思科 Threat Grid 设备  
版本说明



**版本： 2.7.2 ag**

上次更新时间： 8/8/2019

思科公司 www.cisco.com

本文所有内容版权所有 © 2015-2019 思科公司和/或其附属公司。版权所有。

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与 Cisco 代表联系以获取副本。

思科所采用的 TCP 信头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。© 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上面所提及的提供商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，Cisco 及其供应商概不负责，即使 Cisco 及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问以下网址：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：[www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。

封面照片版权所有 © 2016 Mary C. Ecsedy。版权所有。已获得使用许可。

本文所有内容版权所有 © 2015-2019 思科公司和/或其附属公司。版权所有。

# 目录

[User Documentation 9](#_Toc18050393)

[Backup FAQ 9](#_Toc18050394)

[Clustering Overview and FAQ 9](#_Toc18050395)

[Installing Updates 9](#_Toc18050396)

[Build Number/Release Version Lookup Table 10](#_Toc18050397)

[Version 2.7.2ag 14](#_Toc18050398)

[Version 2.7.2 15](#_Toc18050399)

[Fixes and Updates 15](#_Toc18050400)

[Security Updates 15](#_Toc18050401)

[Version 2.7.1 16](#_Toc18050402)

[Fixes and Updates 16](#_Toc18050403)

[Known Issues 16](#_Toc18050404)

[Security Updates 16](#_Toc18050405)

[Version 2.7 17](#_Toc18050406)

[Fixes and Updates 17](#_Toc18050407)

[Known Issues 19](#_Toc18050408)

[Other Notes 19](#_Toc18050409)

[Version 2.6 20](#_Toc18050410)

[Fixes and Updates 20](#_Toc18050411)

[Version 2.5 21](#_Toc18050412)

[Fixes and Updates 21](#_Toc18050413)

[Version 2.4.3.3 22](#_Toc18050414)

[Fixes and Updates 22](#_Toc18050415)

[Version 2.4.3.2 23](#_Toc18050416)

[Fixes and Updates 23](#_Toc18050417)

[Version 2.4.3.1 24](#_Toc18050418)

[Version 2.4.3 24](#_Toc18050419)

[Fixes and Updates 24](#_Toc18050420)

[Version 2.4.2 25](#_Toc18050421)

[Fixes and Updates 25](#_Toc18050422)

[Version 2.4.1 27](#_Toc18050423)

[Fixes and Updates 27](#_Toc18050424)

[Known Issues 27](#_Toc18050425)

[Security Updates 28](#_Toc18050426)

[Version 2.4.0.1 29](#_Toc18050427)

[Fixes and Updates 29](#_Toc18050428)

[Security Updates 29](#_Toc18050429)

[Version 2.4 30](#_Toc18050430)

[Fixes and Updates 30](#_Toc18050431)

[Version 2.3.3 31](#_Toc18050432)

[Fixes and Updates 31](#_Toc18050433)

[Version 2.3.2 32](#_Toc18050434)

[Fixes and Updates 32](#_Toc18050435)

[Version 2.3.1 33](#_Toc18050436)

[Fixes and Updates 33](#_Toc18050437)

[Version 2.3 34](#_Toc18050438)

[Fixes and Updates 34](#_Toc18050439)

[Version 2.2.4 35](#_Toc18050440)

[Fixes and Updates 35](#_Toc18050441)

[Version 2.2.3 36](#_Toc18050442)

[Important Note 36](#_Toc18050443)

[Fixes and Updates 36](#_Toc18050444)

[Security Updates 36](#_Toc18050445)

[Version 2.2.2 37](#_Toc18050446)

[Important Note 37](#_Toc18050447)

[Bug Fixes 37](#_Toc18050448)

[Enhancements 37](#_Toc18050449)

[Version 2.2.1 38](#_Toc18050450)

[IMPORTANT NOTE 38](#_Toc18050451)

[New Features 38](#_Toc18050452)

[Bug Fixes 38](#_Toc18050453)

[Security Fixes 38](#_Toc18050454)

[Version 2.2mfg 39](#_Toc18050455)

[Version 2.2 40](#_Toc18050456)

[REQUIREMENT 40](#_Toc18050457)

[Documentation 40](#_Toc18050458)

[About This Release 40](#_Toc18050459)

[New Features 40](#_Toc18050460)

[Bug Fixes 41](#_Toc18050461)

[Security Fixes 41](#_Toc18050462)

[Version 2.1.6 42](#_Toc18050463)

[New Features 42](#_Toc18050464)

[Known Issues 42](#_Toc18050465)

[Version 2.1.5 43](#_Toc18050466)

[New Features 43](#_Toc18050467)

[Bug Fixes 43](#_Toc18050468)

[Known Issues 43](#_Toc18050469)

[Version 2.1.4 44](#_Toc18050470)

[New Features 44](#_Toc18050471)

[Bug Fixes 44](#_Toc18050472)

[Known Issues 44](#_Toc18050473)

[Version 2.1.3 45](#_Toc18050474)

[New Features 45](#_Toc18050475)

[Bug Fixes 45](#_Toc18050476)

[Known Issues 45](#_Toc18050477)

[Version 2.1.2 46](#_Toc18050478)

[Bug Fixes 46](#_Toc18050479)

[Known Issues 46](#_Toc18050480)

[Version 2.1.1 47](#_Toc18050481)

[New Features 47](#_Toc18050482)

[Bug Fixes 47](#_Toc18050483)

[Security Fixes 47](#_Toc18050484)

[Known Issues 47](#_Toc18050485)

[Version 2.1 48](#_Toc18050486)

[New Features 48](#_Toc18050487)

[Bug Fixes 48](#_Toc18050488)

[Security Fixes 48](#_Toc18050489)

[Known Issues 49](#_Toc18050490)

[Version 2.0.4 50](#_Toc18050491)

[New Features 50](#_Toc18050492)

[Bug Fixes 50](#_Toc18050493)

[Version 2.0.3 51](#_Toc18050494)

[Version 2.0.2 52](#_Toc18050495)

[Security Updates 52](#_Toc18050496)

[Version 2.0.1 53](#_Toc18050497)

[Bug Fixes 53](#_Toc18050498)

[Known Issues 53](#_Toc18050499)

[Version 2.0 54](#_Toc18050500)

[New Features 55](#_Toc18050501)

[Bug Fixes 55](#_Toc18050502)

[Security Fixes 55](#_Toc18050503)

[Known Issues 55](#_Toc18050504)

[Version 1.4.6 55](#_Toc18050505)

[New Features 55](#_Toc18050506)

[Version 1.4.5 57](#_Toc18050507)

[Version 1.4.4 58](#_Toc18050508)

[Bug Fixes 58](#_Toc18050509)

[Version 1.4.3 59](#_Toc18050510)

[New Features 59](#_Toc18050511)

[Security Updates 59](#_Toc18050512)

[Known Issues 59](#_Toc18050513)

[Version 1.4.2 60](#_Toc18050514)

[Bug Fixes 60](#_Toc18050515)

[Known Issues 60](#_Toc18050516)

[Version 1.4.1 61](#_Toc18050517)

[Upgrading from a Release Prior to 1.4 61](#_Toc18050518)

[Bug Fixes 61](#_Toc18050519)

[Version 1.4 62](#_Toc18050520)

[New Features 62](#_Toc18050521)

[Bug Fixes 62](#_Toc18050522)

[Version 1.3 64](#_Toc18050523)

[New Features 64](#_Toc18050524)

[Bug Fixes 64](#_Toc18050525)

[Security Updates 65](#_Toc18050526)

[Other Notes 65](#_Toc18050527)

[Version 1.2.1 66](#_Toc18050528)

[New Features 66](#_Toc18050529)

[Security Updates 66](#_Toc18050530)

[Version 1.2 67](#_Toc18050531)

[New Features 67](#_Toc18050532)

[Bugs Fixed 67](#_Toc18050533)

[Security Updates 67](#_Toc18050534)

[Other Improvements 68](#_Toc18050535)

[Known Issues 68](#_Toc18050536)

[Version 1.1 Hotfix 1 69](#_Toc18050537)

[Version 1.1 70](#_Toc18050538)

[New Features 70](#_Toc18050539)

[Bugs Fixed 70](#_Toc18050540)

[Security Updates 70](#_Toc18050541)

[1.0+hotfix2 Update - Mandatory 72](#_Toc18050542)

# 用户文档

Threat Grid 设备用户文档可在[思科网站上的“Threat Grid 设备安装和升级指南”页面](https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html)获取。

**注意：**[Threat Grid 设备产品和支持页面](https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html)**提供了**较新的文档。

## 备份常见问题

有关技术信息和说明，请参阅[备份说明和常见问题解答](https://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/backup-faq-2-2-4.pdf)。

## 集群概述和常见问题解答

有关其他信息，请参阅[集群概述和常见问题解答](https://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/clustering-overview-faq-v2-4-2.pdf)。

# 安装更新

您必须先按照思科网站 [Threat Grid 设备安装和升级指南页面上提供的](https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html)《AMP Threat Grid 设备设置和配置指南》中所述完成初始设置和配置步骤，然后才能使用更高版本更新 Threat Grid 设备。

