More security,
More freedom

AhnLab MDS

用户操作手册

产品版本：2.1.16

文档版本：2021.02.09

AhnLab

前言

文档版本：2021.02.09 / 产品版本：2.1.16

免责条款

制造商、进口商及代理商对偶发性损伤或因对产品的不适当使用和操作所造成的其他损伤不负任何责任。

此文档的内容是以当前产品为基准编写的。AhnLab 将继续增加和加强新的功能，并在未来继续应用新的技术。产品的所有功能可能会被更改，而不另行通知产品购买者或产品购买企业，因此与此文档的内容会有所偏差。

标记规则

说明文档使用的主要标记规则用于理解此手册。

标记规则	描述
< >	表示窗口名称。
粗体	按键名称、菜单或窗口的字段和弹出信息。（例如：**确定**）
参考	使用该程序时的参考事项。
注意	使用该程序时的注意事项。

缩略语

说明文档使用的业务术语和缩略语的含义，用于理解此手册。

缩略语	描述
MDS	AhnLab MDS，在本文当中以 MDS 表示。
MDS Manager	AhnLab MDS Manager，它是 MDS 设备的中央管理软件。
Agent	AhnLab MDS Agent， 可以执行恶意软件检测、删除和恢复命令，在本文档以 Agent 表示。

技术支持

AhnLab 通过技术支持中心和公司网站，对正式用户在使用产品时遇到的疑难点、产品使用方法和程序错误等问题进行解答。如果在使用产品时遇到问题，请联系我们的技术支持中心。

AhnLab China

- 主页：https://cn.ahnlab.com
- 企业客户热线：+86-10-8260-0932/8(北京) | +86-21-6095-6780(上海)
- 1:1 邮件咨询：cn.sales@ahnlab.com
- 地址：北京市朝阳区望京阜通东大街 1 号望京 SOHO 塔 2 B 座 220502 室 | 上海市闵行区万源路 2158 号 弘毅大厦 1201 室

AhnLab, Inc.(韩国总部)

- 主页：https://global.ahnlab.com
- 1:1 邮件咨询：global.sales@ahnlab.com
- 地址：韩国京畿道城南市盆唐区板桥驿路 220（220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea）

法律声明

商业广播通信设备认证标志

本产品适用于商业用途（A 类）电磁波，可用于除居民区以外的所有区域。

- 设备的名称和型号：所有型号
- 认证公司：AhnLab co., Ltd.
- 产品上市年份：2011 年
- 制造商/制造国家/地区：AhnLab co., Ltd./韩国

有限保修

从产品购买之日起，我们为产品提供 1 年有限保修。自销售之日起一年后，需要签订一份单独的维护合同。有关维护合同，请参阅**公司主页 > 客户支持**。

开放源码

可在本产品的 Web 管理界面的**帮助 >开源许可证信息**中找到与本产品中使用的开源相关的信息。

Hwp 文档文件格式版权

本产品是通过 Hancom 的 Hwp 文档文件（.hwp）公开文件而开发的。

目录

第1章　产品介绍

1.1　产品介绍

MDS 是针对日益增加的 APT（高级持续性威胁）攻击的安全解决方案。通过“收集-检测/分析-监控-响应”的流程，有效应对新型恶意软件（包括勒索软件）和 Exploit 等安全威胁。

主要特征

MDS 通过静态（static）和动态（dynamic）恶意软件分析技术及多年经验相结合的混合分析技术，可以准确检测到未知的新型恶意软件。MDS 还应用了其独特的“基于内存的分析的 Exploit 检测”技术，与恶意行为类型或恶意行为发生与否无关，不仅可以准确检测到零日漏洞攻击，还可以分析绕过沙箱分析的恶意软件。

主要功能

AhnLab MDS （威胁分析和检测） 	- 收集和分析主要互联网服务协议（HTTP、SMTP、SMB/CIFS 和 FTP 等） - 对文件流入与流出的双向流量监控 - 电子邮件正文和附件的威胁检测和隔离（应用 MTA 许可证） - 通过特征码、机器学习的静态分析和基于沙箱的动态分析检测新的威胁 - 配备检测非可执行型（non-PE）文件（如 MDS Office 和 Hangul）的专用引擎 - 对 VM 分析过程和 C&C 检测历史记录的基于 PCAP 的数据包捕获和 PCAP 文件下载 - 检测并阻止通过受感染计算机访问有害网站和 C&C 通信 - 通过 MDS Manager 共享行为分析结果和基于云的行为分析信息
AhnLab MDS Manager （综合监控与日志管理） 	【Data Viewer】 - 通过仪表板提供安全状态及主要事件信息 - 实时查看恶意软件入侵现状及是否发生异常流量 - 事件类型、IP 地址、行为历史记录（文件/进程/注册表/网络）的详细日志 - 提 MDS 检测事件和日志的集成管理部署在多个途径中，例如网络区间、电子邮件区间和共享文件夹 - 共享 MDS 设备的行为分析结果（配置多个 MDS 设备时，最小化重复分析和检测） - YARA 规则管理及联动功能 - 通过人事数据库和 AD(Active Directory)的连接，提供检测和响应主机信息 - 转发系统日志(Syslog)功能(CEF, LEEF 格式) - 自动或手动数据库备份功能 - 提供各种类型的报告 【MDS Agent 集成管理】 - MDS Agent 组和策略管理 - MDS Agent 安装和补丁管理 - MDS Agent 响应命令和发送通知功能

AhnLab MDS Agent (收集和响应端点的可疑文件)	- 应用专有机器学习技术的端点可疑文件收集功能 - 针对感染恶意代码的可疑主机进行网络隔离等措施 - 检测异常进程的运行并保留可疑文件的运行 - 对误删文件的恢复功能 - 通过 V3 统一 Agent 修复端点区域的恶意代码并加强防御系统

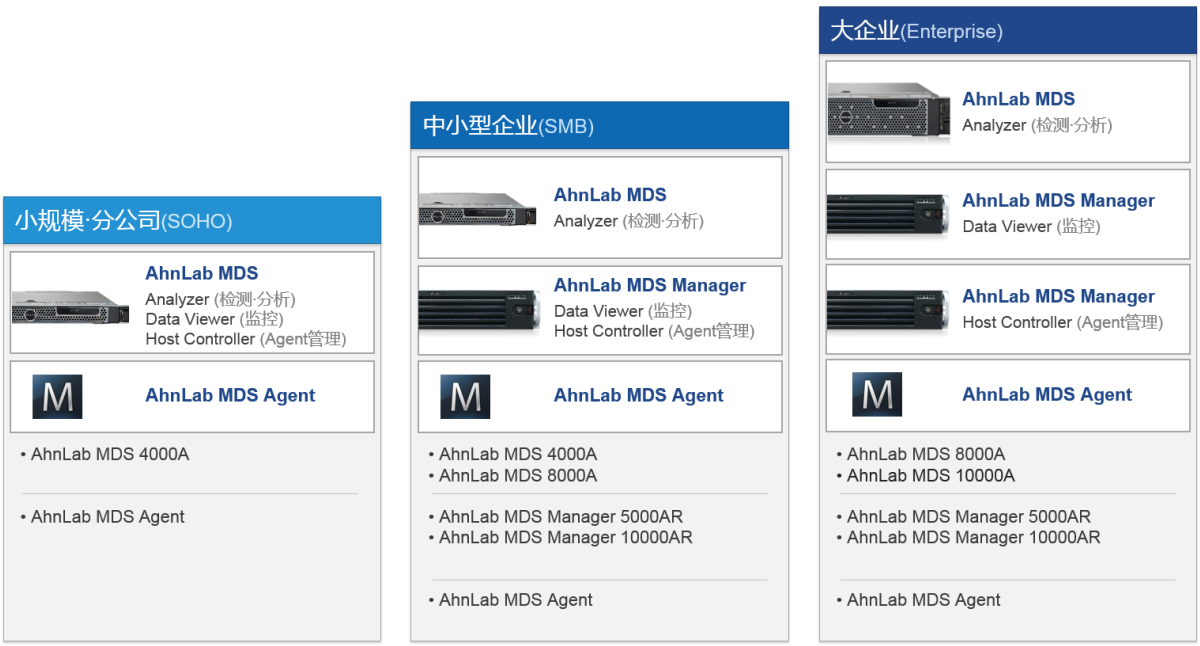
参考

MDS（应用 MTA 许可证：电子邮件保护）的一些组件和功能与 MDS（Web 保护）不同。

1.2 产品构建方案

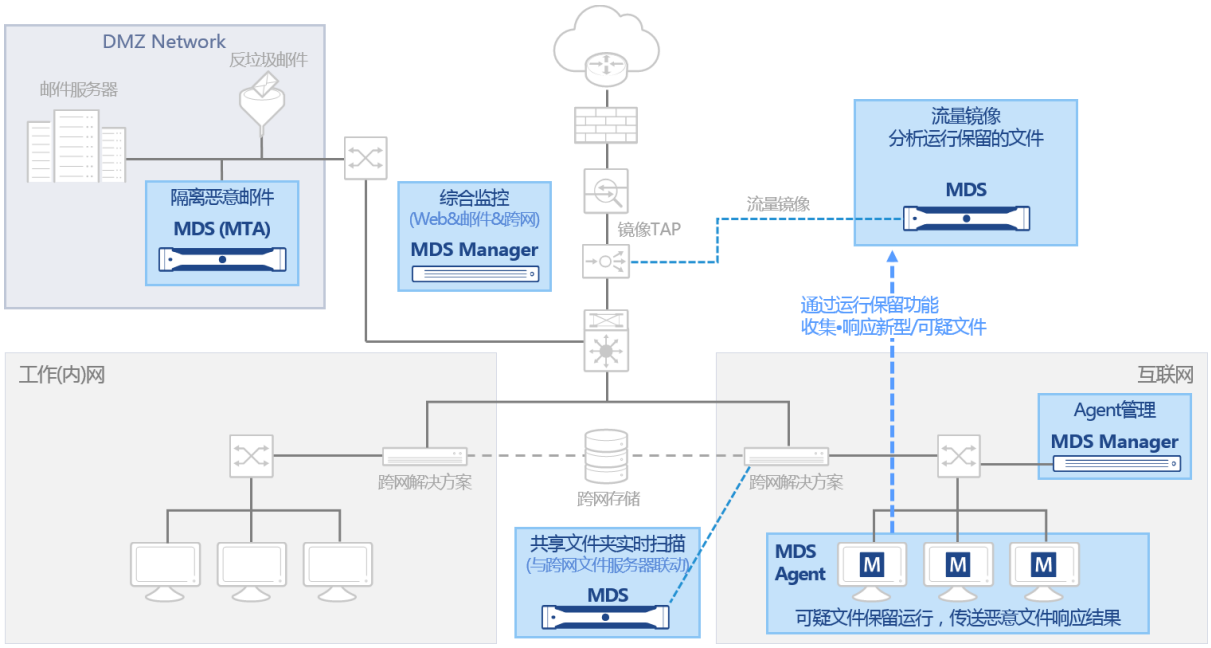
提供含检测、日志及修复功能的一体式设备，也可根据客户公司的环境与安全等级要求，灵活构建及扩张 MDS 与 MDS Manager。

构建方案



结构图

可疑构建有效响应来自网络、电子邮件、端点和跨网区间各种途径和威胁的系统。



第2章　产品配置

2.1　设备系统配置

设备系统配置如下。

<table>
<tr><th>项目</th><th>MDS 4000A</th><th>MDS 8000A</th><th colspan="2">MDS 10000A</th></tr>
<tr><td>动态分析性能</td><td>35,000 件/1 天</td><td>90,000 件/1 天</td><td colspan="2">200,000 件/1 天</td></tr>
<tr><td>管理 Agent 数</td><td>700 个</td><td>2,000 个</td><td colspan="2">5,000 个</td></tr>
<tr><td>Throughout</td><td>800 Mbps</td><td>1.5 Gbps</td><td colspan="2">4 Gbps</td></tr>
<tr><td>HDD</td><td>1 TB x 2ea.</td><td>1 TB x 4ea.</td><td colspan="2">1 TB x 8ea.</td></tr>
<tr><td>RAID</td><td>RAID 1</td><td>RAID 10</td><td colspan="2">RAID 10</td></tr>
<tr><td rowspan="2">网络接口</td><td rowspan="2">1GbE 4 Ports (Copper)
10G SFP + 4 Ports (Optical)</td><td rowspan="2">1GbE 4 Ports (Copper)
10G SFP + 4 Ports (Optical)</td><td>默认</td><td>可选</td></tr>
<tr><td>1GbE 2 Ports (Copper)
1/10G Base-T 2 Ports (Copper)
1/10G SFP+ 4 Ports (Optical)</td><td>1GbE 2 Ports (Copper)
1/10G Base-T 4 Ports (Copper)
1/10G SFP+ 6 Ports (Optical)</td></tr>
<tr><td>电源</td><td>750 W Redundant</td><td>750 W Redundant</td><td colspan="2">750 W Redundant</td></tr>
<tr><td>Rack Mount</td><td>1U, 19 inch</td><td>1U, 19 inch</td><td colspan="2">2U, 19 inch</td></tr>
<tr><td>尺寸(WxDxH, mm)</td><td>482 x 721.91 x 42.8</td><td>482 x 721.91 x 42.8</td><td colspan="2">482.4 x 715.5 x 86.8</td></tr>
</table>

2.2 管理系统配置

当连接 MDS 的管理员界面时，需要如下硬件和软件。

硬件

- RS232(DE-9)规格串联端口
- USB 型串联端口适配器或电缆（没有 DE-9 型串行端口时）

软件

- 支持 SSHv2 的终端客户端软件
- 支持 SSL/TLS 连接的网页浏览器

2.3 Agent 系统配置

与 MDS 设备进行通信的 Agent 需要安装在管理对象 PC 上，应满足如下系统配置要求。

硬件

- CPU：Intel Pentium 4 1.0 GHz 以上
- 内存：1 GB 以上
- 存储设备：1 GB 以上剩余空间
- 1 个以上网络接口卡

软件

- 网页浏览器：Internet Explorer 9.0 以上

操作系统

支持下列操作系统。

- 客户端：Windows XP SP3 以上, Windows 7, Windows 8(8.1), Windows 10
- 服务器：Windows Server 2003 SP2 以上, Windows Server 2008, Windows Server 2012, Windows Server 2016

参考

上述客户端和服务器操作系统均支持 32 位和 64 位。 服务器操作系统不支持服务器核安装模式。

第3章　设备介绍

3.1　MDS 4000A

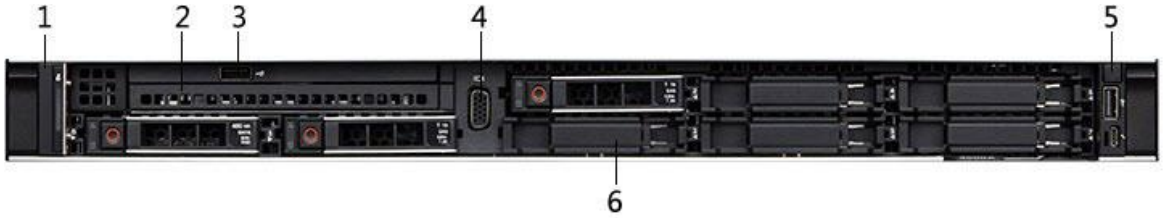
MDS 4000A 的外观分为正面和背面。

设备正面

下面将介绍安装和未安装挡板的正面。

安装挡板后的正面

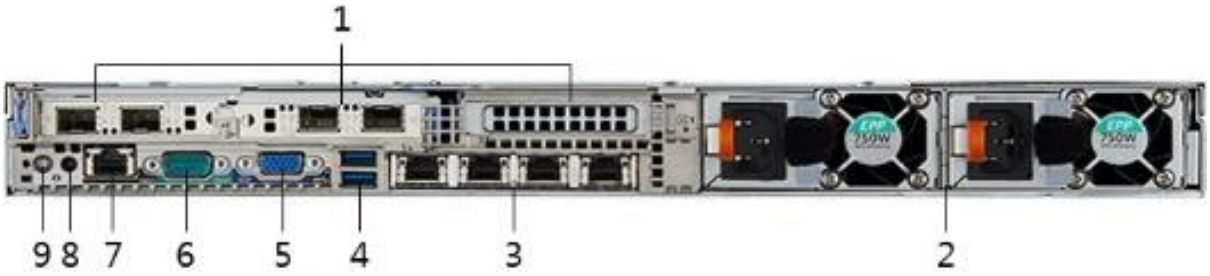
未安装挡板的正面



项目	名称	图标	描述
1	左控制面板	N/A	系统状态和系统 ID，状态 LED 和 iDRAC Quck Sync 2(无线)指示灯。
2	光驱(选项)	N/A	一个超薄 SATA DVD-ROM 驱动器或一个 DVD+/-RW 驱动器。

3	USB 端口(选项)		符合 USB 3.0 标准，可 USB 设备可以连接到系统。
4	VGA 端口		可将 VGA 显示器连接到系统。
5	右控制面板	N/A	电源按钮，USB 端口，iDRAC Direct Micro 端口和 iDRAC Direct 状态 LED。
6	驱动器插槽	N/A	可以在系统上安装支持的驱动器。

设备背面



项目	名称	图标	描述
1	PCIe 扩展卡插槽（3 个）	N/A	可以通过扩展槽连接 PCI Express 扩展卡。
2	供电装置（2 个）	N/A	支持 750 W 冗余 AC 电源 。
3	NIC 端口（4 个）		内置 NDC(Network Daughter Card)，提供网络连接配置。
4	USB 端口（2 个）		符合 USB 3.0 标准的 9 针，可将 USB 设备可以连接到系统。
5	VGA 端口		可将 VGA 显示器连接到系统。
6	串行端口		可将串行设备连接到系统。
7	iDRAC9 专用网络端口		iDRAC9 专用网络端口可以安全访问嵌入在单独管理网络中的 iDRAC。
8	系统状态指示灯电缆端口	N/A	如果安装了 CMA，则可以连接状态指示灯电缆并查看系统状态。
9	系统 ID 按钮		位于系统正面和背面，按下按钮并打开系统 ID 按钮以识别机架中的系统。重置 iDRAC 并使用模式中的步骤访问 BIOS。

3.2 MDS 8000A

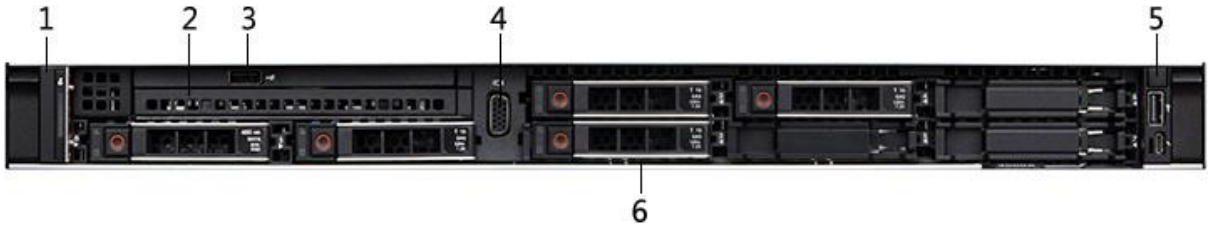
MDS 8000A 的外观分为正面和背面。

设备正面

下面将介绍安装和未安装挡板的正面。

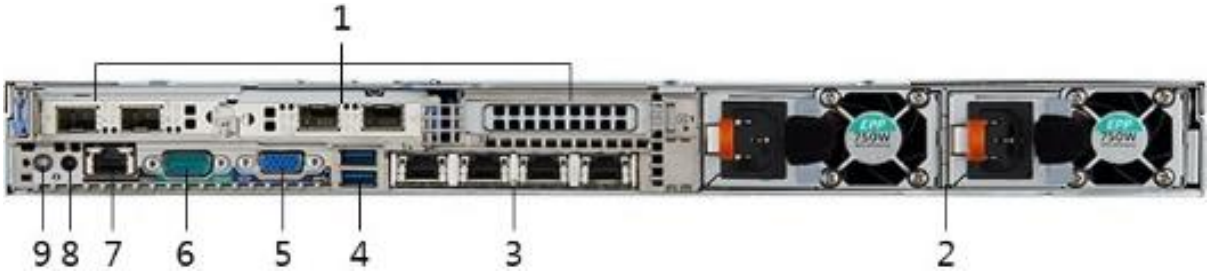
安装挡板后的正面

未安装挡板的正面



项目	名称	图标	描述
1	左控制面板	N/A	系统状态和系统 ID，状态 LED 和 iDRAC Quck Sync 2(无线)指示灯。
2	光驱(选项)	N/A	一个超薄 SATA DVD-ROM 驱动器或一个 DVD+/-RW 驱动器。
3	USB 端口(选项)		符合 USB 3.0 标准，可将 USB 设备可以连接到系统。
4	VGA 端口		可将 VGA 显示器连接到系统。
5	右控制面板	N/A	电源按钮，USB 端口，iDRAC Direct Micro 端口和 iDRAC Direct 状态 LED。
6	驱动器插槽	N/A	可以在系统上安装支持的驱动器。

设备背面



项目	名称	图标	描述
1	PCIe 扩展卡插槽（3 个）	N/A	可以通过扩展槽连接 PCI Express 扩展卡。
2	供电装置（2 个）	N/A	支持 750 W 冗余 AC 电源 。
3	NIC 端口（4 个）		内置 NDC(Network Daughter Card)，提供网络连接配置。
4	USB 端口（2 个）		符合 USB 3.0 标准的 9 针，可将 USB 设备可以连接到系统。
5	VGA 端口		可将 VGA 显示器连接到系统。
6	串行端口		可将串行设备连接到系统。
7	iDRAC9 专用网络端口		iDRAC9 专用网络端口可以安全访问嵌入在单独管理网络中的 iDRAC。
8	系统状态指示灯电缆端口	N/A	如果安装了 CMA，则可以连接状态指示灯电缆并查看系统状态。
9	系统 ID 按钮		位于系统正面和背面，按下按钮并打开系统 ID 按钮以识别机架中的系统。重置 iDRAC 并使用模式中的步骤访问 BIOS。

3.3 MDS 10000A

MDS 10000A 的外观分为正面和背面。

设备正面

下面将介绍安装和未安装挡板的正面。

安装挡板后的正面

未安装挡板的正面

项目	名称	图标	描述
1	左控制面板	N/A	系统状态和系统 ID，状态 LED 和 iDRAC Quck Sync 2(无线)指示灯。
2	驱动器插槽	N/A	可以在系统上安装支持的驱动器。
3	光驱(选项)	N/A	可在 CD(Compact Disc)和 DVD(Digital Versatile Disc)等光盘上搜索和保存数据。
4	右控制面板	N/A	电源按钮， VGA 端口， iDRAC Direct micro USB 端口，USB 2.0 端口。

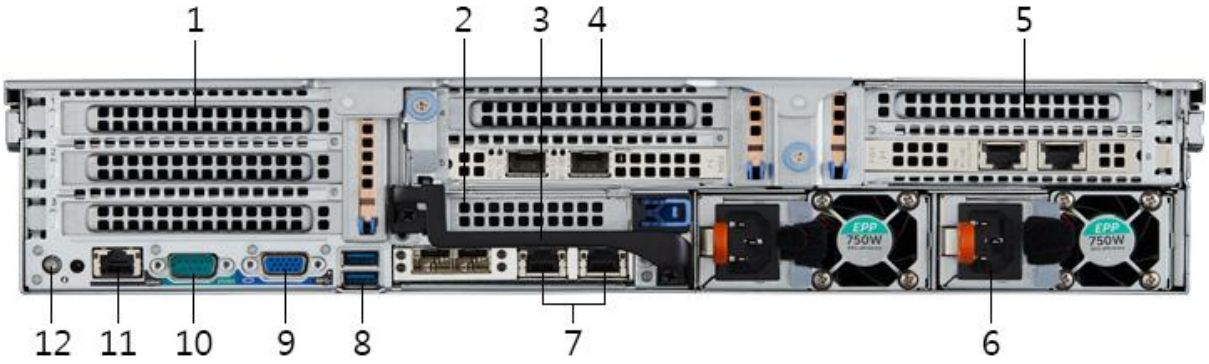
5	信息标签	N/A	信息标签是滑动式标签面板，可根据需要记录系统信息，如服务标签、NIC 和 MAC 地址。如果为 iDRAC 选择 Secure Basic Access，则信息标签还包含 iDRAC 安全默认密码。

iDRAC Direct LED 指示灯

有关 iDRAC Direct LED 指示灯的说明如下。

iDRAC Direc LED 指示灯代码	状态
绿色亮起后持续 2 秒	表示连接到笔记本电脑或平板电脑。
呈绿色闪烁（亮 2 秒，然后熄灭 2 秒）	表示识别连接的笔记本电脑或平板电脑。
熄灭	表示未连接到笔记本电脑或平板电脑。

设备背面

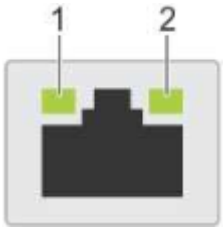


项目	名称	图标	描述
1	全高型 PCIe 扩展卡插槽（3 个）	N/A	PCIe 扩展卡插槽（提升版 1）可将最多三个全高型 PCIe 扩展卡连接到系统。
2	半高型 PCIe 扩展卡插槽	N/A	PCIe 扩展卡插槽（提升版 2）可将一个半高型 PCIe 扩展卡连接到系统。
3	背面手柄	N/A	可以卸下背面手柄，以便为 PCIe 扩展卡插槽 6 中安装的 PCIe 卡启用外部电缆连接。
4	全高型 PCIe 扩展卡插槽（2 个）	N/A	PCIe 扩展卡插槽（提升版 2）可将最多两个全高型 PCIe 扩展卡连接到系统。
5	全高型 PCIe 扩展卡插槽（2 个）	N/A	PCIe 扩展卡插槽（提升版 2）可将最多两个全高型 PCIe 扩展卡连接到系统。
6	供电装置（2 个）	N/A	支持 750 W 冗余 AC 电源 。

7	NIC 端口		内置 NDC(Network Daughter Card)，提供网络连接配置。
8	USB 端口（2 个）		符合 USB 3.0 标准的 9 针，可将 USB 设备可以连接到系统。
9	VGA 端口		可将 VGA 显示器连接到系统。
10	串行端口		可将串行设备连接到系统。
11	iDRAC9 Enterprise 端口		可以远程访问 iDRAC。
12	系统 ID 按钮		位于系统正面和背面，按下按钮并打开系统 ID 按钮以识别机架中的系统。重置 iDRAC 并使用模式中的步骤访问 BIOS。

NIC 指示灯

系统背面的每个 NIC 都有一个指示灯，提供给有关活动和链接状态的信息。1 是链接 LED 指示灯，表示连接网络的速度；2 是运转 LED 指示灯，表示数据是否通过 NIC 传输。



有关 NIC 指示灯的说明如下。

NIC 指示灯代码	状态
1 链接 LED 指示灯：关闭 2 运转 LED 指示灯：关闭	NIC 未连接到网络。
1 链接 LED 指示灯：红色 2 运转 LED 指示灯：呈绿色闪烁	NIC 以最大端口速度连接到有效网络，并且正在传输或接收数据。

第4章　Web 管理界面

4.1　登录和注销

您可以通过 Web 浏览器登录到 MDS 设备，以便于网络管理和安全策略应用。它使用 SSL 通信来实现数据的完整性和安全性。 AhnLab 提供了一个默认的登录管理员帐户。强烈建议您更改密码设置以进行安全保护，并在初次登录时提示您更改密码。

登录

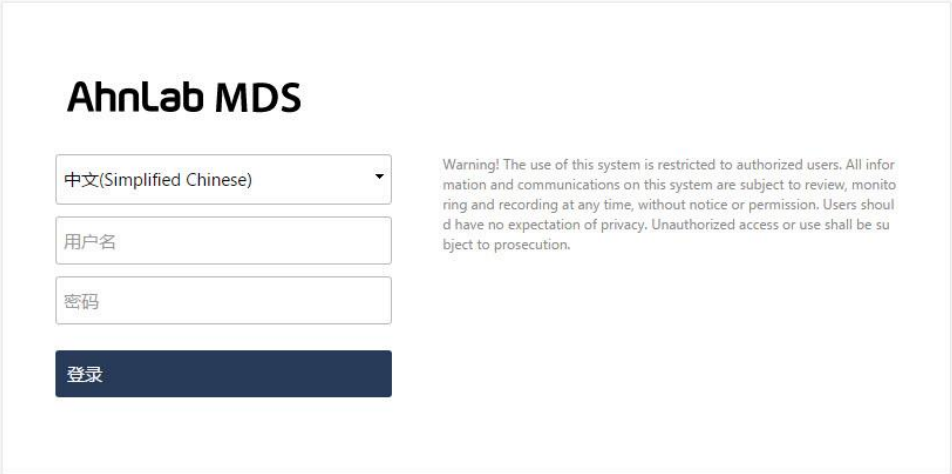
1. 在您的计算机打开 Web 浏览器，该计算机必须在指定的管理员 IP 地址范围。

> **参考**
>
> 您必须使用支持 SSL/TLS 1.2 连接的网页浏览器。建议使用 Goolge Chrome。管理员 IP 地址范围是在安装产品的过程中设置的。

2. Web 浏览器地址栏里输入 *https://MDS 设备 IP 地址:59005* 连接到设备。(例如：https://127.10.0.1:59005， *https://logsvr.example.com:59005*)

> **参考**
>
> MDS 默认使用专用安全证书。如果无法识别 SSL/TLS 证书的颁发机关，有关安全证书有问题的消息会出现。如果没有安装公用安全证书，请单击“继续浏览此网站（不推荐）”，登录到 MDS 设备。

3. 当出现登录窗口，选择语言选项，然后输入**用户名**和**密码**。



4. 单击**登录**，即可登录到管理员界面的首页。

⚠注意

您首次登录时，系统将提示您更改默认帐户信息。使用默认管理员帐户存在安全漏洞，必须更改默认帐户 ID 与密码。登录到设备管理员界面后，点击 **管理 > 系统 > 管理员帐户**，鼠标双击默认管理员帐户，即可出现更改管理员帐户的窗口。

⚠注意

如果登录失败次数超过限制，您的帐户将被锁定一段时间。有关帐户锁定设置的详细信息，请参考帐户策略。

参考

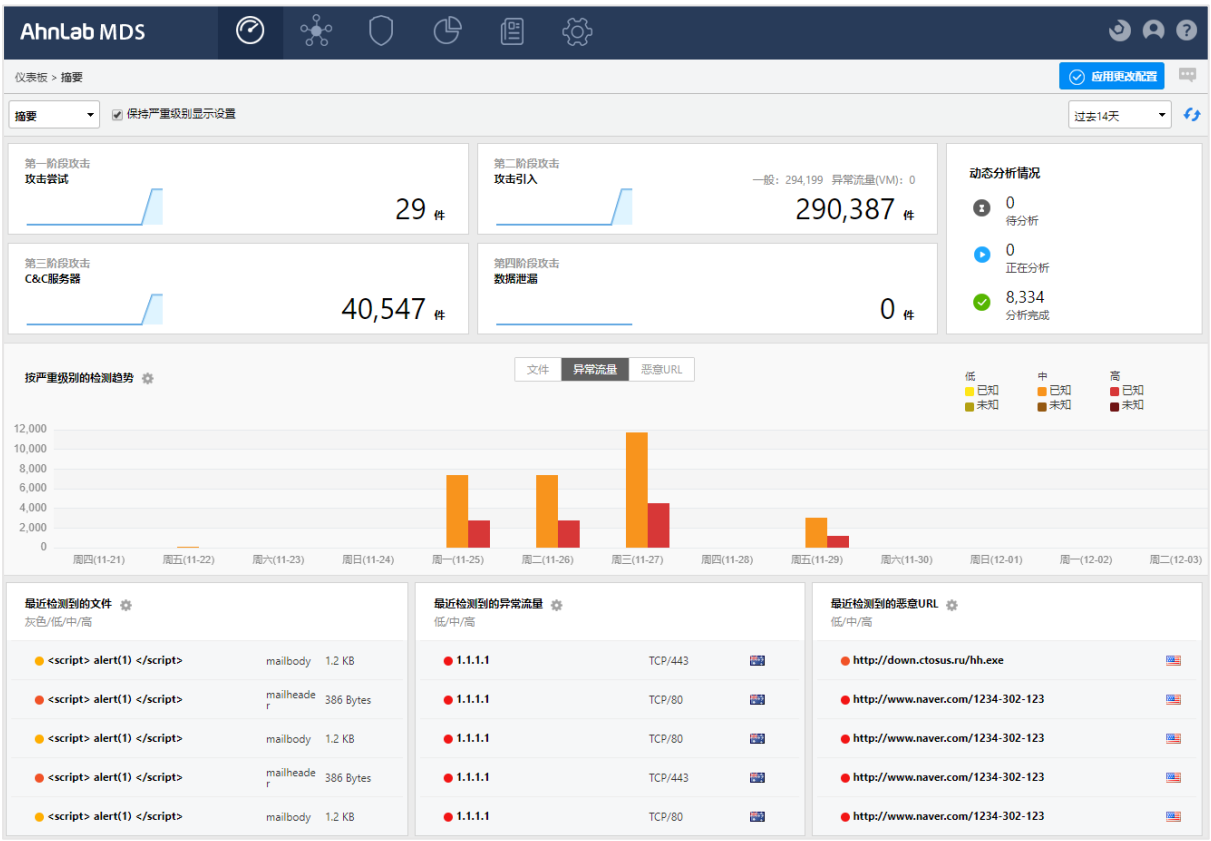
建议定期更改密码以保证安全。有关管理员帐户设置的详细信息，请参考帐户策略。

注销

如要退出 MDS 管理员 Web 界面，请点击右上角的帐户图标，在弹出的窗口中点击**注销**。

4.2 Web 管理界面

MDS 的 Web 管理员界面如下构成：



菜单

菜单区域分为主菜单和常用菜单区域。主菜单包括：

- 仪表板：登录到 Web 界面后的首页。显示最近检测到的威胁情况和动态分析情况等内容。
- 检测情况：显示检测到的威胁、异常流量、感染主机、感染途径和攻击位置等信息，并可以对每一个检测到的威胁采取措施。
- 响应情况：显示响应威胁和异常流量的结果。
- 统计：显示按期间的检测威胁情况、响应情况、管理确认情况和运营情况等统计信息。
- 报告：显示报告并可以创建报告。
- 管理：配置系统设置，如备份和恢复、联动、Agent 和策略设置。

右上角的常用菜单包括：

- 工具：执行系统管理员所需的功能，如检查系统完整性、发送通知和 Pinpoint 扫描等。
- 帐户：显示当前登录的管理 ID、IP 地址和并发用户数等信息。单击**更改密码**，可以更改当前的密码。点击**注销**，结束当前的会话。
- 帮助：打开产品的在线帮助，查看产品的版本信息。

4.3 并发用户管理

查看当前登录到 MDS Web 管理界面的帐户信息。如果有可疑的 ID 和 IP 地址的访问，可以断开此帐户的连接。

断开并发连接的步骤如下：

1. 点击 Web 界面右上角的**帐户**图标。
2. 在弹出的窗口中，点击**并发用户数**。
3. 弹出<并发用户情况>窗口。
4. 确认欲断开连接的帐户，点击**断开连接**图标。
5. 点击**确定**关闭窗口。

参考

点击**帐户**图标出现的窗口中，点击**更改密码**，可以更改当前的密码；点击**注销**，可以断开当前的会话。

4.4 工具

发送通知

您可以向连接服务器的主机发送消息，目的是通知 Agent 受感染情况或提醒主机注意最近流行的安全威胁，还告知恶意软件检测或其他程序的补丁信息或更新相关的安全漏洞以及其他一般管理问题。

> **参考**
>
> 未连接到服务器的主机，无法即时收到服务器发送的通知。发送命令时间到期后，即使与服务器连接，也可能无法收到通知。

向所有的主机发送通知

向所有主机发送通知的方法如下：

1. 点击 Web 界面右上角的**工具**图标。

2. 在弹出的菜单中选择**发送通知**。
3. 弹出<发送通知>窗口。输入**标题**和**内容**。
4. 输入所有内容后，点击**发送**。

向特定主机发送通知

选择特定主机发送通知的方法如下：

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**主机**标签。
3. 选择欲发送通知的 Agent，然后点击**响应**菜单中的**发送通知**。
4. 弹出<发送通知>窗口。输入**标题**和**内容**。
5. 输入所有内容后，点击**发送**。

Pinpoint 扫描

将可疑的文件或 URL 指定为扫描对象进行实时扫描，并显示扫描结果。有关扫描结果，可在**响应情况>Pinpoint 扫描**中查看。

工具菜单中执行 Pinpoint 扫描

在工具菜单中执行 Pinpoint 扫描的方法如下：

1. 点击 Web 界面右上角的**工具**图标。
2. 在弹出的菜单中选择 **Pinpoint 扫描**。
3. 弹出<Pinpoint 扫描>窗口。
4. 选择欲进行 Pinpoint 扫描的对象类型，**文件**或 **URL**。
5. 如果选择了“**文件**”，则点击**浏览...**选择欲扫描的文件；如果选择了“**URL**”，则输入欲扫描的 URL，然后输入如下信息：
   - 动态分析时间：输入在虚拟机环境中分析文件的最长时间，有效值为 40 到 3,600 秒之间。
   - 密码：如要扫描加密的文件（例如压缩文件），请输入用于加密的密码。扫描 URL 时，可能不使用密码。
   - 参数：如要通过特定参数进行扫描，请输入参数。这些参数可能会导致恶意可执行文件的恶意行为。
   - 已知恶意代码：如要在虚拟机上运行诊断为已知恶意代码的文件以进行分析，请选择复选框。
6. 点击**执行**。

检测界面中执行 Pinpoint 扫描

扫描可疑文件

选择特定文件进行 Pinpoint 扫描的方法如下：

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**文件**标签。
3. 在文件列表中选择欲进行 Pinpoint 扫描的文件，然后选择**响应**菜单中的 **Pinpoint 扫描**。

扫描可疑 URL

选择特定 URL 进行 Pinpoint 扫描的方法如下：

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**恶意 URL** 标签。
3. 在 URL 列表中选择欲进行 Pinpoint 扫描的 URL，然后选择**响应**菜单中的 **Pinpoint 扫描**。

完整性检验

固件首次安装在设备时，MDS 保存系统内部的所有文件的信息。完整性检验是将初期保存的文件和当前的文件进行比较，检验系统文件是否被更改或删除，判断完整性受损与否。

执行完整性检验的方法如下：

1. 点击 Web 界面右上角的**工具**图标。
2. 在弹出的菜单中选择**完整性检验**。
3. 弹出<完整性检验>窗口，系统自动执行设备的完整性检验。
4. 完整性检验结束后，点击**确定**。

关机/重启

根据需要可以关机或重启设备。

设备关机

关机按如下步骤：

1. 点击 Web 界面右上角的**工具**图标。
2. 在弹出的菜单中选择**关机/重启**。
3. 弹出“您要关闭或重新启动系统？如果关闭系统，该期间发生的日志有可能不会被保存。”提示窗口。
4. 点击**关闭**。

设备重启

重新启动按如下步骤：

1. 点击 Web 界面右上角的**工具**图标。
2. 在弹出的菜单中选择**关机/重启**。
3. 弹出“您要关闭或重新启动系统？如果关闭系统，该期间发生的日志有可能不会被保存。”提示窗口。
4. 点击**重新启动**。

> ⚠**注意**
>
> 当重新启动时，系统可能会处于危险之中。请在绝对必要时才执行关机或重新启动操作。另外，请注意，如果结束系统，该期间发生的日志可能不会被保存。

第5章　部署配置说明

5.1　接口

管理 MDS 网络的物理接口和逻辑接口，并根据 MDS 所在网络环境特性，配置各种形式的接口。

更改网络接口

更改网络接口的方法如下。

> **参考**
>
> 网络接口是物理构成的接口，因此无法添加或删除，但可以更改。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在网络接口列表中，鼠标双击欲更改的接口，打开<更改网络接口>界面。
4. 更改所需的项目。
   - 启用：显示网络接口的启用状态。
   - 名称：显示网络接口的名称，无法更改。
   - IP 分配：选择 IP 地址的分配方式。
     - 固定：物理接口分配固定的 IP 地址。
     - DHCP：物理接口不分配固定的 IPv4 地址，分配 DHCP 服务器自动分配的 IPv4 地址。
   - IPv4 地址：当类型选择‘固定’的时候输入 IPv4 地址，分配给网络接口。
   - IPv6 地址：当类型选择‘固定’的时候输入 IPv6 地址，分配给网络接口。
   - 访问控制：选择必要的协议，通过网络接口管理 MDS 设备。
   - 最大传输单位（MTU）：设置 MTU，有效值为 100~1500，默认值为 1500。
   - 通信模式：显示网络接口的传输速度和方式。
     - Auto：自动设置速度和方式。
     - 10Mbps 半双工：使用 10Mbps 半双工传输（Half Duplex）方式设置速度和方式。
     - 10Mbps 全双工：使用 10Mbps 全双工传输方式（Full Duplex）设置速度和方式。
     - 100Mbps 半双工：使用 100Mbps 半双工传输（Half Duplex）方式设置速度和方式。
     - 100Mbps 全双工：使用 100Mbps 全双工传输方式（Full Duplex）设置速度和方式。

- 1000Mbps 全双工：使用 1000Mbps 全双工传输方式（Full Duplex）设置速度和方式。

参考

全双工传输（Full Duplex）是指在一个接口同时进行双向通信的方式。半双工传输（Half Duplex）也是一个接口双向通信，但是一次只能向一个方向通信。如果设置为 **自动**，则检查接口并自动设置为最合适的通信模式。若无法得知通信模式或无法设置适当速度时，请选择**自动**。

- MAC 地址：显示网络接口的 MAC 地址。
- 输入描述：输入最多 63 个字符的描述。

5. 点击**确定**。
6. 点击**应用更改配置**。

配置聚合接口

可以组合多个物理接口，并将其配置为可以高速处理数据的一个逻辑接口。配置聚合接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择**聚合**，则出现<添加聚合接口>界面。
4. 设置各项目。
   - 启用：选择复选框启用接口。如果不启用接口，则只添加接口，而不使用。
   - 名称：输入聚合接口的名称，组合英文和数字，且不能超过 15 个字符。
   - 运行模式：选择聚合接口的运行模式。
     - Active-Backup：在基本物理接口发生问题时，由备用物理接口代替工作。虽然产生容错（fault tolerance），但没有负载均衡（Load balancing）。
     - Active-Active：所有的物理接口都能正常工作，所以会有容错和负载均衡。
     - 802.3ad：将支持动态聚合，所有的物理接口都能正常工作，所以会有容错和负载均衡。
   - 网络接口：选择以聚合方式配置的物理接口，必须选择两个以上。
   - IPv4 地址：设置接口使用的 IPv4 地址和 CIDR。
   - IPv6 地址：设置接口使用的 IPv6 地址和 CIDR。
   - 访问控制：选择必要的协议，通过网络接口管理 MDS 设备。
   - 最大传输单位（MTU）：设置 MTU，有效值为 100~1500，默认值为 1500。
   - 输入描述：输入最多 63 个字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改聚合接口

更改聚合接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 鼠标双击聚合接口列表中的欲更改项目，打开<更改聚合接口>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除聚合接口

删除聚合接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在聚合接口列表中选择欲删除项目 左侧的 ✕，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

配置 Tap 接口

可以配置一个既可以监控流量而不影响网络流量的 TAP 接口。配置 Tap 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择 **Tap**，则出现<添加 Tap 接口>界面。
4. 设置各项目。
   - 启用：选择复选框启用接口。如果不启用接口，则只添加接口，而不使用。
   - 名称：输入 Tap 接口的名称，组合英文和数字，且不能超过 15 个字符。
   - 选择接口：从下拉框中选择网络接口。
   - 配对接口：根据选择接口，自动显示。
   - 最大传输单位（MTU）：设置 MTU，有效值为 1000~1500，默认值为 1500。
   - 输入描述：输入最多 63 个字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改 Tap 接口

更改 Tap 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 鼠标双击 Tap 接口列表中的欲更改项目，打开<更改 Tap 接口>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 Tap 接口

删除 Tap 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在 Tap 接口列表中选择欲删除项目 左侧的 ❌ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

配置 VLAN 接口

可以通过将其逻辑接口分割成多个接口，当作多个虚拟网络来使用。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择 **VLAN**，则出现<添加 VLAN 接口>界面。
4. 设置各项目。
   - 启用：选择复选框启用接口。如果不启用接口，则只添加接口，而不使用。
   - 名称：输入聚合接口的名称，组合英文和数字，且不能超过 15 个字符。
   - VLAN ID：输入 VLAN ID。VLAN ID 可以是 1 到 4095 之间的任何数字。
   - 网络接口：从下拉框中，选择连接到 VLAN 的接口。
   - IPv4 地址：设置接口使用的 IPv4 地址和 CIDR。
   - IPv6 地址：设置接口使用的 IPv6 地址和 CIDR。
   - 访问控制：选择必要的协议，通过网络接口管理 MDS 设备。
   - 最大传输单位（MTU）：设置 MTU，有效值为 100~1500，默认值为 1500。
   - 输入描述：输入最多 63 字符的描述。

5. 点击**确定**。
6. 点击**应用更改配置**。

更改 VLAN 接口

更改 VLAN 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 鼠标双击 VLAN 接口列表中的欲更改项目，打开<更改 Tap 接口>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 VLAN 接口

删除 VLAN 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在 VLAN 接口列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

参考

配置逻辑接口（聚合，Tap，VLAN）的物理接口即网络接口的状态必须是启用，而且一个网络接口不能在多个逻辑接口中同时使用。

参考

IPv4 地址/CIDR 有效范围：IPv4 地址需要输入 0.0.0.0~255.255.255.255 之间；CIDR 需要输入 0~32 之间。
IPv6 地址/CIDR 有效反问：IPv6 地址需要输入 ::~ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff 之间；CIDR 需要输入 0~128 之间。

配置监控接口

MDS 镜像流入网络的流量，以检测恶意代码和异常流量。为了检查流量，物理连接镜像接口到 MDS 设备，然后在 MDS 设备上设置监控接口。因此，在配置监控接口之前，必须配置用于监控的接口。

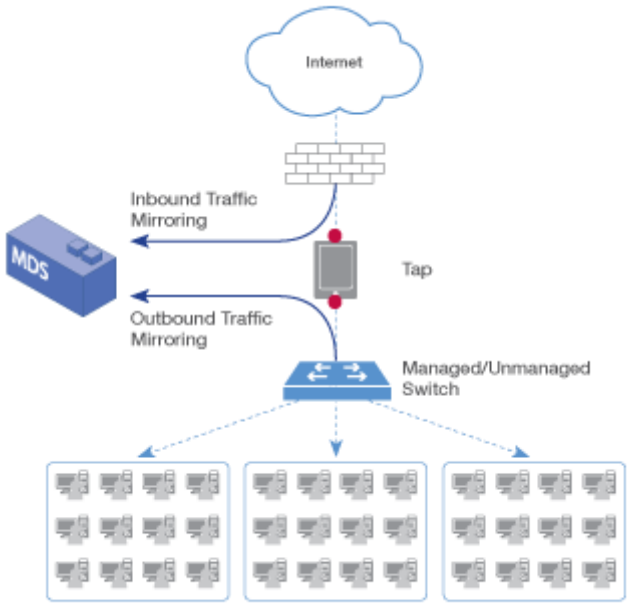
参考

未指定为监控接口的接口默认状态称为管理接口。

镜像接口可以通过多种方式进行配置，例如连接 Tap 设备或交换机/路由器的镜像接口。通过配置的镜像接口将流量传送到 MDS 设备进行监控。

下面的示例使用 Tap 来镜像网络顶部上的所有入站/出站的流量。将两个物理接口连接到 MDS 的 eth2 和 eth3，以分别接收 Rx、Tx 流量。

将上述配置镜像的内容用图表示如下：



- MDS 连接两个物理接口（eth2，eth3），分别接收 Rx 和 Tx 流量
- 配置聚合接口，使接收 MDS 镜像的流量的网络接口视为逻辑上一个接口
- 监控所有 LAN 和 WAN 流量

