Datenvolumen für einen ausgewählten Zeitraum an. Der in Ihr LAN eingehende Datenverkehr wird getrennt vom ausgehenden Datenverkehr ausgewiesen.

Dieser Bericht gibt Antworten auf Fragen wie diese:

- » Was sind die wichtigsten Unterhaltungen in meinem Netzwerk?
- » Könnte es sein, dass ein Gespräch den anderen Anwendungsverkehr abwürgt?

Anhand dieser Informationen können Sie feststellen, ob Sie Richtlinien für Konversationen mit hohem Datenvolumen erstellen müssen. Möglicherweise möchten Sie für bestimmte Hosts oder Benutzer, die auf bestimmte Anwendungen zugreifen, [einschränkende Richtlinien](#) erstellen.

Eine Konversation ist definiert als der Datenverkehr zwischen zwei Host-Rechnern, die dieselbe Anwendung innerhalb eines bestimmten nutzen. Konversationen können auch als Sitzungen bezeichnet werden.

Top 10 Inbound Conversations

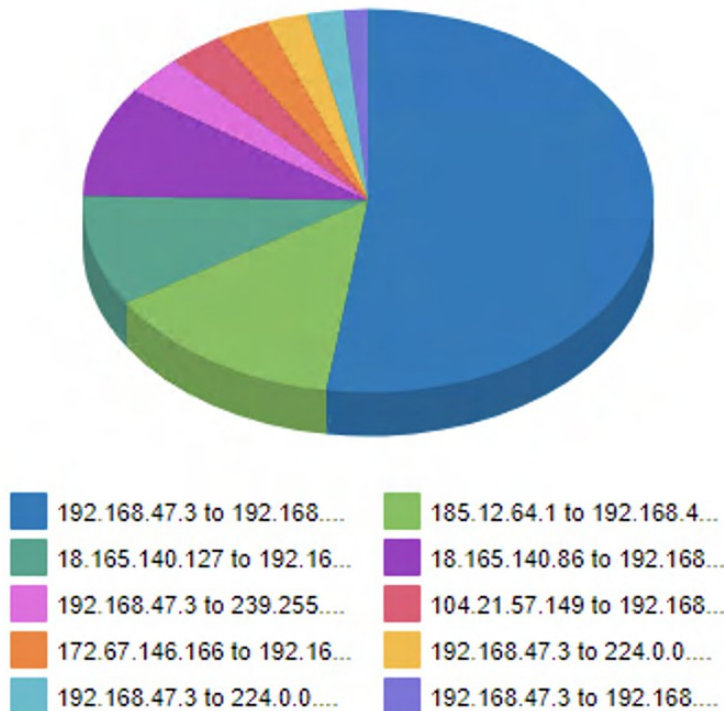


Bild 113: Der Bericht "Konversationen" zeigt das Verkehrsaufkommen nach Konversationen an.

Die Tabellen im unteren Teil des Berichts zeigen für jede der Top-Konversationen die Gesamtdatenmenge, die maximalen und durchschnittlichen Durchsatzraten, die Anzahl der Pakete und die Anzahl der Flows für den ausgewählten Zeitraum. Weitere Netzwerkmetriken, wie z. B. Round-Trip-Time (RTT), Netzwerk- und Serververzögerungen und TCP-Effizienz können durch Klicken auf den Link **Details anzeigen** in den Tabellen angezeigt werden.

Top 30 Inbound Conversations						
External Host	Internal Host	Application	Data (MB)	Throughput (kbps)		Flows
				Average	Max	
192.168.47.3	192.168.47.15	SSL	4.694	1.81	11.87	13
185.12.64.1	192.168.47.15	DNS	1.229	0.20	0.26	15
18.165.140.127	192.168.47.15	Amazon Cloud	0.839	703.72	703.72	1
18.165.140.86	192.168.47.15	Amazon Cloud	0.839	703.55	703.55	1
192.168.47.3	239.255.255.250	ssdp	0.297	0.69	0.71	13
104.21.57.149	192.168.47.15	ICMP	0.283	0.09	0.09	15
172.67.146.166	192.168.47.15	ICMP	0.268	0.09	0.09	15
192.168.47.3	224.0.0.22	igmp	0.207	0.17	0.23	15
192.168.47.3	224.0.0.251	mDNS	0.187	0.32	0.98	15
192.168.47.3	192.168.47.255	NetBIOS	0.126	0.40	0.86	15
18.165.140.86	192.168.47.15	HTTPS	0.016	0.88	1.54	13
192.168.47.3	224.0.0.252	udp ports 5355 & 52630	0.011	0.09	0.11	15
18.165.140.127	192.168.47.15	HTTPS	0.011	0.83	1.12	9
18.165.140.66	192.168.47.15	HTTPS	0.009	0.66	0.89	8
18.235.20.216	192.168.47.15	HTTPS	0.007	2.81	2.81	1
18.165.140.55	192.168.47.15	HTTPS	0.005	0.98	1.54	4
192.168.47.3	224.0.0.252	udp ports 5355 & 65535	0.004	0.08	0.11	14
192.168.47.3	224.0.0.252	udp ports 5355 & 52641	0.002	0.09	0.11	8
185.12.64.2	192.168.47.15	DNS	0.001	0.19	0.19	6

Zugang zu diesem Bericht :

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).

2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Überwachen>Gespräche**.

Um mit den tortenbasierten Berichten zu interagieren, können Sie den Mauszeiger über die Tortenscheiben bewegen, um die übertragene Datenmenge sowie den prozentualen Anteil der Torte anzuzeigen. Beachten Sie, dass der Kuchen nur die obersten Elemente anzeigt, so dass der Anteil relativ zu den obersten Elementen ist - nicht relativ zum gesamten Datenverkehr durch die Appliance. Das heißt, wenn ein Keil 50 % des Datenverkehrs anzeigt, bedeutet das, dass es sich um 50 % der Top-Elemente handelt, nicht um 50 % des gesamten Datenverkehrs durch die Appliance.

» Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).

» Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter

[Aufschlüsseln der Daten](#). » Um zu verstehen, wie man den Bericht druckt oder plant, siehe [Drucken und Planen Berichte](#).

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

3.2.9 Überwachung von Subnetzen

Ein Subnetz, eine Art von Netzwerkobjekt, kann mehrere Netzwerk-Subnetze und/oder mehrere IP-Adressen umfassen. Der Bericht "Subnets" zeigt die wichtigsten Subnetze nach Volumen und ihren durchschnittlichen Durchsatz für den ausgewählten Zeitraum.

Wenn Subnetze definiert werden, können sie als intern oder extern zu Ihrem Netzwerk angegeben werden. Eingehender und ausgehender Datenverkehr für diese Teilnetze werden getrennt ausgewiesen. Eingehender und ausgehender Datenverkehr bezieht sich auf das Subnetz, nicht auf die GFI ClearView Appliance.

Die Subnetze müssen sich nicht gegenseitig ausschließen. Der Verkehr kann in mehr als einem Teilnetz gemeldet werden. Sie können optional die drei wichtigsten Anwendungen für jedes der wichtigsten Subnetze anzeigen.

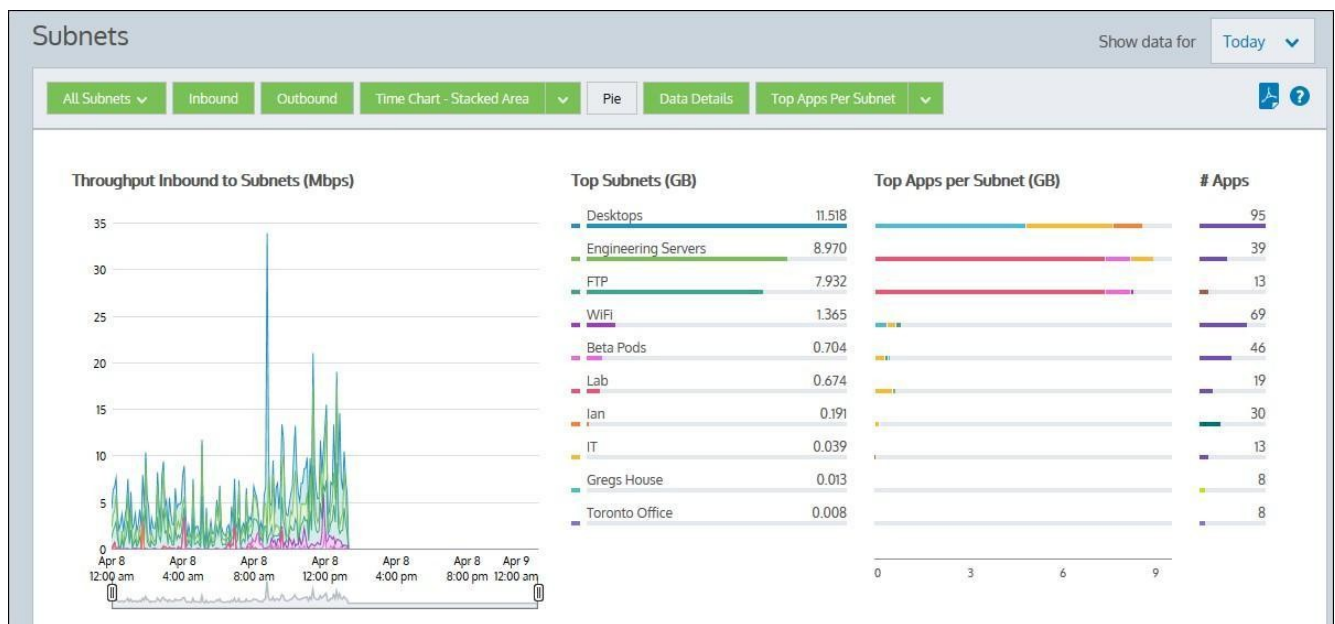
Diese Diagramme können Fragen wie diese beantworten:

» Welches sind die wichtigsten Subnetze in meinem Netz?

» Wie viel Bandbreite verbraucht mein Subnetz für die Niederlassung in New York oder für meine Finanzabteilung oder für meine PBX-Telefone normalerweise?

» Haben alle meine Zweigstellen oder Abteilungen (unterteilt nach Teilnetzen) die gleichen Top-Anwendungen?

Schalten Sie die Diagrammkomponenten ein und aus, indem Sie auf die Schaltflächen am oberen Rand des Berichts klicken. Beachten Sie, dass bei der Erstellung eines PDF-Berichts für diesen Bildschirm die Umschaltzustände berücksichtigt werden.



NOTE

Average bandwidth is calculated as the total bits observed in the charting interval divided by the number of seconds in that interval. E.g. For a chart with an hour of data, the intervals are five minutes.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor> Teilnetze**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

So konfigurieren Sie ein Teilnetz für die Überwachung von

Erstellen Sie ein Netzwerkobjekt. Weitere Informationen finden Sie unter [Hinzufügen von Netzwerkobjekten](#).

Ich sehe meine Subnetzdaten nicht

Wenn die Sammlung von Netzwerkobjekten/Subnetzstatistiken deaktiviert ist, enthält der Subnetzbericht keine Anwendungsdaten für den Zeitraum, in dem die Sammlung deaktiviert war. Weitere Informationen finden Sie unter [Hinzufügen von Netzwerkobjekten](#).

Wenn das Kontrollkästchen Teilnetzbericht bei der Definition des Teilnetzes nicht aktiviert ist, die Daten nicht in den Bericht aufgenommen. Wenn die Daten erfasst wurden, werden sie bei Aktivierung des Teilnetzberichts sofort im Diagramm angezeigt.

So ändern Sie das Durchsatzdiagramm in gestapelte Flächendiagramme oder Liniendiagramme

Drücken Sie den Abwärtspfeil neben der Schaltfläche Gestapeltes Diagramm, um Liniendiagramm zu wählen und zum Liniendiagramm zu wechseln. Drücken Sie umgekehrt den Abwärtspfeil neben der Schaltfläche Liniendiagramm, um Stapeldiagramm auszuwählen und zum gestapelten Flächendiagramm zu wechseln. Das Liniendiagramm zeigt die Subnetze im Vergleich zur gemeinsamen Null-Basislinie, so dass der Durchsatz der Subnetze miteinander verglichen werden kann und das Muster eines bestimmten Subnetzes deutlicher wird. Sie können nach bestimmten Mustern wie Spitzen oder flachen Spitzen Ausschau halten. Wenn Ihre Subnetze nicht so definiert sind, dass sie sich gegenseitig ausschließen, ist die Darstellung des Durchsatzes in einem Liniendiagramm mit einer gemeinsamen Null-Basislinie möglicherweise am sinnvollsten, da das Diagramm der kumulierten Werte einige Daten doppelt zählt und möglicherweise nicht aussagekräftig ist. Wenn Sie Ihre Teilnetze jedoch so definiert haben, dass sie sich gegenseitig ausschließen, sind gestapelte Bereichsdiagramme eine Option.

So zeigen Sie das Datenvolumen der Subnetze als Tortendiagramm an

Schalten Sie das Kreisdiagramm ein, indem Sie auf die Schaltfläche Kreis klicken. Beachten Sie, dass das Tortendiagramm wenig aussagekräftig ist, wenn Ihre Subnetze nicht so definiert sind, dass sie sich gegenseitig ausschließen, d. h. wenn Daten in mehr als einem Subnetz erfasst werden.

So zeigen Sie mehr oder weniger Subnetze im Diagramm der Top-Subnetze und im Diagramm des Durchsatzes an

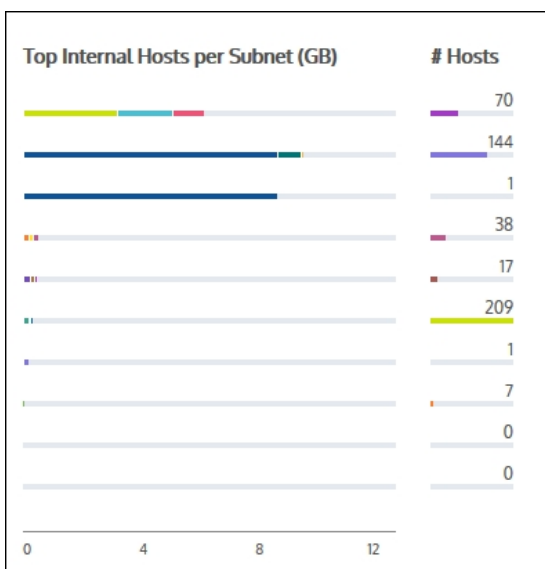
Die Anzahl der angezeigten Subnetze ist konfigurierbar. Beachten Sie, dass diese Konfiguration für alle Diagramme auf der Appliance gilt. Weitere Informationen finden Sie unter [Überwachungskonfiguration](#).

Sollten die Summen der Subnetze mit den Summen der virtuellen Schaltkreise übereinstimmen, wenn der virtuelle Schaltkreis und das Subnetz auf demselben Netzwerkobjekt basieren?

Im Allgemeinen ja. Es gibt jedoch einige Fälle, in denen die Verkehrsrichtung für Subnetze und virtuelle Leitungen unterschiedlich ist, so dass die Summen nicht übereinstimmen. Weitere Informationen finden Sie unter [Bestimmen der Verkehrsrichtung und die Auswirkungen des direktionalen Datenflusses auf Berichte](#).

Kann ich in diesem Bericht die wichtigsten internen oder externen Hosts pro Subnetz anzeigen?

Standardmäßig zeigt dieser Bericht die Top-Apps pro Subnetz an, aber Sie können die Ansicht in Top interne oder Top externe Hosts pro Subnetz ändern. Klicken Sie auf den Dropdown-Pfeil neben der Schaltfläche Top Apps pro Subnetz, um diese anderen Optionen anzuzeigen. Wenn die Anzeige aktualisiert wird, werden die Daten der Top-Hosts in einem Balkendiagramm dargestellt. Sie können über jeden Host streichen, um dessen IP-Adresse und Durchsatzdaten anzuzeigen.



Wie kann ich in diesem Bericht aufschlüsseln?

Sie können die Anwendungen für ein bestimmtes Teilnetz aufschlüsseln, indem Sie auf den Namen des Teilnetzes im Diagramm Top-Teilnetze oder auf den Namen des Teilnetzes in der Tabelle unter den Diagrammen klicken. Sie können sich auch die Hosts, Benutzer oder Konversationen für ein bestimmtes Subnetz anzeigen lassen, indem Sie auf die Links **Benutzer anzeigen**, **Konversationen anzeigen** oder **URLs anzeigen** in der Tabelle klicken. Das Diagramm mit den Anwendungen, Hosts, Benutzern, Gesprächen oder URLs wird gefiltert für das angegebene Subnetz angezeigt.

Wie interagiere ich mit den neuen Zeitreihen- und Balkendiagrammberichten ?

- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Um zu verstehen, wie die Diagramme interagieren und was die Schaltflächen bewirken, lesen Sie den Abschnitt [Die Beziehung zwischen Diagrammen verstehen](#).
- » Wie Sie die Daten aufschlüsseln können, um bestimmte gefilterte Daten zu finden, erfahren Sie unter [Aufschlüsseln der Daten](#).
- » Um den Unterschied zwischen eingehendem und ausgehendem Datenverkehr zu verstehen, lesen Sie bitte den Abschnitt [Verkehrsrichtung verstehen](#).
- » Um zu verstehen, wie viele Datenpunkte für jede Zeitperiode angezeigt werden, lesen Sie bitte den Abschnitt [Verkehrsgranularität verstehen](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Erstellung eines detaillierten Subnetz-Aktivitätsberichts

Erstellen Sie einen PDF-Bericht, der alle Netzwerkaktivitäten für Anwendungen, Konversationen, Hosts, URLs und Benutzer in den ausgewählten Subnetzen auflistet.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Bericht> PDF-Berichte**.
6. Klicken Sie auf **Neuen PDF-Bericht hinzufügen**.
7. Wählen Sie im Bereich Berichtsauswahl die Option **Detaillierte Teilnetzberichte**.
8. Wählen Sie in der Teilnetzliste ein Teilnetz aus, das dem Bericht hinzugefügt werden soll, und klicken Sie auf **Teilnetz zum Bericht hinzufügen**. Wiederholen Sie diesen Vorgang für jedes Teilnetz, das in den Bericht aufgenommen werden soll.
9. Wählen Sie im Bereich "Ausgewählte Teilnetze" den Netzwerkverkehr aus, der in den Bericht aufgenommen werden soll.
10. Geben Sie im Bereich Berichtsdetails den Namen des Berichts, den Zeitraum, den der Bericht widerspiegeln soll, und eine E-Mail-Adresse an, an die der Bericht gesendet werden kann.

NOTE

Reports can be sent to multiple recipients by separating email addresses with a comma or semi-colon.

11. Klicken Sie auf **Neuen Bericht hinzufügen**.

3.2.11 Überwachung der Systemleistung von GFI ClearView Appliance

Informieren Sie sich über die Berichte, die Sie über die Leistung Ihrer GFI ClearView Appliance informieren. Die Berichte umfassen Aspekte der Betriebsleistung wie die Anzahl der gleichzeitigen Verbindungen, die CPU-Auslastung, die CPU-Temperatur, die Speichernutzung, die Festplatten-IO und die Nutzung des Swap-Bereichs.

Überwachung von Verbindungen zu einer GFI ClearView Appliance

Der Bericht "Verbindungen" zeigt die Anzahl der gleichzeitigen Verbindungen sowie die Verbindungsaufbaurrate im Zeitverlauf für den ausgewählten Zeitraum.

Dieser Bericht beantwortet Fragen wie:

- » Gibt es eine ungewöhnliche Anzahl von Verbindungen oder ist die Verbindungsrate besonders hoch?
- » Könnte es sich um eine Art Denial-of-Service-Attacke oder ein Netzwerkproblem handeln?"

NOTE

Systems reporting unusually high spikes in the number of connections or rate of connections may be experiencing a denial of service attack or network problem.

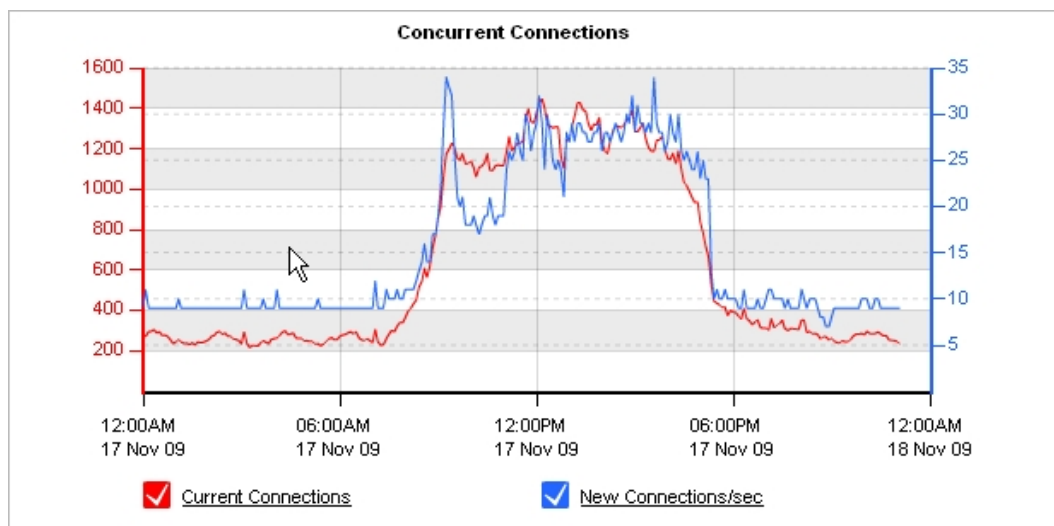


Bild 128: Das Diagramm "Gleichzeitige Verbindungen" zeigt die Verbindungsstatistiken im Zeitverlauf an.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> System > Verbindungen.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Um zu verstehen, wie man einen besseren Überblick über die Verkehrsmuster erhält und die Unordnung in der Zeit beseitigt

Diagramm, siehe [Interaktive Zeitdiagramme verwenden](#).

» Wie Sie den gewünschten Zeitbereich für ein Diagramm festlegen können, erfahren Sie unter [Einstellen des Zeitbereichs](#). » Um zu verstehen, wie Sie den drucken oder planen können, siehe [Drucken und Planen Berichte](#).

Überwachung der CPU-Auslastung der GFI ClearView Appliance

Der CPU-Auslastungsbericht zeigt, wie stark die CPU im Laufe der Zeit belastet wird. Dieser Bericht beantwortet Fragen wie z. B.:

» Sind einige der anderen Probleme, die ich mit meinem Datenverkehr habe, auf eine Überlastung des Geräts zurückzuführen?

» Ich sehe, dass die CPU der Appliance stark ausgelastet ist. Welche Verkehrsprobleme könnten dies verursachen?

Ein hoher CPU-Verbrauch kann auf eine Reihe von verarbeitungsintensiven Verkehrsmerkmalen

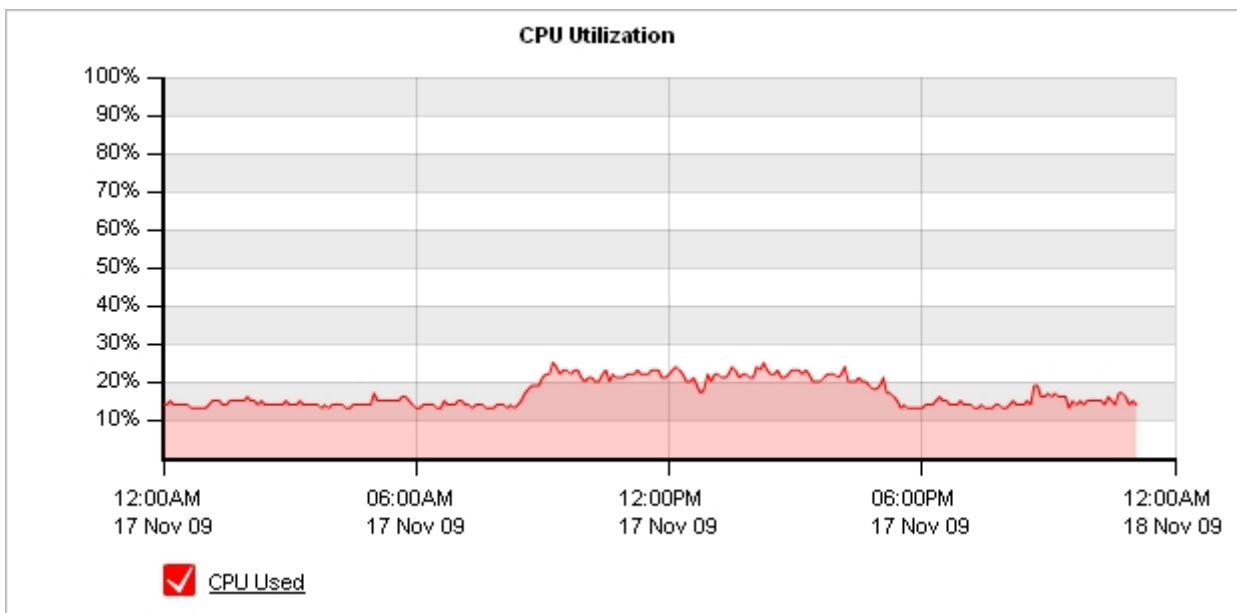
zurückzuführen sein: » Die Anzahl der neuen Verbindungen pro Sekunde ist hoch

» Die Zahl der beschleunigten Verbindungen ist hoch

» Die Appliance ist mit mehr beschleunigtem Datenverkehr konfrontiert, als sie verarbeiten kann. In diesem kann es zu Latenzzeiten kommen, wenn die Appliance die Pakete für die Beschleunigung in eine Warteschlange stellt und sie nicht schnell verarbeiten kann. Mit virtuellen Schaltkreisen können Sie die Menge des zu verarbeitenden beschleunigten Datenverkehrs begrenzen.

» Die Appliance ist mit mehr analyseintensivem Datenverkehr konfrontiert, als sie bewältigen kann. So ist beispielsweise VoIP-Verkehr aufgrund der für die Berechnung von Metriken wie rFactor, MOS, Jitter usw. erforderlichen Verarbeitung sehr rechenintensiv.

Um ein CPU-Nutzungsproblem zu diagnostizieren, vergleichen Sie für jeden Zeitraum, in dem die CPU-Nutzung hoch ist, mit dem Bericht Verbindungen, dem Bericht Beschleunigte Verbindungen, dem Bericht Reduzierung und dem Bericht VoIP-Lösung.



Screenshot 131: Die Grafik zur CPU-Auslastung zeigt, wie stark die GFI ClearView Appliance im Laufe der Zeit arbeitet.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor> System> CPU-Auslastung**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wo finde ich die anderen Berichte zur Diagnose der Ursache für die hohe CPU-Nutzung ?

- » Der Bericht über die Anzahl der neuen Verbindungen kann unter **Monitor> System > Verbindungen** abgerufen werden. Weitere [finden Sie unter Überwachen von Verbindungen zu einer GFI ClearView-Appliance](#).
- » Den Bericht über die Anzahl der beschleunigten Verbindungen finden Sie unter **Monitor> System > Beschleunigte Verbindungen**. Weitere Informationen finden Sie unter [Überwachung beschleunigter Verbindungen](#).
- » Der Bericht über die Menge des beschleunigten Datenverkehrs kann unter **Monitor> Optimierung > Reduzierung** abgerufen werden. Weitere Informationen finden Sie unter [Überwachung der Verkehrsreduzierung](#).
- » Der Bericht für den VoIP-Verkehr ist im Solution Center zu finden (**Solution Center> Solution Center anzeigen**). Weitere Informationen finden Sie unter [Verwendung des Berichts Application Performance Monitor VoIP](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Interaktive Zeitdiagramme verwenden](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Überwachung der CPU-Temperatur der GFI ClearView Appliance

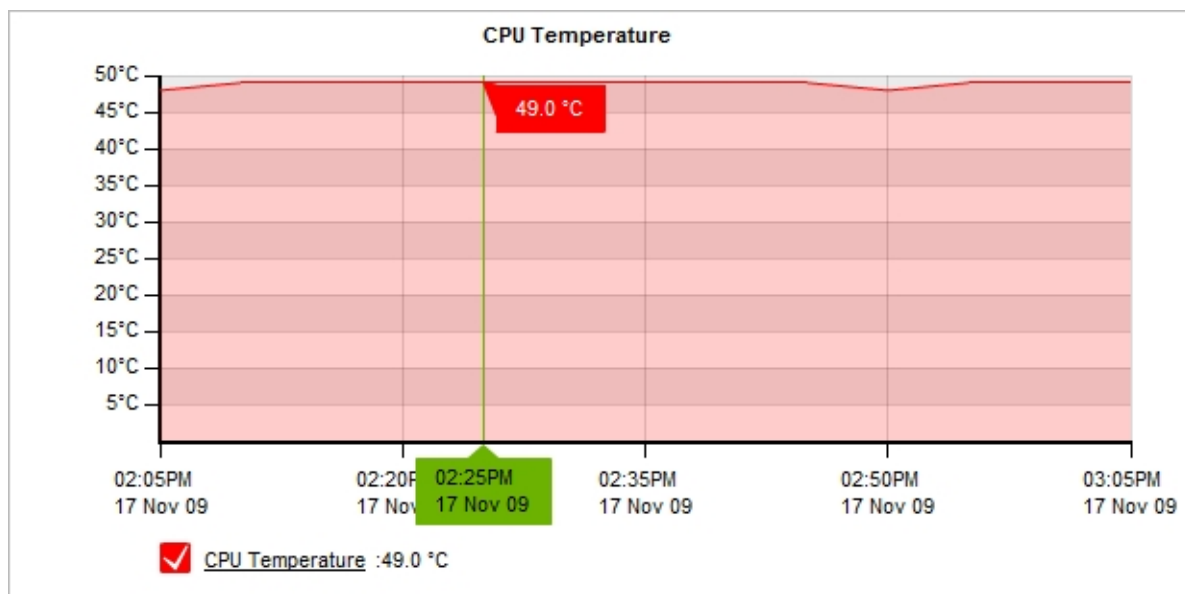
Der CPU-Temperaturbericht zeigt die Temperatur der Appliance-CPU in Grad Celsius über die Zeit für den ausgewählten Zeitraum an.

Dieser Bericht beantwortet Fragen wie:

- » Sind einige der anderen Probleme, die ich mit meinem Datenverkehr habe, auf eine Überlastung des Geräts zurückzuführen?
- » Ich sehe, dass die CPU-Temperatur der Appliance hoch ist. Liegt das an der hohen CPU-Auslastung oder ist die Umgebungstemperatur der GFI ClearView Appliance zu warm?

Sie sollten erwarten, dass die CPU-Temperatur deutlich unter 80 Grad Celsius liegt, normalerweise zwischen 35 und 50 Grad. Bei Systemen, die mit sehr hohen Temperaturen laufen, kann ein Problem auftreten und die Systemleistung beeinträchtigt werden. Sobald die Temperatur zu hoch wird (80-90 Grad), drosselt das Gerät seine Verarbeitungsgeschwindigkeit, um die Wärmeabgabe zu verringern.

Sehen Sie sich den CPU-Nutzungsbericht an, um festzustellen, ob die Temperatur mit der Verarbeitungsaktivität auf der Appliance korreliert.



Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu Monitor> System > CPU-Temperatur.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wo finde ich den Bericht zur CPU-Auslastung ?

Der Bericht zur CPU-Auslastung kann unter **Monitor> System> CPU-Auslastung** abgerufen werden. Weitere Informationen finden Sie unter [Überwachen der CPU-Auslastung der GFI ClearView Appliance](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Verwendung von interaktiven Zeitdiagrammen](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Überwachung der RAM-Nutzung von GFI ClearView Appliance

Der Bericht über die RAM-Nutzung zeigt, wie viel Speicher die Appliance im Verhältnis zum verfügbaren Speicher für den ausgewählten Zeitraum verwendet.

Dieser Bericht beantwortet Fragen wie:

- » Könnte die Leistung meines Geräts durch zu wenig Arbeitsspeicher beeinträchtigt werden?

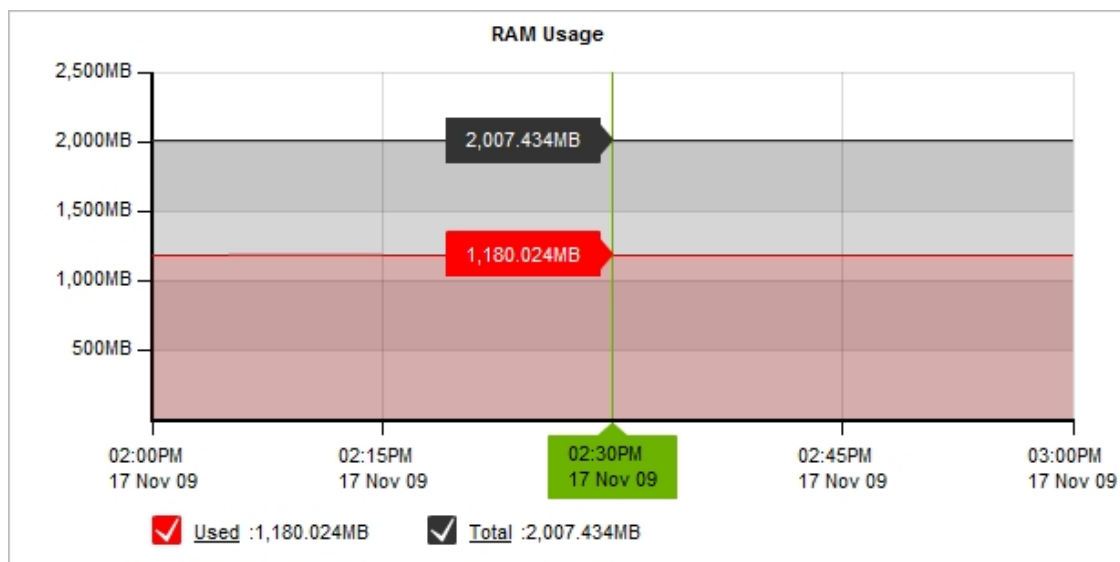


Bild 132: Das Diagramm zur RAM-Auslastung zeigt den Speicherverbrauch im Zeitverlauf an.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor> System> RAM-Auslastung**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Interaktive Zeitdiagramme verwenden](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Überwachung der GFI ClearView Appliance Disk IO

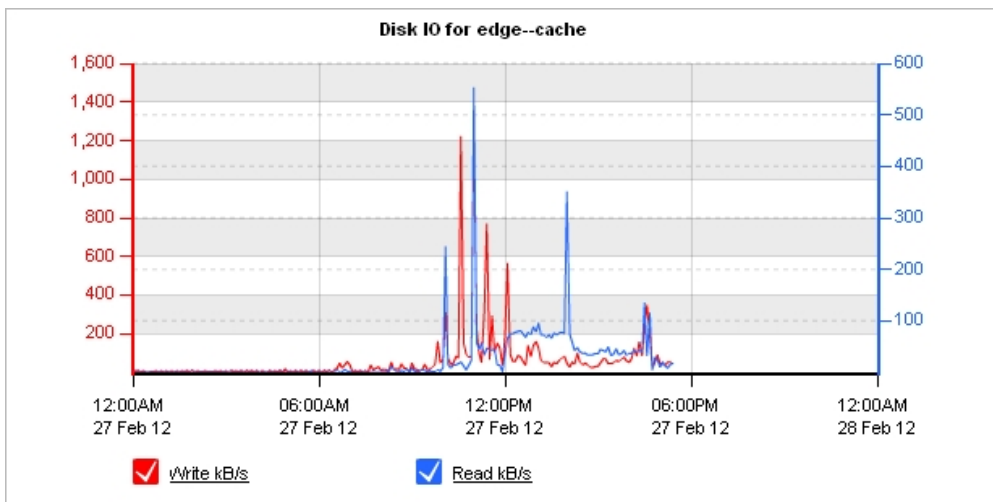
Der Bericht "Disk IO" zeigt die Lese- und Schreibnutzung der Festplatte für jeden Dienst in kB/s über einen bestimmten Zeitraum an. Dieser Bericht beantwortet Fragen wie z. B.:

- » Ist meine Festplatten-E/A-Nutzung plötzlich oder im Laufe der Zeit gestiegen? Wenn ja, welches Subsystem ist für die erhöhte Festplatten-E/A-Nutzung verantwortlich?
- » Wenn die WAN-Speicherbeschleunigung, die CIFS-Beschleunigung oder die Edge-Cache-Leistung leidet, gab es dann einen Rückgang der E/A-Last?
- » War die verringerte E/A-Last auf die erhöhte E/A-Last eines anderen Subsystems zurückzuführen?

Ich habe eine Appliance ausgetauscht und die gleiche Konfiguration geladen, und sie scheint langsamer zu sein. Wenn alle E/A-Raten niedriger aussehen, dann ist das vielleicht ein Problem mit der physischen Festplatte.

Die Festplattennutzung für jeden der folgenden Dienste kann durch Auswahl des gewünschten Dienstes in der Dienstauswahl angezeigt werden.

- » **System (vda)** - Gesamte Festplattennutzung für alle Dienste zusammen für die einzelne Festplatte; beachten Sie, dass es zwei Festplatten geben kann.
- » **monitor** - Für die Speicherung der Überwachungsdaten erforderliche Festplattennutzung
- » **swap** - Für Swapping/Paging benötigte Festplattennutzung
- » **Benutzer** - Festplattenverbrauch, der für die Speicherung der Benutzerinformationen erforderlich ist (d. h. vom AD-Konnektor gesendete Daten, manuell erfasste Benutzer und Gruppen, Details zu dynamischen Netzwerkobjekten)
- » **wan** - memory - Erforderliche Festplattennutzung für WAN-Speicherbeschleunigungstechniken
- » **edge-cache** - Erforderliche Festplattennutzung für die Speicherung von zwischengespeicherten Inhalten für Edge Cache
- » **cifs** - Erforderliche



Festplattennutzung für CIFS-Beschleunigungstechniken

Bild 133: Das Diagramm Disk IO zeigt die vom Edge-Cache genutzten IO an.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor > System > Disk IO**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

» Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Verwendung von interaktiven Zeitdiagrammen](#).

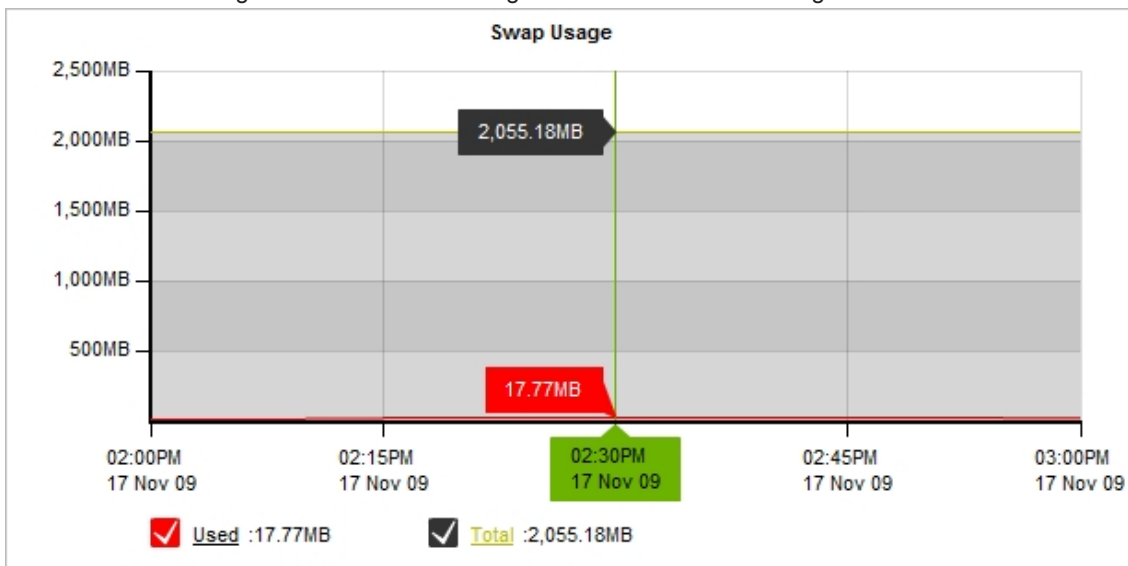
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

Überwachung der Nutzung des Swap-Speicherplatzes der GFI ClearView Appliance

Der Bericht über die Swap-Nutzung zeigt, wie viel die Appliance im ausgewählten Zeitraum auslagert.

Dieser Bericht beantwortet Fragen wie z. B.:

- » Könnte übermäßiges Auswecheln Leistung meines Geräts beeinträchtigen?



Screenshot 134: Das Diagramm Swap Usage zeigt die Auslastung des System-Swap-Bereichs im Zeitverlauf an.

Wo kann ich diesen Bericht finden?

Um den Bericht zu lesen:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Monitor > System > Swap Usage**.

Überwachungsberichte können als PDF-Dokument exportiert, als geplanter Bericht gespeichert oder direkt über die Web-UI gedruckt werden. Weitere Informationen finden Sie unter [Exportieren, Drucken und Planen von Berichten](#).

Wie kann ich mit den interaktiven Flash-Zeitdiagrammen interagieren?

- » Wie Sie sich einen besseren Überblick über die Verkehrsmuster verschaffen und die Unordnung im Zeitdiagramm beseitigen können, erfahren Sie unter [Interaktive Zeitdiagramme verwenden](#).
- » Wie Sie den gewünschten Zeitbereich für ein Diagramm einstellen können, erfahren Sie unter [Einstellen des Zeitbereichs](#).
- » Wie Sie den Bericht drucken oder planen können, erfahren Sie unter [Drucken und Planen von Berichten](#).

3.2.12 Anzeigen der Überwachungsstatistiken

Die GFI ClearView Appliance bietet verschiedene Möglichkeiten, die bei der Überwachung Ihres Netzwerks erfassten Statistiken anzuzeigen. In diesem Abschnitt finden Sie Informationen zum Zugriff auf diese Statistiken und zur Interpretation bereitgestellten Informationen.

Verstehen der Beziehungen zwischen Diagrammen und Daten

Auf den neuen Bildschirmen zur Überwachung von Zeitreihen werden ein Torten- und ein Balkendiagramm mit den wichtigsten Daten nach Volumen für den angegebenen Zeitraum und ein Zeitdiagramm mit denselben wichtigsten Zeiten angezeigt.

Es gibt einen Satz dieser Diagramme für den eingehenden Verkehr und einen für den ausgehenden Verkehr. In einigen Fällen gibt es ein weiteres Diagramm, das die drei wichtigsten Elemente eines anderen Anwendungstyps für jedes wichtigste Datenelemente zeigt. Betrachtet man beispielsweise das Diagramm der virtuellen Schaltungen, so sieht man die wichtigsten virtuellen Schaltungen als Balkendiagramm. Neben dem Balkendiagramm befindet sich ein gestapeltes horizontales Balkendiagramm, das die drei wichtigsten Anwendungen für jede der wichtigsten virtuellen Schaltungen anzeigt.



Screenshot 135: Details der virtuellen Schaltung

Wenn Sie über ein Element in einem dieser Diagramme streichen, wird das Element in allen Diagrammen hervorgehoben.

Am oberen Rand des Diagramms befinden sich Schaltflächen, mit denen Sie die verschiedenen Diagrammelemente ein- und ausschalten können.

» Schaltfläche **Eingehend** - Schaltet alle Berichte für eingehenden Verkehr ein oder aus, einschließlich aller Diagramme und der Datentabellen unterhalb der Diagramme.

» Schaltfläche **Ausgehend** - Schaltet die gesamte Berichterstattung für den ausgehenden Datenverkehr ein oder aus, einschließlich aller Diagramme und der Datentabelle unter den Diagrammen.

» Schaltfläche **Stacked Chart** oder **Line Chart** - Schaltet die Zeitreihendiagramme ein oder aus oder wählt eine andere Ansicht der Daten aus. Drücken Sie den Abwärtspfeil neben der Schaltfläche Stacked Chart, um Liniendiagramm auszuwählen und zum Liniendiagramm zu wechseln. Drücken Sie umgekehrt den Abwärtspfeil neben der Schaltfläche Liniendiagramm, um Stapeldiagramm auszuwählen und zum gestapelten Flächendiagramm zu wechseln. Im Liniendiagramm werden die virtuellen Schaltkreise im Vergleich zur gemeinsamen Null-Basislinie dargestellt, so dass der Durchsatz der virtuellen Schaltkreise miteinander verglichen werden kann und das Muster eines bestimmten virtuellen Schaltkreises deutlicher wird. Sie können nach bestimmten Mustern wie Spitzen oder flachen Spitzen suchen.

» Torten-Schaltfläche - Schaltet die Datenträger-Tortendiagramme ein oder aus.

» Schaltfläche **"Restlicher Verkehr"** - Schaltet den Rest der Daten, die nicht in den oberen virtuellen Schaltkreisen dargestellt werden, ein oder aus.

Wenn diese Option aktiviert ist, wird in allen Diagrammen (Durchsatz, Torte, Top-Virtual-Circuits) eine graue Diagrammreihe angezeigt, die alle virtuellen Verbindungen in Ihrem Netzwerk darstellt, die nicht explizit in den Top-Virtual-Circuits enthalten sind. Wenn die verbleibenden virtuellen Schaltkreise ein weitaus größeres Datenvolumen aufweisen als die Top-Virtual Circuits, können die Top-Virtual Circuits im Verhältnis zur Gesamtzahl unbedeutend erscheinen, so dass Sie

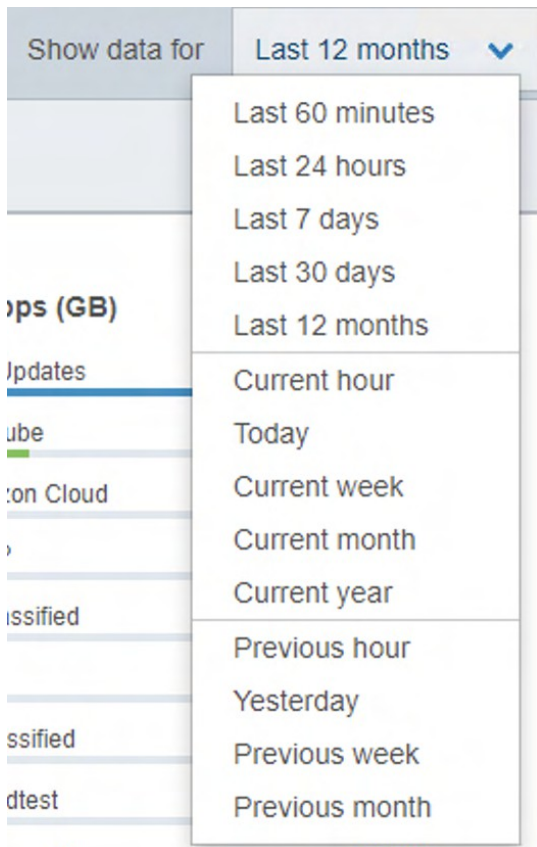
müssen Sie die verbleibende Verkehrskategorie ausschalten, um die relativen Unterschiede und der wichtigsten virtuellen Leitungen zu sehen.

» Schaltfläche **Datendetails** - Schaltet die Datentabellen unter den Diagrammen ein oder aus.

» Schaltfläche "**Top-Apps pro X**(Balkendiagrammzeile)" - Schaltet zusätzliche Diagramme ein oder aus, die die Top 3 Apps für jede Zeile im Balkendiagramm und die Anzahl der Apps für jede Zeile im Balkendiagramm anzeigen.

Zoomen auf ein Zeitintervall in den Zeitdiagrammen

Um Daten innerhalb eines Zeitraums anzuzeigen, können Sie die Dropdown-Liste **Daten anzeigen für** verwenden, um den Bereich einzugrenzen. Wenn die Liste nicht die gewünschten Details enthält, können Sie die Suche weiter eingrenzen, indem Sie innerhalb des Diagramms klicken und ziehen oder die Zoomsteuerung unterhalb des Diagramms verwenden. Mit diesen Methoden können Sie einen




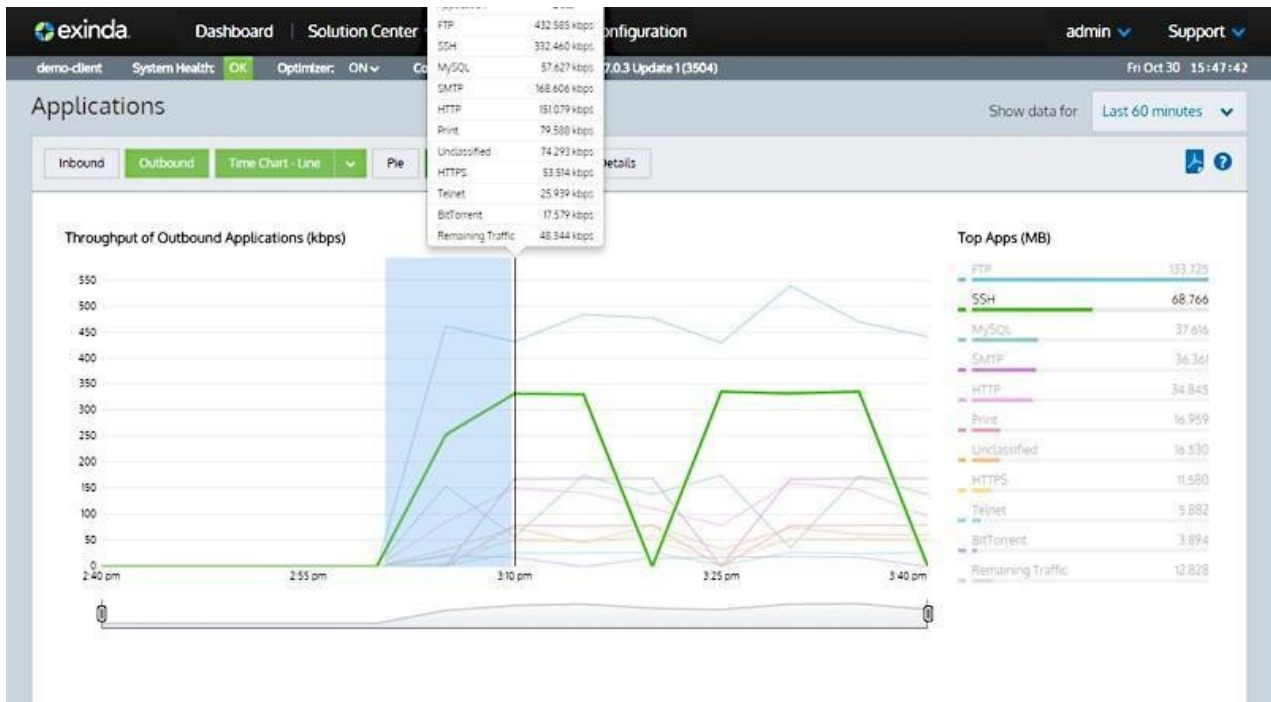
benutzerdefinierten Zeitbereich festlegen.

Screenshot 136: Die Dropdown-Liste "Daten anzeigen für"

Klicken und ziehen Sie mit der Maus auf das Diagramm, um den gewünschten Zeitbereich auszuwählen.

Ziehen Sie die Griffe auf dem Zoomregler, um den Zeitbereich zu ändern. Während Sie ziehen, wird der Bereich zwischen den Ziehpunkten schattiert. Wenn Sie loslassen, dehnt sich der schattierte Bereich auf das gesamte Diagramm aus. Um zum ursprünglichen Zeitbereich zurückzukehren, klicken Sie auf die Schaltfläche

Verkleinern , um links neben dem Zoomregler.



Sie können auch die Zoom-Steuerelemente verwenden, die unterhalb des Diagramms erscheinen. Ziehen Sie die Griffe von links und/oder rechts heran, um die gewünschten Daten zu isolieren. Das Diagramm ist dynamisch, so dass Sie die Daten sofort sehen können. Die Griffe bleiben an den Positionen, an denen Sie sie verlassen haben, so dass der Umfang des ursprünglichen Berichts ersichtlich bleibt. Wenn Sie fertig sind, klicken

Sie auf die Schaltfläche Verkleinern .

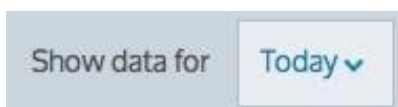


Screenshot 137: Die Zoomsteuerung

Einstellen von Zeitbereichen für Diagramme und Diagramme

Für jedes Diagramm können Sie den Zeitbereich festlegen, der im Diagramm angezeigt wird.