**新设备：**如果您的新设备出厂时安装了较低的版本，并且您希望安装更新，则必须先完成初始配置。**请在**完成所有设备配置之后再应用更新。

除非已安装许可，否则将不会下载设备更新；并且，如果尚未完全配置设备（包括数据库），则可能无法正确应用设备更新。

Threat Grid 设备更新是通过 OpAdmin 门户应用的。

更新是不可逆的：在升级到最新版本后，您无法再将其恢复到先前版本。

要测试更新，请提交一个样本进行分析。

# 内部版本号/发行版本查询表

| **内部版本号** | **发行版本** | **发布日期** | **说明** |
| --- | --- | --- | --- |
| 2019.02.20190808 t000800 srchash. b61789e86a09. rel | 2.7.2 ag | 8/8/2019 | 仅限空气有空隙的设备。 |
| 2019.02.20190723 t224935 srchash. bb8b40c2e248. rel | 2.7.2 | 7/23/2019 | 备份修剪修复;安全和 M5 制造更新。 |
| 2019.02.20190703 t201951 srchash. 0f2b9bc45628. rel | 2.7.1 | 7/3/2019 | 网络模拟;将 ES 索引迁移到版本6。 |
| 2019.02.20190601 t155353 srchash. b67f91c65917. rel | 2.7 | 6/1/2019 | 刷新到 3.5.27；ES6；XFS；Wal-G；重置时擦除的数据驱动器。 |
| 2018.12.20190204 t162246 srchash. cb9269c1357f. rel | 2.6 | 2/4/2019 | 硬保留限制 |
| 2018.08.20180914205342.474 e26a8. rel | 2.5 | 9/14/2018 | Win10；示例删除。刷新到 3.5.11 |
| 2017.12.20180601200650.e0c052b0.rel | 2.4.3.3 | 2018 年 6 月 1 日 | 修复集群初始化、删除过时的 ES/PG 迁移支持。 |
| 2017.12.20180519011227.ed8a11e9.rel | 2.4.3.2 | 2018 年 5 月 19 日 | CVE-2018-1000085 的 ClamAV 更新。漏洞修复。 |
| 2017.12.20180501005218.4e3746f4.rel | 2.4.3.1 | 2018 年 5 月 1 日 | 更新检查时的 DDL 错误检测 PG 架构报告。 |
| 2017.12.20180427231427.e616a2f2.rel | 2.4.3 | 2018 年 4 月 27 日 | 远程虚拟出口定位；直接“单机到集群”迁移。 |
| 2017.12.20180302174440.097e2883.rel | 2.4.2 | 2018 年 3 月 2 日 | 集群。 |
| 2017.12.20180219033153.bb5e549b.rel | 2.4.1 | 2018 年 2 月 19 日 | OpAdmin 中支持集群功能。将应用刷新到 3.4.59 |
| 2017.12.20180130110951. ce6dd56e | 2.4.0.1 | 2018 年 1 月 30 日 | 仅 ClamAV 安全更新。 |
| 2017.12.20171214191003.4b7fea16.rel | 2.4 | 2017 年 12 月 14 日 | 集群 EFT。 jp/kr contsubs。门户更新到 3.4.57。 |
| 2016.05.201711300223355.1c7bd023.rel | 2.3.3 | 2017 年 11 月 30 日 | 版本 2.4 升级的起点。 |
| 2016.05.20171007215506.0700e1db.rel | 2.3.2 | 2017 年 10 月 7 日 | ElasticSearch 分片数量减少。 |
| 2016.05.20170828200941.e5eab0a6.rel | 2.3.1 | 2017 年 8 月 28 日 | 漏洞修复。 |
| 2016.05.20170810212922.28c79852.rel | 2.3 | 2017 年 8 月 11 日 | 自动下载许可证。门户软件更新到 3.4.47 。 |
| 2016.05.20170710175041.77c0b12f.rel | 2.2.4 | 2017 年 7 月 10 日 | 此版本引入了备份功能。 |
| 2016.05.20170519231807.db2f167e.rel | 2.2.3 | 2017 年 5 月 20 日 | 此次要版本更新提供了不需要 Windows XP 即可运行的新出厂设置。 |
| 2016.05.20170508195308.b8dc88ed.rel | 2.2.2 | 2017 年 5 月 8 日 | 次要版本更新，对网络配置和操作系统组件进行了若干更改以支持即将推出的功能。 |
| 2016.05.20170323020633.f82e66fe.rel | 2.2.1 | 2017 年 3 月 24 日 | 禁用 SSLv3；修复资源问题 |
| 2016.05.20170308211223.c92516ee.rel | 2.2mfg | 2017 年 3 月 8 日 | 仅在制造上有所更改。对客户无影响。未通过更新服务器进行部署。 |
| 2016.05.20170303034712.1b205359.rel | 2.2 | 2017 年 3 月 3 日 | 系统迁移、  新门户 UI 、“Mask”、  可为处置服务配置多个 URL |
| 2016.05.20170105200233.32f70432.rel | 2.1.6 | 2017 年 1 月 7 日 | 为 OpAdmin/tgsh-dialog 提供 LDAP 身份验证支持 |
| 2016.05.20161121134140.489f130d.rel | 2.1.5 | 2016 年 11 月 21 日 | ElasticSearch5；修复 CSA 性能问题。 |
| 2016.05.20160905202824.f7792890.rel | 2.1.4 | 2016 年 9 月 5 日 | 主要面向制造业 |
| 2016.05.20160811044721.6af0fa61.rel | 2.1.3 | 2016 年 8 月 11 日 | 离线更新支持密钥，支持 M4 擦除。 |
| 2016.05.20160715165510.baed88a3.rel | 2.1.2 | 2016 年 7 月 15 日 |  |
| 2016.05.20160706015125.b1fc50e5.rel-1 | 2.1.1 | 2016 年 7 月 6 日 |  |
| 2016.05.20160621044600.092b23fc | 2.1 | 2016 年 6 月 21 日 |  |
| 2015.08.20160501161850.56631ccd | 2.0.4 | 2016 年 5 月 1 日 | 版本 2.1 更新的起点。必须先升级到版本 2.0.4，然后才能更新到版本 2.1。 |
| 2015.08.20160315165529.599f2056 | 2.0.3 | 2016 年 3 月 15 日 | 引入 AMP 集成、CA 管理和分离 DNS。 |
| 2015.08.20160217173404.ec264f73 | 2.0.2 | 2016 年 2 月 18 日 |  |
| 2015.08.20160211192648.7e3d2e3a | 2.0.1 | 2016 年 2 月 12 日 |  |
| 2015.08.20160131061029.8b6bc1d6 | v2.0 | 2016 年 2 月 11 日 | 强制从此版本更新到版本 2.0.1。 |
| 2014.10.20160115122111.1f09cb5f | v1.4.6 | 2016 年 1 月 27 日 | 2.0.4 更新的起点。 |
| 2014.10.20151123133427.898f70c2 | v1.4.5 | 2015 年 11 月 25 日 |  |
| 2014.10.20151116154826.9af96403 | v1.4.4 |  |  |
| 2014.10.20151020111307.3f124cd2 | v1.4.3 |  |  |
| 2014.10.20150904134201.ef4843e7 | v1.4.2 |  |  |
| 2014.10.20150824161909.4ba773cb | v1.4.1 |  |  |
| 2014.10.20150822201138.8934fa1d | v1.4 |  |  |
| 2014.10.20150805134744.4ce05d84 | v1.3 |  |  |
| 2014.10.20150709144003.b4d4171c | v1.2.1 |  |  |
| 2014.10.20150326161410.44cd33f3 | v1.2 |  |  |
| 2014.10.20150203155143+hotfix1.b06f7b4f | v1.1  + hotfix1 |  |  |
| 2014.10.20150203155142.b06f7b4f | v1.1 |  |  |
| 2014.10.20141125162160+hotfix2.8afc5e2f | v1.0  +hotfix2 |  | **注意：**版本 1.0+hotfix2 是强制更新，可对更新系统本身进行修复，使该系统无需拆分大文件即可对其进行处理。 |
| 2014.10.20141125162158.8afc5e2f | v1.0 |  |  |

# 版本 2.7.2 ag

此版本与威胁网格设备版本 2.7.2 相同，只是它增加了对更高效的离线更新介质生成机制的支持。

# 版本 2.7.2

此版本修复了导致 NFS 备份在 2.7.0 和 2.7.1 版本中需要过多存储的问题;并增加了能够通过 clean 接口（作为控制台中的显式切换）访问 opadmin 的功能。

## 修复和更新

* 现在，只有在成功创建新的基本备份后，才会保留数据库基础备份。
* 现在，控制台配置接口支持 "enable\_clean\_opadmin" 选项，默认情况下禁用此选项（在应用配置和重新启动后），允许访问分配的 clean IP 的端口 8443 上的管理界面。