根据上面的示例来配置监控接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择**聚合**，则出现<添加聚合接口>界面。
4. 设置各项目。
   - 启用：选择复选框。
   - 名称：输入 agg0。
   - 运行模式：选择 Acitve-Active。
   - 网络接口：选择 eth2 和 eth3。

- IPv4 地址：输入 0.0.0.0/0。
- 访问控制：不选择。
- 最大传输单位（MTU）：输入 1500。

5. 点击**确定**。

参考

完成聚合接口配置后，网络接口列表中的 eth2 和 eth3 更改为 0.0.0./0（默认路由器）。

6. 点击**配置监控接口**，弹出<配置监控接口>窗口。
7. 从列表中选择 **agg0**。
8. 点击**确定**。
9. 点击**应用更改配置**。

参考

最多可以选择 4 个接口为监控接口。

参考

应用邮件过滤的网络接口应与检测检测恶意代码和异常流量的网络接口区分。检测恶意代码和异常流量的监控接口应配置为镜像流量，用于邮件过滤的网络接口应在邮件服务器和外部网络之间内联。

5.2 镜像接口

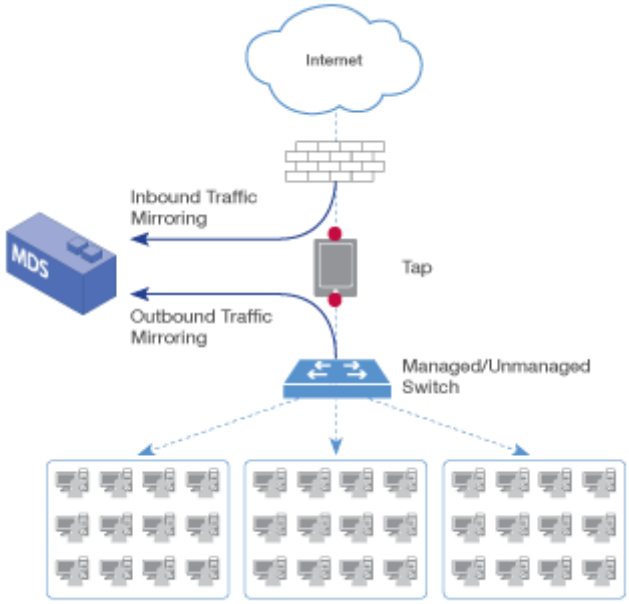
配置镜像接口有很多种不同的方式。镜像流量的常见的方法如下：

- 配置方法 1：使用 Tap 以镜像连接到顶部（WAN）的交换机/路由器端口的 Rx 和 Tx 流量。
- 配置方法 2：使用 Tap 以镜像连接到底部（LAN）的交换机/路由器端口的 Rx 和 Tx 流量。
- 配置方法 3：使用托管交换机镜像连接到顶部（WAN）的交换机/路由器端口的 Rx 和 Tx 流量。
- 配置方法 4：使用托管交换机镜像连接到底部（LAN）的交换机/路由器端口的 Rx 和 Tx 流量。
- 配置方法 5：使用托管交换机将连接到顶部（WAN）的交换机/路由器端口的 Rx 和 Tx 流量和连接到底部（LAN）的交换机/路由器端口的 Rx 和 Tx 流量镜像到不同的端口。

无论以何种方式配置镜像，请将防火墙位于顶部，以保护网络，并最大限度地减少 MDS 处理的流量。因此，请根据您的网络特性选择最佳的镜像配置。

配置方法 1

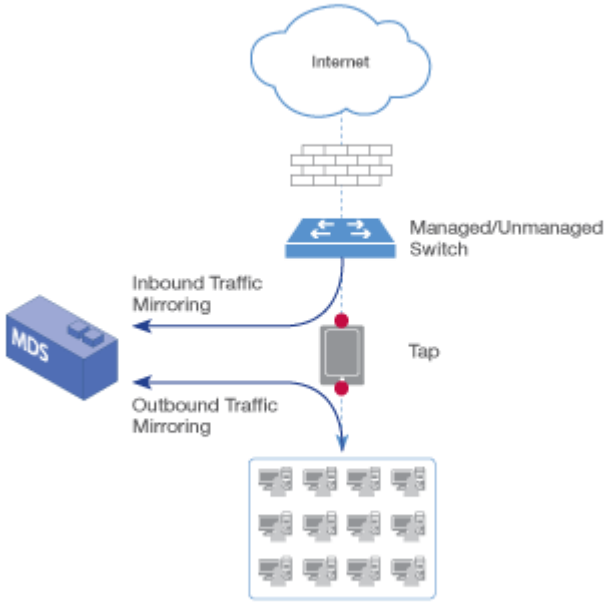
使用 Tap 从顶部（WAN）镜像网络上的所有入站/出站流量。类型 1 的镜像配置如下图所示。



- MDS 需要两个物理网络端口分别从 Tap 设备接收 Rx 和 Tx 流量。
- 必须配置聚合，以便 MDS 将逻辑上接收镜像流量的网络端口识别为另一个端口。
- 交换机/路由器没有性能负载。
- 可以监控 LAN 和 WAN 之间的所有流量。
- 它不适合大规模的网络，因为要监控的流量可能超出需求。
- 无法监控子网之间的流量。
- 随着 MDS 分析的流量的增减，性能可能会降低。

配置方法 2

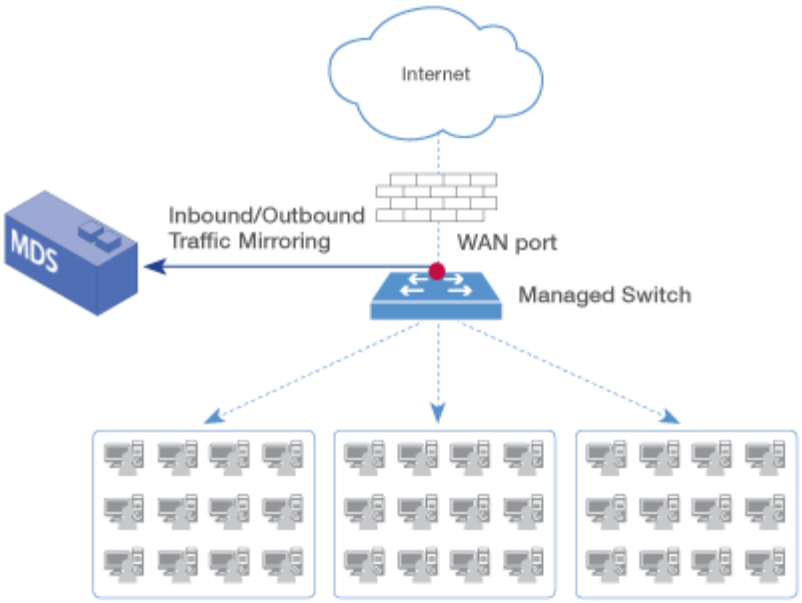
使用 Tap 从底部（LAN）镜像网络上的所有入站/出站流量。类型 2 的镜像配置如下图所示。



- MDS 需要两个物理网络端口分别从 Tap 设备接收 Rx 和 Tx 流量。
- 必须配置聚合，以便 MDS 将逻辑上接收镜像流量的网络端口识别为另一个端口。
- 交换机/路由器没有性能负载。
- 只能监控要保护的子网的入站/出站流量。
- 可以监控子网之间的流量。
- 由于通过子网单位制定监控范围，因此可以根据需要部署 MDS。

配置方法 3

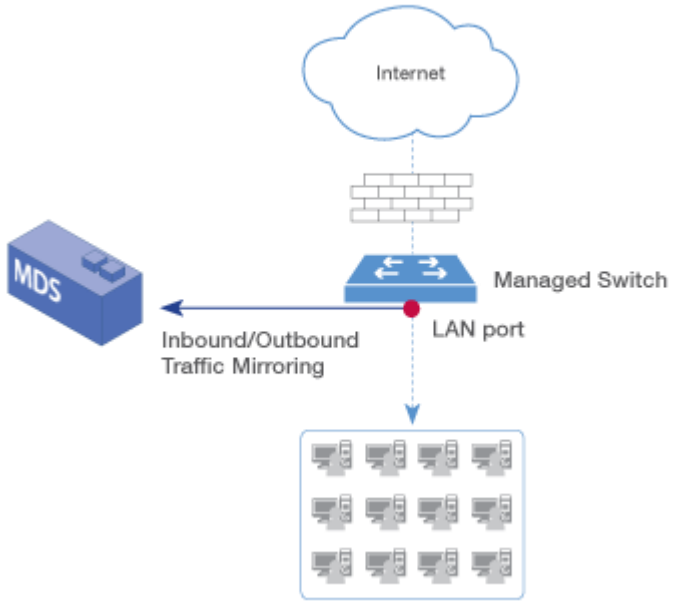
使用托管交换机镜像连接到顶部（WAN）的交换机/路由器端口的 Rx 和 Tx 流量。类型 3 的镜像配置如下图所示。



- MDS 接收一个物理网络端口镜像的流量。
- 要连接到 MDS，需要交换机/路由器单独配置镜像。
- 需要高性能交换机/路由器，因为它可能导致交换/路由器的性能负载。
- 可以监控 LAN 和 WAN 之间的所有流量。
- 它不适合大规模的网络，因为要监控的流量可能超出需求。
- 可以监控子网之间的流量。
- 随着 MDS 分析的流量的增减，性能可能会降低。

配置方法 4

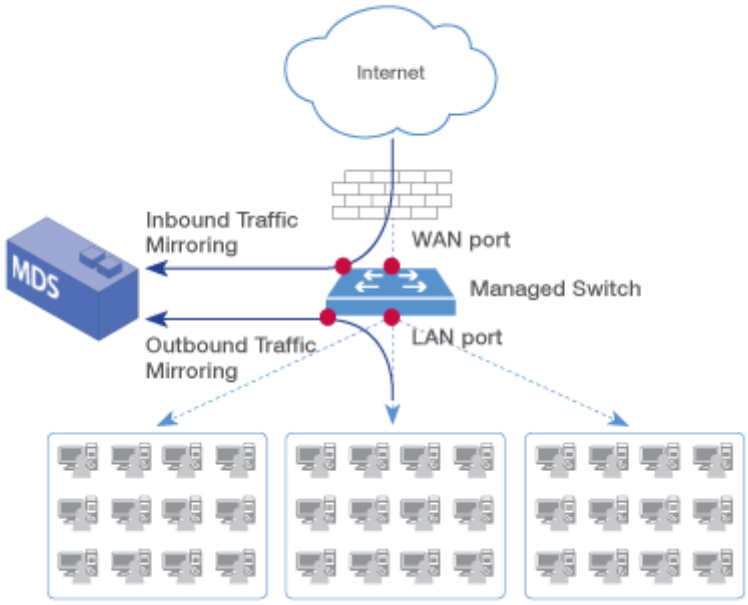
使用托管交换机从底部（LAN）镜像网络上的所有入站/出站流量。类型 4 的镜像配置如下图所示。



- MDS 接收一个物理网络端口镜像的流量。
- 要连接到 MDS，需要交换机/路由器单独配置镜像。
- 需要高性能交换机/路由器，因为它可能导致交换/路由器的性能负载。
- 只能监控要保护的子网的入站/出站流量。
- 可以监控子网之间的流量。
- 由于通过子网单位制定监控范围，因此可以根据需要部署 MDS。

配置方法 5

使用托管交换机可将连接到顶部（WAN）的交换机/路由器端口 Rx 流量以及底部（LAN）的交换机/路由器端口的 Rx 流量以不同的端口镜像。类型 5 的镜像配置如下图所示。



- MDS 需要两个物理网络端口分别从 Tap 设备接收 Rx 和 Tx 流量。
- 必须配置聚合，以便 MDS 将逻辑上接收镜像流量的网络端口识别为另一个端口。
- 要连接到 MDS，需要交换机/路由器单独配置镜像。
- 可以监控 LAN 和 WAN 之间的所有流量。
- 它不适合大规模的网络，因为要监控的流量可能超出需求。
- 可以监控子网之间的流量。
- 随着 MDS 分析的流量的增减，性能可能会降低。

5.3 检测设置

为了更有效检测各种安全威胁，配置检测相关的各种配置，如引入途径、检测日志、扫描条件、动态分析操作系统和动态分析对象等。

引入途径

配置 MDS 检测威胁的服务协议和 BCC。如果将每个协议设置为检测对象，则通过该协议收集到的数据包以镜像方式检查。按如下步骤设置。

参考

BCC 是 Blind Carbon Copy 的简称，中文名称为密件抄送。如果使用 BCC 方式，MDS 服务器作为密件添加到接收邮件的邮件头，MDS 服务器则对接收邮件执行扫描。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置检测对象的引入途径。
   - 镜像：选择 MDS 检测对象引入时使用的协议。如要全选，请选择**镜像**复选框。
   - E-mail BCC：选择 **E-mail BCC** 以检测发送到特定邮件服务器的邮件的正文或附件是否被恶意代码感染。当启用该选项，MDS 服务器将密件抄送收件人的邮件，并检查邮件正文或附件是否感染恶意代码。如果不启用该选项，则使用镜像方法通过 SMTP 扫描传入的数据包，以检查邮件是否被感染。
4. 点击**确定**。
5. 点击**应用更改配置**。

检测日志显示设置

MDS 将从镜像流量中收集的文件的检查结果记录在日志文件中，并设置在 Web 界面监视检测日志与否。按如下步骤设置。

注意

对于压缩文件或电子邮件，恶意状态由检测日志设置决定。即使是恶意的，但是没有设置为显示检测日志的话，则不被判定为恶意。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置检测日志。
   - 文件：选择记录日志的检测文件严重级别。

- C&C：选择记录日志的检测 C&C 服务器的严重级别。
- 恶意 URL：选择记录日志的检测恶意 URL 的严重级别。

4. 点击**确定**。
5. 点击**应用更改配置**。

扫描条件设置

配置恶意代码的扫描条件。按如下步骤设置。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置扫描条件。
   - 扫描大小限制：输入要扫描的最大文件大小。有效值为 1~300MB。
   - 扫描压缩文件：启用复选框，将对压缩文件进行扫描。
     - 最多压缩次数：输入要扫描的文件的最多压缩次数。有效值为 1~5 次。
   - 潜在的有害程序（PUP）：选择复选框，将潜在的有害程序检测为恶意。潜在的有害程序包括：生根程序、黑客工具或用户不知情的情况下安装到用户计算机并窃取个人信息的任何恶意软件。
   - 可能有害程序：选择复选框，将 MDS 分类为可能有害的程序(如键盘记录、远程访问工具等)检测为恶意。
4. 点击**确定**。
5. 点击**应用更改配置**。

动态分析设置

配置执行动态分析的虚拟机（VM）使用的操作系统和其他动态分析对象。按如下步骤设置。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置如下项目。
   - 分析时间：输入动态分析时间。有效值为 10~300 秒。
   - 操作系统：选择虚拟机（VM）使用的操作系统。

> **参考**
> 用户可以配置自定义的虚拟机（VM）环境，有关详细的内容，请参考更新。

   - 其他动态分析对象
     - 已知恶意代码：选择复选框，将已知恶意代码添加到动态分析对象。

- 创建可能正常的行为分析报告：选择复选框，将在虚拟机中运行被诊断为可能正常的文件后，分析行为并创建其行为分析报告。创建报告后，将记录检测日志。

参考

如果配置其他动态分析对象，则检测日志的记录可能会延迟，并且可能会影响到虚拟机（VM）的性能。

4. 点击**确定**。
5. 点击**应用更改配置**。

5.4 VirusTotal

在 MDS 设备利用 MDP 或 DICA 等自身引擎扫描文件之前，配置 VirusTotal 策略先进行扫描。联动 VirusTotal 时，需要使用 VirusTotal 颁发的个人密钥（Private key）作为联动密钥。

参考

如果未联动 VirusTotal，则根据产品的最新引擎判断是否恶意。

配置 VirusTotal 策略联动

配置 VirusTotal 策略联动的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > VirusTotal**。
3. 启用**联动 VirusTotal** 复选框，配置使用 virusTotal 策略。输入下面的各项值。
   - Virus Total：点击【更改联动密钥】，弹出<VirusTotal 联动密钥>窗口，输入 Virus Total(www.virustotal.com)颁发的个人密钥（Private Key），然后点击**确定**。
4. 点击**保存**。
5. 点击**应用更改配置**。

代表防病毒软件设置

从 VirusTotal 提供的防病毒软件中，可以设置代表防病毒软件，并根据指定的优先级显示恶意软件诊断名。

设置代表防病毒软件的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > VirusTotal**。
3. 请参考上面的配置 virusTotal 策略联动，联动 virusTotal 策略。
4. 联动成功后，将显示 VirusTotal 提供的防病毒软件列表。

5. 在左侧的列表中选择欲指定为代表防病毒软件的项目，点击  ，所选项目将移动到代表防病毒列表中。
6. 设置已知威胁基准。可以选择**检出比率**或**优先级**。
   - 检出比率：选择**检出比率**后，输入判断为已知威胁的检出比率。

参考

当选择**检出比率**作为已知威胁基准时，如果在代表防病毒软件列表中，检出威胁的防病毒软件数超过指定的检出比率，则该威胁被视为已知威胁。例如，当选择 5 个防病毒软件作为代表防病毒软件，检出比率输入 3，则表示至少有 3 个代表防病毒软件检出，则该威胁视为已知威胁。

   - 优先级：选择**优先级**。

参考

当选择**优先级**作为已知威胁基准时，如果在代表防病毒软件列表中，检出威胁的防病毒软件至少有一个，则该威胁被视为已知威胁。

7. 点击**保存**。
8. 点击**应用更改配置**。

参考

Virus Total(www.virustotal.com)颁发 Public Key 和 Private Key。如果加入 Virus Total，免费颁发 Public Key，但是功能存在限制，因此 MDS 仅使用通过 Private Key 联动。有关 Virus Total 的更多内容，请参考 https://www.virustotal.com 的 FAQ。

5.5 YARA 规则

使用来自谷歌（google）的开源项目实用程序 YARA，利用恶意文件或进程特征码来设置策略以判断恶意与否。使用字符串模式、二进制模式和正则表达式创建 YARA 规则，检查文件和进程是否包含恶意特征码来诊断为恶意。

注意

如果 MDS Manager 服务器中设置的策略与 MDS 服务器的策略联动使用，则无法使用 YARA 规则修改策略。要上传 YARA 规则或删除，必须禁用与 MDS Manager 服务器的联动。

添加 YARA 规则

添加 YARA 规则的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > YARA 规则**。
3. 点击**添加**，弹出<添加 YARA 规则>窗口。
4. 点击**浏览...**，选择 YARA 规则文件。

5. 选择**严重级别**。
6. 输入有关此 YARA 规则的描述。
7. 点击**确定**。

> **注意**
> 如果已存在与要添加的 YARA 规则文件名相同的文件，则将使用新添加的文件覆盖该文件。

> **参考**
> 上传的 YARA 规则文件不能大于 10MB，且最多可以添加 4,096 个。

> **参考**
> 如要将添加的 YARA 规则文件保存到本地计算机，请点击**导出**键。

更改 YARA 规则

更改 YARA 规则的步骤如下。

1. 在 YARA 规则列表中，点击要更改的 YARA 规则名称，弹出<更改 YARA 规则>窗口。
2. 更改所需的项目。
3. 点击**确定**。

移动 YARA 规则

移动 YARA 规则的步骤如下。

1. 在 YARA 规则列表中，选择要移动的 YARA 规则（选择复选框），然后点击**移动**。
2. 在弹出的菜单中，选择要移动的严重级别。
3. 弹出确认移动的提示，点击**确定**。

> **参考**
> 如果选择的 YARA 规则中包含了与要移动的规则具有相同严重级别的规则，则无法移动。

导出 YARA 规则

导出 YARA 规则有两种方式，一个是选择导出，另一个是按严重级别全部导出。

选择导出

1. 在 YARA 规则列表中，选择要导出的 YARA 规则（选择复选框），然后点击**导出**。
2. 在弹出的菜单中，选择**选择导出**。

3. 所选的 YARA 规则将保存到本地计算机。

全部导出

1. 在 YARA 规则列表中，点击**导出**。
2. 在弹出的菜单中，选择**全部导出**，弹出<导出 YARA 规则>窗口。
3. 选择要导出的 YARA 规则严重级别。
4. 点击**导出**。
5. 所选的严重级别的 YARA 规则将全部保存到本地计算机。

编写 YARA 规则

YARA 规则由“规则名”和用于特征码模式匹配的“标识符”和“条件”组成。 标识符（strings）利用特殊字符（$）支持字符串、十六进制和正则表达式形式。条件（condition）以 Boolean 值表示结果。编写 YARA 规则的规则原型如下：

```
rule [YARA 规则名]
{
     strings:
        [标识符]

     condition:
        [条件]
}
```

标识符（strings）

- 字符串形式： ASCII 编码的文本需要使用双引号（""）括起来，并区分大小写。（如要转换为不区分大小写模式，请使用 nocase 修饰符 ）
- 十六进制形式：十六进制值需要使用大括号（ { }）括起来。
- 正则表达式形式：正则表达式需要使用斜杠（/ /）括起来。

条件（condition）

条件语法（syntax）必须使用标识符创建并表示为 Boolean 值。条件语法所有 C 语言运算符都可以使用条件语法使用的运算符。

可以使用的运算符如下：

- and, or, not, >=, <=, >, <, ==, !=, +, -, *, \, &, /, <<, >>, ~

一次将多个标识符应用于条件语法的规则如下：

- all of them：适用于所有标识符
- any of them：适用于其中至少一个标识符
- all of ($a*)：适用于以$a 开头的所有字符串
- any of ($a, $b, $c)：适用于$a, $b, $c 中的至少一个

YARA 规则编写案例

```
rule yara001                              // YARA 规则名
{

     meta:                 // 不影响 YARA 规则元数据，特征码模式匹配
        version = "1.0"
       author = "ahnlab"
       description = "yara test"
     strings:
       $string1 = "shutdown -r -t 0"  // 标识符：字符串形式
       $hex1 = { E2 00 [4-8] 34 FA}   //  标识符：十六进制形式
        $re1 = /[0-9a-z]{24}/          //  标识符：正则表达式形式
     condition:
        all of them                    // 条件：适用于所有标识符
}
```

5.6 响应设置

设置当检测到恶意文件、C&C 服务器和恶意 URL 时的响应方法。

自动响应设置

设置 MDS 检测到威胁时自动响应的方法。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 在自动相应设置部分，设置当检测恶意文件，访问 C&C 服务器和访问恶意 URL 时的响应方法。
   - 检测到恶意文件时：选择当检测到恶意文件时的处理方法。

- 删除文件：当检测到的恶意文件符合设置的条件（“已知/未知”和“严重级别”）时，删除该文件。
- 删除压缩文件：当检测到的恶意压缩文件的严重级别为“低”时，不管未知或已知，都将删除该文件。
- 隔离系统：当检测到的恶意文件符合设置的条件（“已知/未知”和“严重级别”）时，隔离该文件。
- 添加引入途径到黑名单：当检测到的恶意文件符合设置的条件（“已知/未知”和“严重级别”）时，将该恶意文件引入途径添加到黑名单。

- 当检测到访问 C&C 服务器时： 选择当检测到访问 C&C 服务器的行为时的处理方法。
  - 阻止网络：当检测到的访问 C&C 服务器的行为符合设置的条件（“已知/未知”和“严重级别”）时，阻止网络。
  - 隔离系统：当检测到的访问 C&C 服务器的行为符合设置的条件（“已知/未知”和“严重级别”）时，隔离系统。
- 当检测到访问恶意 URL 时：选择当检测到访问恶意 URL 的行为时的处理方法。
  - 阻止访问：当检测到的访问恶意 URL 的行为符合设置的条件（“已知/未知”和“严重级别”）时，阻止访问。
  - 隔离系统：当检测到的访问恶意 URL 的行为符合设置的条件（“已知/未知”和“严重级别”）时，隔离系统。

4. 点击**保存**。
5. 点击**应用更改配置**。

引入途径(URL) - 阻止访问设置

设置检测到引入途径(URL)时阻止的有效期间。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 在**引入途径(URL) - 阻止访问设置**部分，设置**阻止有效期间**。
   - 阻止有效期：可以选择 7 天、14 天或 30 天。在该期间，引入途径 URL 将被阻止访问。
4. 点击**保存**。
5. 点击**应用更改配置**。

阻止恶意 URL 选项

设置阻止恶意 URL 的详细。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 设置阻止恶意 URL 选项。可以选择重定向或弹出拦截信息。

- 重定向地址：选择单选按钮，然后输入重定向地址。当检测到访问恶意 URL 时，重定向其转向指定的网址。
- 拦截信息：选择单选按钮，然后输入警告信息。当检测到访问恶意 UR 时，拦截并显示警告信息。

4. 点击**保存**。
5. 点击**应用更改配置**。

系统隔离设置

设置系统隔离的详细。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 设置系统隔离的详细。
   - 自动解除：选择复选框启用自动解除功能，并输入隔离时间。当系统被隔离，经过该时间后自动解除隔离。
   - 允许 IP/域设置：设置允许访问的 IP/域。输入 IP 地址、域和描述，然后单击  。即使在系统被隔离的情况下，指定的 IP/域始终被允许访问。
4. 点击**保存**。
5. 点击**应用更改配置**。

5.7 黑名单

您可以通过黑名单来管理无法信任的文件、C&C 服务器、URL、电子邮件地址和数字签名。添加到黑名单的项目始终检测为恶意并拦截。

添加黑名单 - 文件(MD5)

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择**文件**，则出现<添加黑名单 - 文件(MD5)>界面。
4. 设置各项目。
   - 文件名：输入要添加到黑名单的文件名。
   - MD5：输入要添加到黑名单的文件的 MD5 值。具有该 MD5 值的文件将被拦截。最多可以输入英文数字组合的 32 个字符。
   - 处理方法：选择当检测到该 MD5 值时的处理方法。可以在**检测**或**删除**中选择。
   - 严重级别：指定添加到黑名单的文件的严重级别。可以在**高**、**中**、**低**中选择.

- 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。

5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 - C&C 服务器

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择 **C&C 服务器**，则出现<添加黑名单 - C&C 服务器>界面。
4. 设置各项目。
   - 类型：选择要添加到黑名单的 C&C 服务器的类型，可以在 **IP**、**域**和 **URL** 中选择。
   - 名称：输入要添加到黑名单的 C&C 服务器的名称。
   - C&C 服务器：根据选择的 C&C 服务器的类型，输入 C&C 服务器的 IP 地址、域或 URL。
   - 处理方法：选择当检测到该 C&C 服务器时的处理方法。可以选择**检测**或**删除**。
   - 严重级别：指定添加到黑名单的 C&C 服务器的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 -URL

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择 **URL**，则出现<添加黑名单 - URL>界面。
4. 设置各项目。
   - 名称：输入要添加到黑名单的 URL 的名称。
   - URL：输入要添加到黑名单的 URL。
   - 处理方法：选择当检测到该 URL 时的处理方法。可以选择**检测**或**删除**。
   - 严重级别：指定添加到黑名单的 URL 的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。

6. 点击**应用更改配置**。

添加黑名单 - 电子邮件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择**电子邮件**，则出现<添加黑名单 - 电子邮件>界面。
4. 设置各项目。
   - 分类：选择要添加到黑名单的电子邮件地址类型。
   - 名称：输入要添加到黑名单的电子邮件名称。
   - 电子邮件地址：输入要添加到黑名单的电子邮件地址，根据选择的类型，输入发件人地址或收件人地址。
   - 严重级别：指定添加到黑名单的电子邮件的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 -数字签名

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择**数字签名**，则出现<添加黑名单 - 数字签名>界面。
4. 设置各项目。
   - 签名：输入要添加到黑名单的签名。
   - 严重级别：指定添加到黑名单的数字签名的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

导入/导出黑名单

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 执行以下操作。
   - 要导入列入黑名单的列表，单击**导入**后选择类型（文件(MD5)、C&C、URL、电子邮件和数字签名），在弹出的导入界面单击**浏览**选择导入的文件。
   - 要导出黑名单，单击**导出**后选择类型（文件(MD5)、C&C、URL、电子邮件和数字签名），将导出的文件保存到本地系统中。

5.8 白名单

您可以通过白名单来管理可信任的文件、C&C 服务器、URL 和电子邮件地址。添加到白名单的项目将被排除在恶意软件扫描和检测之外。

添加白名单 - 文件(MD5)

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择**文件**，则出现<添加白名单 - 文件(MD5)>界面。
4. 设置各项目。
   - 文件名：输入要添加到白名单的文件名。
   - MD5：输入要添加到白名单的文件的 MD5 值。具有该 MD5 值的文件将被允许。最多可以输入英文数字组合的 32 个字符。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - C&C 服务器

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择 **C&C 服务器**，则出现<添加白名单 - C&C 服务器>界面。
4. 设置各项目。

- 类型：选择要添加到白名单的 C&C 服务器的类型，可以在 **IP**、**域**和 **URL** 中选择。
- 名称：输入要添加到白名单的 C&C 服务器的名称。
- C&C 服务器：根据选择的 C&C 服务器的类型，输入 C&C 服务器的 IP 地址、域或 URL。
- 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。

5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 -URL

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择 **URL**，则出现<添加白名单 - URL>界面。
4. 设置各项目。
   - 名称：输入要添加到白名单的 URL 的名称。
   - URL：输入要添加到白名单的 URL。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - 电子邮件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择**电子邮件**，则出现<添加白名单 - 电子邮件>界面。
4. 设置各项目。
   - 类型：选择要添加到白名单的电子邮件地址类型。
   - 名称：输入要添加到白名单的电子邮件名称。
   - 邮件地址：输入要添加到白名单的电子邮件地址，根据选择的类型，输入发件人地址或收件人地址。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 -数字签名

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择**数字签名**，则出现<添加白名单 - 数字签名>界面。
4. 设置各项目。
   - 签名：输入要添加到白名单的签名。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - Snort 规则 ID

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择 **Snort 规则 ID**，则出现<添加白名单 - Snort 规则 ID>界面。
4. 设置各项目。
   - Snort 规则 ID：输入要添加到白名单的 Snort 规则 ID。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

导入/导出白名单

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 执行以下操作。
   - 要导入列入白名单的列表，单击**导入**后选择类型（文件(MD5)、C&C、URL、电子邮件、数字签名、Snort 规则 ID），在弹出的导入界面单击**浏览**选择导入的文件。
   - 要导出白名单，单击**导出**后选择类型（文件(MD5)、C&C、URL、电子邮件、数字签名、Snort 规则 ID），将导出的文件保存在系统中。

5.9 检测例外

设置检测例外 IP/域，被视为白名单，即使可能会产生可疑流量（包括访问异常或恶意文件）也不会被检测到。

添加检测例外 IP/域 - 文件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 点击**添加**键，选择**添加检测例外 IP/域 - 文件**，则出现<添加检测例外 IP/域- 文件>界面。
4. 选择类别，可以选择 **IP 地址/网络掩码**或**域**。
5. 类别选择“IP 地址/网络掩码”时，输入以下项目：
   - 源 IP 地址：输入 IP 地址和网络掩码。IP 地址可以输入 IPv4 或 IPv6 格式。
   - 目标 IP 地址：输入目标 IP 地址和网络掩码。IP 地址可以输入 IPv4 或 IPv6 格式。
   - 条件：选择“AND”或“OR”。如果选择“AND”，必须同时满足输入的源 IP 地址和目标 IP 地址，才将其处理为检测例外；如果选择“OR”，仅满足源 IP 地址和目标 IP 地址之一，也会将其处理为检测例外。
   - 输入描述：输入最多 63 字符的描述。
6. 类别选择“域”时，输入以下项目：
   - 域：输入域。
   - 地址：输入域地址。
   - 输入描述：输入最多 63 字符的描述。
7. 点击**确定**。
8. 点击**应用更改配置**。

更改检测例外 IP/域 - 文件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 鼠标双击列表中的欲更改项目，打开<更改检测例外 IP/域 - 文件>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除检测例外 IP/域 - 文件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 在列表中选择欲删除项目左侧的 ❌，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

添加检测例外 IP - 异常流量

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 点击**添加**键，选择**检测例外 IP - 异常流量**，则出现<添加检测例外 IP- 异常流量>界面。
4. 设置各项目。
   - 地址：输入对异常流量检测例外的 IP 地址和网络掩码。
   - 输入描述：输入最多 63 字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改检测例外 IP - 异常流量

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 鼠标双击列表中的欲更改项目，打开<更改检测例外 IP - 异常流量>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除检测例外 IP - 异常流量

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 在列表中选择欲删除项目左侧的 ❌，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

导入/导出检测例外 IP

如果要一次添加两个以上的项目，可以编写列表以将其添加到 csv 文件中，然后单击**导入**。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 执行以下操作。
   - 要导入列入检测例外的列表，单击**导入**后选择类型（文件或异常流量），在弹出的导入界面单击**浏览...**选择要导入的文件。
   - 要导出检测例外列表，单击**导出**后选择类型（文件或异常流量），将导出的文件保存在系统中。

以下是在 csv 文件中写入检测例外 IP 列表的方法。

项目为“文件”的时，写入示例如下：

第一列：IP 地址或域	第二列：条件	第三列：描述	第四列：类别
1.2.3.4/1~22.3.4.5/2	AND	ddd	IP 地址/网络掩码
1.2.3.4/2~1.3.4.5/4	OR	ccc	IP 地址/网络掩码
ahnlab.com		abc	域

项目为“异常流量”时，写入示例如下：

第一列：IP 地址	第二列：描述	第三列：类别
1.2.3.4/1	ddd	IP 地址/网络掩码

5.10 更新

本章介绍引擎更新设置和立即更新的方法，还有固件和虚拟机的更新方法，使维持最新的版本，以便及时响应安全威胁和紧急情况。设置更新周期进行更新或者由管理员直接点击**立即更新**即可。在进行更新之前，先检查一下 设备是否已连接到互联网。

引擎更新

自动更新设置

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 配置引擎的更新设置。选择**自动更新**复选框，然后输入**更新间隔**。
4. 点击**保存**。

参考

各引擎在 MDS 设备执行的功能如下：
- C&C 服务器数据库：检测 C&C 服务器的访问。
- 文件 DNA：通过使用本地引擎或向云引擎发送查询来分析文件的数字 DNA 信息，检测和防止未知的恶意软件。
- 恶意 URL 数据库：检测和阻止恶意网站。
- 非执行型文件分析引擎：用于分析非执行型文件（Non-PE），如 RTF, OLE(DOC, XLS, PPT), OOXML(DOCX, XLSX, PPTX), PDF 等。
- 动态平台引擎：显示动态分析引擎相关的更新信息。
- MDP 引擎：执行多维度的分析，从已知和未知的恶意软件中保护系统。执行基于行为的检测和基于特征码的检测，还通过基于信誉的分析和主动防御来提供恶意软件检测率和准确性。
- DICA 引擎：执行动态智能内容分析，可以准确检测利用 MS Office、PDF 及 Hangul 等程序存在的漏洞入侵的非执行型（non-PE）恶意软件。它还可以检测和防止零日漏洞攻击。
- 内存扫描引擎：执行内存扫描。

立即更新

点击**立即更新**（  ），不管更新间隔立即执行更新。

手动更新

点击静态分析引擎或动态分析引擎的**浏览**，弹出手动更新对话框，点击**浏览...**选择更新文件或将文件拖放到此窗口，然后点击**确定**。

参考

手动更新主要在封闭网络环境中使用，如果不是封闭的网络，建议使用自动更新。

在封闭的网络环境中引擎更新设置

如果在封闭的网络环境中使用 MDS，则很难做到在典型的网络环境中那样自动更新静态和动态分析引擎。虽然可以通过跨网解决方案对特定 IP 和端口进行更新，但实际上不可能将所有正在使用的 IP 地址跨网连接。为解决这个问题，MDS 提供了手动更新的方法。然而，手动更新麻烦，而且无法即时将引擎更新为最新版本，因此不足以应对最新的安全威胁。因此，MDS 提供 MDS Manager 来充当更新服务器，通过 MDS Manager 自动更新引擎。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 选择**使用 MDS Manager 作为更新服务器**复选框，然后输入 **MDS Manager IP 地址**和**端口号**。
4. 点击**保存**。

固件升级

您可以升级固件。如要升级固件，请联系 AhnLab 或供应商。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 点击固件区的**浏览...**，弹出<固件更新>窗口。
4. 点击固件文件的**浏览...**，选择 AhnLab 提供的固件文件。固件文件的扩展名为“enc”。选择固件文件后，点击哈希文件的**浏览...**，选择该固件文件的哈希文件。
5. 点击**确定**。
6. 完成更新后，需要重启设备。如果出现确认设备重新启动的对话框，请单击**是**。

虚拟机(VM)更新

更新虚拟机以进行恶意软件动态分析。在上传到 MDS 设备的虚拟环境中运行并分析扫描对象。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 可以确认虚拟机的当前版本、最新更新时间。MDS 支持 Windows XP（32 位）、Windows 7（32/64 位）和 Windows 10（64 位）镜像。
4. 如要更新虚拟机，点击虚拟机区的**浏览...**，弹出<虚拟机(VM)更新>窗口。
5. 点击虚拟机镜像文件的**浏览...**，选择虚拟机镜像文件。
6. 点击哈希文件的**浏览...**，选择哈希文件。
7. 点击**确定**。

参考

如果虚拟机更新失败，则原因可能如下：
-没有图像文件或哈希文件
-哈希值不匹配
-文件解压缩失败
-文件解密失败
-图像转换失败

参考

本产品支持用户自定义的 Windows 系列 32 和 64 位虚拟机环境，创建的虚拟机镜像文件和哈希文件可以通过 Web 管理界面上传到 MDS 服务器。有关创建自定义虚拟机的方法，请参考虚拟机 VirtualBox·安装 win 10 完整步骤。

5.11 默认设置

配置管理 Agent 相关的基本设置，安全有效管理网络上的主机，并从各种安全威胁中保护主机。

Agent 默认设置按如下操作：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 默认设置**。
3. 配置管理 Agent 的 MDS 服务器。
   - Agent 管理服务器 IP：输入管理 Agent 的 MDS 服务器的 IP 地址。

参考

根据操作环境，MDS 可以与单独的 MDS Manager 联动。此时，Agent 由 MDS Manager 管理，因此需要输入 MDS Manager 的 IP 地址作为 Agent 管理服务器 IP 地址。

4. 设置安装 Agent 程序相关的选项，以管理未安装 Agent 程序的主机。
   - 重定向：选择复选框启用“网页重定向”功能。当未安装 Agent 的主机请求访问互联网时，将重定向其转向 MDS Agent 安装向导网页。

参考

如果重定向 Agent 安装网页不启动，请点击**删除安装信息缓存**以删除 Agent 计算机的缓存。当缓存被已删除，将重新收集 Agent 安装信息，并执行重定向安装 Agent 网页。

   - 安装网页：输入 MDS Agent 安装网页的网址。
   - 以静默模式安装 Agent：选择复选框，启用静默模式安装 Agent。
   - 输入 PIN 代码时允许删除 Agent：点击**[生成 PIN 码]**，弹出<生成 PIN 码>对话框。输入 Agent 验证码后点击**生成**键。

参考

当应用“输入 PIN 码时允许删除”策略的 Agent 请求删除时，生成 PIN 码并转达。

5. 设置 Agent 执行 MDS 发送的命令相关的选项。
   - 命令有效时间：选择 MDS 发送命令到 Agent 的有效时间。
   - 使用性能控制：选择复选框，则当 Agent 执行 MDS 发出的命令时，控制使用最低的 CPU。

参考

如果 Agent 没有在命令有效期内通知 MDS 执行命令的结果，MDS 将处理为命令执行失败。

6. 设置**通过 Agent 删除文件**相关的选项。当 MDS 检出 Agent 的恶意代码时，可以发出删除命令。Agent 则根据下面的设置，删除文件。
   - 区域：选择 Agent 执行删除命令时可以删除的区域。

- 删除时提醒：选择复选框，则在执行删除命令时，通过弹窗提醒用户。

参考

从 MDS Agent 2.2.7 及更高版本开始，遵循[Agent 策略 > 提示设置]中的“删除文件时提示”选项的设置。

7. 设置收集 Agent 可疑文件的手动收集范围和自动收集方法。
   - 手动收集范围：从下拉框中选择收集可疑文件的范围。
   - 自动收集：选择复选框，然后设置自动收集方法。自动收集方法可以选择“计划收集”或“实时收集”。
     - 计划收集：在指定的时间收集可疑文件。选择收集范围和收集对象并指定收集时间，然后点击  。
     - 实时收集：通过 Agent 实时收集可疑文件。
8. 点击**保存**。
9. 点击**应用更改配置**。

5.12 策略设置

配置应用于 Agent 的策略。

Agent 策略列表

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 显示 Agent 策略列表，可以查看如下信息。
   - 策略名：显示 Agent 策略名称。
   - 策略应用组：显示策略应用的 Agent 组名称。
   - 描述：显示该策略的描述。
   - 应用状态：显示 Agent 应用策略的状态。
   - 策略创建时间：显示策略创建的时间。
   - 最近更改时间：显示策略最近更改的时间。

新建 Agent 策略

创建 Agent 策略按如下步骤进行。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 点击**添加**键，弹出<新建 Agent 策略>窗口。
4. 设置**策略名**标签下面的各项目。
   - 策略名：输入新建的策略名称。
   - 应用组：选择要应用新建策略的 Agent 组。
   - 描述：输入有关新建策略的描述。
5. 点击**下一步**或**默认设置**标签。
6. 设置**默认设置**标签下面的个项目。
   - 删除 Agent：设置是否允许删除主机上安装的 Agent 程序。
     - 允许删除：选择此选项，则允许删除 Agent。
     - 输入 PIN 代码时允许删除：选择此选项并输入 6 位 PIN 代码，则当删除 Agent 时要求输入 PIN 代码。
     - 不允许删除：选择此选项，则不允许删除 Agent。
   - 在任务栏中显示 MDS Agent：选择复选框，则在 Agent 的任务栏中显示 MDS Agent 图标。
   - 联动 Agent：选择此选项可在您同时安装了 APC Agent、V3 和 MDS Agent 时，可以使用统一 Agent 而不是使用每个 Agent。当选择使用 APC Agent 托盘图标时，可以通过 APC Agent 转发 MDS Agent 的通知，并从任务栏中隐藏 MDS Agent 的托盘图标。
   - 在 Agent 弹窗中显示消息：如要在 Agent 上发生的所有的弹出窗口中显示管理员引导用户的文本，请选择该选项并输入文本内容。文本内容最大不能超过 75 字节。示例：[咨询]联系人：OOO（安全小组） 电话：OOO）
   - 自我保护：选择此选项，可防止用户或其他进程强制关闭或重新启动 Agent 进程，并防止篡改注册表信息。
     - 阻止产品由 rootkit 等其他程序强制结束：选择此选项，可以防止被 rootkit（被视为一种外部程序）强制终止 Agent。
   - 更新 Agent：选择此选项，从 MDS 检查 Agent 的最新版本，并在分发新版本时是否自动更新 Agent。
     - 更新间隔：输入 Agent 更新间隔时间。Agent 根据指定的间隔时间从 MDS 检查 Agent 程序的最新版本，如果已发布新版本，则进行更新。
   - 扫描进程内存：选择此选项，则使用扫描进程内存策略。
     - 自动修复：扫描后，自动修复内存。

    - 传输日志到服务器：扫描后，将结果日志传输到服务器。
- 策略更新间隔：输入 Agent 策略更新间隔时间。Agent 根据指定的间隔时间从 MDS 检查 Agent 策略并应用。
- 隔离区大小：输入隔离区空间的最大大小。隔离区是隔离并存储由 Agent 删除的恶意代码的空间。（默认值：100MB）
- 备用服务器 IP 地址： 输入服务器连接失败时的备用 IP 地址。
- 组密钥：从下拉框中选择策略应用组密钥。
- 联动 MDS：选择复选框，并输入下面各项目。
    - 设备 IP 地址：输入要联动的 MDS 设备的 IP 地址。
    - 备份设备 IP 地址：输入备份设备的 IP 地址。

参考

Agent 策略设置中的 MDS 联动具有比 Agent 管理服务器中的 MDS 联动设置更高的优先级。

7. 点击**下一步**或**运行保留**标签。
8. 设置**文件运行保留**标签下面的各项目。
    - 启用文件运行保留（Execution Holding）：选择此选项可将策略设置为暂时不运行未判断恶意与否的可执行文件。
    - 基本扫描（可执行文件）：设置对可执行文件的扫描的各种选项。保留可执行文件的运行，并检查恶意与否。
        - 扫描对象：输入要扫描的可执行文件的创建时间。（默认值：60 分钟）
        - 等待时间：输入在分析可执行文件的时等待响应的时间。（默认值：5 秒）
            - 超过等待时间时：选择当超过等待时间时的处理方法，可以选择**阻止运行**、**允许运行**和**用户选择**。
        - 连接 MDS 服务器出现问题时：选择当连接 MDS 服务器出现问题而无法分析文件时的处理方法，可以选择**禁用**、**阻止运行**、**允许运行**和**用户选择**。
        - 保存 Agent 缓存：选择此选项，可将运行保留的文件分析结果以 Agent 缓存保存以供用在后续分析。使用 Agent 缓存分析可以减少分析时间。
            - Agent 启动时删除缓存：选择此选项，则删除每次 Agent 服务启动时保存的缓存，以减少服务器负载。此设置可以独立于“保存 Agent 缓存”和“缓存删除间隔”设置。
            - 缓存删除间隔：输入 1 到 24 小时之间的整数。例如，输入 3 的话，每隔 3 小时删除保存的 Agent 缓存。
        - 传输到 MDS 服务器的文件的最大大小：设置 Agent 发送文件到服务器的最大文件大小。最大可以设置 300MB，默认值为 3MB。
9. 点击**下一步**或点击**文件运行保留高级设置**标签。
    - 禁用：选项此选项，则不使用文件运行保留高级设置。

- 高级扫描（包括 Dropper 文件 - 不可执行文件）：设置对不可执行文件的运行保留的各种选项。
  - 包括由 Rundl 执行的 DLL：选择此选项，保留由 Rundll 执行的 DLL 文件的运行。
  - 其他扫描对象：设置不可执行文件的扫描对象。各项目最多可以输入 512 字节。
    - 不可执行文件扩展名： 输入执行扫描的不可执行文件扩展名。（默认值：pdf/doc/ppt/xls/docx/pptx/xlsx/rtf/hwp/gul）
    - 不可执行文件的执行进程名： 输入执行扫描的不可执行文件的执行进程名。（默认值：acrord32.exe, winword.exe, powerpnt.exe, excel.exe, hwp.exe, jungumgw.exe）
    - 不可执行文件的保存进程名：输入执行扫描的不可执行文件的保存进程名。（默认值：iexplore.exe, chrome.exe, firefox.exe, outlook.exe, v3zip.exe, alzip.exe, 7zg.exe, winrar.exe）
- 运行后扫描（包括 Dropper 文件 - 不可执行文件）：运行文件后对其进行扫描，如果该文件是恶意的，则将结果通知给用户。
  - 其他扫描对象：设置运行后扫描的文件的扫描对象。如同上述。

10. 点击**下一步**或点击**文件运行保留例外**标签。

- 非扫描区域（文件夹）：选择复选框，可以添加运行保留例外的非扫描区域的文件夹。输入**文件夹路径**和**描述**，然后点击 。最多可以添加 64 个。
- 非扫描区域（文件）：选择复选框，可以添加运行保留例外的非扫描区域的文件。输入 16 进制 32 字节的文件**哈希值**（MD5 值）和**描述**，然后点击 。最多可以添加 128 个。
- 非扫描区域（文件签名）：选择复选框，可以添加运行保留例外的非扫描区域的文件签名。输入**文件签名**和**描述**，然后点击 。文件签名长度最大不能超过 64 字节，且不允许输入特殊字符（`）。最多可以添加 64 个。

11. 点击下一步或点击**检测**标签，设置下面的项目。

- 检测对象及响应方法
  - 文件异常运行：选择是否检测文件的异常运行以及检测到文件异常运行时如何响应。
  - 文件异常下载：选择是否检测文件的异常下载以及检测到文件异常下载时如何响应。
  - 后门程序：选择是否检测后门程序的运行以及检测到后门程序运行时如何响应。
  - 浏览器异常提升权限：选择是否检测浏览器的异常提升权限行为以及检测到浏览器异常提升权限时如何响应。
- 拦截例外：对于下面设置的进程或 URL/IP 地址，及时检测到也不拦截。启用**拦截例外**复选框，选择**进程**或 **URL/IP 地址**，然后根据选择的类别输入**可执行文件名称**或 **URL/IP 地址**和**描述**，然后点击 。最多可以添加 128 个。