Wählen Sie oben rechts im Bericht den gewünschten Datumsbereich aus der Dropdown-Liste aus. Benutzerdefinierte Zeiträume werden nicht unterstützt.



Nachdem der Datumsbereich ausgewählt wurde, werden die Diagramme und Tabellen sofort aktualisiert.

Aufschlüsselung der Daten in der Tabelle

Diagramme, die Daten wie Anwendungen, Anwendungsgruppen, Benutzer, Hosts, URLs, Subnetze und virtuelle Schaltkreise anzeigen, ermöglichen es Ihnen, ein bestimmtes Element aufzuschlüsseln, um die nach diesem Element gefilterten Details zu untersuchen.

Zum Aufschlüsseln:

- » Für Diagramme klicken Sie auf ein Element in der Tabelle unter den Diagrammen. » Für Balkendiagramme klicken Sie auf ein Element im Balkendiagramm.

Sie können die folgenden Details für jeden der Anwendungstypen aufschlüsseln: »

Anwendungsgruppen > Anwendungen > Hosts

» Anwendungen > Gastgeber URLs > Gastgeber

» Benutzer> Anwendungen oder Konversationen oder URLs oder

Hosts» Hosts> Anwendungen oder Konversationen oder URLs»

Subnets > Anwendungen > Hosts

» Teilnetze> Hosts> Anwendungen oder Konversationen oder URLs»

Teilnetze> Benutzer> Anwendungen oder Hosts oder Konversationen oder

URLs» Teilnetze > Konversationen

» Teilnetze > URLs

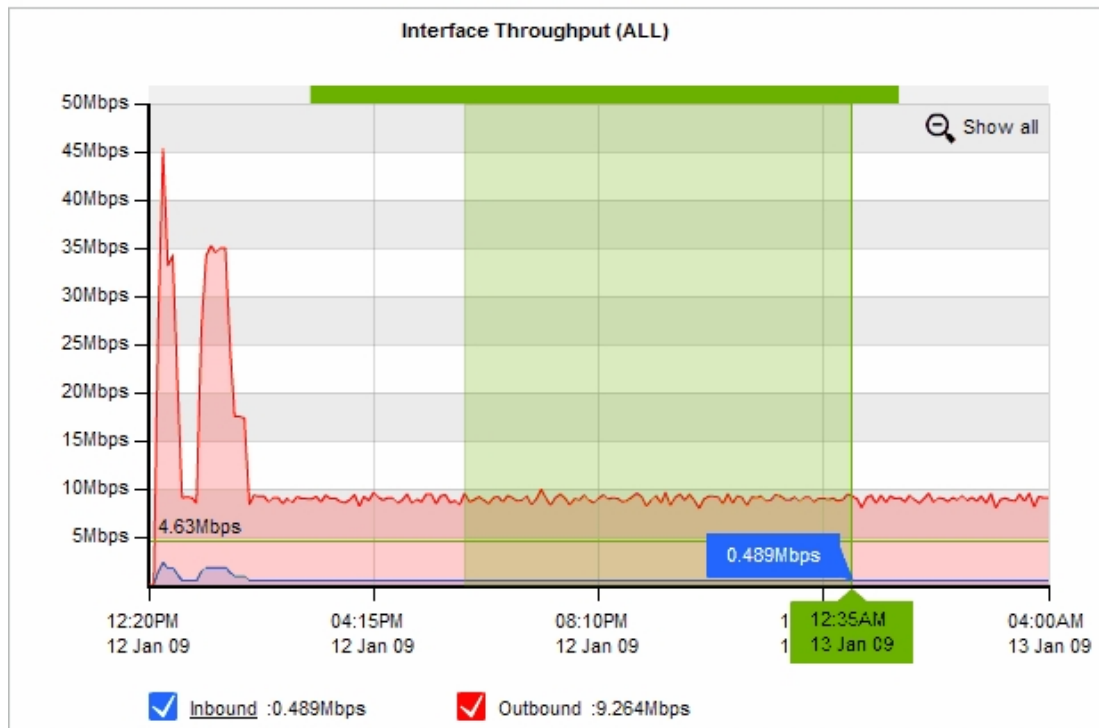
» Virtuelle Schaltkreise> Anwendungen

Wenn Sie über diese Ebenen hinausgehen, wird der Filter erweitert. Wenn Sie zum Beispiel von den Benutzern zu den Anwendungen gehen, werden die Anwendungen für diesen Benutzer gefiltert. Wenn Sie dann jedoch zu einer der Anwendungen für diesen Benutzer gehen, werden alle Hosts angezeigt, die diese Anwendung verwenden.

Verwendung interaktiver Zeitdiagramme

Wenn Sie einen besseren Überblick über ein Verkehrsmuster wünschen oder das Diagramm zu unübersichtlich ist, können Sie einen benutzerdefinierten Zeitbereich vergrößern und Zeitreihenlinien, die Sie nicht interessieren, aus den Zeitdiagrammen entfernen.

Um in einen benutzerdefinierten Zeitbereich zu zoomen, klicken und ziehen Sie mit der Maus auf das Diagramm, um den gewünschten Zeitbereich auszuwählen. Um zum ursprünglichen Zeitbereich zurückzukehren, klicken Sie auf das Lupensymbol "Alles anzeigen". Alle Daten, die unterhalb dieser interaktiven Diagramme angezeigt werden, werden automatisch mit den Daten für den ausgewählten Zeitbereich aktualisiert.



Um eine Zeitreihenlinie zu entfernen, klicken Sie auf das Häkchen in der Legende des Diagramms oder in einigen Fällen in der Tabelle unterhalb des Diagramms, um die Anzeige dieser Linie zu deaktivieren.

NOTE

The interactive feature is only applicable to Flash generated graphs. To change the graph display option navigate to **Configuration > System > Setup > Monitoring**.

Exportieren, Drucken und Planen von Berichten

Überwachungsberichte können als PDF-Dokument exportiert, als zeitgesteuerter Bericht gespeichert oder direkt über die Web-Benutzeroberfläche gedruckt werden. Die folgenden Symbole erscheinen oben rechts auf der



Benutzeroberfläche:

» **Drucken:** Wenn Sie auf das Druckersymbol klicken, wird ein neues Browserfenster geöffnet und der aktuelle Bericht für den Druck formatiert. Anschließend werden Sie aufgefordert, einen Drucker auszuwählen.

NOTE

The print option is not available from the new application, subnet, and virtual circuit monitoring pages.

» **Planen Sie PDF:** Wenn Sie auf das Zeitplan-Symbol klicken, wird die Berichtskonfiguration in den geplanten Berichten gespeichert. Sie werden aufgefordert, einen Berichtsnamen, die geplante Häufigkeit, die E-Mail-Adressen, an die der Bericht gesendet werden soll, und optional ein Passwort einzugeben, wenn Sie die PDF-Datei mit einem Passwort schützen möchten.

» **PDF:** Wenn Sie auf das PDF-Symbol klicken, wird der aktuelle Bericht als PDF-Dokument dargestellt und Sie werden aufgefordert, die PDF-Datei zu speichern oder zu öffnen, sobald sie fertig ist.

NOTE

Printed report and PDF reports may appear slightly different from the reports displayed on the Web UI.

Erstellung von PDF-Berichten

PDF-Berichte können bei Bedarf erstellt und heruntergeladen oder in regelmäßigen Abständen erstellt und per E-Mail versandt werden. Der Inhalt der PDF-Berichte kann auf zwei Arten konfiguriert werden:

» die Daten in den Monitorbildschirmen zu untersuchen
und » einen Bericht anzufordern, indem Sie auf die Seite Bericht gehen, um

die Details des PDF-Berichts konfigurieren

Die folgenden Szenarien für die Erstellung von PDF-Berichten werden unterstützt:

Untersuchen Sie die Daten in den Überwachungsbildschirmen und erstellen Sie einen Ad-hoc-PDF-Bericht über das, was » auf dem Bildschirm angezeigt wird. Untersuchen Sie die Daten in den Überwachungsbildschirmen und planen Sie einen PDF-Bericht, der

» die anhand der auf dem Bildschirm angezeigten Konfiguration und Dateien erstellt werden.

» Konfigurieren Sie einen PDF-Bericht auf der Seite Bericht .

» Konfigurieren Sie einen PDF-Bericht auf der Seite Bericht und fordern Sie eine On-Demand-Generierung des PDF-Berichts an.

Geplante Berichte können per E-Mail an eine oder mehrere E-Mail-Adressen gesendet werden, indem die E-Mail-Adressen im entsprechenden Feld durch Komma oder Semikolon getrennt werden.

Geplante Berichte können stündlich, täglich, wöchentlich oder monatlich erstellt werden. Der im Bericht enthaltene Zeitbereich entspricht der Häufigkeit, d.h. tägliche Berichte berichten über die Daten eines Tages und sind

einmal pro Tag generiert.


NOTE

- » Hourly scheduled reports are emailed to users at 22 minutes past
- » the hour. Hourly reports cannot be generated on-demand.
- » Daily scheduled PDF Reports are generated every morning at 1 a.m.

On-Demand-Berichte auf den Überwachungsseiten können jeden Zeitbereich umfassen, der Überwachungsbildschirmen zur Verfügung steht, einschließlich benutzerdefinierter Zeitbereiche.

Geplante PDF-Berichte können durch Hochladen Ihres Logos, das auf der Titelseite der Berichte angezeigt wird, gekennzeichnet werden. Berichte, die auf der Berichtsseite geplant werden, können ein oder mehrere Diagramme in der PDF-Datei enthalten, indem eine beliebige Anzahl von Diagrammen ausgewählt wird. So generieren Sie einen PDF-Bericht auf Abruf von einem Monitorbildschirm

1. Gehen Sie zu einem beliebigen Überwachungsbildschirm (mit Ausnahme des Echtzeitbildschirms) und konfigurieren Sie ihn entsprechend den verfügbaren Steuerelementen, wie z. B. der Auswahl des Datumsbereichs, der Auswahl "Intern" oder "Extern" für Hosts und Benutzerdiagramme und Subnetze, der Einsicht in die Daten durch Auswahl der Links in den Datentabellen unter den Diagrammen usw.

2. Klicken Sie auf das Adobe PDF-Symbol in der oberen rechten Ecke des Bildschirms 

3. Das System erstellt und präsentiert einen PDF-Bericht, der dem entspricht, was Sie auf dem Bildschirm sehen.

So planen Sie einen PDF-Bericht von einem Bildschirm aus

1. Gehen Sie zu einem beliebigen Überwachungsbildschirm (mit Ausnahme des Echtzeitbildschirms) und konfigurieren Sie ihn entsprechend den verfügbaren Steuerelementen, wie z. B. der Auswahl des Datumsbereichs, der Auswahl "Intern" oder "Extern" für Hosts und Benutzerdiagramme und Subnetze, der Einsicht in die Daten durch Auswahl der Links in den Datentabellen unter den Diagrammen usw.

NOTE

When you use this method to generate a report, the time range that appears on the front page of the report is updated to reflect the scheduled time range: "last 60 minutes" is updated to "last hour", "last 24 hours" is updated to "yesterday", etc. For example, the time range may be mapped to the following: 'Report Time Range 04:55PM 07 April 2015 to 05:55PM 07 April 2015'.

1. Klicken Sie auf das PDF-Symbol in der oberen rechten Ecke des Bildschirms.

2. Optional können Sie PDF-Dokumente durch die Angabe eines Kennworts schützen.

PDF Security Option	
<input checked="" type="checkbox"/>	PDF Password Protected
Enter Password:	<input type="text"/>
Re-enter Password:	<input type="text"/>

3. Geben Sie auf der Seite Berichtsdetails den Berichtsnamen, die Berichtsfrequenz und die E-Mail-Adressen an, an die der Bericht gesendet werden soll.

- **Berichtsname** - ein aussagekräftiger Name für den neuen PDF-Bericht.

Berichtshäufigkeit - Diese Option ist deaktiviert, wenn Sie in einem Überwachungsbildschirm auf die Schaltfläche Planen klicken, da das System davon ausgeht, dass Sie den Zeitbereich aus dem Überwachungsbildschirm verwenden möchten. Wenn Sie den Zeitbereich ändern möchten, klicken Sie oben auf der Seite auf den Link Neuen PDF-Bericht hinzufügen.

• **E-Mail-Adressen** - eine oder mehrere E-Mail-Adressen für geplante PDF-Berichte. E-Mail-Adressen sind optional für On-Demand-PDF-Berichte. Um mehrere E-Mail-Adressen anzugeben, trennen Sie die Adressen durch Komma oder Semikolon.

4. Das System fügt diesen geplanten Bericht zur Berichtsseite hinzu (**Monitor> Berichte planen**).

NOTE

PDF reports that were scheduled from a monitoring page cannot be edited. Ensure that you specify all the email addresses that you need it emailed to.

So planen Sie einen neuen PDF-Bericht auf der Seite Reporting

1. Gehen Sie zu Monitor> Berichte planen > PDF-Berichte.

2. Klicken Sie auf den Link **Neuen PDF-Bericht hinzufügen** am oberen Rand der Seite.

3. Wählen Sie die verschiedenen Berichte aus, die Sie in den PDF-Bericht aufnehmen möchten. Viele der über die Web-Benutzeroberfläche verfügbaren Berichte sind auch als PDF-Berichte verfügbar.

- Zusammenfassung **des Schnittstellendurchsatzes** - kann eine bestimmte Schnittstelle(n), WCCP oder alle WAN-Schnittstellen auswählen Bridge PPS (Packets per Second)
- **Zusammenfassung** - kann bestimmte Brücke(n), WCCP oder alle Brücken auswählen
- **Netzwerk Zusammenfassung**
- **Zusammenfassung der Subnetze**
- **Detaillierte** Subnetzberichte - können bestimmte Subnetze und spezifische Details für jedes Subnetz auswählen (z. B. Anwendungsdetails, Gesprächsdetails, Hostdetails, URL-Details und Benutzerdetails)
- **APS**
- **SLA**
- **TCPHealth**
- **TCPEffizienz**
- **VoIP**
- Appliance-Statistiken - Sie können bestimmte Appliance-Systemstatistiken auswählen (z. B. gleichzeitige Verbindungen, CPU-Auslastung, CPU-Temperatur, RAM-Auslastung, SWAP-Auslastung, Festplatten-IO)

4. Optional können Sie PDF-Dokumente durch Angabe eines Kennworts schützen.

PDF Security Option	
<input checked="" type="checkbox"/>	PDF Password Protected
Enter Password:	<input type="text"/>
Re-enter Password:	<input type="text"/>

5. Geben Sie auf der Seite Berichtsdetails den Berichtsnamen, die Berichtsfrequenz und die E-Mail-Adressen an


senden Sie den Bericht an.

- **Berichtsname** - ein aussagekräftiger Name für den neuen PDF-Bericht.
- **Berichtshäufigkeit** - der Zeitbereich des Berichts und die Häufigkeit, mit der er gesendet wird. Bei der täglichen Häufigkeit werden beispielsweise die Daten eines Tages dargestellt und einmal täglich per E-Mail versandt.
- **E-Mail-Adressen** - eine oder mehrere E-Mail-Adressen für geplante PDF-Berichte. E-Mail-Adressen sind optional für On-Demand-PDF-Berichte. Um mehrere E-Mail-Adressen anzugeben, trennen Sie die Adressen durch Komma oder Semikolon.

6. Das System fügt diesen geplanten Bericht zur Liste der geplanten Berichte hinzu.

So zeigen Sie einen geplanten Bericht bei Bedarf an oder bearbeiten oder löschen einen Bericht

1. Gehen Sie zu Monitor> Berichte planen > PDF-Berichte.
2. Die geplanten PDF-Berichte werden mit einer Beschreibung der im Bericht enthaltenen Diagramme und der Liste der E-Mail-Adressen, an die der Bericht gesendet wird, aufgelistet.

PDF Reports					
Name	Exported Data	Email(s)	On-Demand	Edit	Delete
Desktop_b_b (Last 60 Minutes)	Virtual Circuit Detailed (Desktop Networks): Peak vs Average Throughput Report Optimization Policy Throughput Statistics		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
hosts_yesterday (Scheduled Daily)	Custom Selection		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Test (Last 60 Minutes)	Subnet Detailed (Desktops): Applications Conversations Hosts URLs Users Virtual Circuit Detailed (Desktop Networks): Peak vs Average Throughput Report		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
test (Scheduled Daily)	Custom Selection		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
VC-report (Last 7 Days)	Virtual Circuit Detailed (Engineering Servers): Peak vs Average Throughput Report Optimization Policy Throughput Statistics		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

3. Klicken Sie auf das Adobe PDF-Symbol, um den Bericht anzuzeigen.
4. Um den Bericht bei per E-Mail zu versenden, klicken Sie auf das Mail-Symbol.
5. Um einen konfigurierten PDF-Bericht zu bearbeiten oder zu löschen, klicken Sie auf die entsprechende Schaltfläche neben dem Bericht in der Tabelle.

NOTE

PDF reports that were scheduled from a monitoring page cannot be edited. Ensure that you specify all the email addresses that you need it emailed to.

PDF reports can only be emailed on-demand if the report was configured with one or more email addresses.

So fügen Sie ein benutzerdefiniertes Logo auf Deckblatt der geplanten Berichte hinzu

1. Gehen Sie zu Monitor> Berichte planen > Benutzerdefiniertes Logo
2. Laden Sie Ihr eigenes Logo hoch.
3. Das System fügt das Logo auf dem Deckblatt jedes geplanten PDF-Berichts ein.

Custom Logo

Upload New Custom Logo:

NOTE

Files should be no more than 300px wide by 300px high and must be in PNG format with maximum file size of 3MB.

CSV Berichterstattung





Mit der CSV-Berichterstellung können Sie den Export von CSV-Rohdaten konfigurieren, die entweder bei Bedarf oder in regelmäßigen Abständen per E-Mail versandt oder heruntergeladen werden. Die exportierten Daten können durch Komma oder Semikolon getrennte E-Mail-Adressen an mehrere Empfänger gesendet werden.

NOTE

To configure a CSV Report, navigate to Report | CSV Reports on the Web UI, advanced mode.

Die CSV-Berichte sind in der Tabelle auf dieser Seite aufgeführt. CSV-Berichte können bei Bedarf erstellt und entweder per E-Mail versandt oder heruntergeladen werden, indem Sie entweder auf das ZIP-Symbol (zum Erstellen und Herunterladen) oder auf das Umschlagsymbol (zum Erstellen und Versenden per E-Mail) klicken. CSV-Berichte können nur dann per E-Mail verschickt werden, wenn der Bericht mit einer oder mehreren E-Mail-Adressen konfiguriert wurde.

Sie können einen konfigurierten CSV-Bericht auch bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben Bericht in der Tabelle klicken.

CSV Reports					
Name	Exported Data	Email(s)	On-Demand	Edit	Delete
currentweek (Current Week)	Summary Reports: flows		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
currentday (Today)	Summary Reports: flows		 	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Neue CSV-Berichte können mit Hilfe des Formulars oben auf der Seite hinzugefügt werden.

Report Details

Report Name:

Report Frequency:

Email Addresses:

[Email Addresses is Optional for On-Demand Report]

Screenshot 138: Berichtsdetails

Property	Description
Report Name	Specify a meaningful name for the new CSV Report.
Report Frequency	Specify a time range for this CSV Report. Scheduled reports can be generated Daily, Weekly or Monthly. On- demand reports can include any time range available to the Exinda appliance.
Email Addresses	Specify 1 or more email addresses for scheduled CSV Reports. Email addresses are optional for on-demand CSV Reports. To specify multiple email addresses, comma or semicolon separate the addresses.

NOTE

Daily scheduled CSV Reports are generated every morning at 1am.

Informationen über das in CSV-Berichten verwendete Schema finden Sie im SQL Access using ODBC How to Guide. Sie finden diese Funktion unter **Monitor> Berichte planen > CSVReports**.

3.3 Überwachung von Anwendungen mit dem ClearView Solution Center

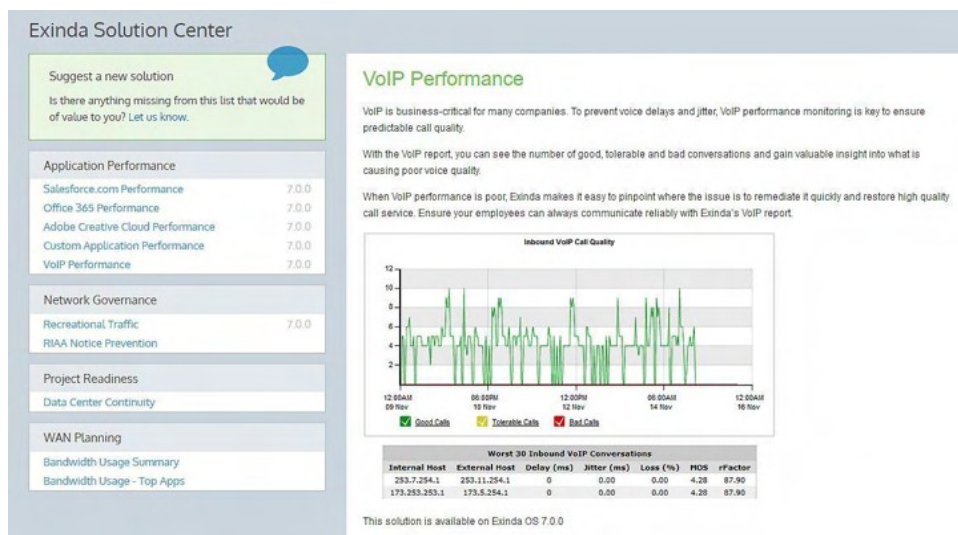
Das ClearView Solution Center bietet eine Reihe von vordefinierten Monitoren, die Sie ausführen können, um Berichte über die Netzwerkleistung für Anwendungen wie FTP, SSH, Salesforce.com, Office365 VoIP und viele andere zu erstellen.

Die erstellten Berichte beantworten Fragen wie z. B.:

- » Wie ist die Leistung von salesforce.com für Netzwerkbenutzer?
- » Wie verhalten sich kritische Anwendungen im Netzwerk? » Wie

kann ich Katastrophen im Rechenzentrum am besten abfedern?

In jeder Lösungsbeschreibung ist angegeben, welche Version von GFI ClearView OS für die Ausführung der Lösung erforderlich ist, und zwar sowohl in der Lösungsliste als auch in der jeweiligen Lösungsbeschreibung. Möglicherweise müssen Sie Ihre GFI ClearView OS-Version aktualisieren, um die gewünschten Lösungen nutzen zu können. Einige Lösungen sind möglicherweise noch nicht verfügbar und werden als "In Kürze" angezeigt.



Screenshot 139: Das GFI ClearView Solution Center

Die Leistungsmonitore sind in vier Lösungskategorien unterteilt: Anwendungsleistung, Netzwerk-Governance, Projektbereitschaft und WAN-Planung.

Zu jedem Monitor gibt es eine Beschreibung, die Sie durch Klicken auf den Link im linken Fensterbereich anzeigen können. In den Beschreibungen finden Sie Informationen zur Verwendung des Monitors sowie die für die Ausführung des Monitors erforderliche GFI ClearView OS-Version. Einige Monitore haben auch kurze Videobeschreibungen.

3.3.1 Wie Leistungsberichte funktionieren

Eine GFI ClearView-Appliance sammelt kontinuierlich Daten zum Netzwerkverkehr. Die Leistungsberichte im GFI ClearView Solution Center geben Aufschluss über diese Daten, indem sie sie auf sinnvolle Weise gruppieren und in Diagrammen, Tabellen und Schaubildern darstellen.

Der Prozess beginnt mit der Analyse des Datenverkehrs und der Berechnung der ersten Schwellenwerte, um eine Basislinie zu erstellen. Für eine Basislinie sind Daten zum Netzwerkverkehr im Umfang von einer Stunde erforderlich. Wenn für eine Anwendung während einer Baseline-Periode kein Datenverkehr beobachtet wird, wird der Prozess fortgesetzt, bis genügend Daten gesammelt wurden.

Der Baseline-Prozess darf nicht eine Stunde dauern. Wenn eine GFI ClearView Appliance den Datenverkehr für die Anwendung innerhalb der Stunde, in der der Baseline-Prozess startet, beobachtet und gespeichert hat, verwendet der Baseline-Prozess diese gespeicherten Informationen und wartet nur so lange, bis eine Stunde an Daten gesammelt wurde.

Wenn Sie beispielsweise einen Anwendungsmonitor erstellen, während noch zehn Minuten einer Stunde verbleiben, und GFI ClearView in dieser den Netzwerkverkehr für die Anwendung erfasst hat, analysiert der Baseline-Prozess die letzten fünfzig Minuten der erfassten Verkehrsdaten und vervollständigt die Baseline-Periode mit den in den verbleibenden zehn Minuten erfassten Daten.

3.3.2 Verwendung von Berichten zur Anwendungsleistung

Die Anwendungsperformance-Monitore generieren Berichte, die Informationen über die Benutzer der Anwendung, die Anwendungsperformance, den Bandbreitenverbrauch der Anwendung und die erreichte Reduzierung (falls zutreffend) anzeigen.

Lösungen für die Anwendungsleistung bieten einen vordefinierten Satz von Anwendungsmonitoren. Außer für VoIP, Anwendungsmonitore erstellen ähnliche Berichte.

Sie können einen Monitor auf dem Hauptbildschirm des GFI ClearView Solution Centers auswählen oder auf den Link **Custom Application Performance** klicken, um eine Liste von Anwendungen aufzurufen, aus der Sie wählen können.

NOTE

The report description lists the minimum version of GFI ClearView OS required to run the report. If your GFI ClearView OS does not meet or exceed the requirement, the Run button will not be available.

Ausführen eines Berichts zur Anwendungsleistung

Das GFI ClearView Solution Center listet auf dem Hauptbildschirm des Solution Centers eine Reihe von vordefinierten Berichten auf. Sie können entweder einen dieser Berichte oder einen der zahlreichen anderen Berichte ausführen, indem Sie auf "**Custom Application Performance**" klicken.

1. Gehen Sie zu Solution Center> Solution Center anzeigen.
2. Klicken Sie unter **Anwendungsleistung** auf den Namen des auszuführenden Berichts
3. Klicken Sie auf **Ausführen**. Ein Bestätigungsbildschirm wird geöffnet.
4. Klicken Sie auf **Ok**.

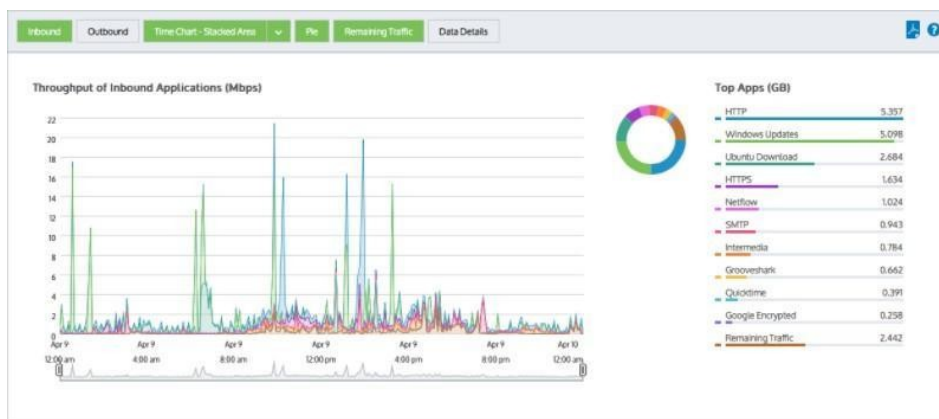
NOTE

After the initial run, you can access the report by clicking **Solution Center**, hovering over **Applications** and clicking the report name.

Verstehen der in einem Bericht zur Anwendungsleistung angezeigten Daten

Ein Bericht über die Anwendungsleistung zeigt die Netzwerkbenutzererfahrung einer Anwendung anhand einer Reihe von Diagrammen, Tabellen und Schaubildern.

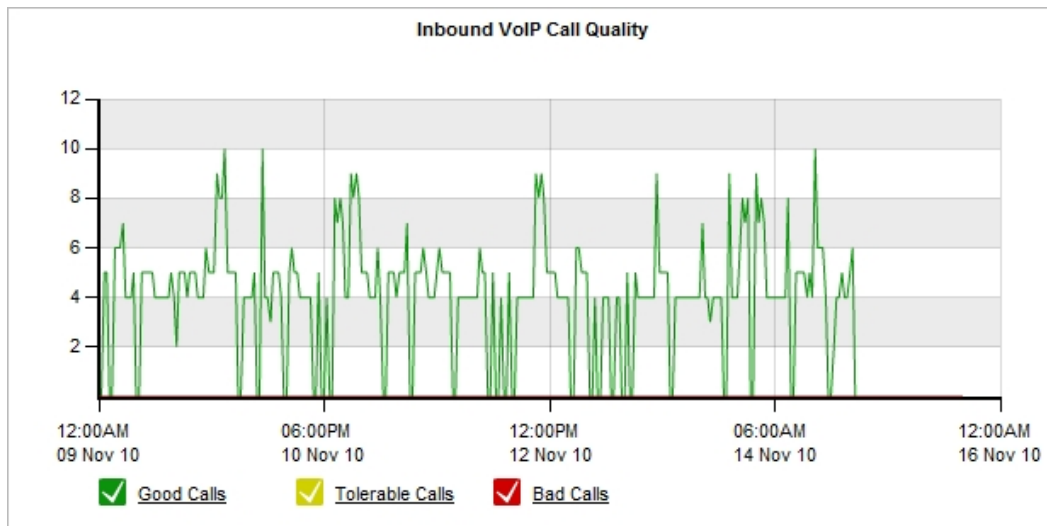
Die Diagramme zur eingehenden und ausgehenden Bandbreite zeigen, wie viel Bandbreite eine Anwendung verbraucht. Die Diagrammlinien zeigen in der Regel Spitzen anstelle von erhöhten flachen Spitzen. Flache Spitzen können auf Verkehrseinschränkungen durch [Richtlinien](#) hinweisen.



Screenshot 142: Balkendiagramme für Benutzer und Hosts.

Balkendiagramme für Benutzer und Moderatoren zeigen das Bandbreitenvolumen nach den wichtigsten Zuhörern und Sprechern an. Multi-User-Anwendungen zeigen in der Regel eine gleichmäßige Verteilung auf die Top-Benutzer oder Hosts. Wenn ein Benutzer oder Host mehr Bandbreitenvolumen anzeigt als andere Benutzer und Hosts, kann es sinnvoll sein, diese Situation zu untersuchen.

Sie können wählen, ob interne Endpunkte (LAN-Seite einer GFI ClearView-Appliance), externe Endpunkte (WAN-Seite einer GFI ClearView-Appliance), nur Benutzer oder nur Hosts angezeigt werden sollen. Weitere Informationen finden Sie unter [Überwachung der Echtzeit-Anwendungsreaktion](#).



Worst 30 Inbound VoIP Conversations						
Internal Host	External Host	Delay (ms)	Jitter (ms)	Loss (%)	MOS	rFactor
253.7.254.1	253.11.254.1	0	0.00	0.00	4.28	87.90
173.253.253.1	173.5.254.1	0	0.00	0.00	4.28	87.90

Bild 143: Die Tabelle mit den Anwendungsleistungswerten und -metriken.

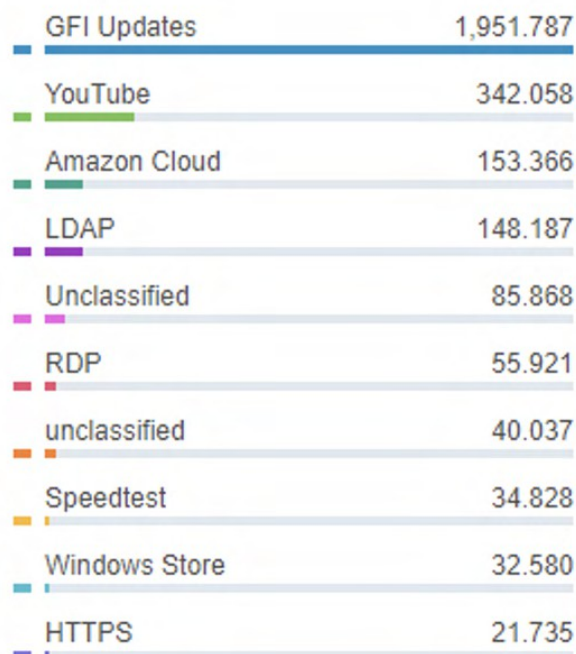
Application Performance Scores and Metrics zeigt den APS-Score für die Anwendung an. Ein guter Wert liegt zwischen 8,5 und 10,0. Ein Wert unter 7,0 kann eine Untersuchung rechtfertigen.

3.3.3 Bandbreitennutzung

Bandbreitennutzung - Top-Anwendungen

Wenn Sie wissen, wie viel Bandbreite Ihre wichtigsten Anwendungen verbrauchen, können Sie herausfinden, ob die Kontrolle bestimmter Anwendungen dazu beitragen kann, Ihren Durchsatz effektiv zu verringern.

Top Apps (GB)



Screenshot 144: Diagramm zur Nutzung der wichtigsten Apps

Um zu sehen, wie viel Bandbreite Ihre wichtigste Anwendung verbraucht, gehen Sie zu **Monitor> Anwendungen**. Weitere Informationen finden Sie unter [Anzeigen des Datenverkehrsvolumens von Anwendungen](#).

Bandbreitennutzung - Top-Zusammenfassung

Für die Verwaltung Ihres Netzwerks ist es wichtig zu wissen, wie viel Bandbreite Ihre Nutzer verbrauchen. Wenn Ihre Verbindung überlastet ist, müssen Sie wissen, ob Sie ein Bandbreiten-Upgrade planen müssen, oder ob Richtlinienbasiertes Shaping kann stattdessen den Durchsatz effektiv reduzieren.

Um zu sehen, wie viel der Bandbreite Ihres Netzwerks genutzt wird, gehen Sie zu **Monitor> Schnittstellen**. Weitere Informationen finden Sie unter [Überwachung des Schnittstellendurchsatzes](#).

3.3.4 Verwendung des Berichts Application Performance Monitor VoIP

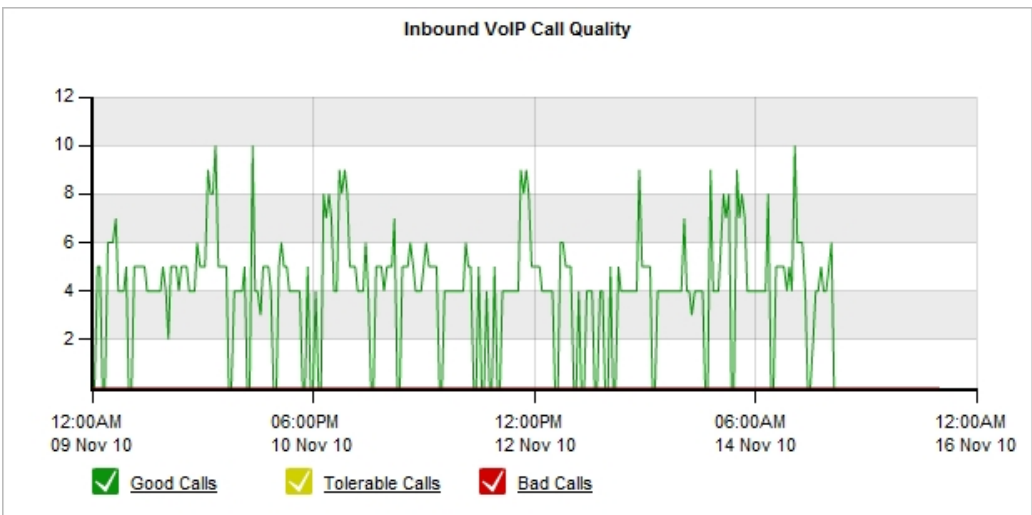
Der VoIP-Bericht überwacht und berichtet über die Qualität von VoIP-Transaktionen in einem Netz. Er zeigt Daten unter Verwendung von Standardmaßen der Telekommunikationsbranche wie MOS und rFactor an.

Ausführen des Berichts Anwendungsleistung VoIP

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Gehen Sie zu **Solution Center> Solution Center anzeigen**.
5. Klicken Sie unter **Anwendungsleistung** auf **VoIP-Leistung> Ausführen**. Ein Bestätigungsbildschirm wird geöffnet.
6. Klicken Sie auf **Ok**. Der Bericht wird geöffnet.

NOTE
After the initial run, you can access the report by clicking **Solution Center> VoIP Performance**.

Verstehen der Daten, die in einem Bericht zur Anwendungsleistung VoIP angezeigt werden



Worst 30 Inbound VoIP Conversations						
Internal Host	External Host	Delay (ms)	Jitter (ms)	Loss (%)	MOS	rFactor
253.7.254.1	253.11.254.1	0	0.00	0.00	4.28	87.90
173.253.253.1	173.5.254.1	0	0.00	0.00	4.28	87.90

Das Diagramm zeigt drei Reihen, die die Anzahl der "guten", "erträglichen" und "schlechten" Anrufe im Laufe der darstellen. In der Tabelle unterhalb des Diagramms sind die schlechtesten eingehenden und ausgehenden VoIP-Anrufe für den angegebenen Zeitraum aufgeführt.

Die Bedeutungen der Farben:

» Gut (grün) - MOS größer als 4. » Tolerabel (gelb)

- MOS zwischen 2 und 4. » Schlecht (rot) - MOS

kleiner als 2.

Was ist MOS?

MOS, oder Mean Opinion Score, ist ein Maß für die Qualität. Früher bewerteten die Nutzer ihr Anruferlebnis auf einer fünfstufigen Skala.

Eine GFI ClearView Appliance automatisiert die MOS-Bewertung unter Berücksichtigung der Netzwerkabhängigkeit. Die Bewertungen haben die folgende Bedeutung.

5 - Perfekt, wie Gespräche von Angesicht zu Angesicht oder Radioempfang.

4 - Mittelmäßig, es werden Mängel wahrgenommen, aber der Klang ist klar. Mobiltelefongespräche werden in der Regel als mittelmäßig eingestuft. 3 - Lästig.

2 - Sehr ärgerlich, fast unmöglich zu kommunizieren. 1 -

Unmöglich zu kommunizieren.

Was ist rFactor?

rFactor ist ein Maß für die Anrufqualität in IP-Netzen unter Berücksichtigung von Netzverzögerungen und Beeinträchtigungen. rFactor reicht von 0 (extrem schlechte Qualität) bis 100 (hohe Qualität). Ein rFactor von weniger als 50 ist nicht akzeptabel.

3.3.5 Freizeitverkehr

Der Bericht über den Freizeitverkehr zeigt die Nutzung von Freizeitanwendungsgruppen im Laufe der Zeit für den angegebenen Zeitraum. Er zeigt Informationen für Spiele, Instant Messaging, Peer-to-Peer, soziale Netzwerke und Streaming. Dieser Bericht kann Fragen beantworten wie:

» Wie viele Daten werden für Freizeitanwendungen über mein Netz übertragen? »

Wie viele Hosts sind beteiligt?

» Wie viel Zeit wird für die Übertragung der Daten über das Netz benötigt?

Die Einsicht in wichtige Freizeitanwendungen ist der erste Schritt, um sie zu verwalten. Diese Anwendungen sind in der Regel unerwünscht, da sie die Leistung wichtiger Geschäftsanwendungen beeinträchtigen, die Kundenerfahrung negativ beeinflussen, die Produktivität der Benutzer verringern, Viren in das Netzwerk einschleusen und das Herunterladen von illegalem oder urheberrechtlich geschütztem Material ermöglichen können.

Wie wird dieser Bericht erstellt?

Der Bericht für den Freizeitverkehr kann über das GFI ClearView Solution Center erstellt werden

1. Gehen Sie zu Solution Center> Solution Center anzeigen.

2. Klicken Sie unter **Network Governance** auf **Recreational Traffic**> **Run**. Ein Bestätigungsbildschirm wird geöffnet.

3. Klicken Sie auf **Ok**.

NOTE

Once the report has been set up, you can access it by clicking **Solution Center > Recreational Traffic**.

3.3.6 Verwendung der Berichte der Netzwerk-Governance

Netzwerk-Governance-Berichte liefern Daten, die es Ihnen ermöglichen, Ihre Netzwerkressourcen gemäß den von Ihrem Unternehmen festgelegten ethischen Grenzen zu verwalten. Zu den Lösungskategorien gehören Freizeitverkehr und RIAA Notice Prevention.

Verständnis der im Bericht "Freizeitverkehr" angezeigten Daten

Der Bericht zum Freizeitverkehr zeigt den Bandbreitenverbrauch von Freizeitanwendungen für einen bestimmten Zeitraum an. Er zeigt Netzwerkverkehrsdaten für Spiele, Instant Messaging, Peer-to-Peer, soziale Netzwerke und Streaming.

Freizeitanwendungen werden in Unternehmensnetzwerken im Allgemeinen als unerwünscht angesehen, da sie die Leistung wichtiger Geschäftsanwendungen beeinträchtigen, die Kundenzufriedenheit negativ beeinflussen, die Benutzerproduktivität verringern, Viren in das Netzwerk einschleusen und das Herunterladen von illegalem oder urheberrechtlich geschütztem Material ermöglichen.

Recreational - -		More details ?		
Application	Hosts	Time	Data	
	2	11m	2MB	
Games	1	10s	0MB	
Instant Messaging	0	0s	0MB	
P2P	0	0s	0MB	
Social Networking	2	4m 30s	2MB	
Streaming	1	6m 20s	0MB	

Screenshot 146: Der Bericht über den Freizeitverkehr.

Ausführen des Berichts "Freizeitverkehr"

1. Gehen Sie zu **Solution Center> Solution Center anzeigen**.
2. Klicken Sie unter **Network Governance** auf **Recreational Traffic**.
3. Geben Sie alle Details an, die der Assistent benötigt.
4. Klicken Sie auf **Ok**.

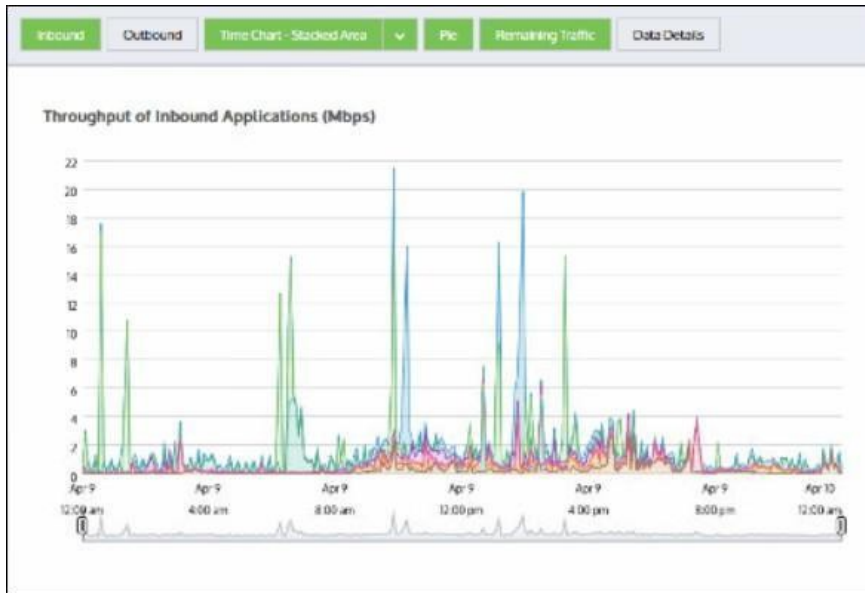
NOTE

After the initial run, you can access the report by clicking **Solution Center> Recreational Traffic**.

3.3.7 Antworten auf häufig gestellte Fragen zur Leistung der Solution Center-Anwendung

Welche Arten von Daten sind in einem Bericht zur Anwendungsleistung verfügbar?

Ein Bericht über die Anwendungsleistung zeigt die Netzwerkbenutzererfahrung einer Anwendung anhand einer Reihe von Diagrammen, Tabellen und Schaubildern.



Screenshot 147: Antrag auf Inbound-Bandbreite

Die Diagramme "Eingehende" und "Ausgehende Bandbreite" zeigen, wie viel Bandbreite die Anwendung verbraucht. Sie sollten erwarten, dass die Bandbreite Spitzen anstelle von erhöhten flachen Spitzen aufweist.

Das Diagramm zeigt Daten, die auf der WAN-Seite der Appliance gemessen wurden, bevor der beschleunigte Datenverkehr für den eingehenden Verkehr dekomprimiert wird und nachdem die Beschleunigungs- und Traffic-Shaping-Richtlinien für den ausgehenden Verkehr angewendet wurden.

Sie können die auf der LAN-Seite der Appliance gemessenen Daten überlagern, um den Umfang der durch die Beschleunigung und das Traffic Shaping erzielten Reduzierung aufzuzeigen.

Die Balkendiagramme für Benutzer und Hosts zeigen das WAN-seitige Datenvolumen, das von den wichtigsten Benutzern und Hosts für die Anwendung verbraucht wird. In der Regel werden die Anwendungen von mehreren Benutzern oder Hosts genutzt, und der Datenverkehr ist relativ gleichmäßig auf die wichtigsten Benutzer oder Hosts verteilt.

Wenn ein Benutzer oder Host deutlich mehr Datenvolumen aufweist als die anderen Benutzer, kann dies ein vernünftiges Verhalten sein oder auf ein Problem hinweisen, das eine weitere Untersuchung erfordert. Sie können auch wählen, ob Sie nur interne Endpunkte, d. h. Hosts und Benutzer auf der LAN-Seite Ihrer Appliance, oder nur externe Endpunkte, d. h. Hosts und Benutzer auf der WAN-Seite Ihrer Appliance, anzeigen möchten. Sie können auch wählen, ob Sie nur Benutzer, nur Hosts oder beides anzeigen möchten. Metriken für die Anwendungsleistungsbewertung Sie sollten eine gute Bewertung (zwischen 8,5 und 10,0) erwarten. Wenn der Wert unter 7,0 liegt, sollten Sie sich die Sache genauer ansehen.

Was ist der Anwendungsleistungsbericht baselining?

Die Überwachung der Anwendungsleistung erfordert ein grundlegendes Verständnis des beobachteten Datenverkehrs für eine Anwendung in Ihrem Netz. Der Prozess des Sammelns von Daten und des Festlegens einer Baseline wird als Baselining bezeichnet.

Sobald Sie einen Monitor erstellt haben, beginnt der Baselining-Vorgang automatisch mit der Analyse des Datenverkehrs und

beginnt der Prozess der Berechnung der anfänglichen Schwellenwerte. Für diesen Prozess sind Daten des Netzwerkverkehrs einer Stunde erforderlich.

Wenn für eine Anwendung während einer Baseline-Periode kein Datenverkehr beobachtet wird, wird der Baseline-Prozess wiederholt, bis Datenverkehr beobachtet und Schwellenwerte berechnet werden.

Der Baseline-Prozess muss nicht immer eine Stunde dauern, wenn eine GFI ClearView Appliance den Datenverkehr für die Anwendung innerhalb der Stunde, in der der Baseline-Prozess beginnt, beobachtet und gespeichert hat.

Wenn Sie beispielsweise einen Anwendungsmonitor erstellen, während noch zehn Minuten einer Stunde verbleiben, und GFI ClearView in dieser Stunde den Netzwerkverkehr für die Anwendung erfasst hat, analysiert der Baseline-Prozess die letzten fünfzig Minuten der erfassten Verkehrsdaten. Anschließend wird die Baseline-Periode in den verbleibenden 10 Minuten der Stunde vervollständigt.

Was ist, wenn das Solution Center anzeigt, dass es keine Lösungen gibt?

Die Lösungsbeschreibungen werden von einem von GFI ClearView gehosteten Server bereitgestellt. Wenn Ihr GFI ClearView Solution Center anzeigt, dass keine Lösungen vorhanden sind, überprüfen Sie die Internetverbindung und die Verbindung zum gehosteten GFI ClearView-Server. Wenn der von GFI ClearView gehostete Server nicht verfügbar ist, sind zuvor instanziierte Lösungen weiterhin in Ihrem Solution Center verfügbar.

Was ist, wenn eine Lösung eine höhere Version von GFI ClearView OS erfordert?

Die Schaltfläche **Ausführen** der Lösung ist erst verfügbar, wenn Sie Ihr GFI ClearView OS auf entsprechende oder eine höhere Version aktualisiert haben.

Kann ich eine Lösung mehr als einmal ausführen?

Ja. Sie können eine Lösung mehrfach ausführen, wenn die Lösung Konfigurationsparameter enthält. Sie können zum Beispiel mehrere benutzerdefinierte Anwendungsleistungsmonitore erstellen, wobei jeder Bericht eine andere Anwendung überwacht. Für Lösungen ohne Konfigurationsparameter, wie z. B. VoIP-Leistung, können Sie die Lösung nur einmal erstellen.

3.3.8 Hinzufügen und Löschen von Lösungen

Anhand der folgenden Anweisungen können Sie GFI ClearView-Lösungen zu Ihrer Konfiguration hinzufügen und später bei Bedarf wieder löschen. Wenn die Lösungen definiert sind, bieten sie Zugriff auf Berichte, die sich auf angegebenen Anwendungen konzentrieren.

So fügen Sie eine Lösung hinzu

Das GFI ClearView Solution Center enthält mehrere vordefinierte Lösungen, Sie können aber auch eigene Lösungen definieren.

1. Gehen Sie zu **Lösungszentrum > Lösungszentrum anzeigen**. Die in Kategorien unterteilten Lösungen sind über die verschiedenen Links auf der linken Seite zugänglich.
2. Wählen Sie die gewünschte Lösung aus der Liste aus.
3. Klicken Sie auf die Schaltfläche **Ausführen**.
4. Geben Sie alle Details an, die der Assistent benötigt. Auf der letzten Seite des Assistenten wird angegeben, wo der Bericht zu finden ist.
5. Wenn Sie auf **Ok** klicken, gelangen Sie zu Ihrem Bericht.

NOTE

Once a report has been set up, a link to it is available from the main task bar at the top of the page. Click **Solution Center**> **Report Name**.

So löschen Sie eine Lösung

Die einzige Möglichkeit, eine Lösung zu löschen, ist über die Befehlszeile. Bei einigen Lösungen müssen Sie jedoch die Lösungs-ID über die Web-Benutzeroberfläche ermitteln, bevor Sie die Lösung entfernen können.

1. Gehen Sie zu Konfiguration > Objekte> Service Levels> Application Performance Scores.
2. Suchen Sie die Anwendung in der Spalte **APS-Name**.

NOTE

The formatting of the name includes "Solution Center" and the ID. For example the CIFS APS object would be called CIFS Solution Center (208).

3. Notieren Sie sich die Lösungs-ID.
4. Öffnen Sie die CLI.
5. Geben Sie an der Eingabeaufforderung `no solutionc <id>` ein. Beispiele:

- `keine Lösungc 208`
- `keine Lösungc VoIPPerformance`
- `keine Lösungc Freizeitverkehr`

3.3.9 Festlegung einer neuen Basislinie

Verwenden Sie die folgenden Anweisungen, um eine neue Basislinie für die Leistungsbewertung einer Anwendung festzulegen. Wenn Sie eine neue Basislinie festlegen müssen, sollten Sie dies tun, wenn Sie erwarten, dass die Anwendung eine angemessene Leistung erbringt.

1. Gehen Sie zu Konfiguration > Objekte> Service Levels> Application Performance Score (APS).
2. Suchen Sie das APS-Objekt und wählen Sie es aus.

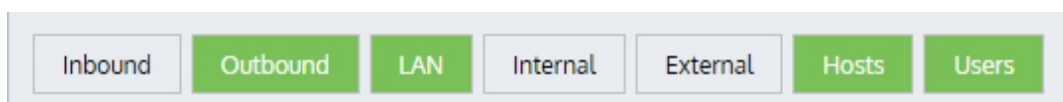
NOTE

The object name includes "Solution Center" and is suffixed with an application ID.

3. Wählen Sie **Auto Baseline Period** und klicken Sie auf **Start Baseline**.

3.3.10 Arbeiten mit Diagrammen zur Anwendungsleistung

Sie können die auf der Seite angezeigten Daten filtern, indem Sie die verschiedenen Diagramme ein- und ausschalten. Klicken Sie auf die Schaltflächen am oberen Rand der Seite, um zwischen den Ansichten zu wechseln. Wenn eine Schaltfläche grün ist, werden die Daten auf der Seite angezeigt.