## 安全更新

更新 redis 以获取数据损坏修复，包括 CVE-2019-10192 和 CVE-2019-10193。

# 版本 2.7.1

此版本增加了设备的网络模拟支持，为某些安全问题实施规避，修复可能导致在 2.7.0 上进行数据重置后导致集群设置失败的漏洞，从而实现后台迁移以实现与未来的兼容性版本基于 Elasticsearch 的较新版本，并进行了各种更小的改进。

## 修复和更新

* 网络模拟现已在设备上提供，解决了2.7.0 中的已知限制。
* 设备配置 UI 的 "退出" 部分现在有一种额外的模式，即只有本地模拟的网络可用于虚拟机。在管理性选择此选项的情况下，API 和 UI 用户无法选择任何会将来自 Vms 的网络流量发送到本地设备之外的目标的任何选项。
* 在此版本中，后台 Elasticsearch 索引迁移到 ES6-native 索引已启用。必须先安装需要 Elasticsearch 7.0 或更高版本的任何威胁 Grid 设备版本，才能成功完成此迁移。
* 命令行配置工具中的配置选项名称拼写错误，现在使用更有意义的错误消息进行处理。
* 可能导致支持修改其配置的集群的问题（而不是严格通过支持的 UI 进程进行安装和配置），从而在已解决升级到 2.7.0 时失败。
* 改进了用于查询状态或手动触发计划后台作业执行的设备。

## 已知问题

Elasticsearch 索引迁移可能会在 NFS 备份过程中导致大量延迟，从而导致与相同的警告相关。应忽略这些警告，因为服务通知表明正在积极地进行索引迁移，并且仅当索引迁移过程无法在扩展期内进行时，才会引发支持。

## 安全更新

* 通过禁用 TCP 选择性确认支持，并丢弃请求最大数据段大小低于 300 字节的数据包，规避 CVE-2019-11477、CVE-2019-11478 和 CVE-2019-11479。
* 通过禁用 Kibana Timelion 支持来规避 CVE-2019-7608。
* Patch bzip2 以纳入 CVE-2019-12900 的修复。

# 版本 2.7

此版本将更新核心威胁网格软件，使其遵循云 3.5.27 版本，移至 Elasticsearch 6.5，并对设备特定工具和基础设施进行多项增强。

## 修复和更新

* 示例删除功能的范围已扩展为包括人为因素、匹配云产品的行为。
* 现在，数据重置过程更加全面;虽然在确定所有客户相关数据的破坏下仍需要擦除过程（恢复加载项菜单），但重置过程现在会清除以前保留的操作系统日志和其他状态。

成功重置设备将在其控制台上显示新的随机生成的密码（与新安装状态中的行为相同）。

请注意，此改进的过程现在会多次重启，并且可以从恢复模式调用（而不是之前的过程，只有在启动正常操作时才能成功调用）。

* TLSv1.0 和 TLSv1.1 在管理接口上禁用，默认情况下为主应用禁用该功能。如果出于集成兼容目的需要其中一种协议，则可以从 tgsh 对话重新启用（仅适用于主应用）。
* Elasticsearch 6.5.4 用于核心威胁 Grid 应用的可搜索数据存储。请注意，需要进行后台迁移，才能在以后仅支持 Elasticsearch 7.x 的任何版本中安装历史索引，而不会丢失数据；请注意未来版本的发行说明。
* 主机名：设备现在使用其序列号作为主机名，以便更好地实现与某些 NFSv4 服务器的互通性。
* 最初使用此版本或更高版本制造的设备将使用 XFS 作为其主文件系统。除非另有说明，否则此更改不会影响已存在的设备。
* 如果设备已重置数据，则其数据存储将更改为 XFS。这提高了向前兼容性，并为每个服务器提供 I/O 使用情况监控的操作系统级别支持。
* WAL-E 不再维护，因此将其替换为 WAL-G 进行 PostgreSQL 备份/恢复。现有的 WAL-E 存档将保持兼容，并且恢复大型备份应会显著减少 PostgreSQL 时间。
* 用于客户支持连接的 IP 地址列表应在已更新支持模式时，DNS 解析不能正确运行，以准确反映在生产中使用的服务器。
* 现在配置 SSH 公共密钥以访问设备，通过 SSH 禁用基于密码的身份验证，使 SSH 身份验证方法成为一个或另一个，但不是两者。（使用基于密钥的身份验证成功建立 SSH 连接后，tgsh 对话框将提示密码，因此需要两个令牌）。
* 恢复模式下的网络配置现在会镜像整个系统：所有接口都已启动;防火墙规则和策略路由，用于限制哪些进程可以在正在运行的接口上进行通信;等。（请注意，端口 19791 上的支持模式流量在所有三个接口上均已列出）。
* 在此版本中，用于显示系统监控图形的工具已更新。通过此迁移不会保留历史系统监控数据。

## 已知问题

在设备上尚不支持网络模拟支持，这与上游 3.5.27 文档相反。

## 其他说明

现在，数据重置过程需要足够的存储，以包含在系统的 SSDs 上全新安装所需的所有内容;只有在此内容的存在和有效性已被确保之后，才会删除任何已存在的数据。很可能是系统（特别是第一代硬件）已用于延长期，可能没有足够的空间可立即获得;如果需要，客户支持部门可以提供帮助。

# 版本 2.6

**发布 2/4/2019**

此版本将更新核心威胁网格软件，使其遵循云 3.5.19 版本，并包含不足的增强功能，以允许今后更短的释放周期。

## 修复和更新

* 配置选项可用于强制严格实施保留期间限制（不会将项目从分析中存储的时间超过 15 天，即使存储可用性允许更长的时间）也是如此。默认情况下，此设置处于禁用状态。
* Microsoft Office 现在包含在可选的日语和韩语虚拟机映像中。
* 在将独立节点迁移为集群的初始节点时，可能会导致配置失败的问题。
* 已解决的问题可能会导致 "tgsh 对话" 命令（运行寻呼机、已修改的服务状态或调整本地时区）发生故障。
* Elasticsearch 可以在一个循环中结束的场景（由于在启动时允许不一致索引被修复/恢复的监视程序超时不足），已得到解决。

# 版本 2.5

**发布 9/14/2018**

此版本将更新核心威胁网格软件，使其遵循云 3.5 系列。

这是第一个设备版本，包括对 Windows 10 的支持。

安装此更新将修改与此设备集成的 ESA/CSA 设备的帐户名称（因为之前的名称可能会泄漏敏感信息）。在此过程中遇到的任何问题都将在标题 "设备名称迁移" 下进行报告。不需要对您的 ESA 或 CSA 设备进行任何更改。如果有任何问题，请联系客户支持。

## 修复和更新

* 已添加 Windows 10 VM 支持。
* 现在，设备上提供了示例删除支持。（请注意，在安装此版本之前最初上传的样本不能删除存储在设备上其他位置的样本的副本; 但是，这些额外的副本会受到 "磁盘工件" 记录的保留规则的制约。在 \* Threat Grid 设备数据保留说明 \* 中，随着新内容的添加，最终会老化。）
* VM 存储格式已修改，以提高存储和更新效率。
* 用于生成系统监控图的工具已更新;需要更改任何直接 URLs。
* 在已完成配置的设备上，禁用 NFS 现在已更好地受支持。
* 连接的 USB 存储设备无法再生成虚假的智能硬件状态警告。
* 已修改 IP 分段设置，以使用 CVE-2018-5391 规避任何拒绝服务攻击。（请注意，需要从客户网络（而不是沙盒恶意软件）发起这些攻击才能生效。
* 现在，整个系统都是使用最新版本的 gcc 构建的，在内核中启用完整的 retpoline 支持。
* 即使未启用集群，也会自动修正损坏的 redis 存储，从而修复 2.4.0 中引入的回归。

# 版本 2.4.3.3

**发布 6/1/2018**

此版本解决了从头开始创建新集群时数据库初始化过程中的问题（从独立设备创建的备份中初始化的新集群不受影响）;并删除一些未使用的软件库。

## 修复和更新

* 这是一种主动补救措施--已使用空白数据库初始化集群的客户将收到一份包含 "数据库编码未正确设置" 的服务通知，并应与客户支持联系以安排追溯性修复。
* 未准备创建设备集群的客户不需要安装此更新。
* **不再支持来自 2.2 以前版本的数据迁移：**

请注意，由于删除了未使用的代码，因此从未成功运行 ElasticSearch 5 迁移的设备（在 2.1 系列的末尾）不再附带允许客户支持在实际执行此迁移的工具。

同样，PostgreSQL 从未更新到 9.6 的系统（类似地发生在 2.2.0 之前），不再附带允许延迟完成此更新的工具。。

未完成这些迁移的系统不能在任何 2.3 或 2.4 版本下正常工作，并且在运行 2.1.6 时显示服务通知，指导用户在执行前允许迁移完成或联系客户支持任何进一步更新。在应用更新之前，务必确保系统处于通常良好的工作状态，除非提供版本说明或客户支持的特定相反建议。