12. 点击**下一步**或点击**提示设置**标签，设置下面的各项目。

- 全选：选择复选框，下面的选项将被全选。
- 弹出最终用户许可协议（EULA）提示对话框：选择此选项，则弹出最终用户许可协议提示对话框。
- 弹出可疑文件收集同意提示对话框：选择此选项，则 Agent 在收集可疑文件之前向 Agent 计算机用户询问是否同意数据收集。
- 弹出文件运行保留提示对话框：当文件运行保留后等待时间超过指定的时间时，弹出提示对话框使用户选择响应方法。
  - 隐藏允许文件运行选项：当弹出文件运行保留提示对话框时，无论扫描结果如何，都会隐藏允许文件运行选项。
- 显示气球帮助提示窗口：以气球帮助形式显示对诊断文件的信息。
- 删除文件时提示：选择此选项，则删除文件时出现提示窗口，用户确认后将其删除。
- 恢复文件时提示：选择此选项，则恢复文件时出现提示窗口，用户确认后将其恢复。

13. 点击**确定**。

参考

即使不选择**保存 Agent 缓存**选项，以前保存的缓存也将继续用于文件分析。如果对文件的分析结果发生变化，通过 CLI 命令执行删除缓存，使可以应用新的分析结果分析文件。

参考

当您运行可疑文件收集命令时，Agent 会在开始收集可疑文件之前向 Agent PC 用户显示收集数据同意提示对话框。用户同意后，才可以进行可疑文件收集。

更改 Agent 策略

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 鼠标双击列表中的欲更改项目，打开<更改 Agent 策略>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 Agent 策略

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 在列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

5.13 安装 IP 地址

设置使用“引导安装 Agent 网页”重定向功能的网络，当未安装 Agent 的主机尝试连接互联网时，重定向其转向安装 Agent 网页。有关引导安装 Agent 的详细内容，请参考 Agent 默认设置。

添加安装 IP 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 安装 IP 地址**。
3. 点击**添加**键，弹出<添加安装 IP 地址>窗口。
4. 设置各项目。
   - IP 地址：输入安装 Agent 程序的 IP 地址和网络掩码。
   - 输入描述：输入有关安装 Agent IP 的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除安装 IP 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 安装 IP 地址**。
3. 在列表中选择欲删除项目 左侧的 ❌，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

5.14 补丁集

将最新版本的 Agent 修补程序和签名文件上传到服务器，使 MDS 再分发给主机。

> **参考**
>
> 有关将上传的最新版本的修补程序文件和签名文件通过命令分发到 Agen 的说明，请参阅 Aennt 列表的响应命令。

上传 Agent 修补程序文件和签名文件的步骤如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 补丁集**。
3. 点击 Agent 修补程序文件的**浏览...**，选择修补程序文件。
4. 点击签名文件的**浏览...**，选择签名文件。

5. 点击**上传**。
6. 点击**应用更改配置**。

参考

如要应用 Aent 补丁集，请同时上传 Agent 修补程序文件和签名文件。

参考

如果 Agent 修补程序或签名文件有问题，或者上传时发生错误，则会在上传进度屏幕上显示弹出消息。

5.15 安装 MDS Agent

在主机上安装 Agent 程序，以执行 MDS 发出的命令。主机安装 Agent 程序才可以使用 MDS 提供的恶意代码检测、发送通知和文件运行保留（Excution Holding）功能。

安装 MDS Agent 的步骤按如下：

1. 登录到 MDS 的 Web 管理界面，设置与 Agent 相关的所有配置。有关 Agent 相关的设置，请参考 Agent 列表、Agent 默认设置、Agent 策略、安装 Agent 网络、安装 Agent 网络例外和上传 Agent 补丁集。
2. 打开网页浏览器，地址栏里输入下载安装 Agent 程序的网址。形式如下：https://MDS 服务器 IP 地址:端口号。（示例：https://192.1.1.1.:8290）
3. 出现下载 MDS Agent 安装文件的界面。点击下载，下载 Agent 程序安装文件。
4. 运行安装文件，打开安装向导，安装 Agent。
5. 安装结束后，主机的任务栏里将显示图标（  ）。

5.16 安装 MDS-V3 统一 Agent

在同时提供 V3 和 MDS 的环境中，通过统一安装文件一次安装每个 Agent。

参考

统一安装文件只是一次安装 V3 Agent 和 MDS Agent，不会集成每个 Agent 的托盘图标。如要整合使用 V3 Agent 和 MDS Agent 托盘图标，请到**管理 > Agent > Agent 策略**中，请启用**使用 V3-MDS 统一 Agent** 选项。

如要安装统一 Agent，请考虑以下事项：

- 统一安装不支持通过 Web 引导安装 Agent 功能
- 不支持 V3 8.0 或更早版本
- V3 9.0 仅支持在 Windows Vista、Windows 7、Windows 8、Windows 10 等操作环境中安装

- 如果 V3 安装失败，则 Agent 集成安装也将中止，MDS Agent 安装也将中止。

安装统一 Agent

安装统一 Agent 的步骤按如下：

1. 运行统一安装文件。
2. 在安装向导中，单击“**安装**”并继续 V3 安装。
3. 成功安装 V3 后，将自动安装 Agent。
4. 完成 V3 和 MDS Agent 的安装后，单击**完成**。

5.17 控制台连接并登录

MDS 提供一个 Web 管理界面和一个终端界面用于管理访问。终端接口可以通过串口或 SSH 协议进行连接。

参考

通过串行端口的控制台连接，请参考“安装指南”中的**初始控制台连接**。

通过 SSH 连接控制台

使用指定为管理端口的 IP 地址连接到控制台。有关管理端口的指定，请参考“安装指南”的**初始登录及管理员设置**。 并且需要一个终端客户端，如支持 SSHv2 的 Putty、SecureCRT 和超级终端。

1. 将管理员计算机的 IP 地址更改为**初始登录及管理员设置**中注册的 IP 地址。
2. 运行终端客户端，输入 MDS 的 IP 地址和端口号（22）并进行连接。
3. 当出现登录提示符，输入管理员 ID。
4. 当出现输入密码的提示符，输入管理员密码，然后按 Enter 键。
5. 如果登录成功，则输出#>提示符。

参考

请保存连接设置。大部分的终端客户端软件提供保存连接设置信息的功能。

参考

如果韩文输出异常，请将终端客户端的编码设置更改为 EUC-KR。如果您不需要韩文输入和输出，请使用 UTF-8。

第6章　仪表板展示说明

6.1　摘要

仪表板的第一个菜单“**摘要**”显示今天、过去 24 小时、过去 7 天和过去 14 天的所有系统的安全水平、文件引入和分析情况以及最近检测到的文件、异常流量和恶意 URL 情况。

参考

在屏幕的右上方的选择框中，您可以选择**今天**、**过去 24 小时**、**过去 7 天**和**过去 14 天**查看信息。单击**刷新**()实时更新数据以查看最新的信息。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**摘要**。
3. 可以查看如下信息。
   - 攻击阶段：显示选择期间的第一阶段攻击（攻击尝试）、第二阶段攻击（攻击引入）、第三阶段攻击（C&C 服务器）和第四阶段攻击（数据泄漏）检测到的威胁的统计数据。
   - 动态分析情况：显示动态分析情况。
     - 待分析：显示正在等待动态分析的对象数量。点击待分析数，则弹出<动态分析情况>界面，显示待分析对象列表，可以确认分析对象的详细信息，如分析对象文件名，文件类型，文件大小和收集时间。
     - 正在分析：显示正在进行动态分析的对象数量。点击正在分析数，则弹出<动态分析情况>界面，显示正在进行分析的对象的详细列表。如分析对象文件名，文件类型，文件大小和分析所需时间。
     - 分析完成：显示已完成分析的对象的数量。
   - 按严重级别的检测趋势：按严重级别显示检测到的恶意文件、异常流量和恶意 URL 趋势。
   - 最近检测到的恶意文件：显示最近检测到的排名前五位的恶意文件的名称、类型和大小。
   - 最近检测到的异常流量：显示最近检测到的排名前五位的发生异常流量的 IP 地址、协议和端口号。
   - 最近检测到的恶意 URL：显示最近检测到的排名前五位的恶意 URL 的地址和国家信息。

参考

C&C 服务器（Command & Control Server, 攻击命令服务器）是一个远程控制服务器，用于命令和控制受感染的僵尸 PC 执行攻击者期望的攻击。主要发出的命令有恶意代码分发，网络钓鱼，垃圾邮件 DDoS 攻击等。

参考

点击各图表标题旁边的**设置**(⚙)，可以指定显示威胁的严重级别和未知/已知状态。要想始终重点监控特严重级别的威胁情况，先在**显示设置**中选择严重级别，然后必须打勾**保持严重级别显示设置**前面的复选框。如果未选中此功能，当您刷新或转到另一页面再返回到仪表板时，显示设置将被重置。

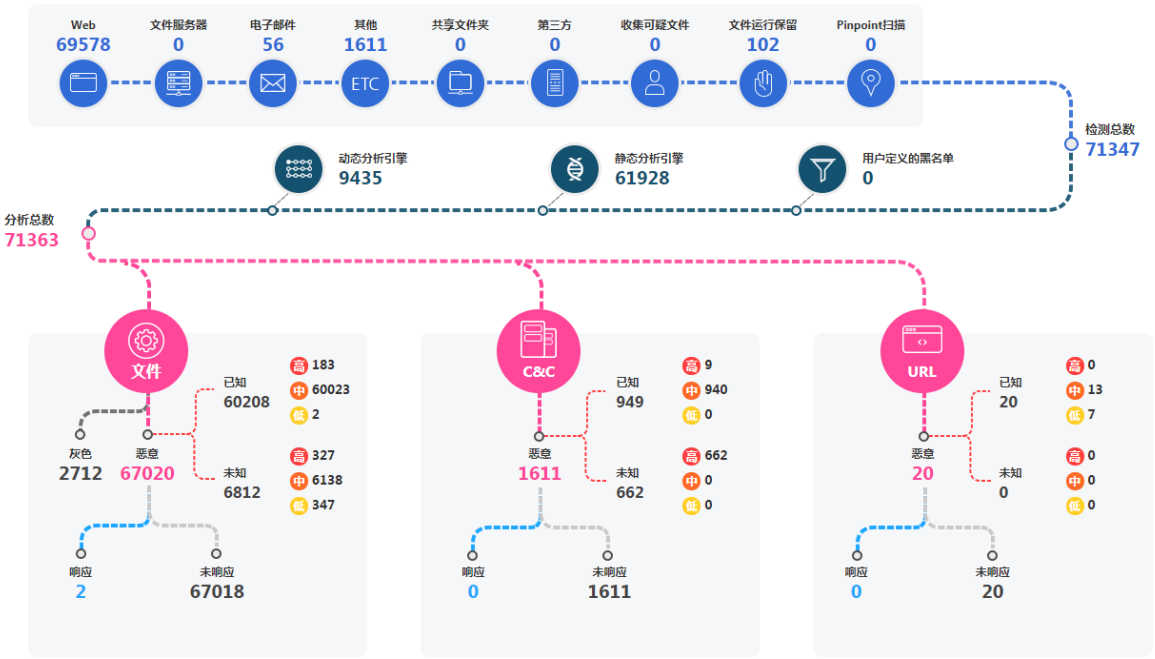
6.2 威胁趋势

仪表板的第二个菜单“威胁趋势”以图表形式显示通过 MDS 检测到的威胁的整体情况。

参考

在屏幕的右上方的选择框中，您可以选择**最近 24 小时**、**最近 7 天**和**最近 14 天**查看信息。单击**刷新**(🔄)实时更新数据以查看最新的信息。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**威胁趋势**。
3. 出现<威胁趋势>界面，可以查看威胁检测、分析和结果等整体情况。



- 检测总数：显示通过 Web、文件服务器、电子邮件、共享文件夹、第三方软件、收集可疑文件、运行保留和 Pinpoint 检测等途径和手段检测到威胁的总数。
- 分析总数：通过 MDS 提供的引擎和策略分析威胁的总数。
- 文件/C&C/URL：显示分析结果的各统计数据。首先显示判断为恶意的威胁数（文件还显示“灰色”状态的威胁数）；恶意再分为“已知”和“未知”威胁；已知和未知威胁再根据严重级别分为“高”、“中”、“低”显示各级别的威胁数。最后，显示对分析结果 MDS 响应和未响应的威胁数量。

6.3 监视对象

仪表板的第三个菜单“**监视对象**”界面可以管理设置为监视对象的**文件(MD5)**和**主机 IP**。管理员可将经常被发现的可疑文件(MD5)或相对容易受到安全威胁攻击的主机 IP 设置为监视对象，并将其配置为在检出威胁时自动响应。此外，可以根据管理员的判断将一些特定文件(MD5)和主机 IP 设置为监视对象后进行监视和快速响应，从而防止整个系统发生安全威胁。

参考

在屏幕的右上方的选择框中，您可以选择**最近 24 小时**、**最近 7 天**和**最近 14 天**查看信息。单击**刷新**()实时更新数据以查看最新的信息。

要更好地了解监视对象的概念和配置，您需要先正确了解仪表板的其他菜单和相关功能。与此相关的详细说明，请参考以下内容。

- 仪表板的其他菜单的内容：摘要, 威胁趋势
- 响应结果相关的内容： 响应情况, 隔离区, 隔离系统, 统计

监视对象 - 文件(MD5)

在监视对象界面无法将文件(MD5)添加为新的监视对象，您只可以查看和管理已设置为监视对象的文件(MD5)。如要将特定的文件(MD5)设置为监视对象，请到<检测情况>界面中确认文件后添加为监视对象。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**文件(MD5)**。
4. 显示设置为监视对象的文件(MD5)列表。可以确认如下的文件信息。
   - MD5：显示文件的固有哈希值 MD5 值，根据 MD5 值来标识恶意代码。
   - 自动响应：当检测到具有该 MD5 值的文件时的自动相应方式。
     - 删除文件：删除检测到的文件。
     - 隔离系统：拦截持有该恶意文件的 Agent 的网络使用。
   - 检测次数：显示检测到该文件的次数。

参考

仅包含检测结果为“可能正常”以上的严重级别。

   - 删除次数：显示删除该文件的次数。
   - 隔离次数：显示隔离持有该文件的 Agent 系统的次数。
   - 文件名：显示文件名。

- 文件类型：显示文件的扩展名。
- 文件大小：显示文件的大小。
- 严重级别[U/K]：显示文件的严重级别和未知（Unknown）/已知（Known）状态。
  - 高[U]：这意味着高风险和未知的恶意代码。
  - 高[K]：这意味着高风险和已知的恶意代码。
  - 中[U]：这意味着中等风险和未知的恶意代码。
  - 中[K]：这意味着中等风险和已知的恶意代码。
  - 低[U]：这意味着较低风险和未知的恶意代码。
  - 低[K]：这意味着较低风险和已知的恶意代码。
  - 灰色 2：这意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。
  - 灰色 1：这意味着虽然不是恶意，但需要检查。
  - 可能正常：分析结果为正常，且是一个未知的文件。
  - 正常：正常或是由管理员添加到白名单的文件。
- 诊断名：显示文件被检出的诊断名。
- 最近检测时间：显示文件最近被检出的时间。

5. 单击 **MD5** 值，可以查看该文件的详细分析内容。

参考

如果设置为监视对象的文件被检出威胁，则在**检测情况>文件**中，MD5 值标记监视对象图标（）。

添加监视对象 - 文件(MD5)

在<监视对象>界面中，您可以更改监视对象文件的自动响应方式，或从监视列表中删除文件，但无法添加新的监视对象文件。要将文件添加为监视对象，请在**检测情况 > 文件**中选择所需的文件后单击**响应**，从弹出的菜单中选择**添加为监视对象**。有关详细的说明，请参考文件检测情况。

更改监视对象 - 文件(MD5)

可以更改对监视对象文件的自动响应方式。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**文件(MD5)**。
4. 出现监视对象-文件列表。
5. 鼠标双击欲更改的文件，弹出<更改监视对象-文件(MD5)>。
6. 更改所需的项目。

7. 点击**确定**。

删除监视对象 - 文件(MD5)

当不再需要监视已设置为监视对象的文件时，可以从监视对象列表中删除该文件。

> **参考**
> 删除监视对象不会删除文件本身，而是将其从监视对象列表中除去。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**文件(MD5)**。
4. 出现监视对象-文件列表。
5. 在列表中选择欲删除项目左侧的 或**删除**键，弹出删除对话框。
6. 如果弹出确认删除的对话框， 点击**确定**。

监视对象 - 主机 IP

监视对象-主机 IP 列表中可以确认如下的信息。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**主机 IP**。
4. 显示设置为监视对象的主机 IP 列表。可以确认如下的主机信息。
   - 主机 IP：显示主机的 IP 地址。
   - 检测次数：显示在该主机 IP 上检测到威胁的次数。
   - 攻击尝试：显示在该主机 IP 上检测到尝试攻击的次数。
   - 攻击引入：显示在该主机 IP 上检测到攻击引入的次数，分为“一般”、“C&C(VM)”和“数据泄漏(VM)”显示。
   - C&C 服务器：显示在主机 IP 上发现的 C&C 服务器的 IP 地址。
   - 数据泄漏：显示在主机 IP 上检测到的数据泄漏次数。
   - 严重级别[U/K]：显示在主机 IP 上检测到的威胁的严重级别和已知/未知状态。
   - 诊断名：显示在主机 IP 上检测到的威胁的诊断名。
   - 最近检测时间：显示主机 IP 最近被检出威胁的时间。
5. 单击**主机 IP** 地址，可以查看该主机的详细分析内容。

添加监视对象 - 主机 IP

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**主机 IP**。
4. 显示主机 IP 列表。
5. 点击**添加**键，弹出<添加监视对象 - 主机 IP>界面。
6. 输入欲监视的**主机 IP** 地址。
7. 点击**确定**。

更改监视对象 - 主机 IP

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**主机 IP**。
4. 显示主机 IP 列表。
5. 鼠标双击列表中的欲更改项目，打开<更改监视对象 - 主机 IP>界面。
6. 更改所需的项目。
7. 点击**确定**。
8. 点击**应用更改配置**。

删除监视对象 - 主机 IP

当不再需要监视已设置为监视对象的主机时，可以从监视对象列表中删除该主机。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**监视对象**。
3. 出现<监视对象>界面，在左上的第二个选择框中选择**主机 IP**。
4. 出现监视对象-主机 IP 列表。
5. 在列表中选择欲删除项目左侧的 或**删除**键，弹出删除对话框。
6. 如果弹出确认删除的对话框， 点击**确定**。

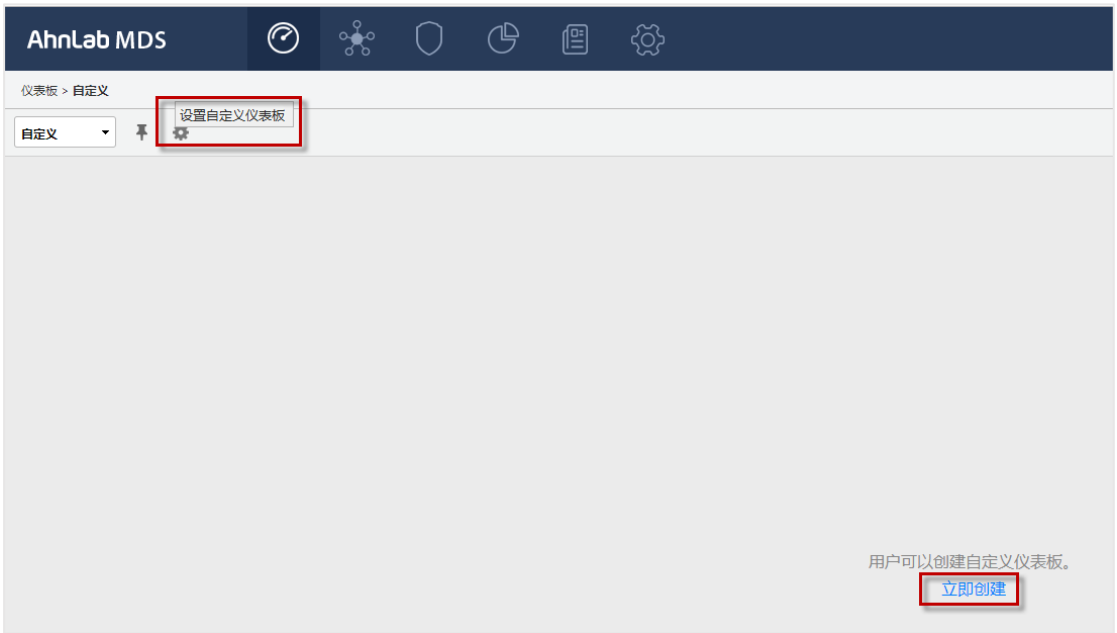
6.4 自定义仪表板

根据管理员需要可设置自定义的仪表板来方便确认各种信息。

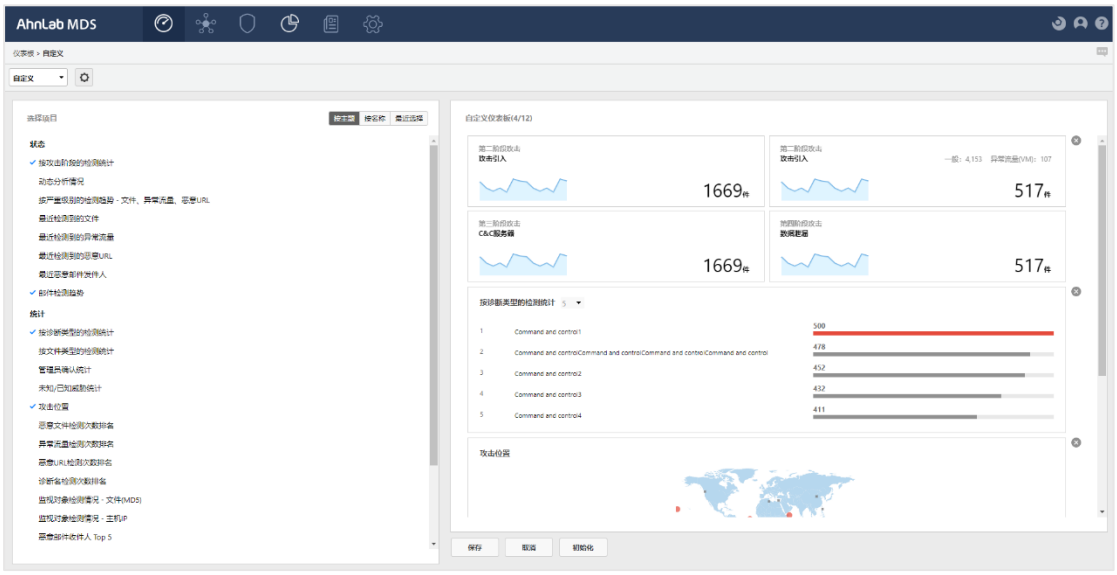
设置自定义仪表板的步骤如下。

1. 点击 Web 界面主菜单中的**仪表板**图标。
2. 在屏幕左上的选择框中选择**自定义**。

3. 如果还没有设置自定义仪表板，则点击**立即创建**；如果已有自定义的仪表板，则点击  ，更改自定义的仪表板。



4. 出现设置自定义仪表板的界面。



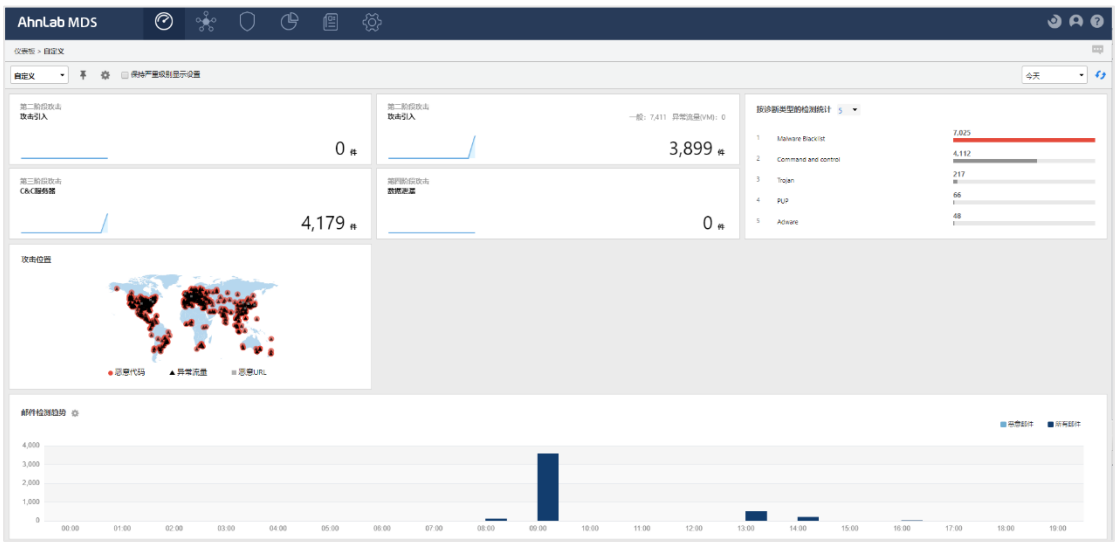
5. 左侧列出自定义仪表板中可显示的**项目**，项目可以**按主题**、**按名称**和**最近选择**排列。

6. 左侧列表中选择项目，右侧显示所选项目的统计图表或表格。仪表板项目最多可以选择 12 个。

7. 项目选择完后点击**保存**。

8. 出现“**成功创建自定义仪表板。**”的提示。

9. 点击**确定**，则出现如下的自定义的仪表板。



参考

如要将自定义的仪表板设置为仪表板首页，点击；如要取消首页设置，则点击。

第7章　检测情况分析

7.1　检测情况

查看 MDS 检测到的威胁的详细信息，并响应威胁。

> **⚠注意**
>
> 当响应检测结果时，“删除文件”、“恢复文件”、“隔离系统”、“解除隔离系统”、“收集可疑文件”和“发送通知”命令在未安装 Agent 的主机上不可用。这可能会使主机系统受到致命的安全威胁。除非有特别的目的，否则建议在所有主机上安装 Agent 程序。

查看检测事件

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**检测情况**标签。
3. 显示指定期间的检测事件列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 事件 ID：显示检测事件的 ID。
   - 确认状态：显示管理确认状态。状态分为**未确认**()，**待定**()，**已确认**()，**已确认(误诊)**()和**管理员确认除外项目**()。

> **参考**
>
> 管理员确认除外项目表示分析结果归类为“正常”，管理员不需要额外确认的项目，此项目的严重级别为“可能正常”或“正常”。

   - 严重级别[U/K]：显示文件的严重级别和未知（Unknown）/已知（Known）状态。
     - 高[U]：意味着高风险和未知的恶意代码。
     - 高[K]：意味着高风险和已知的恶意代码。
     - 中[U]：意味着中等风险和未知的恶意代码。
     - 中[K]：意味着中等风险和已知的恶意代码。
     - 低[U]：意味着较低风险和未知的恶意代码。
     - 低[K]：意味着较低风险和已知的恶意代码。
     - 灰色 2：意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。
     - 灰色 1：意味着虽然不是恶意，但需要检查。

  - 可能正常：分析结果为正常，且是一个未知的文件。
  - 正常：正常或是由管理员添加到白名单的文件。
  - : 意味着包含严重级别为【高】的恶意文件、URL 和脚本的电子邮件。
  - : 意味着包含严重级别为【高】的恶意文件的压缩文件。
  - : 意味着包含严重级别为【中】的恶意文件、URL 和脚本的电子邮件。
  - : 意味着包含严重级别为【中】的恶意文件的压缩文件。
  - : 意味着包含严重级别为【低】的恶意文件、URL 和脚本的电子邮件。
  - : 意味着包含严重级别为【低】的恶意文件的压缩文件。
  - : 意味着严重级别为【灰色】的电子邮件，可能含有恶意文件、URL 和脚本。
  - : 意味着严重级别为【灰色】的压缩文件，可能含有恶意文件。
  - : 意味着分析结果为正常的电子邮件，且没有发现恶意文件、URL 或脚本。
  - : 意味着分析结果为正常的压缩文件，且没有发现恶意文件。
- 检测对象：显示检测威胁的对象“主机”、“文件”、“C&C 服务器”、“URL”和“途径”。
- MD5：当检测对象为文件的时候显示该文件的 MD5 值。
- 文件格式：当检测对象为文件时，显示检测到文件的扩展名(exe, dll, js, doc, hwp, pdf, html)。
- 文件大小：显示检测到文件的大小。
- 攻击阶段：显示检测结果的攻击阶段。攻击阶段分为“攻击尝试”、“攻击引入（一般/C&C/数据泄漏)”、C&C 服务器和数据泄漏。
- 诊断名：显示检测到的恶意代码的诊断名。
- 自定义检测规则诊断名：显示通过自定义检测规则检测到的恶意代码的诊断名。
- 分析信息来源：显示检测到威胁的分析信息来源，优先显示动态分析信息的来源。
  来自本地的分析结果标记为 (本地)；来自 MDS Manager 的分析结果标记为 (MDS Manager)；来自云端的分析结果标记为 (云)。

参考

您可以指定来源查看检测情况。点击工具栏的**分析信息来源**的选择要查看的来源项目的复选框，然后点击**应用**，如图所示。如果不选择任何来源，则显示所有来源的信息。

  - 杀毒软件检测状态： 当检测到恶意代码时被杀毒软件检出，则显示杀毒软件的诊断名。
  - 攻击对象：显示作为攻击对象的 Agent 的连接状态。连接状态分为“已连接()”、“未连接()”、“未知()”。点击攻击对象，可以查看攻击对象的详细信息。
  - 主机名：显示成为攻击对象的主机名。
  - 途径：显示威胁引入的途径。
  - 途径详细：显示威胁引入途径的详细信息。

- 会话：显示检测事件的源 IP 地址和目标 IP 地址和各端口号。
- 攻击位置：显示发出攻击命令的 C&C 服务器的所在的国家和城市。
- 方向：显示威胁的移动方向，分为“外部->内部”、“内部->内部”、“内部->外部”显示。
- 响应状态：显示对检出威胁的响应状态。分为自动响应和手动响应显示。“A”表示自动响应；“M”表示手动响应。
- 分析所需时间：显示分析该威胁所需的时间（秒）。
- 引入时间：表示收集完成并带入设备的时间。
- 检测时间：表示分析完成确认检测结果的时间。
- 日志记录时间：显示记录日志的时间。
- 最近响应时间：显示对该威胁最近响应的时间。

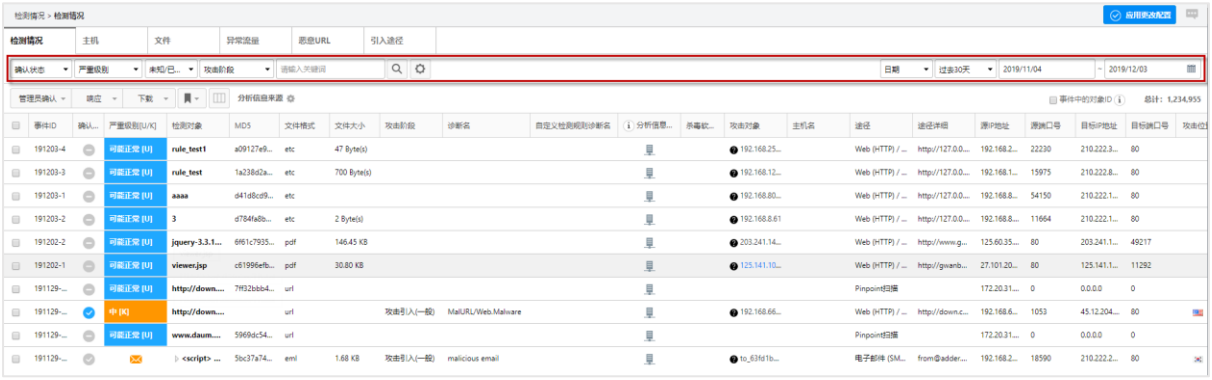
5. 如要查看事件的详细分析内容信息，请双击该事件行。
6. 显示事件的详细分析界面。详细的内容，请参考本章的最下面。

参考

为了更有效地查看检测情况中显示的大量的检测事件，可以利用列设置功能来指定屏幕上显示的列。点击  ，弹出<列设置>对话框，选择要在屏幕上显示的列，然后点击**确定**。如要设置为默认值，请点击**恢复默认值**。

搜索检测事件

检测情况的每个界面都会出现如下图所示的搜索区。



搜索按如下操作。

1. 选择搜索条件（确认状态、严重级别、已知/未知、攻击阶段）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜索符合关键词的检测事件并显示在列表中。
3. 如要更详细地指定搜索条件，点击  。
4. 弹出<高级搜索>窗口。

5. 选择搜索条件或输入搜索关键词。
6. 点击**搜索**，窗口将关闭，搜索结果显示在列表中。

参考

当搜索期间选择“时间”搜索时，搜索结果显示大于或等于开始时间且小于结束时间的数据。此内容同样适用于其他搜索界面。

设置书签

即使指定搜索期间和搜索条件，列表将显示很多的检测事件。此时，使用书签功能，将管理员随时要查看的事件设置书签。

设置书签的具体步骤如下。

1. 首先在检测事件列表中，选择要为其指定书签的一个事件。
2. 点击  ，在弹出的菜单中选择**添加书签**。
3. 弹出“事件已添加书签。书签将在 30 天后自动删除。”的提示。
4. 指定书签的事件 ID 将显示书签标记  。
5. 如要定位到指定书签所在的事件，点击  ，在弹出的菜单中选择**定位到书签**。
6. 如要删除书签，点击  ，在弹出的菜单中选择**删除书签**。

参考

只有上级事件可以设置书签，下级事件则无法设置书签。并且，不能为超过 30 天的事件添加书签。

管理员确认

对于检测到的一些恶意事件，可以标记“管理员确认”状态。如要使用该功能，请到管理 > 管理员 > 管理员确认界面先启用**管理员确认**功能。如果不启用该功能，则不会在检测情况和统计界面显示该功能。

参考

您只能选择严重级别为“灰色”以上的项目设置管理员确认状态。

管理员确认的具体步骤如下。

1. 首先在检测事件列表中，选择要标记管理员确认状态的事件，可以多选。
2. 点击**管理员确认**，在弹出的菜单中选择确认状态。从**未确认**、**待定**、**已确认**、**已确认（误诊）**中选择。
3. 弹出提示对话框，点击**是**。
4. 经过管理员确认的事件将出现如下的确认状态标记。
   - 未确认()：对于检测事件标记“未确认”。
   - 待定()：对于检测事件标记“待定”。

- 已确认()：对于检测事件标记“已确认”。
- 已确认(误诊)()：对于检测事件标记“已确认（误诊）”。已确认（误诊）状态的事件将被添加到白名单，并且严重级别更改为“正常”。

响应检测事件

管理员可以选择响应方法来响应威胁，以防止由检测到的事件对整个系统造成严重的安全威胁。

响应检测事件按如下步骤。

1. 首先在检测事件列表中，选择要响应的事件。
2. 点击**响应**，在弹出的菜单中选择响应方法。从**删除文件**、**恶意代码分析请求**、**Pinpoint 检测**中选择。
   - 删除文件：将选择的恶意文件从 Agent 中删除。可以选择所有 Agent 中删除恶意文件。
   - 恶意代码分析请求：将选择的文件发送到 AhnLab，请求分析。
   - Pinpoint 扫描：对选择的文件执行 Pinpoint 扫描。

对每个响应方法的详细说明如下。

响应方法	执行状态	执行结果	相关帮助
删除文件	响应情况 >响应情况	响应情况 >响应情况，响应情况 > 隔离区	响应情况, 隔离区
恶意代码分析请求	响应情况 >响应情况, 响应情况 >恶意代码分析请求	响应情况 >响应情况, 响应情况 >恶意代码分析请求	响应情况, 恶意代码分析请求
Pinpoint 扫描	响应情况 >响应情况, 响应情况 >Pinpoint 扫描	响应情况 >响应情况, 响应情况 >Pinpoint 扫描	响应情况, Pinpoint 扫描

下载检测文件

您可以将检测到的文件下载的本地 PC 进行技术分析，或发送到外部机关请求分析。

1. 首先在检测事件列表中，选择要下载文件的事件。
2. 点击**下载**，在弹出的菜单中选择**下载文件**。
3. 选择的文件将下载到本地 PC。
4. 如要将检测事件列表以 CSV 形式下载到本地 PC，请选择**导出列表**。

⚠注意

“下载检测文件”时将恶意文件的 MD5 值压缩后保存到本地 PC。如果选择一个文件下载时，使用文件的 MD5 哈希值作为压缩文件名使用；选择两个以上的文件下载时，使用当前日期作为压缩文件名使用。对于下载文件（MD5）而有可能造成本地计算机的损失 AhnLab 不负任何责任。

导出检测事件列表

您可以将搜索期间发生的检测事件列表以 CSV 文件格式保存到本地计算机。

1. 在检测事件列表中，点击**下载**。
2. 在弹出的菜单中选择**导出列表**，弹出<导出检测事件列表>窗口。
3. 选择要另存为文件的信息，然后点击**下载**。

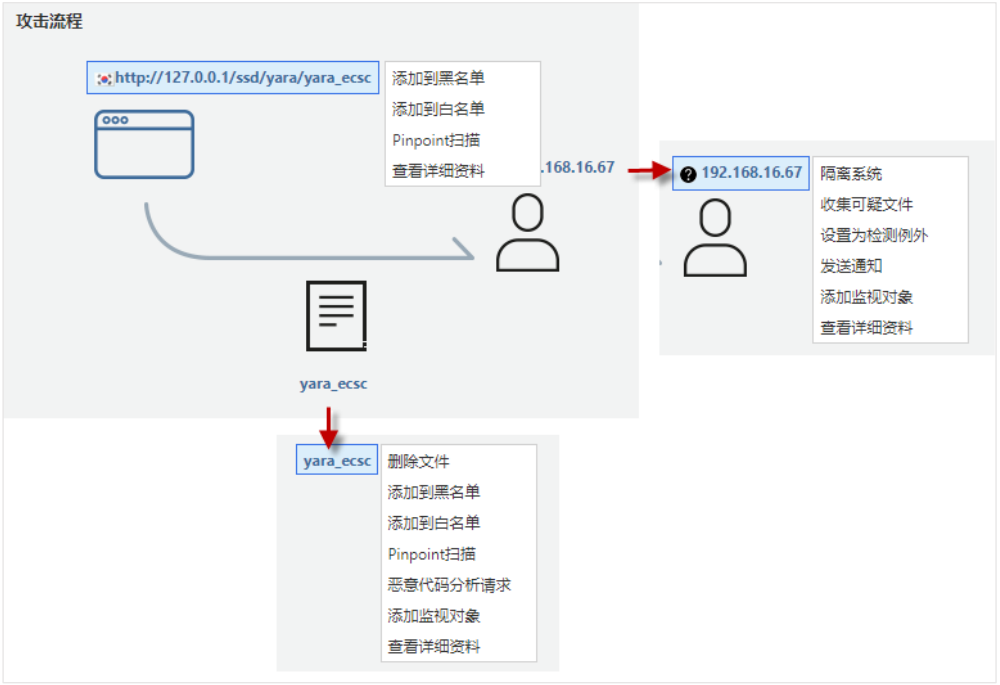
参考

如果是压缩文件，则显示压缩前的上下级文件夹和文件信息；如果是邮件文件，则显示组件信息，如标题和附件等。

检测事件详细分析

可以查看检测事件的详细分析内容。

1. 从检测事件列表中，鼠标双击要查看的事件。
2. 出现检测事件的详细分析界面。
3. 可以查看检测事件的详细分析内容。
   - 摘要：显示检测事件的摘要信息，如“攻击流程”图、“基本信息”和“检测原因”。
     - 攻击流程：使用图显示了攻击引入途径、攻击目标以及检测对象之间的关系等。将鼠标放到个图标上，出现各图标表示的内容，点击图标上方的标题，出现不同的响应方法。



     - 基本信息：检测到事件的基本信息。根据检测事件的种类，显示的内容将有所不同。
     - 检测原因：显示为什么检测为威胁。

- 历史记录管理：显示管理员响应检测事件的历史记录。
- 管理员意见：可以输入对该检测事件的管理员意见。点击**输入**，出现文本框，输入内容后再点击**输入**。如要删除输入的意见，点击✕即可删除。

> **参考**
>
> 根据检测事件类型，显示的详细分析内容可能与上述的内容有所差异。

> **参考**
>
> 点击界面左上的☰，可以快速移动到您要查看的分析内容。
> 如要对该事件执行管理员确认，点击**未确认**，在出现的菜单中选择您要处理的确认状态。
> 如要对该事件响应，点击**响应**，在出现的菜单中选择您要处理的响应方法。根据事件类型，显示的响应方法也有所不同。

7.2 检测情况 - 主机

查看 MDS 检测到的受感染主机的详细信息，并对主机进行响应措施。

查看检测主机

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**主机**标签。
3. 显示指定期间的检测到的主机列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 连接状态：显示主机连接到服务器的状态。连接状态分为“已连接(🟢)”、“未连接(⚫)”、“未知(❓)”显示。
   - 隔离状态：显示主机的隔离状态。隔离状态分为“未隔离”、“已隔离(Agent)”、“已隔离(安全开关)”显示。
   - 主机：显示主机的 IP 地址。
   - 检测次数：显示主机检测到攻击的总数。
   - 攻击尝试：显示主机检测到尝试攻击的总数。
   - 攻击引入[一般/C&C(VM)/数据泄漏(VM)]：显示主机检测到的攻击引入总数。分为“一般”、“C&C(VM)”和“数据泄漏(VM)”显示。
   - C&C：显示主机与 C&C 服务器进行通信的总数。
   - 数据泄漏：显示主机检测到数据泄漏的总数。
   - 严重级别[U/K]：显示在主机检测到的攻击的严重级别和未知（Unknown）/已知（Known）状态。
     - 高[U]：这意味着高风险和未知的恶意代码。

- 高[K]：这意味着高风险和已知的恶意代码。
- 中[U]：这意味着中等风险和未知的恶意代码。
- 中[K]：这意味着中等风险和已知的恶意代码。
- 低[U]：这意味着较低风险和未知的恶意代码。
- 低[K]：这意味着较低风险和已知的恶意代码。
- 灰色 2：这意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。
- 灰色 1：这意味着虽然不是恶意，但需要检查。
- 可能正常：分析结果为正常，且是一个未知的文件。
- 正常：正常或是由管理员添加到白名单的文件。

- 最近检测到的事件：显示主机最近检测到的攻击事件类型。
- 最近检测时间：显示主机最近检测到攻击的时间。

5. 如要查看主机的详细信息，请双击该主机行。
6. 出现检出威胁的主机的详细分析界面。

搜索检测主机

搜索按如下操作。

1. 选择搜索条件（连接状态、隔离状态）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜素符合关键词的检测主机并显示在列表中。
3. 如果选择“仅显示监视对象”选项，则列表仅显示设置为监视对象的检测到的主机列表。

参考

设置为监视对象的主机标记图标。

响应检测主机

管理员可以选择响应方法来响应检测到的主机，以防止由检测到的主机对整个系统造成严重的安全威胁。

响应检测主机按如下步骤。

1. 首先在检测主机列表中，选定要响应的主机。
2. 点击**响应**，在弹出的菜单中选择响应方法。
   - 隔离系统(Agent)：当检测到受感染主机时，通过 Agent 命令隔离主机系统并无法使用网络。
   - 隔离系统(安全开关)：当检测到受感染主机时，通过安全开关隔离主机系统并无法使用网络。
   - 解除隔离系统：解除隔离的主机。
   - 收集可疑文件：即使在主机没有检测为恶意，但是收集可能被感染的文件。

- 设置为检测例外：对判断为没有感染风险的主机，可以设置为检测例外。
- 发送通知：通知主机被感染事件或告知最近流行的恶意代码的信息。
- 添加到黑名单：将选择的主机添加到黑名单，以后始终检测为恶意或拦截。
- 添加到白名单：将选择的主机添加到白名单，以后始终处理为检测例外或不进行拦截。
- 添加到监视对象：将选择的主机添加到监视对象列表，以后可以设置自动响应。
- 删除监视对象：当不再需要监视已设置为监视对象的主机时，可以从监视对象列表中删除该主机。

对每个响应方法的详细说明如下。

响应方法	执行状态	执行结果	相关帮助
隔离系统(Agent) 隔离系统(安全开关)	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 隔离区	响应情况, 隔离区
解除隔离系统	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 隔离区	响应情况, 隔离区
收集可疑文件	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 收集可疑文件	响应情况, 收集可疑文件
设置为检测例外	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略 > 检测例外 IP	响应情况, 检测例外 IP
发送通知	响应情况 > 响应情况	响应情况 > 响应情况	响应情况, 发送通知
添加到黑名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略 > 黑名单	响应情况, 黑名单
添加到白名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略 > 白名单	响应情况, 白名单
添加到监视对象	响应情况 > 响应情况	响应情况 > 响应情况, 仪表板 > 监视对象	响应情况, 监视对象
删除监视对象	响应情况 > 响应情况	响应情况 > 响应情况, 仪表板 > 监视对象	响应情况, 监视对象

导出检测主机列表

您可以将检测到的主机列表下载的本地 PC。

1. 在检测主机列表中，点击**导出。**
2. 主机列表以 CSV 形式下载到本地 PC。

检测主机详细分析

可以查看检测主机的详细分析内容。

1. 从检测主机列表中，鼠标双击要查看的主机。
2. 出现检测主机的详细分析界面。
3. 可以查看检测主机的详细分析内容，并根据详细的分析内容进行响应措施。

参考

点击界面左上的☰，可以快速移动到您要查看的分析内容。
如要对主机进行响应，点击**响应**，在出现的菜单中选择您要处理的响应方法。

7.3 检测情况 - 文件

查看 MDS 检测到的恶意文件的详细信息，并设置响应方法。

参考

恶意文件是指检测到恶意代码的文件。

查看检测文件

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**文件**标签。
3. 显示指定期间的检测到的恶意文件列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - MD5：显示检测到的恶意文件的 MD5 值。
   - 文件名：显示检测到的恶意文件的名称。
   - 文件格式：显示检测到的恶意文件的扩展名。
   - 严重级别[U/K]：显示检测到的恶意文件的严重级别和未知（Unknown）/已知（Known）状态。
     - 高[U]：这意味着高风险和未知的恶意代码。
     - 高[K]：这意味着高风险和已知的恶意代码。
     - 中[U]：这意味着中等风险和未知的恶意代码。
     - 中[K]：这意味着中等风险和已知的恶意代码。
     - 低[U]：这意味着较低风险和未知的恶意代码。
     - 低[K]：这意味着较低风险和已知的恶意代码。
     - 灰色 2：这意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。

- 灰色 1：这意味着虽然不是恶意，但需要检查。
- 可能正常：分析结果为正常，且是一个未知的文件。
- 正常：正常或是由管理员添加到白名单的文件。

- 诊断名：显示检测到恶意代码的诊断名。
- 攻击阶段：显示检测到的恶意文件的攻击阶段。
- 检测次数：显示恶意文件被检出的总数。

参考

仅包含检测结果为“灰色”以上的严重级别。

- 检测到的主机数：显示检出该恶意文件的主机数。
- 删除次数：显示删除该恶意代码的总数。
- 首次检测时间：显示首次检测到该恶意文件的时间。
- 最近检测时间：显示最近检测到该恶意文件的时间。

5. 如要查看恶意文件的详细信息，请双击该恶意文件行。
6. 出现恶意文件的详细分析界面。

参考

无论文件的扩展名，MDS 都可以识别文件的类型。

搜索检测文件

搜索按如下操作。

1. 选择搜索条件（严重级别、已知/未知、攻击阶段、文件格式）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜素符合关键词的检测到的文件并显示在列表中。
3. 如果选择“仅显示监视对象”选项，则列表仅显示设置为监视对象的检测到的主机列表。