Bestimmung der Durchsatzwerte für bestimmte Zeitpunkte in der Durchsatztabelle

Bewegen Sie den Mauszeiger über das Diagramm. Es erscheint ein Datenpinsel, der den durchschnittlichen Durchsatz für jeweiligen Zeitpunkt anzeigt.

3.3.11 Untersuchung einer schlechten Anwendungsleistungsbewertung (APS)

Klicken Sie in einem Anwendungsleistungsdiagramm auf **Details anzeigen**. Ein neuer Bildschirm zeigt die Maßnahmen an, die zur APS beitragen:

- » Netzwerkverzögerung und normalisierte Netzwerkverzögerung - die Zeit, die die Daten benötigen, um das Netzwerk (auf der Leitung) zu durchlaufen
- » Serververzögerung und normalisierte Serververzögerung - die Zeit, die ein Server benötigt, um auf Anfrage zu antworten
- » Round Trip Time - die Zeit, die Daten benötigen, um von einem Gerät über ein Netzwerk zu gelangen und wieder zurückzukehren
- » Jitter - ein Maß für die Variabilität der Netzwerkverzögerung. Wir definieren ihn als eine Standardabweichung der Netzwerkverzögerung.
- » Eingehender Verlust und ausgehender Verlust - die Menge der erneut übertragenen Daten

Prüfen Sie die Diagramme, um festzustellen, welches Attribut das schlechte APS-Ergebnis verursacht hat. Wenn beispielsweise die Messwerte für die Serververzögerung gut, die Messwerte für die Netzwerkverzögerung aber schlecht sind, dann wissen Sie, dass das Netzwerk die Schuld trägt, und können vielleicht etwas dagegen tun. Wenn die Netzwerkverzögerungswerte gut, die Serververzögerungswerte jedoch schlecht sind, sollten Sie untersuchen lassen, warum der Server eine schlechte Leistung erbringt.

Beachten Sie, dass die berechneten Schwellenwerte zu hoch oder zu niedrig sein können, wenn der Baseline-Zeitraum nicht typisch war. Wurde die Anwendung beispielsweise an einem Wochenende mit sehr geringem Datenverkehr baselined, können die Schwellenwerte viel niedriger sein, als es bei einer typischen Nutzung des Netzwerks zu erwarten wäre. Wurde die Anwendung in einer Zeit mit extrem hohem Verkehrsaufkommen gestartet, z. B. wenn die meisten Mitarbeiter einen Online-CEO-Webcast verfolgen, können die Schwellenwerte viel höher sein, als bei einer typischen Nutzung des Netzwerks zu erwarten wäre.

3.3.12 Untersuchung ungewöhnlicher Leistungen

Zoomen Sie in den gewünschten Bereich hinein, indem Sie die Dropdown-Liste **Daten anzeigen für** öffnen und eine der definierten Zeitspannen auswählen. Verwenden Sie bei Bedarf die Schieberegler unterhalb des Diagramms, um den Zeitraum weiter einzuzugrenzen. Alle Zeitreihendiagramme auf diesem Bildschirm (eingehender Durchsatz, ausgehender Durchsatz) werden synchronisiert, so dass Sie nach Korrelationen in den Daten suchen können.

Wenn ein flacher Spitzenwert mit einem Rückgang der Anwendungsleistung einhergeht, liegt wahrscheinlich ein Problem vor, das mit einer Richtlinie (oder mehreren Richtlinien) zusammenhängt, die die Anwendung steuern. Es kann sein, dass die Richtlinienumgebung der Anwendung nicht genügend Bandbreite garantiert oder dass weniger wichtige Anwendungen, wie z. B. Freizeitanwendungen, zu viel Bandbreite haben. Um die beste Vorgehensweise zu bestimmen, sollten Sie sich die Diagramme für andere Anwendungen oder Anwendungsgruppen ansehen, um festzustellen, ob die zulässige Bandbreite angemessen ist.

3.3.13 Löschen eines Berichts zur Anwendungsleistung

Die einzige Möglichkeit, eine Lösung zu löschen, ist über die Befehlszeile. Bei einigen Lösungen müssen Sie jedoch die Lösungs-ID über die Web-Benutzeroberfläche ermitteln, bevor Sie die Lösung entfernen können.

1. Gehen Sie zu Konfiguration > Objekte> Service Levels> Application Performance Scores.
2. Suchen Sie die Anwendung in der Spalte **APS-Name**.

NOTE

The formatting of the name includes "Solution Center" and the ID. For example the CIFS APS object would be called CIFS Solution Center (208).

3. Notieren Sie sich die Lösungs-ID.
4. Öffnen Sie die CLI.
5. Geben Sie an der Eingabeaufforderung `no solutionc <id>` ein. Beispiele:
 - `keine Lösungc 208`
 - `keine Lösungc VoIPPerformance`
 - `keine Lösungc Freizeitverkehr`

4 Einstellungen

Erfahren Sie, wie Sie die GFI ClearView Appliance entsprechend Ihren Anforderungen konfigurieren können.

4.1 Netzwerk Einstellungen

Erfahren Sie, wie Sie die Netzwerkeinstellungen für Ihre GFI ClearView Appliance(s) konfigurieren können.

4.1.1 NIC Konfiguration

Auf der Seite NIC-Einstellungen werden Geschwindigkeit, Duplex und MTU der System-NICs eingestellt.

Schnittstelle Einstellungen

Die GFI ClearView-Appliance und die an die Appliance angeschlossenen Geräte müssen die gleichen Geschwindigkeits- und Duplex-Einstellungen für ihre Netzwerkschnittstellen haben. In den meisten Fällen genügen die Standardeinstellungen, da GFI ClearView für die automatische Aushandlung eingerichtet ist. Einige Geräte sind damit jedoch nicht kompatibel.

Wenn die Appliance und die angeschlossenen Geräte unterschiedliche Geschwindigkeits- und Duplex-Einstellungen verwenden, können die Geräte möglicherweise nicht miteinander kommunizieren und der Datenverkehr kann unterbrochen werden. In diesem Fall können Sie Kollisionen, Fehler, Paketverluste und Netzwerkverzögerungen feststellen

auf den GFI ClearView NICs, wodurch der Systemstatus als "Warnung" angezeigt wird und die fehlerhafte(n) Schnittstelle(n) hervorgehoben werden.

Prüfen Sie, ob der Router oder Switch fest auf eine bestimmte Geschwindigkeit oder Duplex-Einstellung festgelegt ist. Wenn dies der Fall ist, stellen Sie entweder alle Geräte auf Auto-Negotiate oder das GFI ClearView-Gerät auf die gleiche Geschwindigkeit und den gleichen Duplex-Modus ein.

NOTE

For further troubleshooting, click on the system warning or view the NIC Diagnostics by clicking on the View NIC Diagnostics link.

View NIC Diagnostics...

Interface	Media	HW Address	Speed	Duplex	MTU	Link Status
eth1	Twisted Pair	00:22:19:D4:8D:C4	Auto	Auto	1500	Admin UP, Link UP, Speed: 100Mb/s (auto), Duplex: Full (auto)
eth2	Twisted Pair	00:22:19:D4:8D:C5	Auto	Auto	1500	Admin UP, Link DOWN, Speed: UNKNOWN, Duplex: UNKNOWN
eth10	Twisted Pair	00:E0:ED:13:73:C2	Auto	Auto	1500	Admin UP, Link UP, Speed: 100Mb/s (auto), Duplex: Full (auto)
eth11	Twisted Pair	00:E0:ED:13:73:C3	Auto	Auto	1500	Admin UP, Link UP, Speed: 1000Mb/s (auto), Duplex: Full (auto)

Apply Changes

Screenshot 205: Einstellen und Anzeigen von Geschwindigkeit, Duplex und MTU der NIC-Schnittstellen

Wo kann ich diese Konfiguration finden?

Gehen Sie zu **Konfiguration > System > Netzwerk > NICs**.

So konfigurieren Sie die NIC Schnittstellen

1. In der Schnittstellentabelle werden Sie sehen:

- **Schnittstelle** - Jede Schnittstelle entspricht einem physischen Anschluss.
- (z. B. eth1, eth2) **Media** - Gibt das Schnittstellenmedium an. Die Optionen sind Twisted Pair oder Glasfaser. **HW-Adresse** - Zeigt die MAC-Adresse der Schnittstelle.

2. Geben Sie die **Geschwindigkeit** und den **Duplex** an, die GFI ClearView mit benachbarten Geräten aushandeln soll. Verwenden Sie **Auto** speed, damit die GFI ClearView-Appliance die Geschwindigkeit mit benachbarten Geräten automatisch aushandeln kann. Verwenden Sie Auto-Duplex, damit die GFI ClearView-Appliance den Duplex mit benachbarten Geräten automatisch aushandeln.

3. Geben Sie die MTU-Größe (Maximum Transmission Unit) in Bytes an.

4. **Link-Status** anzeigen: Der Link-Status zeigt an, ob die Schnittstelle aktiviert/deaktiviert ist, ob die Verbindung aktiviert/deaktiviert ist sowie die Geschwindigkeit/Duplex, die mit dem benachbarten Gerät ausgehandelt wurde.

5. Klicken Sie auf **Änderungen übernehmen**.

4.1.2 IP-Adresse Konfiguration

Mit der GFI ClearView-Appliance lassen sich Netzwerkschnittstellen nach Bedarf konfigurieren, und einer Schnittstelle können Rollen zugewiesen (Mirror) und IP-Einstellungen vorgenommen werden.

NOTE

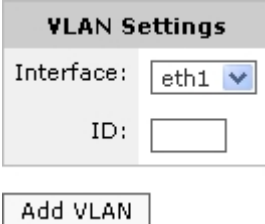
For GFI ClearView, only the "Mirror" option is relevant, the other options are for the optimization-enabled version of GFI ClearView i.e. Exinda Network Orchestrator."

Für GFI ClearView ist nur eine einzige Rolle erforderlich:

» Mirror - Eine oder mehrere Schnittstellen können im Mirror-Modus konfiguriert werden. Dieser Betriebsmodus wird für die Out-of-Path-Überwachung mit einem Hub- oder Switch-Spiegel/SPAN-Port verwendet.

Die DHCP-Option ist auf der GFI ClearView-Appliance standardmäßig aktiviert. Wenn ein DHCP-Server verfügbar ist, wird automatisch eine IP-Adresse zugewiesen. Rufen Sie in einem Webbrowser [die Seite http://findmy.exinda.com/](http://findmy.exinda.com/) auf. Dadurch wird ein Java-Applet heruntergeladen und die GFI ClearView-Appliance automatisch gefunden. Klicken Sie auf die gefundene GFI ClearView-Appliance, um auf sie zuzugreifen. Wenn keine DHCP-Adresse verwendet wird, verwendet GFI ClearView standardmäßig die IP-Adresse 172.14.1.57.

In der VLAN-Konfiguration kann eine 802.1Q VLAN-ID für eine Schnittstelle festgelegt werden. Die VLAN-ID kann zwischen 1 und 4094 liegen.



VLAN Settings

Interface: eth1 ▼

ID:

Add VLAN

Weitere Informationen zu Clustering/HA, Mirroring und WCCP finden Sie in den zugehörigen How To Guides.

Wo kann ich diese Konfiguration finden?

Gehen Sie zu **Konfiguration > System > Netzwerk > IP-Adresse**.

So konfigurieren Sie automatisch eine Schnittstellenadresse und Netzmaske

1. Aktivieren Sie für die angegebene Schnittstelle oder Bridge entweder das Kontrollkästchen **DHCP** für IPv4-Netzwerke oder **SLAAC** für IPv6-Netzwerke.
2. Wenn **DHCP** ausgewählt ist, wird automatisch eine IP-Adresse zugewiesen.
3. Wenn **SLAAC** für IPv6-Netzwerke ausgewählt ist, werden die folgenden zusätzlichen Optionen angezeigt:
 - **Datenschutzadresse** - Aktivieren Sie die SLAAC-Datenschutzerweiterung. Wenn Sie diese Option auswählen, wird die automatisch zugewiesene IPv6-Adresse regelmäßig geändert.
 - **Gateway** - Weisen Sie ein IPv6-Gateway dynamisch zu.

So konfigurieren Sie eine statische Adresse

1. Geben Sie eine IPv4- oder IPv6-Adresse und eine Netzmaske ein.
2. Sie können optional einen Kommentar hinzufügen, der beschreibt, wie die Schnittstelle verwendet werden soll, und zwar im Feld **Kommentar** Feld.

So konfigurieren Sie die Einstellungen des Gateways

Geben Sie die Adresse der Standard-IPv4- und IPv6-Gateways Ihres Netzwerks ein.

4.1.3 Leitwege Konfiguration

Statische Routen müssen eventuell definiert werden, wenn der Zugang zu externen Netzwerken nicht über das Standard-Gateway erreicht werden kann. Dies kann notwendig sein, damit die Appliance eine Verbindung zu Diensten wie DNS oder NTP herstellen kann.

Routing-Tabelleneinträge werden für IPv4- und IPv6-Netzwerke angezeigt. Für jede Route werden das Ziel, das Gateway, die Schnittstelle, die Quelle und der Status angezeigt. Routing-Tabelleneinträge können mehrere Quellen haben:

static	A manually configured route.
interface	Derived from the addresses assigned to an interface.
SLAAC	Assigned from SLAAC autoconfiguration.
DHCP	Assigned from DHCP autoconfiguration.

IPv4 routes					
	Destination	Gateway	Interface	Source	Active
<input type="checkbox"/>	default	172.16.1.254	eth1	static	<input checked="" type="checkbox"/>
	172.16.0.0/23	0.0.0.0	eth1	interface	<input checked="" type="checkbox"/>

Remove Selected

IPv6 routes					
	Destination	Gateway	Interface	Source	Active
	2001:44b8:62:690::/64	::	eth1	SLAAC interface	<input checked="" type="checkbox"/>
	default	fe80::210:f3ff:fe0e:f4d0	eth1	SLAAC	<input checked="" type="checkbox"/>
	fe80::/64	::	br10	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth2	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth20	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth21	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	br12	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	br20	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	brvm2	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth1	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth10	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth11	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth12	interface	<input checked="" type="checkbox"/>
	fe80::/64	::	eth13	interface	<input checked="" type="checkbox"/>

Remove Selected

Add New Static Route	
Destination:	<input type="text"/> / <input type="text"/>
Gateway (Next Hop):	<input type="text"/>

Add Route

Screenshot 209: Routenkonfiguration

Destination	The IPv4 or IPv6 address and netmask of the destination
Gateway (Next Hop)	The IPv4 or IPv6 address of the gateway (next hop).

4.1.4 DNS und Domännennamen Konfiguration

Auf der Seite DNS können Sie einen Hostnamen für Ihre GFI ClearView-Appliance festlegen und den Standort Ihres DNS-Servers bzw. Ihrer DNS-Server konfigurieren. Sie können auch Domännennamen konfigurieren, die zur Auflösung von Hostnamen in anderen Konfigurationsbildschirmen verwendet werden können.

Der Hostname der GFI ClearView-Appliance sollte im Netzwerk eindeutig sein. Die DNS-Server-Einstellung kann dynamisch sein, d. h. vom DHCP-Server konfiguriert werden, oder sie kann durch Eingabe einer oder mehrerer IP-Adressen Ihrer DNS-Server konfiguriert werden.

Static and Dynamic Name Servers		
IP Address	Active	Source
10.1.0.2	<input checked="" type="checkbox"/>	configured

System Host Name	
Host Name	<input type="text" value="weber-exinda-monitor"/>
Primary DNS	<input type="text" value="10.1.0.2"/>
Secondary DNS	<input type="text"/>
Tertiary DNS	<input type="text"/>

NOTE

A valid DNS server is required for system alerts, scheduled reports, firmware updates, license updates, and Anonymous Proxy updates

Static and Dynamic Domain Names		
Domain	Active	Source
<input type="radio"/> wat.exinda.com	<input checked="" type="checkbox"/>	configured

Remove Selected

Add New Domain Name	
Domain Name	<input type="text"/>

Add New Domain Name

Wo kann ich diese Konfiguration finden?

Gehen Sie zu **Konfiguration > System > Netzwerk > DNS**.

So konfigurieren Sie den Hostnamen der Appliance

1. Geben Sie im Abschnitt **System Host Name** in das Feld **Host Name** den Namen für diese Appliance ein.
2. Klicken Sie auf **Änderungen übernehmen**.

Wie kann man feststellen, ob der DNS vom DHCP Server konfiguriert wurde?

Im Abschnitt **Statische und dynamische Namensserver** wird eine IP-Adresse angezeigt, deren Quelle als dynamisch gekennzeichnet ist. Dynamisch bedeutet, dass sie vom DHCP-Server konfiguriert wurde.

So konfigurieren Sie den Standort der DNS-Server

1. Geben Sie im Abschnitt **System Host Name** die IP-Adressen Ihrer DNS-Server in eines oder mehrere der Felder **Primary DNS** ein, **Sekundäres DNS-Feld**, und **Tertiäres DNS-Feld**.
2. Klicken Sie auf **Änderungen übernehmen**. Die eingegebenen IP-Adressen werden im Abschnitt **Statische und dynamische Namensserver** wie vorgesehen angezeigt.

So fügen Sie einen Domainnamen hinzu

1. Geben Sie im Bereich **Neuen Domänennamen hinzufügen** den neuen Domänennamen ein.
2. Klicken Sie auf **Neuen Domänennamen hinzufügen**. Der Domänenname wird zur Liste der statischen und dynamischen Domänennamen hinzugefügt. Alle manuell hinzugefügten Domänennamen sind statisch.

So entfernen Sie einen Domainnamen

1. Wählen Sie in der Liste **Statische und dynamische Domänennamen** die zu entfernende Domäne aus. Nur manuell hinzugefügte Domänennamen können entfernt werden.
2. Klicken Sie auf **Ausgewählte entfernen**.

4.1.5 HTTP-Proxy Konfiguration

Geben Sie einen HTTP-Proxy an, wenn die Appliance über einen HTTP-Proxy auf den Server von GFI ClearView zugreifen soll. Der Zugriff auf den HTTP-Server von GFI ClearView ist für Firmware-Updates, Lizenz-Updates und Anonymous Proxy-Updates erforderlich. Wenn Sie SDP aktiviert haben, stellen Sie bitte sicher, dass Ihr Proxy HTTPS unterstützt.

Wo kann ich diese Konfiguration finden?

Gehen Sie zu **Konfiguration > System > Netzwerk > HTTPProxy**.

So konfigurieren Sie den Zugriff auf den GFI ClearView-Server über einen HTTP -Proxy

1. Geben Sie den Hostnamen oder die IP-Adresse und den HTTP-Proxy-Port des HTTP-Proxys an. Es können IPv4- oder IPv6-Adressen angegeben werden.
2. Wählen Sie die Art der Authentifizierung für den HTTP-Proxy.
3. Geben Sie den **Benutzernamen** und das **Passwort** für den HTTP-Proxy ein.
4. Um SSL-Zertifikate zu überprüfen, deaktivieren Sie das Kontrollkästchen **SSL-Zertifikate nicht überprüfen**.
5. Klicken Sie auf **Änderungen übernehmen**.

4.1.6 E-Mail Konfiguration

Für den E-Mail-Versand von der GFI ClearView-Appliance ist ein SMTP-Server erforderlich. Die Appliance kann geplante Berichte, Systemwarnungen und automatische Support-Benachrichtigungen per E-Mail versenden. Zunächst müssen Sie die Verbindung zum SMTP-Server konfigurieren und dann die Benutzer verwalten, die die Systembenachrichtigungen erhalten.

SMTP Server	
SMTP Server Name	<input type="text" value="smtp.wat.exinda.com"/>
SMTP Server Port	<input type="text" value="25"/>
"From" Address	<input type="text" value="bob.loblaw@exinda.com"/>
SMTP Domain Name	<input type="text" value="localdomain"/>
SMTP Authentication	<input type="checkbox"/>

Notify Recipients			
Email Address	Verbose	Info Emails	Failure Emails
<input type="checkbox"/> antonio.cucci@abc.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> joseph.king@abc.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Remove Recipients

Send Test Email to All

Add New Notify Recipients	
Email Address	<input type="text"/>
Verbose Detail	<input checked="" type="checkbox"/>
Info Emails	<input checked="" type="checkbox"/>
Failure Emails	<input checked="" type="checkbox"/>

Add New Recipient

Konfigurieren der Einstellungen für den SMTP-Server

Gehen Sie wie folgt vor, um die Einstellungen des SMTP-Servers zu konfigurieren.

1. Gehen Sie zu Konfiguration > System > Netzwerk > E-Mail > SMTPServer.
2. Geben Sie in das Feld **SMTPServer Name** den Namen ein.

NOTE

You can use IPv4 or IPv6 addresses, or DNS names.

3. Geben Sie in das Feld **SMTPServer Port** die Portnummer ein.

NOTE

The default port number is 25.

4. Geben Sie in das Feld "**Von**"-Adresse die E-Mail-Adresse ein, von der die Systemwarnungen und Berichtsbenachrichtigungen gesendet werden sollen.
5. Wenn eine Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **SMTP-Authentifizierung**, und geben Sie den **Benutzernamen** und **Passwort**.
6. Aktivieren Sie ggf. das Kontrollkästchen **Secure Sockets Layer (SSL) verwenden**.
7. Klicken Sie auf **Änderungen übernehmen**.

Testen der SMTP-Konfiguration

Verwenden Sie die folgenden Anweisungen, um die SMTP-Konfiguration zu testen.

1. Gehen Sie zu Konfiguration > System > Netzwerk > E-Mail > Neue Benachrichtigungsempfänger hinzufügen.

2. Fügen Sie Ihre eigene E-Mail-Adresse hinzu und klicken Sie auf **Neuen Empfänger hinzufügen**. Die Liste im Abschnitt "Empfänger benachrichtigen" oben wird aktualisiert.
3. Klicken Sie im Abschnitt **Empfänger benachrichtigen** auf **Test-E-Mail an alle senden**.

Hinzufügen von E-Mail-Benachrichtigungsempfängern

Gehen Sie wie folgt vor, um neue E-Mail-Empfänger für Benachrichtigungen hinzuzufügen.

1. Gehen Sie zu Konfiguration > System > Netzwerk > E-Mail > Neue Benachrichtigungsempfänger hinzufügen.
2. Geben Sie in das Feld **E-Mail-Adresse** die E-Mail-Adresse ein.
3. Wählen Sie die Arten von Benachrichtigungen aus, die der Benutzer erhalten soll:
 - **Ausführliches Detail: Sendet** detaillierte Ereignis-E-Mails an den Benutzer.
 - **Info-E-Mails - Senden Sie** Informations-E-Mails an den Benutzer.
 - **Fehler-E-Mails - Senden Sie** Fehler-E-Mails an den Empfänger.
4. Klicken Sie auf **Neuen Empfänger hinzufügen**. Die neuen Empfänger werden zur obigen Liste der Benachrichtigungsempfänger hinzugefügt.

NOTE

The types of emails being received by a user cannot be modified. To change which emails a user receives, you must first delete the user, and then add the email address again with the appropriate types of notifications selected.


Entfernen von E-Mail-Benachrichtigungen Empfängern

Gehen Sie wie folgt vor, um Benutzer aus der Liste der E-Mail-Empfänger für Benachrichtigungen zu entfernen.

1. Gehen Sie zu Konfiguration > System > Netzwerk > E-Mail > Empfänger benachrichtigen.
2. Wählen Sie in der Liste den zu löschenden Benutzer aus.
3. Klicken Sie auf **Empfänger entfernen**. Der Benutzer wird aus der Liste entfernt und erhält keine E-Mail-Benachrichtigungen mehr.

4.1.7 SNMP Konfiguration

Die GFI ClearView-Appliance ermöglicht den Datenexport an SNMP-Systeme. Konfigurieren Sie die SNMP-Einstellungen, oder laden Sie die GFI ClearView SNMP MIB herunter.

SNMP Configuration	
SNMP	<input checked="" type="checkbox"/> Enable
SNMP Traps	<input checked="" type="checkbox"/> Enable
SNMP Multiple Communities	<input checked="" type="checkbox"/> Enable
Sys Contact	<input type="text"/>
Sys Location	<input type="text"/>
Read-Only Community	<input type="text" value="public"/>
Default Trap Community	<input type="text" value="public"/>
Download SNMP MIB	

Apply Changes


NOTE

To disable or enable SNMP traps for system alerts, see For more information, refer to [Alerts](#) (page 581)..

SNMP konfigurieren

Gehen Sie wie folgt vor, um SNMP zu konfigurieren.

1. Gehen Sie zu Konfiguration > System > Netzwerk> SNMP> SNMPConfiguration.

SNMP Configuration	
SNMP	<input checked="" type="checkbox"/> Enable
SNMP Traps	<input checked="" type="checkbox"/> Enable
SNMP Multiple Communities	<input checked="" type="checkbox"/> Enable
Sys Contact	<input type="text"/>
Sys Location	<input type="text"/>
Read-Only Community	<input type="text" value="public"/>
Default Trap Community	<input type="text" value="public"/>
Download SNMP MIB	

Apply Changes

2. Aktivieren Sie je nach Bedarf die folgenden Funktionen:
- SNMP
 - SNMP-Traps
 - SNMP Mehrere Gemeinschaften

NOTE

When the Multiple Communities option is disabled, the Community list area does not appear.

4. Geben Sie im Feld **Sys Contact** die Variable syscontact in MIB-II an.
5. Geben Sie im Feld **Sys Location** die Variable syslocation in MIB-II an.
6. Geben Sie die Community-Zeichenfolge **Read-only** und **Default Trap** ein.

NOTE

When the Read-only community is changed to have a value that does not match an existing community, a new SNMP community is added to the list.

7. Klicken Sie auf **Änderungen übernehmen**.

Entfernen einer unerwünschten SNMP Community

Gehen Sie wie folgt vor, um eine unerwünschte SNMP-Community zu entfernen.

1. Gehen Sie zu Konfiguration > System > Netzwerk > SNMP> Liste der konfigurierten SNMPCommunities.

	Community	Access Type
<input type="checkbox"/>	public	Read-only

Remove Selected

2. Aktivieren Sie im Bereich Liste der **SNMPCommunities** das Kontrollkästchen neben dem Community-Eintrag und klicken Sie auf **Ausgewählte entfernen**.

Herunterladen der SNMP-MIB-Datei

Verwenden Sie die folgenden Anweisungen, um die SNMP-MIB-Datei herunterzuladen. Die Datei enthält zusätzliche Überwachungsinformationen.

1. Gehen Sie zu Konfiguration > System > Netzwerk > SNMP.

2. Klicken Sie unter **SNMPConfiguration** auf **SNMPMIB herunterladen**. Die `EXINDA-MIB.txt` Datei wird an den von Ihnen angegebenen Ort heruntergeladen.

Ändern von SNMP-Authentifizierung für den Benutzer Admin

Gehen Sie wie folgt vor, um die SNMP-Authentifizierung für den Benutzer Admin zu ändern.

1. Gehen Sie zu Konfiguration > System > Netzwerk> SNMP> SNMPv3 Admin User.

SNMP v3 Admin User	
Admin User	<input type="checkbox"/> Enable
Authentication Type	SHA1
Privacy Type	AES-128
Authentication Password	<input type="text"/> (leave blank to not change)
Privacy Password	<input type="text"/> (leave blank to not change)

Apply Changes

2. Aktivieren Sie das Kontrollkästchen, wenn **Admin User** aktivieren möchten.

3. Wählen Sie aus dem Drehfeld **Authentifizierungstyp** entweder SHA1 oder MD5.

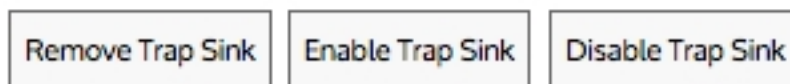
4. Wählen Sie aus dem Drehfeld **Datenschutztyp** entweder AES-128 oder DES.

5. Ändern Sie bei Bedarf das **Authentifizierungskennwort**, indem Sie das neue Kennwort eingeben.
6. Ändern Sie ggf. das **Datenschutz-Passwort**, indem Sie das neue Passwort eingeben.
7. Klicken Sie auf **Änderungen übernehmen**.

Vorübergehende Unterbrechung des Versands von SNMP-Traps

Gehen Sie wie folgt vor, um das Senden von SNMP-Traps an den Sink-Server zu deaktivieren.

Trap Sinks			
Host	Community	Version	Enabled
No trap sinks.			



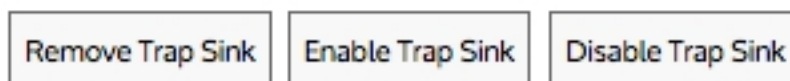
1. Gehen Sie zu Konfiguration > System > Netzwerk > SNMP > Trap Sinks.
2. Aktivieren Sie in der Liste das Kontrollkästchen für Server und klicken Sie auf **Trap Sink deaktivieren**.
3. Um den Server wieder zu aktivieren, wählen Sie den Server in der Liste aus und klicken Sie auf oder **Trap Sink aktivieren**.

Entfernen von Trap Sink servern

Gehen Sie wie folgt vor, um einen Trap-Sink-Server zu entfernen.

1. Gehen Sie zu Konfiguration > System > Netzwerk > SNMP.

Trap Sinks			
Host	Community	Version	Enabled
No trap sinks.			



2. Wählen Sie im Bereich **Trap Sinks** den Server aus der Liste aus und klicken Sie auf **Remove Server**.

Definieren von SNMP-Trap-Zielen

Verwenden Sie die folgenden Anweisungen, um festzulegen, wohin SNMP-Traps gesendet werden.

1. Gehen Sie zu Konfiguration > System > Netzwerk > SNMP.



Add New Trap Sink

2. Geben Sie im Bereich **Add New Trap Sink** den Hostnamen oder die IP-Adresse des SNMP-Trap-Sink-Servers an.

TIP

You can specify IPv4 or IPv6 addresses, or a hostname.

3. Geben Sie den Community-String für den SNMP-Trap-Sink-Server ein.

4. Wählen Sie den entsprechenden SNMP-Trap-Typ aus, der an den Sink-Server gesendet werden soll.

5. Klicken Sie auf **Neue Trap-Senke hinzufügen**.

4.1.8 Integration mit Active Verzeichnis

NOTE

You can configure the options in the Active Directory tab only after the GFI ClearView AD Connector is installed and configured on a designated network server that has access to the Active Directory Server. You will see the Active Directory Server details on this tab only when the configuration is completed successfully.

Die Konfiguration von Active Directory ermöglicht es der GFI ClearView Appliance, Netzwerkbenutzer und -gruppen aus Active Directory zu akzeptieren (z. B. Logins, IP-Adressen, Gruppenmitgliedschaft), so dass in der Lage ist:

- » Active-Directory-Benutzernamen in der Überwachung und Berichterstattung offenlegen, sodass Benutzer nicht mehr als IP-Adressen angezeigt werden müssen. Verwendung von Active Directory-Gruppen und -
- » Benutzernamen in Optimierungsrichtlinien, wodurch QoS und Optimierung implementiert werden.

Richtlinien, die auf einzelnen Benutzern oder ganzen Gruppen basieren.

Um Active Directory zu konfigurieren, müssen Sie den GFI ClearView AD Connector auf einem bestimmten Netzwerkserver installieren, verschiedene Einstellungen konfigurieren und dann die Port- und Kennworteinstellungen auf der Registerkarte Active Directory auf jeder GFI ClearView Appliance vornehmen.

So funktioniert die Active Directory-Integration

Die Active Directory-Integration ermöglicht es Ihnen, AD-Benutzernamen im Rahmen der Überwachung und Berichterstattung über

der GFI ClearView Appliance, anstatt die Standard-IP-Adressen anzuzeigen. Sie können auch AD-Gruppen und Benutzernamen in Optimierungsrichtlinien verwenden, um QoS- und Optimierungsrichtlinien auf der Basis einzelner Benutzer oder ganzer Gruppen zu implementieren.

Die Integration erfordert einen proprietären GFI ClearView AD Connector-Dienst, der auf einem Server im Netzwerk installiert wird, der Zugriff auf den Active Directory-Server hat. Nach der Konfiguration fungiert der Connector als Gateway zwischen dem Active Directory-Server und den GFI ClearView Appliances, um Benutzer- und Gruppeninformationen bereitzustellen. Wenn sich ein Benutzer mit seinen Active Directory-Anmeldedaten anmeldet, werden die Informationen vom Connector erfasst und an die GFI ClearView Appliances weitergeleitet. In den Monitor-Berichten werden die IP-Adressen durch die Benutzer- und Gruppennamen ersetzt, die aus Active Directory bezogen wurden.

Integrationsprozess

Führen Sie die folgenden Aufgaben aus, um den GFI ClearView AD Connector mit dem Active Directory-Server zu verbinden und die einzelnen GFI ClearView Appliances auszuwählen, die die AD-Informationen erhalten sollen

NOTE

Each installation of the Active Directory Connector can have a maximum of 20 GFI ClearView Appliances connected to it.

If there are more than 20 GFI ClearView Appliances, you will need to install the connector on multiple Windows servers and divide the appliances across multiple instances of the Active Directory Connector. The instructions below step you through configuring a single Connector. Repeat these instructions if you are installing more than one instance of the Active Directory Connector.

1. Installieren Sie den GFI ClearView AD Connector. [Weitere Informationen finden Sie unter Installieren des GFI ClearView AD Connector.](#)
 - a. Fügen Sie die GFI ClearView Appliances zum GFI ClearView AD Connector hinzu. [Weitere Informationen finden Sie unter Hinzufügen der GFI ClearView Appliances zum GFI ClearView AD Connector.](#)
 - b. Identifizieren Sie den Active Directory Server. Weitere Informationen finden Sie unter [Identifizieren des Active Directory-Servers.](#)
 - c. Wählen Sie die Informationen aus, die zwischen der GFI ClearView-Appliance und dem Active Directory-Server gesendet werden. Weitere [finden Sie unter Auswählen der Informationen, die zwischen der GFI ClearView-Appliance und dem Active Directory-Server gesendet werden.](#)
 - d. Die Portnummer von GFI ClearView AD Connector. [Weitere Informationen finden Sie unter Die Portnummer von GFI ClearView AD Connector.](#)
2. Identifizierung von Benutzern. Weitere Informationen finden Sie unter [Identifizierung von Benutzern.](#)
3. Überprüfen Sie die Kommunikation zwischen dem Active Directory-Server und der GFI ClearView-Appliance. Weitere Informationen finden Sie unter [Überprüfen der Kommunikation zwischen dem Active und der GFI ClearView-Appliance.](#)

NOTE

If you encounter any issues, see [Troubleshoot issues with Active Directory configuration.](#)

Konfigurationsoptionen

Nach erfolgreicher Integration können Sie die folgenden Aufgaben ausführen, um Benutzernamen in Überwachungsberichten anzuzeigen und Optimierungsrichtlinien auf der Grundlage von Benutzergruppen zu implementieren.

» Ansicht der wichtigsten internen und externen Benutzer im Netzwerk» Steuerung des Datenverkehrs auf der Grundlage von Benutzern

Installieren Sie den GFI ClearView AD Connector

Um Active Directory mit der GFI ClearView Appliance zu integrieren, muss der GFI ClearView AD Connector-Dienst auf einem Windows-Server installiert werden, der dann eine Verbindung zum Active Directory-Server herstellen kann. Jeder GFI ClearView AD Connector kann mit bis zu 20 GFI ClearView Appliances kommunizieren.

Sie können den Active Directory Connector über die Registerkarte **Konfiguration > System > Netzwerk > Active Directory** auf der GFI ClearView-Appliance herunterladen. Klicken Sie auf den Link Microsoft Installer Executable, und speichern Sie das Installationsprogramm an einem Speicherort, auf den alle Windows-Server im Netzwerk zugreifen können.

Anforderungen an die Installation

- » Der GFI ClearView AD Connector wird auf den folgenden Plattformen unterstützt
 - Windows Server 2019 und frühere Versionen
- » Für den GFI ClearView AD Connector ist das .NET Framework 4.0 erforderlich.
- » Logon Auditing muss auf dem Active Directory-Server aktiviert sein, um den GFI ClearView AD Connector zu installieren.
- » Der WMI-Dienst muss auf dem Active Directory-Server und auf dem Server, auf dem GFI ClearView AD Connector installiert ist, gestartet sein.
- » Für den Active Directory-Server und den Server, auf dem GFI ClearView AD Connector installiert ist, müssen die Ports RPC Endpoint Mapper und LDAP in Ihrer Firewall geöffnet sein. Diese Ports sind standardmäßig geöffnet. Um Ihre Einstellungen zu überprüfen, besuchen Sie <http://support.microsoft.com/kb/179442>.

Bereitstellen der erforderlichen Berechtigungen für den Dienst GFI ClearView AD

Wenn Sie den ClearView AD Connector auf einem Server installieren, der kein Domänencontroller ist, stellen Sie sicher, dass das Konto, das für die Ausführung des Dienstes zuständig ist, ein Active Directory-Domänenadministratorkonto ist.

Um die erforderlichen Genehmigungen zu erteilen

1. Führen Sie **Services.msc** als Administrator aus.



2. Suchen Sie den Eintrag für den **GFI ClearView AD-Dienst**.
3. Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Anmelden** auf **Durchsuchen** und wählen Sie die Domäne und das Administratorkonto aus.

NOTE

The domain and slash (\) are required.

5. Geben Sie das **Passwort** ein und bestätigen Sie es.



6. Klicken Sie auf **OK** oder **Übernehmen**, um die Änderungen zu speichern.
7. Starten Sie den Dienst neu.

Installieren des GFI ClearView AD Connector

Gehen Sie wie folgt vor, um den GFI ClearView AD Connector zu installieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die Installationsanforderungen beachtet haben. [Weitere Informationen finden Sie unter Installieren des GFI ClearView AD Connector.](#)

So installieren Sie den Connector Service

1. Führen Sie auf dem Server, auf dem der GFI ClearView Active Directory Connector installiert werden soll, die Installationsdatei aus.

2. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und gehen Sie dann durch die Bildschirme, treffen Sie die unten angegebenen Auswahlen und klicken Sie bei Bedarf auf Weiter:

- Geben Sie das Verzeichnis an, in dem der GFI ClearView Active Directory Connector installiert werden soll.
- Wählen Sie aus, ob sich der Active Directory-Server auf **diesem** oder **einem anderen Server** befindet. Wenn der Connector nicht auf dem Server mit Active Directory installiert ist, geben Sie die IP-Adresse oder den Hostnamen des Active Directory-Servers sowie den Benutzernamen und das Passwort des Administratorkontos auf dem Active Directory-Server ein.

IMPORTANT

When the Active Directory server is running Windows Server, the GFI ClearView Active Directory Connector must be installed on the Active Directory server and cannot be installed on a remote server.

IMPORTANT

When installing the GFI ClearView AD Connector on a server that is not a domain controller, ensure that the account in charge of running the service is an Active Directory domain admin account. See *To ensure the GFI ClearView AD service has the appropriate permissions* below.

- Geben Sie optional die IP-Adresse oder den Hostnamen der GFI ClearView-Appliance, die Portnummer und das Administratorkennwort ein. Dieser Schritt ist optional, da Sie eine GFI ClearView Appliance auch nach der Installation von GFI ClearView Active Directory Connector hinzufügen können.
- Geben Sie im Feld **Include log entries newer than the specified age (Protokolleinträge einbeziehen, die jünger als das angegebene Alter sind)** das maximale Alter der Protokolleinträge (in Sekunden) an, die analysiert und an die GFI ClearView Appliance gesendet werden sollen, wenn der GFI ClearView Active Directory Connector-Dienst startet.

3. Wenn Warnungen angezeigt werden, beheben Sie die Probleme wie im Dialogfeld angegeben.

4. Klicken Sie auf **Installieren**. Stellen Sie sicher, dass **Launch GFI ClearView Active Directory Connector** ausgewählt ist, und klicken Sie auf **Finish**.

Nach Abschluss der Installation startet der GFI ClearView Active Directory Connector automatisch und versucht, mit der konfigurierten GFI ClearView-Appliance zu kommunizieren. Wenn Sie den GFI ClearView Active Directory Connector zum ersten Mal installieren, kann es 24 Stunden oder länger dauern, bis alle Zuordnungen von Benutzern zu IP-Adressen vorliegen, da sich die Benutzer nach und nach anmelden.

Hinzufügen der GFI ClearView Appliances zum GFI ClearView AD Connector

Identifizieren Sie die GFI ClearView Appliance, die diesen GFI ClearView AD Connector zum Abrufen von Benutzer- und Gruppeninformationen verwendet.

NOTE

Each installation of the Active Directory Connector can have a maximum of 20 GFI ClearView Appliances connected to it. If there are more than 20 GFI ClearView Appliances, install the connector on multiple Windows servers and divide the appliances across multiple instances of the Active Directory Connector.

Geben Sie im **GFI ClearView ADConfiguration Utility** auf der Registerkarte **GFI ClearView Appliances** die IP-Adresse und den Hostnamen jeder Appliance in eine leere Zeile ein. Außerdem müssen Sie für jede Appliance das **Admin-Kennwort** eingeben. Die Portnummer bezieht sich auf den Port, den der GFI ClearView AD Connector für die Kommunikation mit den Clients verwendet, und alle GFI ClearView Appliances müssen dieselbe Portnummer verwenden. Die Standard-Portnummer des Active Directory-Clients ist 8015.

Weitere [Informationen finden Sie unter Die Port-Nummer von GFI ClearView AD Connector](#).

Legen Sie im Feld **Sync-Intervall** fest, wie oft der GFI ClearView AD Connector die GFI ClearView Appliances kontaktiert, um Active Directory-Benutzer- und Gruppeninformationen zu synchronisieren. Der Standardwert ist 5 Minuten.

Die Nummer des Ports von GFI ClearView AD Connector

Standardmäßig wird der Port 8015 für die Kommunikation von Active Directory-Informationen zwischen dem GFI ClearView AD Connector und den angeschlossenen GFI ClearView Appliances verwendet. Sie sollten die Portnummer nur ändern, wenn ein Konflikt die Änderung erforderlich macht. Wenn Sie den Port auf dem Connector ändern, müssen Sie auch den Port auf jeder GFI ClearView Appliance ändern.

NOTE

Ensure that the firewall on the server running the GFI ClearView AD Connector is configured to allow inbound and outbound traffic on the configured port.

Ändern der Portnummer von GFI ClearView AD Connector

Falls erforderlich, können Sie die AD Connector-Portnummer anhand der folgenden Anweisungen ändern. Die Änderung der Portnummer muss sowohl auf dem Server, der den AD Connector hostet, als auch auf jeder GFI ClearView-Appliance vorgenommen werden.

So ändern Sie die Port-Nummer des GFI ClearView AD Connector

1. Starten Sie das **Dienstprogramm GFI ClearView ADConfiguration**.
2. Wählen Sie die Registerkarte **GFI ClearView Appliances**.
3. Geben Sie eine neue Portnummer in das Feld ein. Die Standardanschlussnummer ist 8015.

So ändern Sie die Port-Nummer auf jeder GFI ClearView-Appliance

1. Melden Sie sich bei der GFI ClearView Web UI an.
2. Klicken Sie auf **Konfiguration**, und wählen Sie in der Gruppe System die Option **Netzwerk> Active Directory**.
3. Geben Sie dieselbe Portnummer ein, die Sie oben im GFI ClearView AD Configuration Utility festgelegt haben.
4. Übernehmen Sie die Änderungen.
5. Wiederholen Sie diese Schritte für jede GFI ClearView Appliance, die mit dieser Instanz GFI ClearView AD Connector kommuniziert.

So ermitteln Sie, ob die Portänderung auf der GFI ClearView Appliance erfolgreich war

Warten Sie einige Augenblicke, um sicherzustellen, dass die Informationen auf der Registerkarte Active Directory mit neuen Informationen aktualisiert werden:

- » IPAdresse- Die IP-Adresse des Servers, auf dem der GFI ClearView AD Connector läuft.
- » **Windows-Version** - Die Version von Windows auf dem Active Directory-Server.
- » Version - Die Version von GFI ClearView AD Connector.
- » Agentenname - Der Name des GFI ClearView AD Connector.
- » **Letzter Kontakt** - Das letzte Mal, dass der Active Directory-Server kontaktiert wurde.

Wählen Sie die Informationen aus, die zwischen der GFI ClearView-Appliance und dem Active Directory-Server übertragen werden

Legen Sie fest, welche Informationen zwischen dem Active Directory-Server und der GFI ClearView-Appliance übertragen werden sollen. Wenn Sie den GFI ClearView AD Connector zum ersten Mal installieren, kann es eine Weile dauern, bis der Vorgang abgeschlossen ist

alle Zuordnungen von Benutzern zu IP-Adressen, da sich jeder Benutzer anmelden muss.

NOTE

User accounts that have been disabled on the Active Directory server are not included in the data sent to the GFI ClearView Appliances

1. Wechseln Sie im GFI ClearView AD Connector auf die Registerkarte **ADServer**.
2. Um beim Start des Dienstes eine Liste der Benutzer und Gruppen an die GFI ClearView-Appliances zu senden, wählen Sie **Active Directory-Benutzer- und Gruppeninformationen an GFI ClearView-Appliances senden**. Wenn diese Option nicht ausgewählt ist, stehen den GFI ClearView-Appliances nur angemeldete Benutzer zur Verfügung. Informationen über Gruppen sind nicht verfügbar. Diese Informationen werden über eine LDAP-Abfrage an den Active Directory-Server übermittelt.

CAUTION

If there are multiple domain controllers, Sending the users/groups to the GFI ClearView appliances on startup should only be selected on one of the domain controllers. For more information, refer to [GFI ClearView Appliance Reboots Every Night](#).

3. Um Benutzernamen in Überwachungsberichte aufzunehmen, lassen Sie die Analyse des Anmeldeverlaufs zu.
 - a. Um diese Option zu aktivieren, wählen Sie **Anmeldeverlauf analysieren und an die GFI ClearView-Appliance senden**. Diese Informationen werden über eine Abfrage des Windows-Ereignisprotokolls auf dem Active Directory-Server ermittelt.
 - b. Geben Sie im Feld **Include log entries newer than the specified age (Protokolleinträge einbeziehen, die jünger als das angegebene Alter sind)** das maximale Alter der Protokolleinträge (in Sekunden) an, die analysiert und an die GFI ClearView Appliance gesendet werden sollen, wenn der GFI ClearView AD Connector-Dienst startet.
4. Klicken Sie auf **OK**.

Identifizieren Sie den Active Directory Server

Der GFI ClearView AD Connector kann auf jedem Server im Netzwerk installiert werden, der Zugriff auf den Active Directory-Server hat. Wenn der Connector an einem anderen Ort als auf dem Active Directory-Server installiert wird, müssen Sie den Speicherort und die Authentifizierungsdaten des Active Directory-Servers angeben.

NOTE

You need to complete these instructions only if the Exinda AD Connector is NOT installed on the Active Directory server.

1. Starten Sie das Konfigurationsprogramm von GFI ClearView AD, und wechseln Sie zur Registerkarte AD-Server.
2. Wählen Sie **einen anderen Server** aus, und geben Sie dann die **IP-Adresse** oder den **Hostnamen** des Active Directory-Servers ein.
3. Um sich am Server zu authentifizieren, geben Sie den **Benutzernamen** und das **Kennwort** des Administratorkontos auf dem Active Directory-Server ein.

Überprüfen Sie die Kommunikation zwischen dem Active Directory Server und der ClearView Appliance

Um sicherzustellen, dass die Kommunikation zwischen dem Active Directory-Server und der GFI ClearView-Appliance erfolgreich verläuft, können Sie die Registerkarte Active Directory auf der GFI ClearView-Appliance schnell überprüfen. Melden Sie sich bei der GFI ClearView Web UI an. Klicken Sie auf **Konfiguration**, und wählen Sie in der Gruppe System die Option **Netzwerk > Active Directory**.

NOTE

User accounts that have been disabled on the Active Directory server are not included in the data sent to the GFI ClearView Appliances

Vergewissern Sie sich, dass der Active Directory-Server aufgeführt ist und dass der Dienst **ausgeführt wird**.

Wenn die GFI ClearView Appliance erfolgreich mit dem Active Directory-Client kommuniziert, werden die folgenden Informationen in der Tabelle angezeigt:

» Agentenname - Der Name des Active Directory-Servers. »

IPAdresse- Die IP-Adresse des Active Directory-Servers.

» Version - Die Windows-Client-Version von GFI ClearView Active Directory. »

Windows-Version - Die Windows-Version des Active Directory-Servers.

» Letzter Kontakt - Das letzte Mal, dass der Active Directory-Server kontaktiert wurde.

Wenn der Dienst nicht in der Liste angezeigt wird, führen Sie die Ereignisanzeige auf Ihrem Active Directory-Server aus, und überprüfen Sie die Windows-Protokolle:

1. Wählen Sie im Menü **Start** die Option **Systemsteuerung> Verwaltung**.
2. Doppelklicken Sie auf **Dienste**, und überprüfen Sie den Status des **GFI ClearView AD-Dienstes**. Wenn der Dienst angehalten wurde, starten Sie ihn neu.
3. Im Bereich **Windows-Protokolle> Anwendung** sollte eine Meldung "Dienst erfolgreich gestartet" von GFI ClearView Networks Active Directory Connector angezeigt werden.

Wenn die Kommunikation zwischen dem Active Director und der GFI ClearView Appliance fehlschlägt, wird in diesen Protokollen eine Fehlermeldung des GFI ClearView Networks Active Directory Connector angezeigt.

Anforderung aktualisierter Benutzer- und Gruppeninformationen vom Active Directory Server

Wenn die Liste der Benutzer und Gruppen, die den Active Directory-Client verwenden, zu sein scheint, löschen Sie alle Zuordnungen von Benutzernamen zu IP-Adressen und aktualisieren Sie die vom Active Directory-Server gesendete Liste.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration> System> Netzwerk**, und wechseln Sie auf die Registerkarte **Active Directory**.
6. Um die Benutzer-, Gruppen- und Anmeldedaten von der Appliance zu löschen und eine Aktualisierung von den Active Directory-Clients anzufordern, klicken Sie auf **Renumerate**.

Ändern Sie den Status des GFI ClearView AD Connector

Halten Sie die Active Directory-Integration vorübergehend an oder deaktivieren Sie sie, um die Fehlersuche zu erleichtern und Fehler beim Ändern der Einstellungen von GFI ClearView AD Connector zu vermeiden.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration> System> Netzwerk**, und wechseln Sie auf die Registerkarte **Active Directory**.
6. Ändern Sie den Status des Active Directory-Dienstes.

Dienstleistung.

- Um den GFI ClearView AD Connector vorübergehend anzuhalten, klicken Sie auf Anhalten.
- Wenn Sie Probleme mit dem ClearView AD Connector haben, starten Sie den
- Wenn Sie GFI ClearView AD Connector nicht mehr benötigen, klicken Sie auf Deaktivieren.
- Wenn der Dienst deaktiviert wurde, klicken Sie auf Aktivieren, um ihn wieder zu starten.

Bestimmte Benutzernamen von Berichten ausschließen

Möglicherweise verfügen Sie über Benutzerkonten, die bei der Berichterstellung auf der GFI ClearView Appliance nicht mit IP-Adressen verknüpft werden sollten, wie z. B. das Konto, das für die Signatur des SMB-Datenverkehrs verwendet wird. Konfigurieren Sie den GFI ClearView AD Connector so, dass die Zuordnung von IP-Adressen zu Benutzernamen nicht an die GFI ClearView Appliance gesendet wird.

Bevor Sie beginnen...

Sie müssen den Prozess verstehen:

- » Anfordern von aktualisierten Benutzer- und Gruppeninformationen von Active Directory. Weitere Informationen finden Sie unter [Anfordern aktualisierter Benutzer- und Gruppeninformationen vom Active Directory-Server](#).
- » Starten Sie den Active Directory-Dienst neu. [Weitere Informationen finden Sie unter Ändern des Status des GFI ClearView AD Connector](#).

So schließen Sie Benutzernamen aus

1. Klicken Sie im Menü **Start** auf **Alle Programme > ClearView Networks > ClearView ADConfiguration Utility**.
2. Wählen Sie die Registerkarte **Ausgeschlossene Benutzer**.
3. Klicken Sie in den Bereich **Ignorierte Benutzer** und geben Sie den vollständigen Benutzernamen jedes zu ignorierenden Benutzers ein. Bei Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden. Wenn das Active Directory den Benutzer Domain/Test.User enthält und die Ausschlussliste den Benutzer als Domain/Test.User enthält, wird der Datenverkehr nicht ausgeschlossen.