# 版本 2.4.3.2

**发布 5/19/2018**

此版本包括一个安全更新和两个漏洞修复。

## 修复和更新

* ClamAV 已更新，解决 CVE-2018-1000085。
* 增强更新机制，以允许修复 "win7-x64" 虚拟机可能不可用的情况。  
    
  此条件仅影响之前已更新为 2.4.1 或更高版本的系统。  
    
  更新下载必须在 2.4.3.2 安装后成功完成，然后重新启动，才能应用此修复。
* 软件故障可以阻止在安装 2.4.3 或更高版本后执行至少一次更新检查之前运行样本。现在已更正此情况。

如果从预 2.4.3 版本进行更新，请参阅 2.4.3 和 2.4.3.1 版本说明。

# 版本 2.4.3.1

**发布 5/1/2018**

此外，2.4.3.1 还添加了对数据库架构异常的诊断报告。不作为此部分向更新服务器报告任何客户数据--所有报告仅为元数据（DDL），旨在确保未来升级的可靠性。

# 版本 2.4.3

**发布 4/27/2018**

此功能更新了核心威胁网格软件，将对独立设备的升级添加到集群的初始节点，而无需进行干预重置过程，并添加客户可访问的远程退出机制（替换有限的可用性 “tg-tunnel ”一种在其前面的机制）。在应用此更新之前，使用 tg-tunnel 的客户应仔细阅读这些说明，并与客户支持部门联系，以解决任何问题。

## 修复和更新

* 使用新版本的核心威胁网络软件，对应于云门户版本 3.4.65。

请注意，云和设备软件之间的功能可用性可能有所不同。API 文档的相关部分中注明了 APIs 的差异。门户联机帮助中介绍了 UI 中的差异：帮助 > 威胁网格简介 > 威胁网格云和设备比较。

* 数据备份到 NFS 的独立设备不需要再进行数据库重置和从备份中恢复即可成为新集群的初始节点。
* 提供远程出口支持。如果已激活（对于之前配置为使用 tg-tunnel 的设备，此功能默认为打开），这会将来自恶意软件虚拟机的流量隧道传输到思科数据中心，并从那里发送到退出位置。

请注意，当下载软件更新时，会检索与此服务一起使用的新密钥（即使没有可用的更新）。这意味着必须先进行至少一次更新检查，然后才能使用此服务;具有已过期许可证的设备可能无法检索新密钥，因此可能会失去对此服务的访问权限;而仅通过离线更新机制安装更新的设备可能不会使用此服务。

* 虚拟机的存储方式已更改，以减少部署虚拟机的少量更改时所需的最小可能数据传输量。

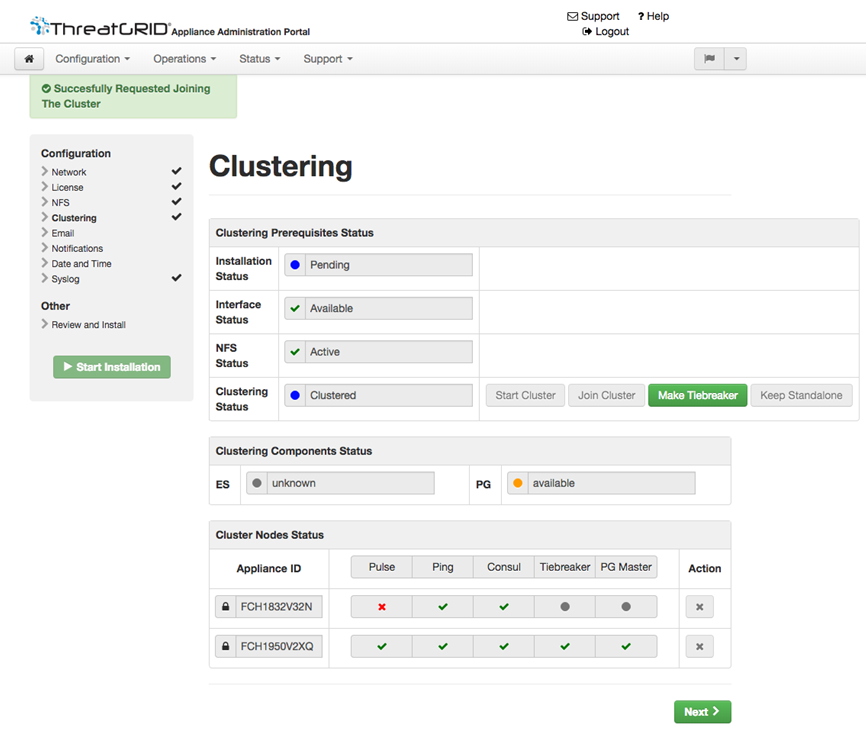
# 版本 2.4.2

**发布 3/2/2018**

这是第一个发行版，设备集群通常作为功能提供。自 2.4.1 以来进行了各种设置和工作流程改进，这是最终版本，集群仍被视为早期的现场试用功能。

## 修复和更新

* 添加了安全功能，以防止通过多个威胁网格设备将单个数据存储安装到具有相同密钥的读/写访问权限，除非这些设备是同一集群的成员。
* 集群不再需要许可证来表示参加早期的现场实验。
* 解决了在扩展正常运行时间后，在集群上进行监控时可能偶尔无法确定 Elasticsearch 集群运行状况的场景。
* 在主动安装时，NFS 设置可能不再更新。当节点不属于集群时，可在 OpAdmin 管理界面中使用 "卸载" 选项。
* 解决了可能导致客户协商失败的问题，这些客户正在通过威胁网格数据中心传输出站流量。
* 新的群集配置页面：



# 版本 2.4.1

**发布 2/19/2018**

此版本更新了核心威胁网格软件，并引入了用于设备集群设置和维护的配置 UI。

此版本还修复了一个漏洞，该漏洞可能允许设备进入不能在重新启动之前运行新的样本分析操作的状态，对集群支持做出大量的稳定性改进，并且在以前仅提供了安全更新中的折叠在 2.4.0.1 临时版本中。

## 修复和更新

* 使用新版本的核心威胁网络软件，对应于云门户版本 3.4.59;值得注意的是，这包括对示例报告的增强。有关详细信息，请参阅门户联机帮助（\* 帮助 > 版本说明 \*）中提供的版本说明。

（请注意，威胁网格云和设备软件之间的功能可用性可能有所不同。有关详细信息，请参阅 文档。在 API 文档的相关部分中注明了不同之处。门户联机帮助中介绍了 UI 中的差异： \* 帮助 > 威胁网格简介> 威胁网格云和设备比较 \*。）

* 如果在一段时间内运行了许多虚拟机，"管理" 组件可能会导致分配大量的冲压盘存储，从而防止在设备重新启动之前进行进一步分析操作。现在已解决此问题。
* 对集群支持进行了许多稳定性改进。
* 集群状态在 OpAdmin UI 中公开。参与集群 EFT 的客户可以从独立节点构建集群;将具有空数据库的新设备添加到现有集群;请参阅集群状态;确定集群是否具有容错能力;删除失效节点;以及（如果可能）控制哪些节点持有的角色在故障切换或过渡事件期间可能会导致服务中断。

## 已知问题

* 集群：如果不正确删除和擦除系统，而不使用 UI 中的 "删除" 选项来通知其他节点删除，则如果重新添加系统，则镜像到该系统的数据库可能会失败。
* NFS/集群安全：
* 安全功能尚未激活，以防止用户尝试共享单个 NFS 数据存储：跨多个非集群设备、集群与一个或多个非集群设备之间或多个不同的集群之间。
* 按照文档或客户支持的明确指导，仅安装与预先存在的备用存储相关联的加密密钥。
* NFS：管理（OpAdmin） UI 当前不禁止在配置激活后对 NFS 配置进行更改。进行此类更改是不受支持的操作，特别是当节点是集群的成员时，采取此操作会将未指定的后果提高到并包括数据丢失。

## 安全更新

在临时版本 2.4.0.1 中引入的安全修复程序将通过并包含在此常规版本中。

# 版本 2.4.0.1

**发布 1/30/2018**

此临时版本会将 ClamAV 更新为 0.99.3。强烈建议您立即安装此更新。

## 修复和更新

* 解决病毒定义无法更新的文件描述符泄漏。

## 安全更新

解决以下威胁：

* CVE-2017-12374
* CVE-2017-12375
* CVE-2017-12376
* CVE-2017-12377
* CVE-2017-12378
* CVE-2017-12379
* CVE-2017-12380

# 2.4 版

**发布 12/14/2017**

此版本更新了核心威胁网格软件;添加了对可选虚拟机（包括包含单独许可的第三方软件）的支持，这些虚拟机可作为更新下载;并为参与早期现场实验的客户引入了有限的可用性集群支持作为预发布功能。

## 修复和更新

* 使用新版本的核心威胁网络软件，对应于云门户版本 3.4.57。（云和设备软件之间的功能可用性可能不同; 请参阅文档）。
* 虚拟机分布使用一种新的带宽更高的机制，可避免多次下载多个虚拟机之间共享的内容，并允许将不同的虚拟机分发给不同的客户。请注意：在为支持 2.4.0 更新而专门生成的 2.3. x 版本中也存在此机制。
* 新的虚拟机 "win7-x64-2" 可供所有客户使用。
* 新的虚拟机 "win7-x64-kr" 可供客户自行下载，其许可证表示购买许可证以在其威胁网格设备上运行 Hancom Office。其他可选虚拟机（具有特定于区域设置特定兴趣的第三方许可软件）可能在不久的将来可用。
* 集群：引入了对构建多个设备集群的预发布支持。这需要额外的硬件，并且目前仅适用于符合条件的客户，并已选择加入，并进行了提前现场试用。