参考

设置为监视对象的文件标记图标。

响应检测文件

管理员可以选择响应方法来响应检测到的恶意文件，以防止由恶意文件对整个系统造成严重的安全威胁。

响应检测文件按如下步骤。

1. 首先在检测文件列表中，选定要响应的文件。
2. 点击**响应**，在弹出的菜单中选择响应方法。

- 删除文件：向选择的文件发出删除命令。
- 恢复文件：向选择的文件发出恢复命令。
- 添加到黑名单：将选择的文件添加到黑名单，以后始终检测为恶意或拦截。
- 添加到白名单：将选择的文件添加到白名单，以后始终处理为检测例外或不进行拦截。
- 添加到监视对象：将选择的文件添加到监视对象列表，以后可以设置自动响应。
- 删除监视对象：当不再需要监视已设置为监视对象的文件时，可以从监视对象列表中删除该文件。
- Pinpoint 扫描：将选择的文件发送到 AhnLab，请求分析。
- 恶意代码分析请求：对选择的文件执行 Pinpoint 扫描。

对每个响应方法的详细说明如下。

响应方法	执行状态	执行结果	相关帮助
删除文件	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 隔离区	响应情况, 隔离区
恢复文件	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 隔离区	响应情况, 隔离区
添加到黑名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 黑名单	响应情况, 黑名单
添加到白名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 白名单	响应情况, 白名单
添加到监视对象	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 监视对象	响应情况, 监视对象
删除监视对象	响应情况 > 响应情况	响应情况 > 响应情况, 响应情况 > 监视对象	响应情况, 监视对象
Pinpoint 扫描	响应情况 > 响应情况, 响应情况 > Pinpoint 扫描	响应情况 > 响应情况, Pinpoint 扫描	响应情况, Pinpoint 扫描
恶意代码分析请求	响应情况 > 响应情况, 响应情况 > 恶意代码分析请求	响应情况 > 响应情况, 响应情况 > 恶意代码分析请求	响应情况,, 恶意代码分析请求

下载检测文件或导出列表

您可以将检测到的文件下载的本地 PC 进行技术分析，或发送到外部机关请求分析。

1. 首先在检测文件列表中，选择要下载的文件。
2. 点击**下载**，在弹出的菜单中选择**下载文件**。
3. 选择的文件将下载到本地 PC。
4. 如要将检测文件列表以 CSV 形式导出，请选择**导出列表**。

⚠注意

恶意文件将以压缩文件形式保存到本地 PC。要解除压缩，需要输入密码。对于运行恶意代码而造成的损失 AhnLab 不负任何责任。

检测文件详细分析

可以查看检测文件的详细分析内容。

1. 从检测文件列表中，鼠标双击要查看的文件。
2. 出现检测文件的详细分析界面。
3. 可以查看检测文件的详细分析内容，并根据详细的分析内容进行响应措施。

参考

点击界面左上的☰，可以快速移动到您要查看的分析内容。
如要对检测到的恶意文件进行响应，点击**响应**，在出现的菜单中选择您要处理的响应方法。

7.4 检测情况 - 异常流量

查看 MDS 检测到的异常流量的详细信息，并设置响应方法。

参考

C&C 服务器(Command & Control Server)是一个远程控制服务器，用于命令和控制受感染的僵尸 PC，执行攻击者发出的攻击命令，主要发出恶意代码分发、网络钓鱼、垃圾邮件和 DDoS 攻击等命令。

查看异常流量检测情况

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**异常流量**标签。
3. 显示指定期间的检测到的异常流量列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 攻击者：显示检测到的异常流量的攻击者的 IP 地址。
   - 端口：显示检测到的异常流量回调活动使用的端口号。
   - 协议：显示检测到的异常流量回调活动使用的协议。
   - 攻击位置：显示检测到的异常流量所在的国家和城市。
   - 严重级别[U/K]：显示在检测到的异常流量的严重级别和未知（Unknown）/已知（Known）状态。
     - 高[U]：这意味着高风险和未知的恶意代码。
     - 高[K]：这意味着高风险和已知的恶意代码。

- 中[U]：这意味着中等风险和未知的恶意代码。
- 中[K]：这意味着中等风险和已知的恶意代码。
- 低[U]：这意味着较低风险和未知的恶意代码。
- 低[K]：这意味着较低风险和已知的恶意代码。
- 灰色 2：这意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。
- 灰色 1：这意味着虽然不是恶意，但需要检查。
- 可能正常：分析结果为正常，且是一个未知的文件。
- 正常：正常或是由管理员添加到白名单的文件。

- 诊断名：显示检测到的异常流量回调活动的诊断名。
- 攻击阶段：显示检测到的异常流量回调活动的攻击阶段。
- 检测次数：显示异常流量回调活动被检出的总数。
- 检测到的主机数：显示访问该异常流量的主机数。
- 阻止访问次数：显示阻止访问该异常流量的次数。
- 首次检测时间：显示首次检测到该异常流量的时间。
- 最近检测时间：显示主机最近检测到该异常流量的时间。

5. 如要查看该异常流量的详细信息，请双击该异常流量行。
6. 出现检测到异常流量的详细分析界面。

搜索异常流量检测情况

1. 选择搜索条件（严重级别、已知/未知、攻击阶段）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜索符合关键词的异常流量并显示在列表中。

响应检测到的异常流量

管理员可以选择响应方法来响应检测到的异常流量，以防止由异常流量对整个系统造成严重的安全威胁。

响应检测到的异常流量按如下步骤。

1. 首先在检测到的异常流量列表中，选定要响应的异常流量。
2. 点击**响应**，在弹出的菜单中选择响应方法。
   - 添加到黑名单：将选择的异常流量添加到黑名单，以后始终检测为恶意或拦截。
   - 添加到白名单：将选择的异常流量添加到白名单，以后始终处理为检测例外或不进行拦截。

对每个响应方法的详细说明如下。

响应方法	执行状态	执行结果	相关帮助
添加到黑名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 黑名单	响应情况, 黑名单
添加到白名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 白名单	响应情况, 白名单

导出检测到的异常流量列表

您可以将检测到的异常流量列表下载的本地 PC。

1. 在检测异常流量列表中，点击**导出。**
2. 异常流量列表以 CSV 形式下载到本地 PC。

异常流量详细分析

可以查看检测到的异常流量的详细分析内容。

1. 从异常流量列表中，鼠标双击要查看的异常流量。
2. 出现检测异常流量的详细分析界面。
3. 可以查看检测异常流量的详细分析内容，并根据详细的分析内容进行响应措施。

参考

点击界面左上的☰，可以快速移动到您要查看的分析内容。
如要对异常流量进行响应，点击**响应**，在出现的菜单中选择您要处理的响应方法。

7.5 检测情况 - 恶意 URL

查看 MDS 检测到的恶意 URL 的详细信息，并设置响应方法。

查看恶意 URL 检测情况

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**恶意 URL** 标签。
3. 显示指定期间的检测到的恶意 URL 列表。默认期间为**过去 24 小时。**
4. 可以确认如下信息。
   - URL：显示检测到恶意 URL。
   - 端口：显示检测到的恶意 URL 使用的端口号。

- 协议：显示检测到的恶意 URL 使用的协议。
- 攻击位置：显示检测到的恶意 URL 所在的国家和城市。
- 严重级别[U/K]：显示在检测到的恶意 URL 的严重级别和未知（Unknown）/已知（Known）状态。
  - 高[U]：这意味着高风险和未知的恶意代码。
  - 高[K]：这意味着高风险和已知的恶意代码。
  - 中[U]：这意味着中等风险和未知的恶意代码。
  - 中[K]：这意味着中等风险和已知的恶意代码。
  - 低[U]：这意味着较低风险和未知的恶意代码。
  - 低[K]：这意味着较低风险和已知的恶意代码。
  - 灰色 2：这意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。
  - 灰色 1：这意味着虽然不是恶意，但需要检查。
  - 可能正常：分析结果为正常，且是一个未知的文件。
  - 正常：正常或是由管理员添加到白名单的文件。
- 诊断名：显示检测到的恶意 URL 的诊断名。
- 攻击阶段：显示检测到的恶意 URL 的攻击阶段。
- 检测次数：显示恶意 URL 被检出的总数。
- 检测到的主机数：显示访问该恶意 URL 的主机数。
- 拦截次数：显示拦截该恶意 URL 的次数。
- 首次检测时间：显示首次检测到该恶意 URL 的时间。
- 最近检测时间：显示主机最近检测到该恶意 URL 的时间。

5. 如要查看该 C&C 服务器的详细信息，请双击该恶意 URL 行。
6. 出现检测到恶意 URL 的详细分析界面。

搜索恶意 URL 检测情况

1. 选择搜索条件（严重级别、已知/未知、攻击阶段）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜索符合关键词的恶意 URL 并显示在列表中。

响应检测到的恶意 URL

管理员可以选择响应方法来响应检测到的恶意 URL，以防止由恶意 URL 对整个系统造成严重的安全威胁。

1. 首先在检测到的恶意 URL 列表中，选定要响应的恶意 URL。
2. 点击**响应**，在弹出的菜单中选择响应方法。
   - 添加到黑名单：将选择的恶意 URL 添加到黑名单，以后始终检测为恶意或拦截。

- 添加到白名单：将选择的恶意 URL 添加到白名单，以后始终处理为检测例外或不进行拦截。
- Pinpoint 扫描：将选择的恶意 URL 发送到 AhnLab，请求分析。

对每个响应方法的详细说明如下。

响应方法	执行状态	执行结果	相关帮助
添加到黑名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 黑名单	响应情况, 黑名单
添加到白名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 白名单	响应情况, 白名单
Pinpoint 扫描	响应情况 > 响应情况, 响应情况 > Pinpoint 扫描	响应情况 > 响应情况, Pinpoint 扫描	响应情况, Pinpoint 扫描

导出检测到的恶意 URL 列表

您可以将检测到的恶意 URL 列表下载的本地 PC。

1. 在检测到的恶意 URL 列表中，点击**导出。**
2. 恶意 URL 列表以 CSV 形式下载到本地 PC。

恶意 URL 详细分析

可以查看检测到的恶意 URL 的详细分析内容。

1. 从恶意 URL 列表中，鼠标双击要查看的恶意 URL。
2. 出现恶意 URL 的详细分析界面。
3. 可以查看检测到的恶意 URL 的详细分析内容，并根据详细的分析内容进行响应措施。

参考

点击界面左上的☰，可以快速移动到您要查看的分析内容。
如要对恶意 URL 进行响应，点击**响应**，在出现的菜单中选择您要处理的响应方法。

7.6 检测情况 - 引入途径

查看 MDS 检测到威胁引入或收集的途径详细信息，并设置响应方法。

查看检测引入途径情况

1. 点击 Web 界面主菜单中的**检测情况**图标。
2. 选择**引入途径**标签。

3. 显示指定期间的检测到的 C&C 服务器列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 类别：显示检测到的威胁的引入途径的种类。威胁引入或收集的途径分为“Web”、“文件服务器”、“电子邮件”、“共享文件夹”、“其他”以及“第三方”显示。
   - 组：显示基于途径类别的详细途径的上级路径，如 IP 地址或域。
   - 途径详细：显示引入途径详细。
   - 检测次数：显示该途径被检出的次数。
   - 检测到的主机数：显示通过该途径受感染的主机数。
   - 首次检测时间：显示首次检测到该途径的时间。
   - 最近检测时间：显示主机最近检测到该途径的时间。
5. 如要查看该途径的详细信息，请双击该途径行。
6. 出现检测到的途径的详细分析界面。

搜索引入途径检测情况

搜索按如下操作。

1. 选择搜索条件（类型）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜素符合关键词的途径并显示在列表中。

响应检测到的引入途径

管理员可以选择响应方法来响应检测到的途径，以防止由途径对整个系统造成严重的安全威胁。

响应检测到的途径按如下步骤。

1. 首先在检测到的途径列表中，选定要响应的途径。
2. 点击**响应**，在弹出的菜单中选择响应方法。
   - 添加到黑名单：将选择的恶意 URL 添加到黑名单，以后始终检测为恶意或拦截。
   - 添加到白名单：将选择的恶意 URL 添加到白名单，以后始终处理为检测例外或不进行拦截。
   - Pinpoint 扫描：将选择的恶意 URL 发送到 AhnLab，请求分析。

对每个响应方法的详细说明如下。

响应方法	执行状态	执行结果	相关帮助
添加到黑名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 黑名单	响应情况, 黑名单
添加到白名单	响应情况 > 响应情况	响应情况 > 响应情况, 管理 > 策略设置 > 白名单	响应情况, 白名单
Pinpoint 扫描	响应情况 > 响应情况, 响应情况 > Pinpoint 扫描	响应情况 > 响应情况, Pinpoint 扫描	响应情况, Pinpoint 扫描

导出引入途径列表

您可以将检测到的途径列表下载的本地 PC。

1. 在检测到的途径列表中，点击**导出。**
2. 途径列表以 CSV 形式下载到本地 PC。

引入途径详细分析

可以查看检测到的途径的详细分析内容。

1. 从途径列表中，鼠标双击要查看的途径。
2. 出现途径的详细分析界面。
3. 可以查看检测到的途径的详细分析内容，并根据详细的分析内容进行响应措施。

参考

点击界面左上的☰，可以快速移动到您要查看的分析内容。
如要对途径进行响应，点击**响应**，在出现的菜单中选择您要处理的响应方法。

第8章　响应情况说明

8.1　响应情况

查看 MDS 响应威胁的详细情况，并对响应失败的事件可以重新作出响应。

查看响应情况

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择**响应情况**标签。
3. 显示指定期间的响应事件列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 响应状态：显示响应检测结果的进行状态。 状态分为“**完成(成功)()**”、“**正在进行()**”和“**完成(失败)()**”显示。
   - 手动/自动：显示该响应是手动还是自动执行。
   - 响应方法：显示响应方法。
   - 对象：显示响应对象。对象分为“**组**”和“**主机**”显示。
   - 对象详细：显示主机或组的详细信息。
   - 管理员：显示发出响应命令的管理员的信息。
   - 事件 ID：显示检测事件 ID。
   - 事件详细：显示事件的详细内容。
   - 响应内容：显示响应内容。
   - 响应开始时间：显示发出响应命令的时间。
   - 响应完成时间：显示完成响应命令的时间。
5. 如要查看响应的详细信息，双击欲查看详细信息的行。
6. 弹出<响应情况详细>窗口，可以查看详细的响应信息。

参考

为了更有效地查看响应情况中显示的大量的响应结果，可以利用列设置功能来指定屏幕上显示的列。点击  ，弹出<列设置>对话框，选择要在屏幕上显示的列，然后点击**确定**。如要设置为默认值，请点击**恢复默认值**。

搜索响应事件

搜索按如下操作。

1. 选择搜索条件（响应状态、响应方法）或输入关键词，还可以指定搜索期间。
2. 点击  ，则在所有字段搜素符合关键词的响应事件并显示在列表中。
3. 如要更详细地搜索，点击  。
4. 弹出<高级搜索>窗口。
5. 选择搜索条件或输入搜索关键词。
6. 点击**搜索**，窗口将关闭，搜索结果显示在列表中。

参考

如要将搜索的响应事件列表下载的本地 PC，请点击**导出**。

重新发出响应命令

由于某种原因，即使向检测到的事件发出响应命令，但响应命令无法完成，并且显示为**完成(失败)**。或者，虽然命令没有失败，但可能需要再次重复发出相同的命令。 此时，可以使用重试响应命令。通过重试响应命令可以重新发出管理员所需的响应命令，或者对所有的失败的项目重新发出相同的命令。

1. 首先在响应事件列表中，选择要重新发出响应命令的事件。
2. 点击**重试**，在弹出的菜单中选择重试方法。
   - 重试所选项目：可对选择的项目重新发出命令。
   - 重试所有失败的项目：与选择的项目无关，对整个失败的项目重新发出命令。

8.2 隔离区

可以查看隔离区中的文件。当 Agent 执行“删除文件”命令时，运行中的恶意进程将被终止，并更改文件结构使恶意文件无法运行，然后将文件发送到隔离区保存。当误删不该删除的文件时，可以利用隔离区的恢复功能来恢复已删除的文件，将其还原到原始位置。另外，还可以下载文件用在恶意代码分析请求。

注意

如果文件超过隔离区大小，Agent 将删除隔离区的文件。隔离区大小在管理 > Agent > Agent 策略中设置。

查看隔离区文件

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择**文件隔离区**标签。
3. 显示指定期间的隔离区文件列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - MD5：显示 Agent 删除的恶意文件的 MD5 值。点击 MD5 值，可以移动到 MD5 详细页面。
   - Agent：显示删除该恶意文件的 Agent 名。当删除该恶意文件的 Agent 超过一个以上，则显示 Agent 数。点击该数，则弹出 Agent 列表。可以查看所有删除该恶意文件的 Agent 列表。
   - 严重级别[U/K]：显示该恶意文件的严重级别和未知（Unknown）/已知（Known）状态。
     - 高[U]：这意味着高风险和未知的恶意代码。
     - 高[K]：这意味着高风险和已知的恶意代码。
     - 中[U]：这意味着中等风险和未知的恶意代码。
     - 中[K]：这意味着中等风险和已知的恶意代码。
     - 低[U]：这意味着较低风险和未知的恶意代码。
     - 低[K]：这意味着较低风险和已知的恶意代码。
     - 灰色 2：这意味着不是一个明显的恶意，但它很有可能是恶意的，因此需要小心。
     - 灰色 1：这意味着虽然不是恶意，但需要检查。
     - 可能正常：分析结果为正常，且是一个未知的文件。
     - 正常：正常或是由管理员添加到白名单的文件。
   - 诊断名：显示该恶意文件被检出恶意代码的诊断名。
   - 最近相关事件 ID：显示最近发出删除文件命令的事件 ID。
   - 最近删除时间：显示该恶意文件最近被删除的时间。

参考

如要查看特定 MD5 值的文件，请在搜索栏里输入 MD5 值，然后点击  ，则符合条件的文件将显示在列表中。

恢复隔离区文件

恢复已在 Agent 系统删除的文件，将其还原到原始位置。恢复文件命令可以针对管理员选择的 Agent 执行，或针对查询期间删除指定文件的所有 Agent 执行。

1. 首先在隔离文件列表中，选择要恢复的文件。
2. 点击**恢复**。

参考

文件恢复还可以在<Agent 列表>中进行。选择一个或多个 Agent 进行恢复，文件将恢复到选择的 Agent 系统。

下载文件或导出列表

您可以将隔离区的文件下载到本地 PC 进行技术分析，或发送到外部机关请求分析。

1. 首先在隔离文件列表中，选择要下载文件的事件。
2. 点击**下载**，在弹出的菜单中选择**下载文件**。
3. 选择的文件将下载到本地 PC。
4. 如要将隔离文件列表以 CSV 形式下载到本地 PC，请选择**导出列表**。

注意

恶意文件将以压缩文件形式保存到本地 PC。要解除压缩，需要输入密码。对于运行恶意代码而造成的损失 AhnLab 不负任何责任。

8.3 系统隔离

可以查看被隔离后网络访问被阻止的主机系统。如果确定主机系统包含感染恶意代码的文件或存在安全威胁因素，管理员将执行隔离主机系统命令以阻止主机使用网络。

注意

尽管是一个隔离的主机系统，但是为了特殊的目的可能需要允许网络访问。这种情况，请在管理 > 检测和响应 > 响应设置中设置系统隔离例外 IP/域。请注意使用，因为它可能会在设置过程中面临安全威胁。

查看隔离的系统

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择**系统隔离**标签。
3. 显示指定期间的隔离系统列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 类别：显示隔离的类型。分为**隔离(安全开关)**和**隔离(Agent)**显示。
   - 主机：显示被隔离的主机名和 IP 地址，鼠标点击即可移动到该主机详细信息界面。另外在主机名前面标记与服务器的连接状态。连接状态分为“**已连接**(🟢)“、 “**未连接**(⚫)”、 “**未知**(❓)”。
   - 主机详细信息：显示主机的详细信息。
   - 事件 ID：显示发出隔离系统命令的事件 ID。
   - 隔离时间：显示隔离系统的时间。

参考

如要将搜索的隔离系统列表下载的本地 PC，请点击**导出**。

解除隔离系统

1. 首先在隔离的主机列表中，选择要解除隔离的主机。
2. 点击**解除隔离**。

参考

您可以配置自动解除隔离，当经过一段时间后自动解除。该选择是在管理 > 检测和响应 > 响应设置中设置。

8.4 收集可疑文件

查看 MDS 收集的可疑文件。可疑文件收集是从用户系统收集虽然未被诊断为恶意代码但被怀疑感染恶意代码或有可能给系统带来威胁的文件，并将其发送到 MDS 的命令。收集的可疑文件通过 MDS 的各种分析方法诊断恶意与否。

查看收集的可疑文件按如下操作：

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择**收集可疑文件**标签。
3. 显示指定期间收集的可疑文件列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - Agent：显示收集可疑文件的 Agent 系统和连接服务器状态。连接状态分为“**已连接**(🟢)“、“**未连接**(⚫)”、“**未知**(❓)”。
   - Agent 详细信息：显示 Agent 的详细信息。
   - 可疑文件：显示收集的可疑文件数。
   - 事件 ID：显示发出收集可疑文件命令的事件 ID。
   - 收集开始时间：显示开始收集可疑文件的时间。
   - 收集结束时间：显示结束收集可疑文件的时间。

参考

如要查看特定的文件，请在搜索栏里输入关键词，然后点击 🔍，则符合条件的可疑文件将显示在列表中。

参考

如要将搜索的可疑文件列表下载的本地 PC，请点击**导出**。

8.5 Pinpoint 扫描

查看通过 Pinpoint 扫描功能对可疑文件或 URL 执行扫描的结果。

查看 Pinpoint 扫描结果

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择 **Pinpoint 扫描**标签。
3. 显示指定期间执行 Pinpoint 扫描的结果列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 状态：显示 Pinpoint 扫描进行状态。分为**正在进行**、**成功**和**失败**显示。
   - 扫描结果：显示 Pinpoint 扫描结果。分为**正常**和**恶意**显示。
   - 类别：显示 Pinpoint 扫描的类型。类型有**文件**和 **URL**。
   - 扫描对象：显示执行 Pinpoint 扫描的文件或 URL 信息。
   - Pinpoint 扫描事件 ID：显示 Pinpoint 扫描事件的 ID。
   - 事件 ID：显示发出 Pinpoint 扫描命令时发生的事件 ID。
   - 扫描请求时间：显示请求 Pinpoint 扫描的时间。
   - 扫描完成时间：显示完成 Pinpoint 扫描的时间。

参考

如要查看特定的 Pinpoint 扫描结果，选择搜索条件（状态、扫描结果）或输入关键词，然后点击  ，则符合条件的扫描结果将显示在列表中。

参考

如要将 Pinpoint 扫描结果列表下载的本地 PC，请点击**导出**。

执行 Pinpoint 扫描

选择特定文件或 URL 执行 Pinpoint 扫描的步骤按如下。

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择 **Pinpoint 扫描**标签。
3. 点击列表左上的 **Pinpoint 扫描**键。
4. 弹出<Pinpoint 扫描>窗口。
5. 选择欲进行 Pinpoint 扫描的对象类型，**文件**或 **URL**。
6. 如果选择了**文件**，则点击**浏览**选择欲扫描的文件；如果选择了 **URL**，则输入欲扫描的 URL。

7. 点击**发出**。

8.6 恶意代码分析请求

查看发出恶意代码分析请求的结果。恶意代码分析请求是将 MDS 检测到的，或者是从主机收集的可疑文件传送到指定的分析系统，并请求分析。有关收集可疑文件的更多信息，请参考收集可疑文件。

查看恶意代码分析请求结果

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择**恶意代码分析请求**标签。
3. 显示指定期间发出恶意代码分析请求的结果列表。默认期间为**过去 24 小时**。
4. 可以确认如下信息。
   - 状态：显示执行恶意代码分析请求的进行状态。分为**待定**、**正在分析**、**完成**和**非对象**显示。
   - 查看结果：完成分析的项目将出现**查看报告**和**移动到网站**的链接。
     - 查看报告：点击可以查看恶意代码分析报告。
     - 移动到网站：点击可以移动到恶意代码分析服务网站。
   - 检查结果：显示执行恶意代码分析的结果。分为**恶意**、**正常**、**非对象**、**待定**、**可能正常**、**未知**、**受损**和**需要重新确认**显示。
   - 检查对象：显示发出恶意代码分析请求的对象文件名。
   - MD5：显示请求恶意代码分析的文件的 MD5 值。
   - 事件 ID：显示发出恶意代码分析请求命令的事件 ID。
   - 分析请求时间：显示请求恶意代码分析的时间。
   - 分析完成时间：显示完成恶意代码分析的时间。

参考

如要查看特定的分析请求，选择搜索条件（状态、检查结果）或输入关键词，然后点击  ，则符合条件的分析请求将显示在列表中。

参考

如要将搜索的分析请求结果列表下载的本地 PC，请点击**导出**。

恶意代码分析请求

1. 点击 Web 界面主菜单中的**响应情况**图标。
2. 选择**恶意代码分析请求**标签。

3. 点击**恶意代码分析请求**，弹出<恶意代码分析请求>窗口。
4. 点击**浏览...**选择要请求分析的可疑文件，或将文件拖放到指定的空间。
5. 点击**分析请求**，窗口将关闭。

第9章　统计分析

9.1　统计

MDS 提供各种统计分析结果，并根据这些结果生成报告模版。管理员可以通过直接在网页上查看报告并下载或打印到本地 PC 来应对安全威胁。

统计及报告类型

MDS 提供各种统计信息。每个统计结果都可以作为有用的资料来分析和响应安全威胁，以保护当前的系统。此外，统计结果可以作为报告保存或打印到本地 PC，与各部门共享。

提供的统计种类和相应生成的报告类型如下所述。

汇总

- 综合报告：摘要显示文件检测、异常流量检测、恶意 URL 检测、按途径/攻击阶段/诊断类型的检测统计、管理员确认统计、响应情况、已知/未知威胁统计等各种统计数据。
- 文件检测统计：显示 MDS 检测到的恶意文件的各种统计数据，如已知/未知威胁统计、按严重级别的检测统计、按文件类型的检测统计，并显示前 10 位的恶意文件和检测对象。
- 异常流量检测统计：显示 MDS 检测到的异常流量的各种统计数据，如已知/未知威胁统计、按严重级别的检测情况、按类型的检测情况，并显示检出的前 10 位的异常流量和访问异常流量的主机。
- 恶意 URL 检测统计：显示 MDS 检测到的恶意 URL 的各种统计数据，如已知/未知威胁统计、按严重级别的检测情况、按类型的检测情况，并显示检出的前 10 位的恶意 URL 和访问恶意 URL 的 Agent。

按途径的统计

- 按途径的检测统计：显示 MDS 检测到的按途径的威胁（文件、恶意异常流量和恶意 URL）的统计数据。

按类型的统计

- 按诊断类型的检测统计：显示 MDS 检测到的按诊断类型（文件、异常流量和恶意 URL）的威胁的统计数据。
- 按文件类型的检测统计：显示 MDS 检测到的按文件类型（可执行文件、文档文件、其他）的威胁的统计数据。

按攻击阶段的统计

- 按攻击阶段的检测统计：按攻击阶段（攻击尝试、攻击引入、C&C 服务器和数据泄漏）显示 MDS 检测到的威胁的统计数据。

管理员确认统计

- 管理员确认统计：显示管理员对 MDS 检测到的威胁的确认统计数据，分为“已确认”、“已确认（误诊）”、“待定”、“未确认”详细表示。

响应统计

- 响应统计：显示 MDS 响应（自动、手动）检出威胁的统计数据，状态分为“尝试”、“正在进行”、“成功”、“失败”。

按严重级别的统计

- 按严重级别的检测统计：按严重级别（高、中、低、灰色 2、灰色 1、可能正常、正常）显示 MDS 检测到的已知/未知威胁的统计数据。

已知/未知威胁统计

- 已知/未知威胁统计：按严重高级别（高、中、低）显示 MDS 检测到的未知/已知威胁（恶意文件、异常流量和恶意 URL）的统计数据。

按攻击位置的统计

- 按攻击位置的检测统计：在地图上表示 MDS 检测到的威胁的位置。表格则详细显示传播该威胁的国家/城市、检测次数和最近检测时间等统计数据。

参考

只有在互联网连接的情况下，才能在地图上确认相关信息。

检测次数排名

- 恶意文件检测次数排名：根据 MDS 检测到的恶意文件，按检测次数最多的顺序显示恶意文件名、收集路径、事件 ID、严重级别和检测次数等信息。
- 异常流量检测次数排名：根据 MDS 检测到的异常流量，按检测次数最多的顺序显示异常流量 IP、事件 ID、端口、攻击位置、严重级别、诊断名和检测次数等信息。
- 恶意 URL 检测次数排名：根据 MDS 检测到的恶意 URL，按检测次数最多的顺序显示恶意 URL、事件 ID、端口、攻击位置、严重级别、诊断名和检测次数等信息。
- 恶意邮件收件人检测次数排名：根据 MDS 检测到恶意邮件收件人，按检测次数最多的顺序显示收件人、文件数、恶意 URL 数和邮件接收次数。

- 恶意邮件发件人检测次数排名：根据 MDS 检测到恶意邮件发件人，按检测次数最多的顺序显示发件人、文件数、恶意 URL 数和邮件接收次数。

系统运营情况

- 系统资源：按时间显示 MDS 系统资源（CPU、内存、磁盘）的使用情况详细。
- 网络流量：按时间显示 MDS 网络发生的接收流量情况。
- Agent 连接状态：按时间显示 Agent 连接 MDS 的状态（已连接、未连接）。

导出或打印统计结果

将 MDS 提供的统计数据导出或打印。

1. 点击 Web 界面主菜单中的**统计**图标。
2. 在左侧菜单中选择欲导出或打印的项目。
3. 工具栏中选择期间，然后点击**查看**。
4. 下面将显示查询的统计结果。
5. 如要将结果导出，点击**导出**以 PDF 文件形式保存到本地 PC。
6. 如要将结果打印，点击**打印**。

第10章　报告分析

10.1 报告情况

通过日历一目了然地确认根据报告计划生成的报告状态，并且可以查看或下载详细的报告。

查看报告情况按如下操作：

1. 点击 Web 界面主菜单中的**报告**图标。
2. 选择**报告情况**标签。
3. 日历中表示的图标是根据报告计划生成的报告。将鼠标悬停在图标，则出现该报告的名称、周期和类型。
4. 如要查看报告，请点击报告图标。各报告图标表示如下内容。
   - 

：表示报告生成周期为“每日”的报告。
   - 

：表示报告生成周期为“每周”的报告。
   - 

：表示报告生成周期为“每月”的报告。
   - 

：表示报告生成周期为“每年”的报告。
   - 

：表示报告生成周期为“一次”的报告。

10.2 报告计划

将多个报告模版组合成一个综合报告，创建报告计划。综合报告可以在网页上查看，还可以下载或打印。

添加报告计划

1. 点击 Web 界面主菜单中的**报告**图标。
2. 选择**报告计划**标签。
3. 点击**添加**，弹出<添加报告计划>窗口。
4. 输入如下项目。
   - 报告名称：输入报告名称。
   - 周期：选择生成报告的时间。
   - 报告类型：选择报告类型。当选择“用户定义报告”时，下面将出现报告模版。选择您要生成的报告模版。

- 文件格式：选择报告文件的格式。
- 通过邮件接收报告：如要将定期生成的报告通过邮件接收，请选择复选，然后下面输入电子邮件地址。

5. 点击**保存**。

更改报告计划

1. 点击 Web 界面主菜单中的**报告**图标。
2. 选择**报告计划**标签。
3. 从报告列表中，鼠标双击欲更改的项目，弹出<更改共享文件夹扫描>窗口。
4. 更改所需的项目。
5. 点击**确定**。

删除报告计划

1. 点击 Web 界面主菜单中的**报告**图标。
2. 选择**报告计划**标签。
3. 在报告计划列表中，点击欲删除项目左侧的 ❌ 。
4. 如果弹出确认删除的对话框， 点击**确定**。

参考

在报告计划列表中，点击每个报告的最近创建日期旁边的【查看报告】，可以查看详细的报告内容。

第11章　系统管理

11.1 系统

系统状态

显示 MDS 设备的资源状态如 CPU、内存、磁盘和数据库使用率，系统信息和端口连接状态。

参考

点击各项目的设置图标( )，将移动到该项目的设置界面。

系统资源

显示 MDS 设备的资源使用率。每 5 秒更新一次。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统状态**。
3. 在系统资源栏中确认各项目如 CPU、内存、磁盘和数据库的使用率。

参考

可在管理 > 警报 > 警报条件设置中设置系统资源使用量阈值，当超过指定的阈值时，向指定的邮件地址发送警报邮件。

网络流量

显示网络流量状态。以当前时间为基准，显示设备所有接口的总流量吞吐量(Rx/Tx)，单位为 Kbps（千字节/秒）和 pps（每秒数据包）。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统状态**。
3. 在网络流量栏中确认网络流量状态。纵轴时网络流量处理速度值，横轴是每 10 秒左移的时间值。

虚拟机状态

显示虚拟机运行状态。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统状态**。
3. 在虚拟机栏中确认按运行状态虚拟机数量。虚拟机状态分别显示为等待、正在运行和错误。

- 等待：已准备检查文件的虚拟机数量
- 正在运行：正在检查文件的虚拟机数量
- 错误：连续 10 次发生错误的虚拟机数量

参考

除了上述的三个状态，虚拟机还有“正在准备”状态。“正在准备”状态是指正在更新或者重新启动中的虚拟机，因此也是正常运行的虚拟机。“正在准备”状态的虚拟机的数量仅通过用户 CLI 提供。

系统信息

显示 MDS 设备的基本信息、引擎更新和固件/虚拟机版本等信息。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统状态**。
3. 在系统信息栏中查看设备的各项信息。
   - 基本信息
     - 设备名：显示 MDS 设备的名称。为了在网络中识别各设备而赋予设备名，通过 SNMP 注册系统时赋予设备名。点击，移动到系统设置界面，更改设备名。
     - 联动 MDS manager：显示与 MDS Manager 的联动状态。当**策略继承**显示为 ON，则 MDS 设备联动 MDS Manage 并继承 MDS Manage 配置的策略。当传输日志显示为 ON，则表示 MDS 设备将日志传输到 MDS Manage 设备。点击，移动到联动设置界面，更改联动配置。
     - Agent 连接状态：显示已连接 MDS 设备的 Agent 数量。

参考

Agent 最大允许连接数为 5,000 台。如果超过该最大值，设备的性能有可能会降低。

   - 引擎更新
     - 静态分析引擎：显示 MDS 设备使用的静态分析引擎最近更新的时间。
     - 动态分析引擎：显示 MDS 设备使用的动态分析引擎最近更新的时间。
   - 固件/虚拟机版本
     - 固件：显示 MDS 设备的最近应用的固件版本。
     - 虚拟机：显示虚拟机的最近更新的版本。

网络接口

显示网络接口的连接状态和使用情况。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统状态**。
3. 在网络接口栏中查看网络接口的连接状态和使用情况。

- Down：显示网络接口已断开连接的数量。
- Up：显示网络接口已正常连接的数量。
- Off：显示网络接口禁用的数量。
- 接口：显示网络接口名称。
- IP：显示接口使用的 IP 地址。
- RX（bpx）：显示通过该接口入站的流量。
- TX（bpx）：显示通过该接口出站的流量。
- 监控接口：显示是否使用监控接口。

日志

可以搜索 MDS 设备收到的系统日志、引导安装 Agent 日志、Agent 管理日志和管理员事件日志。

> **参考**
> 该界面提供日志搜索功能。选择第一个下拉框中的日志类型，并输入搜索关键词，然后点击**搜索**键。

系统日志

显示管理员登录/注销、各项操作、引擎更新、接口连接状态、守护程序状态等系统发生的各种事件相关的日志。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>日志**。
3. 第一个下拉框中选择**系统日志**。显示以下信息：
   - 发生时间：显示日志发生的时间。
   - 日志内容：显示日志内容。

引导安装 Agent 日志

显示 MDS 检测到未安装 Agent 的主机的连接，并引导安装 Agent 的事件相关的日志。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>日志**。
3. 第一个下拉框中选择**引导安装 Agent**。显示以下信息：
   - 发生时间：显示日志发生的时间。
   - 主机 IP：显示访问引导安装页面的流量的源 IP 地址。
   - 目标 IP：显示访问引导安装页面的流量的目标 IP 地址。
   - 重定向地址：显示引导安装 Agent 的重定向地址（URL）。

Agent 管理日志

显示连接到 MDS 服务器的 Agent 发生的日志。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>日志**。
3. 第一个下拉框中选择 **Agent 管理**。显示以下信息：
   - 发生时间：显示日志发生的时间。
   - MDS 服务器名(IP)：显示 MDS 服务器的 IP 地址。
   - Agent IP：显示连接 MDS 服务器的 Agent 的 IP 地址。
   - Agent 名：显示连接 MDS 服务器的 Agent 的名称。
   - 日志内容：显示 Agent 发生的日志内容。内容包括 Agent 发生的开始、结束、策略的应用和应用结果、Agent 更新和更新结果、完整性检验和检验结果等。

管理员事件日志

显示管理员执行各种操作的事件日志。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>日志**。
3. 第一个下拉框中选择**管理员事件日志**。显示以下信息：
   - 发生时间：显示日志发生的时间。
   - 类别：显示管理员事件日志的分类。
   - 日志内容：显示日志内容。

参考

磁盘清理和日志备份可能会影响日志搜索。通过备份功能已进行备份的日志无法搜索。如要查看已备份的日志，需要先恢复日志。有关日志的备份和恢复的详细内容，请参考备份和恢复。

设备

可以查看和更改设备名称、时间和语言。

设备名称

更改设备名按如下步骤进行：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统设置**。
3. 在**新的设备名称**栏里输入新的设备名称。有效值为包括英文和数字 1~64 字节。

4. 点击**保存**。
5. 点击**应用更改配置**。

> **参考**
> 设备名是为了识别设备的目的而使用的名称，因此在运行多台设备的情况下，最好不要重复使用设备名。

设备时间

时间是记录事件和应用策略的重要标准，请正确设置时间。

时间设置按如下步骤进行：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统设置**。
3. 设置各项值：
   - 系统时间：显示当前 MDS 设备的时间。
   - 标准时区：从下拉框中选择时区。系统默认的标准时区是 **(GMT+09:00) Seoul, Tokyo**。
   - 时区设置方法：可以选择**与 NTP 服务器同步**或者**直接输入**方式。
     - 当选择**直接输入**时：点击 选择日期，并输入时间。
     - 当选择**与时间服务器同步**时：输入**时间服务器地址**和**运行同步时间**。

> **参考**
> 在应用直接输入的时间时，Web 界面访问可能暂时不可用。

4. 点击**保存**。
5. 点击**应用更改配置**。

设备语言

设置 MDS Web 界面使用的语言，设置语言的方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统设置**。
3. 从**设备语言**的下拉框中选择 MDS Web 界面使用的语言，默认值为**韩语**，可在**韩语、英语、中文(简体)**中选择。
4. 点击**保存**。
5. 点击**应用更改配置**。

> **参考**
> 通过 Web 界面登录时，也可以选择语言登录。

NFS/代理

网络文件系统（Network File System, NFS）是一种分布式文件系统协议，允许客户端计算机上的用户以与本地存储访问相似的方式通过网络访问文件。

NFS 设置

MDS 可将检测到的恶意文件保存到远程 NFS。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>NFS/代理**，打开<NFS/代理>界面。
3. 设置如下项目。
   - 启用 NFS：选择复选框，启用 NFS，可以向 NFS 传送文件。
   - NFS 服务器 IP：输入接收文件的 NFS 服务器的 IP 地址。
   - NFS 路径：输入 NFS 服务器中保存文件的目录。
4. 点击**保存**。
5. 点击**应用更改配置**。

参考

当未能连接到已配置的 NFS，文件临时保存到内部硬盘。

代理服务器设置

当跟新固件和引擎时，需要连接到网络。如果由于安全原因，无法直接连接到外部网络时，可以配置代理服务器。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>NFS/代理**，打开<NFS/代理>界面。
3. 设置如下项目。
   - 启用代理服务器：选择复选框，启用代理服务器以更新系统。
     - 代理服务器 IP：输入代理服务器的 IP 地址。
     - 端口号：输入代理服务器的端口号。
   - 启用代理服务器认证：选择复选框，则在登录代理服务器时使用身份验证。
     - ID：输入代理服务器登录 ID。
     - 密码：输入代理服务器登录密码。
4. 点击**保存**。
5. 点击**应用更改配置**。

SNMP

简单网络管理协议（Simple Network Management Protocol, 简称为 SNMP）是用于复杂网络管理的一套协议。MDS 利用 SNMP 协议来监控网络连接设备的状态。

如何配置使用 SNMP

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>SNMP**。
3. 首先配置 SNMPv2 共同体。输入下面的内容后，点击 完成。如要删除已添加的项目，请点击 。
   - 共同体名：输入 SNMP 共同体名称。public 或者 private 存在安全漏洞，因此请不要使用该类名称。
   - IPv4/CIDR：输入 SNMP 共同体的 IPv4 地址和 CIDR。
   - 描述：输入有关 SNMPv2 的信息。
4. 如果需要与 SNMPv3 服务器进行通信，请配置 SNMPv3 用户。输入下面的内容后，点击 完成。如要删除已添加的项目，请点击 。
   - 用户名：输入 SNMPv3 用户的名称。public 或者 private 存在安全漏洞，因此不要使用该类名称。
   - 哈希算法：选择用于用户认证的算法。
   - 认证密码：输入认证密码。
   - 加密算法：选择信息加密的算法。
   - 加密密钥：输入信息加密的密钥。
   - IPv4/CIDR：输入与 SNMPv2 进行通信的网络或主机的 IPv4 地址/ CIDR。
   - 描述：输入有关 SNMPv3 的信息。
5. 选择**启用 SNMP** 前面的复选框，启用 SNMP 服务。
6. 点击**保存**。
7. 点击**下载 MIB**，将下载的 MIB 文件注册到 NMS 主机。

如何终止使用 SNMP

解除选择**启用 SNMP** 前面的复选框，即可终止 SNMP 服务。

> ⚠**注意**
>
> SNMP 共同体名称用于 SNMP 的认证。常用于共同体名的“public”或“private”存在安全漏洞，因此不要该类名称。

文件下载

如果将 MDS 检测到的恶意文件（MD5）下载到本地 PC，则会将其保存为压缩文件。此时，如果要以带有密码的压缩文件形式下载检测到的恶意文件，可以设置使用压缩文件密码。

下载压缩文件时设置密码的方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>文件下载**。
3. 选择“**压缩文件使用密码进行下载**”前面的复选框，然后输入 8 到 20 个字符的密码。
4. 点击**保存**。

参考

要查看已设置的密码，请单击  。

许可证

本章将介绍如何将您获取的 MDS 各模块的许可证注册到 MDS 设备。

如何查看许可证信息?

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>许可证**，打开<许可证>界面。
3. 可以确认如下信息。
   - 型号名称：显示设备的型号。
   - 设备 ID：设备 ID 是识别设备的唯一标识符。
   - 产品编号：显示设备的产品序列号。产品序列号必须与购买产品时获取的产品序列号一致。
   - 许可证类型：显示设备当前正在使用的许可证列表。
   - 注册与否：显示许可证的注册与否。
   - 注册许可证：点击**注册**，打开注册许可证界面。
   - 注册日期：显示注册许可证的时间。
   - 到期日：显示许可证到期日。

如何注册许可证?