NOTE

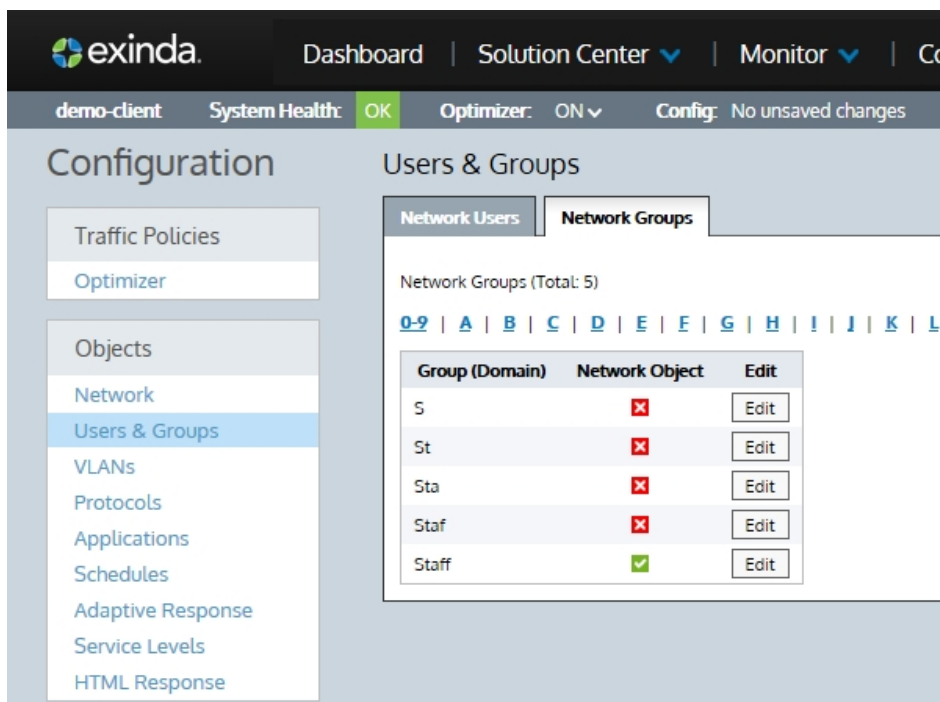
Regardless of the case of usernames in Active Directory, the ClearView Appliance displays the usernames with the first name capitalized and the surname in lower case; for example Domain/Test.user. Do not use the value in the ClearView Appliance when adding a username to the Excluded list.

4. Klicken Sie auf **Anwenden**.
5. Anforderung aktualisierter Benutzer- und Gruppeninformationen vom Active Directory-Server.
6. Starten Sie den Active Directory-Dienst neu.

Verwendung von Adaptive Response mit Active Directory

Im letzten Beispiel wurde ein statisches Netzwerkobjekt als Quelle für IPs verwendet. Es ist auch möglich, ein dynamisches Netzwerkobjekt, das von einer Active Directory-Gruppe zugeordnet wurde, als Quelle zu verwenden.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration > Objekte > Benutzer & Gruppen**.
6. Klicken Sie auf **Bearbeiten**, um die gewünschte Benutzergruppe zu bearbeiten.



7. Aktivieren Sie die Optionen **Auf Netzwerkobjekt zuordnen** und **Domäne ignorieren**.

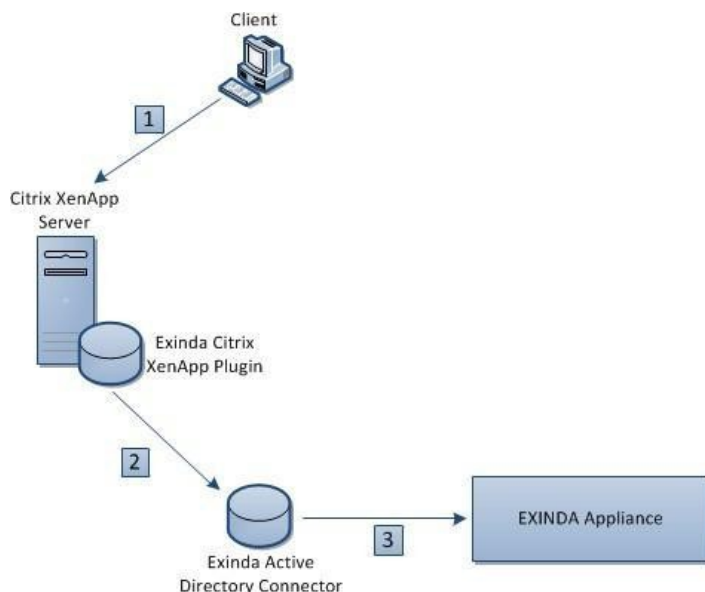
8. Klicken Sie auf **Anwenden**.

Es wird ein Netzwerkobjekt mit einem Namen ähnlich dem Namen der Benutzergruppe erstellt, das alle IPs in der Active Directory-Gruppe "Student" enthält. Dieses Netzwerkobjekt kann bei der Erstellung einer Regel für die adaptive Reaktion genau wie im vorherigen Beispiel verwendet werden.

Identifizierung von Nutzern

Ein Citrix XenApp-Server hostet einen virtuellen Desktop mit vorinstallierter Software, auf die Benutzer mit den richtigen Anmeldedaten bei Bedarf zugreifen können. Auf diese Weise kann das Unternehmen Zugang zu häufig genutzter Software bieten, ohne dass die Installationen auf jedem Client-Computer im Netzwerk gewartet und aktualisiert werden müssen.

Da der Citrix XenApp-Server von der GFI ClearView-Appliance als eine einzige IP-Adresse behandelt wird und die IP-Adressen der Clients, die eine Verbindung zum Server herstellen, ignoriert werden, kann die GFI ClearView-Appliance die Namen der Benutzer, die auf die Anwendungen auf dem XenApp-Server zugreifen, nicht aufnehmen.



Wenn sich ein Benutzer auf einem Client-Computer bei einem Citrix XenApp-Server (1) anmeldet, werden seine IP-Adresse und sein Benutzername vom GFI ClearView Citrix XenApp Plugin erfasst und an den GFI ClearView AD Connector (2) weitergeleitet. Der Connector sendet dann den Benutzernamen und die des XenApp-Benutzers an die GFI ClearView Appliance, um sie in Berichte aufzunehmen (3).

Installieren und konfigurieren Sie das GFI ClearView Citrix XenApp Plugin, um Aktivitäten bestimmter Benutzer auf dem XenApp-Server zu erkennen.

Installieren Sie das GFI ClearView Citrix XenApp Plugin

Das GFI ClearView Citrix XenApp Plugin sendet die IP-Adresse und den Benutzernamen des Benutzers, der die Anwendung auf dem XenApp-Server verwendet, an den GFI ClearView AD Connector, damit die Benutzernamen in Berichten auf den GFI ClearView Appliances angezeigt werden können. Das GFI ClearView Citrix XenApp Plugin muss auf jedem Citrix XenApp-Server im Netzwerk installiert werden.

NOTE

The GFI ClearView Citrix XenApp Plugin is supported on Citrix XenApp Servers version 6.0.

1. Laden Sie das Installationsprogramm für die GFI ClearView-Appliance herunter.
 - a. Klicken Sie auf **Konfiguration > System > Netzwerk**, und wechseln Sie auf die Registerkarte **Active Directory**.
 - b. Laden Sie die **ausführbare Datei des Microsoft-Installationsprogramms** herunter.
2. Speichern Sie die Installation des GFI ClearView Citrix XenApp Plugin an einem Speicherort, auf den Citrix XenApp-Server zugreifen kann.
3. Suchen Sie auf dem Server, auf dem das GFI ClearView Citrix XenApp Plugin installiert werden soll, die Installationsdatei, und doppelklicken Sie darauf.
4. Klicken Sie im Dialogfeld Willkommen auf **Weiter**.
5. Geben Sie das Verzeichnis an, in dem das GFI ClearView Citrix XenApp Plugin installiert werden soll, und klicken Sie auf **Nächste**.
6. Lesen Sie die Endbenutzer-Lizenzvereinbarung. Wählen Sie **Ich stimme zu** und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Weiter**, um die Installation zu bestätigen. Das GFI ClearView Citrix XenApp Plugin wird installiert.
8. Wenn die Installation abgeschlossen ist, klicken Sie auf **Schließen**.

Hinzufügen des GFI ClearView AD Connector zum GFI ClearView Citrix XenApp Plugin

Um sicherzustellen, dass Benutzeraktivitäten auf dem Citrix XenApp-Server auf der GFI ClearView-Appliance gemeldet werden, fügen Sie die Verbindungsdetails für den GFI ClearView AD Connector zum GFI ClearView Citrix XenApp Plugin hinzu.

1. Öffnen Sie das GFI ClearView Citrix XenApp Plugin.
2. Wählen Sie die Registerkarte **Synchronisierung** und doppelklicken Sie auf den Bereich **Speicherort** in der ersten leeren Zeile.
3. Geben Sie die IP-Adresse oder den Hostnamen und die Portnummer des Computers ein, auf dem der GFI ClearView AD Connector installiert ist.

NOTE

The port number used to communicate between the GFI ClearView AD Connector and the GFI ClearView Citrix XenApp Plugin cannot be the same as the port number used to communicate between the GFI ClearView AD Connector and the GFI ClearView Appliances.

4. Legen Sie im Feld **Synchronisierungsintervall** fest, wie oft GFI ClearView AD Connector die Daten sendet.

XenApp-Server-Benutzerinformationen an den GFI ClearView AD Connector. Der Standardwert ist 1 Minute.

5. Klicken Sie auf **Anwenden**.

Aufzeichnung der GFI ClearView Citrix XenApp Plugin-Aktivitäten in einer Log Datei

Je nach gewählter Protokollierungsstufe zeichnet das GFI ClearView Citrix XenApp Plugin verschiedene Arten von Daten in einer Protokolldatei auf. Die verfügbaren Protokollebenen umfassen Fehler, Warnung, Info und Ausführlich. Standardmäßig ist die Protokollempfindlichkeit Warnung. Der Speicherort der Protokolldatei und die Detailstufe, die in der Protokolldatei aufgezeichnet wird, sind konfigurierbar.

1. Öffnen Sie das GFI ClearView Citrix XenApp Plugin.
2. Geben Sie auf der Registerkarte **ADServer** den Ort an, an dem die Protokolldateien gespeichert werden sollen.
3. Wechseln Sie zur Registerkarte "**Konsole**" und wählen Sie unter "**Protokollempfindlichkeit**" die Ebene der Meldungen aus, die in der Protokolldatei aufgezeichnet werden.
Liste.
4. Klicken Sie auf **Anwenden**.
5. Um den Inhalt des Protokolls anzuzeigen, klicken Sie auf der Registerkarte **Konsole** auf **Protokoll öffnen**.

Ändern Sie die Nummer des GFI ClearView Citrix XenApp Plugin Port

Geben Sie den Port an, über den der GFI ClearView AD Connector mit den angeschlossenen GFI ClearView Citrix XenApp Plugins kommuniziert. Die Standardportnummer ist 8016.

Schritt 1: Ändern Sie die Port-Nummer für das GFI ClearView Citrix XenApp Plugin.

1. Klicken Sie im Menü **Start** auf **Alle Programme > ClearView Networks > ClearView Citrix XenApp Plugin Configuration**.
2. Wechseln Sie zur Registerkarte **Synchronisierung**.
3. Doppelklicken Sie auf die Portnummer für den entsprechenden GFI ClearView AD Connector, und geben Sie die neue Portnummer in das Feld ein.
4. Klicken Sie auf **OK**.

Schritt 2: Ändern Sie die Port-Nummer auf dem GFI ClearView AD Connector.

1. Klicken Sie im Menü **Start** auf **Alle Programme > ClearView Networks > ClearView ADConfiguration Utility**.
2. Wechseln Sie zur Registerkarte **XenApp**.
3. Geben Sie die Anschlussnummer in das Feld ein.
4. Klicken Sie auf **OK**.

Abfrage aktualisierter Benutzerinformationen über das GFI ClearView Citrix XenApp Plugin

Wenn die Benutzerdaten zwischen dem GFI ClearView Citrix XenApp Plugin und GFI ClearView AD Connector nur selten synchronisiert werden, veranlassen Sie das GFI ClearView Citrix XenApp Plugin, die Daten sofort an den GFI ClearView AD Connector zu senden.

1. Klicken Sie im Menü **Start** auf **Alle Programme > ClearView Networks > ClearView ADConfiguration Utility**.
2. Wechseln Sie zur Registerkarte **XenApp**.
3. Klicken Sie auf **Renumerieren**.

Die aktuellen Daten werden vom GFI ClearView Citrix XenApp Plugin an den GFI ClearView AD Connector gesendet.

Hinzufügen einer neuen Anwendung

Gehen Sie wie folgt vor, um eine neue Anwendung hinzuzufügen.

1. Klicken Sie auf Konfiguration > Objekte> Anwendungen> Anwendungen.
2. Geben Sie im Bereich **Neue Anwendung hinzufügen** einen Namen für die neue Anwendung ein. Definieren Sie eine Anwendung, die auf einem der folgenden Punkte basiert:
 - L7 Unterschrift
 - L7-Signatur + Ports oder Protokolle
 - Netzwerkobjekt + Ports oder Protokolle
 - Netzwerk-Objekt
 - Ports oder Protokolle

NOTE

Network objects cannot be used in conjunction with a layer 7 signature.

3. Wählen Sie das **Netzwerkobjekt** für die Anwendung aus. Wenn das Netzwerkobjekt intern ist, wird der in das LAN eingehende Verkehr mit dem Netzwerkobjekt als Ziel dieser Anwendung zugeordnet, und der aus dem LAN ausgehende Verkehr mit dem Netzwerkobjekt als Quelle dieser Anwendung zugeordnet. Wenn das Netzwerkobjekt extern ist, wird der in das LAN eingehende Verkehr mit dem Netzwerkobjekt als Quelle dieser Anwendung zugeordnet, und der aus dem LAN ausgehende Verkehr mit dem Netzwerkobjekt als Ziel dieser Anwendung zugeordnet.

4. Wählen Sie die **L7-Signatur** für die Anwendung. Einige Layer 7-Signaturen haben zusätzliche Optionen, die es Ihnen ermöglichen, Anwendungsobjekte auf der Grundlage bestimmter Teile dieser L7-Signatur zu definieren. Wenn eine Layer-7-Signatur ausgewählt ist, geben Sie die Parameter für die Signatur

EXAMPLE

To create an application object that matches traffic to and from the Exinda.com website, in the **L7 Signature** field, select **http --->**, **host**, and type **exinda.com**.

an.

5. In den Steuerelementen **Ports/Protocols** geben Sie entweder TCP-Ports/Portbereiche, UDP-Ports/Portbereiche oder ein Layer-3-Protokoll an. Mehrere Ports und Portbereiche können angegeben werden, indem die Werte durch Kommata getrennt werden.
6. Klicken Sie auf die Schaltfläche **Neue Anwendung hinzufügen**.

Welche L7-Signaturoptionen gibt es ?

Einige Layer-7-Signaturen verfügen über zusätzliche Optionen, mit denen Sie Anwendungsobjekte auf der Grundlage bestimmter Teile dieser L7-Signatur definieren können. Bei der Konfiguration eines neuen Anwendungsobjekts bieten die L7-Signaturen, auf die in der Dropdown-Liste ein "--->" folgt, zusätzliche Optionen. Die meisten bieten Optionen, die Sie einfach auswählen. Einige erfordern eine Auswahl und zusätzliche Informationen. In der folgenden Tabelle werden die verschiedenen Optionen erläutert, die mehr als nur die Auswahl einer Option erfordern.

NOTE

Citrix-based sub-types are no longer supported.

Layer 7 Signature	Sub-Type	Description
Blitzlicht	Gastgeber	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Feldes "host" in der Datei HTTP-Header (wenn Flash über http läuft).

http	inhalts_type	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Feldes "Content-Type" im HTTP-Header.																					
	Akteno	Ermöglicht Ihnen die Definition eines Anwendungsobjekts auf der Grundlage des in der HTTP-URL angeforderten Dateinamens																					
	rdner	Ermöglicht es Ihnen, ein Anwendungsobjekt auf der Grundlage des Feldes "host" im HTTP-Header zu definieren.																					
	Methode	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage der HTTP-Methode (z. B. GET PUT HEAD DELETE).																					
	user_agent	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Feldes "user-agent" im HTTP-Header.																					
	advanced	<p>Definieren Sie benutzerdefinierte Kriterien mit der folgenden Syntax:</p> <p>" Ein String-Literal ist in Anführungszeichen(") eingeschlossen.</p> <p>" Ein Backslash kann in die Zeichenkette eingefügt werden, indem er durch einen weiteren Backslash ersetzt wird</p> <p>" Die Schlüsselwörter sind einfach (common_name) ohne Anführungszeichen.</p> <p>" Schlüsselwörter sind "bare" (host) ohne Anführungszeichen</p> <p>Gruppierung wird durch Klammern unterstützt</p> <p>* Unterstützte Operatoren sind oder und und und hat einen höheren Vorrang als oder</p> <p>* Die verfügbaren Vergleichsoperatoren sind:</p>																					
	Dwription	<table border="1"> <thead> <tr> <th></th> <th>sMe</th> <th>Exemplarisch</th> </tr> </thead> <tbody> <tr> <td>equa</td> <td><Stichwort> <Wert></td> <td>Host "Beispiel.com"</td> </tr> <tr> <td>dces nicht gleich</td> <td><Stichwort> <Wert></td> <td>Host "Beispiel.com"</td> </tr> <tr> <td>enthält Teilstring</td> <td><Stichwort> =8 <Wert></td> <td>host =% "beispiel.de"</td> </tr> <tr> <td>dces enthält keine Teilzeichenfolge</td> <td>Ake ord> !8 <Wert></td> <td>host !% "example.com"</td> </tr> <tr> <td>Die rechte Seite ist ein regulärer Ausdruck und entspricht der gesamten linken Seite</td> <td>4keywozd4 <Wert></td> <td>Gastgeber == "Beispiel.*"</td> </tr> <tr> <td>Die rechte Seite ist ein regulärer Ausdruck und rt> stimmt nicht mit der vollständigen linken Seite überein</td> <td><Schlüsselwo <Wert></td> <td>host !- "Beispiel.*"</td> </tr> </tbody> </table>		sMe	Exemplarisch	equa	<Stichwort> <Wert>	Host "Beispiel.com"	dces nicht gleich	<Stichwort> <Wert>	Host "Beispiel.com"	enthält Teilstring	<Stichwort> =8 <Wert>	host =% "beispiel.de"	dces enthält keine Teilzeichenfolge	Ake ord> !8 <Wert>	host !% "example.com"	Die rechte Seite ist ein regulärer Ausdruck und entspricht der gesamten linken Seite	4keywozd4 <Wert>	Gastgeber == "Beispiel.*"	Die rechte Seite ist ein regulärer Ausdruck und rt> stimmt nicht mit der vollständigen linken Seite überein	<Schlüsselwo <Wert>	host !- "Beispiel.*"
	sMe	Exemplarisch																					
equa	<Stichwort> <Wert>	Host "Beispiel.com"																					
dces nicht gleich	<Stichwort> <Wert>	Host "Beispiel.com"																					
enthält Teilstring	<Stichwort> =8 <Wert>	host =% "beispiel.de"																					
dces enthält keine Teilzeichenfolge	Ake ord> !8 <Wert>	host !% "example.com"																					
Die rechte Seite ist ein regulärer Ausdruck und entspricht der gesamten linken Seite	4keywozd4 <Wert>	Gastgeber == "Beispiel.*"																					
Die rechte Seite ist ein regulärer Ausdruck und rt> stimmt nicht mit der vollständigen linken Seite überein	<Schlüsselwo <Wert>	host !- "Beispiel.*"																					
		<p>* Reguläre Ausdrücke verwenden die Perl-Syntax</p> <p>* Die Schlüsselwörter für HTTP sind: host, file, user_agent, content_type, method, content_len und encoding</p> <p>E "mper</p> <p>* (url =8 "index" oder Datei =% "login") und host =% "example.org" und content_type.case= "MyContentType" " (Host =8 "facebook.com" und Datei !% "cgi-bin/abcd") oder Host =% "facebook2.com"</p>																					

Unter-Tytae

mpeg	Gastgeber	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Feldes "host" im HTTP-Header (wenn mpeg über http läuft).																					
quicktime	Gastgeber	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Feldes "host" im HTTP-Header (wenn Quicktime über HTTP läuft).																					
silverlight	Gastgeber	Ermöglicht die Definition eines Application Objects basierend auf Feld "host" im HTTP-Header (wenn silverlight über http läuft).																					
ssl	gemeinsamer_Name	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Feldes "Common Name" im SSL-Zertifikat.																					
	erweiterte	<p>Definieren Sie benutzerdefinierte Kriterien mit der folgenden Syntax:</p> <ul style="list-style-type: none"> " Ein String-Literal ist in Anführungszeichen (") eingeschlossen. " Interne Anführungszeichen können mit dem Zeichen backslash (\) escaped werden. " Ein Backslash kann in die Zeichenkette eingefügt werden, indem er durch einen weiteren Backslash ersetzt wird <p>* Schlüsselwörter sind bloße (common_name) ohne Anführungszeichen.</p> <p>" Die Gruppierung wird durch Klammern unterstützt</p> <p>Die unterstützten Operatoren sind OR und AND. AND hat einen höheren Vorrang als OR.</p> <p>" Die Schlüsselwörter für SSL sind common_name (cn) und organization_name (o)</p> <p>" Die verfügbaren Vergleichsoperatoren sind:</p> <table border="1"> <thead> <tr> <th>Dez:ription</th> <th>SMS</th> <th>Beispiel</th> </tr> </thead> <tbody> <tr> <td>ist gleich</td> <td><Schlüsselwort> <Wert></td> <td>gemeinsamer_name "John"</td> </tr> <tr> <td>ist nicht gleich</td> <td>!<Schlüsselwort> <Wert></td> <td>gemeinsamer_name "John"</td> </tr> <tr> <td>enthält Teilstring</td> <td><Schlüsselwort> common_name =% =<Wert></td> <td>"Johannes"</td> </tr> <tr> <td>ist nicht Teilstring</td> <td>!<Schlüsselwort> common_name != =<Wert></td> <td>"John"</td> </tr> <tr> <td>Die rechte Seite ist ein regulärer Ausdruck und lautet</td> <td><Stichwort></td> <td>common_name =~ "John*"</td> </tr> <tr> <td>die vollständige linke Seite</td> <td><Wert></td> <td></td> </tr> </tbody> </table> <p>¹ Reguläre Ausdrücke verwenden die Perl-Syntax</p>	Dez:ription	SMS	Beispiel	ist gleich	<Schlüsselwort> <Wert>	gemeinsamer_name "John"	ist nicht gleich	!<Schlüsselwort> <Wert>	gemeinsamer_name "John"	enthält Teilstring	<Schlüsselwort> common_name =% =<Wert>	"Johannes"	ist nicht Teilstring	!<Schlüsselwort> common_name != =<Wert>	"John"	Die rechte Seite ist ein regulärer Ausdruck und lautet	<Stichwort>	common_name =~ "John*"	die vollständige linke Seite	<Wert>	
Dez:ription	SMS	Beispiel																					
ist gleich	<Schlüsselwort> <Wert>	gemeinsamer_name "John"																					
ist nicht gleich	!<Schlüsselwort> <Wert>	gemeinsamer_name "John"																					
enthält Teilstring	<Schlüsselwort> common_name =% =<Wert>	"Johannes"																					
ist nicht Teilstring	!<Schlüsselwort> common_name != =<Wert>	"John"																					
Die rechte Seite ist ein regulärer Ausdruck und lautet	<Stichwort>	common_name =~ "John*"																					
die vollständige linke Seite	<Wert>																						
	organisation_name	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des Namensfeldes "Organisation" im SSL-Zertifikat.																					
	spdy	Dieses Feld sollte leer bleiben, da alle hier eingegebenen Werte ignoriert werden.																					
rtp	Codec	Ermöglicht die Definition eines Anwendungsobjekts auf der Grundlage des in einem RTP-Stream verwendeten "Codec".																					
windowsmedia	Host	Ermöglicht die Definition eines Application Objects basierend auf dem Feld "host" im HTTP-Header (wenn windowsmedia über http läuft).																					

Beispiel: Erstellen einer benutzerdefinierten Anwendung auf der Grundlage des Protokolls HTTPS

Ermitteln Sie den allgemeinen Namen der (https) SaaS-Site und erstellen Sie eine Anwendung unter Verwendung der ssl L7-Signatur mit dem allgemeinen Namen.

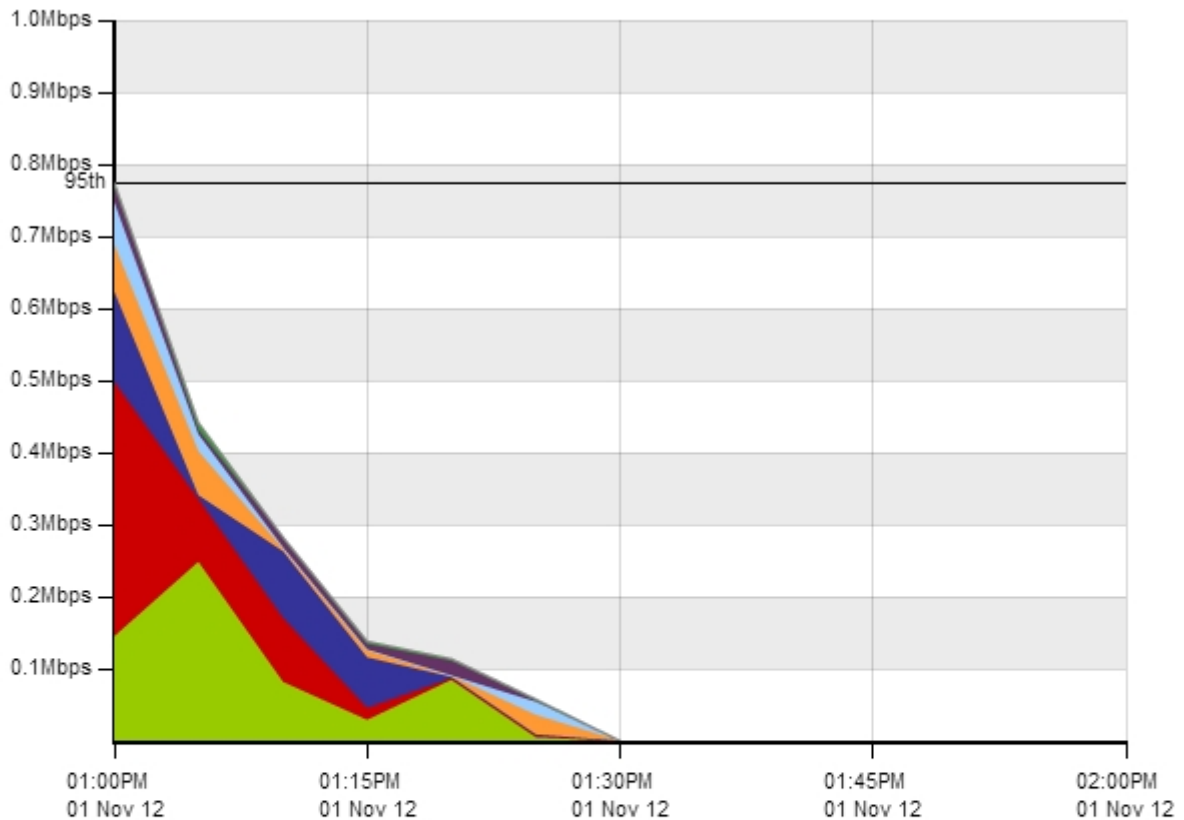
1. Gehen Sie zu der Website, die Sie interessiert.
2. Klicken Sie in der Adressleiste der meisten Browser auf https oder das Schloss-Symbol.
3. Zeigen Sie die Zertifikatsdetails an.
4. Kopieren Sie den in den Zertifikatsdetails angegebenen Common Name.
5. Gehen Sie zu Konfiguration > Objekte> Anwendungen.
6. Wählen Sie im Feld **L7-Signatur 'ssl --- '**.
7. Wählen Sie Feld neben der L7-Signatur den **allgemeinen Namen**.
8. Geben Sie den allgemeinen Namen der Website, den Sie aus dem Zertifikat erhalten haben, in den Browser ein.

Die wichtigsten internen und externen Benutzer im Netzwerk

Die Berichte "Netzwerk - Benutzer (intern)" und "Benutzer (extern)" zeigen die wichtigsten Benutzer an, die Datenverkehr durch das Netzwerk senden.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
 2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
 3. Klicken Sie auf **Anmelden**.
 5. Klicken Sie auf **Monitor> Netzwerk**.
 6. Wählen Sie in der Liste Auswahl der anzuzeigenden Grafik die Option **Benutzer - Intern** oder **Benutzer - Extern**.
 7. Legen Sie den Zeitraum fest, der im Bericht berücksichtigt werden soll. Weitere Informationen finden Sie unter [Festlegen des Zeitraums für einen Bericht](#). Nachdem der Datumsbereich ausgewählt wurde, werden die Diagramme und Tabellen sofort aktualisiert.
 8. Entfernen Sie bestimmte Arten von Datenverkehr aus dem Diagramm, indem Sie das entsprechende Kontrollkästchen in der Legende unter dem Diagramm deaktivieren.
 9. Um zu bestimmen, auf welche Größe Ihre WAN-Verbindung konfiguriert werden sollte, **wählen** Sie aus dem Dialogfeld **Perzentilmarker für die Anzeige auswählen** Wählen Sie die **95**.
- Verwenden Sie die 95. Perzentilmarke für die Durchsatzgeschwindigkeit, um Ihre WAN-Verbindung zu konfigurieren.

Throughput for Top 10 Inbound Users - Internal LAN



	Name	Total Data (MB)	Throughput Max (Mbps)	Throughput Avg (Mbps)
<input checked="" type="checkbox"/>	EXANET\Brad	8.866	0.249	0.020
<input checked="" type="checkbox"/>	EXANET\Dale	14.765	0.354	0.033
<input checked="" type="checkbox"/>	EXANET\Jan	9.689	0.125	0.022
<input checked="" type="checkbox"/>	EXANET\Micheal	4.834	0.065	0.011
<input checked="" type="checkbox"/>	EXANET\Ian	0.228	0.008	0.001
<input checked="" type="checkbox"/>	EXANET\Vince	0.152	0.002	0.000

4.2 System Einrichtung

Erfahren Sie, wie Sie Ihre GFI ClearView-Appliance(s) einrichten. Die bereitgestellten Konfigurationsinformationen beziehen sich auf die Appliance und nicht auf die GFI ClearView-Firmware.

4.2.1 Datum und Uhrzeit Konfiguration

Es ist wichtig, das Datum und die Uhrzeit der GFI ClearView-Appliance genau einzustellen, damit alle zeitbasierten Funktionen die richtige Zeit verwenden. Es wird dringend empfohlen, das Datum und die Uhrzeit mit Hilfe eines NTP-Servers einzustellen. Dies ist besonders wichtig, wenn Sie mehrere GFI ClearView-Appliances einsetzen wenn Sie die Überwachungsdaten korrelieren oder aggregieren müssen oder wenn Sie die exportierten NetFlow-Datensätze mit NetFlow-Datensätzen von anderen Netzwerk-Appliances synchronisieren müssen.

Es wird empfohlen, das Datum und die Uhrzeit mit Hilfe eines oder mehrerer NTP-Server einzustellen. Je mehr NTP-Server konfiguriert werden, desto genauer wird die Zeit sein. Es ist allgemein anerkannt, dass vier

NTP-Servern ist die optimale Anzahl von Servern für eine extrem genaue Zeit. Eine Erklärung, warum vier NTP-Server als optimale Anzahl von Servern angesehen werden, finden Sie unter <http://www.ntp.org/ntpfaq/NTP-s-algo-real.htm>

Eine gute Quelle für NTP-Server ist das NTP-Pool-Projekt unter <http://www.pool.ntp.org/en/use.html>.

Die Einstellung von Datum und Uhrzeit hat Auswirkungen auf die folgenden Funktionen:

- » Überwachungsdaten sind mit Zeitstempeln versehen, und die Überwachungsdiagramme werden relativ zu diesen» Zeitstempeln berichtet Exportierte NetFlow-Datensätze haben Zeitstempel
- » Zeitplanbasierte Richtlinien müssen zu den richtigen Zeitpunkten in Kraft treten
- » Geplante Ereignisse, wie z. B. geplante Berichte oder geplante Aufträge, müssen zu geeigneten Zeiten stattfinden.

Wenn die aktuelle Zeit auf der Appliance nicht mit der von NTP-Servern gelieferten Datumszeit übereinstimmt, passen die NTP-Server die Uhrzeit langsam an. Wenn die Zeit der Appliance erheblich von der Synchronisation mit den NTP-Servern abweicht (z. B. 1000 Sekunden oder etwa 15 Minuten), sollten Sie die Appliance zwingen, mit dem Befehl ntpd aus der Befehlszeile auf die korrekte Zeit zu springen.

Wo kann ich diese Konfiguration finden?

Gehen Sie zu **Konfiguration >System> Setup> Datum und Uhrzeit**.

So stellen Sie das Datum und die Uhrzeit mit einem NTP-Server ein

NTP Servers			
	Server	Version	Enabled
<input type="checkbox"/>	0.pool.ntp.org	4	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1.pool.ntp.org	4	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2.pool.ntp.org	4	<input checked="" type="checkbox"/>
<input type="checkbox"/>	3.pool.ntp.org	4	<input checked="" type="checkbox"/>

Remove Server

Enable Server

Disable Server

Add New NTP Server	
Server address	<input type="text"/>
Version	<input type="text" value="4"/>
Enabled	<input type="checkbox"/>

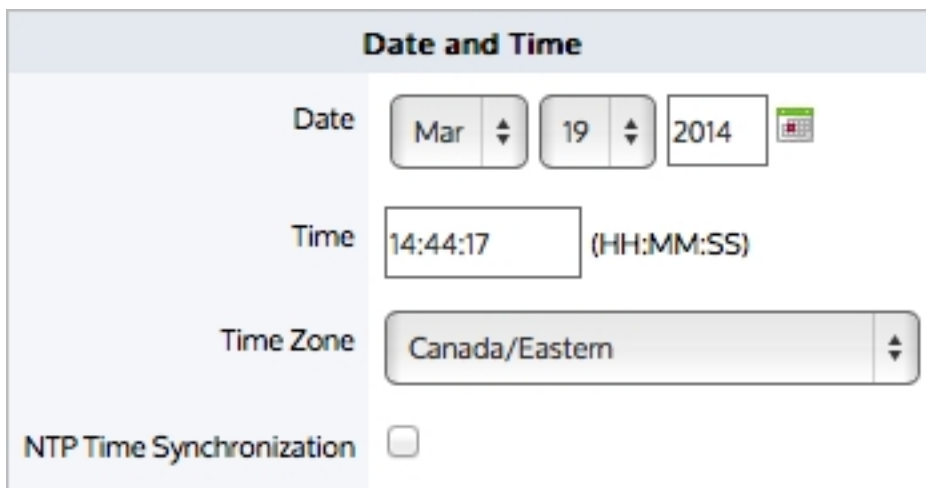
Add New NTP Server

1. Fügen Sie einen oder mehrere NTP-Server hinzu, indem Sie die IP-Adresse oder den Hostnamen des NTP-Servers sowie die vom Server unterstützte NTP-Version eingeben und ihn durch Aktivieren des Kontrollkästchens "Aktivieren" im Bereich "Neuen NTP-Server hinzufügen" aktivieren. Es werden nur Hostnamen und IPv4-Adressen unterstützt.
2. Aktivieren Sie im Bereich Datum und Uhrzeit das Kontrollkästchen **NTPTIME-Synchronisation** und **übernehmen Sie die Änderungen**.



Die Änderung wird nur übernommen, wenn Sie die Meldung Neustart akzeptieren, um die Benutzeroberfläche neu zu starten. Jeder der NTP-Server kann deaktiviert, wieder aktiviert oder entfernt werden, indem Sie auf die entsprechende Schaltfläche klicken - **Server deaktivieren**, **Server aktivieren**, **Server entfernen**.

So stellen Sie das Datum und die Uhrzeit manuell ein



1. Vergewissern Sie sich im Bereich Datum und Uhrzeit, dass das Kontrollkästchen **NTPTIME-Synchronisation** nicht aktiviert ist.
2. Stellen Sie das gewünschte Datum, die Uhrzeit und die Zeitzone ein und klicken Sie auf **Änderungen übernehmen**.

WARNING
 If you change the time manually, you will be prompted to restart the UI. If you do not accept the Restart, the configuration change is not applied. If the NTP Time Synchronization checkbox is checked, then the manual date-time setting will not be applied.

So erzwingen Sie eine Zeitrückstellung, wenn die Zeit erheblich von der Synchronisation abweicht

Geben Sie in die Befehlszeile ein: `ntpdate <ntp-server-address>`

- `<ntp-server-address>` - Der Standort eines NTP-Servers, angegeben als Hostname oder IPv4/IPv6-Adresse.

Dieser Befehl ist dem veralteten Befehl `ntpdate` ähnlich.

4.2.2 UI Zugriff Konfiguration

Auf der Seite Zugriff können Sie festlegen, wie lange die Web-Benutzeroberfläche der Appliance inaktiv sein darf, bevor der Benutzer automatisch wird. In ähnlicher Weise können Sie festlegen, wie lange die CLI inaktiv sein darf, bevor sie abgemeldet wird. Sie können angeben, ob Sie den http- oder https-Zugang aktivieren und welche Portnummern verwendet werden sollen. Falls gewünscht, können Sie die Web-Benutzeroberfläche auch ganz deaktivieren. Sie können festlegen, ob der CLI-Zugriff über Telnet oder SSH erfolgt.

NOTE

Once you disable the Web UI, you can only re-enable it via the CLI.

Web UI Options	
Web UI	<input checked="" type="checkbox"/> Enable
Auto Logout Timeout	<input type="text" value="0"/> minutes
HTTP Access	<input type="checkbox"/> Enable
HTTP Port	<input type="text" value="80"/>
HTTPS Access	<input checked="" type="checkbox"/> Enable
HTTPS Port	<input type="text" value="443"/>
Web Session Renewal	<input type="text" value="60"/> minutes
Web Session Timeout	<input type="text" value="1440"/> minutes

Screenshot 224: Web-UI-Optionen zur Einstellung des HTTP- oder HTTPS-Zugriffs, des Zeitraums für die automatische Abmeldung und zur Deaktivierung der Web-UI

CLI Options	
Auto Logout Timeout	<input type="text" value="900"/> seconds
Telnet Access	<input type="checkbox"/> Enable
SSH Access	<input checked="" type="checkbox"/> Enable
SSH Version	<input type="text" value="SSH v2 or v1"/>

Screenshot 225: CLI-Optionen zum Einstellen des Telnet- oder SSH-Zugangs und des Zeitlimits für die automatische Abmeldung

So konfigurieren Sie die Web-Benutzeroberfläche so, dass sie sich nach einer bestimmten Leerlaufzeit automatisch abmeldet

1. Vergewissern Sie sich, dass das Kontrollkästchen **Web UI Enable** aktiviert ist.
2. Legen Sie die Zeitspanne für **die automatische Abmeldung** auf die angegebene Anzahl von Minuten fest, die der Benutzer inaktiv sein kann, bevor er automatisch abgemeldet wird. Um das System so zu konfigurieren, dass es sich nie automatisch abmeldet, setzen Sie das Feld auf **0** Minuten. Es wird nicht empfohlen, die Werte im Feld **Websitzungserneuerung** oder im Feld **Websitzungszeitlimit** zu ändern.
3. Klicken Sie auf **Änderungen übernehmen**.

So aktivieren Sie den HTTP- oder HTTPS-Webzugriff

1. Vergewissern Sie sich, dass das Kontrollkästchen **Web UI Enable** aktiviert ist.
2. Um den HTTP-Zugriff zu aktivieren, aktivieren Sie das Kontrollkästchen **HTTPAccess** und geben Sie den **HTTPPort** Nummer zu verwenden. Die Standard-Portnummer ist 80.
3. Um den HTTPS-Zugang zu aktivieren, aktivieren Sie das Kontrollkästchen **HTTPS-Zugang** und geben Sie den **HTTPS-Port** an Nummer zu verwenden. Die Standard-Portnummer ist 443.
4. Klicken Sie auf **Änderungen übernehmen**.

So deaktivieren Sie die Benutzeroberfläche von Web

1. Deaktivieren Sie das Kontrollkästchen **Web UI Enable**.
2. Klicken Sie auf **Änderungen übernehmen**.

Um die Benutzeroberfläche von Web wieder zu aktivieren

Geben Sie in der CLI ein: `web enable`

So konfigurieren Sie die CLI für den Zugriff über Telnet oder SSH

1. Um den Telnet-Zugang zu aktivieren, markieren Sie das Kontrollkästchen **Telnet-Zugang**.
2. Um den SSH-Zugang zu aktivieren, aktivieren Sie das Kontrollkästchen **SSH-Zugang** und wählen Sie die zu verwendende **SSH-Version**.
3. Klicken Sie auf **Änderungen übernehmen**.

So konfigurieren Sie CLI so, dass es sich nach einer bestimmten Leerlaufzeit automatisch abmeldet

1. Legen Sie die Zeitspanne für die **automatische Abmeldung** auf die angegebene Anzahl von Sekunden fest, die der Benutzer inaktiv sein kann, bevor er automatisch abgemeldet wird. Um das System so zu konfigurieren, dass es sich nie automatisch abmeldet, setzen Sie das Feld auf **0** Minuten.
2. Klicken Sie auf **Änderungen übernehmen**.

4.2.3 Konfigurieren Sie SQL Zugriff

Die SQL-Access-Funktion einer GFI ClearView-Appliance ermöglicht den Zugriff auf die Verkehrsüberwachungsdatenbank aus jeder ODBC-kompatiblen Anwendung.

Um diese Funktion nutzen zu können, muss der SQL-Zugriff auf der GFI ClearView-Appliance konfiguriert und ein ODBC-Treiber auf einem Client installiert und konfiguriert werden. ODBC-fähige Anwendungen, die auf dem Client laufen, können dann die interne Monitoring-Datenbank der GFI ClearView-Appliance abfragen.

In dieser Anleitung wird erläutert, wie Sie die GFI ClearView-Appliance so konfigurieren, dass sie Remote-SQL-Verbindungen akzeptiert, und wie Sie den ODBC-Treiber auf Windows 8- und Windows 10-Clients einrichten.

Laden Sie den ODBC-Treiber herunter.

Laden Sie die ODBC-Treiberversion herunter, die Ihrem Client-Betriebssystem entspricht. Folgen Sie den Anweisungen auf dieser Seite, um den ODBC-Treiber auf Ihrem Client-Betriebssystem zu installieren.

Der ODBC-Treiber kann heruntergeladen werden von:

Optionen für Remote SQL festlegen

Damit die GFI ClearView-Appliance Remote-SQL-Verbindungen von einem externen ODBC-Connector akzeptieren kann, müssen Sie die Einstellungen unter **Konfiguration > System > Setup > SQL Access** vornehmen.

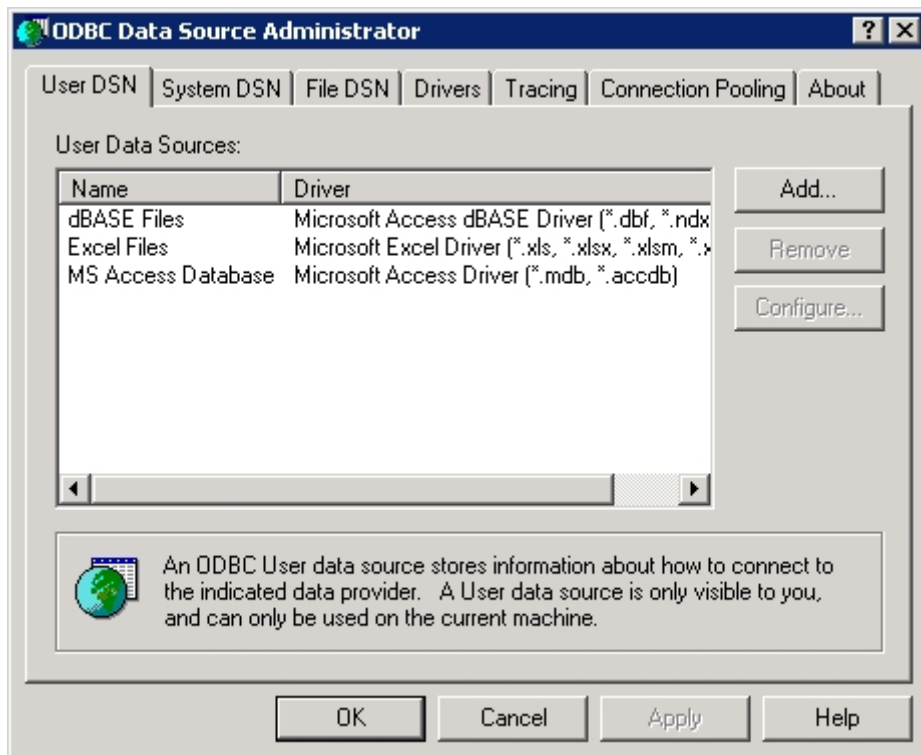
- » **Remote-SQL:** Wählen Sie diese Option, damit die GFI ClearView-Appliance Remote-SQL-Verbindungen von externen ODBC-Konnektoren akzeptieren kann.
- » **Zugriff zulassen von (Hostname oder IP):** Verwenden Sie diese Option, um die Hosts einzuschränken, die eine Verbindung zur SQL-Datenbank herstellen können. Geben Sie "%" ein, um allen Hosts die Verbindung zu erlauben, oder geben Sie eine IP-Adresse oder den Hostnamen bestimmten Hosts ein, um den Zugriff zu beschränken.
- » **Benutzername:** Geben Sie einen Benutzernamen an, der für die Authentifizierung verwendet werden soll (z. B. "Datenbank").
- » **Passwort:** Geben Sie ein Passwort an, das für die Authentifizierung verwendet werden soll.
- » **Bestätigen Sie das Passwort:** Geben Sie das oben angegebene Passwort erneut ein.

Übernehmen Sie die Änderungen. Der SQL-Zugang wird sofort verfügbar gemacht. Eine erfolgreich konfigurierte Appliance würde etwa so aussehen:

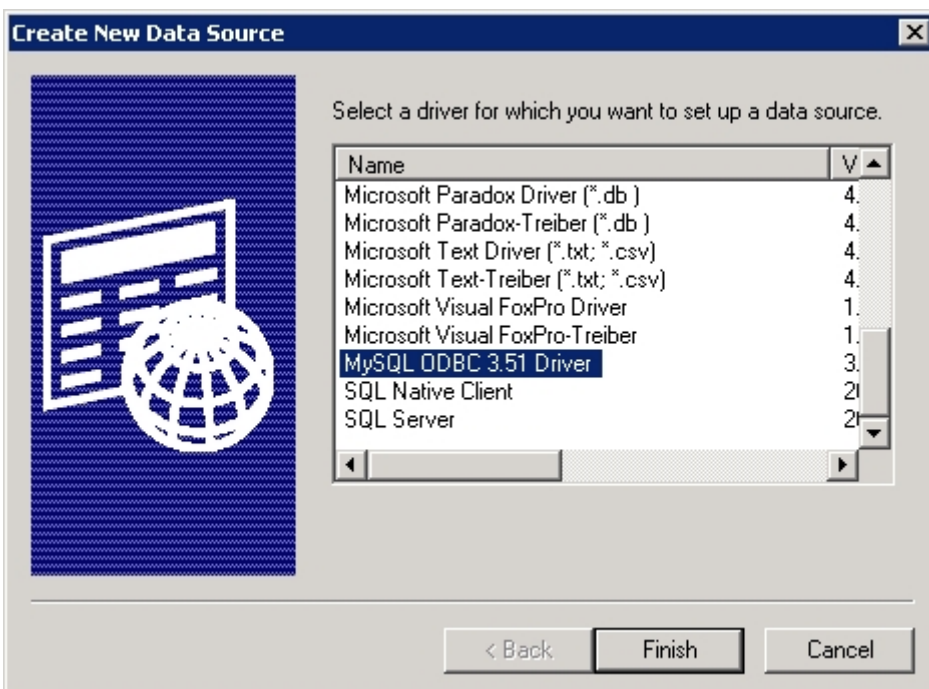
Remote SQL Options	
Remote SQL	<input checked="" type="checkbox"/> Enable
Allow access from (Hostname or IP)	<input type="text" value="%"/> <small>(% = 'any')</small>
Username	<input type="text" value="database"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

Nachdem der Remote-SQL-Zugriff auf der GFI ClearView-Appliance konfiguriert wurde, im nächsten Schritt eine ODBC-Datenquelle auf dem Client erstellt werden.

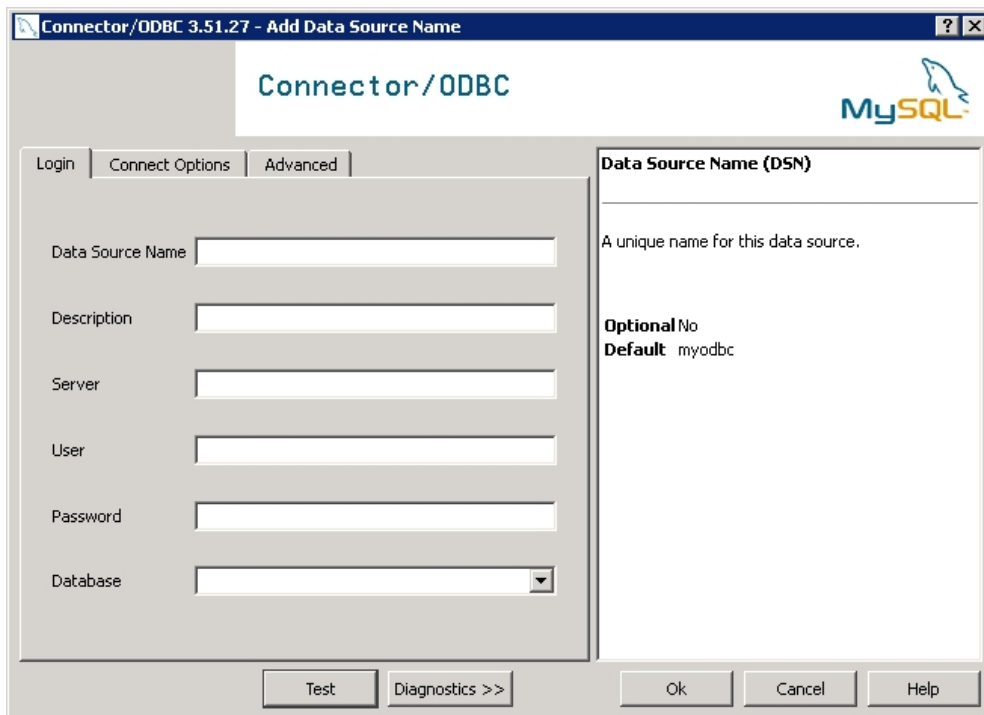
1. Öffnen Sie die **Verwaltungswerkzeuge** und wählen Sie **Datenquellen (ODBC)**. Es sollte das folgende Dialogfeld angezeigt werden.



2. Wählen Sie die Registerkarte **Benutzer-DSN** oder die Registerkarte **System-DSN**, je nachdem, ob die SQL-Daten nur dem aktuellen Benutzer (Benutzer-DSN) oder allen Benutzern (System-DSN) zur Verfügung gestellt werden sollen. Klicken Sie dann auf **Hinzufügen**. Dadurch wird ein Assistent gestartet, mit dem Sie eine neue Datenquelle erstellen können.

