كيف يمكنني تسجيل رؤوس الرسائل؟

المحتويات

المقدمة

يوضح هذا المستند كيفية تسجيل رؤوس الرسائل التي تمت معالجتها من خلال جهاز أمان البريد الإلكتروني (ESA) من Cisco.

كيف يمكنني تسجيل رؤوس الرسائل؟

في بعض الحالات، من المفيد تسجيل وجود محتويات رؤوس الرسائل أثناء مرورها عبر الجهاز. أنت تعين الرؤوس أن تسجل عن طريق **logConfig > loghaders**. سيقوم ESA بتسجيل رؤوس الرسائل المحددة في سجلات البريد النصي ل IronPort وسجلات تسليم IronPort وسجلات إرتداد IronPort. إذا كان الرأس موجودا، يقوم النظام بتسجيل اسم الرأس والقيمة. سيتم إسترداد معلومات الرأس بعد معلومات التسليم.

فيما يلي مثال على كيفية تمكين التسجيل لتسجيل أي رسالة بالعنوانين X-IPAS-Result و X-IronPort-AV:

```
my_esa.local> logconfig

:Currently configured logs
Log Name Log Type Retrieval Interval
-----------------------------------------------------------------------------
amp AMP Engine Logs Manual Download None .1
amparchive AMP Archive Manual Download None .2
antispam Anti-Spam Logs Manual Download None .3
antivirus Anti-Virus Logs Manual Download None .4
asarchive Anti-Spam Archive Manual Download None .5
authentication Authentication Logs Manual Download None .6
avarchive Anti-Virus Archive Manual Download None .7
bounces Bounce Logs Manual Download None .8
cli_logs CLI Audit Logs Manual Download None .9
encryption Encryption Logs Manual Download None .10
error_logs IronPort Text Mail Logs Manual Download None .11
euq_logs Spam Quarantine Logs Manual Download None .12
euqgui_logs Spam Quarantine GUI Logs Manual Download None .13
ftpd_logs FTP Server Logs Manual Download None .14
gui_logs HTTP Logs Manual Download None .15
mail_logs IronPort Text Mail Logs Manual Download None .16
mail_logs_copy IronPort Text Mail Logs SCP Push - Host .17
Port 22None :192.168.0.200
repeng Reputation Engine Logs Manual Download None .18
reportd_logs Reporting Logs Manual Download None .19
reportqueryd_logs Reporting Query Logs Manual Download None .20
```

```
                                    scanning Scanning Logs Manual Download None .21
                                slbld_logs Safe/Block Lists Logs Manual Download None .22
                                    snmp_logs SNMP Logs Manual Download None .23
                                    sntpd_logs NTP logs Manual Download None .24
                                     status Status Logs Manual Download None .25
                                system_logs System Logs Manual Download None .26
                            trackerd_logs Tracking Logs Manual Download None .27
                              updater_logs Updater Logs Manual Download None .28
                              upgrade_logs Upgrade Logs Manual Download None .29

                                                :Choose the operation you want to perform
                                                            .NEW - Create a new log -
                                                    .EDIT - Modify a log subscription -
                                                .DELETE - Remove a log subscription -
                                                        .SETUP - General settings -
                                                .LOGHEADERS - Configure headers to log -
                                            .HOSTKEYCONFIG - Configure SSH host keys -
                                                                    logheaders <[]

                                Please enter the list of headers you wish to record in the
                                                                            .log files
                                                        .Separate multiple headers with commas
                                                    X-IPAS-Result, X-IronPort-AV <[]
```

ارجع إلى موجه أوامر واجهة سطر الأوامر (CLI) الرئيسية، **وقم** بتنفيذ أي/جميع التغييرات.