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>许可证**，打开<许可证>界面。
3. 选择欲注册许可证的项目，点击**注册**，弹出注册许可证窗口。

4. 根据许可证类型，输入许可证密钥或者启用该服务。
   - 镜像设备：在弹出的<注册镜像设备许可证>窗口中，输入许可证密钥后点击**确定**。
   - 云（Beta）服务：点击注册，弹出<云(Beta)服务>窗口，选择复选框启用该服务，然后点击**我同意**。
   - 恶意代码分析请求服务：选择复选框启用该服务并输入分析服务的 **ID** 和**密码**，然后点击**确定**。
5. 点击**确定**。
6. 点击**应用更改配置**。

参考

许可证到期，则无法更新产品。更改许可证，只能由授权的管理员才可以进行。如需要更新许可证，请向 AhnLab 或者销售产品的代理商询问。

系统诊断报告

如果 MDS 设备发生故障，可以导出综合系统诊断报告，并向 AhnLab 请求分析。通过分析报告，可以确认系统故障的原因。导出系统诊断报告的方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统>系统诊断报告**。
3. 单击**导出**，弹出<导出系统诊断报告>窗口。
4. 如果已有生成的报告，将显示文件名和下载链接。点击[**下载**]，将报告文件保存到本地 PC 的临时下载文件夹中。
5. 如要创建的新的报告，点击**导出**以生成新的报告文件“troubleshooting.enc”，并将其保存到本地 PC 的临时下载文件夹中。
6. 将文件“troubleshooting.enc”转发给 AhnLab 进行分析。

参考

troubleshooting.enc 文件可能包含系统重要信息，为了安全起见文件被加密。文件内容只有 AhnLab 分析专家通过专用工具解密后可以确认。

参考

根据报告文件的大小或网络连接状态，从生成报告到完成导出可能需要很长时间。

证书

MDS 提供更新 Web 服务使用的 SSL 证书的功能。

查看证书

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统 > 证书**。
3. 出现<证书>界面。
4. 如果已有上传的证书，可以查看如下信息。

- 证书：点击**[查看]**，弹出<查看证书>窗口，可以查看上传的证书内容。
- 证书文件：可以查看扩展名为 cert 的证书文件名称。
- 证书密钥文件：可以查看扩展名为 kev 的证书密钥文件名称。

更新证书

更新证书按如下步骤进行。

> ⚠**注意**
>
> 更新证书后，Web 服务将重新启动，这可能会导致服务一时中断。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**系统 > 证书**。
3. 出现<证书>界面。
4. 点击证书文件的**浏览...**，选择要更新的证书文件。
5. 点击证书密钥文件的**浏览...**，选择要更新的证书密钥文件。
6. 点击**上传**。
7. 点击**更新**。

11.2 备份和恢复

备份设置

MDS 可将系统配置、日志和统计数据进行备份。由于本地磁盘保存空间有限，为了安全保存 MDS 本地磁盘保存的日志和数据，请指定备份设置，并定期进行备份。

共同设置

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>备份设置**。
3. 输入共同设置的各项值。自动备份和手动备份时，应用共同设置指定的各种设置进行备份。
   - 保留原始数据：启用复选框，即使运行备份，原始数据还将保留在本地系统中。
   - 备份数据分割：启用复选框，备份数据将分割为指定的分割大小。
     - 分割大小：输入分割大小，将备份数据分割成指定的大小。
   - 备份位置：选择备份数据保存的位置，可以选择本地磁盘、FTP 服务器或 SFTP 服务器。当备份位置选择“FTP”或“SFTP”时，需要输入 **FTP 地址**或 **SFTP 地址**、**FTP 端口号**或 **SFTP 端口号**、**备份路径**、连接 FTP 或 SFTP 的 **ID** 和**密码**。
4. 点击**保存**。

参考

如果备份位置选择“本地磁盘”，则备份文件（*.tar）将保存在“root/data/backup/”路径中。

自动备份

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>备份设置**，打开<备份设置>界面。
3. 配置自动备份设置。系统将按照指定的时间对指定的对象进行备份。
   - 启用自动备份：选择复选框，启用自动备份功能。

- 备份对象期间：输入自动备份数据的范围。如果输入 30 天，则备份对象是 30 天前的数据。
- 备份项目和时间：选择备份项目和备份时间。备份项目将在指定的时间定期执行备份。

4. 点击**保存**。

手动备份

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>备份设置**，打开<备份设置>界面。
3. 输入手动备份的各项值。
   - 备份对象期间：指定备份数据的期间。
   - 备份项目：选择手动备份的项目
4. 点击**立即备份**。

按日期备份

MDS 还提供备份每日日志数据的功能。

按日期备份数据的方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>按日期备份**，打开<按日期备份>界面。
3. 如要保留原始数据，请选择**启用**复选框。
4. 选择您要备份的日期，点击  ，弹出“**是否现在进行备份?**”提示，点击**确定**。

参考

按日期的备份列表最多显示最近 30 天的备份对象。备份数据将保存到**管理>备份设置**界面的**共同设置**中指定的保存位置。

恢复备份数据

恢复保存在本地磁盘或 FTP 服务器中的备份数据。

恢复备份的数据的方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>恢复备份数据**，打开<恢复备份数据>界面。
3. 点击**导入**，弹出<导入恢复对象>对话框。
4. 指定欲恢复数据的各种选项。
   - 备份位置：选择备份数据保存的位置。当备份位置选择“FTP”或“SFTP”时，需要输入 **FTP 地址**或 **SFTP 地址**、**FTP 端口号**或 **SFTP 端口号**、**备份路径**、连接 FTP 或 SFTP 的 **ID** 和**密码**。

- 备份期间：指定备份数据时间范围。
- 备份项目：选择备份项目。

5. 点击**确定**，关闭对话框，界面显示符合指定条件的备份文件列表。
6. 从列表中选择欲恢复的文件，然后点击**恢复**。
7. 如要下载备份文件到本地计算机，请点击欲下载文件左侧的**下载**图标。
8. 如要删除备份文件，请点击欲删除文件左侧的**删除**图标。

配置文件的备份和恢复

备份或恢复当前系统的配置文件和与配置相关的数据库转储数据。

备份配置文件

备份配置文件的过程如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>配置文件的备份和恢复**。
3. 在**备份配置文件**中，输入**密码**。密码必须介于 8 到 15 个字符之间，并且要包括英文字母、数字和特殊字符。
4. 单击**备份**按钮进行配置文件的备份。
5. 备份完成后，将生成备份文件(conf.enc)并保存在 PC 上。

参考

备份文件(conf.enc)的保存位置取决于本地 PC 的浏览器设置。

恢复配置文件

使用备份文件恢复配置文件的过程如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**备份和恢复>配置文件的备份和恢复**。
3. 在**恢复配置文件**中，单击浏览...选择要恢复的备份文件。
4. 输入**密码**。此密码是在备份时设置的密码。
5. 单击**恢复**按钮进行恢复。
6. 恢复完成后，系统会自动重启以应用恢复的配置文件。

11.3 网络

接口

管理 MDS 网络的物理接口和逻辑接口，并根据 MDS 所在网络环境特性，配置各种形式的接口。

更改网络接口

更改网络接口的方法如下。

参考

网络接口是物理构成的接口，因此无法添加或删除，但可以更改。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在网络接口列表中，鼠标双击欲更改的接口，打开<更改网络接口>界面。
4. 更改所需的项目。
   - 启用：显示网络接口的启用状态。
   - 名称：显示网络接口的名称，无法更改。
   - IP 分配：选择 IP 地址的分配方式。
     - 固定：物理接口分配固定的 IP 地址。
     - DHCP：物理接口不分配固定的 IPv4 地址，分配 DHCP 服务器自动分配的 IPv4 地址。
   - IPv4 地址：当类型选择 ‘固定’ 的时候输入 IPv4 地址，分配给网络接口。
   - IPv6 地址：当类型选择 ‘固定’ 的时候输入 IPv6 地址，分配给网络接口。
   - 访问控制：选择必要的协议，通过网络接口管理 MDS 设备。
   - 最大传输单位（MTU）：设置 MTU，有效值为 100~1500，默认值为 1500。
   - 通信模式：显示网络接口的传输速度和方式。
     - Auto：自动设置速度和方式。
     - 10Mbps 半双工：使用 10Mbps 半双工传输（Half Duplex）方式设置速度和方式。
     - 10Mbps 全双工：使用 10Mbps 全双工传输方式（Full Duplex）设置速度和方式。
     - 100Mbps 半双工：使用 100Mbps 半双工传输（Half Duplex）方式设置速度和方式。
     - 100Mbps 全双工：使用 100Mbps 全双工传输方式（Full Duplex）设置速度和方式。
     - 1000Mbps 全双工：使用 1000Mbps 全双工传输方式（Full Duplex）设置速度和方式。

参考

全双工传输（Full Duplex）是指在一个接口同时进行双向通信的方式。半双工传输（Half Duplex）也是一个接口双向通信，但是一次只能向一个方向通信。如果设置为 **自动**，则检查接口并自动设置为最合适的通信模式。若无法得知通信模式或无法设置适当速度时，请选择**自动**。

- MAC 地址：显示网络接口的 MAC 地址。
- 输入描述：输入最多 63 个字符的描述。

5. 点击**确定**。
6. 点击**应用更改配置**。

配置聚合接口

可以组合多个物理接口，并将其配置为可以高速处理数据的一个逻辑接口。配置聚合接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择**聚合**，则出现<添加聚合接口>界面。
4. 设置各项目。
   - 启用：选择复选框启用接口。如果不启用接口，则只添加接口，而不使用。
   - 名称：输入聚合接口的名称，组合英文和数字，且不能超过 15 个字符。
   - 运行模式：选择聚合接口的运行模式。
     - Active-Backup：在基本物理接口发生问题时，由备用物理接口代替工作。虽然产生容错（fault tolerance），但没有负载均衡（Load balancing）。
     - Active-Active：所有的物理接口都能正常工作，所以会有容错和负载均衡。
     - 802.3ad：将支持动态聚合，所有的物理接口都能正常工作，所以会有容错和负载均衡。
   - 网络接口：选择以聚合方式配置的物理接口，必须选择两个以上。
   - IPv4 地址：设置接口使用的 IPv4 地址和 CIDR。
   - IPv6 地址：设置接口使用的 IPv6 地址和 CIDR。
   - 访问控制：选择必要的协议，通过网络接口管理 MDS 设备。
   - 最大传输单位（MTU）：设置 MTU，有效值为 100~1500，默认值为 1500。
   - 输入描述：输入最多 63 个字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改聚合接口

更改聚合接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 鼠标双击聚合接口列表中的欲更改项目，打开<更改聚合接口>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除聚合接口

删除聚合接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在聚合接口列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

配置 Tap 接口

可以配置一个既可以监控流量而不影响网络流量的 TAP 接口。配置 Tap 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择 **Tap**，则出现<添加 Tap 接口>界面。
4. 设置各项目。
   - 启用：选择复选框启用接口。如果不启用接口，则只添加接口，而不使用。
   - 名称：输入 Tap 接口的名称，组合英文和数字，且不能超过 15 个字符。
   - 选择接口：从下拉框中选择网络接口。
   - 配对接口：根据选择接口，自动显示。
   - 最大传输单位（MTU）：设置 MTU，有效值为 1000~1500，默认值为 1500。
   - 输入描述：输入最多 63 个字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改 Tap 接口

更改 Tap 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 鼠标双击 Tap 接口列表中的欲更改项目，打开<更改 Tap 接口>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 Tap 接口

删除 Tap 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在 Tap 接口列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

配置 VLAN 接口

可以通过将其逻辑接口分割成多个接口，当作多个虚拟网络来使用。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择 **VLAN**，则出现<添加 VLAN 接口>界面。
4. 设置各项目。
   - 启用：选择复选框启用接口。如果不启用接口，则只添加接口，而不使用。
   - 名称：输入聚合接口的名称，组合英文和数字，且不能超过 15 个字符。
   - VLAN ID：输入 VLAN ID。VLAN ID 可以是 1 到 4095 之间的任何数字。
   - 网络接口：从下拉框中，选择连接到 VLAN 的接口。
   - IPv4 地址：设置接口使用的 IPv4 地址和 CIDR。
   - IPv6 地址：设置接口使用的 IPv6 地址和 CIDR。
   - 访问控制：选择必要的协议，通过网络接口管理 MDS 设备。
   - 最大传输单位（MTU）：设置 MTU，有效值为 100~1500，默认值为 1500。
   - 输入描述：输入最多 63 字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改 VLAN 接口

更改 VLAN 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 鼠标双击 VLAN 接口列表中的欲更改项目，打开<更改 Tap 接口>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 VLAN 接口

删除 VLAN 接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 在 VLAN 接口列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

参考

配置逻辑接口（聚合，Tap，VLAN）的物理接口即网络接口的状态必须是启用，而且一个网络接口不能在多个逻辑接口中同时使用。

参考

IPv4 地址/CIDR 有效范围：IPv4 地址需要输入 0.0.0.0~255.255.255.255 之间；CIDR 需要输入 0~32 之间。
IPv6 地址/CIDR 有效反问：IPv6 地址需要输入 ::~ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff 之间；CIDR 需要输入 0~128 之间。

配置监控接口

MDS 镜像流入网络的流量，以检测恶意代码和异常流量。为了检查流量，物理连接镜像接口到 MDS 设备，然后在 MDS 设备上设置监控接口。因此，在配置监控接口之前，必须配置用于监控的接口。

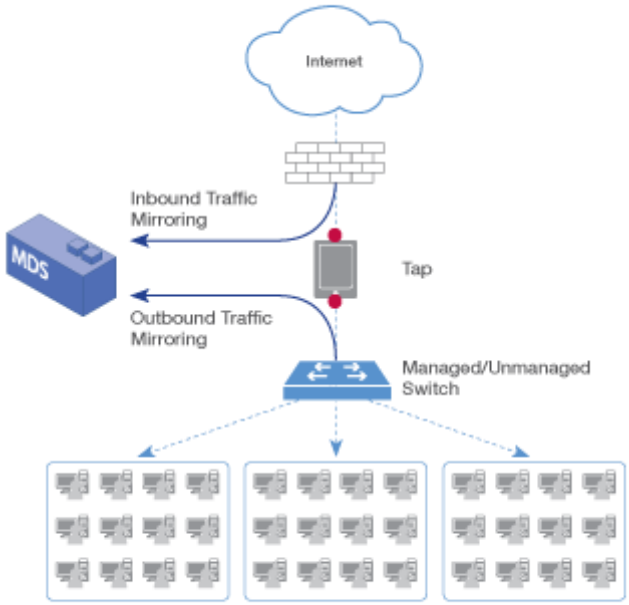
参考

未指定为监控接口的接口默认状态称为管理接口。

镜像接口可以通过多种方式进行配置，例如连接 Tap 设备或交换机/路由器的镜像接口。通过配置的镜像接口将流量传送到 MDS 设备进行监控。

下面的示例使用 Tap 来镜像网络顶部上的所有入站/出站的流量。将两个物理接口连接到 MDS 的 eth2 和 eth3，以分别接收 Rx、Tx 流量。

将上述配置镜像的内容用图表示如下：



- MDS 连接两个物理接口（eth2，eth3），分别接收 Rx 和 Tx 流量
- 配置聚合接口，使接收 MDS 镜像的流量的网络接口视为逻辑上一个接口
- 监控所有 LAN 和 WAN 流量

根据上面的示例来配置监控接口的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>接口**。
3. 点击**添加**键，选择**聚合**，则出现<添加聚合接口>界面。
4. 设置各项目。
   - 启用：选择复选框。
   - 名称：输入 agg0。
   - 运行模式：选择 Acitve-Active。
   - 网络接口：选择 eth2 和 eth3。
   - IPv4 地址：输入 0.0.0.0/0。
   - 访问控制：不选择。

- 最大传输单位（MTU）：输入 1500。

5. 点击**确定**。

参考

完成聚合接口配置后，网络接口列表中的 eth2 和 eth3 更改为 0.0.0./0（默认路由器）。

6. 点击**配置监控接口**，弹出<配置监控接口>窗口。
7. 从列表中选择 **agg0**。
8. 点击**确定**。
9. 点击**应用更改配置**。

参考

最多可以选择 4 个接口为监控接口。

参考

应用邮件过滤的网络接口应与检测检测恶意代码和异常流量的网络接口区分。检测恶意代码和异常流量的监控接口应配置为镜像流量，用于邮件过滤的网络接口应在邮件服务器和外部网络之间内联。

路由

为 MDS 设备的互联网通信配置默认路由，并根据需要配置源路由和目标路由。

添加 IPv4 路由

添加 IPv4 路由的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 点击**添加**键，选择**添加 IPv4 路由**，则出现<添加 IPv4 路由>界面。
4. 设置各项目。
   - 优先级：输入源路由的优先级，优先级可输入 1~128 之间的整数，不能与已存在的优先级重复。
   - 类型
     - 源路由：主机接收到的数据包的源 IP 地址为标准设置 IPv4 路由。
     - 目标路由：主机接收到的数据包的目标 IP 地址为标准设置 IPv4 路由。
   - 源 IP：如果选择源路由，则输入应用源路由的 IPv4 地址和 CIDR 值。来自源 IP 的流量路由到源路由指定的网关。
   - 目标 IP：如果选择目标路由，则输入应用目标路由的 IPv4 地址和 CIDR 值。来自目标 IP 的流量路由到目标路由指定的网关。
   - 网关：输入路由路径的网关地址。

- 网络接口：选择用于路由的接口。
- 输入描述：输入最多 63 字符的描述。

5. 点击**确定**。
6. 点击**应用更改配置**。

更改 IPv4 路由

更改 IPv4 路由的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 鼠标双击 IPv4 路由列表中的欲更改项目，打开<更改 IPv4 路由>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 IPv4 路由

删除 IPv4 路由的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 在 IPv4 路由列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

添加 IPv6 路由

添加 IPv6 路由的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 点击**添加**键，选择**添加 IPv6 路由**，则出现<添加 IPv6 路由>界面。
4. 设置各项目。
   - 优先级：输入路由的优先级，优先级可输入 1~256 之间的整数，不能与已存在的优先级重复。
   - 类型
     - 默认路由：对于作为所有路由的基础的 IP 地址，并且没有被指定为源路由或目标路由，系统向网关发送请求处理数据包。如果配置了默认路由，则默认路由不会显示在选项中。
     - 源路由：主机接收到的数据包的源 IP 地址为标准设置 IPv4 路由。
     - 目标路由：主机接收到的数据包的目标 IP 地址为标准设置 IPv4 路由。

- 源 IP：如果选择源路由，则输入应用源路由的 IPv6 地址和 CIDR 值。来自源 IP 的流量路由到源路由指定的网关。
- 目标 IP：如果选择目标路由，则输入应用目标路由的 IPv6 地址和 CIDR 值。来自目标 IP 的流量路由到目标路由指定的网关。
- 网关：输入路由路径的网关地址。
- 网络接口：选择用于路由的接口。
- 输入描述：输入最多 63 字符的描述。

5. 点击**确定**。
6. 点击**应用更改配置**。

参考

默认路由在开始时只配置一次。

更改 IPv6 路由

更改 IPv6 路由的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 鼠标双击 IPv6 路由列表中的欲更改项目，打开<更改 IPv6 路由>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 IPv6 路由

删除 IPv6 路由的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 在 IPv6 路由列表中选择欲删除项目 左侧的 ， 弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

参考

IPv4 地址/CIDR 有效范围：IPv4 地址需要输入 0.0.0.0~255.255.255.255 之间；CIDR 需要输入 0~32 之间。
IPv6 地址/CIDR 有效范围：IPv6 地址需要输入 ::~ffff.ffff.ffff.ffff.ffff.ffff.ffff.ffff 之间；CIDR 需要输入 0~128 之间。

监控路由

可以查看系统使用的所有静态路由表，包括管理员在系统中指定的静态路由路径。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>路由**。
3. 点击**监控**，弹出<监控路由>界面。
4. 监控列表中，显示内容如下。（可以选择 **IPv4** 或 **IPv6** 标签）
   - 总计：显示路由表中注册的项目总数。
   - 优先级：显示路由的优先级。
   - 源 IP：显示应用路由的源 IP 地址。
   - 目标 IP：显示应用路由的目标 IP 地址。
   - 网关：显示路由路径的网关地址。
   - 接口：显示路由使用的物理，逻辑网络的接口。
   - 标记：显示路由的状态。
     - U：表示路由路径有效(RTF_USABLE)
     - G：表示该路径已连接到网关(RTF_GATEWAY)
     - H：表示该路径已连接到主机(RTF_HOST)

DNS

设置设备所使用的域名服务器（DNS）用于域地址查询。设置 DNS 服务器的方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>DNS**。
3. 设置各项目。
   - 首选 DNS 服务器：输入执行 DNS 查询时使用的第一个 DNS 服务器的 IP 地址。
   - 备用 DNS 服务器：输入首选 DNS 服务器未响应 DNS 查询时使用的 DNS 服务器的 IP 地址。
   - 本地域名：输入英文字母、数字和句号（.)组合的 0~64 字符的本地域名。
4. 点击**确定**。
5. 点击**应用更改配置**。

参考

备用 DNS 服务器是选项。

参考

本地域名通过诸如 mDNS 等服务在网站有限使用。

内部服务器 IP 设置

可以在 MDS 管理的网络内分配多个 IP 带宽。因此，在需要通过检查所收集的数据来源和途径来追踪的时候，需要能够区分每个数据是从内部移动到内部还是外部移动到内部。为此，MDS 分别注册和管理内部网络。

设置内部服务器 IP

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>内部服务器 IP 设置**。
3. 点击**添加**键，则出现<添加内部服务器 IP>界面。
4. 设置各项目。
   - IP 地址：输入内部服务器 IP 地址和 CIDR。
   - 输入描述：输入最多 63 字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改内部服务器 IP

更改内部服务器 IP 的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>内部服务器 IP 设置**。
3. 鼠标双击内部服务器 IP 列表中的欲更改项目，打开<更改内部服务器 IP>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除内部服务器 IP

删除内部服务器 IP 的方法如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**网络>内部服务器 IP**。
3. 在内部服务器 IP 列表中选择欲删除项目 左侧的 ✕ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

导入内部服务器 IP

在 Web 界面， 您只能逐一添加内部服务器 IP 地址。如果要一次添加多个项目，可以将要添加的 IP 地址列表创建 CSV 文件，然后单击**导入**键即可。将内部服务器 IP 地址列表创建为 CSV 文件的方法如下。

```
IP 地址 / 网络掩码 描述
```

参考

要将添加的内部服务器 IP 地址列表以 CSV 文件保存到本地 PC，点击**导出**即可。

11.4 管理员

管理员帐户

产品支持多个管理员同时登录到系统。当然，帐户管理权限（包括创建、更改或删除帐户）仅授予具有最高权限的管理员。这是因为多个管理员同时登录到系统并同时进行配置更改，可能会导致系统冲突。具有完全权限的最高管理员帐户只能创建一个。

管理员帐户的权限类型

MDS 提供如下管理员帐户的权限类型。

- 超级管理员：具有完全权限的最高管理员。可以控制和管理 MDS 设备所有功能，包括系统配置和所有安全策略。
- 策略管理员：具有不完全权限的管理员，仅对部分策略具有管理权限。
- 一般管理员：对于设置和所有安全策略仅提供只读权限。

以下是各帐户权限的说明。

帐户类型		超级管理员		策略管理员		一般管理员	
权限范围		只读	读写	只读	读写	只读	读写
仪表板	摘要	O	-	O	-	O	-
	威胁趋势	O	O	O	O	O	X
	监视对象	O	O	O	O	O	X
检测情况	检测情况	O	O	O	O	O	X
	主机	O	O	O	O	O	X
	文件	O	O	O	O	O	X
	C&C 服务器	O	O	O	O	O	X
	恶意 URL	O	O	O	O	O	X

	引入途径		O	O	O	O	O	X
响应情况	响应情况		O	O	O	O	O	X
	隔离区		O	O	O	O	O	X
	隔离系统		O	O	O	O	O	X
	收集可疑文件		O	O	O	O	O	X
	Pinpoint 扫描		O	O	O	O	O	X
	恶意代码分析请求		O	O	O	O	O	X
统计	统计		O	O	O	O	O	X
报告	报告情况		O	O	O	O	O	X
	报告计划		O	O	O	O	X	X
管理	系统	系统状态	O	-	O	-	O	-
		日志	O	O	O	O	O	X
		系统设置	O	O	X	X	X	X
		NFS/代理	O	O	X	X	X	X
		SNMP	O	O	X	X	X	X
		许可证	O	O	X	X	X	X
		系统诊断报告	O	O	O	O	X	X
	备份和恢复	备份设置	O	O	O	O	X	X
		按日期备份	O	O	O	O	X	X
		恢复备份数据	O	O	X	X	X	X
	网络	接口	O	O	X	X	X	X
		路由	O	O	X	X	X	X
		DNS	O	O	X	X	X	X
		内部服务器 IP	O	O	X	X	X	X
	管理员	管理员帐户	O	O	X	X	X	X
		管理员 IP 地址	O	O	X	X	X	X
		帐户策略	O	O	X	X	X	X
		管理员确认	O	O	X	X	X	X
	更新	更新	O	O	O	O	X	X
	警报	警报邮件	O	O	X	X	X	X
		警报条件	O	O	X	X	X	X
	联动	MDS Manager	O	O	X	X	X	X
		CEF	O	O	O	X	X	X

		LEEF	O	O	O	X	X	X
		外部日志服务器	O	O	X	X	X	X
		Active Directory 服务器	O	O	X	X	X	X
		第三方	O	O	X	X	X	X
	Agent	Agent 列表	O	O	O	O	O	X
		默认设置	O	O	O	X	X	X
		Agent 策略	O	O	O	X	X	X
		安装 Agent 网络	O	O	O	X	X	X
		安装 Agent 例外网络	O	O	O	X	X	X
		上传 Agent 修补程序	-	O	-	X	-	X
	共享文件夹	共享文件夹	O	O	X	X	X	X
	检测和响应	检测设置	O	O	X	X	X	X
		VirusTotal	O	O	O	X	X	X
		YARA 规则	O	O	X	X	X	X
		响应设置	O	O	X	X	X	X
		威胁警报	O	O	X	X	X	X
		黑名单	O	O	O	O	X	X
		白名单	O	O	O	O	X	X
		检测例外	O	O	O	O	X	X
工具	发送通知		O	O	O	O	X	X
	Pinpoint 扫描		O	O	O	O	X	X
	完整性检验		O	O	O	O	X	X
	MDS 2.1.9 日志		O	O	O	O	X	X
	系统关闭/重启		O	O	X	X	X	X

参考

标记“X”表示该功能在 Web 界面上不可见。

添加管理员帐户

按如下步骤创建管理员帐户：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员帐户**。
3. 点击**添加**键，打开<添加管理员帐户>界面。

4. 点击**基本信息**标签，输入如下项目。
   - 帐户权限：从下拉框中选择管理员的帐户权限类型。
   - ID：输入管理员 ID。请输入 5~64 个字符，且必须包含英文字母、数字和特殊符号（_ . @）。
   - 密码安全级别：选择密码的安全级别。
     - 中：如果选择‘中’，密码必须使用 9~15 个字符内的英文、数字和特殊符号（$ & ' " < > 除外）组合。
     - 高：如果选择‘高’，密码必须使用 15 个字符的英文、数字和特殊符号（$ & ' " < > 除外）组合。
   - 密码：根据选择的安全级别输入管理员的密码。

参考

如要防止旧密码再使用，请到管理 > 管理员 > 帐户策略中启用**限制使用旧密码**选项。

参考

不适合作为密码的情况如下。
- 没有包含英文字母或数字或特殊字符
- 像 ab， bc，cd，de，ef，按顺序或者倒序排列 5 个以上英文字母或数字的情况（例如：abcdef13!）
- 反复使用同一数字或文字三次以上（例如：aaa，111）
- 不能使用的特殊符号为 $ & ' " < >

   - 确认密码：再次输入密码。
   - 密码更新周期：启用复选框，然后输入密码更新周期。有效值为 0~365 日，如果输入“0”，则不设置密码更新周期。
   - 电子邮件地址：输入管理员的电子邮件地址。
   - 输入描述：输入最多 63 字符的描述。

5. 点击**允许访问 IP 设置**标签，设置允许访问的 IP 地址。选择 **IPv4** 或 **IPv6**，输入 **IP 地址**后点击 。

参考

允许访问 IP 地址不能超过 10 个，但超级管理员不能超过 2 个。

6. 点击**注册验证密钥**标签，注册验证密钥。如果注册验证密钥，则可以通过发送验证密钥值来建立 SSH 连接，而无需在登录时输入密码。
   - 注册与否：显示建立 SSH 连接时使用的验证密钥的注册与否。如果已注册，则显示 ；如果未注册，则显示 。点击**浏览...**选择验证密钥文件或拖放要注册的验证密钥文件，然后点击**确定**。
7. 点击**确定**。
8. 点击**应用更改配置**。

更改管理员帐户

1. 在管理员帐户列表中，鼠标双击欲更改的帐户，弹出<更改管理员帐户>界面。
2. 更改各项值。
3. 点击**确定**。
4. 点击**应用更改配置**。

删除管理员帐户

1. 在管理员帐户列表中选择帐户(可以多选)，然后点击**删除**键，或者点击 ID 左侧的 ✕ ，弹出删除对话框。
2. 点击**确定**。

管理员 IP 地址

设置 IP 地址范围，允许属于该 IP 地址范围的管理员登录设备。

添加管理员 IPv4 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员 IP 地址**。
3. 点击**添加**键，选择 **IPv4**，则出现<添加管理员 IPv4 地址>界面。
4. 设置各项目。
   - IPv4 地址：输入 IPv4 形式的 IP 地址范围。（如：192.168.1.0 /24）。
   - 输入描述：输入最多 63 字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改管理员 IPv4 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员 IP 地址**。
3. 鼠标双击列表中的欲更改项目，打开<更改管理员 IPv4 地址>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除管理员 IPv4 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员 IP 地址**。

3. 在列表中选择欲删除项目 左侧的 ❌ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

添加管理员 IPv6 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员 IP 地址**。
3. 点击**添加**键，选择 **IPv6**，则出现<添加管理员 IPv6 地址>界面。
4. 设置各项目。
   - IPv6 地址：输入 IPv6 形式的 IP 地址范围。（如：2001: db8:1234:5678:ab:cd:ef:1/128）
   - 输入描述：输入最多 63 字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改管理员 IPv6 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员 IP 地址**。
3. 鼠标双击列表中的欲更改项目，打开<更改管理员 IPv6 地址>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除管理员 IPv6 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员 IP 地址**。
3. 在列表中选择欲删除项目(可以多选)，然后点击**删除**键，或者点击 ❌ ，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

⚠注意

即使系统中注册了管理员 IP 地址，系统的管理端口未设置为允许 HTTP 或者 SSH 连接，无法进行通信。请参考网络端口，设置为网络接口允许 HTTP 和 SSH 连接，使可以与管理员 IP 地址进行通信。

⚠注意

如果管理员系统和 MDS 设备之间存在 NAT 设备，MDS 可以识别的 IP 地址是转换后的 IP 地址。由于通过 NAT 设备有可能会发生未受到认可的访问，因此需要配置单独的 NAT 或路由策略以连接管理员 IP 地址。

帐户策略

设置管理员帐户、密码、会话和登录有关的各种策略。

帐户锁定设置

设置登录 Web 界面时的最大登录失败次数。当登录失败超过允许次数时，锁定帐户。锁定时间也可以指定。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 帐户策略。**
3. 输入**帐户锁定设置**的各项目。
   - 登录失败次数：输入允许登录失败的最大值，有效值为 1~5。
   - 锁定时间：输入登录失败次数超过限制时，限制登录的时间，有效值为 5~360。
4. 点击**保存。**
5. 点击**应用更改配置。**

限制使用旧密码

为了安全限制重复使用相同的密码。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **管理员 > 帐户策略。**
3. 设置限制使用旧密码的各项值。
   - 限制使用旧密码：选择复选框，将启用限制使用旧密码功能。
   - 旧密码重复使用限制次数：输入 1~5 之间的值。
4. 点击**保存。**
5. 点击**应用更改配置。**

会话超时设置

设置会话超时时间，当登录后，设置的时间没有任何操作，则自动注销。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 帐户策略。**
3. 设置会话超时时间。
   - 会话超时：选择复选框，将启用会话超时功能。
   - 等待时间：输入时间（分钟），可以输入 10~1440 之间的值。
4. 点击**保存。**
5. 点击**应用更改配置。**

SSH 连接设置

设置 SSH 连接，当访问设备时使用的登录方式是认证密钥值而不是 ID 和密码方式， SSH 连接提供比密码方式更高的安全性。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 帐户策略**。
3. 在 SSH 连接设置，单击**浏览...**选择管理员为 SSH 连接创建的身份验证密钥文件。
4. 点击**保存**。
5. 点击**应用更改配置**。
6. 确认验证密钥是否正常注册。

参考

用于 SSH 连接的认证密钥生成为公钥（Public Key）和私钥（Private Key）。私钥必须位于 SSH 客户端（要连接到 MDS 设备的管理员的 PC），而公钥必须位于 SSH 服务器端，当 SSH 客户端尝试连接时，比较 SSH 客户端的私钥和 SSH 服务器的公钥，如果一致，则正常认证并可以访问服务器。管理员必须使用身份验证密钥生成器创建身份验证密钥。有关生成认证密钥的更多信息，请联系 AhnLab 技术支持中心。

登录提示设置

为了登录安全性，输入将在登录屏幕上向用户显示的安全建议消息。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 帐户策略**。
3. 在登录提示，输入登录提示内容，最多可以输入 2048 字符。
4. 点击**保存**。
5. 点击**应用更改配置**。

管理员确认

对于诊断为恶意的事件，标识确认与否。如果禁用此功能，则不会在检测趋势和统计信息界面中显示该信息。

设置管理员确认功能的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**管理员 > 管理员确认**。
3. 选择复选框，启用**管理员确认功能**。
4. 点击**保存**。
5. 点击**应用更改配置**。

11.5 更新

本章介绍引擎更新设置和立即更新的方法，还有固件和虚拟机的更新方法，使维持最新的版本，以便及时响应安全威胁和紧急情况。设置更新周期进行更新或者由管理员直接点击**立即更新**即可。在进行更新之前，先检查一下 设备是否已连接到互联网。

引擎更新

自动更新设置

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 配置引擎的更新设置。选择**自动更新**复选框，然后输入**更新间隔**。
4. 点击**保存**。

参考

各引擎在 MDS 设备执行的功能如下：
- C&C 服务器特征码：检测和阻止可疑的 C&C 流量。
- C&C 服务器数据库：检测 C&C 服务器的访问。
- 文件 DNA：通过使用本地引擎或向云引擎发送查询来分析文件的数字 DNA 信息，检测和防止未知的恶意软件。
- 恶意 URL 数据库：检测和阻止恶意网站。
- 非执行型文件分析引擎：用于分析非执行型文件（Non-PE），如 RTF, OLE(DOC, XLS, PPT), OOXML(DOCX, XLSX, PPTX), PDF 等。
- 动态平台引擎：显示动态分析引擎相关的更新信息。
- MDP 引擎：执行多维度的分析，从已知和未知的恶意软件中保护系统。执行基于行为的检测和基于特征码的检测，还通过基于信誉的分析和主动防御来提供恶意软件检测率和准确性。
- DICA 引擎：执行动态智能内容分析，可以准确检测利用 MS Office、PDF 及 Hangul 等程序存在的漏洞入侵的非执行型（non-PE）恶意软件。它还可以检测和防止零日漏洞攻击。
- 内存扫描引擎：执行内存扫描。

立即更新

点击**立即更新**（  ），不管更新间隔立即执行更新。

手动更新

点击静态分析引擎或动态分析引擎的**浏览**，弹出手动更新对话框，点击**浏览...**选择更新文件或将文件拖放到此窗口，然后点击**确定**。

> **参考**
> 手动更新主要在封闭网络环境中使用，如果不是封闭的网络，建议使用自动更新。

在封闭的网络环境中引擎更新设置

如果在封闭的网络环境中使用 MDS，则很难做到在典型的网络环境中那样自动更新静态和动态分析引擎。虽然可以通过跨网解决方案对特定 IP 和端口进行更新，但实际上不可能将所有正在使用的 IP 地址跨网连接。为解决这个问题，MDS 提供了手动更新的方法。然而，手动更新麻烦，而且无法即时将引擎更新为最新版本，因此不足以应对最新的安全威胁。因此，MDS 提供 MDS Manager 来充当更新服务器，通过 MDS Manager 自动更新引擎。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 选择**使用 MDS Manager 作为更新服务器**复选框，然后输入 **MDS Manager IP 地址**和**端口号**。
4. 点击**保存**。

固件升级

您可以升级固件。如要升级固件，请联系 AhnLab 或供应商。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 点击固件区的**浏览...**，弹出<固件更新>窗口。
4. 点击固件文件的**浏览...**，选择 AhnLab 提供的固件文件。固件文件的扩展名为“enc”。选择固件文件后，点击哈希文件的**浏览...**，选择该固件文件的哈希文件。
5. 点击**确定**。
6. 完成更新后，需要重启设备。如果出现确认设备重新启动的对话框，请单击**是**。

虚拟机(VM)更新

更新虚拟机以进行恶意软件动态分析。在上传到 MDS 设备的虚拟环境中运行并分析扫描对象。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**更新 > 更新**，打开<更新>界面。
3. 可以确认虚拟机的当前版本、最新更新时间。MDS 支持 Windows XP（32 位）、Windows 7（32/64 位）和 Windows 10（64 位）镜像。

4. 如要更新虚拟机，点击虚拟机区的**浏览...**，弹出<虚拟机(VM)更新>窗口。
5. 点击虚拟机镜像文件的**浏览...**，选择虚拟机镜像文件。
6. 点击哈希文件的**浏览...**，选择哈希文件。
7. 点击**确定**。

参考

如果虚拟机更新失败，则原因可能如下：
-没有图像文件或哈希文件
-哈希值不匹配
-文件解压缩失败
-文件解密失败
-图像转换失败

参考

本产品支持用户自定义的 Windows 系列 32 和 64 位虚拟机环境，创建的虚拟机镜像文件和哈希文件可以通过 Web 管理界面上传到 MDS 服务器。有关创建自定义虚拟机的方法，请参考虚拟机 VirtualBox·安装 win 10 完整步骤。

11.6 警报

警报邮件设置

设置邮件服务器，当设备异常使用系统资源或检测到威胁时，立即发送警报提醒。

设置邮件服务器

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**警报 > 警报邮件**。
3. 设置各项目。
   - 邮件服务器 IP：输入邮件服务器的 IP 地址。
   - 端口号：输入邮件服务器的端口号。
   - 服务器登录帐户：登录邮件服务器时需要输入的帐户 ID。服务器登录帐户 ID 长度不能超过 50 个字符。
   - 服务器登录密码：登录邮件服务器时的帐户 ID 的密码。可以输入英文字母、数字和特殊字符，且长度不能超过 40 个字符。
   - 发件人邮件地址：输入发件人的电子邮件地址。
   - 威胁检测发送间隔：输入定期发送警报邮件的间隔时间，可以输入 1 到 1440 之间。

- 启用警报邮件：选择复选框，启用警报邮件功能。当发生警报事件时，发送各警报邮件到下面收件人。
  - 系统资源警报：输入当系统资源警报时的收件人电子邮件地址。
  - 威胁检测警报：输入当威胁检测警报时的收件人电子邮件地址。

参考

如果要检查邮件服务器正常连接，并且警报邮件正常发送，请点击**连接测试**进行测试。

4. 点击**保存**。
5. 点击**应用更改配置**。

警报条件设置

设置发送警报邮件的事件和事件级别。在设置警报条件之前，需要先配置警报邮件。有关警报邮件的内容，请参考警报邮件设置。

警报条件和基准按如下方法设置。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**警报 > 警报条件设置**。
3. 发送警报的事件主要分为检测到系统资源异常使用和检测到威胁的情况。设置每个事件的警报条件和基准。
   - 系统资源：当检测到系统资源的使用量超过阈值持续指定的时间以上的时候，发送警报邮件。
     - 当 CPU 使用量超过指定的阈值：选择复选框，输入阈值和持续时间。阈值的有效值为 1~100，持续时间的有效值为 1~60。
     - 当内存使用量超过指定的阈值：选择复选框，输入阈值和持续时间。阈值的有效值为 1~100，持续时间的有效值为 1~60。
     - 当磁盘使用量超过指定的阈值：选择复选框，输入阈值和持续时间。阈值的有效值为 1~100，持续时间的有效值为 1~60。
   - 威胁检测：当检测到威胁时，发送警报邮件。
     - 当检测到已知威胁：选择复选框，然后选择严重级别，最后选择是否将威胁的分析报告附加到电子邮件。
     - 当检测到未知威胁：选择复选框，然后选择严重级别，最后选择是否将威胁的分析报告附加到电子邮件。
4. 点击**保存**。
5. 点击**应用更改配置**。

11.7 联动

MDS Manager

MDS Manager 是管理多台 MDS 设备的中央管理设备。设置与 MDS Manager 设备联动，可以使 MDS 设备继承 MDS Manager 设置的策略。

MDS 设备与 MDS Manager 设备联动后，可以继承如下的策略。

- 管理 >策略>黑名单>文件(MD5)
- 管理 >策略>白名单>文件(MD5)
- 管理 >策略>黑名单>C&C 服务器
- 管理 >策略>白名单>C&C 服务器

上述的策略可在 MDS Manager 的 Web 界面进行更改。您不能在 MDS Web 界面上单独设置或更改 MDS Manager 中设置的策略。如要与 MDS Manager 联动，必须先在 MDS Manager 设备上注册 MDS 设备。

联动 MDS Manager

联动 MDS Manager 设备并继承策略的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > MDS Manager**。
3. 设置各项目。
   - 联动 MDS Manager 策略：选择复选框，将继承 MDS Manager 设置的策略。
   - 传输密码：输入 MDS Manager 设备传送策略到 MDS 设备时使用的密码。

参考

用于从 MDS Manager 服务器接收策略的传输密码也用于 MDS 传输收集文件。MDS 将检测到的恶意代码或可疑文件使用 SCP（Secure Copy Protocol，文件传输协议）协议传输到与 MDS 连接的其他设备。此时，SCP 协议使用 MDS Manager 传输策略时使用的传输密码来进行文件传输。

   - 传输日志：选择 MDS 设备传输日志到 MDS Manager 设备的类型。
   - 联动对象：设置欲联动的 MDS Manager 设备的各项信息。输入 IP、端口号，并选择安全传输与否，然后点击添加图标。
     - MDS Manager IP：输入 MDS Manager 设备的 IP 地址。
     - 端口号：输入 MDS Manager 设备的端口号。
     - 安全传输：选择复选框， 启用安全传输。

- MDS Analysis Manager：选择复选框，与 MDS Analysis Manager 联动。如果选择此选项，则无法选择安全传输。

4. 点击**保存**。
5. 点击**应用更改配置**。

参考

如果解除联动，请点击 MDS Manager IP 左侧的❌，将欲解除联动的 MDS Manager IP 地址从列表中删除即可。

联动 ArcSight CEF

MDS 支持 ArcSight 联动。通过 CEF(Common Event Format)认证方式将 MDS 生成的日志存储到 ArcSight 日志服务器上。

联动 ArcSight 的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > CEF**。
3. 设置各项目。
   - 联动 CEF：选择复选框，联动 CEF。
   - 日志服务器：添加日志服务器。输入 IP 地址和端口号，然后单击⊕。
     - IP 地址：输入日志服务器的 IP 地址。
     - 端口号：输入日志服务器的端口号。
   - 传输日志：选择传输日志的类型。
   - 编辑日志：编辑欲传输的系统日志和检测日志中使用的 CEF 认证内容。如要恢复为默认值，请单击↻。
4. 点击**保存**。
5. 点击**应用更改配置**。

参考

CEF 格式如下：
CEF:Version | Device Vendor | Device Product | Device Version | Signature ID | Name | Serverity | Extension

联动 LEEF

MDS 支持 QRadar 联动。通过 LEEF(Log Event Extended Format)认证方式将 MDS 生成的日志存储到 QRadar 日志服务器上。

联动 QRadar 的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > LEEF**。
3. 设置各项目。
   - 联动 LEEF：选择复选框，联动 LEEF。
   - 日志服务器：添加日志服务器。输入 IP 地址和端口号，然后单击  。
     - IP 地址：输入日志服务器的 IP 地址。
     - 端口号：输入日志服务器的端口号。
   - 传输对象：选择传输日志的类型。
   - 编辑日志：编辑欲传输的系统日志和检测日志中使用的 CEF 认证内容。有效值为 1 到 2048 个字符之间。如要恢复为默认值，请单击  。
4. 点击**保存**。
5. 点击**应用更改配置**。

参考

LEEF 格式如下：
LEEF: Version | Vendor | Product | Version | EventID |

外部日志服务器

配置外部日志服务器，将 MDS 生成的日志保存到外部日志服务器。

配置外部日志服务器的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > 外部日志服务器**。
3. 选择传输日志的类型。
4. 添加日志服务器。输入 IP 地址和端口号，然后单击  。
   - IP 地址：输入日志服务器的 IP 地址。
   - 端口号：输入日志服务器的端口号。
   - 安全传输：选择复选框， 启用安全传输。
5. 点击**保存**。

6. 点击**应用更改配置**。

参考

端口号是 UDP 端口号。一般传输时，端口号为 514；安全传输时，端口号为 516。

人事信息

通过联动人事信息，可以更加准确知道 MDS 检测到的对象是谁。人事信息与 Active Directory 服务器联动使用，并利用 Active Directory 服务器收集的帐户信息。如果没有 Active Directory 服务器，则可以使用手动上传的人事信息文件。如果公司已有构建的人事信息数据库，则可以与数据库服务器联动使用。

通过联动 Active Directory 服务器更新人事信息

通过联动 Active Directory 服务器更新人事信息。如果使用 Active Directory 服务器，可以利用 Active Directory 服务器收集的帐户信息来查出谁是设备检测到的攻击的目标。

通过联动 Active Directory 服务器更新人事信息按如下操作。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > 人事信息**。
3. 启用**联动人事信息**复选框。
4. **联动方法**选择 **Active Directory 服务器**。
5. 设置**联动信息**。
   - Active Directory 服务器 IP：输入要使用的 Active Directory 服务器的 IP 地址。
   - Base DN：输入 Active Directory 服务器的 Base DN。
   - Bind DN：输入可以连接到 Active Directory 服务器的 ID。

参考

访问 Active Directory 服务器所需的 ID 必须能够远程查询 Active Directory 服务器的审核日志，并有权通过 LDAP 搜索收集 Active Directory 帐户信息。

   - 密码：输入 Bind DN 的密码。
   - 确认密码：再一次输入密码。
6. 点击【**连接测试**】，检查是否正常连接到上面输入的 Active Directory 服务器。
7. 如果连接测试成功，继续设置**联动项目**，即连接 Active Directory 收集的项目。
   - AD 帐户：输入 AD 帐户的字段名，以在 Active Directory 服务器收集。默认值为 sAMAccountName。
   - 名称： 输入名称的字段名，以在 Active Directory 服务器收集。默认值为 name。

- 部门：输入部门的字段名，以在 Active Directory 服务器收集。默认值为 department。
- 邮件地址： 输入邮件地址的字段名，以在 Active Directory 服务器收集。默认值为 mail。
- 联系电话：:输入联系电话的字段名，以在 Active Directory 服务器收集。默认值为 telephoneNumber。

8. 指定**联动时间**。从下拉框中选择与 Active Directory 服务器定期联动的时间。默认值是**每日上午 1 点**。
9. 输入**帐户信息收集间隔时间**。有效值为 10~180 分钟。
10. 点击**保存**。
11. 点击**应用更改配置**。

通过上传人事信息文件更新人事信息

如果没有 Active Directory 服务器，可以通过上传人事信息文件更新人事信息。

通过上传人事信息文件更新人事信息按如下操作。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > 人事信息**。
3. 启用**联动人事信息**复选框。
4. **联动方法**选择上传人事信息文件，然后点击**浏览...**选择人事信息文件或将文件拖放到此框。
5. 点击**上传**。
6. 点击**保存**。
7. 点击**应用更改配置**。

参考

当通过上传文件更新人事信息时，来自 Active Directory 服务器的人事不会更新。

通过联动数据库服务器更新人事信息

如果没有 Active Directory 服务器，可以通过联动数据库服务器更新人事信息。

通过联动数据库服务器更新人事信息按如下操作。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > 人事信息**。
3. 启用**联动人事信息**复选框。
4. **联动方法**选择**数据库服务器**，然后设置各项值。
5. 设置**联动信息**。
   - 数据库类型：选择要连接的数据库类型。目前仅支持 Mysql。
   - 服务器 IP 地址：输入要连接的数据库服务器的 IP 地址。
   - 端口号：输入要连接的数据库服务器的端口号。

- 数据库名称：输入要连接的数据库名称。
- ID：输入访问数据库服务器时所需的 ID。
- 密码：输入数据库服务器 ID 的密码。
- 确认密码：再一次输入密码。

6. 点击**【连接测试】**，检查是否正常连接到上面输入的数据库服务器。
7. 如果连接测试成功，继续设置联动信息。
   - 表名称：输入要联动的数据库表名称。
   - 帐户：输入数据库表中相当于帐户信息的列的名称。
   - IP 地址：输入数据库表中相当于 IP 地址信息的列的名称。
   - 邮件地址：输入数据库表中相当于邮件地址信息的列的名称。
   - 部门：输入数据库表中相当于部门信息的列的名称。
   - 联系电话：输入数据库表中相当于联系电话信息的列的名称。
8. 指定**联动时间**。从下拉框中选择与数据库服务器定期联动的时间。默认值是**每日上午 1 点。**
9. 点击**保存。**
10. 出现“您要启用人事信息联动吗？要应用更改，您必须重新登录。”的提示。如果要使用更改后的设置加载的人事信息并立即应用，请选择**立即应用**。如果要按设置的联动时间重新加载人事信息，请取消选择**立即应用**。

参考

如果人事信息中有重复的 IP 地址，则该人事信息从联动中除外。

11. 点击**确定。**
12. 点击**应用更改配置。**

参考

如果使用与数据库服务器联动，则无法使用 Active Directory 服务器联动功能。

第三方

MDS 支持与 3rd-Patry(RSA SA(NetWitness))联动。管理员基于 MDS 提供的信息，可以利用 NetWitness 提供的仪表板、流量分析等信息。

配置第三方联动的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**联动 > 第三方。**
3. 启用**联动 RSA SA（NetWitness）**复选框，输入下面的各项值。
   - IP 地址：输入要使用的 NetWitness 的 IP 地址。

- 端口：输入 NetWitness 的端口号。
- ID：输入连接 NetWitness 时使用的 ID。

4. 点击**保存**。
5. 点击**应用更改配置**。

11.8 Agent

Agent 列表

可以查看基于组密钥和 IP 地址分组的 Agent 的信息，并保护和管理 Agent，使其免受安全威胁。

组管理

MDS 可以通过分组来管理 Agent。创建组时，可以指定该组所覆盖的 IP 地址范围，属于该 IP 地址范围的 Agent 将自动注册到该组。但有些组，创建时可以不使用 IP 地址条件的分组方式。根据不同的上级组，可以添加不同类型的子组。

点击  ，显示组列表，图标 ▷ 表示该组下面存在子组，点击即可展开，点击 ◢ 重新折叠。如下图所示。

MDS 采用不同的颜色的图标直观地表示组。各图标表示的内容如下：

-  ：该图标表示具有组密钥的组，也是组结构中位于最上级的一个组。它只能在<组密钥>界面创建，包括更改和删除。
-  ：该图标表示根据 IP 地址条件自动注册 Agent 的组。根据管理服务器访问 IP 地址和本地 IP 地址范围，自动将满足 IP 地址条件的 Agent 分类到该组。
- ：该图表示不是根据 IP 地址条件分类的组。由于特殊的管理问题，一些 Agent 需要另外分组，而不是根据 IP 地址。
-  ：该图标表示的是一个叫“特设响应组”的虚拟组，系统默认创建在最上级组的下面。该组仅用于传送响应命令而不应用策略的组。因为这是一个虚拟组，所以 Agent 的实际所属组是另外存在的。
-  ：该图标表示根据所属组条件自动注册 Agent 的组。在<自动分组设置>窗口中，选择“所属组”作为分组方式后通过上传用户信息文件自动注册到该组。