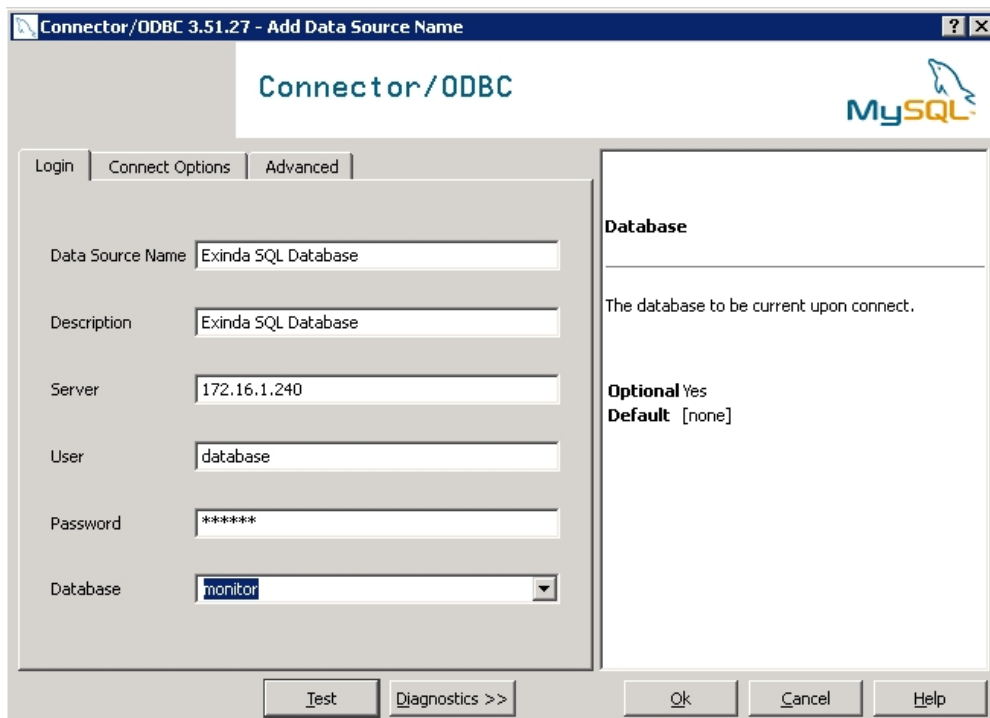


3. Wählen Sie **MySQL ODBC Driver** und klicken Sie auf **Finish**. Sie werden aufgefordert, Details über den SQL-Zugang in das unten stehende Formular einzugeben:

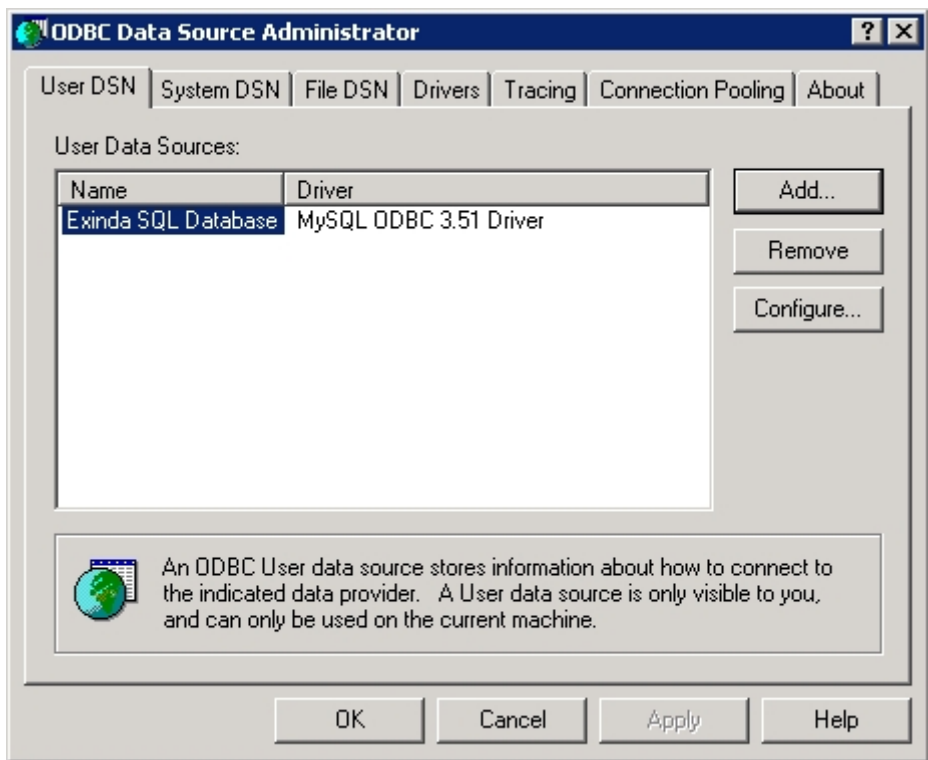


Datenquelle Name / Beschreibung	Geben Sie einen beschreibenden Namen für den DSN ein. Z. B. "GFI ClearView SQL Database".
Server	Geben Sie die IP-Adresse GFI ClearView-Appliance ein.
Benutzer	Geben Sie den Benutzernamen ein, den Sie bei der Aktivierung des SQL-Zugriffs auf die ClearView-Appliance angegeben haben.
Passwort	Geben Sie das Passwort ein, das Sie bei der Aktivierung des SQL-Zugriffs auf die ClearView-Appliance angegeben haben.
Datenbank	Sobald die oben genannten Felder konfiguriert sind, klicken Sie auf die Schaltfläche "Test". Wenn der Verbindungsversuch erfolgreich war, wird die Dropdown-Liste "Datenbank" mit einer Liste der verfügbaren Datenbanken ausgefüllt. Wählen Sie "überwachen".

So sieht eine erfolgreiche Konfiguration aus:

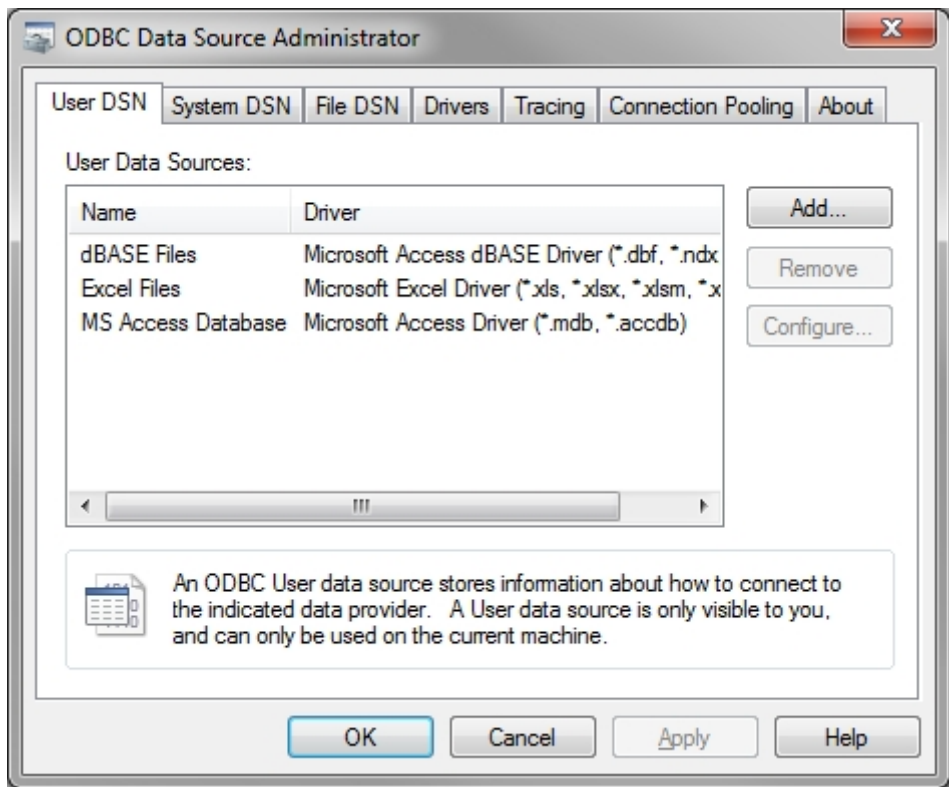


Klicken Sie auf **OK**. Dadurch wird die "GFI ClearView SQL Database" zur Liste der verfügbaren Datenquellen hinzugefügt, die von Drittanbieteranwendungen auf diesem Client verwendet werden können.



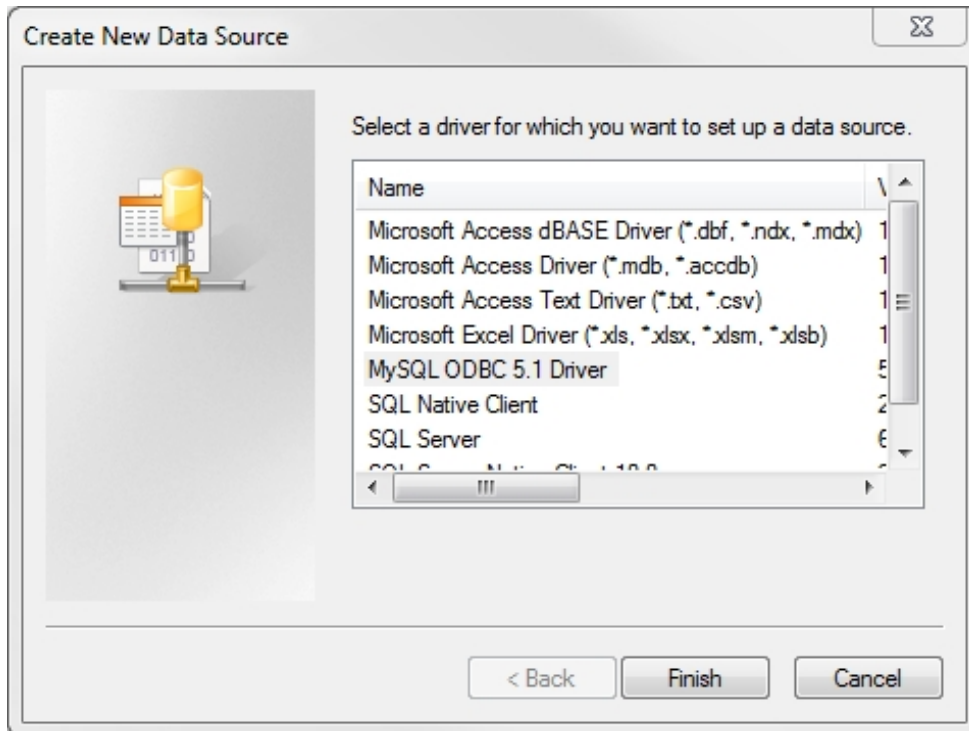
ODBC-Datenquelle unter Windows 7 erstellen

Öffnen Sie die **Verwaltungswerkzeuge** und wählen Sie **Datenquellen (ODBC)**. Es sollte das folgende Dialogfeld angezeigt werden.

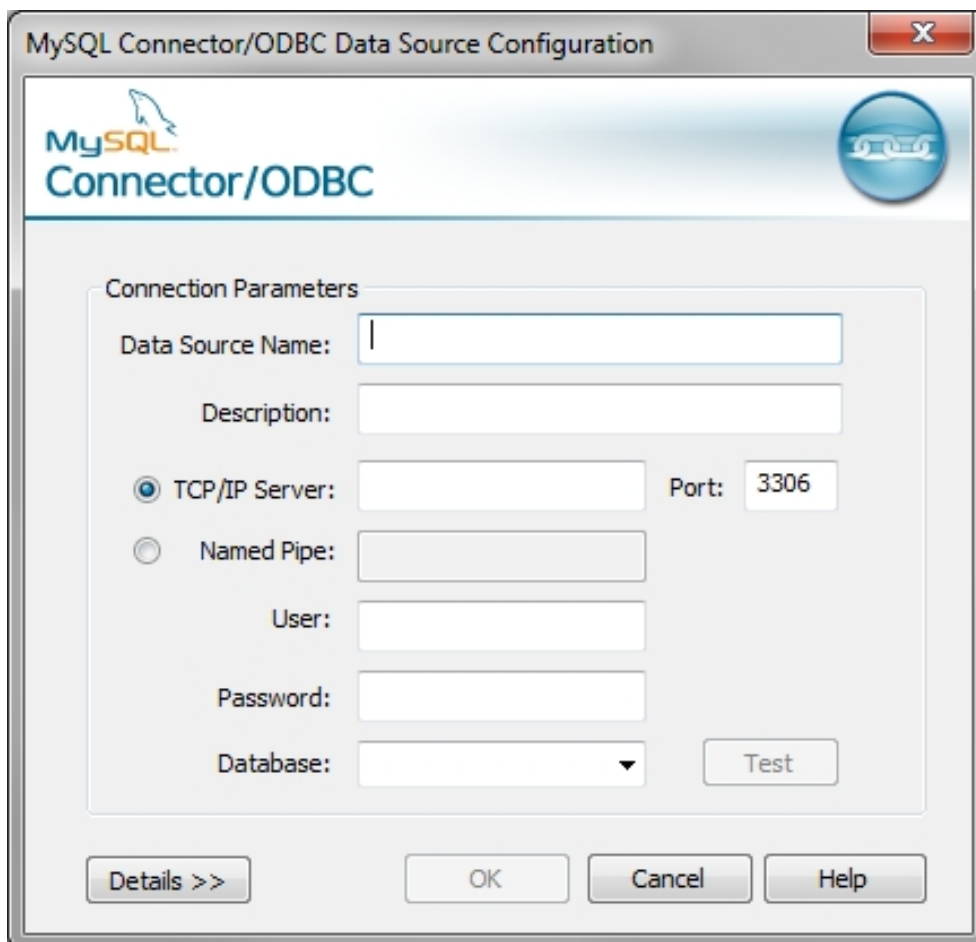


Wählen Sie die Registerkarte Benutzer-DSN oder die Registerkarte System-DSN, je nachdem, ob die SQL-Daten nur dem aktuellen Benutzer (Benutzer-DSN) oder allen Benutzern (System-DSN) zur Verfügung gestellt werden sollen.

Klicken Sie dann auf **Hinzufügen**. Dadurch wird ein Assistent gestartet, mit dem Sie eine neue Datenquelle erstellen können.

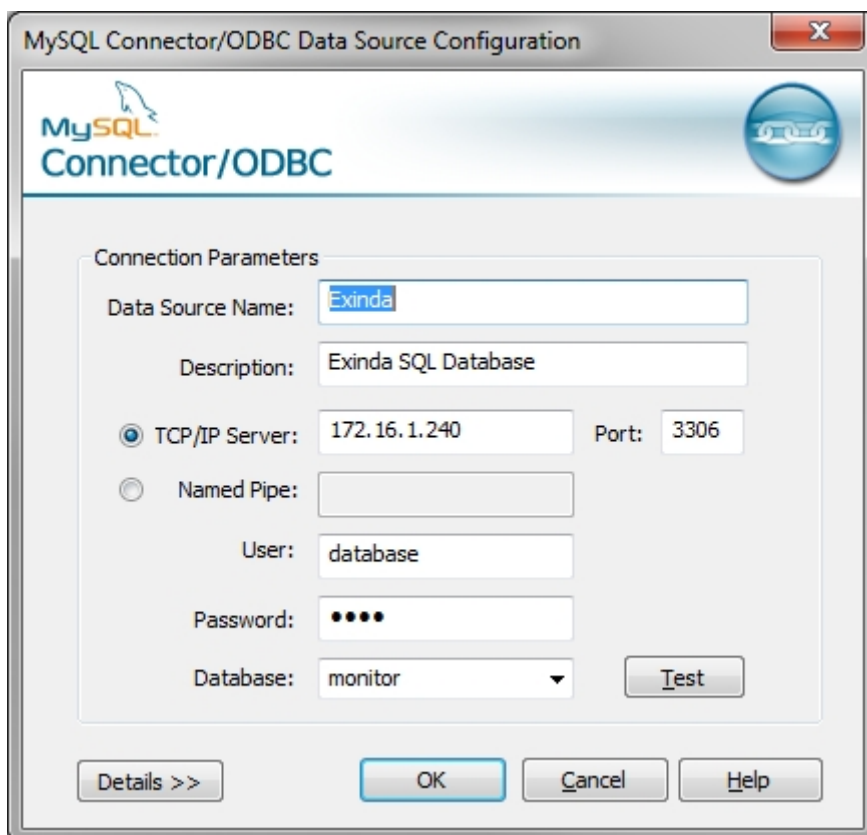


Wählen Sie **MySQL ODBC Driver** und klicken Sie auf **Finish**. Sie werden aufgefordert, Details über den SQL-Zugang in das unten stehende Formular einzugeben:

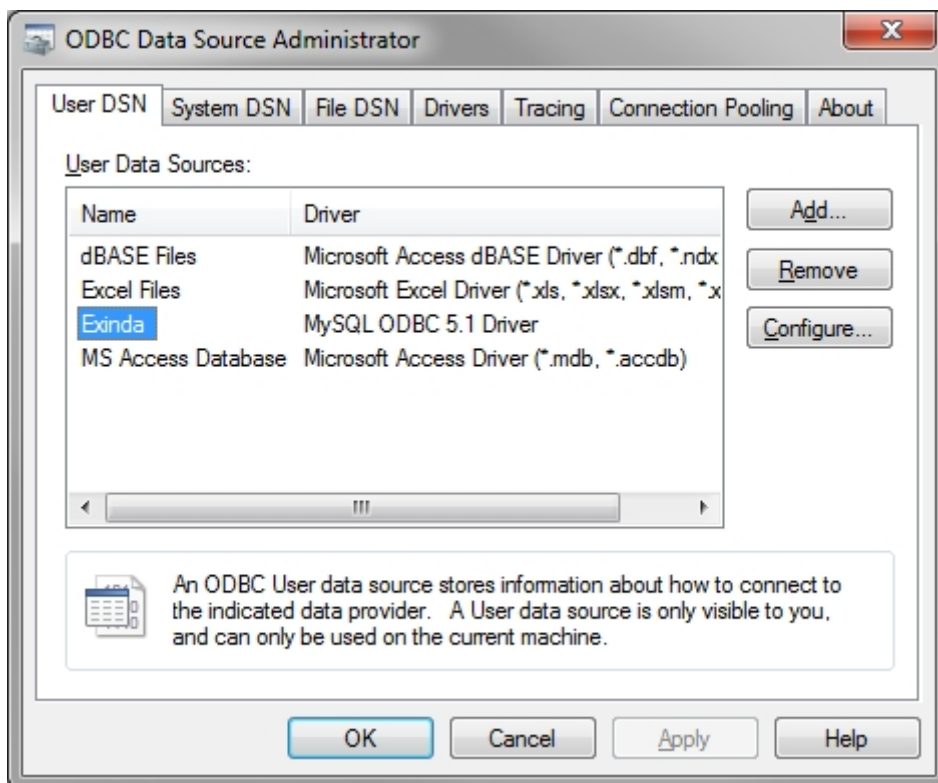


Name der Datenquelle / Beschreibung	Geben Sie einen beschreibenden Namen für den DSN ein. Z. B. "GFI ClearView SQL Database".
Server	Geben Sie die IP-Adresse GFI ClearView-Appliance ein.
Benutzer	Geben Sie den Benutzernamen ein, den Sie bei der Aktivierung des SQL-Zugriffs auf ClearView-Appliance angegeben haben.
Passwort	Geben Sie das Passwort ein, das Sie bei der Aktivierung des SQL-Zugriffs auf ClearView-Appliance angegeben haben.
Datenbank	Sobald die oben genannten Felder konfiguriert sind, klicken Sie auf die Schaltfläche "Test". Wenn der Verbindungsversuch erfolgreich war, wird die Dropdown-Liste "Datenbank" mit einer Liste der verfügbaren Datenbanken ausgefüllt. Wählen Sie "überwachen".

So sieht eine erfolgreiche Konfiguration aus:



Klicken Sie auf **OK**. Dadurch wird die "GFI ClearView SQL Database" zur Liste der verfügbaren Datenquellen hinzugefügt, die von Drittanbieteranwendungen auf diesem Client verwendet werden können.



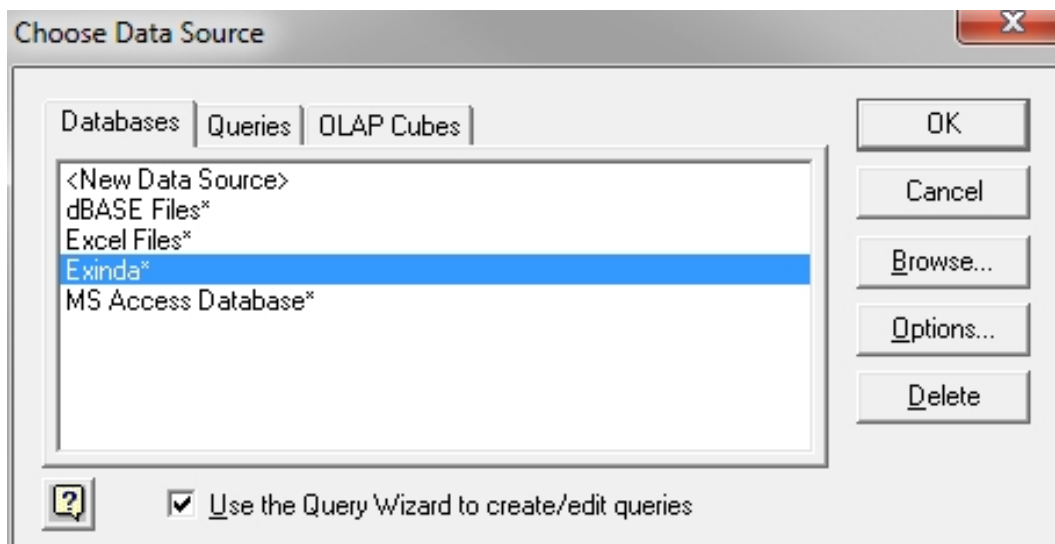
Anzeigen von SQL Access-Daten in Microsoft Excel

Sie benötigen eine Anwendung eines Drittanbieters, die in der Lage ist, auf Daten aus ODBC-Datenquellen zuzugreifen. Für die Zwecke dieser Anleitung verwenden wir Microsoft Excel als Beispiel.

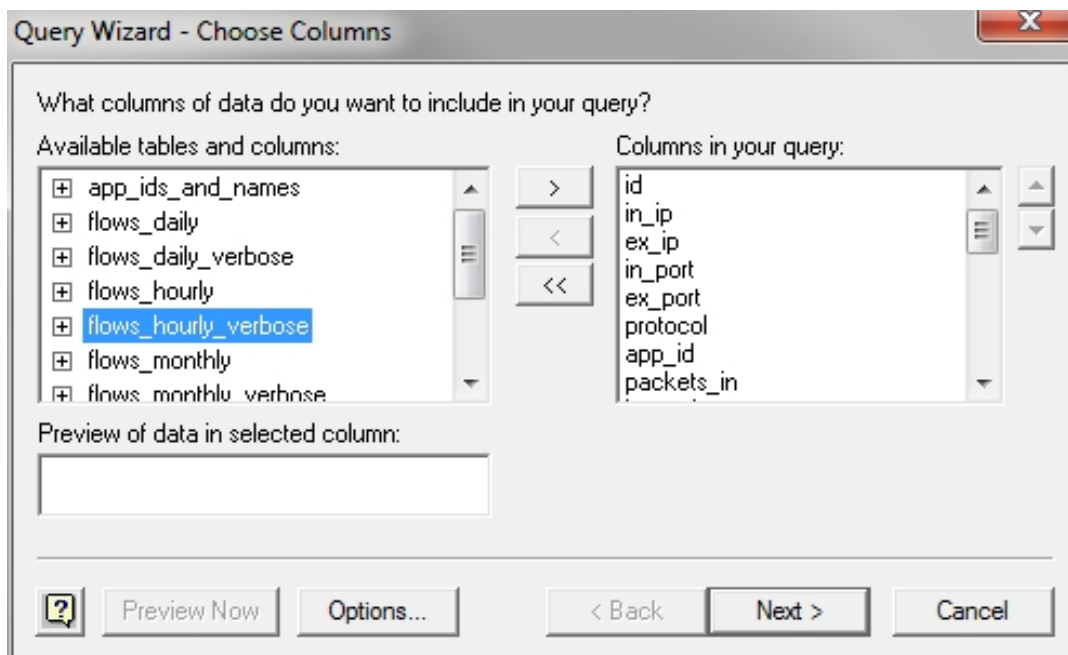
Wählen Sie auf der Registerkarte **Daten** in Excel die Option **Aus anderen Quellen > Aus Microsoft Query**.



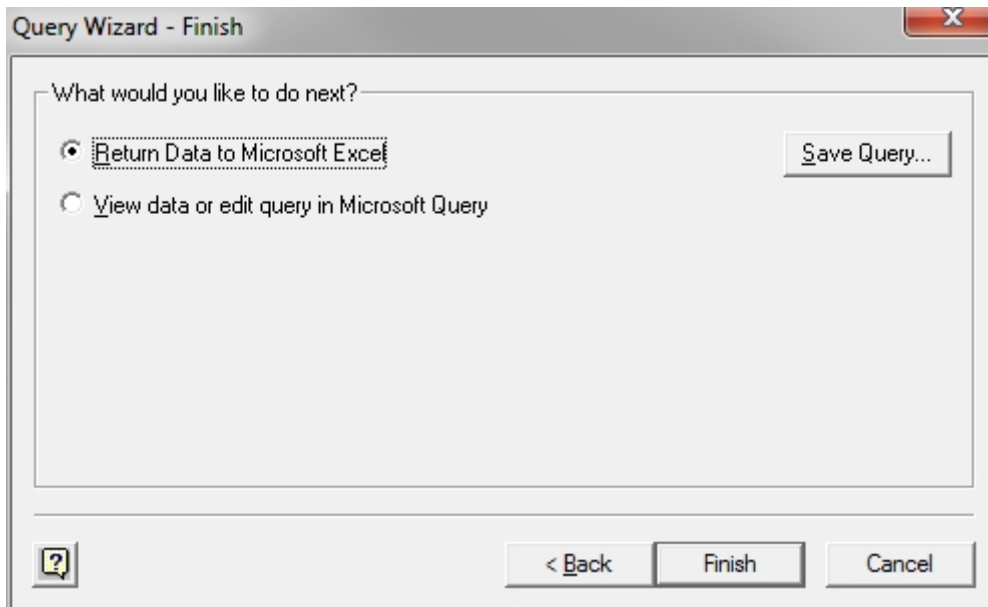
Es wird ein Dialogfeld angezeigt, in dem Sie den DSN auswählen können, den Sie vorherigen Kapitel erstellt haben.



Wählen Sie den **GFI ClearView SQL Database DSN**. Nun können Sie eine der verfügbaren Tabellen und die abzufragenden Spalten auswählen. Wählen Sie eine Tabelle aus, und klicken Sie auf die Schaltfläche >, um die Felder dieser Tabelle in die Liste der abzufragenden Spalten zu verschieben.



Klicken Sie sich durch den Assistenten und geben Sie optional Spalten an, nach denen Sie filtern oder sortieren möchten. Klicken Sie dann auf Fertig stellen, um die Daten an Excel zurückzugeben.



Die GFI ClearView-Appliance wird nun abgefragt, und die Daten werden an die Excel-Tabelle zurückgegeben.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	id	in ip	ex ip	in port	ex port	protocol	app id	packets in	bytes in	packets out	bytes out	max tput in	max tput out
2	2714022	2886729828	3197021980	0	0	17	222	0	0	6	1581	0	
3	2714021	2886729850	2523226833	0	0	6	201	6	1104	6	1621	883	
4	2714020	2886729872	3339138632	0	0	6	201	12	3324	12	1666	1329	
5	2714019	2886729939	3494527776	0	0	1	201	22	1760	0	0	448	
6	2714018	2886729972	1249745235	0	0	6	207	16	3184	19	3825	1185	
7	2714017	2886729877	1494265866	0	0	6	201	7	1942	13	1539	1553	
8	2714016	2886729939	3339139912	0	0	6	201	6	2129	6	877	1703	
9	2714015	2886729939	1113983841	0	0	6	207	7	2162	9	1909	1729	
10	2714014	2886729972	1249733985	0	0	6	201	6	1104	8	2283	883	
11	2714013	2886729882	3413282335	0	0	6	222	119	12450	114	11368	919	
12	2714012	2886729888	3510548001	0	0	6	201	4	2359	5	1317	1887	
13	2714011	2886729828	3416333846	0	0	6	222	211	18338	241	21137	896	
14	2714010	2886730069	2149463094	0	0	6	201	36	5620	44	3580	593	
15	2714009	2886729850	2523226710	0	0	6	201	89	70476	85	14272	11439	
16	2714008	2886729882	3406878235	0	0	6	201	24	2839	18	1330	2271	
17	2714007	2886729855	1114779712	0	0	6	201	6	3055	7	775	2444	
18	2714006	2886729855	3452688776	0	0	6	201	90	47511	90	10534	2546	
19	2714005	2886729888	3452688776	0	0	6	201	6	3183	7	743	2546	
20	2714004	2886729939	3494527776	0	0	6	201	19	2552	37	3483	530	
21	2714003	2886729974	2827985172	0	0	6	207	37	7416	36	4420	1507	
22	2714002	2886729888	3539452941	0	0	6	201	6	1131	8	3813	904	

SQL Schema

Es gibt insgesamt 10 Tabellen, die über SQL zugänglich sind.

Name	Description
fließt_stündlich	Durchflussaufzeichnungen mit stündlicher Auflösung, d.h. die Informationen für jeden Durchfluss werden stündlich, auf die Stunde genau, gespeichert
fließt_täglich	Durchflussaufzeichnungen in Tagesauflösung, d. h. die Informationen für jeden Durchfluss werden täglich um Mitternacht am Tag gespeichert.
fließt_monatlich	Durchflussaufzeichnungen mit monatlicher Auflösung, d. h. die Informationen für jeden Durchfluss werden monatlich am 1. des Monats um Mitternacht gespeichert.
urls_hourly	URL-Datensätze für jeden Flussdatensatz, der 1 oder mehr URLs enthält, mit stündlicher Auflösung, d. . die Informationen für jede URL werden stündlich gespeichert.
urls_daily	URL-Datensätze für jeden Bewegungsdatensatz, der 1 oder mehr URLs enthält, mit täglicher Auflösung, d. h. die Informationen für jede URL werden täglich um Mitternacht gespeichert.
urls_monthly	URL-Datensätze für jeden Stromdatensatz, der 1 oder mehr URLs enthält, mit monatlicher Auflösung, d. die Informationen für jede URL werden monatlich gespeichert, am 1. des Monats um Mitternacht.
app_ids_und_names	Anwendungsdatensätze. Der Datensatz enthält einen Namen, eine ID und ein Kennzeichen, das angibt, ob die Anwendung gelöscht wurde. Gelöschte Anwendungen werden bei der Kennzeichnung von historischen Daten verwendet.
summary_applications	Nach Anwendungen zusammengefasste Durchflussaufzeichnungen. Jeder Datensatz enthält Informationen, die über einen Zeitraum von 5 Minuten gesammelt wurden.
Zusammenfassung_Hosts_ex	Nach externem Host zusammengefasste Verkehrsaufzeichnungen. Jeder Datensatz enthält Informationen, die über einen Zeitraum von 5 Minuten gesammelt wurden.
summary_hosts_in	Nach internem Host zusammengefasste Verkehrsaufzeichnungen. Jeder Datensatz enthält Informationen, die über einen Zeitraum von 5 Minuten gesammelt wurden.

fließt Tabelle

In der folgenden Tabelle wird das Schema der SQL-Tabellen flows_* beschrieben.

Feld	Typ	Beschreibung
id	32-Bit-Ganzzahl ohne Vorzeichen	Eine eindeutige ID, die diesen Datensatz definiert. Dies ist der Primärschlüssel.
in_ip	binär (128 Bit)	Eine 16-Byte-Darstellung (128 Bit) der internen IPv6-Adresse (die IP-Adresse auf der LAN-Seite der GFI ClearView-Appliance) des Datenflusses. IPv4-Adressen werden als IPv4-zugeordnete Formate dargestellt.
ex_ip	binär (128 Bit)	Eine 16-Byte-Darstellung (128 Bit) der externen IPv6-Adresse (die IP-Adresse auf der WAN-Seite der GFI ClearView-Appliance) des Datenflusses. IPv4-Adressen werden als IPv4-zugeordnete Formate dargestellt.
Eingang_Hafen	24-Bit-Ganzzahl ohne Vorzeichen	Die TCP- oder UDP-Portnummer auf der internen Seite (der LAN-Seite der GFI ClearView-Appliance) des Datenflusses.1
ex_port	24-Bit-Ganzzahl ohne Vorzeichen	Die TCP- oder UDP-Portnummer auf der externen Seite (der WAN-Seite der GFI ClearView-Appliance) des Datenflusses.1
Protokoll	24-Bit-Ganzzahl ohne Vorzeichen	Die von der IANA zugewiesene IP-Protokollnummer des Datenflusses. Siehe http://www.iana.org/assignments/protocol-numbers/ für weitere Informationen.
app_id	24-Bit-Ganzzahl ohne Vorzeichen	Die interne GFI ClearView-Anwendungs-ID, die diesem Fluss wurde.
Pakete_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Pakete, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.

Feld	Typ	Beschreibung
Bytes_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Bytes, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
pakete_aus	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Pakete, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
bytes_out	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Bytes, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
max_Ausgang_Ein	64-Bit-Ganzzahl ohne Vorzeichen	Der maximale eingehende (WAN -> LAN) Durchsatz, der für diesen Fluss während Stichprobenzeitraums beobachtet wurde.
max_Output_out	64-Bit-Ganzzahl ohne Vorzeichen	Der maximale ausgehende (LAN -> WAN) Durchsatz, der für diesen Fluss während Stichprobenzeitraums beobachtet wurde.
Intervalle_in	24-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der 10-Sekunden-Intervalle, in denen während des Stichprobenzeitraums eingehender (WAN -> LAN) Verkehr für diesen Fluss beobachtet wurde (bps).
Intervalle_aus	24-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der 10-Sekunden-Intervalle, in denen während des Stichprobenzeitraums ausgehender (LAN -> WAN) Verkehr für diesen Fluss beobachtet wurde (bps).
Zeitstempel	32-Bit-Ganzzahl ohne Vorzeichen	Ein UNIX-Zeitstempel (Anzahl der Sekunden seit Epoche - 1. Januar 1970), der Beginn des Stichprobenzeitraums darstellt.
in_Benutzername	String	Eine String-Darstellung des Benutzernamens, der der internen IP dieses Flusses zugewiesen wurde, als er erstellt wurde (falls verfügbar).
ex_username	String	Eine String-Darstellung des Benutzernamens, der der externen IP dieses Flusses zugewiesen wurde, als er erstellt wurde (falls verfügbar). ¹
rtt	32-Bit-Ganzzahl ohne Vorzeichen	Round Trip Time in Millisekunden. Ein Maß für die Zeit, die ein Paket benötigt, um ein Gerät zu verlassen, ein Netzwerk zu durchqueren und zurückzukehren. ²
netzwerk_verzoegerung	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Zeit, die Transaktionsdaten benötigen, um das Netzwerk zu durchlaufen. ²
netzwerk_jitter	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Variabilität von network_delay. ²
server_delay	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Zeit, die ein Server benötigt, um auf eine Transaktionsanfrage zu antworten. ²
bytes_lost_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der erneute Übertragungen verlorenen Bytes (WAN -> LAN). ²
bytes_lost_out	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der durch erneute Übertragungen verlorenen Bytes (LAN -> WAN). ²
aps	64-Bit-Ganzzahl ohne Vorzeichen	Application Performance Score. Ein Maß für die Leistung einer Anwendung im Netzwerk. ²

» `in_port` und `ex_port` sind nur definiert, wenn das IP-Protokoll TCP (6) oder UDP (17) ist und GFI ClearView den Datenfluss nicht klassifizieren konnte (die `app_id` ist also 0).

» Weitere Informationen finden Sie unter [Verwendung von Anwendungsleistungsberichten](#).

Die `flows_*`-Tabellen sind als Ansichten verfügbar, die die binären IPv6-Adressen im String-Format darstellen. Die Tabellen der Ansichten sind `flows_*_verbose` (z. B. `flows_hourly_verbose`). Die Felder sind mit den oben genannten identisch, mit Ausnahme der folgenden:

Field	Type	Description
<code>in_ip</code>	string	A string representation of the internal address (the IP address on the LAN side of the Exinda appliance) of the flow. IPv4 mapped IPv6 addresses are represented as IPv4 dotted quad.
<code>ex_ip</code>	string	A string representation of the external address (the IP address on the WAN side of the Exinda appliance) of the flow. IPv4 mapped IPv6 addresses are represented as IPv4 dotted quad.

app_ids_and_names Tabelle

Die folgende Tabelle beschreibt das Schema der SQL-Tabelle app_ids_and_names.

Feld	Typ	Beschreibung
app_id	24-Bit-Ganzzahl ohne Vorzeichen	Eine eindeutige ID, die die Anwendung definiert. Dies ist der Primärschlüssel.
app_name	String	Der Name der Anwendung (z. B. HTTP, Hotmail)
gelöscht_Flagge	8-Bit-Ganzzahl ohne Vorzeichen	Ein Flag, das anzeigt, ob die Anwendung aus der Appliance gelöscht wurde (0 = nein, 1 = ja)

urls Tabelle

Die folgende Tabelle beschreibt das Schema der urls_* SQL-Tabellen.

Feld	Typ	Beschreibung
id	32-Bit-Ganzzahl ohne Vorzeichen	Diese ID verweist auf eine ID in der entsprechenden übergeordneten Tabelle flows_*. Es kann mehrere Url-Datensätze geben, die auf dieselbe Fluss-ID verweisen, daher ist dieses Feld nicht eindeutig.
url	string	Die URL (Host), die aus dem HTTP-Header des übergeordneten Flusses extrahiert wurde.
pakete_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Pakete, die für diese URL während Stichprobenzeitraums aufgezeichnet wurden.
Bytes_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Bytes, die für diese URL während des Stichprobenzeitraums aufgezeichnet wurden.
pakete_aus 64-bit	ohne Vorzeichen Ganzzahl	Die Anzahl der ausgehenden (LAN -> WAN) Pakete, die für diese URL während Stichprobenzeitraums aufgezeichnet wurden.
bytes_out	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Bytes, die für diese URL während des Stichprobenzeitraums aufgezeichnet wurden.
max_tput_in 64-Bit	ohne Vorzeichen Ganzzahl	Der maximale eingehende (WAN -> LAN) Durchsatz, der für diese URL während Stichprobenzeitraums beobachtet wurde.
max_tput_out 64-Bit	ohne Vorzeichen Ganzzahl	Der maximale ausgehende (LAN -> WAN) Durchsatz, der für diese URL während Stichprobenzeitraums beobachtet wurde.
Intervalle_in	16-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der 10-Sekunden-Intervalle, in denen für diese URL während des Stichprobenzeitraums eingehender (WAN -> LAN) Verkehr beobachtet wurde.
intervalle_aus 16-Bit	ohne Vorzeichen Ganzzahl	Die Anzahl der 10-Sekunden-Intervalle, in denen für diese URL während des Stichprobenzeitraums ausgehender (LAN -> WAN) Verkehr beobachtet wurde.

NOTE

IDs are only consistent across the same sample periods. For example, IDs in the urls_hourly table only reference IDs in the flows_hourly table.

summary_applications Tabelle

Die Tabelle summary_application fasst die aggregierten Daten von GFI ClearView zusammen. In der folgenden Tabelle wird das Schema der SQL-Tabelle summary_applications beschrieben.

Feld	Typ	Beschreibung
Eingang_Hafen	24-Bit-Ganzzahl ohne Vorzeichen	Die TCP- oder UDP-Portnummer auf der internen Seite (der LAN-Seite der GFI ClearView-Appliance) ¹
ex_port	24-Bit-Ganzzahl ohne Vorzeichen	Die TCP- oder UDP-Portnummer auf der externen Seite (der WAN-Seite der GFI ClearView-Appliance) ¹
Protokoll	ohne Vorzeichen 24-Bit-Ganzzahl	Die von der IANA zugewiesene IP-Protokollnummer des Flusses. Siehe http://www.iana.org/assignments/protocol-Nummern/ für weitere Informationen.
app_id	ohne Vorzeichen 24-Bit-Ganzzahl	Die interne GFI ClearView-Anwendungs-ID, die diesem Fluss zugewiesen wurde. Sie steht für GFI ClearViews Klassifizierung des Flusses. Ein Nullwert ist zu interpretieren als nicht klassifiziert.
Bytes_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Bytes, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
bytes_out	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Bytes, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
Pakete_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Pakete, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
pakete_aus	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Pakete, die für diesen Fluss während Stichprobenzeitraums aufgezeichnet wurden.
Intervalle_in	ohne Vorzeichen 24-Bit-Ganzzahl	Die Anzahl der 10-Sekunden-Intervalle, in denen eingehender Verkehr (WAN -> LAN) beobachtet wurde für diesen Fluss während des Stichprobenzeitraums.
Intervalle_aus	ohne Vorzeichen 24-Bit-Ganzzahl	Die Anzahl der 10-Sekunden-Intervalle, in denen ausgehender Verkehr (LAN -> WAN) stattfand für diesen Fluss während des Stichprobenzeitraums beobachtet.
Zeitstempel	ohne Vorzeichen 32-Bit-Ganzzahl	Ein UNIX-Zeitstempel (Anzahl der Sekunden seit der Epoche - 1. Januar 1970), der Folgendes darstellt dem Beginn des Stichprobenzeitraums.
max_Ausgang_Ein	ohne Vorzeichen 64-Bit-Ganzzahl	Der maximale eingehende (WAN -> LAN) Durchsatz, der für diesen Fluss während Stichprobenzeitraums beobachtet wurde (bps).
max_Output_out	ohne Vorzeichen 64-Bit-Ganzzahl	Der maximale ausgehende (LAN -> WAN) Durchsatz, der für diesen Fluss während Stichprobenzeitraums beobachtet wurde (bps).
rtt	32-Bit-Ganzzahl ohne Vorzeichen	Round Trip Time in Millisekunden. Ein Maß für die Zeit, die ein Paket benötigt, um ein Gerät zu verlassen, ein Netzwerk zu durchqueren und zurückzukehren. ²
Netzwerk_Verzögerung	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Zeit, die Transaktionsdaten benötigen, um das Netzwerk zu durchlaufen. ²
Netzwerk_Jitter	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Variabilität von network_delay. ²
Server_Verzögerung	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Zeit, die ein Server benötigt, um auf eine Transaktionsanfrage zu antworten. ²
Bytes_verloren_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der erneute Übertragungen verlorenen Bytes (WAN -> LAN). ²
bytes_verloren_aus	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der durch erneute Übertragungen verlorenen Bytes (LAN -> WAN). ²

» `in_port` und `ex_port` sind nur definiert, wenn das IP-Protokoll TCP (6) oder UDP (17) ist und GFI ClearView den Datenfluss nicht klassifizieren konnte (die `app_id` ist also 0).

» Weitere Informationen finden Sie unter [Verwendung von Anwendungsleistungsberichten](#).

summary_hosts Tabelle

Die folgende Tabelle beschreibt das Schema der SQL-Tabellen summary_hosts_in und summary_hosts_ex. Die Tabellenfelder sind bis auf das Feld ip identisch - dieses Feld steht für die IPv4- oder IPv6-Adresse eines internen Hosts (summary_hosts_in) oder eines externen Hosts (summary_hosts_ex).

Ein Host ist intern, wenn er sich auf LAN-Seite der Appliance befindet, und extern, wenn er sich auf WAN-Seite befindet.

Feld	Typ	Beschreibung
ip	binäre Zeichenfolge	Eine String-Darstellung der internen oder externen IPv4- oder IPv6-Adresse des Hosts.
Bytes_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Bytes, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
bytes_out	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Bytes, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
Pakete_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der eingehenden (WAN -> LAN) Pakete, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
pakete_aus	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der ausgehenden (LAN -> WAN) Pakete, die für diesen Fluss während des Stichprobenzeitraums aufgezeichnet wurden.
Intervalle_in	ohne Vorzeichen 24-Bit	Die Anzahl der 10-Sekunden-Intervalle, in denen für diesen Datenfluss während des Abtastzeitraums ein ganzzahliger eingehender (WAN -> LAN) Verkehr für diesen Datenfluss während des Stichprobenzeitraums beobachtet (bps).
Intervalle_aus	ohne Vorzeichen 24-Bit Ganzzahl	Die Anzahl der 10-Sekunden-Intervalle, in denen ausgehender (LAN -> WAN) Verkehr für diesen Datenfluss während des Stichprobenzeitraums beobachtet (bps).
Zeitstempel	32-Bit-Ganzzahl ohne Vorzeichen	Ein UNIX-Zeitstempel (Anzahl der Sekunden seit Epoche - 1. Januar 1970), der den Beginn des Stichprobenzeitraums darstellt.
max_Ausgang_Ein	64-Bit-Ganzzahl ohne Vorzeichen	Der maximale eingehende (WAN -> LAN) Durchsatz, der für diesen Fluss während des Stichprobenzeitraums beobachtet wurde.
max_Ausgang_rtt	ohne Vorzeichen 64-Bit	Der maximale ausgehende (LAN -> WAN) Durchsatz, der für diesen Fluss während der Stichprobe beobachtet wurde
netzwerk_verzögerung	32-Bit-Ganzzahl ohne Vorzeichen	Round Trip Time in Millisekunden. Ein Maß für die Zeit, die ein Paket benötigt, um ein Gerät zu verlassen, ein Netzwerk zu durchqueren und zurückzukehren. ¹
Netzwerk_Jitter	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Variabilität von network_delay. ¹
Server_Verzögerung	32-Bit-Ganzzahl ohne Vorzeichen	Ein normalisiertes Maß für die Zeit, die ein Server benötigt, um auf eine Transaktionsanfrage zu antworten. ¹
Bytes_verloren_in	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der erneute Übertragungen verlorenen Bytes (WAN -> LAN). ¹
bytes_verloren_aus	64-Bit-Ganzzahl ohne Vorzeichen	Die Anzahl der durch erneute Übertragungen verlorenen Bytes (LAN -> WAN). ¹

Weitere Informationen finden Sie unter [Verwendung von Anwendungsleistungsberichten](#).

4.2.4 Überwachung der Konfiguration

Sie können Details konfigurieren, die für Überwachungsdiagramme und die gesammelten Überwachungsdaten relevant sind. Sie können konfigurieren, wie die Daten angezeigt werden, wie der Datenverkehr zu Überwachungszwecken analysiert wird, welche Reihenfolge der Auflösungsmethoden bei der Auflösung von IP-Adressen in Hostnamen versucht wird, ob

Daten gesammelt werden, und ob die gesammelten Daten gelöscht werden.

Zur Konfiguration der Datenanzeige können Sie angeben, wie viele Elemente in den Datentabellen angezeigt werden, wie viele Elemente in den Kreisdiagrammen angezeigt werden und wie viele Zeichen in den URLs angezeigt werden sollen.

Für die Analyse des Datenverkehrs können Sie festlegen, ob der Datenverkehr gemäß Layer 7- oder Layer 3-Definitionen erkannt werden soll, und wie empfindlich (oder aggressiv) Sie bei der Erkennung von BitTorrent, eDonkey, Skype und der Datenflusserkennung vorgehen wollen.

Für die Analyse des Datenverkehrs für bestimmte Anwendungstypen (anwendungsspezifische Analysemodule (ASAM)) können Sie angeben, ob Daten aus dem Citrix-, http- und SSL-Verkehr extrahiert werden sollen, ob anonyme Proxys im Datenverkehr identifiziert werden sollen, ob der VoIP-Verkehr analysiert werden soll, ob die Leistung und der Zustand von Verbindungen berechnet werden sollen, ob Informationen zur Verbindungssymmetrie gesammelt werden sollen und ob jede im Datenverkehr gesehene URL protokolliert werden soll.

Für die Auflösung von IP-Adressen in Hostnamen können Sie angeben, welche Methoden als erstes, zweites usw. versucht werden: Netzwerkobjekt, DSN, NetBios-Namenssuche und IP-Adresse.

Für die Sammlung von Überwachungsdaten können Sie angeben, ob Daten für Subnetze und virtuelle Schaltkreise gesammelt werden sollen, ob detaillierte Datensätze für Anwendungen, Hosts, URLs, Benutzer, Konversationen und Subnetze gesammelt werden sollen und ob Daten für den Verkehr zwischen internen Netzwerkobjekten gesammelt werden sollen.

Zum Löschen von Überwachungsdaten können Sie verschiedene Arten von Daten, die von der Appliance erfasst werden, selektiv löschen.

So konfigurieren Sie die Anzeige von Überwachungsdiagrammen Optionen

Gehen Sie zu **Konfiguration > System > Setup > Registerkarte Überwachung** - Formular **Überwachungsoptionen**. In den folgenden Feldern können Sie die Anzeigeeoptionen ändern.

- » **Tabellenelemente** - Legt die maximale Anzahl der in den Überwachungstabellen angezeigten Top-Elemente fest. Zulässige Werte sind 1 - 1000.
- » **Diagrammelemente** - Legt die maximale Anzahl der Top-Elemente fest, die im Diagramm und in den Diagrammen angezeigt werden. Akzeptable Werte sind 1-10. Beachten Sie, dass dieser Wert universell für ALLE Optionen im Menü Monitor gilt.
- » **Maximale URL-Größe** - Legt die maximale Länge von URLs fest, die in den Tabellen des Echtzeitberichts angezeigt werden.
- » **Graph Display Options** - Gibt an, ob die Graphen im Flash- oder Nicht-Flash-Format angezeigt werden. Die Standardeinstellung ist Flash.
- » **Anzeige für Anwendungsdetails pro Subnetz** - Gibt an, ob das Anwendungsdiagramm innerhalb eines Subnetzes in einem geplanten Bericht als Zeitreihendiagramm (Liniendiagramm) oder als Tortendiagramm angezeigt wird. Wenn diese Option ausgewählt ist, wird das Diagramm Anwendungen pro Subnetz im geplanten Bericht als Liniendiagramm angezeigt, während alle anderen Diagramme weiterhin als Tortendiagramm angezeigt werden. Die Standardeinstellung ist Zeitreihendiagramm.
- » **Subnetze nach Namen sortieren** - Subnetze werden in geplanten Berichten nach Namen sortiert, wenn das Kontrollkästchen Aktivieren aktiviert ist; andernfalls werden die Subnetze nach Datenvolumen sortiert.

So konfigurieren Sie, wie der Datenverkehr überwacht wird

Gehen Sie zu **Konfiguration > System > Setup > Registerkarte Überwachung** - Formular **Überwachungsoptionen**.

In den folgenden Feldern können Sie angeben, wie empfindlich die Analyse der Verkehrsklassifizierung sein soll.

- » **Layer 7 Inspection** - Legt fest, ob die Anwendungssignaturen innerhalb eines Pakets analysiert werden sollen, um den Datenverkehr in den Berichten weiter zu klassifizieren. Wenn zum Beispiel bei der Analyse von HTTP- und FTP-Verkehr eine MPEG-Datei in den Paketen erkannt wird, wird die mit der Verbindung verbundene Anwendung in MPEG geändert. Ist die Funktion deaktiviert, werden die Layer-7-Signaturen in den Paketen

nicht analysiert und alle Anwendungserkennungsobjekte mit Layer-7-Regeln werden ignoriert.

» **Monitor IPv6 Link Local Traffic** - Gibt an, ob der IPv6 Link Local Traffic überwacht werden soll, d. h. nicht routbarer Datenverkehr, der nur in einem einzigen Netzwerksegment gültig ist. Standardmäßig wird dieser Verkehr nicht überwacht, da er nicht repräsentativ für den Verkehr Ihrer Netzwerkbenutzer ist. Er wird hauptsächlich für die Netzwerkerkennung verwendet.

» **OpenVPN-Erkennung** - Gibt die Empfindlichkeit für die Erkennung von OpenVPN-Datenverkehr an. Die Einstellung "aggressiv" ist die Standardeinstellung, kann jedoch zu einigen Fehlalarmen führen. Die Einstellung "sicher" kann zu falsch-negativen Ergebnissen führen.

» **Bittorrent-Empfindlichkeit** - Die Einstellung "hoch" wird für die meisten Diensteanbieterumgebungen empfohlen. Die Einstellung "niedrig" wird in Fällen mit vielen Fehlalarmen empfohlen.

» **EDonkey-Empfindlichkeit** - Die Einstellung "hoch" wird für die meisten Diensteanbieterumgebungen empfohlen. Die Einstellung "niedrig" wird für Fälle mit vielen Fehlalarmen empfohlen.