عند مراجعة mail_log، سترى نتيجة الرؤوس التي تم حقنها الآن في السجلات كما تم تكوينها:

```
                Thu Aug 14 08:40:18 2014 Info: New SMTP ICID 10282 interface Management
        address 192.168.0.200 reverse dns host ns.domain.com verified no (192.168.0.199)
            Thu Aug 14 08:40:18 2014 Info: ICID 10282 RELAY SG RELAY_SG match 192.168.0.200
                                                                        SBRS not enabled
                                    Thu Aug 14 08:40:18 2014 Info: Start MID 1403 ICID 10282
        <Thu Aug 14 08:40:18 2014 Info: MID 1403 ICID 10282 From: <orig_user@domain.com
      <Thu Aug 14 08:40:18 2014 Info: MID 1403 ICID 10282 RID 0 To: <end_user@example.com
            Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
                                                                        cached verdict
    ,Thu Aug 14 08:40:18 2014 Info: SPF Verdict Cache cache status: hits = 7, misses = 12
                                expires = 0, adds = 12, seconds saved = 0.06, total seconds = 0.56
    Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: helo identity postmaster@domain.com None
            Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
                                                                        cached verdict
      Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: mailfrom identity orig_user@domain.com
                                                                        (Pass (v=spf1
            Thu Aug 14 08:40:18 2014 Info: MID 1403 using engine: SPF Verdict Cache using
                                                                        cached verdict
      Thu Aug 14 08:40:18 2014 Info: MID 1403 SPF: pra identity orig_user@domain.com None
                                                                        headers from
'<Thu Aug 14 08:40:18 2014 Info: MID 1403 Message-ID '<20140814124103.GC6764@domain.com
'...Thu Aug 14 08:40:18 2014 Info: MID 1403 Subject 'Hello - this is the morning report
        <Thu Aug 14 08:40:18 2014 Info: MID 1403 ready 611 bytes from <orig_user@domain.com
Thu Aug 14 08:40:18 2014 Info: MID 1403 matched all recipients for per-recipient policy
                                                                    DEFAULT in the outbound table
                                        Thu Aug 14 08:40:18 2014 Info: ICID 10282 close
Thu Aug 14 08:40:20 2014 Info: MID 1403 interim verdict using engine: CASE spam negative
                    Thu Aug 14 08:40:20 2014 Info: MID 1403 using engine: CASE spam negative
            Thu Aug 14 08:40:20 2014 Info: MID 1403 interim AV verdict using Sophos CLEAN
                                Thu Aug 14 08:40:20 2014 Info: MID 1403 antivirus negative
                Thu Aug 14 08:40:20 2014 Info: MID 1403 Outbreak Filters: verdict negative
                                Thu Aug 14 08:40:20 2014 Info: MID 1403 DLP no violation
```

```
Thu Aug 14 08:40:20 2014 Info: MID 1403 queued for delivery
Thu Aug 14 08:40:20 2014 Info: New SMTP DCID 173 interface 192.168.0.199 address
                                                                port 25 111.22.111.22
    Thu Aug 14 08:40:20 2014 Info: DCID 173 STARTTLS command not supported
[Thu Aug 14 08:40:20 2014 Info: Delivery start DCID 173 MID 1403 to RID [0
 [Thu Aug 14 08:40:20 2014 Info: Message done DCID 173 MID 1403 to RID [0
X-IPAS-Result', 'AmYGAMSt7FPAqADI/2dsb2JhbABahBuNU6VQAZpbiQV3hCMhYxg0BRi')]
 =JC8VuF4wKg1+DGYEdAQSPCoMNiiEBmHaDHwEBAQ'), ('X-IronPort-AV', 'E=Sophos;i
                                  [('"r\n d="scan\'208";a="1403\ ;"5.01,863,1400040000"
    Thu Aug 14 08:40:20 2014 Info: MID 1403 RID [0] Response '2.0.0 OK
                                                              'F6/FE-18769-93EACE35
  Thu Aug 14 08:40:20 2014 Info: Message finished MID 1403 done
  Thu Aug 14 08:40:25 2014 Info: DCID 173 close
```

من البريد الإلكتروني المتلقى، إذا كنت ستنظر إلى الرؤوس في ذلك البريد الإلكتروني مباشرة، سترى رؤوس X-IPAS-Result و X-IronPort-AV المبرزة في الرؤوس الأصلية قبل أول خطوة مستلمة:

```
                                    X-IronPort-Anti-Spam-Filtered: true
X-IPAS-Result: AmYGAMSt7FPAqADI/2dsb2JhbABahBuNU6VQAZpbiQV3hCMhYxg0BRiJC8VuF4wKg1+
                                                    DGYEdAQSPCoMNiiEBmHaDHwEBAQ
                                  ;"X-IronPort-AV: E=Sophos;i="5.01,863,1400040000
                                                     "d="scan'208";a="1403
  Received: from ns.domain.com (HELO mail.domain.com) ([192.168.0.200])  by
                          myesa_local.domain.com with ESMTP; 14 Aug 2014 08:40:18 -0400
,Received: by mail.domain.com (Postfix, from userid 1000)id 29F4E8033E; Thu
                                                    (Aug 2014 08:41:03 -0400 (EDT 14
                                    Date: Thu, 14 Aug 2014 08:41:03 -0400
                                <From: robert <orig_user@domain.com.com
                                                    <To: <end_user@example.com
                            ...Subject: Hello - this is the morning report
                            <Message-ID: <20140814124103.GC6764@domain.com
                                                    MIME-Version: 1.0
                                  (User-Agent: Mutt/1.5.21 (2010-09-15
                                X-RR-Connecting-IP: 111.22.111.222:25
                                                    X-Cloudmark-Score: 0
                                Return-Path: orig_user@domain.com.com
                  X-MS-Exchange-Organization-AuthSource: xhc-aln-x10.example.com
                                    X-MS-Exchange-Organization-AuthAs: Internal
                                X-MS-Exchange-Organization-AuthMechanism: 10
                                                  ;Content-type: text/plain
                                                          "charset="US-ASCII
                                Content-transfer-encoding: 7bit

                                                    .No info this morning

                                                    Joe-
```

ملاحظة: يوجد RFC لبروتوكول SMTP في http://www.faqs.org/rfcs/rfc2821.html ويحدد الرؤوس المعرفة من قبل المستخدم.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).