# 版本 2.3.3

**发布 11/302017**

此版本引入了一个更有效的更新系统。新的更新系统将仅下载在后续虚拟机版本之间更改的组件，并且将避免多次在多个虚拟机之间下载共享软件组件。

**必填：**

**必须**先安装此版本，然后才能下载即将到来的威胁网络设备 2.4.0 版本。

## 修复和更新

* 虚拟机分布使用一种可提高带宽效率的新机制。它避免了多次下载多个虚拟机之间共享的内容，并允许将不同的虚拟机分发给不同的客户。

# 版本 2.3.2

**发布 10/7/2017**

此版本解决运行版本 2.2 或更高版本时的高优先级搜索问题。当搜索评估的数据超过一定数量的日期时，搜索功能和相关 APIs 可能会失败。（请注意，如果日期包含索引数据，即，至少来自一个样本分析的数据，则该日期仅包含在计算中。）

## 修复和更新

* 用于搜索的索引以提高效率和增加（系数为 5）可查询的搜索数据的天数的方式进行迁移。（未来更新将进一步提升此限制。）
* 在网络上检索的许可证在末尾不再有 NUL 字符。（这不会影响此类许可证的有效性或可用性。）
* 引入了各种更新，以支持即将到来的未发布功能。

# 版本 2.3.1

**发布 8/28/2017**

此版本解决了 2.3.0 版以前版本影响设备在先前版本中更新的一些问题。

## 修复和更新

* 可以防止在 2.1.4 或更早版本中添加的数据出现在某些搜索结果中的问题。
* 这种问题可能会阻止最初安装了软件版本 1.2. x 的设备，并直接升级到 1.4. x 才能成功应用 2.3.0 版以前更新。
* "组织管理" 页面再次正确显示每个组织的速率限制配置，而不是显示仅适用于云产品的组织级许可配置。

# 版本 2.3

**发布 8/11/2017**

此版本更新了核心威胁网格软件;删除云产品不再主动测试和支持的虚拟机;移动到性能更高的网络实施，以使客户不会对恶意软件流量进行隧道传输;实施 SMTP 流量的蜜罐;并阻止来自恶意软件的出站 SSH （以这种方式匹配云服务的行为）。它还引入了自动许可证检索：如果设备连接到Internet，它可以尝试通过网络检索许可证（或替换过期的许可证）。请注意，自动检索功能目前仅适用于本软件（2017-08-11）发布后出售或续约的许可证。

尽管使用 IPv4LL （169.254.0.0/16）地址范围从未经过测试和支持，但它们现在是 \* 明确不受支持 \*，不得使用。

## 修复和更新

* 使用新版本的核心威胁网络软件，对应于云门户版本 3.4.47。（云和设备软件之间的功能可用性可能不同; 有关详细信息，请参阅位于 UI 帮助中的门户版本说明。）
* 只有在云产品中进行积极测试和维护的虚拟机才会出现： Windows XP 被删除，甚至来自之前将的设备。Windows 7 现在仅 64 位。
* 提交到“winxp”或“win7-x86”虚拟机的样本仍然可用。请注意，应相应更改对“winxp”进行硬编码的任何脚本或客户端。
* 除非使用隧道，否则来自恶意软件的出站网络流量使用更高性能机制来从虚拟机传出。这允许将未加密的出站 SMTP 作为本地设备的本地沙盒。
* 现已阻止来自沙盒虚拟机的出站 SSH。
* 由于时间服务器的 DNS 查找失败而导致 NTP 同步失败的情况：如果 NTP 服务没有对等体，则它将定期重新启动。

# 版本 2.2.4

**发布 7/10/2017**

该版本引入了备份功能。

现在，Threat Grid 设备可支持如下操作：向支持 NFS 的存储保存加密备份；从支持 NFS 的存储执行数据初始化；重置为空数据库状态（可加载此类备份）。

（请注意，重置与擦除不同。当设备需要离开客户现场时，可使用擦除来避免信息泄漏。适用于此目的的擦除流程存在于恢复引导加载程序中，但不适用于在恢复备份之前准备系统。要为恢复备份做准备，请使用重置。）

我们提供了其他文档来专门介绍备份功能，请务必在使用备份功能之前仔细参考。有关技术信息和说明，请参阅[备份说明和常见问题解答](http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/backup-faq-2-2-4.pdf)。

## 修复和更新

* 现在支持客户提供的 NFSv4 商店进行备份和恢复。
* 有限的数据重置操作现在可用于准备系统以恢复备份。（重置操作适用于数据库内容，但与恢复模式下可用的安全擦除选项不同，不会使设备永久不可用。）
* 修复了 2.2.2 中引入的回归，这可能会在 DHCP 正在使用，或者网络接口在启动后被热插拔或重新配置时阻止网络流量路由到本地网络（网关除外）。

# 版本 2.2.3

发布 5/19/2017

应 Microsoft 的要求，于 2017 年 7 月 1 日之后（包括 2017 年 7 月 1 日）生产的 Threat Grid 设备将不再包括 Windows XP 许可或发行版。此次要版本更新提供了不需要 Windows XP 即可运行的新出厂设置。

安装此版本不会从以前可用的设备中删除 Windows XP。

这还修复了当 Clean 接口未配置相关联的 DNS 服务器时，可能导致在 OpAdmin 中将更新检查成功报告为失败的一些问题。请注意，如果显示 "运行更新" 按钮，则可以安全地尝试更新，\* 即使存在 \* "更新检查错误" 通知也是如此。

## 重要注意事项

如果从 2.2 版本升级，请阅读设备 2.2 版本说明：

http://www.cisco.com/c/dam/en/us/td/docs/security/amp\_threatgrid/amp-threat-grid-appliance-release-notes-v2-2

## 修复和更新

* 当所创建的可执行文件列入白名单时，无法再触发 "文档已创建可执行文件" 指示器。
* 在未配置干净网络 DNS 服务器时，监控和日志记录服务（kiries 和 syslog-ng）现在能够正常启动。
* 现在，即使无法发送有关该检查的通知，成功的更新检查也会在 OpAdmin 中正确报告。
* 根据 Microsoft 许可要求，此版本的威胁网络设备能够在不是 Windows XP 的情况下进行安装。

## 安全更新

OpenSSL 被提升到 1.0.2k。

# 版本 2.2.2

发布 5/8/2017

此次要版本对网络配置和操作系统组件进行更改，以支持将在即将发布的版本中添加的功能。它修复了支持模式下的漏洞，在连接未成功进行 TLS 握手（直到重新启动服务）后，可能会导致所有未来连接都支持服务器失败，并且可能会阻止下载新的防病毒签名的漏洞已经.

### 重要注意事项

如果从预 2.2 版本进行升级，请阅读设备 2.2 版本说明（http://www.cisco.com/c/dam/en/us/td/docs/security/amp\_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf）。

### 漏洞修复

* 在中断的 TLS 握手后，支持模式不再呈现为不可操作。
* 修复了一个问题，可能会阻止下载新的防病毒签名。
* 孤立的进气队列元素现在会自动清除。

### 增强功能

如果通过 DHCP 在 Clean 接口上提供 DNS 服务器，并且通过 OpAdmin 为该接口配置了 DNS 服务器，则两者都将使用。

# 版本 2.2.1

发布 3/24/2017

### 重要注意事项

请注意，如果 ElasticSearch 迁移在版本 2.1.5 中引入且仍可用且在 2.1.6 中运行不完整，则不得安装 2.2. x。如果有任何问题，请联系客户支持。

[support@threatgrid.com](mailto:support@threatgrid.com)

此次要版本修复了在一段时间内可能会变得很严重的 2.2 中的性能问题。它部分降低了安装 2.2 的影响，而无需允许 2.1.5 和 2.1.6 中的 ElasticSearch 迁移完全完成。此版本还消除了对 SSLv3 的不赞成支持;并确保基于 JVM 的服务能够成功地从内存不足情况中恢复。

如果从 2.2 版本升级，请阅读位于以下位置的设备 2.2 版本说明：

http://www.cisco.com/c/dam/en/us/td/docs/security/amp\_threatgrid/amp-threat-grid-appliance-release-notes-v2-2.pdf

### 新功能

设备现在可以从安装 2.2 系列版本的 ES5 中恢复，而无需允许 2.1.5 和 2.1.6 中的迁移完全完成。

请注意，这是部分缓解。

虽然在版本 2.1.5 和 2.1.6 中，此迁移过程对完整性和可用性没有影响，但在 2.2. x 中，在迁移该索引时添加到索引中的新内容可能会在该索引的迁移过程完成时**丢失**。因此，我们**强烈**建议在 2.1.5 或 2.1.6 中的 ElasticSearch 迁移完成**后**，才安装 2.2. x。