» **Skype-Empfindlichkeit** - Die Einstellung "hoch" wird für die meisten Diensteanbieterumgebungen empfohlen.

» **Reporting Sensitivity** - Steuert die Mindestanzahl von Paketen, die in einem Fluss gesehen werden müssen, bevor er in der aufgezeichnet wird. Akzeptable Werte liegen zwischen 1 und 10, wobei 10 die niedrigste Empfindlichkeit darstellt. Die Einstellung auf einen niedrigen Wert wird in Umgebungen mit hoher Last nicht empfohlen.

Wenn die Empfindlichkeit auf einen niedrigen Wert wie z. B. 9 eingestellt ist, werden Datenströme, die weniger als neun Pakete in einem Zeitraum von fünf Minuten enthalten, nicht in der Datenbank gespeichert. Dadurch wird verhindert, dass Port-Scans Hunderte von unnötigen Datenzeilen in die Datenbank laden.

So aktivieren oder deaktivieren Sie anwendungsspezifische Analysemodule (ASAM)

Gehen Sie zu **Konfiguration > System > Setup > Registerkarte Überwachung** - Formular **ASAM**.

Die GFI ClearView-Appliance analysiert den Datenverkehr und versucht, ihn mit den für den jeweiligen Datenverkehrstyp spezifischen Kriterien abzugleichen. Die Kriterien für den Abgleich des Datenverkehrs werden in anwendungsspezifischen Analysemodulen (ASAM) definiert. Aktivieren und deaktivieren Sie die Module, die für Ihr Netzwerk wichtig sind.

Die folgenden ASAM-Module sind verfügbar:

» **Anonymer Proxy** - Wenn dieses Modul aktiviert ist, versucht das System, anonyme Proxys zu verwenden, indem es den HTTP-Hostnamen und den gemeinsamen SSL-Namen mit der Liste der anonymen Proxy-URLs abgleicht, die von der Appliance täglich heruntergeladen werden. Deaktivieren Sie dieses Modul, wenn es den Anschein hat, dass eine Anwendung fälschlicherweise als anonymer Proxy klassifiziert wird.

» **Citrix** - Wenn aktiviert, versucht die Appliance, Benutzernamen und Anwendungsnamen aus Citrix-Verbindungen zu extrahieren.

Deaktivieren Sie dieses Modul, um die Appliance an Standorten zu stoppen, an denen die Datenschutzrichtlinien diese Art der Benutzeridentifizierung nicht zulassen.

» **DCE/RPC** - Wenn dieses Modul aktiviert ist, kategorisiert es Client-Anfragen für Microsoft-Dienste MAPI und SMB. Dieses Modul sollte immer aktiviert sein.

» **HTTP** - Wenn dieses Modul aktiviert ist, versucht es, die als HTTP identifizierten Verbindungen weiter zu analysieren und Informationen wie Host, URL, Anfragetyp und Inhaltstyp zu extrahieren.

» **Leistungsmetrik** - Wenn dieses Modul aktiviert ist, berechnet es die Netzwerkverzögerung, die Serververzögerung, die Round Trip Time (RTT), den Verlust, die Effizienz und den TCP-Status für TCP-Verbindungen. Deaktivieren Sie dieses Modul, wenn die RAM- oder CPU-Auslastung steigt und die Leistung der Appliance beeinträchtigt. Weitere Informationen finden Sie unter [RAM-Nutzungsbericht](#) und [CPU-Nutzungsbericht](#).

» **SSL** - Wenn dieses Modul aktiviert ist, extrahiert es öffentliche Zertifikate von Verbindungen, die als SSL identifiziert wurden, und dekodiert die Informationen aus diesen Zertifikaten (z. B. den gemeinsamen Namen und die Organisationseinheit).

VoIP - Wenn dieses Modul aktiviert ist, extrahiert es VoIP-bezogene Informationen wie Code-Typ und Anrufqualitätsinformationen (MoS- und rFactor-Bewertung) aus Verbindungen, die als RTP identifiziert wurden.

» **Asymmetrische Route** - Wenn dieses Modul aktiviert ist, sammelt es Informationen zur Symmetrie der Verbindungen. Deaktivieren Sie dieses Modul, wenn das Netzwerk regelmäßig asymmetrische Routen aufweist, da es unnötig ist, Administratoren über asymmetrische Verbindungen zu informieren.

» **URL-Protokollierung** - Wenn diese Option aktiviert ist, wird jede URL, die von der Appliance gesehen wird, in der Datenbank protokolliert. Geben Sie an, wie lange (in Tagen) die Daten gespeichert werden sollen. Dieses Modul ist standardmäßig deaktiviert.

So steuern Sie die Reihenfolge der Auflösungsverfahren, die bei der Auflösung von IP-Adressen in Hostnamen verwendet werden

Gehen Sie zu **Konfiguration > System > Setup > Registerkarte Überwachung** - Formular **Hostauflösungsmethode**.

Es gibt mehrere Hostauflösungsmethoden, die zur Auflösung von IP-Adressen in Hostnamen verwendet werden können. Das System wird versuchen, den Hostnamen mit einer der Methoden aufzulösen. Wenn diese Methode fehlschlägt, versucht es eine andere Methode. Sie können die Reihenfolge der Hostauflösungsmethoden festlegen, die das System verwendet, indem Sie die erste Methode als 1, die nächste als 2 usw. einstufen.

Für die Host-Auflösungsmethoden gibt es folgende Optionen:

» **Netzwerkobjekt** - Die IP-Adressen werden entsprechend den konfigurierten Netzwerkobjekten aufgelöst.

» **DNS** - Die IP-Adressen werden gemäß den DNS-Zuordnungen aufgelöst.

» **IPAdresse(keine Auflösung)** - Die IP-Adressen werden NICHT in Hostnamen aufgelöst. »

NetBIOS Name Lookup - Die IP-Adressen werden in NetBIOS-Namen aufgelöst. **So aktivieren**

oder deaktivieren Sie die Erfassung von Überwachungsdaten

Gehen Sie zu **Konfiguration > System > Setup > Registerkarte Überwachung**

Es werden verschiedene Arten von Daten über den Datenverkehr im Netzwerk gesammelt. Wenn die Appliance nicht wie erwartet funktioniert, kann die Datenerfassung deaktiviert werden, um die Leistung zu verbessern.

Die folgenden Datenerfassungen können deaktiviert werden:

» **Subnets** (wird im Formular "**Statistics Collection**" angezeigt) - Wenn diese Option deaktiviert ist, werden keine Daten für die Subnet-Berichterstattung erfasst.

» **Virtuelle Schaltkreise** (und Anwendungen) (angezeigt im Formular **Statistiksammlung**) - Wenn diese Option deaktiviert ist, werden keine Daten für die Berichterstattung über virtuelle Schaltkreise gesammelt. Die Erfassung globaler Anwendungsstatistiken wird ebenfalls nicht durchgeführt, da die globalen Anwendungsstatistiken von den Statistiken für virtuelle Schaltkreise abgeleitet werden. Beachten Sie, dass die Anwendungsberichte innerhalb eines Subnetzes von dieser Einstellung nicht betroffen sind. Das heißt, wenn die Datensammlung für Subnetze aktiviert und für virtuelle Schaltkreise deaktiviert ist, die Anwendungen innerhalb eines Subnetzes gemeldet, aber die Anwendungen, die über die gesamte Appliance oder innerhalb eines virtuellen Schaltkreises gemeldet werden, werden nicht gemeldet.

» **Interne Hosts** (angezeigt im Formular **Statistiksammlung**) - Wenn diese Option deaktiviert ist, werden für interne Hosts keine Daten gesammelt. Sie können diese Option deaktivieren, um die Menge der gesammelten Daten in Situationen zu kontrollieren, in denen Sie viele Hosts haben und sicherstellen wollen, dass Ihnen der Speicherplatz nicht ausgeht. Wie viel Speicherplatz zugewiesen wurde und wie viel davon frei ist, können Sie unter **Festplattenspeicher für Systemdienste zuweisen** einsehen. Stellen Sie sicher, dass Sie diese Option aktivieren, wenn Sie interne Hostdaten überwachen oder Berichte darüber erstellen oder interne Hostdaten auf den Bildschirmen zur Anwendungsleistung im **Solution Center** anzeigen möchten.

» **Externe Hosts für Subnetze** (im Formular **Statistiksammlung** angezeigt) - Geben Sie ein oder mehrere Netzwerkobjekte an, um externe Hostdaten nur für bestimmte Netzwerkobjekte zu erfassen. In Fällen, in denen Sie ein benutzerdefiniertes Netzwerkobjekt erstellt haben, das sich auf eine bestimmte Gruppe von IP-Adressen bezieht, können Sie

Wählen Sie das Netzobjekt so aus, dass nur die erforderlichen Daten erfasst werden und nicht die Fremddaten von allen Objekten.

NOTE

The amount of statistics collected increases for each network object you specify, which may also increase the amount of time necessary to generate reports that collect external host details. A large number of network objects selected may also increase the usage of the monitoring disk partition.

» **Detaillierte Datensatzaufbewahrung** (im Formular **Überwachungsoptionen** angezeigt) - Steuert, ob detaillierte Überwachungsdatensätze (Anwendungen, Hosts, URLs, Benutzer, Konversationen und Subnetze) gespeichert werden. Wenn ein übermäßiger Datenverkehr durch die Appliance fließt, kann die Deaktivierung dieser Option die CPU-Auslastung verringern. Die detaillierten Aufzeichnungen werden jedoch nicht mehr erfasst, und Drilldown-Informationen für Anwendungen, Hosts und Konversationen sind nicht mehr verfügbar, während zusammenfassende Informationen, d. h. Summen für die gesamte Appliance, für Anwendungen, Hosts und Konversationen verfügbar sind.

» **Intern-zu-Intern ignorieren** (im Formular **Überwachungsoptionen** angezeigt) - Ihr Netzwerk kann Netzwerkobjekte auf der WAN-Seite der Appliance haben, die als interne Objekte konfiguriert wurden, z. B. ein Router oder eine Firewall. Das Aktivieren der Option Intern-zu-Intern ignorieren verhindert, dass der Datenverkehr zwischen internen Netzwerkobjekten in die Berichte aufgenommen wird.

So löschen Sie gesammelte Überwachungsdaten

Gehen Sie zu **Konfiguration > System > Setup > Registerkarte Überwachung** - Formular **Überwachungsdatensätze löschen**. Wenn der Appliance der Speicherplatz ausgeht, können Sie die gesammelten Daten löschen.

Die folgenden Datensatztypen können gelöscht werden:

» **Alle Schnittstellendatensätze** - Löscht alle Daten, die mit den Diagrammen "Schnittstellendurchsatz" und "Schnittstellenpakete pro Sekunde" verbunden sind.

» **Alle Netzwerkübersichtsdatsätze** - Löscht alle mit den Netzwerkübersichtsdiagrammen verbundenen Daten.

» **Alle Kontroll-/Richtliniendatensätze** - Löscht alle Daten, die mit den Kontrollkarten "Richtlinien", "Verwerfen" und "Priorisierungsverhältnis" verbunden sind.

» **Alle Optimierungsdatsätze** - Löscht alle Daten, die mit den Diagrammen "Optimierung", "Reduzierung" und "Edge-Cache" verbunden sind.

» **Alle SLA-Datensätze** - Löscht alle Daten, die mit der Netzwerkreaktionskarte (SLA) verbunden sind.

» **Alle APS-Datensätze** - Löscht alle Daten, die mit der APS-Zusammenfassung (Application Performance Score) verbunden sind.

» **Alle APM-Datensätze** - Löscht alle Daten, die mit APM-Diagrammen (Application Performance Metric), den detaillierten Metrikdiagrammen für den APS-Monitor, verbunden sind.

» **Alle detaillierten Monitor-Datensätze** - Löscht alle detaillierten Daten, d. h. alle Drilldown-Daten für Anwendungen, Hosts, URLs, Benutzer und Konversationen. Zusammenfassende Informationen, d. h. die Gesamtzahlen für die gesamte Appliance, sind weiterhin verfügbar.

» **Alle Appliance-Datensätze** - Löscht alle Daten, die mit den Systemdiagrammen - Verbindungen, beschleunigte Verbindungen, CPU-Auslastung, CPU-Temperatur, RAM-Auslastung, Festplatten-IO und Swap-Auslastung - verbunden sind.

» **Alle Teilnetzdatensätze** - Löscht alle mit Teilnetzdiagrammen verbundenen Daten.

Alle Kontrollkästchen können durch Klicken in das Kontrollkästchen im Kopfbereich ausgewählt werden.

CAUTION

This will permanently delete the selected records from the monitoring database.

4.2.5 Netflow Konfiguration

Netflow ermöglicht es der GFI ClearView-Appliance, Datenflussaufzeichnungen an Überwachungsgeräte von Drittanbietern zu exportieren.

1. Verwenden Sie das folgende Formular, um diese Netflow-Ziele zu konfigurieren.

Add New Netflow Collector	
IP Address	<input type="text"/>
Port	<input type="text" value="2055"/>
Version	<input type="text" value="9"/>

Property	Description
IP Address	Specify the IP Address of the Netflow target. The GFI ClearView appliance will export Netflow data to this IP Address.
Port	Specify the Port number of the Netflow target. The GFI ClearView appliance currently supports Netflow export on UDP ports.
Version	Specify the Netflow version to export. Current supported versions are v1, v5 and v9.

2. Das unten stehende Formular ermöglicht die Anpassung der von Netflow gesendeten Datenflüsse.

Common Optionen

Aktiver Fehler timeout 1 Minuten

Nur V9 Optionen

Lange (64-Bit) Byte-Zähler verwenden -Aktivieren

Long (64-Bit)-Paketzähler verwenden - Aktivieren

flow Packet Payload size 140 Bytes

Vorlage Aktualisierungsrate 100 Pakete

Template Timeout Rate 100 Sekunden

Allgemeine Optionen Aktualisierungsrate 100

Pakete Allgemeine Optionen Timeout-Rate 100 Sekunden

Benutzername Optionen Timeout Rate 100 minutes

Inaktiver Benutzername Verfallsrate 1) 10

Stunden V9 Optionale Felder - Allgemein

L7-Anwendungs-ID exportieren -Aktivieren

EX Ort PDIIC/ID T Freigeben

EX Ort Art des Dienstes (TOP) Aktivieren

EX Ort VLAN-ID - EX Ort Min. und

Max. Paketgrößen einschalten - EX Ort Nlin und

Max TTL aktivieren Aktivieren

Flussrichtung exportieren -Aktivieren

Exportieren von SNMP-Eingangs- und Ausgangsschnittstellen-

Export-Ausgabe von Byte- und Paketzählern aktivieren -

Export von Benutzernamen-Details aktivieren - Aktivieren

VoIP MOS und rFactor exportieren -

Exportieren von Zusatzinformationen (Hasennamen)

aktivieren

Aktivieren

Sie

Traffic CldSB exportieren

Option

alle Felder in V9 aktivieren - gdetrics

EX Ort RR -Freigeben

Netzwerkverzögerung exportieren

Jitter im

Exportnetzwerk aktivieren - Export-

Server-Verzögerung aktivieren - Export

verlorene Bytes aktivieren Aktivieren

APS-Ergebnis exportieren -Aktivieren

Gemeinsame Optionen:

Option	Description
Active Flow Timeout	Specify how often long-term, persistent flows are exported. By default, flows are exported within 10 seconds of the flow terminating (this approach does not work well for long-term or persistent flows). This setting allows you to specify how often these long-term flows should be exported.

Netflow v9 Optionen:

Option	Description
Langbyte-Zähler verwenden	Exportieren von Byte-Zählern als 64bit-Werte anstelle von 32bit.
Lange Paketzähler verwenden	Exportieren Sie Paketzähler als 64bit-Werte anstelle von 32bit.
Netflow-Paket-Nutzlastgröße	Setzen Sie die maximale Netflow-Paket-Nutzlastgröße.
Aktualisierungsrate der Vorlage	Konfigurieren Sie die maximale Anzahl von Paketen zwischen dem Exportieren von Vorlagen.
Zeitüberschreitungsrage für Vorlagen	Legen Sie die maximale Anzahl von Sekunden zwischen dem Exportieren von Vorlagen fest.
Optionen Aktualisierungsrate	Konfigurieren Sie die maximale Anzahl von Paketen zwischen dem Exportieren von Optionen.
Optionen Timeout-Rate	Legen Sie die maximale Anzahl von Sekunden zwischen dem Exportieren von Optionen fest.
Benutzername Optionen Zeitüberschreitung	Konfigurieren Sie die maximale Anzahl von Minuten zwischen dem Exportieren von Benutzernamen-Optionen.
Inaktiver Benutzername Verfallsrate	Legen Sie fest, wie lange inaktive Benutzernamen maximal gespeichert werden sollen.

Netflow v9 Optionale Felder - Allgemein:

Option	Description
L7 ausführen	Exportieren Sie Informationen zur Anwendungsidentifikation. Die Zuordnungen zwischen Anwendungs-ID und Name werden exportiert als eine Optionsvorlage.
ID der Anwendung	
Ausfuhr Art der Dienst (TOS)	Exportieren Sie die minimale und maximale Art des Dienstes (TOS).
VLAN-ID exportieren	VLAN-Bezeichner exportieren.
Paketgrößen exportieren	Exportieren Sie minimale und maximale Paketgrößen.
Min. und Max. TTL exportieren	Exportieren Sie die Mindest- und Höchstlebensdauer (TTL).
Richtung des Exportflusses	Flussrichtung des Exports.
SNMP-Schnittstellen exportieren	SNMP-Eingangs- und Ausgangsschnittstellen exportieren.
Ausgabebezahlter exportieren	Exportieren Sie Ausgangspaket- und -bytezähler, die mit den Eingangsbyte- und -paketzählern verglichen werden können, um die Reduzierung zu berechnen.
Details zum Benutzernamen exportieren	AD-Benutzernamen exportieren.
VoIP MoS und rFactor exportieren	Exportieren Sie MoS- und rFactor-Werte für VoIP-Anrufe.
Zusätzliche Informationen exportieren	Exportiert zusätzliche Flussinformationen, z. B. Domänenname für HTTP-Flüsse, Name der veröffentlichten Anwendung für Citrix.
Verkehrsklasse exportieren	Verkehrsklasse exportieren.

Netflow v9 Optionale Felder - Metriken:

Option	Description
--------	-------------

RTT exportieren	Export der Round-Trip-Zeit (RTT).
Netzwerkverzögerung exportieren	Verzögerung im Exportnetz.
Netzwerk-Jitter exportieren	Netzwerk-Jitter exportieren.
Export Server Verzögerung	Verzögerung des Exportservers.
Exportierte Bytes verloren	Anzahl der verlorenen Bytes exportieren.
APS-Ergebnis exportieren	APS-Ergebnis exportieren.

4.2.6 Erstellen eines geplanten Auftrags

Cache-Pre-Population, Neustarts und Firmware-Installationen können zu einem bestimmten Datum, einer bestimmten Uhrzeit und mit einer bestimmten Häufigkeit geplant werden.

Add New Job

ID	<input style="width: 100%;" type="text" value="5"/>
Name	<input style="width: 100%;" type="text" value="Monthly Sales Collateral"/>
Comment	<input style="width: 100%;" type="text" value="Docs for sales team available 3rd day"/>
Enable	<input type="button" value="Yes"/> ▾
Fail-Continue	<input type="button" value="Yes"/> ▾
Schedule	<input type="button" value="Monthly"/> ▾
Time	<input style="width: 100%;" type="text" value="3:00:00"/> (HH:MM:SS)
Interval	<input style="width: 100%;" type="text" value="1"/> (months)
Day-of-month	<input style="width: 100%;" type="text" value="3"/> (-28 to -1 and 1 to 28)
Please enter one or more commands and separate each command with new line .	
Commands	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div>

Bild 226: Erstellen des Zeitplans

Wo kann ich diese Konfiguration finden?

Gehen Sie zu **Konfiguration > System > Setup > Geplante Aufträge**.

So planen Sie einen Auftrag

1. Geben Sie im Bereich "**Neuen Auftrag hinzufügen**" eine eindeutige **ID** für den Auftrag ein.
2. Geben Sie einen **Namen** für den Auftrag ein.
3. [Optional] Geben Sie im Feld **Kommentar** eine Beschreibung für den Auftrag ein.
4. Um die Ausführung des Auftrags zum nächsten geplanten Zeitpunkt zu ermöglichen, **aktivieren Sie** den Auftrag.
5. Wenn der Auftrag abgeschlossen werden soll, auch wenn ein oder mehrere Befehle nicht ausgeführt werden können, setzen Sie **Fail-Continue** auf **Ja**.
6. Legen Sie den Zeitplan für den Auftrag fest. Aufträge können einmalig, täglich, wöchentlich, monatlich oder periodisch ausgeführt werden.
 - **Einmal:** Legen Sie die Uhrzeit und das Datum fest, an dem dieser Auftrag ausgeführt werden soll.
 - **Täglich:** Legen Sie die Zeit fest, zu der dieser Auftrag täglich ausgeführt werden soll.
 - **Wöchentlich:** Legen Sie die Uhrzeit und den Wochentag fest, an dem dieser Auftrag ausgeführt werden soll.
 - **Monatlich:** Legen Sie die Tageszeit, die Häufigkeit der Wiederholung, gemessen in Monatsintervallen, und den Tag des Monats fest. Der Tag des Monats wird mit 1 bis 28 angegeben (z. B. der 23. März hätte den Tag des Monats 23), oder der Tag des Monats kann mit -1 bis -28 angegeben werden, wobei vom letzten Tag des Monats an gezählt wird (z. B. hätte der 31. März den Tag des Monats -1 und der 23. März könnte -9 sein).
 - **Periodisch:** Legen Sie die Startzeit und das Datum sowie die Häufigkeit der Wiederholung als Intervall fest. Die Startzeit wird angegeben als HH:MM:SS, Startdatum wird als JJJJ/MM/TT eingegeben, Intervall wird als 2h3m4s eingegeben.
7. Nachdem Sie den Zeitplan für den Auftrag ausgewählt haben, geben Sie die Parameter für den Zeitplan an. Legen Sie z. B. die Uhrzeit, das Datum, das Intervall oder den Wochentag fest, an dem der Auftrag ausgeführt werden soll.
8. Geben Sie in das Feld **Befehle** die erforderlichen Befehle für den Auftrag ein, den Sie ausführen möchten. Jeder Befehl muss in einer neuen Zeile stehen. Für geplante Vorbelegungsaufträge lassen Sie das Feld Befehle leer. Geben Sie beim Erstellen des Vorbelegungsobjekts diesen geplanten Auftrag an. Die CLI für den Pre-Population-Objekt wird dieses Befehlsfeld automatisch ausgefüllt.
9. Klicken Sie auf **Auftrag hinzufügen**.

Der Auftrag wird der Liste hinzugefügt und steht nun zur Auswahl im Vorbelegungsobjekt zur Verfügung, falls gewünscht.

4.2.7 Warnungen

Warnmeldungen informieren Sie bei Problemen oder potenziellen Problemen mit dem System der GFI ClearView Appliance (z. B. CPU-Auslastung und Speicherauslagerung) oder mit dem Datenverkehr (z. B. bei einem Leistungsabfall einer Anwendung) per E-Mail oder SNMP-Traps. Mithilfe der Warnmeldungen können Sie sicherstellen, dass das System und Ihr Netzwerk so funktionieren, wie Sie es benötigen.

NOTE

To email alerts, valid SMTP and email settings are required. For more information, refer to [Email configuration](#). Recipients of the email alerts are configured where SMTP is configured.

To send SNMP traps, valid SNMP settings are required. For more information, refer to [SNMP configuration](#).

Name	Enable	Send Email	Send SNMP Trap	Trigger Threshold	Clear Threshold
CPU Utilization	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	95 % Busy	80 % Busy
Disk Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	7 % Free	10 % Free
Memory Paging	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
NIC Collisions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	1 %	1 %
NIC Link Negotiation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
NIC Dropped Packets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
NIC Problems - RX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
NIC Problems - TX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Bridge Link	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Bridge Direction	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
System Startup	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable		
SMB Signed Connections	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
SLA Latency		<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
SLA Loss		<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
APS		<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
APM		<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Redundant Power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Redundant Storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Connection Limiting		<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Max Accelerated Connections Exceeded	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
Asymmetric Route Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		
MAPI Encrypted Connections	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable		

Apply Changes

Einige Alarme sind aktiviert und können nicht deaktiviert werden, aber für alle Alarme müssen Sie entscheiden, ob Sie E-Mail-Benachrichtigungen und/oder SNMP-Traps wünschen. Für einige Alarme können Sie operative Schwellenwerte festlegen, um die Alarme auszulösen oder zu löschen.

Angegebene Schwellenwerte überschritten

- » **SLA-Latenz** - Alarm, der ausgelöst wird, wenn die angegebene Latenzzeit für ein SLA-Objekt überschritten wird (weitere Informationen finden Sie unter [Konfigurieren von Service Level Agreement-Objekten](#)).
- » **SLA-Verlust** - Alarm wird ausgelöst, wenn ein SLA-Verlust auftritt.
- » **APS** - Alarm wird ausgelöst, wenn der definierte Schwellenwert für ein APS-Objekt überschritten wird.
- » **APM** - Alarm wird ausgelöst, wenn der definierte Schwellenwert für ein APM-Objekt überschritten wird.
- » **Verbindungsbegrenzung** - Alarm wird ausgelöst, wenn für einen oder mehrere virtuelle Schaltkreise Verbindungsbegrenzungen aktiviert sind und der Schwellenwert erreicht wurde.

Appliance Probleme

- » **CPU-Auslastung** - Alarm wird ausgelöst, wenn der Schwellenwert für die CPU-Auslastung erreicht wird. Die Standardwerte sind 95% bzw. 80% Auslastung.
- » **Festplattennutzung** - Alarm wird ausgelöst, wenn der Schwellenwert für den belegten Speicherplatz erreicht wird. Die Standardwerte sind 7 % bzw. 10 % freier Speicherplatz.
- » **Memory Paging** - Warnung für Speichernutzung und Paging.
- » **NIC-Kollisionen** - Alarm wird ausgelöst, wenn auf den Schnittstellen Kollisionen auftreten. Die Standardwerte sind 20 bzw. 1 pro 30 Sekunden.
- » **NIC Link Negotiation** - Alarm wird ausgelöst, wenn die Geschwindigkeit/Duplex an einer Schnittstelle auf Auto eingestellt ist, diese aber mit Halbduplex und/oder 10 Mbps verhandelt.
- » **NIC Dropped packets** - Alarm wird ausgelöst, wenn auf den Schnittstellen verworfene Pakete vorhanden sind.
- » **NIC-Probleme - RX** - Alarm wird ausgelöst, wenn RX-Fehler» auf den Schnittstellen vorhanden sind. **NIC-Probleme - TX** - Alarm wird ausgelöst, wenn TX» Fehler auf den Schnittstellen vorhanden sind. **System Startup** - Warnung
wird beim Hochfahren der GFI ClearView-Appliance ausgelöst.
- » **Redundante Stromversorgung** - Alarm wird ausgelöst, wenn eines der Netzteile ausfällt (nur auf Plattformen mit redundanter Stromversorgung verfügbar).
- » **Redundanter Speicher** - Alarm wird ausgelöst, wenn eine der Festplatten ausfällt (nur auf Plattformen mit Speicherredundanz verfügbar).

Aktivieren von Systemwarnungen

Gehen Sie wie folgt vor, um die Systemwarnungen zu aktivieren.

Bevor Sie beginnen, sollten Sie die [Warnmeldungen](#) lesen, um zu verstehen, was die einzelnen Warnmeldungen bewirken.

1. Gehen Sie zu Konfiguration > System > Einrichtung > Alarme.
2. Entscheiden Sie für jede der aufgelisteten Warnungen, welche Sie **aktivieren** möchten.
3. Wählen Sie für jeden der aktivierten Alarme die Art der Benachrichtigung aus, die Sie erhalten möchten:
E-Mail senden, **SNMPTrap senden** oder beides.
4. Wenn Sie **CPU-Auslastung**, **Festplattenauslastung** oder **NIC-Kollisionen** als Warnmeldungen auswählen, geben Sie den **Auslöseschwellenwert** und **Löschen Sie die** Schwellenwerte, die zum Senden der Benachrichtigungen führen.

NOTE

When the Trigger Threshold is reached, an alert notification is sent to the administrator. When the Clear Threshold values are reached, the notifications stop being sent.

5. Klicken Sie auf **Änderungen übernehmen**.

4.2.8 Diskstorage erklärt

Die GFI ClearView-Appliance ist in der Lage, Speichermenge dynamisch zu verändern

die den Systemdiensten zugewiesen sind. Auf der Seite Speicherkonfiguration können Sie sehen, wie viel Festplattenspeicher den einzelnen Systemdiensten derzeit zugewiesen ist und wie viel davon derzeit genutzt wird.

Die Benutzer können die Größe des Speicherplatzes nach Bedarf ändern und neu zuweisen.

Disk Storage Map.



Storage Configuration									
Service	Status	Free		Size	Minimum	Encrypted	Operation		
cifs	available	127.45G	98%	129.67G	1024.00M	✘	Resize	Format	Encrypt
edge-cache	available	127.23G	98%	129.45G	1024.00M	✘	Resize	Format	Encrypt
monitor	available	126.97G	98%	129.45G	10.00G		Resize	Format	
users	available	974.62M	95%	1024.00M	512.00M		Resize	Format	
virt	available	49.04G	98%	50.00G	512.00M		Resize	Format	
wan-memory	available	467.01G	98%	474.65G	5120.00M	✘	Resize	Format	Encrypt
unallocated storage				0.00					
Total Available Storage:				914.22G					

Die Karte des Festplattenspeichers zeigt an, welche Dienste Festplattenspeicher verwenden und wie ihr aktueller Status ist. Sie zeigt auch die jedem Dienst zugewiesene Speichermenge, den freien Speicherplatz und die minimalen Speicheranforderungen. Bestimmte Dienste haben die Möglichkeit, verschlüsselt zu werden. Es wird auch angezeigt, ob der Speicher für diese Dienste derzeit verschlüsselt ist.

Der Abschnitt Festplattenkonfiguration zeigt eine Zusammenfassung des Speichers nach Festplattenpartition.

Disk Configuration			
Disk	Status	Size	Operation
sda9	in-use	914.22 GB	

[Refresh Disk Information](#)

Die Karte des Festplattenspeichers

- » **Dienst** - die Dienste, die Plattenspeicher verwenden
- » **Status** - der Status dieses Speichers; der Plattenspeicher kann sich in einem von mehreren Zuständen befinden, je nachdem, welcher Vorgang ausgewählt wurde:
 - **verfügbar** - Der Speicher ist online und für den Dienst verfügbar.
 - **wachsend** - Der Speicherplatz wurde vergrößert, und das Dateisystem wird neu konfiguriert, um den neu geschaffenen Platz zu nutzen.
 - **shrinking** - Die Speichergröße wurde verringert und das Dateisystem wird neu konfiguriert, um die verringerte Speichermenge zu nutzen.
 - **formatieren** - Der Speicher wird gerade formatiert.
 - **checking** - Das Speicherdateisystem wird auf Konsistenz geprüft.
 - **Fehler** - Der Speicher befindet sich in einem Fehlerzustand. Weitere Informationen über den Fehler werden in einer Statusmeldung am oberen Rand des Formulars angezeigt.
 - **nicht verfügbar** - Der Speicher ist nicht verfügbar.
- » **Frei** - die Menge an verfügbarem Speicherplatz, angezeigt als Anzahl von Bytes sowie als

Prozentsatz der verfügbaren Fläche

- » **Größe** - die Gesamtmenge des für diesen Dienst zugewiesenen Speichers
- » **Minimum** - die für diesen Dienst erforderliche Mindestmenge an Speicherplatz
- » **Verschlüsselt** - gibt an, ob die Speicherung für den Dienst derzeit verschlüsselt ist oder nicht
- » **Operation** - Optionen zur Durchführung von Operationen auf dem Speicher (Größe ändern, formatieren, verschlüsseln).

Änderung der Größe des Festplattenspeichers für einen Dienst

Verwenden Sie die folgenden Anweisungen, um die Größe des Plattenspeichers für einen Dienst zu ändern. Diese Anweisungen gelten für jeden Dienst.

1. Gehen Sie zu Konfiguration > System > Einrichtung > Speicher.
2. Suchen Sie den Eintrag für den Dienst in der Tabelle.
3. Bearbeiten Sie in der Spalte Größe die Menge des für einen Dienst verfügbaren Speichers.

NOTE

The storage size can be specified in terms of kilobytes (K), megabytes (M), gigabytes (G), or percentage (%). Use % when entering a storage size to indicate a storage amount as a percentage of free space available. This can be useful when re-allocating storage between services - entering 100% will increase the storage size by the currently unallocated space.

4. Klicken Sie in der gleichen Zeile auf **Größe ändern**.

NOTE

When decreasing the amount of storage available to a service, the service may be stopped until the storage operation has completed. If you are decreasing the amount of storage to less than is currently being used, then the entire contents of the storage for the specified service will be discarded.

Löschen aller für einen Dienst gespeicherten Daten

Verwenden Sie die folgenden Anweisungen, um alle Daten aus dem Festplattenspeicher für einen Dienst zu löschen. Diese Anweisungen gelten für alle Dienste

CAUTION

Formatting a services storage will remove all associated application data and should not be necessary in most cases. Contact GFI ClearView Support if you are unsure if this is necessary.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf Konfiguration > System > Setup > Speicher.
6. Suchen Sie den Eintrag für den Dienst in der Tabelle.
7. Klicken Sie in der gleichen Zeile auf **Format**.

4.3 Authentifizierung

Lernen Sie den Prozess der Authentifizierung von Benutzern und Benutzergruppen in Ihrem Netzwerk kennen.

4.3.1 Eine Liste der aktiven Benutzer anzeigen

Aktive Benutzer listet die Benutzer auf, die derzeit entweder bei der Web-UI oder bei der CLI angemeldet sind.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf Konfiguration > System > Authentifizierung > Aktive Benutzer.

Die nachstehende Tabelle zeigt ein Beispiel für die derzeit angemeldeten Benutzer zusammen mit dem Sitzungstyp, der IP-Adresse und der Leerlaufzeit der Sitzung in Sekunden.

Active Users			
Username	Line	Host	Idle (seconds)
admin	pts/0	172.16.0.239	1544
admin	web/73	172.16.0.239	2096
monitor	web/75	172.16.0.115	2762
admin	web/76	172.16.0.239	0

4.3.2 Lokale Benutzer Konten

Lokale Benutzerkonten ermöglicht das Hinzufügen/Entfernen lokaler Benutzerkonten sowie das Ändern der Passwörter lokaler Benutzer.

Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).

1. Geben Sie den **Benutzernamen** und das **Passwort** ein.
2. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf Konfiguration > System > Authentifizierung > Lokale Benutzerkonten.

In der Tabelle oben auf der Seite sind die konfigurierten lokalen Benutzer und ihre Fähigkeiten aufgeführt.

Local Users		
User	Capability	Enabled
<input type="checkbox"/> admin	admin	<input checked="" type="checkbox"/>
<input type="checkbox"/> monitor	monitor	<input checked="" type="checkbox"/>

6. Um lokale Benutzerkonten von der GFI ClearView-Appliance zu entfernen oder ein Konto vorübergehend zu deaktivieren, aktivieren Sie das Kontrollkästchen für den Benutzer, und klicken Sie auf **Benutzer entfernen** oder **Benutzer deaktivieren**.

7. Um ein neues lokales Benutzerkonto hinzuzufügen, geben Sie einen Benutzernamen an und wählen eine Fähigkeit aus. Klicken Sie auf **Benutzer hinzufügen**. Admin-Benutzer haben vollen Lese- und Schreibzugriff auf die GFI ClearView-Appliance. Monitor-Benutzer haben nur Lesezugriff.

Add New User	
User Name	<input type="text"/>
Capability	<input type="text" value="Admin"/>

8. Erstellen Sie ein Passwort für einen neuen Benutzer oder ändern Sie das Passwort für einen bestehenden Benutzer, indem Sie den Benutzernamen auswählen, für den Sie ein neues Passwort erstellen oder ändern möchten, und ein neues Passwort eingeben. Klicken Sie auf **Passwort ändern**.

Change Password

User Name

New Password

Confirm Password

4.3.3 AAA

AAA konfiguriert, wie sich Remote-Benutzer bei der GFI ClearView-Appliance authentifizieren sollen und welche Berechtigungen sie erhalten sollen.

1. Um AAA zu konfigurieren, navigieren Sie auf der Web-UI im erweiterten Modus zu **Konfiguration > System > Authentifizierung > AAA**.
2. Legen Sie die Reihenfolge fest, in der Benutzer authentifiziert werden. Wenn sich ein Benutzer anmeldet, versucht die GFI ClearView-Appliance, ihn mit den hier angegebenen Authentifizierungsmethoden zu authentifizieren, und zwar in der Reihenfolge, in der sie konfiguriert wurden.

Authentication Method List

First Method

Second Method

Third Method

Fourth Method

NOTE

This setting is required if you are using a remote access mechanism such as [LDAP](#), [Radius](#) or [TACACS+](#).

3. Klicken Sie auf **Änderungen übernehmen**.
4. Steuern Sie, welche Berechtigungen fernauthentifizierte Benutzer erhalten, wenn sie sich bei der GFI ClearView-Appliance anmelden.

Authorization

Map Order

Map Default User

Map Order	remote-first	Apply user privileges supplied by the remote authentication mechanism first. If that fails, use the 'Map Default User' setting below.
	remote-only	Apply user privileges supplied by the remote authentication mechanism first. If that fails, the user will not be authenticated.
	local-only	Use the 'Map Default User' setting below.
Map Default		If the user authentication is not successful, the user will login with the user specified in the 'Map Default User' setting below.

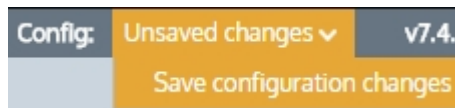
5. Klicken Sie auf **Änderungen übernehmen**.

4.3.4 LDAP Authentifizierung

Mit der LDAP-Authentifizierung können Sie die GFI ClearView-Appliance so konfigurieren, dass sie Anmeldeversuche von Benutzern mit einem entfernten LDAP-Server (einschließlich Active Directory) authentifiziert.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Stellen Sie sicher, dass LDAP als Authentifizierungsmethode auf der Seite [AAA](#) ausgewählt ist.
6. Klicken Sie auf **Konfiguration > System > Authentifizierung** und wechseln Sie auf die Registerkarte **LDAP**.
7. Definieren Sie die globalen LDAP-Authentifizierungsoptionen. Klicken Sie auf **Änderungen übernehmen**.
8. Geben Sie den Hostnamen oder die IP-Adresse des entfernten LDAP-Servers an. Es können IPv4- oder IPv6-Adressen angegeben werden. Es können mehrere LDAP-Server definiert werden.
9. Klicken Sie auf **Neuen LDAP-Server hinzufügen**.
10. Um einen LDAP-Server von der GFI ClearView-Appliance zu entfernen, aktivieren Sie das Kontrollkästchen für Server, und klicken Sie auf **Server entfernen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Ungespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.

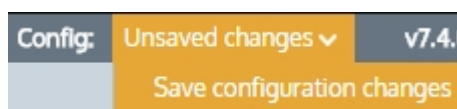


4.3.5 Radius Authentifizierung

Mit der Radius-Authentifizierung können Sie die GFI ClearView-Appliance so konfigurieren, dass sie Anmeldeversuche von Benutzern über einen Remote-Radius-Server authentifiziert.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Stellen Sie sicher, dass RADIUS als Authentifizierungsmethode auf der Seite [AAA](#) ausgewählt ist.
6. Klicken Sie auf **Konfiguration > System > Authentifizierung** und wechseln Sie auf die Registerkarte **Radius**.
7. Definieren Sie die globalen RADIUS-Einstellungen.
8. Klicken Sie auf **Änderungen übernehmen**.
9. Geben Sie den Hostnamen oder die IP-Adresse des entfernten Radius-Servers an. Es können IPv4-Adressen angegeben werden. Es können mehrere Radius-Server definiert werden.
10. Klicken Sie auf **Neuen RADIUS-Server hinzufügen**.
11. Um Radius-Server von der GFI ClearView-Appliance zu entfernen, aktivieren Sie das Kontrollkästchen für den Server, und klicken Sie auf **Server entfernen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Ungespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.



4.3.6 TACACS+ Authentifizierung

Mit der TACACS+-Authentifizierung können Sie die GFI ClearView-Appliance so konfigurieren, dass sie Anmeldeversuche von Benutzern mit einem entfernten TACACS+-Server authentifiziert.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Stellen Sie sicher, dass TACACS+ als Authentifizierungsmethode auf der Seite [AAA](#) ausgewählt ist.
6. Klicken Sie auf **Konfiguration > System > Authentifizierung** und wechseln Sie auf die Registerkarte **TACACS+**.
7. Definieren Sie globale TACACS+-Authentifizierungsoptionen.
8. Klicken Sie auf **Änderungen übernehmen**.
9. Geben Sie den Hostnamen oder die IP-Adresse des entfernten TACACS+-Servers an. Es können IPv4-Adressen angegeben werden. Es können mehrere TACACS+-Server definiert werden.
10. Klicken Sie auf **Neuen TACACS+-Server hinzufügen**.
11. Um TACACS+-Server von der GFI ClearView-Appliance zu entfernen, aktivieren Sie das Kontrollkästchen für Server, und klicken Sie auf **Server entfernen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.

4.4 System Wartung

Erfahren Sie, wie Sie Ihre GFI ClearView Appliances warten können.

Auf dem Bildschirm Systemkonfiguration verwalten können Sie Systemkonfigurationsdateien herunterladen, speichern, wechseln, zurücksetzen und löschen. Sie erfahren, wie Sie Ihre Konfiguration sichern sowie Ihr Konfigurationssystem importieren und exportieren können.

4.4.1 Verwalten des Systems Konfiguration



Auf dem Bildschirm "Systemkonfiguration verwalten" können Sie Systemkonfigurationsdateien herunterladen, speichern, wechseln, rückgängig machen und löschen.

NOTE

To Manage System Configuration, navigate to **Configuration > System > Maintenance > Manage Config** on the Web UI, advanced mode.

In der nachstehenden Tabelle sind die verfügbaren Systemkonfigurationsdateien aufgeführt. Ein Häkchen befindet sich neben dem

aktive Konfiguration. Wenn Sie auf den Namen der Konfigurationsdatei klicken, wird die textbasierte Version Konfigurationsdatei im Fenster am unteren Rand dieser Seite angezeigt. Wenn Sie auf das Symbol "Herunterladen" neben der Konfigurationsdatei klicken, können Sie die textbasierte Version der Konfigurationsdatei herunterladen und speichern/backupen.

Configuration Files		
Filename	Active	Download
<input type="checkbox"/> initial.bak		
<input type="checkbox"/> initial	<input checked="" type="checkbox"/>	

- Delete the selected configuration(s).
- Make the selected configuration active and apply it to the system. (Select only one)
- Download the selected configuration as a binary file. (Select only one)

Wenn Sie eine Konfigurationsdatei auswählen und die Schaltflächen oben verwenden, können Sie die ausgewählten Dateien aus dem System löschen, zur ausgewählten Konfiguration wechseln oder die ausgewählte Konfigurationsdatei im Binärformat herunterladen.

Mit dem nachstehenden Formular können Sie die aktive und die laufende Konfiguration kontrollieren. Wenn es ungespeicherte Änderungen an der aktiven Konfiguration gibt, wird diese als "laufende Konfiguration" bezeichnet.

Active Configuration	
<input type="button" value="Save"/>	Save the running configuration to the active configuration file.
<input type="button" value="Revert"/>	Discard the running configuration and apply the contents of the active configuration file.
<input type="button" value="Save As"/>	Save the running configuration to a new file and make it active.
New filename: <input type="text"/>	

Sie können die laufende Konfiguration speichern und sie zur aktiven Konfiguration machen, die laufende Konfiguration auf den zuvor gespeicherten Zustand der aktiven Konfiguration zurücksetzen oder die laufende Konfiguration in einer neuen Konfigurationsdatei speichern und diese zur neuen aktiven Konfiguration machen.

So sichern Sie Ihre Appliance Einstellungen

Es wird empfohlen, eine Sicherungskopie der Konfiguration der GFI ClearView Appliance erstellen: »

Austausch von Festplatten

» Diagnose durch TAC »

Firmware-Upgrade

In der Regel konfigurieren Benutzer GFI ClearView einmal, und die Konfigurationsdatei muss nicht immer geändert werden. Führen Sie daher einfach die folgenden Schritte aus, um die lokal zu speichern. Wenn aus irgendeinem Grund regelmäßig ein Backup erforderlich ist, können Sie auch einen Auftrag dafür planen. Gehen Sie zu **System > Setup > Geplante Aufträge**.

Es gibt zwei Arten von Konfigurationsdateien für GFI ClearView: »

Binär

» Text (empfohlen)

Zum Herunterladen und Speichern der Konfigurationsdatei:

1. Gehen Sie zu Konfiguration > System > Wartung > Konfig. verwalten.

- Suchen Sie die Konfiguration, die Sie exportieren möchten. Die aktuell aktive Konfiguration ist mit einem grünen Häkchen markiert.
 - Um die Konfiguration als Textdatei zu speichern, klicken Sie auf das Speichersymbol in der Download-Spalte daneben. Die Erstellung der Datei nimmt einige Zeit in Anspruch. Die generierte Textdatei enthält alle CLI-Befehle zur Replikation der Konfiguration.
 - Um die Konfiguration als Binärdatei zu speichern, klicken Sie auf den Dateinamen.

System importieren Konfiguration

Der Bildschirm Systemkonfiguration importieren ermöglicht es Ihnen, zuvor gespeicherte oder gesicherte Systemkonfigurationsdateien zu importieren.

NOTE

To Import System Configuration, navigate to **Configuration > System > Maintenance > Import Config** on the Web UI, advanced mode.

Mit dem unten stehenden Formular können Sie Systemkonfigurationen hochladen, die lokal auf dem PC gespeichert wurden.

Upload Configuration	
<input checked="" type="radio"/> Upload local binary file:	<input type="text"/> <input type="button" value="Browse..."/> (To be saved as separate file with its original name)
<input type="radio"/> Upload local text file: (CLI commands)	<input type="text"/> <input type="button" value="Browse..."/> (To be executed immediately in the running configuration)

Upload Configuration

Screenshot 241: Hochladen von Systemkonfigurationen

Option	Description
Upload	Use this option to upload a saved binary configuration file. This file would have been downloaded as a binary file from the local System > Maintenance > Manage Config page. Once this file is uploaded, it will appear in the list of available configuration files on the System > Maintenance > Manage Config page.
Upload	Use this option to upload a text file containing CLI commands. The CLI commands will be executed in order and any configuration changes will be applied to the running configuration. This text file can contain one or more CLI commands or text. This text file could be a complete text-based system configuration file downloaded from the System > Maintenance > Manage Config page.

Verwenden Sie das nachstehende Formular, um eine Reihe von CLI-Befehlen auf der Web-UI auszuführen. Die CLI-Befehle werden der Reihe nach ausgeführt und alle Konfigurationsänderungen werden auf die laufende Konfiguration angewendet.

Execute CLI Commands

(To be executed immediately in the running configuration)

4.4.2 Werksvorgaben

Auf dem Bildschirm Factory Defaults (Werkseinstellungen) können Sie die Konfiguration der GFI ClearView-Appliance auf die zurücksetzen. Dabei werden auch alle Systemprotokolle und Überwachungsstatistiken entfernt.

NOTE

To restore Factory Defaults, navigate to **Configuration > System > Maintenance > Factory Defaults** on the Web UI, advanced mode.

Bei der Wiederherstellung der Werkseinstellungen bleiben die Einstellungen für die Netzwerkverbindung wie IP-Adresse, DNS-Server und Standard-Gateway erhalten. Es besteht auch die Möglichkeit, alle Überwachungsdaten zu erhalten. Um Überwachungsdaten zu erhalten, aktivieren Sie das Kontrollkästchen "Überwachung beibehalten", bevor Sie die Werkseinstellungen wiederherstellen.

Preserve monitoring data

Nach der Durchführung der Werkseinstellungen wird die GFI ClearView-Appliance automatisch neu gestartet.

4.4.3 Neustart/Herunterfahren

Über den Bildschirm Reboot/Shutdown können Sie Reboot-Optionen konfigurieren und die GFI ClearView-Appliance ordnungsgemäß herunterfahren, um sie neu zu starten oder auszuschalten.

In diesem Bereich GFI ClearView Web UI können Sie:

- [Neustart der GFI ClearView Appliance](#)
- [Automatischer Neustart der GFI ClearView-Appliance](#)
- [Herunterfahren der GFI ClearView-Appliance](#)

Neustart der GFI ClearView Appliance

Nachdem eine neue Version der ExOS-Firmware installiert wurde, müssen Sie die Appliance neu starten.

CAUTION

Any unsaved configuration changes will be lost if the Exinda appliance is rebooted or shutdown without saving the changes first.

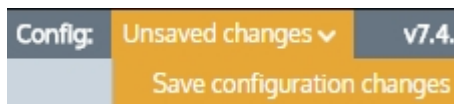
1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration > System > Wartung**, und wechseln Sie zur Registerkarte **Neustart / Herunterfahren**.
6. (Optional) Planen Sie den Neustart der GFI ClearView Appliance zu einem bestimmten Datum oder einer bestimmten Uhrzeit.
 - a. Prüfen Sie den **Zeitplan für den Neustart**.
 - b. Geben Sie das Datum und die Uhrzeit ein, zu der die Appliance neu gestartet werden soll.
7. Wählen Sie den Neustartmodus aus der Liste aus.
 - **Schneller Neustart:** Dies ist ein sanfter Neustart, bei dem nur das Betriebssystem neu gestartet wird. Dabei wird die Festplatte nicht neu gestartet und das BIOS nicht neu geladen.
 - **Langsamer Neustart:** Dies ist ein harter Neustart, bei dem die gesamte Appliance neu gestartet wird. Verwenden Sie diese Option, um auf das BIOS oder andere Startoptionen zuzugreifen.
8. Klicken Sie auf **Neustart**. Der Neustart der GFI ClearView Appliance kann einige Minuten in Anspruch nehmen.

Automatischer Neustart der GFI ClearView Appliance

Wenn die GFI ClearView Appliance nicht mehr reagiert, kann der System Watchdog die Appliance automatisch neu starten.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Configuration > System > Maintenance** und wechseln Sie zur Registerkarte **Reboot / Shutdown**.
6. Wählen Sie im Bereich System-Watchdog die Option **Aktivieren**.
7. Klicken Sie auf **Änderungen übernehmen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.



Herunterfahren der GFI ClearView Appliance

Wenn die GFI ClearView-Appliance ausgeschaltet werden muss, fahren Sie sie über die GFI ClearView Web UI herunter.

IMPORTANT

Any unsaved configuration changes will be lost if the GFI ClearView appliance is rebooted or shutdown without saving the changes first.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Configuration> System> Maintenance** und wechseln Sie zur Registerkarte **Reboot / Shutdown**.
6. Klicken Sie auf **Herunterfahren**.

Die GFI ClearView Appliance lässt sich nicht neu starten, sondern muss erneut eingeschaltet werden.

4.5 System Werkzeuge

Informieren Sie sich über die verschiedenen System-Tools, die auf Ihrer GFI ClearView Appliance zur Verfügung stehen und Sie bei Ihrer täglichen Arbeit unterstützen.

GFI ClearView Appliance bietet Ihnen eine Reihe von Netzwerk-Dienstprogrammen, mit denen Sie Netzwerkaktivitäten überwachen, Netzwerkinformationen sammeln und Netzwerkgeräte überprüfen können.

4.5.1 Ping

Verwenden Sie das Ping-Tool, um die Netzwerkkonnektivität zwischen der GFI ClearView-Appliance und anderen Hosts im WAN oder Internet zu testen.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration> System> Tools> Ping**.