参考

把鼠标放到组上方，出现设置图标（  ），点击该图标，出现该组可以操作的功能菜单。

自动分组设置

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 列表**。
3. 点击  ，显示组列表。
4. 鼠标放到欲设置自动分组的上级组（仅限于）名称，出现设置图标  。
5. 单击  ，在出现的菜单中选择**自动分组设置**，弹出<自动分组设置>界面。
6. 选择分组方式。
   - 自定义 IP 地址：删除所有先前创建的组后，通过新建组时使用“指定 IP 地址条件”重新分组。
   - B 类 IP 地址：根据 Agent IP 地址的 B 类标准自动生成组，并根据 Agent 的 IP 地址自动将 Agent 注册到所属组。假设 Agent 的 IP 地址为 192.168.1.1 的话，将自动生成组 192.168.0.0，并把该 Agent 自动注册到该组。
   - C 类 IP 地址：根据 Agent IP 地址的 C 类标准自动生成组，并根据 Agent 的 IP 地址自动将 Agent 注册到所属组。假设 Agent 的 IP 地址为 192.168.1.1 的话，将自动生成组 192.168.1.0，并把该 Agent 自动注册到该组。
   - B、C 类 IP 地址：根据 Agent IP 地址的 B、C 类标准自动生成两个级别的组，并根据 Agent 的 IP 地址自动将 Agent 注册到所属组。假设 Agent 的 IP 地址为 192.168.1.1 的话，将自动生成组 192.168.0.0 和 192.168.1.0，并把该 Agent 自动注册到组 192.168.1.0。
   - 所属组：根据联动人事信息的所属部门，并根据 Agent 的所属部门自动对 Agent 进行分组。点击**浏览...**选择用户信息文件，或者将人事信息文件拖放到此，然后点击**上传**。

参考

要上传部门的层次结构信息，请单击**下载用户信息模板**以下载到本地系统，打开文件后输入部门信息并上传。示例）咨询总部>咨询团队 1

7. 点击**确定**。

注意

使用自动分组时，将删除基于相同条件创建的现有组，并根据新的条件重新创建组。

新建组

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 列表**。
3. 点击  ，显示组列表。
4. 鼠标放到欲新建组的上级组名称，出现设置图标  。
5. 单击  ，在出现的菜单中选择**新建组**，弹出<新建组>界面。
6. 输入所需的信息。

【当子组创建在下面时】

- 组路径：显示欲新建的组所在的上级组名称。该项目无法更改。
- 组名称：输入新建组的名称。
- 指定 IP 地址条件：如果要创建基于 IP 地址（Agent 管理服务器访问 IP 地址）的组，则选择该项；如果要创建用户定义的组，则不选择。
- IP 地址：如果启用**指定 IP 地址条件**选择，则下面出现输入 IP 地址的栏。输入该组所覆盖的 Agent 的 IP 地址。可以输入单一 IP 地址、IP 地址范围和 IP 地址/网络掩码形式，且最大可以输入 100 个。

【当子组创建在下面时】

- 组路径：显示欲新建的组所在的上级组名称。该项目无法更改。
- 组名称：输入新建组的名称。
- 分组条件：选择是否根据**管理服务器访问 IP 地址**或者是**本地 IP 地址**。
- IP 地址：选择上面的分组条件后，输入该组所覆盖的 Agent 的 IP 地址。可以输入单一 IP 地址、IP 地址范围和 IP 地址/网络掩码形式，且最大可以输入 100 个。

【当子组创建在下面时】

- 组路径：显示欲新建的组所在的上级组名称。该项目无法更改。
- 组名称：输入新建组的名称。

【当子组创建在下面时】

- 组路径：显示欲新建的组所在的上级组名称。该项目无法更改。
- 组名称：输入新建组的名称。

7. 点击**确定**。

参考

如果创建的组采用了根据 IP 地址分组的方式，它的下级组的 IP 范围必须包含在它的 IP 范围。相同级别的组的 IP 范围不能重叠。

更改组

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 列表**。
3. 点击  ，显示组列表。
4. 鼠标放到欲更改的组的名称，出现设置图标  。
5. 单击  ，在出现的菜单中选择**更改组**，弹出<更改组>界面。
6. 更改各项值。
7. 点击**确定**。

删除组

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 列表**。
3. 点击  ，显示组列表。
4. 鼠标放到欲删除的组的名称，出现设置图标  。
5. 单击  ，在出现的菜单中选择**删除组**，弹出提示。
6. 点击**确定**。

参考

具有组密钥的最上级组只能在“组密钥”界面中删除。如果删除组密钥，该组下面的子组也被删除。

查看 Agent 信息

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 列表**。
3. 显示所有的 Agent 组列表。点击要查看的组名称，则显示该组所属的所有 Agent 列表。
   可以确认如下 Agent 信息。
   - 已连接：显示已连接到服务器的 Agent 总数。
   - 未连接：显示未连接服务器的 Agent 总数。

- 未知：显示连接服务器状态为不详的 Agent 总数。
- 已隔离（Agent）：显示通过 Agent 隔离的系统总数。
- 已隔离（安全开关）：显示通过安全开关隔离的系统总数。
- 连接状态：显示 Agent 与服务器的连接状态。状态分为**已连接**（🟢）、**未连接**（⚫）和**未知**（❓）。
- Agent 名：显示 Agent 系统名称。
- 主机 IP：显示主机的 IP 地址。当本地 IP 地址不存在时，使用该 IP 地址。
- 本地 IP：显示安装 Agent 的计算机的 IP 地址。
- 组名称：显示 Agent 所属组的名称。
- 策略名：显示 Agent 应用的策略名。
- MAC 地址：显示 Agent 系统的 MAC 地址。
- IE 版本：显示 Agent 系统安装的 IE 版本。
- 操作系统：显示 Agent 系统的操作系统（OS）信息。
- Agent 版本：显示 Agent 系统安装的 Agent 程序的版本。
- Agent 安装日期：显示 Agent 系统安装 Agent 程序的日期。
- 最近访问日期：显示 Agent 最近访问服务器的时间。

参考

如要删除 Agent，在列表中选择 Agent(可以多选)，然后点击**管理**键后选择**删除**，或者点击 Agent 名左侧的❌。

参考

如要将 Agent 列表导出，点击**导出**键，Agent 列表将以 CSV 文件保存到本地计算机。

参考

点击**显示 Agent**，显示所有 Agent 列表；点击**显示组**，则显示组列表。

Agent 命令

对于检测到或怀疑安全威胁的 Agent，管理员可以直接通过组或 Agent 发送命令，或通过应用预定义的策略进行响应。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 列表**。
3. 选择响应安全威胁的组或 Agent（可以多选）。
4. 点击**响应**键，出现如下响应方法：
   - 隔离系统：通过隔离系统命令来阻止受感染 Agent 系统使用网络。

- 解除隔离系统：发送解除隔离系统命令，允许 Agent 系统使用网络。

参考

解除隔离命令可以设置为自动响应，而不需要每次发送命令。请在管理 >检测和策略 > 响应设置中设置自动响应方法。

- 收集可疑文件：发送收集可疑文件命令，扫描并收集 Agent 系统上的可疑的文件，并将检测到的文件发送到 MDS，以诊断恶意代码与否。

参考

当您发出收集可疑文件命令时，Agent 会在开始收集可疑文件之前向 Agent 计算机用户显示数据收集协议。用户同意该协议之后才可以执行可疑文件收集。对于收集的可疑文件，可以在“**响应情况 > 可疑文件收集**”中确认，并且必须通过“恶意代码分析请求”来检查收集的可疑文件的恶意与否。有关详细的信息，请参阅收集可疑文件和恶意代码分析请求。

- 发送通知：通知特定 Agent 它们受感染情况或通知最近流行的恶意代码。
- 应用策略：发出应用策略命令以应用预先定义的策略。
- 初始化 Agent 缓存：发出初始化 Agent 缓存命令以减少服务器负载。

参考

要在每次启动 Agent 服务或您设置的删除间隔时间初始化 Agent 缓存，请在管理 > Agent > 策略设置中的**新建 Agent 策略**界面的**文件运行保留**选项卡中，启用 **Agent 启动时删除缓存**选项并指定**缓存删除间隔**时间。

- 补丁集更新：通过此命令可以更新 Agent 修补程序和签名文件的最新版本。要发出此命令，必须先将最新版本的补丁集（修补程序文件和签名文件）上传到服务器。
  有关上传补丁集的方法，请参阅补丁集。
- 删除特定文件：通过此命令可以删除一些符合设置条件的文件。在<删除特定文件>窗口中，选择删除对象**组**和删除**范围**，并输入要删除文件的**哈希值**和**文件大小限制**，然后点击**删除**键。如果所选组的 Agent 中有符合设置条件的内容，则将其删除。

默认设置

配置管理 Agent 相关的基本设置，安全有效管理网络上的主机，并从各种安全威胁中保护主机。

Agent 默认设置按如下操作：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 默认设置**。
3. 配置管理 Agent 的 MDS 服务器。
   - Agent 管理服务器 IP：输入管理 Agent 的 MDS 服务器的 IP 地址。

参考

根据操作环境，MDS 可以与单独的 MDS Manager 联动。此时，Agent 由 MDS Manager 管理，因此需要输入 MDS Manager 的 IP 地址作为 Agent 管理服务器 IP 地址。

4. 设置安装 Agent 程序相关的选项，以管理未安装 Agent 程序的主机。
   - 重定向：选择复选框启用“网页重定向”功能。当未安装 Agent 的主机请求访问互联网时，将重定向其转向 MDS Agent 安装向导网页。

参考

如果重定向 Agent 安装网页不启动，请点击**删除安装信息缓存**以删除 Agent 计算机的缓存。当缓存被已删除，将重新收集 Agent 安装信息，并执行重定向安装 Agent 网页。

   - 安装网页：输入 MDS Agent 安装网页的网址。
   - 以静默模式安装 Agent：选择复选框，启用静默模式安装 Agent。
   - 输入 PIN 代码时允许删除 Agent：点击**[生成 PIN 码]**，弹出<生成 PIN 码>对话框。输入 Agent 验证码后点击**生成**键。

参考

当应用“输入 PIN 码时允许删除”策略的 Agent 请求删除时，生成 PIN 码并转达。

5. 设置 Agent 执行 MDS 发送的命令相关的选项。
   - 命令有效时间：选择 MDS 发送命令到 Agent 的有效时间。
   - 使用性能控制：选择复选框，则当 Agent 执行 MDS 发出的命令时，控制使用最低的 CPU。

参考

如果 Agent 没有在命令有效期内通知 MDS 执行命令的结果，MDS 将处理为命令执行失败。

6. 设置**通过 Agent 删除文件**相关的选项。当 MDS 检出 Agent 的恶意代码时，可以发出删除命令。Agent 则根据下面的设置，删除文件。
   - 区域：选择 Agent 执行删除命令时可以删除的区域。
   - 删除时提醒：选择复选框，则在执行删除命令时，通过弹窗提醒用户。

参考

从 MDS Agent 2.2.7 及更高版本开始，遵循[Agent 策略 > 提示设置]中的“删除文件时提示”选项的设置。

7. 设置收集 Agent 可疑文件的手动收集范围和自动收集方法。
   - 手动收集范围：从下拉框中选择收集可疑文件的范围。
   - 自动收集：选择复选框，然后设置自动收集方法。自动收集方法可以选择“计划收集”或“实时收集”。

- 计划收集：在指定的时间收集可疑文件。选择收集范围和收集对象并指定收集时间，然后点击  。
- 实时收集：通过 Agent 实时收集可疑文件。

8. 点击**保存**。
9. 点击**应用更改配置**。

策略设置

配置应用于 Agent 的策略。

Agent 策略列表

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 显示 Agent 策略列表，可以查看如下信息。
   - 策略名：显示 Agent 策略名称。
   - 策略应用组：显示策略应用的 Agent 组名称。
   - 描述：显示该策略的描述。
   - 应用状态：显示 Agent 应用策略的状态。
   - 策略创建时间：显示策略创建的时间。
   - 最近更改时间：显示策略最近更改的时间。

新建 Agent 策略

创建 Agent 策略按如下步骤进行。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 点击**添加**键，弹出<新建 Agent 策略>窗口。
4. 设置**策略名**标签下面的各项目。
   - 策略名：输入新建的策略名称。
   - 应用组：选择要应用新建策略的 Agent 组。
   - 描述：输入有关新建策略的描述。
5. 点击**下一步**或**默认设置**标签。
6. 设置**默认设置**标签下面的个项目。
   - 删除 Agent：设置是否允许删除主机上安装的 Agent 程序。

    - 允许删除：选择此选项，则允许删除 Agent。
    - 输入 PIN 代码时允许删除：选择此选项并输入 6 位 PIN 代码，则当删除 Agent 时要求输入 PIN 代码。
    - 不允许删除：选择此选项，则不允许删除 Agent。
- 在任务栏中显示 MDS Agent：选择复选框，则在 Agent 的任务栏中显示 MDS Agent 图标。
- 联动 Agent：选择此选项可在您同时安装了 APC Agent、V3 和 MDS Agent 时，可以使用统一 Agent 而不是使用每个 Agent。当选择使用 APC Agent 托盘图标时，可以通过 APC Agent 转发 MDS Agent 的通知，并从任务栏中隐藏 MDS Agent 的托盘图标。
- 在 Agent 弹窗中显示消息：如要在 Agent 上发生的所有的弹出窗口中显示管理员引导用户的文本，请选择该选项并输入文本内容。文本内容最大不能超过 75 字节。示例：[咨询]联系人：OOO（安全小组） 电话：OOO）
- 自我保护：选择此选项，可防止用户或其他进程强制关闭或重新启动 Agent 进程，并防止篡改注册表信息。
    - 阻止产品由 rootkit 等其他程序强制结束：选择此选项，可以防止被 rootkit（被视为一种外部程序）强制终止 Agent。
- 更新 Agent：选择此选项，从 MDS 检查 Agent 的最新版本，并在分发新版本时是否自动更新 Agent。
    - 更新间隔：输入 Agent 更新间隔时间。Agent 根据指定的间隔时间从 MDS 检查 Agent 程序的最新版本，如果已发布新版本，则进行更新。
- 扫描进程内存：选择此选项，则使用扫描进程内存策略。
    - 自动修复：扫描后，自动修复内存。
    - 传输日志到服务器：扫描后，将结果日志传输到服务器。
- 策略更新间隔：输入 Agent 策略更新间隔时间。Agent 根据指定的间隔时间从 MDS 检查 Agent 策略并应用。
- 隔离区大小：输入隔离区空间的最大大小。隔离区是隔离并存储由 Agent 删除的恶意代码的空间。（默认值：100MB）
- 备用服务器 IP 地址： 输入服务器连接失败时的备用 IP 地址。
- 组密钥：从下拉框中选择策略应用组密钥。
- 联动 MDS：选择复选框，并输入下面各项目。
    - 设备 IP 地址：输入要联动的 MDS 设备的 IP 地址。
    - 备份设备 IP 地址：输入备份设备的 IP 地址。

参考

Agent 策略设置中的 MDS 联动具有比 Agent 管理服务器中的 MDS 联动设置更高的优先级。

7. 点击**下一步**或**运行保留**标签。

8. 设置**文件运行保留**标签下面的各项目。
   - 启用文件运行保留（Execution Holding）：选择此选项可将策略设置为暂时不运行未判断恶意与否的可执行文件。
   - 基本扫描（可执行文件）：设置对可执行文件的扫描的各种选项。保留可执行文件的运行，并检查恶意与否。
     - 扫描对象：输入要扫描的可执行文件的创建时间。（默认值：60 分钟）
     - 等待时间：输入在分析可执行文件的时等待响应的时间。（默认值：5 秒）
       - 超过等待时间时：选择当超过等待时间时的处理方法，可以选择**阻止运行**、**允许运行**和**用户选择**。
     - 连接 MDS 服务器出现问题时：选择当连接 MDS 服务器出现问题而无法分析文件时的处理方法，可以选择**禁用**、**阻止运行**、**允许运行**和**用户选择**。
     - 保存 Agent 缓存：选择此选项，可将运行保留的文件分析结果以 Agent 缓存保存以供用在后续分析。使用 Agent 缓存分析可以减少分析时间。
       - Agent 启动时删除缓存：选择此选项，则删除每次 Agent 服务启动时保存的缓存，以减少服务器负载。此设置可以独立于“保存 Agent 缓存”和“缓存删除间隔”设置。
       - 缓存删除间隔：输入 1 到 24 小时之间的整数。例如，输入 3 的话，每隔 3 小时删除保存的 Agent 缓存。
     - 传输到 MDS 服务器的文件的最大大小：设置 Agent 发送文件到服务器的最大文件大小。最大可以设置 300MB，默认值为 3MB。
9. 点击**下一步**或点击**文件运行保留高级设置**标签。
   - 禁用：选项此选项，则不使用文件运行保留高级设置。
   - 高级扫描（包括 Dropper 文件 - 不可执行文件）：设置对不可执行文件的运行保留的各种选项。
     - 包括由 Rundl 执行的 DLL：选择此选项，保留由 Rundll 执行的 DLL 文件的运行。
     - 其他扫描对象：设置不可执行文件的扫描对象。各项目最多可以输入 512 字节。
       - 不可执行文件扩展名： 输入执行扫描的不可执行文件扩展名。（默认值：pdf/doc/ppt/xls/docx/pptx/xlsx/rtf/hwp/gul）
       - 不可执行文件的执行进程名： 输入执行扫描的不可执行文件的执行进程名。（默认值：acrord32.exe, winword.exe, powerpnt.exe, excel.exe, hwp.exe, jungumgw.exe）
       - 不可执行文件的保存进程名：输入执行扫描的不可执行文件的保存进程名。（默认值：iexplore.exe, chrome.exe, firefox.exe, outlook.exe, v3zip.exe, alzip.exe, 7zg.exe, winrar.exe）
   - 运行后扫描（包括 Dropper 文件 - 不可执行文件）：运行文件后对其进行扫描，如果该文件是恶意的，则将结果通知给用户。
     - 其他扫描对象：设置运行后扫描的文件的扫描对象。如同上述。

10. 点击**下一步**或点击**文件运行保留例外**标签。
    - 非扫描区域（文件夹）：选择复选框，可以添加运行保留例外的非扫描区域的文件夹。输入**文件夹路径**和**描述**，然后点击  。最多可以添加 64 个。
    - 非扫描区域（文件）：选择复选框，可以添加运行保留例外的非扫描区域的文件。输入 16 进制 32 字节的文件**哈希值**（MD5 值）和**描述**，然后点击  。最多可以添加 128 个。
    - 非扫描区域（文件签名）：选择复选框，可以添加运行保留例外的非扫描区域的文件签名。输入**文件签名**和**描述**，然后点击  。文件签名长度最大不能超过 64 字节，且不允许输入特殊字符（`）。最多可以添加 64 个。
11. 点击下一步或点击**检测**标签，设置下面的项目。
    - 检测对象及响应方法
      - 文件异常运行：选择是否检测文件的异常运行以及检测到文件异常运行时如何响应。
      - 文件异常下载：选择是否检测文件的异常下载以及检测到文件异常下载时如何响应。
      - 后门程序：选择是否检测后门程序的运行以及检测到后门程序运行时如何响应。
      - 浏览器异常提升权限：选择是否检测浏览器的异常提升权限行为以及检测到浏览器异常提升权限时如何响应。
    - 拦截例外：对于下面设置的进程或 URL/IP 地址，及时检测到也不拦截。启用**拦截例外**复选框，选择**进程**或 **URL/IP 地址**，然后根据选择的类别输入**可执行文件名称**或 **URL/IP 地址**和**描述**，然后点击  。最多可以添加 128 个。
12. 点击**下一步**或点击**提示设置**标签，设置下面的各项目。
    - 全选：选择复选框，下面的选项将被全选。
    - 弹出最终用户许可协议（EULA）提示对话框：选择此选项，则弹出最终用户许可协议提示对话框。
    - 弹出可疑文件收集同意提示对话框：选择此选项，则 Agent 在收集可疑文件之前向 Agent 计算机用户询问是否同意数据收集。
    - 弹出文件运行保留提示对话框：当文件运行保留后等待时间超过指定的时间时，弹出提示对话框使用户选择响应方法。
      - 隐藏允许文件运行选项：当弹出文件运行保留提示对话框时，无论扫描结果如何，都会隐藏允许文件运行选项。
    - 显示气球帮助提示窗口：以气球帮助形式显示对诊断文件的信息。
    - 删除文件时提示：选择此选项，则删除文件时出现提示窗口，用户确认后将其删除。
    - 恢复文件时提示：选择此选项，则恢复文件时出现提示窗口，用户确认后将其恢复。
13. 点击**确定**。

参考

即使不选择**保存 Agent 缓存**选项，以前保存的缓存也将继续用于文件分析。如果对文件的分析结果发生变化，通过 CLI 命令执行删除缓存，使可以应用新的分析结果分析文件。

参考

当您运行可疑文件收集命令时，Agent 会在开始收集可疑文件之前向 Agent PC 用户显示收集数据同意提示对话框。用户同意后，才可以进行可疑文件收集。

更改 Agent 策略

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 鼠标双击列表中的欲更改项目，打开<更改 Agent 策略>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除 Agent 策略

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > Agent 策略**。
3. 在列表中选择欲删除项目 左侧的 ❌，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

安装 IP 地址

设置使用“引导安装 Agent 网页”重定向功能的网络，当未安装 Agent 的主机尝试连接互联网时，重定向其转向安装 Agent 网页。有关引导安装 Agent 的详细内容，请参考 Agent 默认设置。

添加安装 IP 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 安装 IP 地址**。
3. 点击**添加**键，弹出<添加安装 IP 地址>窗口。
4. 设置各项目。
   - IP 地址：输入安装 Agent 程序的 IP 地址和网络掩码。
   - 输入描述：输入有关安装 Agent IP 的描述。
5. 点击**确定**。

6. 点击**应用更改配置**。

删除安装 IP 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 安装 IP 地址**。
3. 在列表中选择欲删除项目 左侧的 ✕，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

安装例外 IP 地址

设置从安装 Agent 网络中除外的 IP 地址，当未安装 Agent 的主机尝试连接互联网时，也不重定向其转向安装 Agent 网页。

添加安装例外 IP 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 安装例外 IP 地址**。
3. 点击**添加**键，弹出<添加安装例外 IP 地址>窗口。
4. 设置各项目。
   - IP 地址：输入不重定向安装 Agent 程序网络的 IP 地址和网络掩码。
   - 输入描述：输入有关描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除安装例外 IP 地址

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 安装例外 IP 地址**。
3. 在列表中选择欲删除项目左侧的 ✕，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

参考

如果要一次添加多个安装例外 IP，先将要添加的 IP 地址创建 CSV 文件，然后单击**导入**键。

参考

如果要将已添加的安装例外 IP 列表以 CSV 文件保存到本地 PC，单击**导出**。

补丁集

将最新版本的 Agent 修补程序和签名文件上传到服务器，使 MDS 再分发给主机。

> **参考**
>
> 有关将上传的最新版本的修补程序文件和签名文件通过命令分发到 Agen 的说明，请参阅 Aennt 列表的响应命令。

上传 Agent 修补程序文件和签名文件的步骤如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 补丁集**。
3. 点击 Agent 修补程序文件的**浏览...**，选择修补程序文件。
4. 点击签名文件的**浏览...**，选择签名文件。
5. 点击**上传**。
6. 点击**应用更改配置**。

> **参考**
>
> 如要应用 Aent 补丁集，请同时上传 Agent 修补程序文件和签名文件。

> **参考**
>
> 如果 Agent 修补程序或签名文件有问题，或者上传时发生错误，则会在上传进度屏幕上显示弹出消息。

组密钥

创建组密钥，这是创建组的基准，可以有效地管理 Agent。MDS 根据 Agent 的访问管理服务器的 IP 地址和本地 IP 地址范围自动对 Agent 进行分类来创建组。但是，在多 NAT 环境中，可能会发生 Agent 访问管理服务器的 IP 地址重复的现象，这导致难以识别 Agent 并有效管理。这也显示了仅基于 IP 地址范围分类组的限制。

为了解决此问题，管理员使用组密钥根据其站点环境对 Agent 进行手动分类并创建组。按组密钥初次分组的 Agent 根据管理服务器访问 IP 地址和本地 IP 地址范围再次进行分组。在此界面创建的组也显示在 Agent 列表中，而且是最上级组。

创建组密钥

创建组密钥并设置 Agent 安装网页的步骤如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择 **Agent > 组密钥**。
3. 点击**添加**键，弹出<创建组密钥>窗口。
4. 设置各项目。

- 组密钥：系统自动创建组密钥。
- 组名称：输入要使用自动生成的组密钥进行管理的组名称。

5. 点击**确定**。

> **参考**
>
> 最多可以创建 50 个组密钥。default 是系统默认提供的组密钥，管理员无法更改或删除。

设置 Agent 安装网页

1. 在组密钥列表中，点击要设置 Agent 安全网页的**[更改]**。
2. 弹出<Agent 安装网页设置>窗口。
3. 设置各项目。
   - 徽标：点击**浏览...**以选择徽标图像或拖放要上传的徽标图像，然后点击**上传**。如要下载默认徽标图像作为参考，请点击**[下载默认徽标图片]**。
   - 标题：输入 Agent 安装网页的标题。默认显示“**下载 Agent 安装文件**”。标题最大不能超过 70 字节。
   - 内容：输入在 Agent 安装网页显示的内容。默认显示“**如果 PC 未安装 MDS Agent，请下载并运行 Agent 安装文件**”。内容最大不能超过 2,000 字节。
   - 联系信息：输入在 Agent 安装网页显示的联系信息，如联系人姓名和电话等信息。例如：OOO，010-1234-5678。联系信息不能超过 150 字节。
4. 点击**确定**。
5. 点击**[预览]**，可以查看最终显示在 Agent 安装网页的内容。

11.9 共享文件夹

共享文件夹

设置共享文件夹实时扫描和计划扫描。共享文件夹可能容易受到安全威胁的影像，这可能会导致严重的安全问题。因此需要定期扫描系统的共享文件夹，以最大降低安全威胁。扫描结果标记为“恶意”或“正常”。文件大小超过指定的阈值 100MB 时标记为“未分类”。扫描完成后，文件将根据扫描结果移动到指定的位置。

实时扫描设置

添加共享文件夹实时扫描设置步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**共享文件夹 > 实时扫描**。
3. 输入**共同设置**的各项目。

- 超时时间：输入共享文件夹实时扫描的超时时间。有效值为 60~86,400 秒。
- 扫描对象大小：设置扫描对象文件的最大值。有效值为 1~1,000MB。
- 如果扫描结果为恶意或未知，则创建信息文件：选择复选框，当共享文件夹实时扫描结果为“恶意”或“未分类”时，创建信息文件以查看检测详细信息。
- 移动已扫描文件：选择复选框，则将共享文件夹中的原始文件移动至 MDS 服务器，完成扫描后将其移回原始位置。如果未启用此功能，则在共享文件夹中创建与原始文件相同名称的临时文件，将其移至 MDS 服务器以完成扫描，然后删除共享文件夹中的原始文件。

4. 点击**添加**，弹出<添加共享文件夹扫描>窗口。输入所需的信息后，单击**确定**关闭窗口。
   - 文件系统：选择共享文件夹的文件系统。
   - 扫描对象设置：设置欲扫描的共享文件夹。输入所需的信息后，单击**【连接测试】**以检查是否正常连接到添加的共享文件夹。
     - 共享文件夹名称：输入共享文件夹名称。
     - 共享文件夹 IP：输入共享文件夹 IP 地址。
     - 共享文件夹路径：输入共享文件夹的路径。

参考

共享文件夹路径可以输入英文字母和数字，不能以反斜杠(\)开始或结束，且不能输入除了 ‘-’ 、 ‘_’、 ‘.’ 、'/'以外的特殊字符和空格。

     - ID：输入访问共享文件夹的帐户 ID。
     - 密码：输入访问共享文件夹的帐户密码。
   - 扫描结果：设置文件夹和访问帐户以分别移动扫描结果为恶意、正常或未分类的文件。输入所需的信息后，单击**【连接测试】**以检查是否正常连接到添加的共享文件夹。
     - 恶意：输入当扫描结果为“恶意”的文件进行分类的共享文件夹 IP 地址、路径、ID 和密码。
     - 正常：输入当扫描结果为“正常”的文件进行分类的共享文件夹 IP 地址、路径、ID 和密码。
     - 未分类： 输入当扫描结果为“未分类”的文件进行分类的共享文件夹 IP 地址、路径、ID 和密码。
   - 输入描述：输入最多 63 字符的描述。
5. 点击**保存**。
6. 点击**应用更改配置**。

计划扫描设置

添加共享文件夹计划扫描设置步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**共享文件夹 > 计划扫描**。
3. 点击**添加**，弹出<添加共享文件夹扫描>窗口。
4. 设置各项目。

- 文件系统：选择共享文件夹的文件系统。
- 扫描对象设置：添加欲扫描的共享文件夹。请参考上面**添加共享文件夹实时扫描**的说明。
- 计划时间：选择计划共享文件夹扫描的时间。

5. 点击**确定**。
6. 点击**应用更改配置**。
7. 要更改计划扫描，请在计划扫描列表中鼠标双击要更改的项目。则弹出<更改共享文件夹计划扫描>窗口，更改所需的项目后点击**确定**。
8. 要删除计划扫描，请在列表中选择要删除的项目（可以多选），然后点击**删除**键，或点击项目左侧的❌。如果弹出确认删除的对话框， 点击**确定**。

11.10 检测和响应

检测设置

为了更有效检测各种安全威胁，配置检测相关的各种配置，如引入途径、检测日志、扫描条件、动态分析操作系统和动态分析对象等。

引入途径

配置 MDS 检测威胁的服务协议和 BCC。如果将每个协议设置为检测对象，则通过该协议收集到的数据包以镜像方式检查。按如下步骤设置。

> **参考**
>
> BCC 是 Blind Carbon Copy 的简称，中文名称为密件抄送。如果使用 BCC 方式，MDS 服务器作为密件添加到接收邮件的邮件头，MDS 服务器则对接收邮件执行扫描。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置检测对象的引入途径。
   - 镜像：选择 MDS 检测对象引入时使用的协议。如要全选，请选择**镜像**复选框。
   - E-mail BCC：选择 **E-mail BCC** 以检测发送到特定邮件服务器的邮件的正文或附件是否被恶意代码感染。当启用该选项，MDS 服务器将密件抄送收件人的邮件，并检查邮件正文或附件是否感染恶意代码。如果不启用该选项，则使用镜像方法通过 SMTP 扫描传入的数据包，以检查邮件是否被感染。
4. 点击**确定**。
5. 点击**应用更改配置**。

检测日志显示设置

MDS 将从镜像流量中收集的文件的检查结果记录在日志文件中，并设置在 Web 界面监视检测日志与否。按如下步骤设置。

> ⚠**注意**
> 对于压缩文件或电子邮件，恶意状态由检测日志设置决定。即使是恶意的，但是没有设置为显示检测日志的话，则不被判定为恶意。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置检测日志。
   - 文件：选择记录日志的检测文件严重级别。
   - C&C：选择记录日志的检测 C&C 服务器的严重级别。
   - 恶意 URL：选择记录日志的检测恶意 URL 的严重级别。
4. 点击**确定**。
5. 点击**应用更改配置**。

扫描条件设置

配置恶意代码的扫描条件。按如下步骤设置。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置扫描条件。
   - 扫描大小限制：输入要扫描的最大文件大小。有效值为 1~300MB。
   - 扫描压缩文件：启用复选框，将对压缩文件进行扫描。
     - 最多压缩次数：输入要扫描的文件的最多压缩次数。有效值为 1~5 次。
   - 潜在的有害程序（PUP）：选择复选框，将潜在的有害程序检测为恶意。潜在的有害程序包括：生根程序、黑客工具或用户不知情的情况下安装到用户计算机并窃取个人信息的任何恶意软件。
   - 可能有害程序：选择复选框，将 MDS 分类为可能有害的程序(如键盘记录、远程访问工具等)检测为恶意。
4. 点击**确定**。
5. 点击**应用更改配置**。

动态分析设置

配置执行动态分析的虚拟机（VM）使用的操作系统和其他动态分析对象。按如下步骤设置。

1. 点击 Web 界面主菜单中的**管理**图标。

2. 在左侧菜单中选择**检测和响应 > 检测设置**。
3. 设置如下项目。
   - 分析时间：输入动态分析时间。有效值为 10~300 秒。
   - 操作系统：选择虚拟机（VM）使用的操作系统。

> **参考**
> 用户可以配置自定义的虚拟机（VM）环境，有关详细的内容，请参考更新。

   - 其他动态分析对象
     - 已知恶意代码：选择复选框，将已知恶意代码添加到动态分析对象。
     - 创建可能正常的行为分析报告：选择复选框，将在虚拟机中运行被诊断为可能正常的文件后，分析行为并创建其行为分析报告。创建报告后，将记录检测日志。

> **参考**
> 如果配置其他动态分析对象，则检测日志的记录可能会延迟，并且可能会影响到虚拟机（VM）的性能。

4. 点击**确定**。
5. 点击**应用更改配置**。

VirusTotal

在 MDS 设备利用 MDP 或 DICA 等自身引擎扫描文件之前，配置 VirusTotal 策略先进行扫描。联动 VirusTotal 时，需要使用 VirusTotal 颁发的个人密钥（Private key）作为联动密钥。

> **参考**
> 如果未联动 VirusTotal，则根据产品的最新引擎判断是否恶意。

配置 VirusTotal 策略联动

配置 VirusTotal 策略联动的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > VirusTotal**。
3. 启用**联动 VirusTotal** 复选框，配置使用 virusTotal 策略。输入下面的各项值。
   - Virus Total：点击【更改联动密钥】，弹出<VirusTotal 联动密钥>窗口，输入 Virus Total(www.virustotal.com)颁发的个人密钥（Private Key），然后点击**确定**。
4. 点击**保存**。
5. 点击**应用更改配置**。

代表防病毒软件设置

从 VirusTotal 提供的防病毒软件中，可以设置代表防病毒软件，并根据指定的优先级显示恶意软件诊断名。

设置代表防病毒软件的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > VirusTotal**。
3. 请参考上面的配置 virusTotal 策略联动，联动 virusTotal 策略。
4. 联动成功后，将显示 VirusTotal 提供的防病毒软件列表。
5. 在左侧的列表中选择欲指定为代表防病毒软件的项目，点击  ，所选项目将移动到代表防病毒列表中。
6. 设置已知威胁基准。可以选择**检出比率**或**优先级**。
   - 检出比率：选择**检出比率**后，输入判断为已知威胁的检出比率。

> **参考**
>
> 当选择**检出比率**作为已知威胁基准时，如果在代表防病毒软件列表中，检出威胁的防病毒软件数超过指定的检出比率，则该威胁被视为已知威胁。例如，当选择 5 个防病毒软件作为代表防病毒软件，检出比率输入 3，则表示至少有 3 个代表防病毒软件检出，则该威胁视为已知威胁。

   - 优先级：选择**优先级**。

> **参考**
>
> 当选择**优先级**作为已知威胁基准时，如果在代表防病毒软件列表中，检出威胁的防病毒软件至少有一个，则该威胁被视为已知威胁。

7. 点击**保存**。
8. 点击**应用更改配置**。

> **参考**
>
> Virus Total(www.virustotal.com)颁发 Public Key 和 Private Key。如果加入 Virus Total，免费颁发 Public Key，但是功能存在限制，因此 MDS 仅使用通过 Private Key 联动。有关 Virus Total 的更多内容，请参考 https://www.virustotal.com 的 FAQ。

YARA 规则

使用来自谷歌（google）的开源项目实用程序 YARA，利用恶意文件或进程特征码来设置策略以判断恶意与否。使用字符串模式、二进制模式和正则表达式创建 YARA 规则，检查文件和进程是否包含恶意特征码来诊断为恶意。

⚠注意

如果 MDS Manager 服务器中设置的策略与 MDS 服务器的策略联动使用，则无法使用 YARA 规则修改策略。要上传 YARA 规则或删除，必须禁用与 MDS Manager 服务器的联动。

添加 YARA 规则

添加 YARA 规则的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > YARA 规则**。
3. 点击**添加**，弹出<添加 YARA 规则>窗口。
4. 点击**浏览...**，选择 YARA 规则文件。
5. 选择**严重级别**。
6. 输入有关此 YARA 规则的描述。
7. 点击**确定**。

⚠注意

如果已存在与要添加的 YARA 规则文件名相同的文件，则将使用新添加的文件覆盖该文件。

参考

上传的 YARA 规则文件不能大于 10MB，且最多可以添加 4,096 个。

参考

如要将添加的 YARA 规则文件保存到本地计算机，请点击**导出**键。

更改 YARA 规则

更改 YARA 规则的步骤如下。

1. 在 YARA 规则列表中，点击要更改的 YARA 规则名称，弹出<更改 YARA 规则>窗口。
2. 更改所需的项目。
3. 点击**确定**。

移动 YARA 规则

移动 YARA 规则的步骤如下。

1. 在 YARA 规则列表中，选择要移动的 YARA 规则（选择复选框），然后点击**移动**。
2. 在弹出的菜单中，选择要移动的严重级别。
3. 弹出确认移动的提示，点击**确定**。

参考

如果选择的 YARA 规则中包含了与要移动的规则具有相同严重级别的规则，则无法移动。

导出 YARA 规则

导出 YARA 规则有两种方式，一个是选择导出，另一个是按严重级别全部导出。

选择导出

1. 在 YARA 规则列表中，选择要导出的 YARA 规则（选择复选框），然后点击**导出**。
2. 在弹出的菜单中，选择**选择导出**。
3. 所选的 YARA 规则将保存到本地计算机。

全部导出

1. 在 YARA 规则列表中，点击**导出**。
2. 在弹出的菜单中，选择**全部导出**，弹出<导出 YARA 规则>窗口。
3. 选择要导出的 YARA 规则严重级别。
4. 点击**导出**。
5. 所选的严重级别的 YARA 规则将全部保存到本地计算机。

编写 YARA 规则

YARA 规则由“规则名”和用于特征码模式匹配的“标识符”和“条件”组成。 标识符（strings）利用特殊字符（$）支持字符串、十六进制和正则表达式形式。条件（condition）以 Boolean 值表示结果。编写 YARA 规则的规则原型如下：

```
rule [YARA 规则名]
{
     strings:
        [标识符]

     condition:
        [条件]
}
```

标识符（strings）

- 字符串形式： ASCII 编码的文本需要使用双引号（""）括起来，并区分大小写。（如要转换为不区分大小写模式，请使用 nocase 修饰符 ）
- 十六进制形式：十六进制值需要使用大括号（{ }）括起来。
- 正则表达式形式：正则表达式需要使用斜杠（/ /）括起来。

条件（condition）

条件语法（syntax）必须使用标识符创建并表示为 Boolean 值。条件语法所有 C 语言运算符都可以使用条件语法使用的运算符。

可以使用的运算符如下：

- and, or, not, >=, <=, >, <, ==, !=, +, -, *, \, &, /, <<, >>, ~

一次将多个标识符应用于条件语法的规则如下：

- all of them：适用于所有标识符
- any of them：适用于其中至少一个标识符
- all of ($a*)：适用于以$a 开头的所有字符串
- any of ($a, $b, $c)：适用于$a, $b, $c 中的至少一个

YARA 规则编写案例

```
rule yara001                              // YARA 规则名
{

     meta:                 // 不影响 YARA 规则元数据，特征码模式匹配
        version = "1.0"
       author = "ahnlab"
       description = "yara test"
     strings:
        $string1 = "shutdown -r -t 0"  // 标识符：字符串形式
        $hex1 = { E2 00 [4-8] 34 FA}   //  标识符：十六进制形式
        $re1 = /[0-9a-z]{24}/          //  标识符：正则表达式形式
     condition:
        all of them                    // 条件：适用于所有标识符
}
```

自定义检测规则

MDS 提供通过 Web 管理界面配置自定义行为检测规则的功能，并在检测情况界面查看自定义的检测规则检测到的威胁。

添加自定义检测规则的步骤如下。

1. 点击 Web 界面主菜单中的**管理**图标。

2. 在左侧菜单中选择**检测和响应 > 自定义检测规则**。
3. 点击**添加**，弹出<添加自定义检测规则>窗口。
4. 输入**常规设置**的各项目。
   - 启用与否：选择是否在检测威胁行为时使用此规则。（启用：  ；禁用：  ）
   - 规则名：输入自定义检测规则名。可以输入英文字母、数字和空格，且长度不能超过 128 个字符。
   - 严重级别：选择通过此规则检测到威胁时应用的严重级别。
   - 诊断名：输入通过此规则检测到威胁时应用的诊断名称。可以输入英文字母，且长度不能超过 40 个字符。
   - 诊断信息：输入通过此规则检测到的结果的详细信息。最大不能超过 511 个字符。
5. 设置**动态条件**。点击  ，添加动态条件；点击  ，则删除。

   - 对象：仅可以对当前进程设置动态条件的对象。
   - 行为：选择行为类型。行为主要分为“文件”、“进程”、“注册表”、“网络”和“HTTP”。
   - 条件细节：点击  ，设置上面选择行为的详细条件值。条件细节选项根据上面选择的行为类型而变化，如下表所示。
     - 种类：选择动态条件对象的条件种类。
     - 运算符：选择运算符。有关运算符的详细说明在本章的末尾。
     - 值：输入条件值。
       动态条件的详细输入值，请参考如下表：

行为	条件细节		描述	值输入示例
	种类	值类型		
创建文件	文件路径	字符串	文件的路径	c:\sample.txt
更改文件	文件路径	字符串	文件的路径	c:\sample.txt
	文件偏移	整数	在文件的开头进行修改的位置的值（offset）	0
删除文件	文件路径	字符串	文件的路径	c:\sample.txt

重命名文件	更改前文件路径	字符串	文件重命名前的路径	c:\before.txt
	文件路径	字符串	文件重命名后的路径	c:\after.txt
访问文件	文件路径	字符串	访问的文件路径	c:\sample.txt
***“文件”行为的值不能包含以下字符：** / * ? " < > |				
创建进程	进程图像文件路径	字符串	进程图像文件路径	c:\windows\system32\notepad.exe
	进程运行时命令行数据	字符串	进程运行时输入的命令行	/i 'c:\users\test.exe
运行进程	进程图像文件路径	字符串	进程图像文件路径	c:\windows\system32\notepad.exe
结束另一个进程	进程图像文件路径	字符串	进程图像文件路径	c:\windows\system32\notepad.exe
***“进程”行为的值不能包含以下字符：** / * ? " < > |（但，对于 commandline，没有限制）				
创建注册表项	注册表项路径	字符串	注册表项的路径	HKCU\SOFWARE
删除注册表项	注册表项路径	字符串	注册表项的路径	HKCU\SOFWARE
运行注册表项	注册表项路径	字符串	注册表项的路径	HKCU\SOFWARE
删除注册表值	注册表项路径	字符串	注册表项的路径	HKCU\SOFWARE
	注册表值名称	字符串	注册表项值的名称	valuename
查询注册表值	注册表项路径	字符串	注册表项的路径	HKCU\SOFWARE
	注册表值名称	字符串	注册表项值的名称	valuename
设置注册表值	注册表项路径	字符串	注册表项的路径	HKCU\SOFWARE
	注册表值名称	字符串	注册表项值的名称	valuename
	注册表值类型	字符串	注册表项值的类型	可以在选择框中选择
	注册表值数据	字符串	注册表值的数据	valuedata

* 对于“注册表项（regkey）”，如下定义：

- HKLM, HKCU, HKCR, HKCC（ex. HKLM\SOFTWARE\AhnLab\CommonFilter）

* 对于“注册表项值类型（regvaluetype）”，提供如下选项：

REG_SZ
REG_EXPAND_SZ
REG_BINARY
REG_DWORD
REG_DWORD_BIG_ENDIAN
REG_LINK

REG_MULTI_SZ
REG_RESOURCE_LIST
REG_FULL_RESOURCE_DESCRIPTOR
REG_RESOURCE_REQUIREMENTS_LIST
REG_QWORD

连接特定 IP 地址	协议	-	协议类型（TCP/UDP）	可以在选择框中选择“TCP”或“UDP”
	远程 IP 地址	整数	远程 IPv4 地址	192.168.66.15
	远程端口号	整数	远程端口号	8000
断开与特定 IP 地址的连接	协议	-	协议类型（TCP/UDP）	可以在选择框中选择“TCP”或“UDP”
	远程 IP 地址	整数	远程 IPv4 地址	192.168.66.15
	远程端口号	整数	远程端口号	8000
HTTP Get 请求	远程 IP 地址	整数	远程 IPv4 地址	192.168.66.15
	远程端口号	整数	远程端口号	8000
	域名	字符串	域名	ahnlab.co.kr
	URL	字符串	URI	service.com/tv/turn
	有效载荷数据	字符串	有效载荷数据	Test Data
HTTP Post 请求	远程 IP 地址	整数	远程 IPv4 地址	192.168.66.15
	远程端口号	整数	远程端口号	8000
	域名	字符串	域名	ahnlab.co.kr
	URL	字符串	URI	service.com/tv/turn
	有效载荷数据	字符串	有效载荷数据	Test Data
***“HTTP”行为的“URL”值不能包含以下字符：** ! * ' ( ) ; : @ & = + $, / ? # [ ]				

6. 设置**静态条件**。设置**动态条件**。点击 ，添加静态条件；点击 ，则删除。

- 对象：从下拉框中选择设置静态条件的对象。
- 条件种类：选择静态条件对象的条件种类。
- 运算符：选择运算符。
- 值：输入条件值。
  静态条件的详细输入值，请参考如下表：

对象	条件细节		描述	值输入示例
	种类	值类型		
当前进程 父进程 更改前文件 更改后文件	文件名	字符串	文件的名称	notepad.exe
	文件扩展名	字符串	文件扩展名	exe
	文件大小（字节）	整数	文件的大小（字节）	921600
	文件路径	字符串	文件的路径	c:\sample.txt
	文件格式	-	文件的格式	可以在选择框中选择“Windows 可执行文件”或“Windows 非可执行文件”
	文件签名者	字符串	文件签名者	ahnlab

	系统文件与否	字符串	文件是否是系统文件	可以在选择框中选择“系统文件”或“非系统文件”
***“文件”行为的值不能包含以下字符：** / * ? " < > |				
当前进程父进程	进程运行时命令行数据	字符串	进程运行时输入的命令行	/i 'c:\users\test.exe
	进程 ID	字符串	进程运行时输入的命令行	1920

7. 输入**管理员意见。**
8. 点击**确定。**

动态条件和静态条件共同使用的运算符的详细说明如下表所示：

区分	运算符	描述
字符串	is	输入值（如“before”）与对象值（“更改前文件名”）相同
	is not	输入值与对象值不同
	contains	对象值（如当前进程的文件名）包含输入值（如“aaa”）
	contains not	对象值不包含输入值
	begins with	对象值以输入值开头
	begins not with	对象值不以输入值开头
	ends with	对象值以输入值结束
	ends not with	对象值不以输入值结束
	binary is	输入值与转换为 16 进制的对象值相同
	binary is not	输入值与转换为 16 进制的对象值不同
整数	=	输入值与对象值一致
	<>	输入值与对象值不一致
	>	对象值大于输入值
	<	对象值小于输入值
	>=	对象值等于或大于输入值
	<=	对象值小于或等于输入值

* 字符串运算符不区分大小写。

参考

自定义检测规则仅在 ASDE 3.1.3 或更高版本和 MDS 2.1.14 或更高版本中受支持。

响应设置

设置当检测到恶意文件、C&C 服务器和恶意 URL 时的响应方法。

自动响应设置

设置 MDS 检测到威胁时自动响应的方法。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 在自动相应设置部分，设置当检测恶意文件，访问 C&C 服务器和访问恶意 URL 时的响应方法。
   - 检测到恶意文件时：选择当检测到恶意文件时的处理方法。
     - 删除文件：当检测到的恶意文件符合设置的条件（“已知/未知”和“严重级别”）时，删除该文件。
     - 删除压缩文件：当检测到的恶意压缩文件的严重级别为“低”时，不管未知或已知，都将删除该文件。
     - 隔离系统：当检测到的恶意文件符合设置的条件（“已知/未知”和“严重级别”）时，隔离该文件。
     - 添加引入途径到黑名单：当检测到的恶意文件符合设置的条件（“已知/未知”和“严重级别”）时，将该恶意文件引入途径添加到黑名单。
   - 当检测到访问 C&C 服务器时： 选择当检测到访问 C&C 服务器的行为时的处理方法。
     - 阻止网络：当检测到的访问 C&C 服务器的行为符合设置的条件（“已知/未知”和“严重级别”）时，阻止网络。
     - 隔离系统：当检测到的访问 C&C 服务器的行为符合设置的条件（“已知/未知”和“严重级别”）时，隔离系统。
   - 当检测到访问恶意 URL 时：选择当检测到访问恶意 URL 的行为时的处理方法。
     - 阻止访问：当检测到的访问恶意 URL 的行为符合设置的条件（“已知/未知”和“严重级别”）时，阻止访问。
     - 隔离系统：当检测到的访问恶意 URL 的行为符合设置的条件（“已知/未知”和“严重级别”）时，隔离系统。
4. 点击**保存**。
5. 点击**应用更改配置**。