### 漏洞修复

分析流程处理特定类型的网络事件不再占用大量的时间和内存，或使分析服务崩溃。

### 安全修复

SSLv3 不再需要，并且此过时的协议现在已禁用。

# 版本 2.2 制造业

发布 3/8/2017

仅在制造上有所更改。对客户无影响。未通过更新服务器进行部署。

# 版本 2.2

发布日期：2017 年 3 月 3 日

## 要求

**必须先在 2.1.5/2.1.6 中完成** ElasticSearch 迁移，然后才能安装 2.2。

## 文档

**强烈**建议您阅读《AMP 威胁网格设备迁移说明》和《数据保留说明》。

* 《AMP Threat Grid 设备迁移说明 v2.2》：

http://www.cisco.com/c/dam/en/us/td/docs/security/amp\_threatgrid/amp-threat-grid-appliance-migration-note-v2-2.pdf

* 《AMP Threat Grid 设备数据保留说明》：

http://www.cisco.com/c/dam/en/us/td/docs/security/amp\_threatgrid/amp-threat-grid-appliance-data-retention-v2-2.pdf

## 关于本版本

版本 2.2 会显著提高存储效率，使初始安装有版本 1.x 的系统上之前不可用的磁盘容量可用。

重要提示：

将来可以用这项最新功能对旧内容进行修剪（删除。尽管所有内容都会迁移，但可以不断删除比较旧的内容（特别是大量生成却极少使用的分区磁盘和网络工件）以确保持续运营。有关详细信息，请参阅上面链接的《*数据保留说明*》。

本版本的 Threat Grid 设备与 Threat Grid 云 3.4.37 版属于同等版本。（请注意，这并不意味着 \*功能\* 完全相等：如果功能所需的硬件、服务、第三方许可证或者其他内容或设施仅在云中可用，则相应功能在设备上仍然不可用）。

这也就是说，现在可以为设备配置几项以前只能在云中部署的第三方检测和丰富服务集成，其中包括 VirusTotal、OpenDNS 和 TitaniumCloud。不仅如此，设备还可以每天自动下载 ClamAV 签名的更新，从而提高对已知恶意软件的识别能力。

## 新功能

附带的应用版本具有许多新功能，其中包括：

* 支持为处置更新服务通知配置多个 URL。
* 以传统存档格式存储的内容已迁移为可提高解压效率并按数据类型加以区别存储的内容。
* 现在可以在设备上配置 VirusTotal、OpenDNS 和 TitaniumCloud 集成了。
* 可以每天自动更新 ClamAV 签名。此功能默认启用，并可通过 OpAdmin 中新添加的“集成”页面禁用。
* 样本调用失败可以自动重试，从而降低有效整体失败率。
* 应用前端可将所有时间戳转换为正用来查看信息的浏览器的本地时区。因此，应用本身的非 UTC 时区将不再那么有用，并且也不再那么被人需要。
* *Mask* UI - Threat Grid 门户 3.4.37 版在 2.2 版本的设备上首次提供增强的 UI 功能。

注意：*Mask* 取代了旧版的 *Face* 界面，但用户仍可选择在两个界面间来回切换。*Mask* 提供了许多增强功能，包括完全重新设计的分析报告。有关详细信息，请参阅该应用在线帮助页面上提供的《门户版本说明》。（在页面顶部的门户 UI 导航栏中，点击**帮助**按钮打开帮助主页。）

## 漏洞修复

* 起初安装了 1.x 版本的设备上因使用 MBR 分区表而不可访问的磁盘空间现在已分配和可访问。
* 现在，即使主要引导加载程序损坏或不可用，从 1.x 版本升级的系统也可调用恢复引导加载程序。

## 安全修复

* 已更新底层虚拟化技术以解决 VGA 驱动程序中潜在的缓冲区溢出问题。

# 2.1.6 版

发布日期：2017 年 1 月 5 日

版本 2.1.6 在 Threat Grid 设备的管理员界面中增加了 LDAP 身份验证和授权，还包括各种与未发布或即将发布功能相关的架构改进。

## 新功能

OpAdmin 和 TGSH 对话界面均可配置 LDAP 身份验证。请注意，此功能不会延伸到应用界面。

## 已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 2.1.5 版

发布日期：2016 年 11 月 21 日

本版本显著改善了 CSA API 查询性能，从而提高了与思科 ESA 和 WSA 设备集成的可靠性和速度。本版本还升级了各种后端组件，以增强可靠性并适应未来的发展。

**重要提示：**请注意，CSA API 性能只有在完成迁移过程（本版本安装完毕后于后台运行）后才会获得改进；有关详细信息，请阅读本版本附带的技术说明，可从以下链接获取：

http://www.cisco.com/c/dam/en/us/td/docs/security/amp\_threatgrid/amp-threat-grid-appliance-migration-note-v2-1-5.pdf。）

## 新功能

核心应用经过修改，支持版本高于 1.x 的 ElasticSearch。

除以前的 1.7.x 版本以外，还支持 ElasticSearch 版本 2.x 和 5.x（必须迁移到 2.0 后方可使用 5.0）。

PostgreSQL 已升级到版本 9.6.1。

瞬态故障后自动恢复的功能已延伸到更广泛的内部服务。

## 漏洞修复

对于在 clean 网络中通过 DHCP 成功检索地址时的延迟，现在可防止其在升级时阻止服务成功启动或重新配置。

放宽 ElasticSearch 超时，即使在升级到本地 5.0 前也能减少失败次数。

主要版本数据库升级现在比较不容易被错误标记为失败并回滚。

在 ElasticSearch 完成初始化之前，依赖 ElasticSearch 的应用组件无法再启动。

## 已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 2.1.4 版

发布日期：2016 年 9 月 5 日

本版本解决了许多与硬件支持相关的问题，特别是为气隙式部署设备的软件更新提供支持时作为必备条件的那些问题。

## 新功能

监控和报告功能现在可用于 ElasticSearch 服务负载过大的场景。

## 漏洞修复

对失败服务自动重启的支持延伸到（在延迟后）失败频率足以将其暂时禁用的服务。

某些内部服务可能因 Redis 初始化延迟而无法启动的场景已得到解决。

存储设备名称或 ID 更改不会再阻止系统成功启动。

TG-5004-K9 和 TG-5504-K9 硬件现在完全支持系统擦除。

## 已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 2.1.3 版

发布日期：2016 年 8 月 11 日

本版本解决了许多与硬件支持相关的问题，特别是为气隙式部署设备的软件更新提供支持时作为必备条件的那些问题。

## 新功能

监控和报告功能现在可用于 ElasticSearch 服务负载过大的场景。

## 漏洞修复

* 对失败服务自动重启的支持延伸到（在延迟后）失败频率足以将其暂时禁用的服务。
* 某些内部服务可能因 Redis 初始化延迟而无法启动的场景已得到解决。
* 存储设备名称或 ID 更改不会再阻止系统成功启动。
* TG-5004-K9 和 TG-5504-K9 硬件现在完全支持系统擦除。

## 已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 2.1.2 版

发布日期：2016 年 7 月 15 日

本版本是漏洞修复次要版本。

## 漏洞修复

* 不正常关机不会再使系统处于 Redis 键/值存储阻止服务启动的状态。
* 已解决与 tg-tunnel 的 qemu 连接（对于使用此默认关闭功能的客户）的回归问题。
* 将系统修改为不再使用 tg-tunnel 现在是自动完成的过程。

## 已知问题

* 已知在采用某些特定 BIOS 版本的 TG-5004-K9 和 TG-5504-K9 硬件上，擦除支持会出现故障。预计在此硬件发布之前解决此问题。
* 磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 2.1.1 版

发布日期：2016 年 7 月 6 日

本版本解决了单独的 clean-network DNS 支持方面的一些问题，修复了一个重要的安全漏洞，并提供了各种次要修复和改进。

## 新功能

* 用户可以通过修改有关潜在硬盘驱动器故障的 SMART 警告的可视性设置来解除这些警告，这将阻止就同一个错误发出任何进一步通知，除非错误的性质或状态有所更改。

## 漏洞修复

* 单独的 clean-network DNS 现在可以正常运行。
* 避免了重新配置后备份期间的假警告。

## 安全修复

* 已修复 CVE-2016-1443 漏洞。
* SSH 在恢复模式下不再默认启用。

## 已知问题

* 已知在采用某些特定 BIOS 版本的 TG-5004-K9 和 TG-5504-K9 硬件上，擦除支持会出现故障。预计在此硬件发布之前解决此问题。
* 磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 版本 2.1