IPv4 Host:

IPv6 Host:

```

PING ipv6.google.com(2404:6800:8007::63) 56 data bytes
64 bytes from 2404:6800:8007::63: icmp_seq=0 ttl=54 time=220 ms
64 bytes from 2404:6800:8007::63: icmp_seq=1 ttl=54 time=197 ms
64 bytes from 2404:6800:8007::63: icmp_seq=2 ttl=54 time=208 ms
64 bytes from 2404:6800:8007::63: icmp_seq=3 ttl=54 time=225 ms

--- ipv6.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 197.239/212.949/225.904/11.118 ms, pipe 2

```

6. Geben Sie im Feld **IPv4-Host** oder **IPv6-Host** eine IP-Adresse oder einen vollständig qualifizierten Domännennamen an, die bzw. den Sie anpingen möchten.
7. Klicken Sie auf **Ping**. Es kann ein paar Sekunden dauern, bis der Ping-Vorgang abgeschlossen ist und die Ergebnisse angezeigt werden.

4.5.2 Traceroute

Verwenden Sie das Traceroute-Tool, um die Netzwerksprünge von der GFI ClearView-Appliance zu anderen Hosts im WAN oder Internet zu ermitteln.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.

- Klicken Sie auf **Anmelden**.
- Klicken Sie auf Konfiguration> System> Tools> Traceroute.

Host:

```
traceroute to ipv6.google.com (2404:6800:8007::68), 30 hops max, 40 byte packets
 1 2001:44b8:62:690::1 1.783 ms 1.753 ms 1.747 ms
 2 2001:44b8:61::1fc 52.539 ms 53.961 ms 54.147 ms
 3 2001:44b8:8060:8000::1 55.682 ms 56.831 ms 57.364 ms
 4 2001:44b8:8060:e::1 58.248 ms * *
 5 2001:44b8:8060:l::a 83.433 ms * *
 6 2001:4860:1:1:0:1283:0:4 86.152 ms 85.641 ms 86.588 ms
 7 2001:4860::1:0:9f7 92.365 ms 103.509 ms 2001:4860::1:0:9f8 102.835 ms
 8 2001:4860::1:0:165 210.179 ms 209.501 ms 209.033 ms
 9 2001:4860:0:1::e7 216.582 ms 215.693 ms 225.739 ms
10 2404:6800:8007::68 213.035 ms 212.868 ms 219.553 ms
```

- Geben Sie im Feld **Host** eine IPv4- oder IPv6-Adresse oder einen vollständig qualifizierten Domännennamen an, um den Traceroute-Versuch durchzuführen.
- Klicken Sie auf **Traceroute**. Es kann ein paar Sekunden dauern, bis der Vorgang abgeschlossen ist und die Ergebnisse angezeigt werden.

4.5.3 DNS Nachschlagen

Verwenden Sie das DNS-Lookup-Tool, damit die GFI ClearView-Appliance die konfigurierten DNS-Server abfragt, um den angegebenen Domännennamen aufzulösen.

- Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
- Geben Sie den **Benutzernamen** und das **Passwort** ein.
- Klicken Sie auf **Anmelden**.
- Klicken Sie auf Konfiguration> System> Tools> DNS Lookup.

Domain:

```
www.google.com has address 173.194.77.105
www.google.com has address 173.194.77.106
www.google.com has address 173.194.77.147
www.google.com has address 173.194.77.99
www.google.com has address 173.194.77.103
www.google.com has address 173.194.77.104
www.google.com has IPv6 address 2607:f8b0:4003:c01::68
```

- Geben Sie im Feld Domäne einen vollständig qualifizierten Domännennamen an, nach dem gesucht werden soll.
- Klicken Sie auf **Nachschlagen**. Es kann ein paar Sekunden dauern, der Vorgang abgeschlossen ist und die Ergebnisse angezeigt werden.

4.5.4 Abfrage einer entfernten IPMI-Appliance GFI ClearView

Verwenden Sie das IPMI-Tool, um den Energiestatus abzufragen, eine entfernte GFI ClearView-Appliance über IPMI aus- und einzuschalten oder zurückzusetzen. Die Remote-Appliance muss [den IPMI-Zugriff aktiviert](#) haben.

Power Control Options

Command

Remote IPMI Login Details

IPv4 Address

Username

Password

So führen Sie eine IPMI-Aktion auf einer entfernten GFI ClearView-Appliance aus

1. Wählen Sie die gewünschte Aktion aus der Dropdown-Liste **der Stromversorgungsoptionen** aus.

2. Geben Sie die IPMI **IPv4-Adresse** der entfernten Appliance ein.
3. Geben Sie die IPMI-Authentifizierungsdaten für die Remote-Appliance ein.
 - Der Standardbenutzername ist admin.
 - Das Standardpasswort lautet exinda.
4. Klicken Sie auf **Power Action ausführen**.

Beispiel: Schalten Sie die GFI ClearView-Appliance mit der IPMI-Adresse 192.168.110.61 aus.

```
ipmi power adresse 192.168.110.61 benutzername admin passwort exinda control cycle
```

Beispiel: Anzeigen des aktuellen Stromversorgungsstatus der GFI ClearView-Appliance mit der IPMI-Adresse 192.168.110.61 -

```
show ipmi power adresse 192.168.110.61 benutzername admin passwort exinda
```

4.5.5 iPerf Client

iPerf ist ein Tool zur Messung des Netzdurchsatzes. Damit es funktioniert, müssen zwei Geräte die iPerf-Software ausführen, um Bandbreitenmetriken zwischen zwei Endpunkten zu erhalten. Ein Gerät spielt dabei die Rolle des Servers, das andere die Rolle des Clients. In GFI ClearView gibt es eine Web-Benutzeroberfläche, mit der eine GFI ClearView-Appliance als iPerf-Client konfiguriert werden kann:

So konfigurieren Sie eine GFI ClearView Appliance als iPerf-Client:

1. Klicken Sie auf Konfiguration> System> Tools> Iperf Client.

2. Geben Sie in das Feld **Server** die **IP-Adresse** oder den **Hostnamen** eines iPerf-Servers ein, der bereits läuft.

3. Klicken Sie auf Tests ausführen, um die Testergebnisse anzuzeigen. Beispiel Ergebnisse:

EXAMPLE

```
-----  
Client connecting to 10.10.1.201, TCP port 5001  
TCP window size: 23.2 KByte (default)  
-----  
[ 3] local 10.10.1.200 port 58760 connected with 10.10.1.201 port  
5001 [ ID] Interval Transfer Bandwidth  
[ 3] 0.0-10.0 sec 4.74 GBytes 4.07 Gbits/sec
```

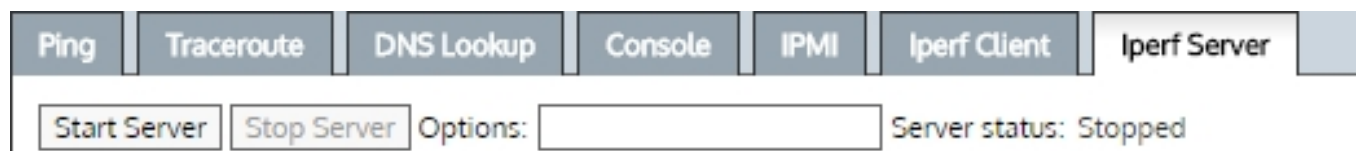
4.5.6 iPerf Server

iPerf ist ein Tool zur Messung des Netzdurchsatzes. Damit es funktioniert, müssen zwei Geräte die iPerf-Software ausführen, um Bandbreitenmetriken zwischen zwei Endpunkten zu erhalten. Ein Gerät spielt dabei die Rolle des Servers, das andere die Rolle des Clients. In GFI ClearView gibt es eine Web-Benutzeroberfläche, mit der eine Appliance als iPerf-Server konfiguriert werden kann:

So konfigurieren Sie eine GFI ClearView Appliance als iPerf-Server:

Verwenden Sie Registerkarte iPerf-Server, wenn die GFI ClearView-Appliance der designierte Server ist.

1. Klicken Sie auf Konfiguration> System> Tools> Iperf Server.



2. (Optional), Standardmäßig lauscht ein iPerf-Server auf TCP-Pakete an Port 5001. Sie können jedoch die folgende Liste von Optionen verwenden, um diese Bedingung zu ändern:

Verwendung: `iperf [-s|-c host]`

[options] Beispiel:

`iperf[-h]--help[-v|--version]`

Optionen für Clients und Server

`-f, --format [kmKM]` zu meldendes Format: Kbits, Mbits, KBytes, MBytes

`-i, --interval #` Sekunden zwischen periodischen Bandbreitenberichten

`-l, --len #[KM]` Länge des zu lesenden oder schreibenden Puffers (Standard 8 KB)

`-m, --print_mss print` TCP maximale Segmentgröße (MTU - TCP/IP-Header)

`-o, --output <Dateiname>` Ausgabe des Berichts oder der Fehlermeldung in angegebene Datei

`-p, --port #` Server-Port zum Abhören/Verbinden mit

`-u, --udp` UDP statt TCP verwenden

`-w, --window #[KM]` TCP-Fenstergröße (Socket-Puffergröße)

`-B, --bind <Host>` bindet an <Host>, eine Schnittstelle oder eine Multicast-Adresse

`-C, --Kompatibilität` zur Verwendung mit älteren Versionen sendet keine zusätzlichen Nachrichten

`-M, --mss #` setzt die maximale TCP-Segmentgröße (MTU - 40 Bytes)

`-N, --nodelay` setzt TCP keine Verzögerung, deaktiviert Nagles Algorithmus

-V, --IPv6Version Setzt die Domäne auf IPv6

Optionen nur für Server

-s, --server Ausführung im Servermodus

-U, --single_udp im Single-Threaded-UDP-Modus ausführen

-D, --daemon lässt den Server als Daemon laufen

Optionen nur für Kunden

-b, --bandwidth #[KM] für UDP, zu sendende Bandbreite in Bits/Sek (Standard 1 Mbit/Sek, impliziert -u)

-c, --client <Host> läuft im Client-Modus und verbindet sich mit <Host>

-d, --dualtest Gleichzeitig einen bidirektionalen Test durchführen

-n, --num #[KM] Anzahl der zu Übertragenden Bytes (anstelle von -t)

-r, --tradeoff Einen bidirektionalen Test einzeln durchführen

-t, --time # Zeit in Sekunden für die Übertragung (Standard 10 Sek.)

-F, --fileinput <Name> Eingabe der zu Übertragenden Daten aus einer Datei

-I, --stdin Eingabe der zu Übertragenden Daten von stdin

-L, --listenport # Port, auf dem bidirektionale Tests empfangen werden

-P, --parallel # Anzahl der parallelen Client-Threads, die ausgeführt werden

-T, --ttl # time-to-live, für Multicast (Standard 1)

-Z, --linux-congestion <algo> Festlegen des TCP-Überlastungssteuerungsalgorithmus (nur Linux)

Verschiedene Optionen

-x, --reportexclude [CDMSV] ausschließen C(Verbindung) D(Daten) M(Multicast) S(Einstellungen) V(Server) Berichte

-y, --reportstyle C-Bericht als kommagetrennte Werte

-h, --help diese Meldung ausgeben und beenden

-v, --version Versionsinformationen ausgeben und beenden

Wenn der Iperf-Server z. B. UDP-Pakete an Port 319 abhören soll, müssen Sie die folgenden Optionen verwenden:

-u -p 319

3. Geben Sie in das Textfeld **Optionen** die gewünschten Optionen ein und klicken Sie dann auf die Schaltfläche **Server starten**. Der Server muss gestartet werden, bevor Verkehr von einem Iperf-Client ausgelöst wird.

Nachdem der Server gestartet wurde, können Sie die Verbindung von einem Iperf-Client aus testen, indem Sie den Hostnamen als Parameter angeben. Beispiel Ergebnisse:

EXAMPLE

```
-----  
Server listening on TCP port 5001  
TCP window size: 85.3 KByte  
(default)  
-----  
[ 4] local 10.10.1.200 port 5001 connected with 10.2.6.228 port  
58665 [ ID] Interval Transfer Bandwidth  
[ 4] 0.0-10.1 sec 112 MBytes 93.2 Mbits/sec
```


5 Fehlersuche





Hier erfahren Sie, wie Sie Probleme, die bei der Verwendung von GFI ClearView Appliances auftreten können, beheben können. Viele der hier aufgeführten Informationen sind auch an anderer Stelle in der Hilfe zu finden, wurden jedoch an dieser Stelle als zentraler Ort für den Zugriff auf Informationen zur Fehlerbehebung zusammengestellt.

5.1 Diagnostik

Lernen Sie die verschiedenen Diagnosetools kennen, die auf Ihrer GFI ClearView Appliance zur Verfügung stehen. Sie können diese Tools zur Fehlerbehebung bei Problemen einsetzen.

5.1.1 Diagnose Dateien

Diagnosedateien enthalten Informationen zum Systemstatus und können bei der Fehlersuche helfen. Diagnosedateien können vom GFI ClearView TAC angefordert werden. Sie können über das unten stehende Formular generiert und heruntergeladen werden.

Diagnostics Files			
<input type="checkbox"/>	File Name	Timestamp	File Size
<input type="checkbox"/>	 sysdump-exinda-2d852c-wsmd-20230830-101625.tgz	Wed Aug 30 10:17:17 UTC 2023	10805140 bytes
<input type="checkbox"/>	 sysdump-exinda-2d852c-sched-20230830-101518.tgz	Wed Aug 30 10:16:24 UTC 2023	10784105 bytes
<input type="checkbox"/>	 sysdump-exinda-2d852c-wccpd-20230816-162215.tgz	Wed Aug 16 16:22:59 UTC 2023	12483594 bytes
<input type="checkbox"/>	 sysdump-exinda-2d852c-tcpad-20230816-162132.tgz	Wed Aug 16 16:22:15 UTC 2023	12495240 bytes

System-Snapshots werden automatisch erstellt, wenn ein Prozess fehlschlägt. Wenn die Option "Automatische Support-Benachrichtigungen" aktiviert ist, werden sie zur weiteren Fehlerbehebung automatisch an GFI ClearView TAC gesendet.

System Snapshot Files			
<input type="checkbox"/>	File Name	Timestamp	File Size
No System Snapshot Files.			

Auto Support	
Auto Support Notifications	<input checked="" type="checkbox"/> Enable

NOTE

Valid SMTP and DNS settings are required for diagnostics to be sent to GFI ClearView TAC.

5.1.2 Monitor

Die Monitordiagnose zeigt die aktuellen Monitoreinstellungen und den Status der Monitor- und Kollektorprozesse an.

NOTE

To configure Monitor settings, navigate to **Configuration > System > Setup > Monitoring** on the Web UI, advanced mode.

```
Table size           : 50
Chart size           : 10
Realtime Window      : 10
Graphing              : flash
Detailed Monitoring   : yes
Ignore Internal-to-Internal : yes

Layer7 Monitoring    :
  Enabled             : yes
  Bittorrent Sensitivity : High
  Bittorrent Sensitivity : High
  EDonky Sensitivity   : Med
  Skype Sensitivity   : High

Host Resolution      :
  Order : DNS Rank : 2
  Order : IP Rank  : 4
  Order : Netbios Rank : 3
  Order : Network_Object Rank : 1

Monitor Status       : OK

Collector Status     : OK
Current Timestamp    : 1287546720
```

5.1.3 NIC Diagnostik

Die NIC-Diagnoseseite kann bei der Behebung von Problemen mit der Netzwerkverzögerung helfen. NIC-Fehler, Kollisionen und Verwerfungen weisen auf ein Verhandlungsproblem hin, das zu Paketverlusten und Netzwerkverzögerungen führen kann. Es wird empfohlen, Verhandlungsprobleme sofort zu beheben.

Die ersten Zeilen zeigen eine Zusammenfassung der installierten Netzwerkadapter. Detaillierte Informationen erhalten Sie mit dem CLI-Befehl "show diag".

NOTE

To configure NIC settings, navigate to **Configuration > System > Network > NICs** on the Web UI, advanced mode.

```
Slot 1: PEG2BPI-SD, 2 ports, 1G/RJ-45/1000BASE-T, 1-tx/rx queue
Slot 2: Empty
```

Interface br10 state

```
Admin up:      yes
Link up:       yes
IP address:
Netmask:
Speed:         N/A
Duplex:        N/A
Interface type: ethernet
Interface source: bridge
MTU:           1500
HW address:    00:E0:ED:13:73:C2
Comment:
```

```
RX bytes:      37940508
RX packets:    514502
RX mcast packets: 514502
RX discards:   0
RX errors:     0
RX overruns:   0
RX frame:      0
```

```
TX bytes:      0
TX packets:    0
TX discards:   0
TX errors:     0
TX overruns:   0
TX carrier:    0
TX collisions: 0
```

5.1.4 RAID Diagnose

Die RAID-Diagnoseseite ist bei Modellen verfügbar, die Redundant Storage unterstützen. Es werden eine Zusammenfassung des Status des logischen Volumens sowie Details zu RAID-Adaptoren, logischen Volumina und physischen Laufwerken angezeigt.

```

Adapter: 0 Logical: 0 Size: 1429248MB State: Optimal
Adapter: 0
  Model:          PERC 6/i Integrated
  Serial:         1122334455667788
  Firmware:      6.2.0-0013
  Host Interface: PCIE
  Supported Drives: SAS, SATA
  Levels:        RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
  Memory:        Present, 256MB
  Battery:       Yes
  Alarm:         Disabled
  Current Time:  3:53:4 3/29, 2011
Logical Drive: 0
  Adapter:       0
  Size:          1429248MB
  Stripe:        64kB
  Raid Level:    Primary-1, Secondary-3, RAID Level Qualifier-0
  Drives:       2
  Span Depth:    3
  Cache Policy: WriteBack, ReadAheadNone, Direct, No Write Cache if Bad BBU
  State:         Optimal
Drive: 0
  Adapter:       0
  Slot:          0
  Type:          SAS
  Inquiry:       SEAGATE ST3500414SS      KS679WJ01HND
  Firmware:      Online
  Raw Size:      476940MB [0x3a386030 Sectors]
  Media Errors:  0
  Other Errors:  0
  Predictive Errors: 0
  Sequence:      2
Drive: 1
  Adapter:       0
  Slot:          1
  Type:          SAS
  Inquiry:       SEAGATE ST3500414SS      KS679WJ0275D
  Firmware:      Online
  Raw Size:      476940MB [0x3a386030 Sectors]
  Media Errors:  0
  Other Errors:  0
  Predictive Errors: 0
  Sequence:      2
Drive: 2
  Adapter:       0
  Slot:          2
  Type:          SAS
  Inquiry:       SEAGATE ST3500414SS      KS679WJ033KN
  Firmware:      Online
  Raw Size:      476940MB [0x3a386030 Sectors]

```

5.1.5 TCP Dump

Ein TCP-Dump erfasst Pakete, die von den angegebenen Schnittstellen übertragen oder empfangen werden, und kann bei der Fehlersuche helfen. Ein TCP-Dump kann von GFI ClearView TAC angefordert werden.

Führen Sie einen TCP-Dump von der GFI ClearView Appliance aus

Klicken Sie auf Konfiguration > Diagnostik> TCPDump.

Run TCP Dump

Interface

Timeout

Filter

Status **Stopped**

Treffen Sie die folgenden Auswahlen und klicken Sie dann auf TCP-Dumps generieren:

Interface	Select an interface to run the TCP dump on. Select ALL to capture packets on all (link up) interfaces. Note When ALL is selected for the Interface, only those interfaces which are link up will be included.
Timeout	Select the amount of time for which the TCP Dump will run.
Filter	Set a filter if required. Refer to the Common User Case examples below for specific filters to use in common circumstances.
Status	Shows the status of a running TCP Dump

Allgemeine Verwendung Fälle

Die folgenden Beispiele zeigen die Syntax, die in das Feld Filter eingegeben werden muss, um Daten aus einer bestimmten Quelle zu erfassen.

So sammeln Sie den Datenverkehr von/zu einem einzelnen Host

Host <IP-Adresse>

Beispiel: Host 1.2.3.4

So erfassen Sie den Datenverkehr von einem einzelnen Host, der die Quelle des Datenverkehrs ist

src <IP-Adresse>

Beispiel: src 1.2.3.4

So erfassen Sie den Datenverkehr von einem einzelnen Host, der das Ziel für den Datenverkehr ist

dst <IP-Adresse>

Beispiel: dst 1.2.3.4

So erfassen Sie den Datenverkehr zwischen zwei Hosts

Host <IP-Adresse 1> und Host <IP-Adresse 2>

Beispiel Host 1.2.3.4 und Host 5.6.7.8

So sammeln Sie den Datenverkehr zu/von einem Subnetz

Netz <IP-Teilnetz>

Beispiel: Netz 1.2.3.0/24






So erfassen Sie den Datenverkehr zwischen zwei Subnetzen

src-Netz <IP-Subnetz> und dst-Netz <IP-Subnetz>

Beispiel: src-Netz 1.2.3.0/24 und dst-Netz 1.2.4.0/24

Senden Sie einen TCP-Dump an GFI ClearView TAC

Gespeicherte TCP-Dumps können über das unten stehende Formular heruntergeladen und/oder per E-Mail an GFI ClearView TAC gesendet werden.

TCP Dump Files			
<input type="checkbox"/>	File Name	Timestamp	File Size
<input type="checkbox"/>	 capture-weber-monitor-20150220-154907.tar.gz	Fri Feb 20 15:49:07 EST 2015	308224 bytes
<input type="checkbox"/>	 capture-weber-monitor-20150213-104642.tar.gz	Fri Feb 13 10:46:43 EST 2015	3087354 bytes
<input type="checkbox"/>	 capture-weber-monitor-20141217-162605.tar.gz	Wed Dec 17 16:26:19 EST 2014	224519218 bytes
<input type="checkbox"/>	 capture-weber-monitor-20141217-133350.tar.gz	Wed Dec 17 13:33:53 EST 2014	31631085 bytes
<input type="checkbox"/>	 capture-weber-monitor-20141217-133348.tar.gz	Wed Dec 17 13:33:50 EST 2014	31631085 bytes

Weitere Informationen über TCP-Dump-Filter finden Sie unter <https://danielmiessler.com/study/tcpdump/#common>.

5.1.6 Anzeigen des Status eines Alarms

Systemwarnungen informieren Sie über Systemprobleme, die möglicherweise weitere Aufmerksamkeit und Fehlerbehebung erfordern. Wenn ein Systemalarm ausgelöst wird, wird der Systemstatus auf "Warnung" gesetzt und eine E-Mail-Benachrichtigung gesendet.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie auf **Konfiguration > System > Diagnose**, und wechseln Sie zur Registerkarte **System**. Alles, was Alarme generiert hat, zeigt das letzte Mal an, als ein Alarm ausgelöst wurde, sowie die Gesamtzahl der Alarme, die gesendet wurden.
5. Um den Alarm, der die Warnung ausgelöst hat, anzuzeigen, klicken Sie auf den Namen des Alarms. Verwenden Sie die Informationen in dieser Warnung, um das Problem zu beheben.
6. Um den Verlauf einer Warnung zu löschen, klicken Sie auf **Zurücksetzen**. Der Systemzustandsstatus wird auf OK zurückgesetzt.

Alert Name	Beschreibung
CPU-Auslastung	Alarm wird ausgelöst, wenn der Schwellenwert für die CPU-Auslastung erreicht wird. Die Auslöse- und Löschwelldwerte können geändert werden. Die Standardwerte sind 95 % bzw. 80 % Auslastung.
Systemplatte voll	Alarm wird ausgelöst, wenn der Schwellenwert für den belegten Speicherplatz erreicht wird. Die Schwellenwerte für Auslösung und Löschen können geändert werden. Die Standardwerte sind 7 % bzw. 10 % freier Speicherplatz.
Speicherauslagerung	Warnung vor Speichernutzung und Paging. Dies bedeutet, dass die Daten im RAM auf die Festplatte ausgelagert werden. Übermäßige Paging-Warnungen können auf ein System hinweisen, das über zu wenig RAM-Ressourcen verfügt. Prüfen Sie die RAM- und SWAP-Diagramme unter Überwachung > System.
Link-Verhandlung	Alarm wird ausgelöst, wenn die Geschwindigkeit/Duplex auf einer Schnittstelle auf Auto eingestellt ist, diese aber mit Halbduplex und/oder 10 Mbps verhandelt.
NIC-Probleme	Warnung, die ausgelöst wird, wenn auf den Schnittstellen Fehler auftreten.

NIC-Kollisionen	Alarm, der ausgelöst wird, wenn auf den Schnittstellen Kollisionen vorhanden sind. Die Auslöse- und Löschschwellenwerte können geändert werden. Die Standardwerte sind 20 bzw. 1 pro 30 Sekunden.
NIC Verlorene Pakete	Warnung, die ausgelöst wird, wenn auf den Schnittstellen verworfene Pakete vorhanden sind.
Signierte SMB-Verbindungen	Warnung, die ausgelöst wird, wenn signierte SMB-Verbindungen vorhanden sind.
Redundante Stromversorgung	Alarm, der ausgelöst wird, wenn eines der Netzteile ausfällt (nur auf Plattformen mit Stromredundanz verfügbar).
Redundanter Speicher	Alarm, der ausgelöst wird, wenn eine der Festplatten ausfällt (nur auf Plattformen mit Speicherredundanz verfügbar).

5.1.7 Eröffnen Sie einen Fall mit ClearView Support Services

Wenn Sie ein Problem oder eine Frage zu GFI ClearView haben, lesen Sie bitte in der Wissensdatenbank nach, oder erstellen Sie über das Support-Portal ein Ticket beim Kunden-Support-Team.

5.2 Log Dateien

Informieren Sie sich über die verschiedenen Protokolldateien, die auf einer GFI ClearView Appliance gespeichert sind, und erfahren Sie, wie Sie diese Protokolle bei der Behebung von Problemen nutzen können, die bei Ihnen auftreten können.

5.2.1 Live Protokoll

Auf der Seite Live Log können Sie neue Einträge im System Log in Echtzeit sehen.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration > System > Logging** und wechseln Sie auf die Registerkarte **Live Log**.

NOTE

A dot/period (.) character is displayed after a few seconds of inactivity to indicate the Live Log is still active.

5.2.2 Schwanz Log

Auf der Seite Tail Log können Sie die letzten Einträge in der Systemprotokolldatei einsehen.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.

3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration> System> Logging** und wechseln Sie auf die Registerkarte **Tail Log**.
6. Legen Sie fest, wie viele Zeilen angezeigt werden sollen und in welcher Reihenfolge die Protokolleinträge angezeigt werden sollen.

View Last: Lines View Log Order: ▼

7. Um diese Seite zu aktualisieren und sicherzustellen, dass alle neuen Protokolleinträge seit der Aktualisierung dieser Seite angezeigt werden, klicken Sie auf **Go**.

5.2.3 Systemprotokollierung Konfiguration

Auf der Seite Konfiguration der Systemprotokollierung können Sie verschiedene Aspekte der Systemprotokollierung anpassen, einschließlich des Exports an entfernte Syslog-Server.

In diesem Bereich GFI ClearView Web UI können Sie:

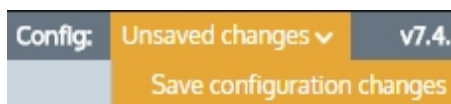
- [Konfigurieren Sie die Appliance-Protokolldateien](#)
- [Hinzufügen eines entfernten Syslog-Servers](#)
- [Entfernen eines entfernten Syslog-Servers](#)

Konfigurieren Sie die Appliance-Protokolldateien

Auf der Seite Konfiguration der Systemprotokollierung können Sie verschiedene Aspekte der Systemprotokollierung anpassen, einschließlich des Exports an entfernte Syslog-Server.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration> System> Protokollierung** und wechseln Sie auf die Registerkarte **Einrichtung**.
6. Geben Sie das Format an, in dem die Protokolldateien gespeichert werden sollen. Die Standardform ist in der Regel ausreichend, jedoch bevorzugen einige externe Protokolldateiparser die Protokolldatei im WELF-Format.
7. Wählen Sie den Schweregrad der Protokolleinträge, die gespeichert werden sollen. Jeder Protokolleintrag mit diesem Schweregrad oder niedriger wird in der Systemprotokolldatei gespeichert.
8. Wählen Sie aus, wann die Protokolle gedreht werden sollen. Um die Rotation des Systemprotokolls sofort zu erzwingen, klicken Sie auf **Rotation jetzt erzwingen**.
9. Geben Sie an, wie viele Protokolldateien aufbewahrt werden sollen, bevor sie dauerhaft von der GFI ClearView-Appliance entfernt werden.
10. Klicken Sie auf **Änderungen übernehmen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.



Hinzufügen eines entfernten Syslog-Servers

Fügen Sie der GFI ClearView-Appliance Remote-Syslog-Server hinzu, um Systemprotokolleinträge mit einem bestimmten Schweregrad an einen oder mehrere Remote-Syslog-Server weiterzuleiten.

Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).

1. Geben Sie den **Benutzernamen** und das **Passwort** ein.
2. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration > System > Protokollierung** und wechseln Sie auf die Registerkarte **Einrichtung**.
6. Geben Sie im Bereich Add New Remote Sink den Hostnamen oder die IPv4-Adresse des entfernten Syslog-Servers ein. IPv6-Adressen werden für entfernte Senken nicht unterstützt.
7. Wählen Sie den Schweregrad der Protokolleinträge, die an den entfernten Syslog-Server gesendet werden. Jeder Protokolleintrag mit diesem Schweregrad oder niedriger wird gesendet.
8. Klicken Sie auf **Neue entfernte Senke hinzufügen**.

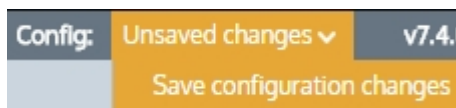
Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.

Entfernen eines entfernten Syslog-Servers

Um die Weiterleitung von Systemprotokolleinträgen an einen entfernten Syslog-Server zu beenden, entfernen Sie den Server von der GFI ClearView-Appliance.

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Konfiguration > System > Protokollierung** und wechseln Sie auf die Registerkarte **Einrichtung**.
6. Wählen Sie den Server aus der Liste Entfernte Protokollsenken aus, und wählen Sie **Ausgewählte entfernen**.
7. Klicken Sie auf **Neue entfernte Senke hinzufügen**.

Um die Änderungen in der Konfigurationsdatei zu speichern, klicken Sie in der Statusleiste auf das Menü Nicht gespeicherte Änderungen und wählen Sie Konfigurationsänderungen speichern.



Entfernen von Ereignissen aus dem Protokoll des Appliance-Systems

Der BMC-Prozessor führt ein Protokoll der Systemereignisse, einschließlich Stromversorgungsstatus, Stromredundanz und Eindringen in das Gehäuse. Der folgende Befehl kann verwendet werden, um diese Ereignisse regelmäßig in das Systemprotokoll der Appliance zu übertragen.

```
(config) # ipmi sel enable
```

5.3 Behebung von Problemen mit der Konfiguration von Active Directory

Wenn Sie Probleme mit der Active Directory-Integration haben, finden Sie hier Informationen zur Fehlerbehebung

kann helfen, das Problem zu lösen.

5.3.1 GFI ClearView Appliance wird jede Nacht neu gestartet

Problem

Wenn bei mehreren Installationen des GFI ClearView AD Connector die Option **Active Directory-Benutzer- und Gruppeninformationen beim Start an die GFI ClearView-Appliance(n) senden** aktiviert ist, kann die GFI ClearView-Appliance mit doppelten Daten von den Konnektoren überlastet werden, was zu einer Abschaltung der Appliance führen kann.

Lösung

1. Überprüfen Sie auf jeder Instanz des GFI ClearView AD Connector, ob die Option **Active Directory-Benutzer- und Gruppeninformationen beim Start an die GFI ClearView-Appliance(s) senden** aktiviert ist.
2. Wenn die Option in mehr als einer Instanz aktiviert ist, deaktivieren Sie sie in allen GFI ClearView AD Connectors.
3. Wählen Sie eine Instanz des GFI ClearView AD Connector, aktivieren Sie das Kontrollkästchen **Active Directory-Benutzer- und Gruppeninformationen beim Start an GFI ClearView-Appliance(s) senden**, und klicken Sie auf **OK**.

5.3.2 Der WMI-Dienst wird nicht ausgeführt

Problem

Wenn ich versuche, auf den GFI ClearView AD Connector zuzugreifen, wird die folgende Meldung angezeigt: "Das Installationsprogramm hat festgestellt, dass der WMI-Dienst nicht ausgeführt wird. In der Windows-Hilfe finden Sie Informationen zum Starten des WMI-Dienstes".

Lösung

Diese Meldung zeigt an, dass der Windows Management Information (WMI)-Dienst deaktiviert ist. Der GFI ClearView AD Connector kann erst dann ordnungsgemäß ausgeführt werden, wenn der WMI-Dienst gestartet wurde.

Um den WMI-Dienst zu starten, geben Sie an einer Eingabeaufforderung den folgenden Befehl ein: `net start winmgmt`

5.3.3 Anzeige des Systemkontos in den Verkehrsberichten

Problem

Bei der Anzeige von Konversationen werden die IP-Adresse und der Benutzername eines Kontos, das für das Signieren von SMB-Datenverkehr erstellt wurde, als Datenverkehr erzeugend angezeigt und nicht der tatsächliche Benutzer, der den Datenverkehr erzeugt.

Lösung

Wenn die SMB-Signatur konfiguriert und aktiviert ist, ist das SMB-Signaturkonto das letzte Benutzerkonto

als IP-Adresse registriert ist, überträgt der GFI ClearView AD Connector das SMB-Signaturkonto als den Benutzernamen, der den Datenverkehr erzeugt. Um das SMB-Signaturkonto zu ignorieren und den Datenverkehr als vom tatsächlichen Benutzer generiert zu melden, konfigurieren Sie GFI ClearView AD Connector so, dass das SMB-Signaturkonto ignoriert wird. Weitere Informationen finden Sie unter [Ausschluss bestimmter Benutzernamen aus Berichten](#).

5.3.4 Keine Kommunikation zwischen dem GFI ClearView AD Connector und der GFI ClearView Appliance

Problem

Sie sehen eines der folgenden Symptome:

- » Es kann keine Verbindung zwischen dem GFI ClearView AD Connector und der GFI ClearView Appliance hergestellt werden.
- » Der Status Letzter Kontakt auf der Registerkarte **Konfiguration** > **System** > **Netzwerk** > **Active Directory** ist leer oder rot.

Auflösung

1. Stellen Sie sicher, dass Ihre Firewall den ein- und ausgehenden Datenverkehr an dem für die GFI ClearView Appliance konfigurierten Port für die Kommunikation mit dem GFI ClearView AD Connector zulässt.

5.3.5 GFI ClearView AD Connector stoppt die Ausführung von

Problem

Nach einem Neustart des GFI ClearView AD Connector oder des GFI ClearView AD-Dienstes kann es vorkommen, dass der GFI ClearView AD Connector nicht weiterläuft und immer wieder neu gestartet werden muss.

Lösung

Um dies zu beheben:

1. Der GFI ClearView AD Connector erfordert die .NET-Version 4.0, damit er auf anderen Server als dem Active Directory-Server erfolgreich ausgeführt werden kann. Stellen Sie sicher, dass .NET 4.0 oder höher auf dem Server installiert ist, auf dem GFI ClearView AD Connector ausgeführt wird.
2. Wenn der Active Directory-Server unter Windows 2003 R2 läuft, muss der GFI ClearView AD Connector direkt auf dem Active Directory-Server installiert werden.
3. Überprüfen Sie Ihre Ereignisprotokolle auf .NET RunTime-Fehler und versuchen Sie, diese Fehler zu beheben. Möglicherweise muss die .NET-Installation neu installiert werden und die .NET 4.0-Dienste und andere Umgebungsdienste wie WMI müssen aktualisiert werden.

5.3.6 Ausgeschlossene Benutzer werden weiterhin auf der GFI ClearView Appliance angezeigt

Problem

Obwohl ein Benutzername zur Liste der ausgeschlossenen Benutzer auf GFI ClearView AD Connector hinzugefügt wurde,

wird der Benutzername weiterhin mit dem Datenverkehr auf der GFI ClearView Appliance in Verbindung gebracht.

Lösung

1. Überprüfen Sie, ob der Benutzername auf der Registerkarte "Ausgeschlossen" des GFI ClearView AD Connector mit dem Benutzernamen in Active Directory übereinstimmt. Beim Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden. Wenn das Active Directory beispielsweise den Benutzer `Domain/Test.User` enthält und die Ausschlussliste den Benutzer als `Domain/test.user` enthält, wird der Datenverkehr nicht ausgeschlossen.

NOTE

Regardless of the case of usernames in Active Directory, ClearView Appliance displays the usernames with the first name capitalized and the surname in lower case; for example `Domain/test.user`. Do not use the value in the Exinda Appliance when adding a username to the Excluded list.

2. Wenn der Fall bei den Benutzernamen übereinstimmt, starten Sie den AD-Client-Dienst neu, und nummerieren Sie die GFI ClearView-Appliance neu.

5.3.7 Änderungen am GFI ClearView Active Directory Controller haben keine Auswirkungen

Problem

Nach Änderungen an der Konfiguration des GFI ClearView Active Directory Controllers scheinen die von der GFI ClearView Appliance gemeldeten Informationen die gleichen zu sein wie vor den Änderungen.

Lösung

Starten Sie den AD Client Service neu, und führen Sie die GFI ClearView Appliance erneut aus, um sicherzustellen, dass die neueste Konfiguration verwendet wird.

5.3.8 Die IP-Adressen werden nicht den AD-Benutzern und Gruppen zugeordnet.

Problem

Bei der Integration des AD-Clients mit der GFI ClearView-Appliance werden die IP-Adressen nicht den Benutzern und Gruppen auf der GFI ClearView-Appliance zugeordnet.

Lösung

Die Anmeldeüberprüfung muss aktiviert sein, damit die IP-Adresse den Benutzern zugeordnet werden kann.

Sie können überprüfen, ob der Domänencontroller bestimmte Ereignis-IDs protokolliert. Wenn diese Ereignisse nicht vorhanden sind, müssen Sie die Anmeldeüberprüfung aktivieren.

Gehen Sie auf dem Domänencontroller zu **Ereignisanzeige > Windows Logs > Security Logs**.

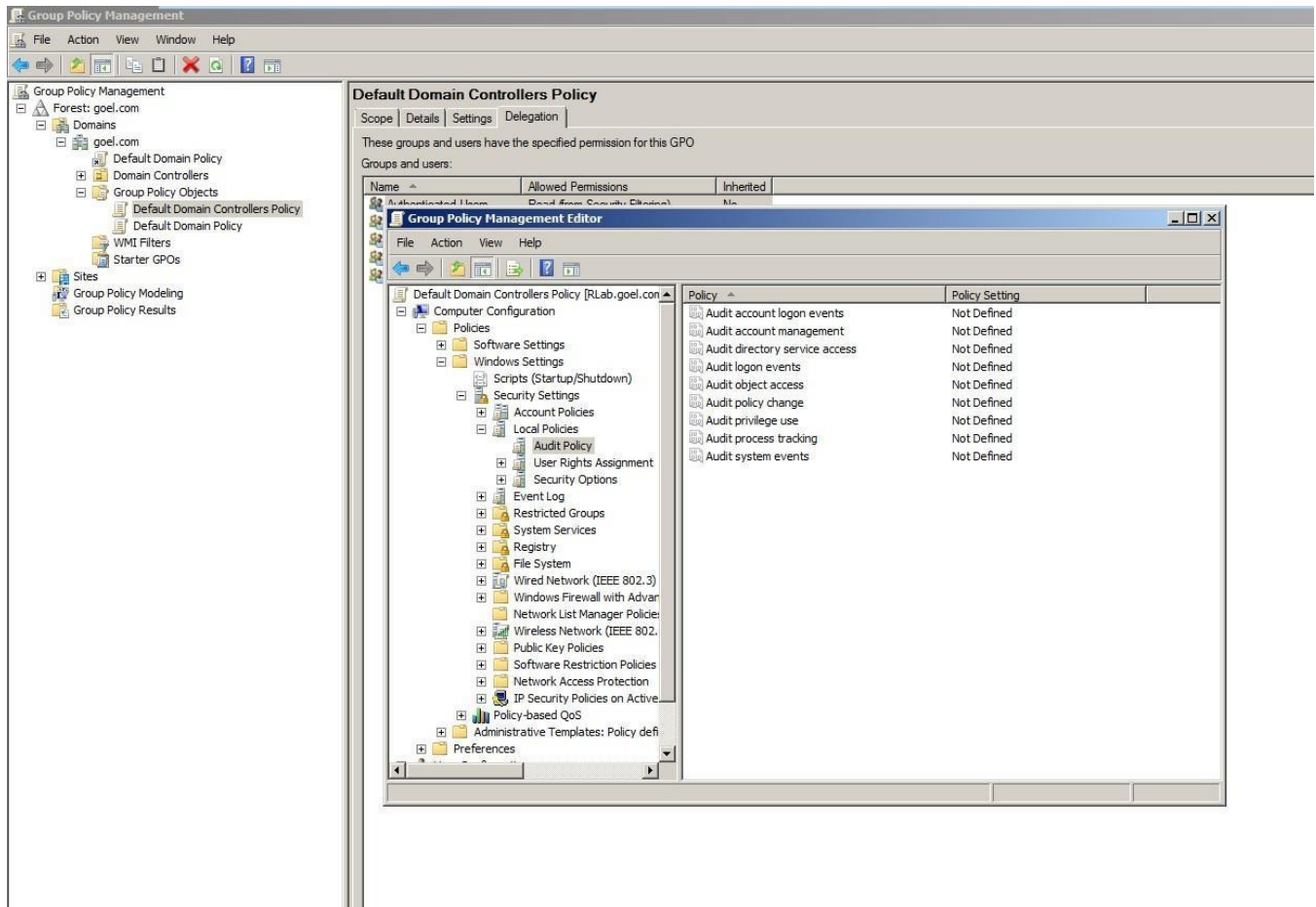
- Für Windows Server 2008, 2008 R2, 2012 und 2012 R2 sollten Sie die Ereignis-ID

#4624

- Für Windows Server 2003, 2003 R2 sollten Sie die Ereignis-IDs 528 und 540 sehen.

Wenn der Domänencontroller diese Ereignisse nicht protokolliert, müssen Sie die **Anmeldeüberprüfung** auf dem Domänencontroller aktivieren und den AD-Client auf der GFI ClearView-Appliance neu nummerieren.

1. Wählen Sie auf dem Domänencontroller **das Menü Start> Verwaltung> Snap-In Gruppenrichtlinienverwaltung**.
2. Gehen Sie in der Baumstruktur der Gruppenrichtlinienverwaltung zu Ihrer Domäne, erweitern Sie den Knoten **Gruppenrichtlinienobjekte** und wählen Sie die **Richtlinie Standarddomänencontroller**.



3. Klicken Sie mit der rechten Maustaste auf die **Richtlinie Standarddomänencontroller** und wählen Sie im Kontextmenü die Option **Bearbeiten**.
4. Erweitern Sie im Dialogfeld **Gruppenrichtlinienverwaltung** die Struktur und wählen Sie **Computerkonfiguration> Richtlinien> Windows-Einstellungen> Sicherheitseinstellungen> Lokale Richtlinien> Audit-Richtlinie**.
5. Klicken Sie in der Richtlinienliste auf der rechten Seite auf **Anmeldeereignisse überprüfen** und stellen Sie sicher, dass **Erfolg** markiert ist.
6. Gehen Sie auf der GFI ClearView-Appliance zu **Konfiguration> System> Netzwerk> Active Directory**.
7. Klicken Sie auf die Schaltfläche **Renumerieren**.
8. Wenden Sie die Änderungen an, indem Sie den folgenden Befehl über eine CMD-Konsole auf Domänencontroller ausführen: `gpup- date /force`

6 ClearView Befehlszeilenschnittstelle (CLI)

Erfahren Sie, wie Sie die GFI ClearView-Befehlszeilenschnittstelle (CLI) verwenden können.

6.1 Verwendung der Befehlszeilenschnittstelle

Viele der in der GFI ClearView Web UI verfügbaren Aktionen können auch über die Befehlszeilenschnittstelle (CLI) ausgeführt werden.

TIP

- ▶ Auto complete is available by pressing the tab key after typing the first several letters of a command. Use the tab key to view available options for any of the commands.
- ▶ Use `?` at the end of a command to view available options and descriptions.
- ▶ Command history is available by using the up and down arrow keys. Command line editing is available, using the left and right keys to navigate.
- ▶ Use `ctrl-w` to delete from the cursor to start of line.


6.1.1 Zugriff auf die Befehlszeilenschnittstelle

Es vier Möglichkeiten, auf die GFI ClearView CLI zuzugreifen (in der Reihenfolge ihrer Präferenz):

1. Secure Shell (SSH) (empfohlen)
2. GFI ClearView Web UI
3. Telnet
4. Serielle Konsolenschnittstelle

Mit diesem Tool können Sie von Web-UI aus eine Verbindung zum Command Line Interface (CLI) der GFI ClearView-Appliance herstellen. Dieses Tool stellt die Verbindung zur Appliance über die Weboberfläche her und erfordert keinen SSH-Zugang.

Open new fullscreen console



login:

1. Öffnen Sie in Ihrem Browser die GFI ClearView Web UI (https://ClearView_IP_address).
2. Geben Sie den **Benutzernamen** und das **Passwort** ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie auf Konfiguration> System> Tools> Konsole.
5. Geben Sie den Appliance-Benutzernamen und das Kennwort bei den entsprechenden Aufforderungen ein. Führen Sie einen der folgenden Schritte aus:
 - Um in den privilegierten EXEC-Modus (enable) zu gelangen, führen Sie an der Eingabeaufforderung den Befehl: `hostname> enable`
Es erscheint die Eingabeaufforderung `hostname #`.
 - Um in den Konfigurationsmodus (config) zu gelangen, führen Sie an der Eingabeaufforderung die folgenden Befehle aus: `hostname # configure terminal`

Es erscheint die Eingabeaufforderung `hostname (config)#`.

6.1.2 CLI-Konfiguration Schnelleinstieg

Wenn Sie sich zum ersten bei der CLI anmelden, haben Sie die Möglichkeit, den CLI-Startassistenten auszuführen. Dabei handelt es sich um einen geführten Assistenten, der Sie bei der Erstkonfiguration der GFI ClearView-Appliance unterstützt.

NOTE

Changes are applied immediately after pressing **Enter** at each step. If changing network settings use the serial console or vga/keyboard to access the CLI.

1. IPv6 aktivieren? - Mit diesen Fragen können Sie die IPv6-Unterstützung für das gesamte System aktivieren. Wenn Ihr Netzwerk IPv6 unterstützt, geben Sie "J" ein, andernfalls "N".
2. IPv6-Autokonfiguration (SLAAC) auf der Schnittstelle eth1 aktivieren? - Wenn Sie IPv6 aktivieren, haben Sie die Möglichkeit, die IPv6-SLAAC-Autokonfiguration zu aktivieren. Geben Sie "Y" ein, wenn Sie eine Adresse und Netzmaske automatisch konfigurieren lassen möchten und Ihr Netzwerk diese Option unterstützt.
3. Verwenden Sie eth0 für den Verwaltungszugang. Hinweis: Dadurch wird br0 deaktiviert (J/N)?
- Wählen Sie, ob eth0 für den Zugriff auf die Verwaltungsfunktionen verwendet werden soll.
4. DHCP auf eth1 verwenden (J/N)? - Bei dieser Frage werden Sie gefragt, ob Sie DHCP für den automatischen Erwerb von IP-Konnektivitätseinstellungen verwenden möchten. Wenn Sie hier 'N' angeben, werden Sie aufgefordert, statische IP-Konnektivitätseinstellungen einzugeben, z. B. IP-Adresse und Netzmaske, Standardgateway und DNS-Server.
5. Aktivieren Sie br10 (J/N)? und DHCP auf br10 verwenden (J/N)?
- Für GFI ClearView wählen Sie "N". Mit diesen Fragen können Sie Bridges aktivieren und optional eine Adresse manuell oder per DHCP konfigurieren.
6. br2 IP-Adresse und Netzmaske? [192.168.2.254/24] - Für GFI ClearView wählen Sie "N". Konfigurieren Sie die IP-Adresse und Netzmaske für die Bridge.
7. Hostname? - Mit dieser Frage werden Sie aufgefordert, einen Hostnamen für die Appliance zu konfigurieren.
8. SMTP-Server-Adresse? - Um Systemwarnungen und Berichte zu erhalten, muss für die GFI ClearView-Appliance ein SMTP-Server konfiguriert werden, damit E-Mails verschickt werden können.
9. Eine E-Mail-Adresse für Berichte und Warnmeldungen? - Wenn Sie Systemwarnungen und Berichte erhalten möchten, geben Sie hier eine E-Mail-Adresse ein.
10. Admin-Kennwort (Eingabe, um es unverändert zu lassen): - Bei dieser Frage werden Sie gefragt, ob Sie das Kennwort für das "admin"-Konto der GFI ClearView-Appliance ändern möchten. Drücken Sie die Eingabetaste, um das Kennwort unverändert zu lassen, oder geben Sie ein neues Kennwort ein.
11. Möchten Sie die Geschwindigkeit und die Duplexeinstellungen der Schnittstelle konfigurieren? (J/N)? - Geben Sie "J" ein, wenn Sie die Schnittstelleneinstellungen konfigurieren möchten, oder "N", wenn sie unverändert bleiben sollen. Wenn Sie "J" eingegeben haben, werden diese Fragen schrittweise für jede Schnittstelle der GFI ClearView-Appliance gestellt und die Einstellungen für die Schnittstellengeschwindigkeit und den Duplex-Modus abgefragt.

Wie hoch ist die Geschwindigkeit von eth1 (auto, 10 oder 100):

Was ist der Duplex-Modus von eth1 (auto, voll oder halb): Wie

hoch ist die Geschwindigkeit von eth2 (auto, 10 oder 100):

Was ist der Duplex-Modus von eth2 (auto, voll oder halb):

12. Möchten Sie die HTTP-Proxy-Einstellungen ändern (J/N)? - Wenn Sie "J" eingeben, werden die Parameter der HTTP-Proxy-Einrichtung schrittweise abgefragt.

HTTP-Proxy-Adresse (0.0.0.0 zum

Deaktivieren)? HTTP-Proxy-Anschluss?

[3128]

HTTP-Proxy-Authentifizierungstyp (N)one oder (B)asic (N/B)?

Unsicheres (ungeprüftes Zertifikat) SSL zulassen (J/N)?

13. Möchten Sie online nach einer neuen Lizenz suchen (J/N)? - Geben Sie "J" ein, damit die GFI ClearView-Appliance auf der GFI ClearView-Website nach einer neueren Lizenz sucht (sofern die GFI ClearView-Appliance über eine Internetverbindung verfügt). Wenn eine neuere Lizenz gefunden wird, werden Sie gefragt, ob Sie diese installieren möchten. Wenn Sie "N" eingeben, werden Sie zur Eingabe eines Lizenzschlüssels aufgefordert.

14. Möchten Sie Optimierungsrichtlinien konfigurieren (J/N): - Antworten Sie hier mit "N".

15. Nach neuer Firmware suchen (J/N)? - Wenn Sie hier mit "J" antworten, sucht die GFI ClearView-Appliance auf der GFI ClearView-Website nach einer neueren Firmware-Version (sofern die GFI ClearView-Appliance über eine Internet-Verbindung verfügt). Wenn ein neueres Firmware-Image gefunden wird, Sie gefragt, ob Sie es herunterladen und installieren möchten.

NOTE

You can re-run the CLI jump-start wizard at anytime by logging into the CLI (configuration mode) and typing: `configuration jump-start`

6.1.3 Konfigurieren der Befehlszeilenooptionen

Konfigurieren Sie die Befehlszeilenschnittstelle nach Ihren Bedürfnissen.

1. Verwenden Sie den folgenden Befehl, um die Zeichenbreite des Terminals und die Anzahl der

```
Zeilen festzulegen: hostname (config)# cli session terminal width <Anzahl  
der Zeichen> hostname (config)# cli session terminal length  
<Anzahl der Zeilen>
```

2. Die automatische Abmeldung ist standardmäßig aktiviert. Um die Zeit für die automatische Abmeldung zu ändern, verwenden Sie den folgenden Befehl:

```
hostname (config)# cli default auto-logout <Minuten>
```

Um die automatische Abmeldung zu deaktivieren, setzen Sie die Minuten auf 0.