引入途径(URL) - 阻止访问设置

设置检测到引入途径(URL)时阻止的有效期间。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 在**引入途径(URL) - 阻止访问设置**部分，设置**阻止有效期间**。
   - 阻止有效期：可以选择 7 天、14 天或 30 天。在该期间，引入途径 URL 将被阻止访问。

4. 点击**保存**。
5. 点击**应用更改配置**。

阻止恶意 URL 选项

设置阻止恶意 URL 的详细。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 设置阻止恶意 URL 选项。可以选择重定向或弹出拦截信息。
   - 重定向地址：选择单选按钮，然后输入重定向地址。当检测到访问恶意 URL 时，重定向其转向指定的网址。
   - 拦截信息：选择单选按钮，然后输入警告信息。当检测到访问恶意 UR 时，拦截并显示警告信息。
4. 点击**保存**。
5. 点击**应用更改配置**。

系统隔离设置

设置系统隔离的详细。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 响应设置**。
3. 设置系统隔离的详细。
   - 自动解除：选择复选框启用自动解除功能，并输入隔离时间。当系统被隔离，经过该时间后自动解除隔离。
   - 允许 IP/域设置：设置允许访问的 IP/域。输入 IP 地址、域和描述，然后单击  。即使在系统被隔离的情况下，指定的 IP/域始终被允许访问。
4. 点击**保存**。
5. 点击**应用更改配置**。

威胁警报

设置当检测到威胁时发出警告信息或发送邮件。

威胁警报设置方法如下：

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 威胁警报**。
3. 选择**启用威胁警报**复选框，当检测到威胁时发出警报。警报方法可以选择重定向或拦截。
   - 重定向地址：选择单选按钮，然后输入重定向地址。当检测到威胁时，重定向其转向指定的网址。

- 拦截信息：选择单选按钮，然后输入警告信息。当检测到威胁时，拦截并显示警告信息。

4. 设置威胁警报应用对象网络。输入 IP 地址后，点击  。
5. 选择**检测到恶意邮件时发送邮件**复选框，当检测到恶意邮件时发送警报邮件。输入**邮件标题**和**邮件正文**。
6. 点击**保存**。
7. 点击**应用更改配置**。

引入途径(URL)

通过此页，您可以查看或删除检测到的恶意文件的引入途径(URL)列表，这些 URL 已被阻止。有关引入途径(URL)的阻止设置，可以在“管理 > 检测和响应 > 响应设置”中进行。

查看被阻止的引入途径(URL)

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 引入途径(URL)**。
3. 出现已添加的阻止访问 URL 列表。可以确认如下信息。
   - URL：显示已被阻止访问的引入途径 URL。
   - 严重级别：显示引入途径(URL)的严重级别。级别分为“高”、“中”和“低”显示。
   - 注册日期：显示引入途径(URL)被阻止的日期。
   - 到期日：显示引入途径(URL)的阻止截止的日期。从注册日期到到期日期，引入途径(URL)被阻止。阻止有效期间在“管理 > 检测和响应 > 响应设置”中进行设置。

参考

对于严重级别而言，由于在“管理 > 检测和响应 > 响应设置”中设置为仅阻止引入所选严重级别的恶意文件的 URL，因此，在界面可能不显示所有严重级别。

参考

有关严重级别和阻止有效期的详细说明，请参考响应设置。

删除恶意文件的引入途径(URL)

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 引入途径(URL)**。
3. 出现已添加的阻止访问 URL 列表。
4. 在列表中选择欲删除项目左侧的 ✕，弹出删除对话框。
5. 如果弹出确认删除的对话框， 点击**确定**。

黑名单

您可以通过黑名单来管理无法信任的文件、C&C 服务器、URL、电子邮件地址和数字签名。添加到黑名单的项目始终检测为恶意并拦截。

添加黑名单 - 文件(MD5)

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择**文件**，则出现<添加黑名单 - 文件(MD5)>界面。
4. 设置各项目。
   - 文件名：输入要添加到黑名单的文件名。
   - MD5：输入要添加到黑名单的文件的 MD5 值。具有该 MD5 值的文件将被拦截。最多可以输入英文数字组合的 32 个字符。
   - 处理方法：选择当检测到该 MD5 值时的处理方法。可以在**检测**或**删除**中选择。
   - 严重级别：指定添加到黑名单的文件的严重级别。可以在**高**、**中**、**低**中选择.
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 - C&C 服务器

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择 **C&C 服务器**，则出现<添加黑名单 - C&C 服务器>界面。
4. 设置各项目。
   - 类型：选择要添加到黑名单的 C&C 服务器的类型，可以在 **IP**、**域**和 **URL** 中选择。
   - 名称：输入要添加到黑名单的 C&C 服务器的名称。
   - C&C 服务器：根据选择的 C&C 服务器的类型，输入 C&C 服务器的 IP 地址、域或 URL。
   - 处理方法：选择当检测到该 C&C 服务器时的处理方法。可以选择**检测**或**删除**。
   - 严重级别：指定添加到黑名单的 C&C 服务器的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 -URL

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择 **URL**，则出现<添加黑名单 - URL>界面。
4. 设置各项目。
   - 名称：输入要添加到黑名单的 URL 的名称。
   - URL：输入要添加到黑名单的 URL。
   - 处理方法：选择当检测到该 URL 时的处理方法。可以选择**检测**或**删除**。
   - 严重级别：指定添加到黑名单的 URL 的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 - 电子邮件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择**电子邮件**，则出现<添加黑名单 - 电子邮件>界面。
4. 设置各项目。
   - 分类：选择要添加到黑名单的电子邮件地址类型。
   - 名称：输入要添加到黑名单的电子邮件名称。
   - 电子邮件地址：输入要添加到黑名单的电子邮件地址，根据选择的类型，输入发件人地址或收件人地址。
   - 严重级别：指定添加到黑名单的电子邮件的严重级别。可以选择**高**、**中**、**低**。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加黑名单 -数字签名

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 点击**添加**键，选择**数字签名**，则出现<添加黑名单 - 数字签名>界面。
4. 设置各项目。

- 签名：输入要添加到黑名单的签名。
- 严重级别：指定添加到黑名单的数字签名的严重级别。可以选择**高**、**中**、**低**。
- 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。

5. 点击**确定**。
6. 点击**应用更改配置**。

导入/导出黑名单

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 黑名单**。
3. 执行以下操作。
   - 要导入列入黑名单的列表，单击**导入**后选择类型（文件(MD5)、C&C、URL、电子邮件和数字签名），在弹出的导入界面单击**浏览**选择导入的文件。
   - 要导出黑名单，单击**导出**后选择类型（文件(MD5)、C&C、URL、电子邮件和数字签名），将导出的文件保存到本地系统中。

白名单

您可以通过白名单来管理可信任的文件、C&C 服务器、URL 和电子邮件地址。添加到白名单的项目将被排除在恶意软件扫描和检测之外。

添加白名单 - 文件(MD5)

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择**文件**，则出现<添加白名单 - 文件(MD5)>界面。
4. 设置各项目。
   - 文件名：输入要添加到白名单的文件名。
   - MD5：输入要添加到白名单的文件的 MD5 值。具有该 MD5 值的文件将被允许。最多可以输入英文数字组合的 32 个字符。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - C&C 服务器

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择 **C&C 服务器**，则出现<添加白名单 - C&C 服务器>界面。
4. 设置各项目。
   - 类型：选择要添加到白名单的 C&C 服务器的类型，可以在 **IP**、**域**和 **URL** 中选择。
   - 名称：输入要添加到白名单的 C&C 服务器的名称。
   - C&C 服务器：根据选择的 C&C 服务器的类型，输入 C&C 服务器的 IP 地址、域或 URL。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - URL

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择 **URL**，则出现<添加白名单 - URL>界面。
4. 设置各项目。
   - 名称：输入要添加到白名单的 URL 的名称。
   - URL：输入要添加到白名单的 URL。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - 电子邮件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择**电子邮件**，则出现<添加白名单 - 电子邮件>界面。
4. 设置各项目。
   - 类型：选择要添加到白名单的电子邮件地址类型。
   - 名称：输入要添加到白名单的电子邮件名称。
   - 邮件地址：输入要添加到白名单的电子邮件地址，根据选择的类型，输入发件人地址或收件人地址。

- 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。

5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 -数字签名

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择**数字签名**，则出现<添加白名单 - 数字签名>界面。
4. 设置各项目。
   - 签名：输入要添加到白名单的签名。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

添加白名单 - Snort 规则 ID

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 点击**添加**键，选择 **Snort 规则 ID**，则出现<添加白名单 - Snort 规则 ID>界面。
4. 设置各项目。
   - Snort 规则 ID：输入要添加到白名单的 Snort 规则 ID。
   - 输入描述：描述最多可以输入 127 个字符的英文、中文和数字，且允许输入以下特殊字符：“@”，“.”，“,”。
5. 点击**确定**。
6. 点击**应用更改配置**。

导入/导出白名单

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 白名单**。
3. 执行以下操作。
   - 要导入列入白名单的列表，单击**导入**后选择类型（文件(MD5)、C&C、URL、电子邮件、数字签名、Snort 规则 ID），在弹出的导入界面单击**浏览**选择导入的文件。

- 要导出白名单，单击**导出**后选择类型（文件(MD5)、C&C、URL、电子邮件、数字签名、Snort 规则 ID），将导出的文件保存在系统中。

检测例外

设置检测例外 IP/域，被视为白名单，即使可能会产生可疑流量（包括访问异常或恶意文件）也不会被检测到。

添加检测例外 IP/域 - 文件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 点击**添加**键，选择**添加检测例外 IP/域 - 文件**，则出现<添加检测例外 IP/域- 文件>界面。
4. 选择类别，可以选择 **IP 地址/网络掩码**或**域**。
5. 类别选择“IP 地址/网络掩码”时，输入以下项目：
   - 源 IP 地址：输入 IP 地址和网络掩码。IP 地址可以输入 IPv4 或 IPv6 格式。
   - 目标 IP 地址：输入目标 IP 地址和网络掩码。IP 地址可以输入 IPv4 或 IPv6 格式。
   - 条件：选择“AND”或“OR”。如果选择“AND”，必须同时满足输入的源 IP 地址和目标 IP 地址，才将其处理为检测例外；如果选择“OR”，仅满足源 IP 地址和目标 IP 地址之一，也会将其处理为检测例外。
   - 输入描述：输入最多 63 字符的描述。
6. 类别选择“域”时，输入以下项目：
   - 域：输入域。
   - 地址：输入域地址。
   - 输入描述：输入最多 63 字符的描述。
7. 点击**确定**。
8. 点击**应用更改配置**。

更改检测例外 IP/域 - 文件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 鼠标双击列表中的欲更改项目，打开<更改检测例外 IP/域 - 文件>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除检测例外 IP/域 - 文件

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 在列表中选择欲删除项目左侧的 ✕，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

添加检测例外 IP - 异常流量

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 点击**添加**键，选择**检测例外 IP - 异常流量**，则出现<添加检测例外 IP- 异常流量>界面。
4. 设置各项目。
   - 地址：输入对异常流量检测例外的 IP 地址和网络掩码。
   - 输入描述：输入最多 63 字符的描述。
5. 点击**确定**。
6. 点击**应用更改配置**。

更改检测例外 IP - 异常流量

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 鼠标双击列表中的欲更改项目，打开<更改检测例外 IP - 异常流量>界面。
4. 更改所需的项目。
5. 点击**确定**。
6. 点击**应用更改配置**。

删除检测例外 IP - 异常流量

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。
3. 在列表中选择欲删除项目左侧的 ✕，弹出删除对话框。
4. 如果弹出确认删除的对话框， 点击**确定**。

导入/导出检测例外 IP

如果要一次添加两个以上的项目，可以编写列表以将其添加到 csv 文件中，然后单击**导入**。

1. 点击 Web 界面主菜单中的**管理**图标。
2. 在左侧菜单中选择**检测和响应 > 检测例外**。

3. 执行以下操作。
   - 要导入列入检测例外的列表，单击**导入**后选择类型（文件或异常流量），在弹出的导入界面单击**浏览...**选择要导入的文件。
   - 要导出检测例外列表，单击**导出**后选择类型（文件或异常流量），将导出的文件保存在系统中。

以下是在 csv 文件中写入检测例外 IP 列表的方法。

项目为“文件”的时，写入示例如下：

第一列：IP 地址或域	第二列：条件	第三列：描述	第四列：类别
1.2.3.4/1~22.3.4.5/2	AND	ddd	IP 地址/网络掩码
1.2.3.4/2~1.3.4.5/4	OR	ccc	IP 地址/网络掩码
ahnlab.com		abc	域

项目为“异常流量”时，写入示例如下：

第一列：IP 地址	第二列：描述	第三列：类别
1.2.3.4/1	ddd	IP 地址/网络掩码

第12章　附录

12.1 虚拟机 VirtualBox 安装 win 10 完整步骤

自定义虚拟机（VM）由管理员创建。自定义的虚拟机图像文件和哈希文件可以通过 MDS Web 管理界面的**管理 > 更新**菜单上载到 MDS 服务器。Oracle VM VirtualBox 是一款免费的虚拟机软件，可以在 VirtualBox 虚拟机上安装多样的操作系统。本章将介绍如何在 VirtualBox 上安装 Windows 10 操作系统。

安装准备

- 进入官网下载地址（https://www.virtualbox.org/wiki/Downloads），下载并安装虚拟机 Virtual Box。
- 下载 Windows 10 虚拟机专用 iso 镜像文件。下载地址：https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso

参考

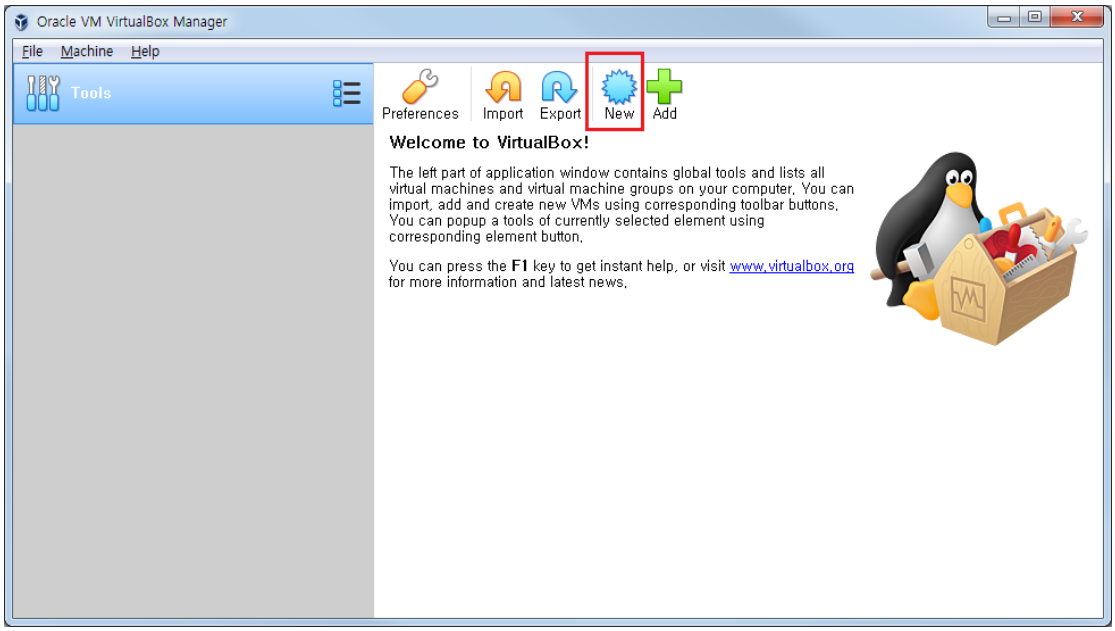
建议所有的操作在连接互联网的环境中进行。

虚拟机 VirtualBox 安装 Windows10 全过程

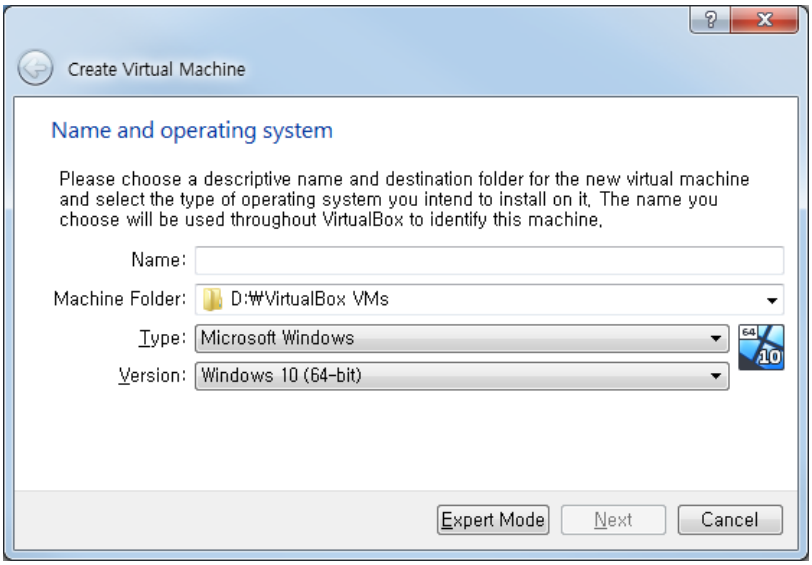
⚠注意

在步骤 4 和 8 中输入的值，以及在步骤 26 中输入的 Windows 用户帐户名和安全密码，必须输入本帮助提示的值。如果管理员输入任意值，则 MDS 无法控制虚拟机。

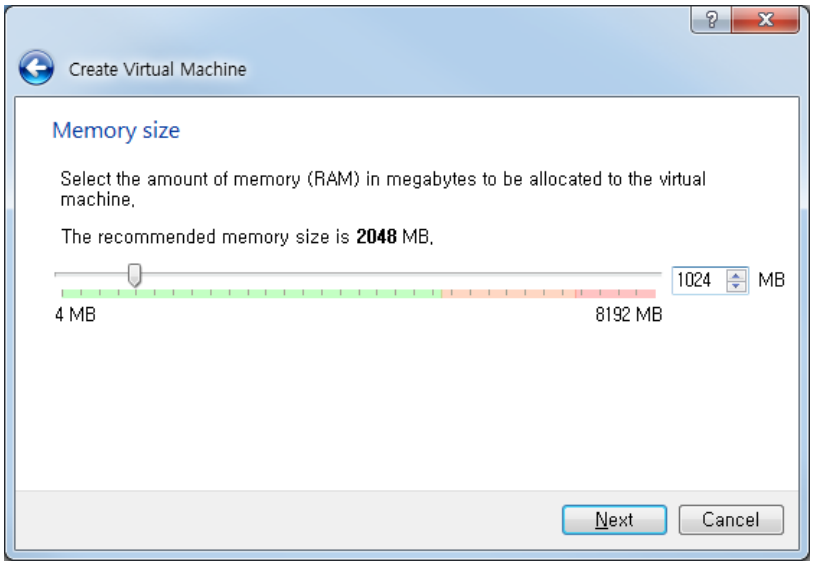
1. 打开 VirtualBox。
2. 出现<Oracle VM VirtualBox Manager>界面。点击**新建**。



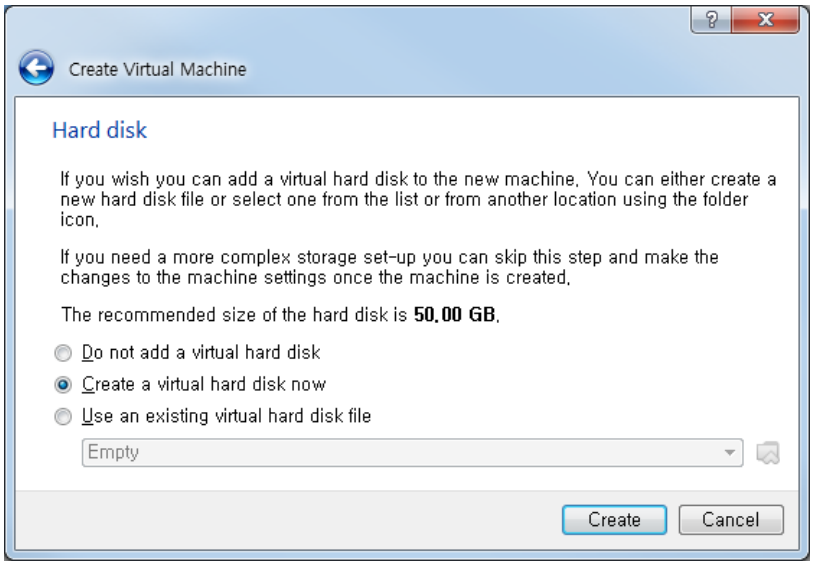
3. 出现<新建虚拟电脑>窗口。输入**名称**为“Windows 10”，**类型**选择“Microsoft Windows”，**版本**选择“Windows 10（64-bit）”，并设置存储**位置**，点击**下一步**。



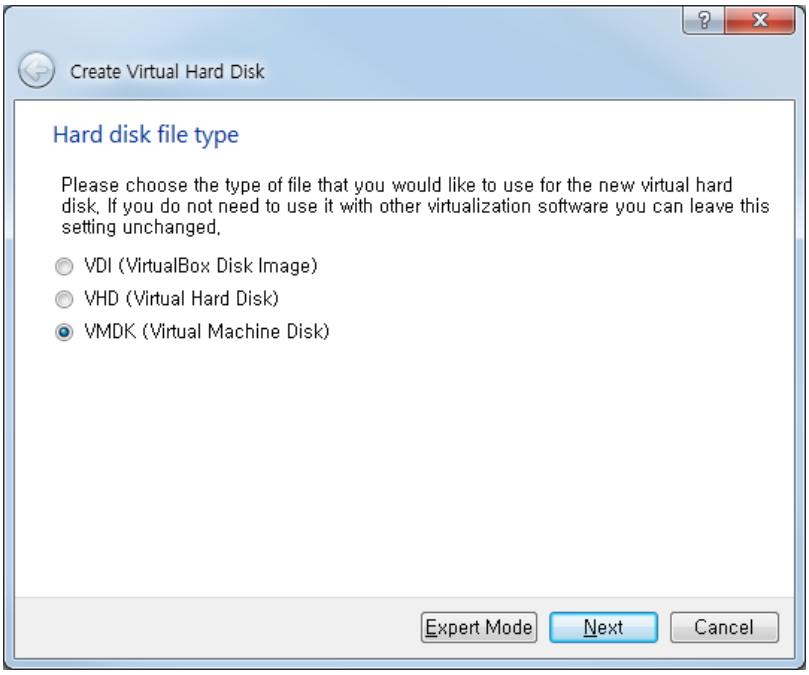
4. **内存大小**设置为 **1024**，点击**下一步。**



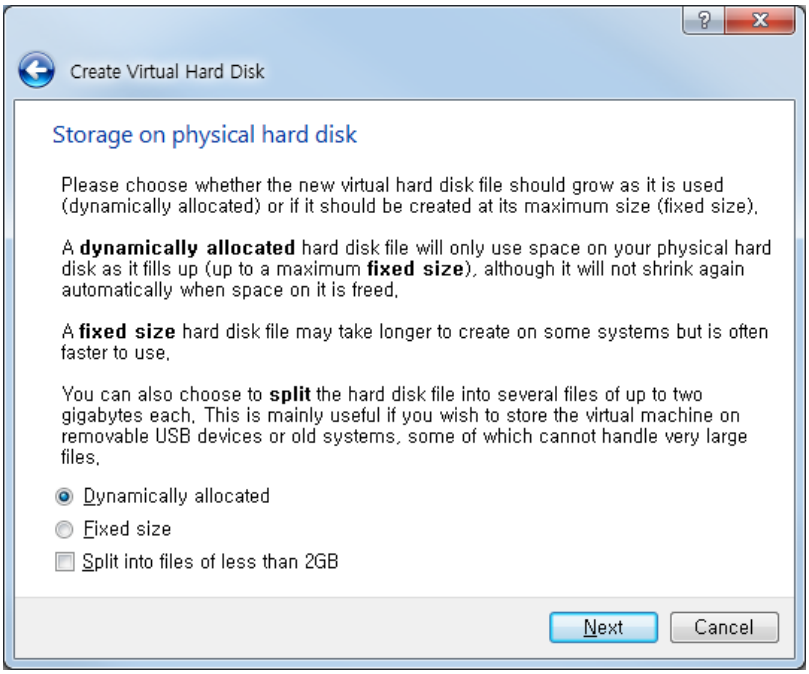
5. 选择“现在创建虚拟硬盘”，点击**创建。**



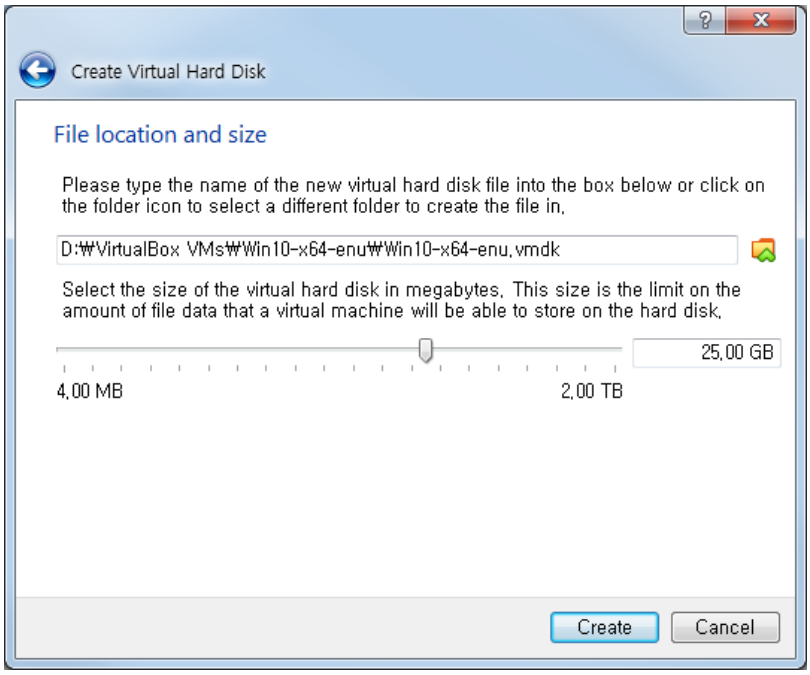
6. **虚拟硬盘文件类型**选择“VMDK（虚拟机磁盘）”，点击**下一步。**



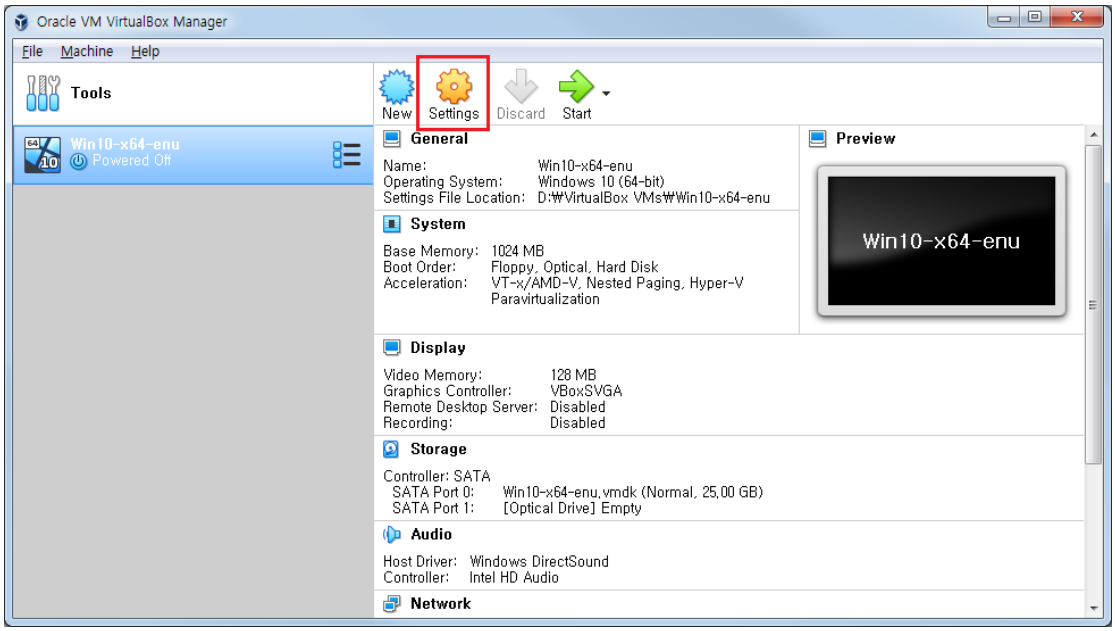
7. 硬盘容量选择“动态分配”，点击**下一步。**



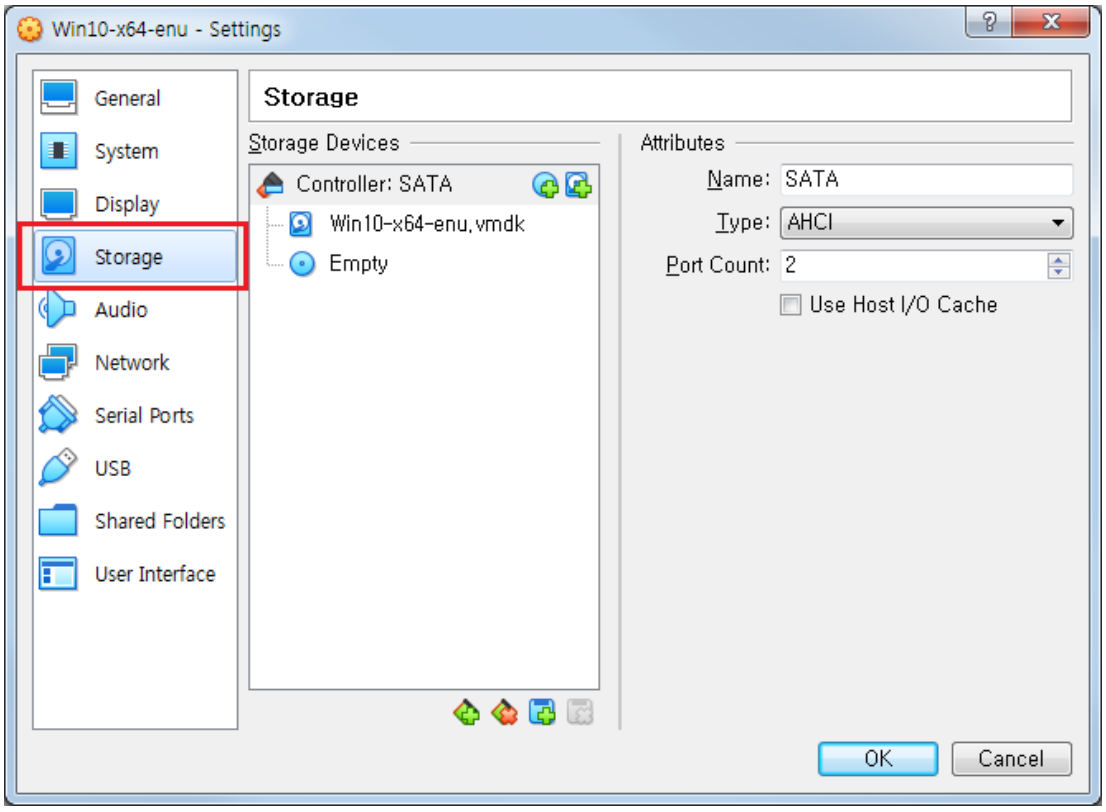
8. 虚拟硬盘的大小设置为“25GB”，点击**创建**。



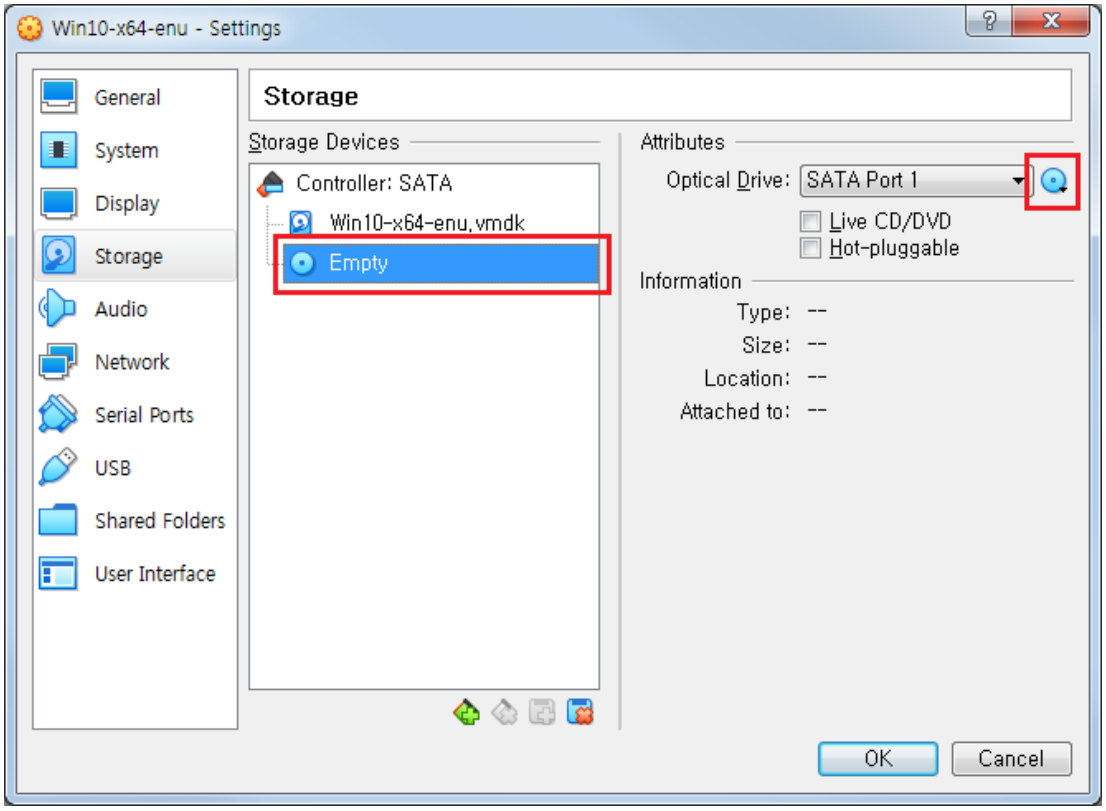
9. 新建了一个 Win10 虚拟机，点击**设置**。



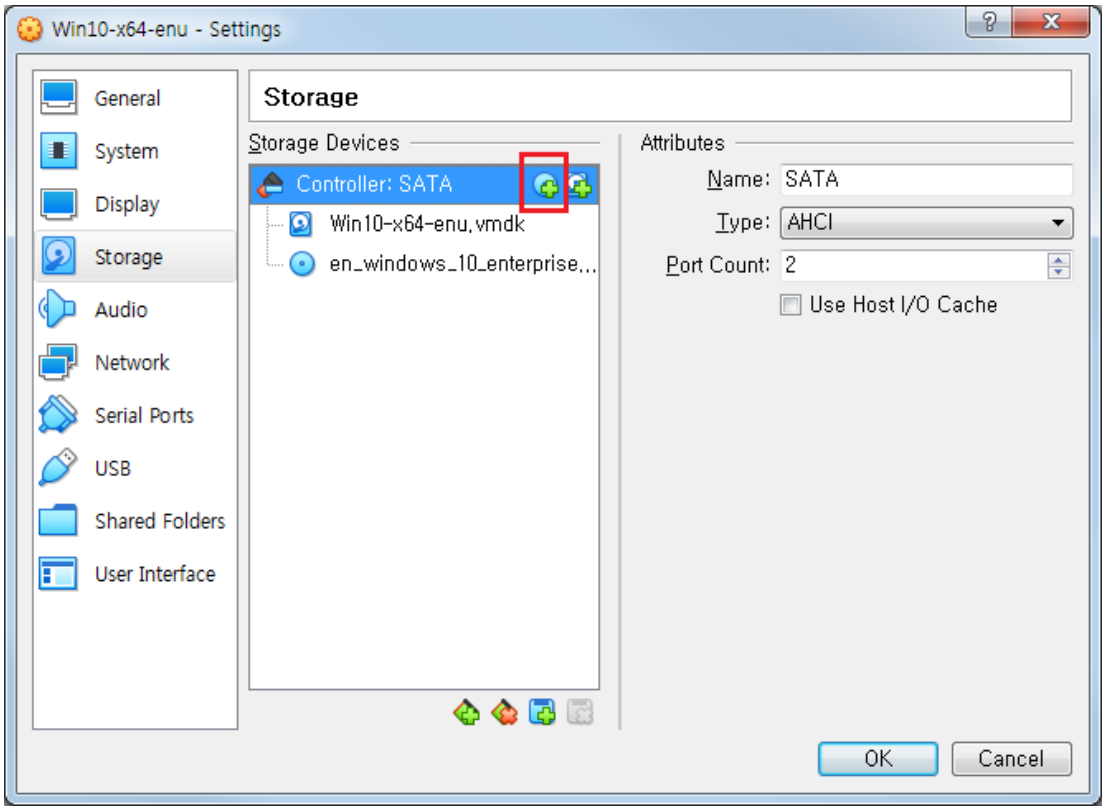
10. 点击**存储**。



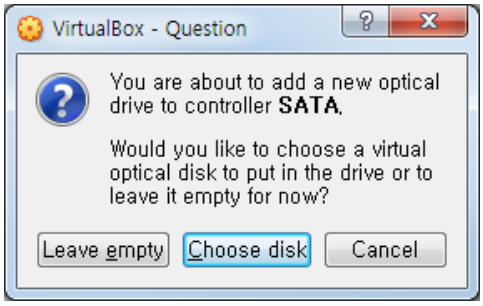
11. 存储设备中选择“没有盘片”，右侧属性中点击光盘图标，选择 iso 镜像文件。



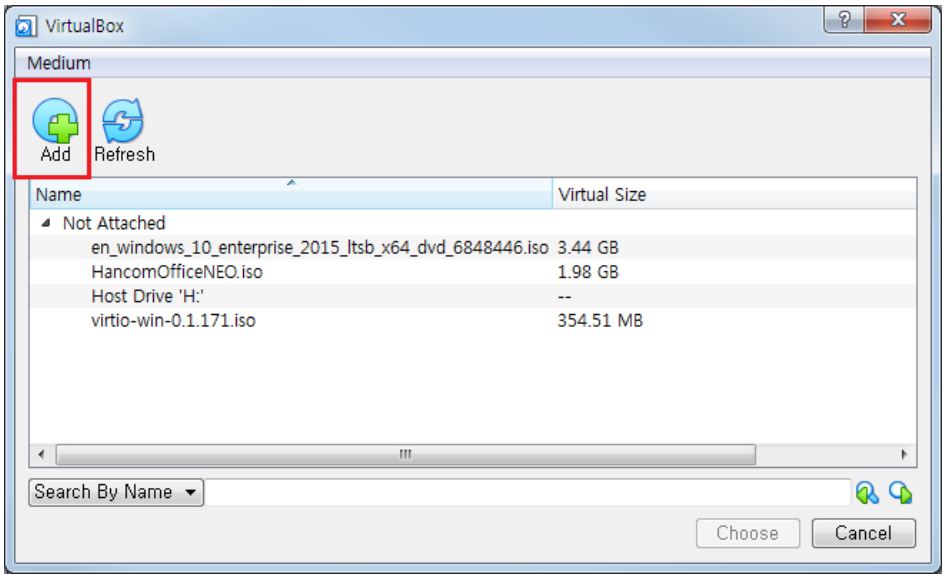
12. 在存储设备中，点击控制器的以添加光盘驱动器。



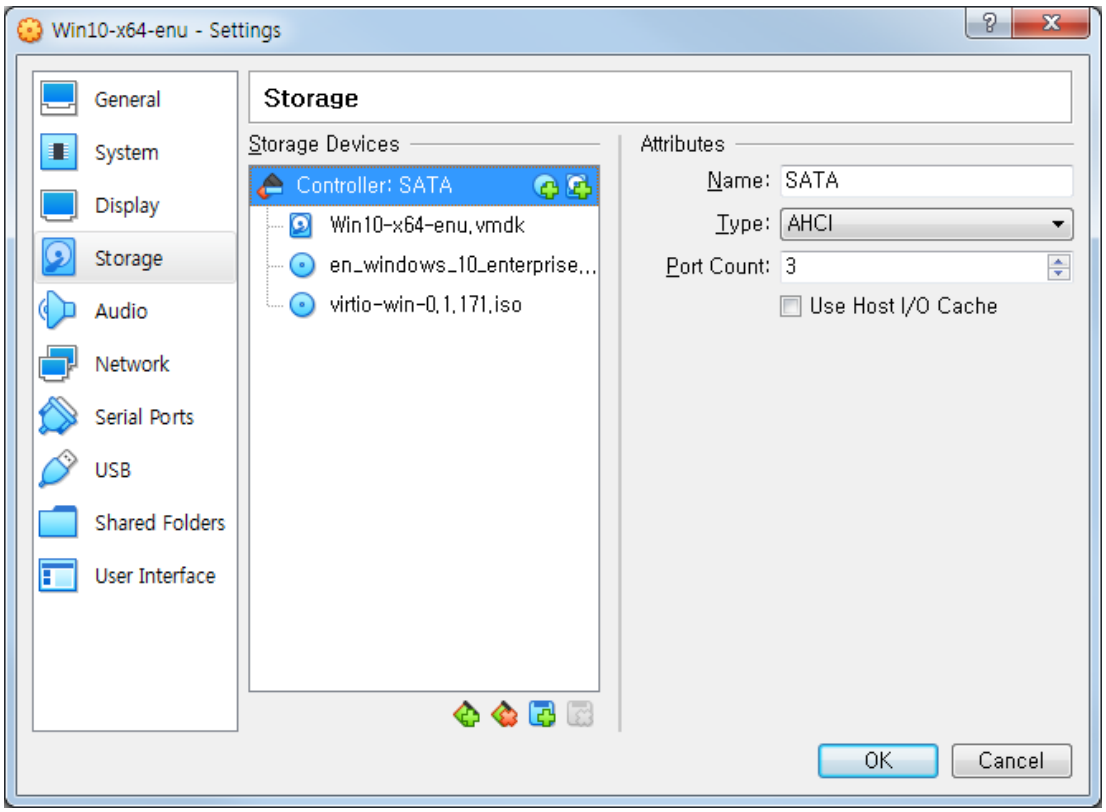
13. 出现<VirtualBox - 问题>窗口，点击**选择磁盘**。



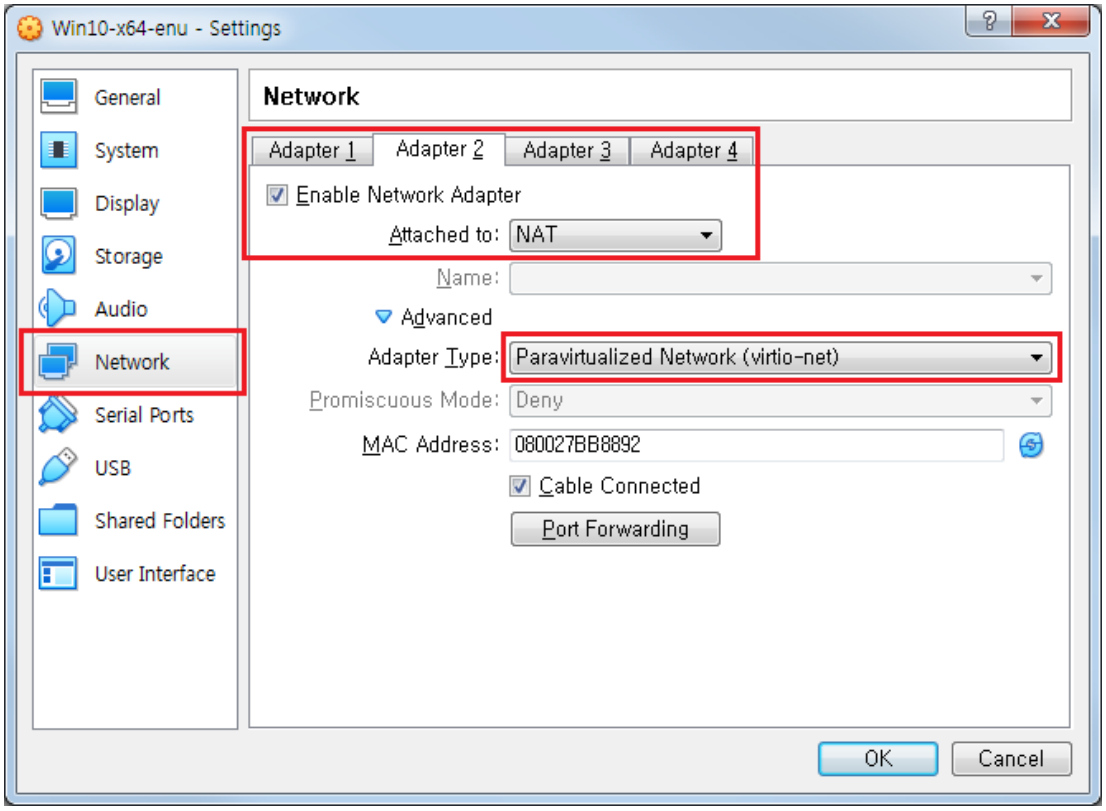
14. 点击**添加**以添加 virtio 驱动程序安装镜像，然后点击**选择**。



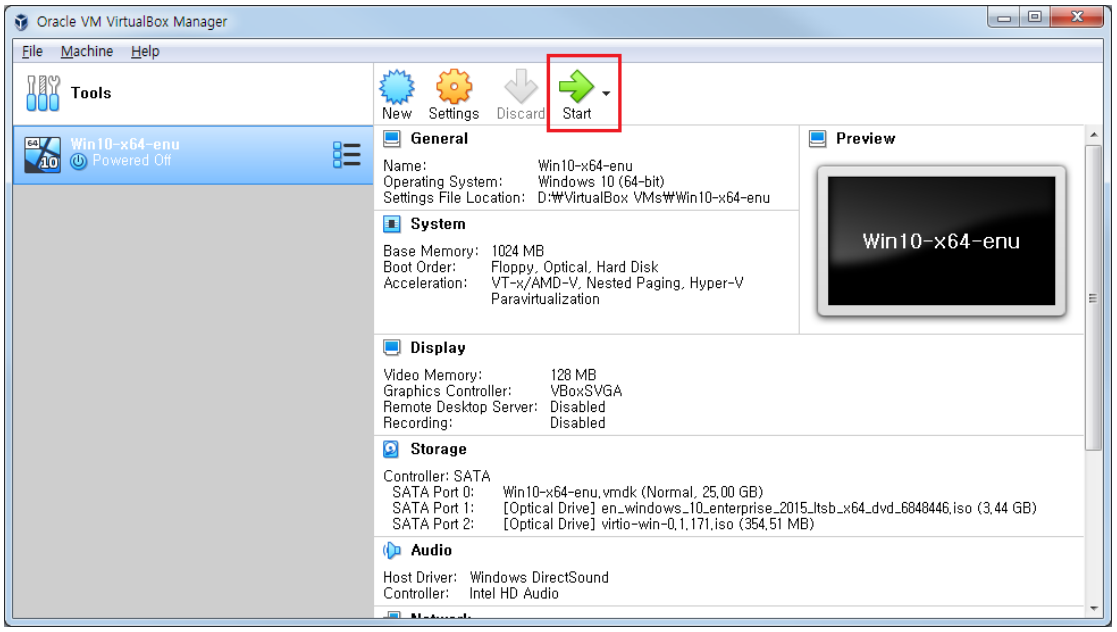
15. 检查添加到存储设备的 virtio 驱动程序安装镜像，然后点击**网络**。