发布日期：2016 年 6 月 21 日

**重要提示：**此更新的最低版本是 v2.0.4。您必须先升级到版本 2.0.4，然后才能升级到版本 2.1。

本版本完全支持即将发布的硬件版本，整合了许多安全增强功能，并升级到 Threat Grid 门户产品的同期版本。

## 新功能

* 现在可将文件类型 js、dot、dotx 和 dotm 作为恶意文件通过处置更新服务提交到 FireAMP 私有云。
* 在所有硬件上，运行时禁用模块加载和 kexec 以减少基于内核的 Rootkit 的风险，并在调用操作系统内核和 initrd 签名前由引导加载程序对其进行验证。
* 可以隐藏与硬盘驱动器 SMART 警告相关的服务通知，使其只能在内容更改的情况下自动重新打开。
* 可以检测过长时间保持打开的数据库事务并将其作为服务通知予以报告，从而有助于在这种情况恶化到需要延长停机时间进行修复之前加以补救。

## 漏洞修复

* Glovebox 的可靠性显著提高。
* 在网络接口需要更长时间才能准备就绪的情况下，恢复模式下的网络可靠性得到提高。
* 来自 IPMI 的硬件错误相关服务通知可能会将已有警告数误报为 0。
* NTP 失败不会再导致在系统配置完成前发出服务通知。
* 启动后至少 10 分钟内无法记录因预期服务处于非活动状态而导致的失败，留出时间供各项服务正确完成初始化。

## 安全修复

* 已更新底层虚拟化技术以解决 VGA 驱动程序中潜在的缓冲区溢出问题。

## 已知问题

* 已知在采用某些特定 BIOS 版本的 TG-5004-K9 和 TG-5504-K9 硬件上，擦除支持会出现故障。预计在此硬件发布之前解决此问题。
* 磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 2.0.4 版

发布日期：2016 年 5 月 1 日

**重要提示：**此更新的最低版本是 v1.4.6。您必须先升级到版本 1.4.6 或更高版本，然后才能完成 2.0.4 更新。

本版本包括许多可靠性改进和漏洞修复。

请注意，启动时间可能会减慢，特别是对具有大量数据的设备而言；但是，这种启动时间的延长解决了几个可能会在启动后不久发生的故障。

## 新功能

* 为邮件警报建立的 SMTP 连接现在可以充分利用本地配置的证书颁发机构。
* 处置更新服务集成得到改进，并与 FireAMP 私有云版本 2.2.0 完全兼容。

## 漏洞修复

* 设备现在可更新处置索引，使其符合预期状态。这样即可修复几个可能由索引状态不一致或过时而导致的客户影响漏洞。
* 设备要等待 ElasticSearch 集群完全可用后才能启动相关服务。
* 增加了为 ElasticSearch 分配的内存量，也因此增加了 ElasticSearch 中可在不出错的情况下编入索引的最大可能数据量。
* 临时启动加载程序配置覆盖（例如从 1.x 升级到 2.x 期间实施的配置覆盖）已清除。因此，已解决可能导致以前从 1.x 版本升级的设备在使用恢复模式时显示升级模式菜单的情况。
* 已解决一个可能导致邮件警报失败的漏洞。

# 2.0.3 版

发布日期：2016 年 3 月 15 日

此版本引入一系列功能以支持 FireAMP 私有云设备集成。这些功能包括在 Clean 和 Dirty 接口之间拆分 DNS 的功能、CA 管理和 FireAMP 集成配置。

现在，生成的 SSL 证书令 CN 复制为 subjectAltName。这解决了与 SSL 客户端的不兼容性问题，即当存在至少一个 subjectAltName 时 SSL 客户端会忽略 CN 字段。如果使用此类工具，则可能需要重新生成之前由设备生成的任何证书。

# 2.0.2 版

**发布日期：2016 年 2 月 18 日**

本漏洞修复专用版本解决了一个紧急安全问题。

## 安全更新

已修复 GNU C 库以修复 CVE-2015-7547 和 CVE-2015-1781 漏洞。

# 2.0.1 版

**发布日期：2016 年 2 月 12 日**

本漏洞修复专用版本更正了版本 2.0 中存在的一些问题。

## 漏洞修复

检查设备配额的调用不再根据该配额进行计数。

已解决一个可能偶尔导致设备在启动时挂起的问题。

## 已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

# 版本 2.0

**发布日期：2016 年 2 月 11 日**

**重要提示：**从本版本起，强制更新为 2.0.1。

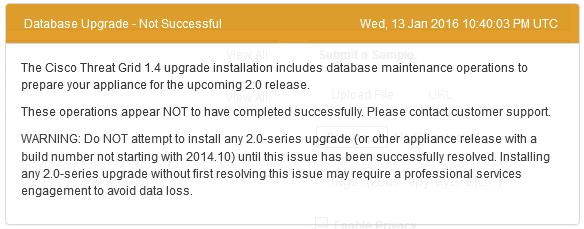
这是主要版本，基于更新的操作系统。它包括支持未来硬件版本的改进，并同 Threat Grid 云门户产品一样能够使用相同的软件。

请注意，由于 ElasticSearch 数据库容量较大，所以 2.0 版升级可能需要一些时间（最长可达数小时）。

首先，完成 1.4.6 升级，它是升级到 2.0 之前的中间步骤。

**请勿中断升级过程**，否则可能需要支持补救。如需查看正在进行的升级的状态，最佳办法是通过控制台访问。

在 1.4.6 升级完成之后、在继续进行 2.0 升级之前，请检查 Threat Grid 门户中的通知以验证是否出现了以下错误：



数据库升级失败通知

*“数据库升级 - 失败*”消息意味着新设备运行的是低于预期的 PostgreSQL 版本，并且自动数据库迁移过程已失败。

如果您没有看到错误通知，则可以继续执行 2.0 升级。

2.0 升级所需的时间

请注意，由于 ElasticSearch 数据库容量较大，所以 2.0 版升级可能需要一些时间（最长可达数小时）。

请勿中断升级过程，否则可能需要支持补救。如需查看正在进行的升级的状态，最佳办法是通过控制台访问。

另外，还包括以下 Threat Grid 设备特定的更新：

## 新功能

* 现在已支持 Windows 7 64 位虚拟机。
* 现在，系统会自动轮换并删除客户支持发起的跟踪，从而延长运行时间，而不会有耗尽可用空间的风险。
* 内部配置备份更加全面彻底，即使两个 SSD 同时发生故障，仍可使设备恢复运行，而不会造成主要数据丢失。

## 漏洞修复

* 即使邮件服务器使用空方法列表通告身份验证（尤其是 Microsoft Exchange），未经身份验证的 SMTP 也能正确工作。
* 现在，夜间更新下载期间相关故障的服务通知也可正确发送。

## 安全修复

* 有关帐户创建或 CSA 设备（即 ESA/WSA 等）注册的应用级别通知会发送到为通知提示所配置的第一个邮件地址。如果未配置任何地址，则不会发送通知。（以往的版本会将这些通知发送到 admin@test，这可能会导致数据泄露。）
* OpenSSL 已更新到版本 1.0.2f。

## 已知问题

磁盘 I/O 吞吐量图仅包含对操作系统专用文件系统（而非客户拥有的数据）的读写操作。通常，这意味着不会显示任何 I/O，因为系统可在启动完成后最大限度地减少与根文件系统之间的交互。

未来版本可能会修改决定 I/O 使用的方法以规避此问题。

# 1.4.6 版

发布日期：2016 年 1 月 27 日

版本 1.4.6 会安装升级到版本 2.0 过程中使用的工具。

## 新功能

版本 1.4.6 的设备可以升级到版本 2.0。

# 1.4.5 版

2015 年 11 月 25 日

现在，擦除设备功能可以在版本 1.4.4 随附的演示设备上使用。有关详细信息，请参阅《[Threat Grid 设备管理员指南](http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/threat-grid-appliance-admin-guide.pdf)》中的“擦除设备”一节。

# 1.4.4 版

本版本修复了一个影响许可证验证的严重问题，并解决了一个阻止向用户显示夜间更新检查期间所发生错误的漏洞。

重要信息：如果从 1.4 之前的版本进行升级，请确保阅读下文版本 1.4 的版本说明。

## 漏洞修复

- 许可证验证不再试图重建内部只读数据库（这可能会导致许可证因无效而被错误拒绝）。

- 现在，夜间更新检查期间发生的错误可以正确地向用户显示。

# 1.4.3 版

本版本包括对底层虚拟化基础设施的少量安全更新，并添加一个用户可访问的机制以擦除设备的磁盘（以供卸载或将租借的硬件返回到 Cisco Demo Loan Program）。

## 新功能

- **擦除：**新的启动菜单选项将允许您擦除 Threat Grid 设备的磁盘。请注意，在执行此操作后，设备将不再运行，无需返回思科进行重新镜像。

## 安全更新

- 潜在的拒绝服务无法再使用专门设计的以太网数据包使正在运行的样本挂起。

## 已知问题

- 在极少数情况下，已知 Windows XP 上的 VM 分析会发生故障。当出现这种情况时，样本分析的屏幕会显示为黑屏。此故障与单个样本无关；如果发生这种情况，建议重新提交样本（或转用 Windows 7）。