3. Um Paging zu aktivieren oder zu deaktivieren, verwenden Sie den folgenden Befehl:

```
hostname (config)# [no] cli default paging enable
```

4. Verwenden Sie den Befehl `show cli`, um die aktuellen CLI-Einstellungen anzuzeigen.

5. Um die laufende Konfiguration zu speichern, geben Sie `configuration write` ein.

7 Urheberrecht

Alle Rechte vorbehalten. Kein Teil dieses Werkes darf ohne schriftliche Genehmigung des Herausgebers in irgendeiner Form oder mit irgendwelchen Mitteln - grafisch, elektronisch oder mechanisch, einschließlich Fotokopien, Aufzeichnungen, Tonbandaufnahmen oder Informationsspeicher- und -abrufsystemen - vervielfältigt werden.

Produkte, auf die in diesem Dokument Bezug genommen wird, können entweder Marken und/oder eingetragene Marken der jeweiligen Eigentümer sein. Der Herausgeber und der Autor erheben keinen Anspruch auf diese Marken.

Obwohl bei der Erstellung dieses Dokuments alle Vorsichtsmaßnahmen getroffen wurden, übernehmen der Herausgeber und Autor keine Verantwortung für Fehler oder Auslassungen oder für Schäden, die sich aus der Verwendung der in diesem Dokument enthaltenen Informationen oder aus der Verwendung von Programmen und Quellcode ergeben, die diesem Dokument möglicherweise beigelegt sind. In keinem Fall haften der Herausgeber und der Autor für entgangenen Gewinn oder andere kommerzielle Schäden, die direkt oder indirekt durch dieses Dokument verursacht wurden oder angeblich verursacht wurden.

7.1 GFI ClearView Endbenutzer-Lizenzvertrag (EULA)

HINWEIS AN DIE NUTZER: LESEN SIE SORGFÄLTIG DIE FOLGENDE RECHTSVEREINBARUNG. MIT DER NUTZUNG DER MIT DIESEM VERTRAG GELIEFERTEN SOFTWARE ("SOFTWARE") ERKLÄREN SIE SICH MIT DIESEN BEDINGUNGEN EINVERSTANDEN. WENN SIE MIT DEN BEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SIND, GEBEN SIE DAS KOMPLETTE SOFTWAREPAKET (UND ALLE ANDEREN MIT DIESEM PAKET GELIEFERTEN GERÄTE) UNVERZÜGLICH AN DEN HÄNDLER ZURÜCK, BEI DEM SIE DIESES PRODUKT ERWORBEN HABEN, UND ERHALTEN SIE EINE VOLLE ERSTATTUNG. WENN SIE FRAGEN ZU DIESER VEREINBARUNG HABEN, WENDEN SIE SICH AN GFI USA, LLC, 2028 E BEN WHITE BLVD, SUITE 240-2650 AUSTIN, TX 78741 ODER PER EMAIL: LEGAL@GFI.COM.

1. LIZENZERTEILUNG: Die SOFTWARE wird lizenziert, nicht verkauft. GFI USA, LLC ("GFI") gewährt Ihnen mit dem gültigen Erwerb einer Lizenz für die SOFTWARE und sofern in einer beiliegenden Lizenzübersicht, Rechnung oder anderen Dokumenten, die den Erwerb der Softwarelizenz belegen, nichts anderes angegeben ist, eine nicht exklusive, nicht übertragbare Lizenz zur Nutzung der SOFTWARE während des Abonnementzeitraums auf Servern, die mit einer maximalen Anzahl von Benutzer-Computern verbunden sind, die die in der der SOFTWARE beiliegenden Verpackung oder in etwaigen Zusatzvereinbarungen angegebene Anzahl von Benutzer-Computern nicht überschreitet. Diese Lizenz zur Nutzung der SOFTWARE ist an die Einhaltung der Bedingungen dieses Vertrages geknüpft. Sie erklären sich damit einverstanden, die SOFTWARE nur in eine maschinenlesbare oder gedruckte Form zu kompilieren, die für die Nutzung in Übereinstimmung mit dieser Lizenz oder für Sicherungszwecke zur Unterstützung Ihrer Nutzung der SOFTWARE erforderlich ist. Diese Lizenz gilt bis zum Ende des Abonnementzeitraums. GFI hat das Recht, diesen Vertrag zu kündigen, wenn Sie eine Bedingung dieses Vertrages nicht einhalten. Sie verpflichten sich, bei einer solchen Kündigung die SOFTWARE zusammen mit allen Kopien der SOFTWARE zu vernichten.

2. REVERSE ENGINEERING. Sie dürfen die SOFTWARE weder ganz noch teilweise zurückentwickeln, dekompilieren, modifizieren oder disassemblieren.

3. COPYRIGHT: Alle Eigentums- und Urheberrechte an der SOFTWARE und dem gedruckten Begleitmaterial sind Eigentum von GFI. Die SOFTWARE ist durch Urheberrechtsgesetze und internationale Verträge geschützt. Die SOFTWARE ist Copyright (c) 2002-2023 GFI USA, LLC, Alle Rechte vorbehalten. Die Software bleibt zu jeder Zeit das alleinige und exklusive Eigentum von GFI.

4. **INGESCHRÄNKTE GARANTIE:** GFI garantiert für einen Zeitraum von dreißig (30) Tagen ab dem Versanddatum von GFI, dass (i) die SOFTWARE bei normalem Gebrauch frei von Verarbeitungsfehlern ist und (ii) die Software im Wesentlichen mit den veröffentlichten Spezifikationen übereinstimmt. Sofern in diesem Vertrag nicht ausdrücklich etwas anderes vereinbart ist, wird die SOFTWARE so geliefert, wie sie ist. GFI oder seine Lieferanten haften in keinem Fall für Schäden jeglicher Art (einschließlich, aber nicht beschränkt auf Schäden aus entgangenem Gewinn, Geschäftsunterbrechung, Verlust von Geschäftsinformationen oder anderen Vermögensschäden), die aus der Nutzung oder der Unmöglichkeit der Nutzung dieser SOFTWARE entstehen, selbst wenn GFI auf die Möglichkeit solcher Schäden hingewiesen wurde. Da in einigen Staaten/Gerichtsbarkeiten der Ausschluss oder die Beschränkung der Haftung für Folgeschäden oder beiläufig entstandene Schäden nicht zulässig ist, gilt die obige Beschränkung möglicherweise nicht für Sie.

5. **KEINE WEITEREN GARANTIEEN.** GFI GEWÄHRLEISTET NICHT, DASS DIE SOFTWARE FEHLERFREI IST. MIT AUSNAHME DER "BESCHRÄNKTEN GEWÄHRLEISTUNG" IN ABSCHNITT 4 ("BESCHRÄNKTE GEWÄHRLEISTUNG") LEHNT GFI ALLE ANDEREN GEWÄHRLEISTUNGEN IN BEZUG AUF DIE SOFTWARE AB, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND. DIES GILT INSBESONDERE FÜR STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER. IN EINIGEN GERICHTSBARKEITEN IST DER AUSSCHLUSS VON STILLSCHWEIGENDEN GARANTIEEN ODER DIE BESCHRÄNKUNG DER DAUER EINER STILLSCHWEIGENDEN GARANTIE ODER DER AUSSCHLUSS ODER DIE BESCHRÄNKUNG VON ZUFÄLLIGEN SCHÄDEN ODER FOLGESCHÄDEN NICHT ZULÄSSIG, SO DASS DIE OBEN GENANNTEN BESCHRÄNKUNGEN ODER AUSSCHLÜSSE FÜR SIE MÖGLICHERWEISE NICHT GELTEN. DIESE GARANTIE GIBT IHNEN BESTIMMTE RECHTE UND SIE KÖNNEN AUCH ANDERE RECHTE HABEN, DIE VON GERICHTSBARKEIT ZU GERICHTSBARKEIT VARIIEREN.

6. **WIDERRUFSPÄHIGKEIT:** Im Falle der Ungültigkeit einer Bestimmung dieser Lizenz vereinbaren die Parteien, dass diese Ungültigkeit die Gültigkeit der übrigen Teile dieser Lizenz nicht berührt.

7. **ANWENDBARES RECHT.** Für diese Lizenz gelten die Gesetze des Staates Texas. Im Falle Streitigkeiten, die sich aus dieser Vereinbarung ergeben, unterwerfen sich die Parteien hiermit der Rechtsprechung der Gerichte des Staates Texas.

8. **GESAMTE VEREINBARUNG:** Dies ist die gesamte Vereinbarung zwischen Ihnen und GFI, die alle früheren Vereinbarungen oder Absprachen, ob schriftlich oder mündlich, in Bezug auf den Gegenstand dieser Lizenz außer Kraft setzt.

7.2 GNU General Public License (GPL)

Version 3, 29. Juni 2007

Copyright © 2007 Free Software Foundation, Inc.

Jedem ist es gestattet, wortwörtliche Kopien dieses Lizenzdokuments zu vervielfältigen und zu verbreiten, aber es ist nicht erlaubt, es zu verändern.

7.2.1 Präambel

Die GNU General Public License ist eine freie Copyleft-Lizenz für Software und andere Arten von Werken.

Die Lizenzen für die meisten Software- und anderen praktischen Werke sind so konzipiert, dass sie Ihnen die Freiheit nehmen, die Werke weiterzugeben und zu verändern. Im Gegensatz dazu soll die GNU General Public License Ihre Freiheit garantieren, alle Versionen eines Programms weiterzugeben und zu verändern - um sicherzustellen, dass es freie Software für alle Benutzer bleibt. Wir, die Free Software Foundation, verwenden die GNU General Public

Lizenz für die meisten unserer Programme; sie gilt auch für alle anderen Werke, die von ihren Autoren auf diese Weise veröffentlicht werden. Sie können sie auch auf Ihre Programme anwenden.

Wenn wir von freier Software sprechen, beziehen wir uns auf die Freiheit, nicht auf den Preis. Unsere Allgemeinen Öffentlichen Lizenzen sollen sicherstellen, dass Sie die Freiheit haben, Kopien freier Software zu verbreiten (und dafür Geld zu verlangen, wenn Sie wollen), dass Sie den Quellcode erhalten oder ihn bekommen können, wenn Sie ihn wollen, dass Sie die Software ändern oder Teile davon in neuen freien Programmen verwenden können und dass Sie wissen, dass Sie diese Dinge tun können.

Um Ihre Rechte zu schützen, müssen wir andere daran hindern, Ihnen diese Rechte zu verweigern oder Sie aufzufordern, diese Rechte aufzugeben. Daher haben Sie bestimmte Pflichten, wenn Sie Kopien der Software verbreiten oder sie verändern: Pflichten, die Freiheit anderer zu respektieren.

Wenn Sie beispielsweise Kopien eines solchen Programms verbreiten, sei es kostenlos oder gegen eine Gebühr, müssen Sie den Empfängern die gleichen Freiheiten einräumen, die Sie selbst erhalten haben. Sie müssen dafür sorgen, dass auch sie den erhalten oder erhalten können. Und Sie müssen ihnen diese Bedingungen zeigen, damit sie ihre Rechte kennen.

Entwickler, die die GNU GPL verwenden, schützen Ihre Rechte in zwei Schritten: (1) Sie machen das Urheberrecht an Software geltend und (2) bieten Ihnen diese Lizenz an, die Ihnen die rechtliche Erlaubnis gibt, die Software zu kopieren, zu verbreiten und/oder zu verändern.

Zum Schutz der Entwickler und Autoren erklärt die GPL deutlich, dass es für diese freie Software keine Garantie gibt. Zum Schutz der Benutzer und Autoren verlangt die GPL, dass geänderte Versionen als geändert gekennzeichnet werden, damit ihre Probleme nicht fälschlicherweise den Autoren früherer Versionen zugeschrieben werden.

Einige Geräte sind so konstruiert, dass sie den Nutzern den Zugang zur Installation oder Ausführung geänderter Versionen der darin enthaltenen Software verwehren, obwohl der Hersteller dies tun kann. Dies ist grundsätzlich unvereinbar mit dem Ziel, die Freiheit der Nutzer zu schützen, die Software zu ändern. Ein solcher Missbrauch findet systematisch bei Produkten statt, die von Privatpersonen genutzt werden, und genau dort ist er am inakzeptabelsten. Deshalb haben wir diese Version der GPL so gestaltet, dass sie diese Praxis für diese Produkte verbietet. Sollten derartige Probleme auch in anderen Bereichen auftreten, sind wir bereit, diese Bestimmung in künftigen Versionen der GPL auf diese Bereiche auszudehnen, wenn dies zum Schutz der Freiheit der Nutzer erforderlich ist.

Schließlich ist jedes Programm ständig durch Softwarepatente bedroht. Die Staaten sollten nicht zulassen, dass Patente die Entwicklung und Verwendung von Software auf Allzweckcomputern einschränken, aber in den Staaten, in denen dies der Fall ist, wollen wir die besondere Gefahr vermeiden, dass Patente auf ein freies Programm dieses effektiv proprietär machen könnten. Um dies zu verhindern, stellt die GPL sicher, dass Patente nicht dazu verwendet werden können, das Programm unfrei zu machen.

Die genauen Bedingungen für die Vervielfältigung, Verbreitung und Veränderung folgen.

7.2.1 BEDINGUNGEN UND BEDINGUNGEN

Definitionen

"Diese Lizenz" bezieht sich auf Version 3 der GNU General Public License.

"Urheberrecht" bedeutet auch urheberrechtsähnliche Gesetze, die für andere Arten von Werken gelten, z. B. Halbleitermasken.

"Das Programm" bezieht sich auf jedes urheberrechtsfähige Werk, das unter dieser lizenziert wird. Jeder Lizenznehmer wird als "Sie" angesprochen. "Lizenznehmer" und "Empfänger" können Einzelpersonen oder Organisationen sein.

Ein Werk zu "verändern" bedeutet, das Werk ganz oder teilweise in einer Weise zu kopieren oder anzupassen, die eine urheberrechtliche Erlaubnis erfordert, ohne eine exakte Kopie zu erstellen. Das daraus resultierende Werk wird "geänderte Fassung" des früheren Werks oder als ein Werk "auf der Grundlage" des früheren Werks bezeichnet.

Ein "betroffenes Werk" ist entweder das unveränderte Programm oder ein auf dem Programm basierendes Werk.

Ein Werk zu "verbreiten" bedeutet, irgendetwas damit zu tun, das Sie ohne Erlaubnis direkt oder sekundär für eine Verletzung des geltenden Haftbar machen würde, mit Ausnahme der Ausführung des Werks auf einem Computer oder der Änderung einer privaten Kopie. Die Verbreitung umfasst die Vervielfältigung, die Verbreitung (mit oder ohne Änderung), die öffentliche Zugänglichmachung und in einigen Ländern auch andere Aktivitäten.

Ein Werk zu "übertragen" bedeutet jede Art der Verbreitung, die es anderen Parteien ermöglicht, Kopien anzufertigen oder zu erhalten. Die bloße Interaktion mit einem Nutzer über ein Computernetz, ohne Übertragung einer Kopie, ist keine Übertragung.

Eine interaktive Benutzeroberfläche zeigt "Angemessene rechtliche Hinweise" in dem Maße an, in dem sie eine bequeme und deutlich sichtbare Funktion enthält, die (1) einen angemessenen Copyright-Hinweis anzeigt, und (2) den Benutzer darauf hinweist, dass keine Garantie für das Werk besteht (außer in dem Umfang, in dem Garantien gegeben werden), dass Lizenznehmer das Werk unter dieser Lizenz übertragen dürfen und wie eine Kopie dieser Lizenz eingesehen werden kann. Wenn die Schnittstelle eine Liste von Benutzerbefehlen oder -optionen präsentiert, etwa ein Menü, erfüllt ein hervorgehobener Punkt in dieser Liste dieses Kriterium.

1. Quelle Code.

Der "Quellcode" eines Werks ist die bevorzugte Form des Werks, um Änderungen vorzunehmen. Unter "Objektcode" ist jede Form eines Werks zu verstehen, die kein Quellcode ist.

Eine "Standardschnittstelle" ist eine Schnittstelle, die entweder ein offizieller Standard ist, der von einem anerkannten Normungsgremium definiert wurde, oder, im Falle von Schnittstellen, die für eine bestimmte Programmiersprache spezifiziert sind, eine Schnittstelle, die unter Entwicklern, die in dieser Sprache arbeiten, weit verbreitet ist.

Die "Systembibliotheken" eines ausführbaren Werks umfassen alles, was nicht zum Werk als Ganzes gehört, was (a) in der normalen Form der Verpackung einer Hauptkomponente enthalten ist, aber nicht Teil dieser Hauptkomponente ist, und (b) nur dazu dient, die Nutzung des Werks mit dieser Hauptkomponente zu ermöglichen oder eine Standardschnittstelle zu implementieren, für die eine Implementierung in Quellcodeform öffentlich verfügbar ist. Eine "Hauptkomponente" bedeutet in diesem Zusammenhang eine wesentliche Komponente (Kernel, Fenstersystem usw.) des spezifischen Betriebssystems (falls vorhanden), auf dem das ausführbare Werk läuft, oder einen Compiler, der zur Erstellung des Werks verwendet wird, oder einen Objektcode-Interpreter, der zur Ausführung des Werks verwendet wird.

Der "korrespondierende Quelltext" für ein Werk in Form von Objektcode ist der gesamte Quelltext, der zum Generieren, Installieren und (bei einem ausführbaren Werk) zum Ausführen des Objektcodes sowie zum Ändern des Werks benötigt wird, einschließlich der Skripte zur Steuerung dieser Aktivitäten.

Er umfasst jedoch nicht die Systembibliotheken des Werks oder allgemein verwendbare Werkzeuge oder allgemein verfügbare freie Programme, die unverändert zur Durchführung dieser Tätigkeiten verwendet werden, aber nicht Teil des Werks sind. Der korrespondierende Quelltext umfasst beispielsweise Schnittstellendefinitionsdateien, die mit den Quelldateien des Werks verbunden sind, sowie den Quelltext für gemeinsam genutzte Bibliotheken und dynamisch verknüpfte Unterprogramme, die das Werk speziell benötigt, z. B. durch eine intime Datenkommunikation oder einen Kontrollfluss zwischen diesen Unterprogrammen und anderen Teilen des Werks.

Die korrespondierende Quelle muss nichts enthalten, was die Benutzer automatisch aus anderen Teilen der korrespondierenden Quelle neu generieren können.

Die korrespondierende Quelle für ein Werk in Quellcodeform ist dasselbe Werk.

2. Grundlegende Berechtigungen.

Alle unter dieser Lizenz gewährten Rechte werden für die Dauer des Urheberrechts an dem Programm gewährt und sind unwiderruflich, sofern die genannten Bedingungen erfüllt sind. Diese Lizenz bekräftigt ausdrücklich Ihre uneingeschränkte Erlaubnis, das unveränderte Programm auszuführen. Das Ergebnis der Ausführung eines betroffenen Werks fällt nur dann unter diese Lizenz, wenn die Ausgabe aufgrund ihres Inhalts ein betroffenes Werk darstellt. Diese Lizenz

erkennt Ihr Recht auf faire Nutzung oder andere gleichwertige Rechte an, wie sie im Urheberrecht vorgesehen sind.

Sie dürfen betroffene Werke, die Sie nicht übertragen, ohne Bedingungen erstellen, ausführen und verbreiten, solange Ihre Lizenz ansonsten in bleibt. Sie dürfen betroffene Werke an andere übertragen, damit diese ausschließlich für Sie Modifikationen vornehmen oder Ihnen Einrichtungen zum Ausführen dieser Werke zur Verfügung stellen, vorausgesetzt, Sie halten sich bei der Übertragung des gesamten Materials, für das Sie nicht das Urheberrecht kontrollieren, an die Bedingungen dieser Lizenz. Diejenigen, die auf diese Weise die betroffenen Werke für Sie herstellen oder betreiben, müssen dies ausschließlich in Ihrem Namen, unter Ihrer Anleitung und Kontrolle tun, und zwar zu Bedingungen, die es ihnen verbieten, Kopien Ihres urheberrechtlich geschützten Materials außerhalb ihrer Beziehung zu Ihnen anzufertigen.

Eine Weitergabe unter anderen Umständen ist nur unter den nachstehend genannten Bedingungen zulässig. Die Vergabe von Unterlizenzen ist nicht zulässig; Abschnitt 10 macht sie überflüssig.

3. Schutz der Rechte von Nutzern vor Umgehungsversuchen Recht.

Kein betroffenes Werk gilt als Teil einer wirksamen technischen Maßnahme nach einem anwendbaren Gesetz, das die Verpflichtungen nach Artikel 11 des am 20. Dezember 1996 angenommenen WIPO-Urheberrechtsvertrags oder nach ähnlichen Gesetzen, die die Umgehung solcher Maßnahmen verbieten oder einschränken, erfüllt.

Wenn Sie ein betroffenes Werk übertragen, verzichten Sie auf jede rechtliche Befugnis, die Umgehung technischer Maßnahmen zu verbieten, soweit eine solche Umgehung durch die Ausübung von Rechten unter dieser Lizenz in Bezug auf das betroffene Werk erfolgt, und Sie lehnen jede Absicht ab, den Betrieb oder die Modifikation des Werks als Mittel zur Durchsetzung Ihrer Rechte oder der Rechte Dritter, die Umgehung technischer Maßnahmen zu verbieten, gegenüber den Nutzern des Werks zu beschränken.

4. Übermittlung von wortgetreuen Kopien.

Sie dürfen wortgetreue Kopien des Quellcodes des Programms, so wie Sie ihn erhalten, in jedem beliebigen Medium weitergeben, vorausgesetzt, daß Sie auf jeder Kopie einen angemessenen Urheberrechtsvermerk veröffentlichen; alle Hinweise, daß diese Lizenz und alle gemäß Abschnitt 7 hinzugefügten nicht-genehmigenden Bestimmungen für den Code gelten, unversehrt lassen; alle Hinweise auf das Fehlen jeglicher Gewährleistung unversehrt lassen; und allen Empfängern zusammen mit dem Programm eine Kopie dieser Lizenz aushändigen.

Sie können für jede Kopie, die Sie übermitteln, einen beliebigen Preis oder keinen Preis verlangen, und Sie können Support oder Garantieschutz gegen eine Gebühr anbieten.

5. Übermittlung von geänderten Versionen der Quelle .

Sie dürfen ein auf dem Programm basierendes Werk oder die Modifikationen, die aus dem hervorgehen, in Form von Quellcode unter den Bedingungen von Abschnitt 4 weitergeben, vorausgesetzt, Sie erfüllen ebenfalls alle diese Bedingungen:

- a. Das Werk muss einen deutlichen Hinweis darauf tragen, dass Sie es geändert haben, und ein entsprechendes Datum nennen.
- b. Das Werk muss auffällige Hinweise tragen, die besagen, dass es unter dieser Lizenz und allen gemäß Abschnitt 7 hinzugefügten Bedingungen freigegeben ist. Diese Anforderung modifiziert die Anforderung in Abschnitt 4, "alle Hinweise unversehrt zu lassen".
- c. Sie müssen das gesamte Werk als Ganzes unter dieser Lizenz an jeden lizenzieren, der in den Besitz einer Kopie kommt. Diese Lizenz gilt daher, zusammen mit allen anwendbaren zusätzlichen Bedingungen von Abschnitt 7, für das gesamte Werk und alle seine Teile, unabhängig davon, wie sie verpackt sind. Diese Lizenz gibt keine Erlaubnis, das Werk auf andere Weise zu lizenzieren, aber sie macht eine solche Erlaubnis nicht ungültig, wenn Sie sie separat erhalten haben.
- d. Verfügt das Werk über interaktive Benutzeroberflächen, so müssen diese die entsprechenden rechtlichen Hinweise anzeigen; verfügt das Programm jedoch über interaktive Benutzeroberflächen, die keine entsprechenden rechtlichen Hinweise anzeigen, so muss Ihr Werk nicht dafür sorgen, dass sie dies tun.

Eine Zusammenstellung eines betroffenen Werks mit anderen separaten und unabhängigen Werken, die nicht ihrer Natur nach Erweiterungen des betroffenen Werks sind und die nicht mit ihm kombiniert werden, um ein größeres Programm zu bilden, in oder auf einem Datenträger eines Speicher- oder Verbreitungsmediums, wird als "Aggregat" bezeichnet, wenn die Zusammenstellung und das sich daraus ergebende Urheberrecht nicht dazu benutzt werden, den Zugang oder die gesetzlichen Rechte der Benutzer der Zusammenstellung über das hinaus zu beschränken, was die einzelnen Werke erlauben. Die Aufnahme eines betroffenen Werkes in ein Aggregat bewirkt nicht, daß diese Lizenz auf die anderen Teile des Aggregats Anwendung findet.

6. Übermittlung von Formularen ohne Quellenangabe .

Sie dürfen ein betroffenes Werk in Objektcodeform unter den Bedingungen der Abschnitte 4 und 5 übertragen, vorausgesetzt, daß Sie auch den maschinenlesbaren korrespondierenden Quelltext unter den Bedingungen dieser Lizenz übertragen, und zwar auf eine der folgenden Arten:

- a. Übermittlung des Objektcodes in einem physischen Produkt (einschließlich eines physischen Vertriebsmediums) oder in einem physischen Produkt (einschließlich eines physischen Vertriebsmediums), dem der entsprechende Quellcode auf einem dauerhaften physischen Medium beiliegt, das üblicherweise für den Austausch von Software verwendet wird.
- b. den Objektcode in einem physischen Produkt (einschließlich eines physischen Vertriebsmediums) zu übermitteln, begleitet von einem schriftlichen Angebot, das mindestens drei Jahre lang gültig ist und so lange gilt, wie Sie Ersatzteile oder Kundensupport für dieses Produktmodell anbieten, jedem, der im Besitz des Objektcodes ist, entweder (1) eine Kopie des korrespondierenden Quelltextes für die gesamte Software des Produkts, die unter diese Lizenz fällt, auf einem dauerhaften physischen Medium, das üblicherweise für den Austausch von Software verwendet wird, zu einem Preis zu überlassen, der nicht höher ist als die angemessenen Kosten, die Ihnen für die physische Übermittlung des Quelltextes entstehen, oder (2) kostenlos Zugang zum Kopieren des korrespondierenden Quelltextes von einem Netzwerkserver zu gewähren.
- c. Übermitteln Sie einzelne Kopien des Objektcodes zusammen mit einer Kopie des schriftlichen Angebots zur Bereitstellung des korrespondierenden Quellcodes. Diese Alternative ist nur gelegentlich und nicht kommerziell erlaubt, und auch nur dann, wenn Sie den Objektcode mit einem solchen Angebot gemäß Absatz 6b erhalten haben.
- d. Übermitteln Sie den Objektcode, indem Sie den Zugang von einer bestimmten Stelle aus (kostenlos oder kostenpflichtig) anbieten, und bieten Sie einen gleichwertigen Zugang zum korrespondierenden Quelltext auf die gleiche Weise über dieselbe Stelle ohne weitere Kosten an. Sie brauchen von den Empfängern nicht zu verlangen, dass sie den korrespondierenden Quelltext zusammen mit dem Objektcode kopieren. Wenn der Ort, an dem der Objektcode kopiert wird, ein Netzwerkserver ist, kann sich der korrespondierende Quelltext auf einem anderen Server befinden (der von Ihnen oder einem Dritten betrieben wird), der gleichwertige Kopiermöglichkeiten bietet, vorausgesetzt, Sie geben neben dem Objektcode klare Hinweise, wo der korrespondierende Quelltext zu finden ist. Unabhängig davon, auf welchem Server sich der korrespondierende Quelltext befindet, sind Sie verpflichtet, dafür zu sorgen, dass er so lange verfügbar ist, wie es zur Erfüllung dieser Anforderungen erforderlich ist.
- e. den Objektcode mittels Peer-to-Peer-Übertragung weitergeben, vorausgesetzt, Sie informieren andere Peers darüber, wo der Objektcode und der korrespondierende Quelltext des Werks gemäß Absatz 6d kostenlos der Allgemeinheit angeboten werden.

Ein abtrennbarer Teil des Objektcodes, dessen Quellcode als Systembibliothek aus dem korrespondierenden Quelltext ausgeschlossen ist, muss nicht in die Übermittlung des Objektcode-Werks einbezogen werden.

Ein "Nutzerprodukt" ist entweder (1) ein "Verbraucherprodukt", d. h. ein materieller persönlicher Gegenstand, der normalerweise für persönliche, familiäre oder Haushaltszwecke verwendet wird, oder (2) alles, was für den Einbau in eine Wohnung konzipiert oder verkauft wird. Bei der Feststellung, ob ein Produkt ein Verbraucherprodukt ist, sind Zweifelsfälle zugunsten des Versicherungsschutzes zu entscheiden. Für ein bestimmtes Produkt, das ein bestimmter Benutzer erhält, bezieht sich der Begriff "normalerweise verwendet" auf eine typische oder übliche Verwendung dieser Produktklasse, unabhängig vom Status des bestimmten Benutzers oder von der Art und Weise, in der der bestimmte Benutzer das Produkt tatsächlich verwendet oder zu verwenden erwartet oder erwarten wird. Ein Produkt ist ein Verbraucherprodukt, unabhängig davon, ob es in erheblichem Umfang für gewerbliche, industrielle oder andere Zwecke verwendet wird, es sei denn, diese Verwendungszwecke stellen die einzige nennenswerte Art der Verwendung des Produkts dar.

"Installationsinformationen" für ein Benutzerprodukt sind alle Methoden, Verfahren, Genehmigungen

Schlüssel oder andere Informationen, die erforderlich sind, um modifizierte Versionen eines betroffenen Werkes in diesem Benutzerprodukt aus einer modifizierten Version seines korrespondierenden Quelltextes zu installieren und auszuführen. Die Informationen müssen ausreichen, um sicherzustellen, daß das weitere Funktionieren des geänderten Objektcodes in keinem Fall verhindert oder gestört wird, nur weil eine Änderung vorgenommen wurde.

Wenn Sie ein Objektcode-Werk gemäß diesem Abschnitt in oder mit einem Benutzerprodukt oder speziell zur Verwendung in einem Benutzerprodukt übertragen und die Übertragung als Teil einer Transaktion erfolgt, bei der das Recht zum Besitz und zur Nutzung des Benutzerprodukts auf Dauer oder für einen bestimmten Zeitraum auf den Empfänger übertragen wird (unabhängig davon, wie die Transaktion charakterisiert ist), müssen dem gemäß diesem Abschnitt übertragenen korrespondierenden Quelltext die Installationsinformationen beigefügt sein. Dieses Erfordernis gilt jedoch nicht, wenn weder Sie noch ein Dritter die Möglichkeit behält, den geänderten Objektcode auf dem Benutzerprodukt zu installieren (z. B. wenn das Werk in einem ROM installiert wurde).

Die Verpflichtung zur Bereitstellung von Installationsinformationen beinhaltet nicht die Verpflichtung, weiterhin Supportleistungen, Garantieleistungen oder Aktualisierungen für ein Empfänger modifiziertes oder installiertes Werk oder für das Benutzerprodukt, in dem es modifiziert oder installiert wurde, zu erbringen. Der Zugang zu einem Netzwerk kann verweigert werden, wenn die Änderung selbst den Betrieb des Netzwerks wesentlich und nachteilig beeinflusst oder die Regeln und Protokolle für die Kommunikation über das Netzwerk verletzt.

Der übermittelte korrespondierende Quellcode und die gemäß diesem Abschnitt bereitgestellten Installationsinformationen müssen in einem Format vorliegen, das öffentlich dokumentiert ist (und dessen Implementierung der Öffentlichkeit in Form von Quellcode zur Verfügung steht), und dürfen kein spezielles Passwort oder Schlüssel zum Entpacken, Lesen oder Kopieren erfordern.

7. Zusätzliche Begriffe.

"Zusätzliche Erlaubnisse" sind Bedingungen, die die Bedingungen dieser Lizenz ergänzen, indem sie Ausnahmen von einer oder mehreren vorsehen. Zusätzliche Erlaubnisse, die auf gesamte Programme anwendbar sind, werden so behandelt, als wären sie in dieser Lizenz enthalten, sie nach geltendem Recht gültig sind. Wenn zusätzliche Erlaubnisse nur für einen Teil des Programms gelten, kann dieser Teil separat unter diesen Erlaubnissen verwendet werden, aber das gesamte Programm unterliegt weiterhin dieser Lizenz, ohne Rücksicht auf die zusätzlichen Erlaubnisse.

Wenn Sie eine Kopie eines geschützten Werks übermitteln, können Sie nach eigenem Ermessen alle zusätzlichen Rechte von dieser Kopie oder von Teilen davon entfernen. (Zusätzliche Rechte können so geschrieben sein, dass sie in bestimmten Fällen selbst entfernt werden müssen, wenn Sie das Werk verändern). Sie können zusätzliche Genehmigungen für Material erteilen, das Sie einem betroffenen Werk hinzugefügt haben und für das Sie eine entsprechende urheberrechtliche Genehmigung haben oder erteilen können.

Ungeachtet anderer Bestimmungen dieser Lizenz dürfen Sie für Material, das Sie einem betroffenen Werk hinzufügen, die Bedingungen dieser Lizenz durch Bedingungen ergänzen (sofern Sie von den Urheberrechtsinhabern dieses Materials dazu ermächtigt wurden):

- a. Gewährleistungsausschlüsse oder Haftungsbeschränkungen, die von den Bestimmungen der Abschnitte 15 und 16 dieser Lizenz abweichen; oder
- b. Erfordernis der Beibehaltung bestimmter angemessener rechtlicher Hinweise oder Autorenzuschreibungen in diesem Material oder in den entsprechenden rechtlichen Hinweisen, die in Werken, die dieses Material enthalten, angezeigt werden; oder
- c. das Verbot, die Herkunft des Materials falsch darzustellen, oder die Vorschrift, dass geänderte Versionen dieses Materials in angemessener Weise als von der verschiedenen gekennzeichnet werden müssen; oder
- d. Einschränkung der Verwendung der Namen von Lizenzgebern oder Urhebern des Materials zu Werbezwecken; oder
- e. Ablehnung der Gewährung von Rechten nach dem Markenrecht für die Verwendung bestimmter Handelsnamen, Marken oder Dienstleistungsmarken; oder
- f. Verpflichtung zur Entschädigung von Lizenzgebern und Urhebern dieses Materials durch jeden, der

das Material (oder modifizierte Versionen davon) mit vertraglichen Haftungsübernahmen an den Empfänger weitergibt, und zwar für jede Haftung, die diese vertraglichen Übernahmen diesen Lizenzgebern und Autoren direkt auferlegen.

Alle anderen nicht zulässigen zusätzlichen Bedingungen werden als "weitere Einschränkungen" im Sinne von Abschnitt 10 betrachtet. Wenn das Programm, so wie Sie es erhalten haben, oder irgendein Teil davon, einen Hinweis enthält, der besagt, daß es dieser Lizenz unterliegt, zusammen mit einer Klausel, die eine weitere Einschränkung darstellt, dürfen Sie diese Klausel entfernen. Wenn ein Lizenzdokument eine weitere Einschränkung enthält, aber die Weiterlizenzierung oder Weitergabe unter dieser Lizenz erlaubt, dürfen Sie einem betroffenen Werk Material hinzufügen, das den Bedingungen dieses Lizenzdokuments unterliegt, vorausgesetzt, daß die weitere Einschränkung eine solche Weiterlizenzierung oder Weitergabe nicht überdauert.

Wenn Sie in Übereinstimmung mit diesem Abschnitt Bedingungen zu einem betroffenen Werk hinzufügen, müssen Sie in den entsprechenden Quelldateien eine Erklärung der zusätzlichen Bedingungen, die für diese Dateien gelten, oder einen Hinweis darauf, wo die anwendbaren Bedingungen zu finden sind, anbringen.

Zusätzliche Bedingungen, erlaubende oder nicht erlaubende, können in Form einer gesonderten schriftlichen Lizenz oder als Ausnahmen angegeben werden; die oben genannten Anforderungen gelten in jedem Fall.

8. Beendigung.

Sie dürfen ein betroffenes Werk nicht verbreiten oder verändern, es sei denn, dies ist in dieser Lizenz ausdrücklich vorgesehen. Jeder Versuch, es anderweitig zu verbreiten oder zu verändern, ist ungültig und beendet automatisch Ihre Rechte unter dieser Lizenz (einschließlich jeglicher Patentreizenzen, die unter dem dritten Absatz von Abschnitt 11 gewährt werden).

Wenn Sie jedoch alle Verstöße gegen diese Lizenz einstellen, wird Ihre Lizenz von einem bestimmten Urheberrechtsinhaber (a) vorläufig wiederhergestellt, es sei denn, der Urheberrechtsinhaber hat Ihre Lizenz ausdrücklich und endgültig gekündigt, und (b) dauerhaft, wenn der Urheberrechtsinhaber Sie nicht vor Ablauf von 60 Tagen nach der Einstellung mit angemessenen Mitteln über den Verstoß informiert.

Darüber hinaus wird Ihre Lizenz von einem bestimmten Urheberrechtsinhaber dauerhaft wiederhergestellt, wenn der Urheberrechtsinhaber Sie auf angemessene Weise von der Verletzung benachrichtigt, dies das erste Mal ist, dass Sie von diesem Urheberrechtsinhaber eine Benachrichtigung über die Verletzung dieser Lizenz (für ein beliebiges Werk) erhalten haben, und Sie die Verletzung vor Ablauf von 30 Tagen nach Erhalt der Benachrichtigung beheben.

Die Beendigung Ihrer Rechte gemäß diesem Abschnitt beendet nicht die Lizenzen von Parteien, die Kopien oder Rechte von Ihnen gemäß dieser Lizenz erhalten haben. Wenn Ihre Rechte gekündigt und nicht dauerhaft wiederhergestellt wurden, sind Sie nicht berechtigt, neue Lizenzen für dasselbe Material gemäß Abschnitt 10 zu erhalten.

9. Die Annahme ist nicht erforderlich, um Kopien zu haben.

Sie sind nicht verpflichtet, diese Lizenz zu akzeptieren, um eine Kopie des Programms zu erhalten oder auszuführen. Die untergeordnete Verbreitung eines betroffenen Werkes, die allein als Folge der Verwendung von Peer-to-Peer-Übertragung zum Empfang einer Kopie auftritt, erfordert ebenfalls keine Annahme. Jedoch gewährt Ihnen nichts anderes als diese Lizenz die Erlaubnis, ein betroffenes Werk zu verbreiten oder zu verändern. Diese Handlungen verletzen das Urheberrecht, wenn Sie diese Lizenz nicht akzeptieren. Indem Sie ein betroffenes Werk verändern oder verbreiten, erklären Sie sich mit dieser Lizenz einverstanden, dies zu tun.

10. Automatische Lizenzierung von nachgeschalteten Empfängern.

Jedes Mal, wenn Sie ein betroffenes Werk übertragen, erhält der Empfänger automatisch eine Lizenz von ursprünglichen Lizenzgebern, um dieses Werk auszuführen, zu verändern und zu verbreiten, vorbehaltlich dieser Lizenz. Sie sind nicht dafür verantwortlich, die Einhaltung dieser Lizenz durch Dritte durchzusetzen.

Eine "Unternehmenstransaktion" ist eine Transaktion, bei der die Kontrolle über eine Organisation oder im Wesentlichen alle Vermögenswerte einer Organisation übertragen wird, eine Organisation aufgeteilt wird oder Organisationen fusioniert werden. Wenn die Verbreitung eines erfassten Werks aus einer Unternehmenstransaktion resultiert, muss jede an dieser Transaktion beteiligte Partei, die eine

Kopie des Werks erhält auch alle Lizenzen an dem Werk, die der Rechtsvorgänger der Partei gemäß dem vorhergehenden Absatz hatte oder erteilen konnte, sowie ein Recht auf den Besitz der korrespondierenden Quelle des Werks von dem Rechtsvorgänger, wenn dieser sie hat oder sie mit angemessenen Anstrengungen beschaffen kann.

Sie dürfen keine weiteren Beschränkungen für die Ausübung der unter dieser gewährten oder bestätigten Rechte auferlegen. Sie dürfen zum Beispiel keine Lizenzgebühren oder andere Gebühren für die Ausübung der unter dieser Lizenz gewährten Rechte erheben, und Sie dürfen keinen Rechtsstreit (einschließlich einer Gegenklage in einem Rechtsstreit) mit der Behauptung anstrengen, dass ein Patentanspruch durch die Herstellung, die Verwendung, den Verkauf, das Anbieten zum Verkauf oder den Import des Programms oder eines Teils davon verletzt wird.

11. Patente.

Ein "Mitwirkender" ist ein Urheberrechtsinhaber, der die Nutzung des Programms oder eines Werks, auf dem das Programm basiert, unter dieser Lizenz gestattet. Das auf diese Weise lizenzierte Werk wird als "Mitwirkerversion" des Mitwirkenden bezeichnet.

Die "wesentlichen Patentansprüche" eines Mitwirkenden sind alle Patentansprüche, die dem Mitwirkenden gehören oder von ihm kontrolliert werden, unabhängig davon, ob sie bereits erworben wurden oder in Zukunft erworben werden, und die durch irgendeine nach dieser Lizenz zulässige Art der Herstellung, der Benutzung oder des Verkaufs seiner Mitwirkerversion verletzt werden würden; sie umfassen jedoch keine Ansprüche, die nur als Folge einer weiteren Modifikation der Mitwirkerversion verletzt würden. Für die Zwecke dieser Definition schließt "Kontrolle" das Recht ein, Patentunterlizenzen in einer Weise zu erteilen, die mit den Anforderungen dieser Lizenz übereinstimmt.

Jeder Mitwirkende gewährt Ihnen eine nicht-exklusive, weltweite, gebührenfreie Patentlizenz unter den wesentlichen Patentansprüchen des Mitwirkenden, um den Inhalt seiner Mitwirkendenversion herzustellen, zu verwenden, zu verkaufen, zum Verkauf anzubieten, zu importieren und anderweitig auszuführen, zu verändern und zu verbreiten.

In den folgenden drei Absätzen ist eine "Patentlizenz" jede ausdrückliche Vereinbarung oder Verpflichtung, wie auch immer sie bezeichnet wird, ein Patent nicht durchzusetzen (z. B. eine ausdrückliche Erlaubnis zur Ausübung eines Patents oder die Zusage, nicht wegen Patentverletzung zu klagen). Einer Partei eine solche Patentlizenz zu "gewähren" bedeutet, eine solche Vereinbarung oder Verpflichtung einzugehen, ein Patent nicht gegen die Partei geltend zu machen.

Wenn Sie ein betroffenes Werk übertragen und sich dabei wissentlich auf eine Patentlizenz berufen, und der korrespondierende Quelltext des Werkes nicht für jedermann kostenlos und unter den Bedingungen dieser Lizenz über einen öffentlich zugänglichen Netzwerkserver oder andere leicht zugängliche Mittel kopierbar ist, dann müssen Sie entweder

- (1) die korrespondierende Quelle auf diese Weise verfügbar zu machen, oder
- (2) dafür sorgen, daß Ihnen der Vorteil der Patentlizenz für dieses bestimmte Werk entzogen wird, oder (3) in Übereinstimmung mit den Anforderungen dieser Lizenz dafür sorgen, daß die Patentlizenz auf nachgeschaltete Empfänger ausgedehnt wird. "Wissentliches Vertrauen" bedeutet, dass Sie tatsächliche Kenntnis davon haben, dass ohne die Patentlizenz Ihre Übertragung des betroffenen Werks in einem Land oder die Nutzung des betroffenen Werks durch Ihren Empfänger in einem Land ein oder mehrere identifizierbare Patente in diesem Land verletzen würde, von denen Sie Grund zu der Annahme haben, dass sie gültig sind.

Wenn Sie gemäß oder in Verbindung mit einer einzigen Transaktion oder Vereinbarung ein betroffenes Werk übertragen oder durch Vermittlung der Übertragung verbreiten und einigen der Parteien, die das betroffene Werk erhalten, eine Patentlizenz erteilen, die sie berechtigt, eine bestimmte Kopie des betroffenen Werks zu verwenden, zu verbreiten, zu verändern oder zu übertragen, dann wird die von Ihnen erteilte Patentlizenz automatisch auf alle Empfänger des betroffenen Werks und der darauf basierenden Werke ausgedehnt.

Eine Patentlizenz ist "diskriminierend", wenn sie eines oder mehrere der Rechte, die im Rahmen dieser Lizenz ausdrücklich gewährt werden, nicht in den Anwendungsbereich einbezieht, ihre Ausübung verbietet oder von der Nichtausübung abhängig macht. Sie dürfen ein betroffenes Werk nicht übertragen, wenn Sie an einer Vereinbarung mit einem Dritten beteiligt sind, der im Vertrieb von Software tätig ist, nach der Sie an den Dritten eine Zahlung auf der Grundlage des Umfangs Ihrer Tätigkeit der Übertragung des Werks leisten und nach der der Dritte jeder der Parteien, die das betroffene Werk von Ihnen erhalten würden, eine diskriminierende Patentlizenz gewährt (a) in Verbindung mit Kopien des betroffenen Werks, die übertragen werden durch

(oder von diesen Kopien hergestellte Kopien) oder (b) in erster Linie für und in Verbindung mit bestimmten Produkten oder Zusammenstellungen, die das geschützte Werk enthalten, es sei denn, Sie sind diese Vereinbarung vor dem 28. März 2007 eingegangen oder die Patenzlizenz wurde vor diesem Zeitpunkt erteilt.

Keine Bestimmung dieser Lizenz ist so auszulegen, dass sie eine stillschweigende Lizenz oder andere Verteidigungsmöglichkeiten gegen eine Verletzung ausschließt oder einschränkt, die Ihnen nach dem geltenden Patentrecht zustehen könnten.

12. Kein Verzicht auf die Freiheit der anderen .

Wenn Ihnen Bedingungen auferlegt werden (sei es durch Gerichtsbeschluss, Vereinbarung oder auf andere Weise), die den Bedingungen dieser Lizenz widersprechen, entbinden sie Sie nicht von den Bedingungen dieser Lizenz. Wenn Sie ein betroffenes Werk nicht so übertragen können, daß Sie gleichzeitig Ihre Verpflichtungen aus dieser Lizenz und andere einschlägige Verpflichtungen erfüllen, dürfen Sie es folglich überhaupt nicht übertragen. Wenn Sie beispielsweise Bedingungen zustimmen, die Sie verpflichten, von denjenigen, denen Sie das Programm übertragen, eine Lizenzgebühr für die Weiterübertragung zu erheben, wäre die einzige Möglichkeit, sowohl diese Bedingungen als auch diese Lizenz zu erfüllen, der vollständige Verzicht auf die Übertragung des Programms.

13. Verwendung unter der GNU Affero General Public License.

Ungeachtet anderer Bestimmungen dieser Lizenz haben Sie die Erlaubnis, ein betroffenes Werk mit einem unter Version 3 der GNU Affero General Public License lizenzierten Werk zu einem einzigen kombinierten Werk zu verbinden oder zu kombinieren und das resultierende Werk zu übertragen. Die Bedingungen dieser Lizenz gelten weiterhin für den Teil, der das betroffene Werk ist, aber die besonderen Anforderungen der GNU Affero General Public License, Abschnitt 13, bezüglich der Interaktion über ein Netzwerk gelten für die Kombination als solche.

14. Überarbeitete Fassungen dieser Lizenz.

Die Free Software Foundation kann von Zeit zu Zeit überarbeitete und/oder neue Versionen der GNU General Public License veröffentlichen. Solche neuen Versionen werden im Geiste der gegenwärtigen Version ähnlich sein, können sich aber im Detail unterscheiden, um neue Probleme oder Anliegen zu behandeln.

Jede Version ist mit einer Versionsnummer gekennzeichnet. Wenn das Programm angibt, dass eine bestimmte nummerierte Version der GNU General Public License "oder eine spätere Version" für es gilt, haben Sie die Möglichkeit, entweder die Bedingungen dieser nummerierten Version oder einer späteren, von der Free Software Foundation veröffentlichten Version zu befolgen. Wenn das Programm keine Versionsnummer der GNU General Public License angibt, können Sie eine beliebige, jemals von der Free Software Foundation veröffentlichte Version wählen.

Wenn das Programm vorsieht, dass ein Bevollmächtigter entscheiden kann, welche zukünftigen Versionen der GNU General Public License verwendet werden können, ermächtigt die öffentliche Erklärung dieses Bevollmächtigten, eine Version zu akzeptieren, Sie dauerhaft, diese Version für das Programm zu wählen.

Spätere Lizenzversionen können Ihnen zusätzliche oder andere Berechtigungen geben. Es entstehen jedoch keine zusätzlichen Verpflichtungen für Autoren oder Urheberrechtsinhaber, wenn Sie sich für spätere Version entscheiden.

15. Ausschluss der Garantie.

Es gibt keine Garantie für das Programm, soweit dies nach geltendem Recht zulässig ist. Sofern nicht schriftlich anders angegeben, stellen die Urheberrechtsinhaber und/oder andere Parteien das Programm "wie es ist" zur Verfügung, ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf die stillschweigende Garantie der Marktgängigkeit und der Eignung für einen bestimmten Zweck. Das gesamte Risiko in Bezug auf die Qualität und Leistung des Programms liegt bei Ihnen. Sollte sich das Programm als fehlerhaft erweisen, übernehmen Sie die Kosten für alle notwendigen Wartungsarbeiten, Reparaturen oder Korrekturen.

16. Beschränkung der Haftung .

in keinem fall, es sei denn, dies ist gesetzlich vorgeschrieben oder schriftlich vereinbart, haftet ein urheberrechtsinhaber oder eine andere partei, die das programm wie oben erlaubt modifiziert und/oder weitergibt, ihnen gegenüber für schäden, einschliesslich allgemeiner, spezieller, zufälliger oder folgeschäden, die sich aus der nutzung oder der unfähigkeit zur nutzung des programms ergeben (einschliesslich, aber nicht beschränkt auf datenverluste oder ungenaue daten oder verluste, die sie oder dritte erleiden, oder ein versagen des programms, mit anderen programmen zusammenzuarbeiten), selbst wenn der urheberrechtsinhaber oder eine andere partei auf die möglichkeit solcher schäden hingewiesen wurde.

17. Auslegung der Abschnitte 15 und 16.

Wenn der oben genannte Gewährleistungsausschluss und die Haftungsbeschränkung nicht gemäß ihren Bestimmungen in gesetzlich werden können, wenden die überprüfenden Gerichte das örtliche Recht an, das einem absoluten Verzicht auf jegliche zivilrechtliche Haftung im Zusammenhang mit dem Programm am nächsten kommt, es sei denn, eine Garantie oder Haftungsübernahme liegt einer Kopie des Programms gegen eine Gebühr bei.

7.3 BSD 2.0

Die BSD 2.0 Lizenz

Copyright (c) 2009 Kontron America, Inc. Alle Rechte vorbehalten.

Die Weiterverbreitung und Verwendung in Quell- und Binärform, mit oder ohne Änderungen, ist gestattet, sofern die folgenden Bedingungen erfüllt sind:

- a. Bei der Weitergabe des Quellcodes müssen der obige Urheberrechtsvermerk, diese Liste von Bedingungen und der folgende Hinweis beibehalten werden.
- b. Weiterverteilungen in Binärform müssen den obigen Copyright-Hinweis, diese Liste von Bedingungen und den folgenden Haftungsausschluss in der Dokumentation und/oder anderen mit der Verteilung gelieferten Materialien wiedergeben.
- c. Weder der Name von Kontron noch die Namen der Mitwirkenden dürfen ohne ausdrückliche vorherige schriftliche Genehmigung verwendet werden, um von dieser Software abgeleitete Produkte zu unterstützen oder zu bewerben.

Diese Software wird von den Urheberrechtsinhabern und Mitwirkenden im Ist-Zustand zur Verfügung gestellt, und alle ausdrücklichen oder stillschweigenden Garantien, einschließlich, aber nicht beschränkt auf die stillschweigenden Garantien der Marktgängigkeit und der Eignung für einen bestimmten Zweck, werden ausgeschlossen. In keinem Fall haften der Urheberrechtsinhaber oder die Mitwirkenden für direkte, indirekte, zufällige, besondere, beispielhafte oder Folgeschäden (einschließlich, aber nicht beschränkt auf die Beschaffung von Ersatzwaren oder -dienstleistungen, Nutzungs-, Daten- oder Gewinnverluste oder Geschäftsunterbrechungen), wie auch immer diese verursacht wurden und auf welcher Haftungstheorie sie beruhen, ob aus Vertrag, verschuldensunabhängiger Haftung oder unerlaubter Handlung (einschließlich Fahrlässigkeit oder anderweitig), die in irgendeiner Weise aus der Verwendung dieser Software entstehen, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.