# 1.4.2 版

本版本更新了产品中使用的底层虚拟化技术，并附带若干较小但重要的漏洞修复。

重要信息：如果从 1.4 之前的版本进行升级，请确保阅读下文版本 1.4 的版本说明。

## 漏洞修复

- Flash (SWF) 文档现在可以正确激活。

- 与“Glovebox”工具中运行的实时样本分析进行交互的支持现在已与 Firefox 40 中的新安全默认值兼容。

- 通过“重新生成”(Regenerate) 按钮生成的 SSL 证书可为某些软件和工具接受，但之前会被拒绝。

- Windows 7 虚拟机在执行期间不再会挂起。

## 已知问题

- 在极少数情况下，已知 Windows XP 上的 VM 分析会发生故障。当出现这种情况时，样本分析的屏幕会显示为黑屏。此故障与单个样本无关；如果发生这种情况，建议重新提交样本（或转用 Windows 7）。

# 1.4.1 版

本版本更新了产品中包含的 Windows 7 镜像，不再显示 Microsoft Office 激活对话框。

## 从 1.4 之前的版本升级

**重要提示：**如果从 1.4 之前的版本进行升级，请确保阅读下文版本 1.4 的版本说明。

## 漏洞修复

- 在使用 Windows 7 分析 Microsoft Office 文档时，不再显示 Microsoft Office 激活对话框。

- 使用客户支持工具分析引导过程中的系统行为不再导致出现服务通知（当这些工具不再活动时）。

# 版本 1.4

本版本集中解决了预备升级到即将发布的 2.0 版本所需的存储格式更改问题。

重要信息：

对于 1.0 系列软件同捆的具有大量数据库内容的设备，可能需要比平时更长的时间来应用此次升级。

对于与版本 1.2 之前的（已使用数月的）软件同捆的设备，我们建议您允许应用本次升级的时间为 90 分钟。

对于从 1.0 以下版本（非思科品牌的）设备转移样本数据的设备，升级过程可能会需要更长时间；如果有任何问题，请联系客户支持。

## 新功能

- 升级所有设备上的数据库存储以使用与标准上游数据库版本兼容的 PostgreSQL 9.4。

- 已向 tgsh-dialog 重新添加“应用”(APPLY) 按钮，并具有新的功能：按照与系统更新后相同的方式自动配置并更新任务。可用来修复更新尝试中止后仍具有不一致状态的系统。

- 已添加一种机制，客户支持通过该机制可选择用于其他思科设备触发作业的默认虚拟机。

## 漏洞修复

- 如果系统写入性能被降级，新虚拟机镜像的更新不再容易出现失败的情况。

- 从控制台调用的更新作业在 Opadmin 中不再易被错误地视为失败。

- 更新过程中不再创建服务通知。

- 已修复生成自某些 Microsoft Office 文档类型的不正确的文件扩展名。

# 版本 1.3

本版本添加了相当数量的设备特定功能，包括：远程系统日志支持、系统级别问题的邮件提示和性能图表的可用性。本版本贴近稍新版本的 ThreatGRID 服务，实现对集成思科 FireSIGHT 管理中心产品的支持。本版本还包含设备特定的漏洞修复。

请注意，如果配置远程系统日志，则请对出站流量使用 clean 接口。有关详细信息，请参阅已更新的 1.3 版管理文档。

## 新功能

- 可以配置通过邮件发送的通知在系统监控事件上触发。

- 已向管理界面的 SSL 配置页面添加按钮以生成新的自签 SSL 证书。

随时间推移的 CPU、I/O 和内存使用量的图表现在在管理界面中可用。

- 操作系统级别的网络接口名称现在会与其用于文档中的逻辑名称（“clean”、“dirty”、“admin”）匹配。

- 支持热插拔网络接口；无需在启动时插入接口以使其稍后可用，而在发生热插拔事件时需要刷新 DHCP 的接口将会如此。（需要 SFP 的接口仍需在启动时安装这些 SFP）。

- 失败的服务会自动重启。

- 失败的服务会在应用中生成服务通知。

- NTP 同步时的失败尝试会在应用中生成服务通知。

- 过多的数据库检查点积压工作会产生用户可见的警告。

- 已为空闲空间事件添加服务通知。

- 已向有关升级可用性的服务通知添加版本说明内容。

## 漏洞修复

- 具有超过 /24 高位的网络掩码不再被过早裁剪。

## 安全更新

- 修复 qemu 已禁止通过 CD-ROM 驱动器执行的漏洞；请参阅 CVE-2015-5154。

- 通过应用调试界面升级本地权限的可能性得到降低。

## 其他说明

- 已更新 EULA 条款。

# 1.2.1 版

这会更新 ThreatGRID 设备基于来自更新版本的云服务的软件。关键功能是支持集成其他思科设备 -- 包括 ESA 和 WSA 设备。

本版本中没有修改任何设备特定代码或基础设施。

## 新功能

- 支持思科沙盒 API

## 安全更新

- 修复 qemu 以禁用软盘控制器模拟，从而避免 CVE-2015-3456

# 版本 1.2

本版本改善与其他思科产品的集成，精简软件更新过程，并添加硬件监控支持。

## 新功能

- 软件更新检查现在会在每天夜间在后台自动发生。

- 当软件更新可用时，Threat Grid 应用内会有通知。

## 已修复的漏洞

- 软件更新在慢速连接上不再超时。

- 关机或重启时正在处理的样本不再丢失或以副本形式插入。应用 1.2 版更新后，样本处理会在达到适当的停止点之前延迟关机。设备重新启动后会继续样本处理。（以往，样本处理可能会导致系统关闭出现更长的延迟，并且会导致样本丢失。）

- 系统启动时不再发生“502 错误的网关”(502 Bad Gateway) 的错误。

- NTP（网络时间协议）同步现在能正确地发生。

- 生成的 SSL 证书序列号现在在所有设备上为唯一。\*\*注意：\*\*本次修复仅影响首次安装 1.2 或更高版本的系统。

- 在处理数量相对较少的样本后导致设备耗尽磁盘空间的存储错误配置已被修复。

- 审计日志现在能正确地显示客户端 IP 地址。

- SSH 密钥配置页面上的文本能正确地反映这是为 threatgrid 用户而非 root 配置密钥。

- 生成的邮件中的密码重置链接现在是正确的了。

## 安全更新

- 管理界面的会话 cookie 在 Threat Grid 设备间不再可移植。

- OpenSSL 经过升级以包含上游修复。

## 其他改进

- 在首次安装 1.2 或更高版本的设备上，PostgreSQL 数据库会使用与上游 PostgreSQL 和相关项目（例如 EnterpriseDB）二进制兼容的存储格式。

## 已知问题

- 在可以运行 Windows 7 作业之前，需要做出以下用户介入行为：

1. 以管理员身份在 clean 接口上登录主 ThreatGRID 应用控制台。2. 点击右上角\*\*欢迎管理员 (Welcome Admin)\*\* 以访问下拉菜单。3. 点击\*\*管理组织 (Manage Orgs)\*\*。4. 点击\*\*初始组织 (Initial Organization)\*\*。5. 在\*\*额外 VMS (Additional VMS)\*\* 字段中，输入 \*\*win7\*\*。6. 点击\*\*更新 (Update)\*\*。

在完成这个之后，当提交样本时，在\*\*高级选项 (Advanced Options)\*\* 下，

用户可以选择 \*\*win7\*\*。

- 许可解析对文本文件格式敏感。许可证必须保存在 UNIX 文本文件中 - 各行由 CR 而非 CRLF 分隔。

# 版本 1.1 在线修正 1

在线修正 1 与 1.1 相同，但同时修复了一个影响慢速连接上更新下载可靠性的漏洞。

# 版本 1.1

本版本向 Threat Grid 设备添加了若干新功能（包括 Window 7 支持），并已修复若干漏洞。

## 新功能

- 已添加 Windows 7 支持。

- 邮件可通过连接在设备 \*\*Clean\*\* 网络上的邮件服务器发送，而不是仅允许使用通过 \*\*Dirty\*\*（即恶意软件）可访问的邮件服务器。

- 支持直接从设备将快照上传给 Threat Grid 支持。

- 支持在将快照提交给 Threat Grid 支持之前对其进行查看。

- 可从字符 (curses) 界面应用更新，而不仅仅通过基于 Web 的管理界面 (\*\*OpAdmin\*\*) 应用更新。

- 可从恢复模式成功修改系统密码。

- 需要重启生效的管理更改变得更少。

- 已对 GUI 配置工作流添加更多客户端的 Javascript 验证。

## 已修复的漏洞

- 已解决各类出站邮件配置问题。

- 管理界面内的通知现在可以正确显示。

- 配置 UI 中长期运行的作业的状态现在以最低延迟传输。

- 已修复某种情况下管理界面拒绝启动的问题。

- 配置 GUI 不能总是准确反映是否需要重启以使配置更改生效。此问题已修复。

- 已从 tgsh-dialog（基于 curses）管理界面删除不支持的菜单项目。

## 安全更新

- 已更新具有已知漏洞的上游程序包（ntpd、bash、openssl）。

- 配置备份不再全局可读。

# 1.0+hotfix2 更新 - 强制更新

1.0+hotfix2 是**强制更新**，用于修复更新系统本身，使其无需拆分大文件即可进行处理。