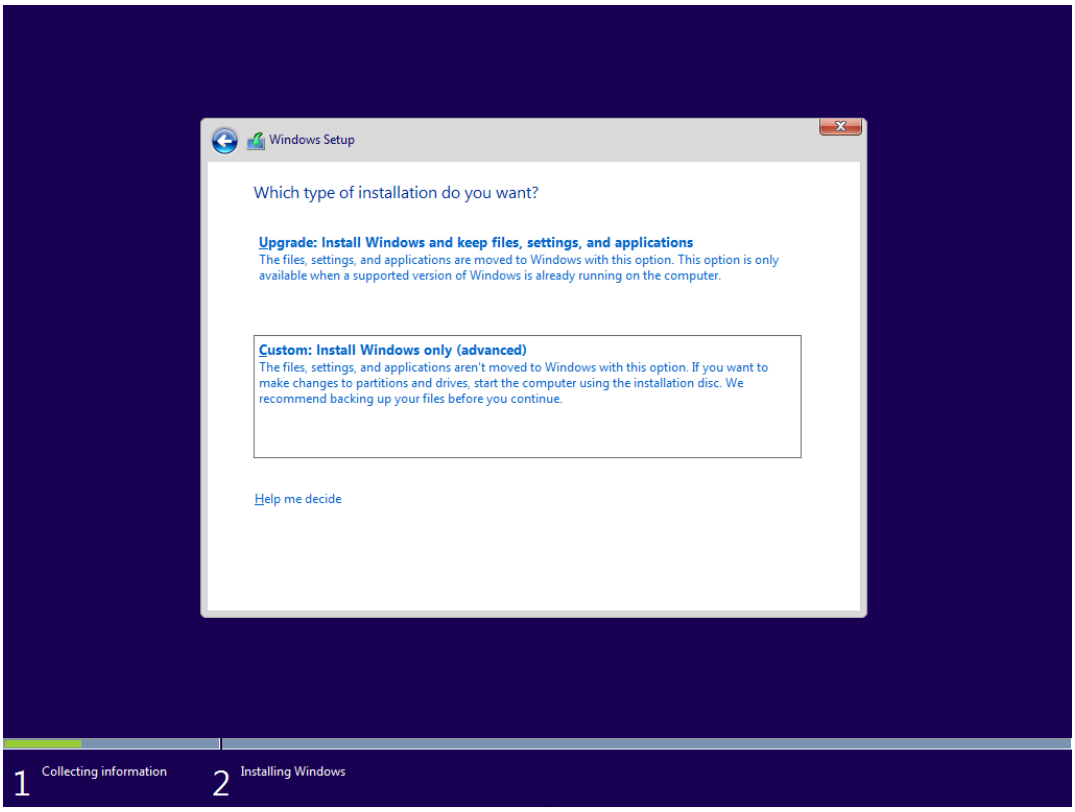
16. 选择**适配器 2** 选项卡。选择“使用网络适配器”，在**附加到**中选择“NAT”，**适配器类型**选择“准虚拟网络”，然后点击**确定**。



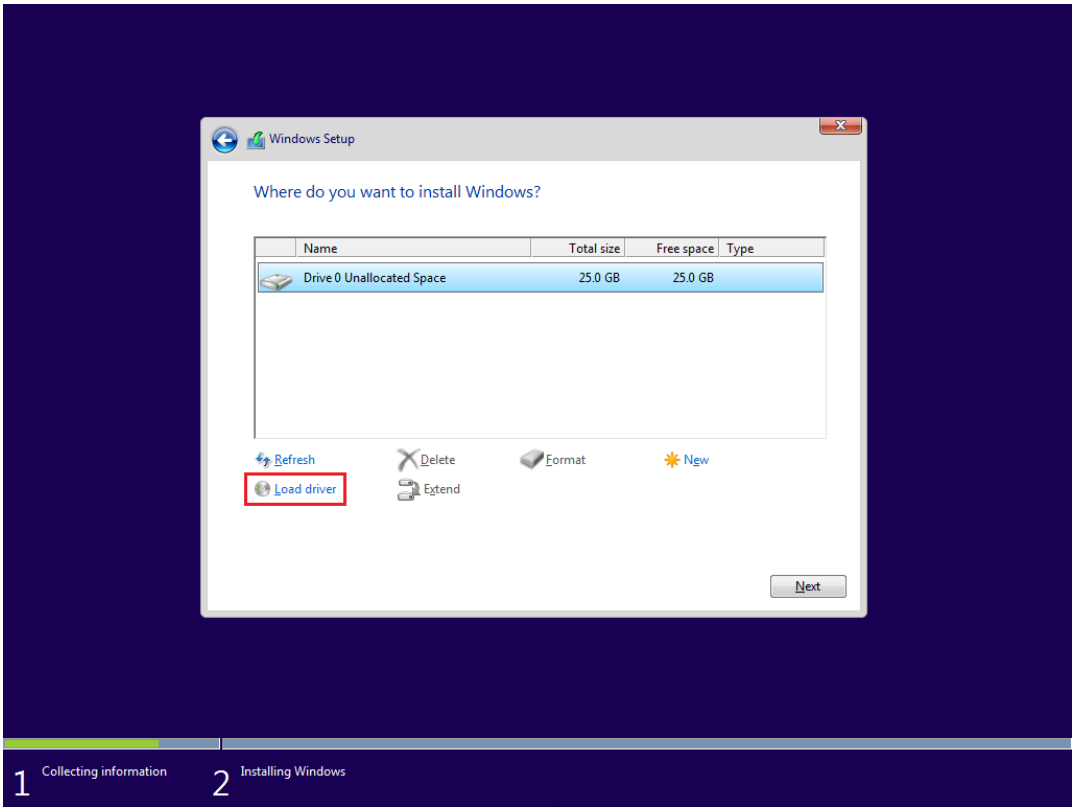
17. 设置完成后，进入 VirtualBox 管理器界面，点击**启动**。



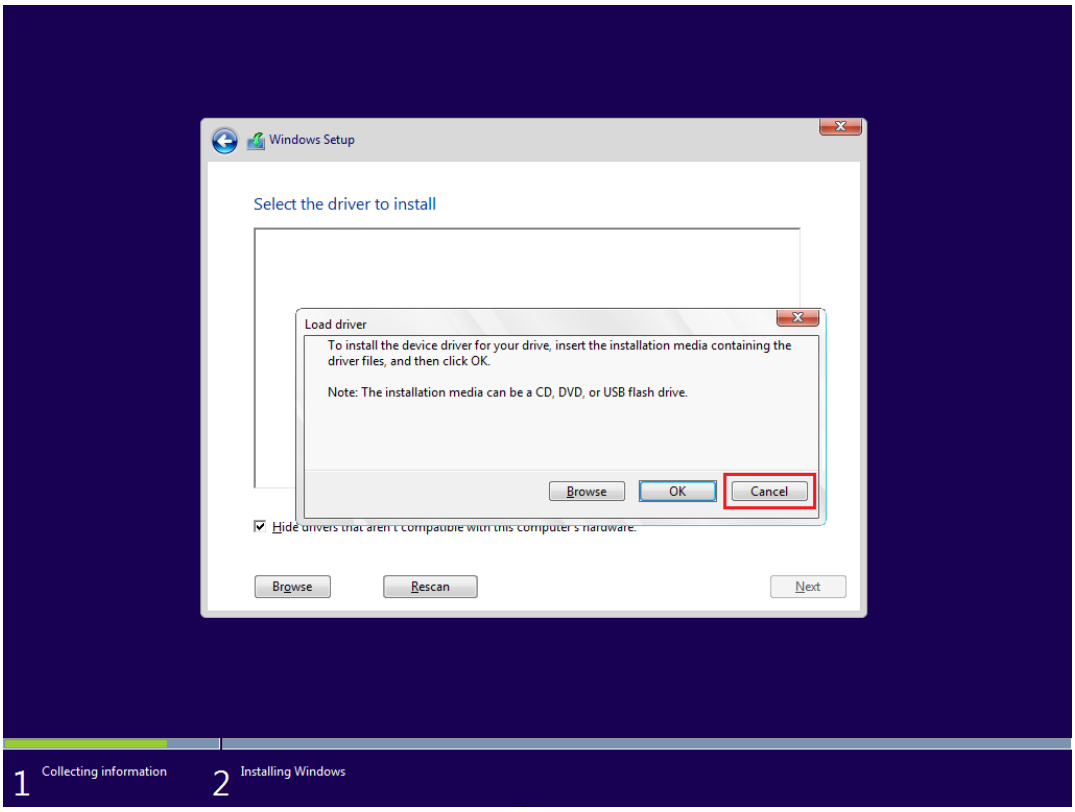
18. 出现<Windows 安装程序>界面。安装类型选择“自定义”。



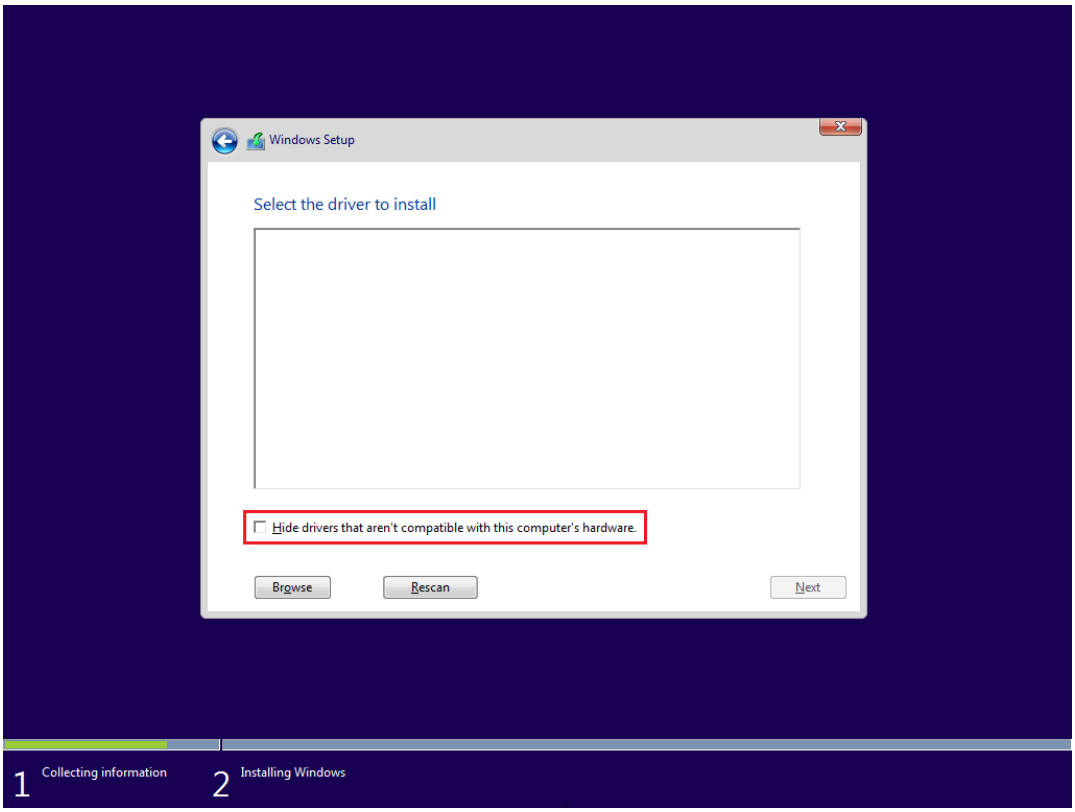
19. 进入安装位置选择，点击“加载驱动程序”。



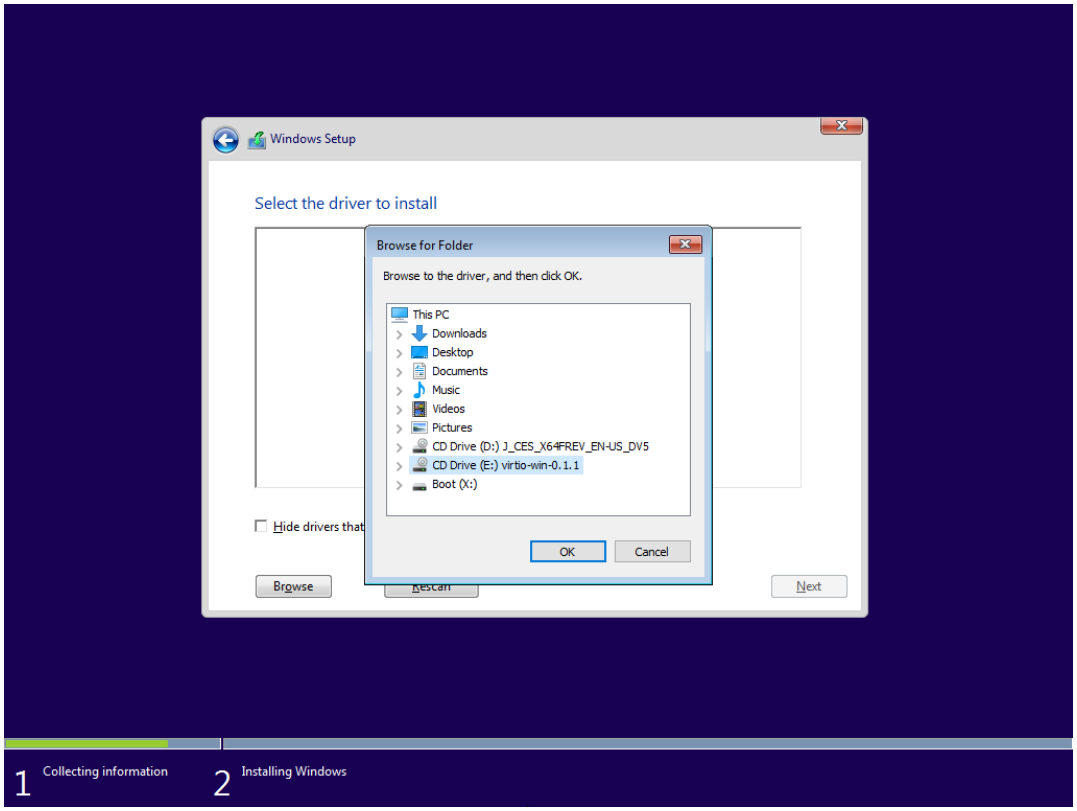
20. 弹出<加载驱动程序>窗口。单击**取消**。



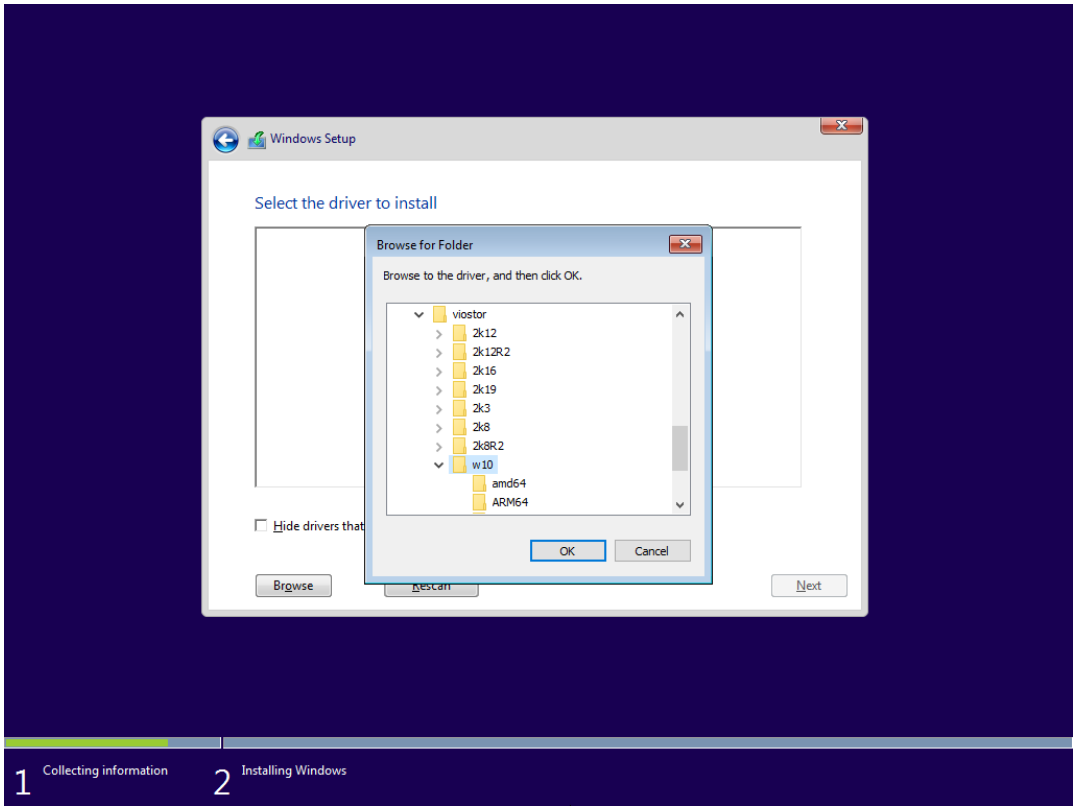
21. 取消选择“隐藏与此计算机的硬件不兼容的驱动程序”，然后单击**浏览**。



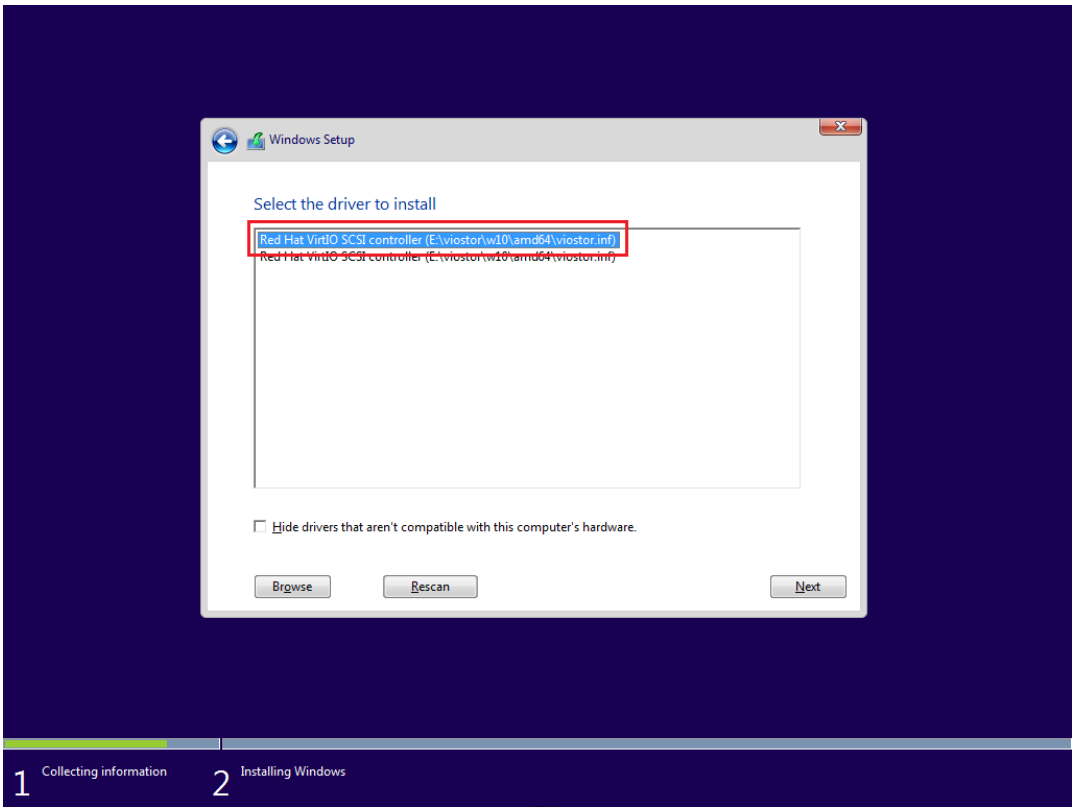
22. 弹出<浏览文件夹>窗口。导航到“w10”文件夹，该文件夹是 virtio 驱动程序镜像的 viostor 文件夹的子文件夹。



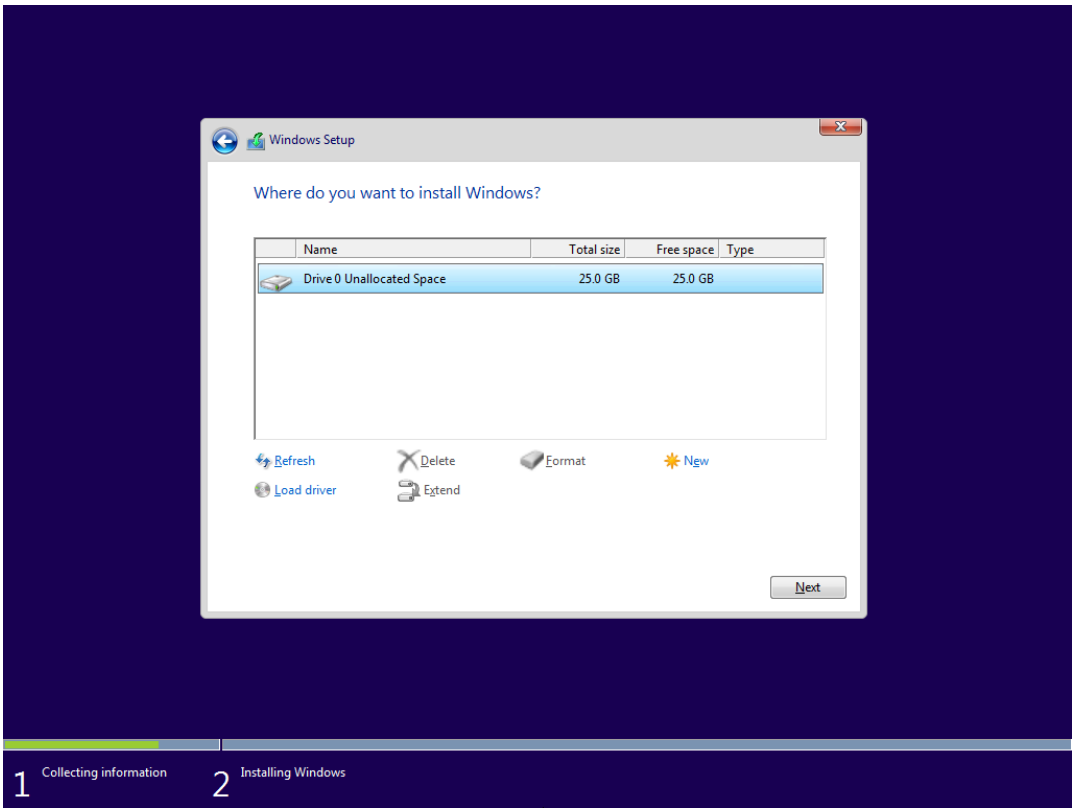
23. 根据要安装的操作系统平台，选择“amd64”或“x86”文件夹，然后单击**确定**。



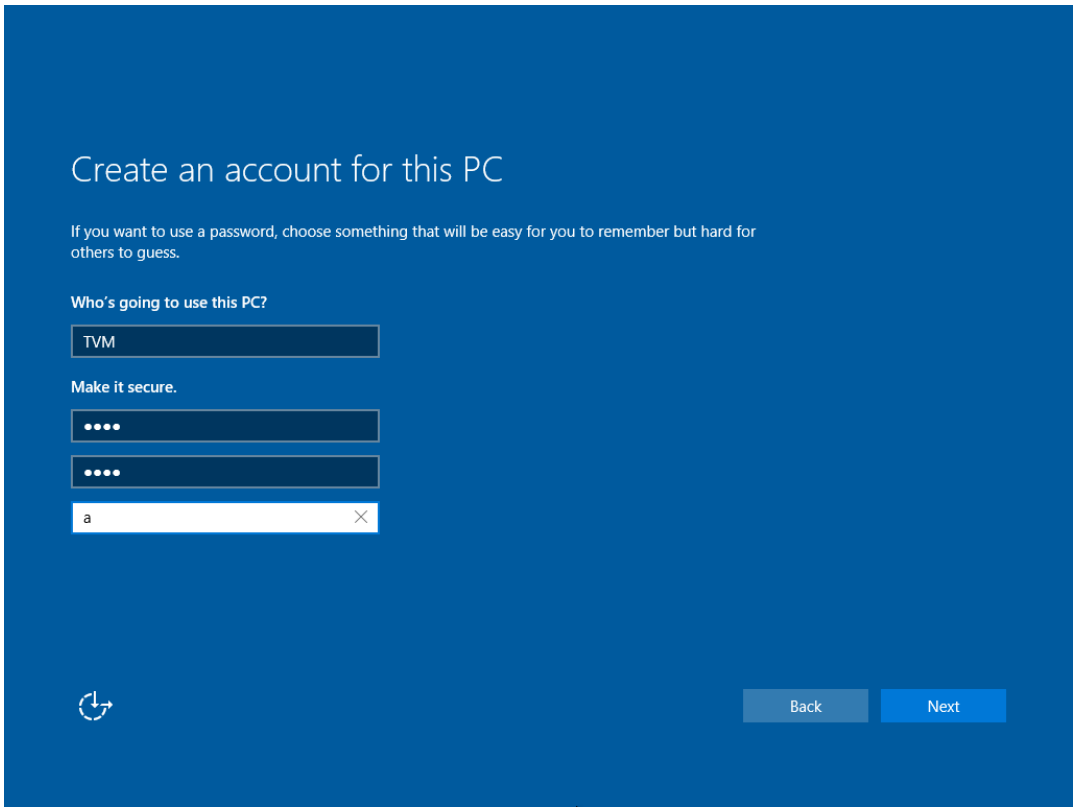
24. 要安装的驱动程序选择“Red Hat VirtIO SCSI controller”，然后单击**下一步**。



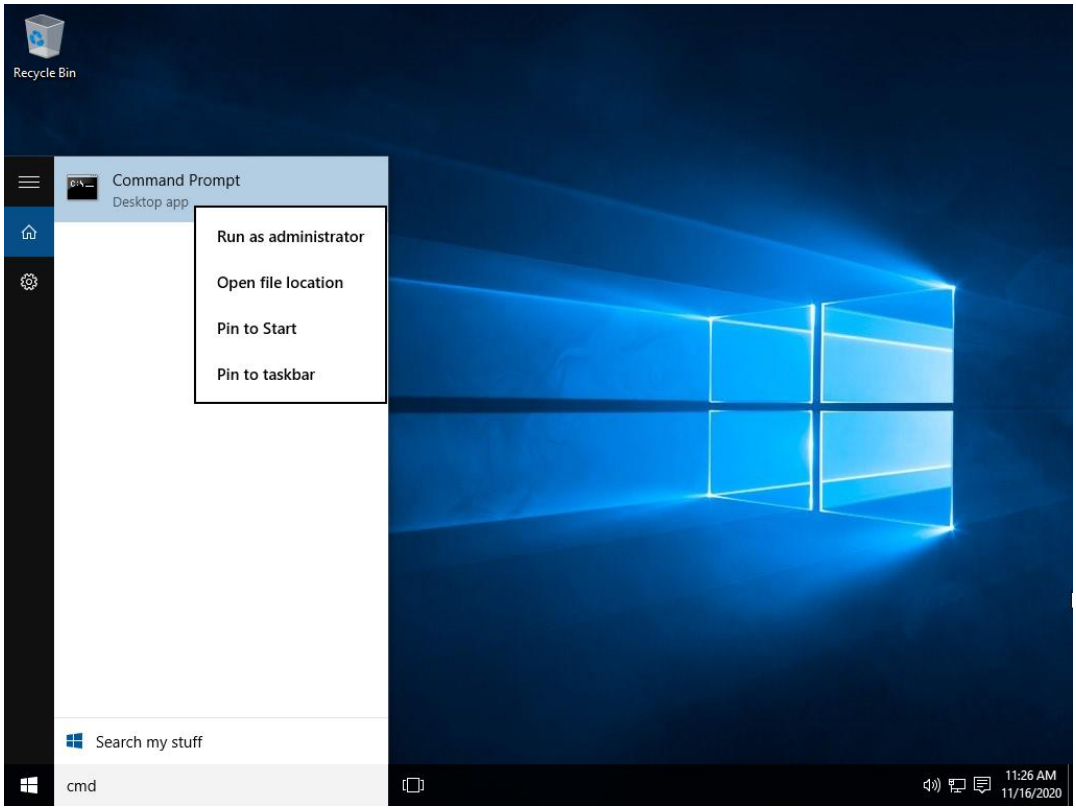
25. 单击**下一步**。



26. 创建帐户。帐户输入“TVM”，密码输入“1111”，然后单击**下一步**。



27. Windows 安装完成，出现桌面。按 **Windows 键**或**开始菜单**，然后键入 cmd，将搜索命令提示符。右键单击命令提示符，然后选择“以管理员身份运行”。



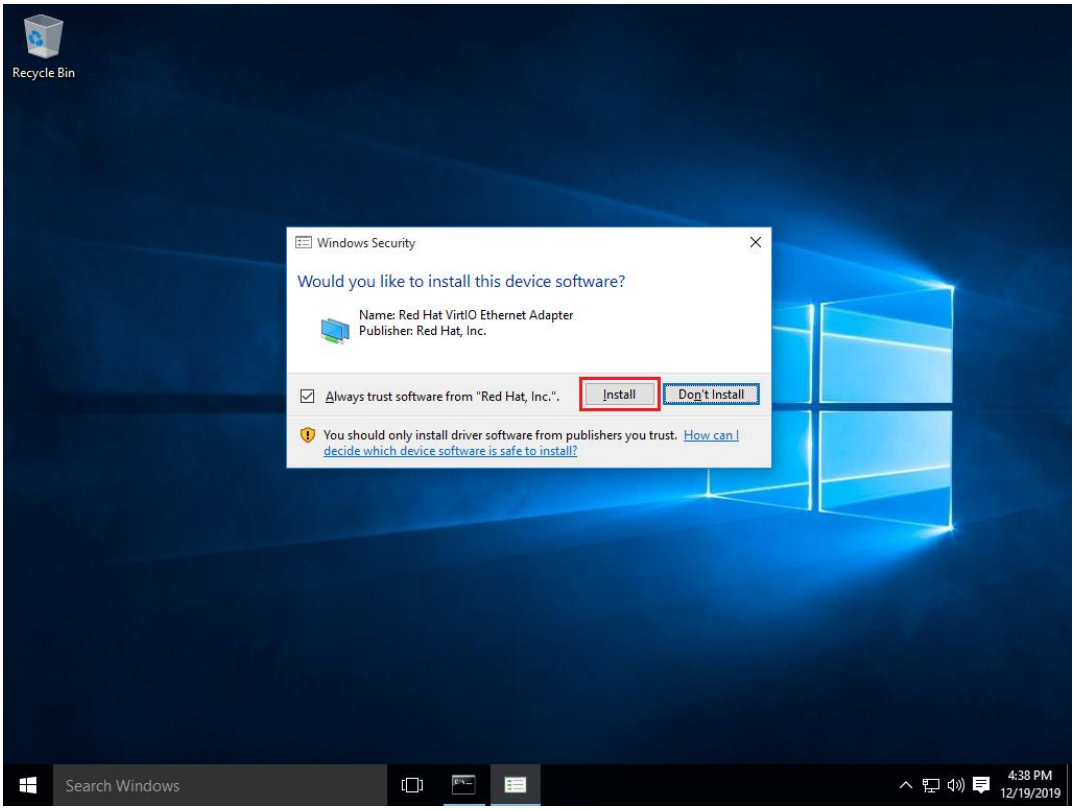
28. 弹出管理员权限的 Windows PowerShell 窗口。按以下顺序输入命令来设置 Windows 自动登录。

```
C:\Windows\system32> REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d TVM /f

C:\Windows\system32> REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f

C:\Windows\system32> REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
```

29. 按以下顺序输入命令以开始安装其他驱动程序。

```
// 64 位操作系统
C:\Windows\system32> pnputil -i -a e:\NetKVM\w10\amd64\netkvm.inf
C:\Windows\system32> pnputil -i -a e:\vioserial\w10\amd64\vioser.inf
C:\Windows\system32> pnputil -i -a e:\Balloon\w10\amd64\balloon.inf
// 32 位操作系统
C:\Windows\system32> pnputil -i -a e:\NetKVM\w10\x86\netkvm.inf
C:\Windows\system32> pnputil -i -a e:\vioserial\w10\x86\vioser.inf
C:\Windows\system32> pnputil -i -a e:\Balloon\w10\x86\balloon.inf
```

30. 如果出现<Windows 安全>窗口，单击**安装**。



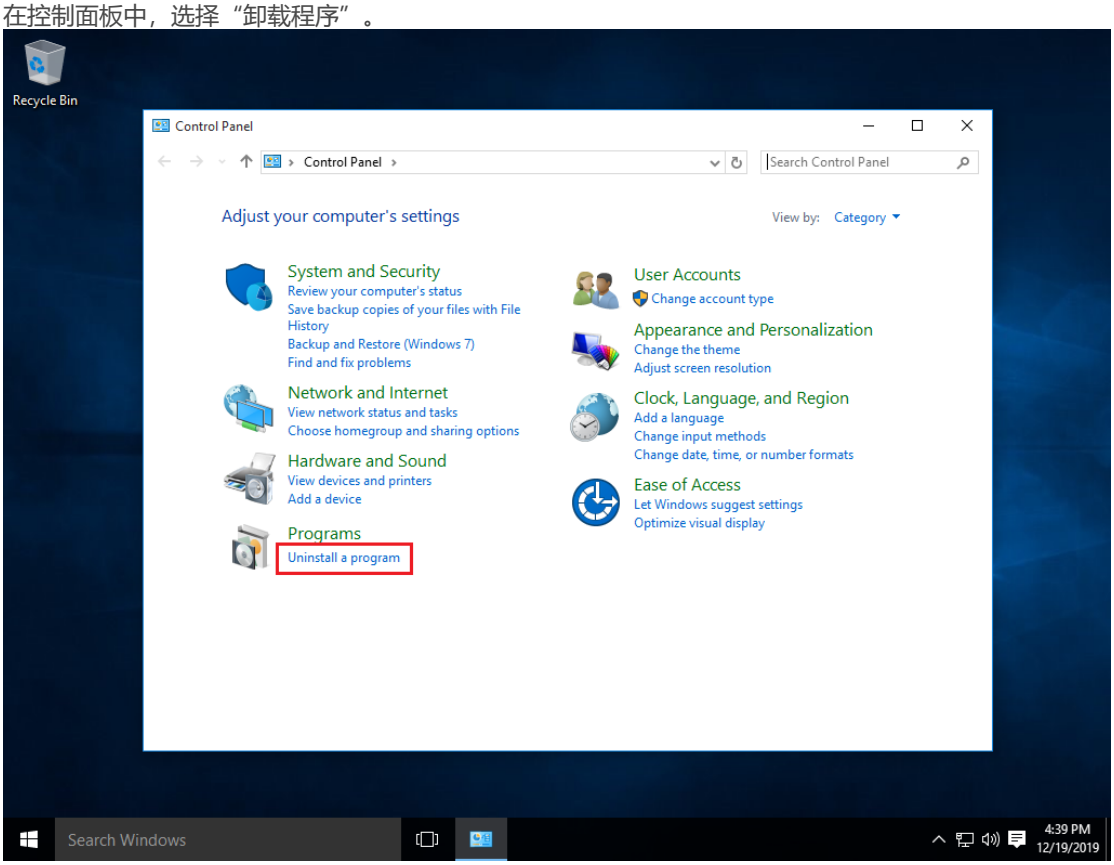
31. 按以下顺序输入命令。

```
C:\Windows\system32> netsh advfirewall set allprofile state off
C:\Windows\system32> powershell -command "& {&'Enable-PSRemoting'-
SkipNetworkProfileCheck -Force}"
C:\Windows\system32> powershell -command "& {&'Set-NetConnectionProfile'-
NetworkCategory Private}"
C:\Windows\system32> winrm quickconfig -force -q
C:\Windows\system32> winrm set winrm/config/service
@{AllowUnencrypted="true"}
C:\Windows\system32> winrm set winrm/config/service/Auth @{Basic="true"}
C:\Windows\system32> sc config winrm start= auto
```

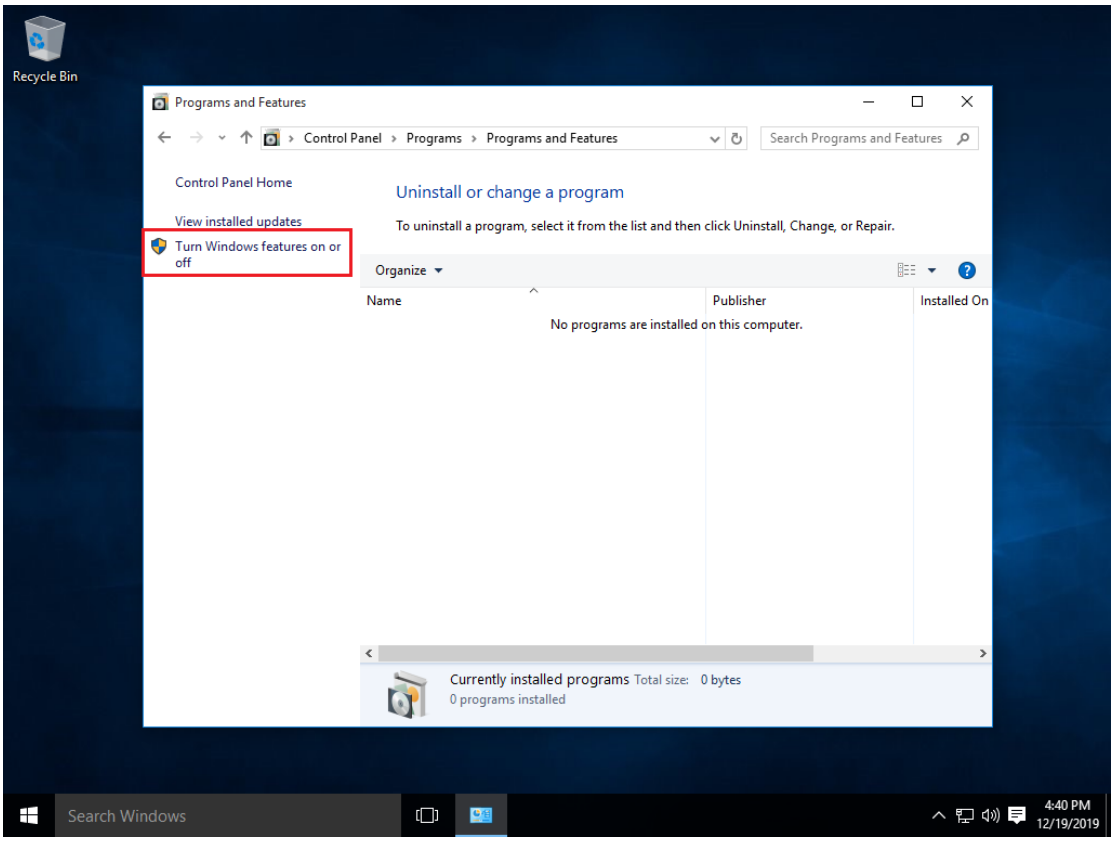
如果您在 PowerShell 中而不是在命令提示符中输入，请按如下输入。此时，请务必小心输入引号的类型。

```
PS C:\Windows\system32> netsh advfirewall set allprofile state off
PS C:\Windows\system32> powershell -command "& {&'Enable-PSRemoting'-
SkipNetworkProfileCheck -Force}"
PS C:\Windows\system32> powershell -command "& {&'Set-
NetConnectionProfile'-NetworkCategory Private}"
PS C:\Windows\system32> winrm quickconfig -force -q
PS C:\Windows\system32> winrm set winrm/config/service
'@{AllowUnencrypted="true"}'
PS C:\Windows\system32> winrm set winrm/config/service/Auth
'@{Basic="true"}'
PS C:\Windows\system32> Set-Service -Name WinRM -StartupType Automatic
```

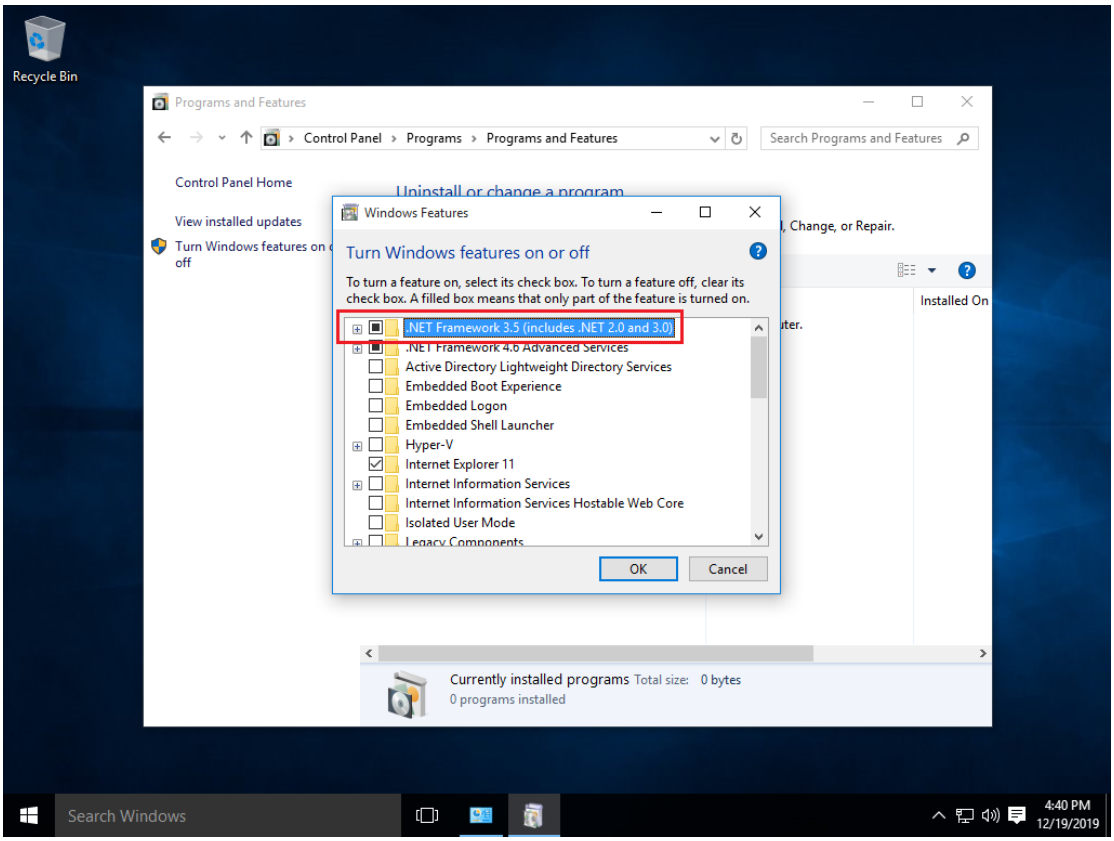
32. 在控制面板中，选择“卸载程序”。



33. 出现<卸载或更改程序>。在左侧菜单中，选择“打开或关闭 Windows 功能”。



34. 出现<Windows 功能>。选择所有的**.Net Framework**，然后单击**确定**。



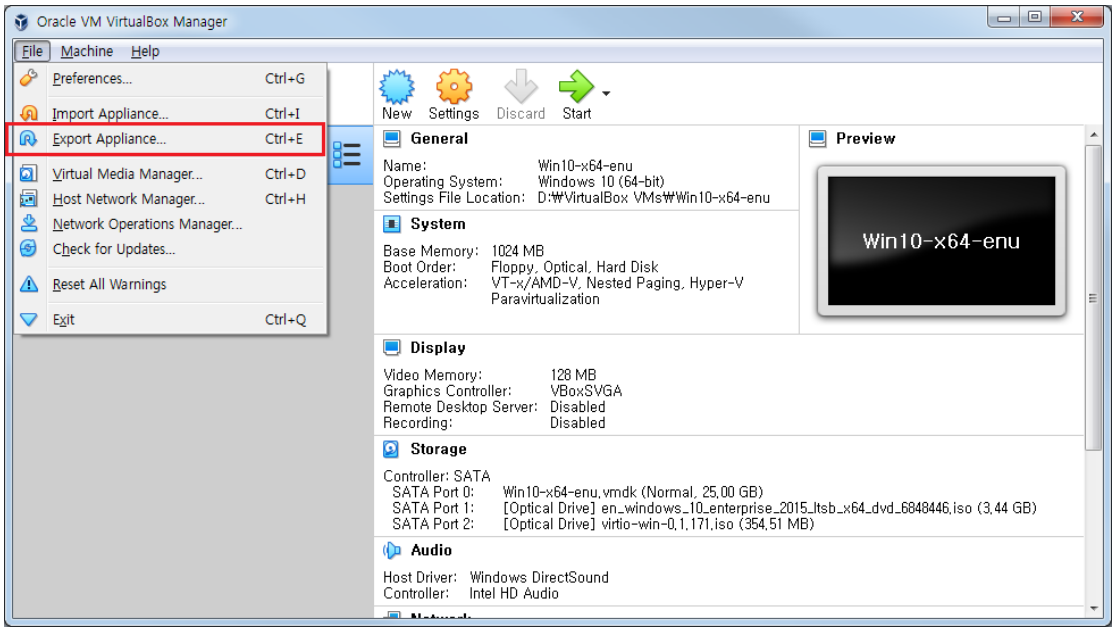
35. 安装下面的软件。

- Adobe Flash Player
- Java Run Time
- Adobe Reader 11 或 Adobe Reader DC
- Microsoft Office 2013 或 Microsoft Office 2016
- Microsoft Visual C++ 重新分发程序包

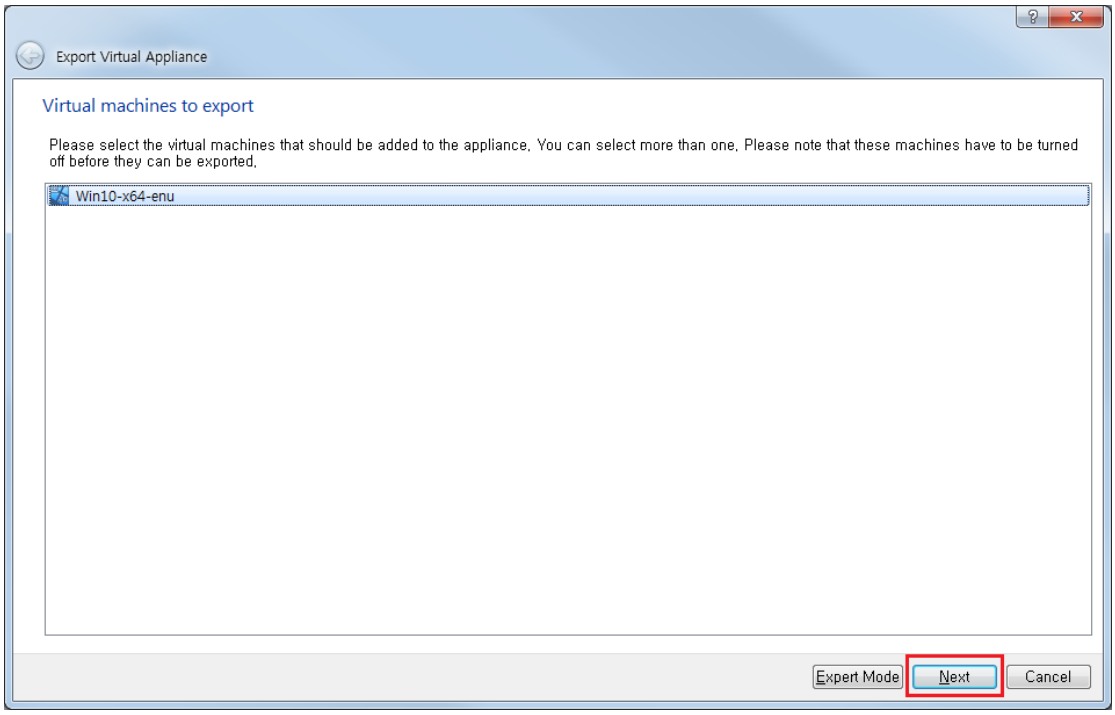
导出虚拟机镜像文件和哈希文件

以下是导出您创建的自定义虚拟机（VM）镜像文件和哈希文件的过程。

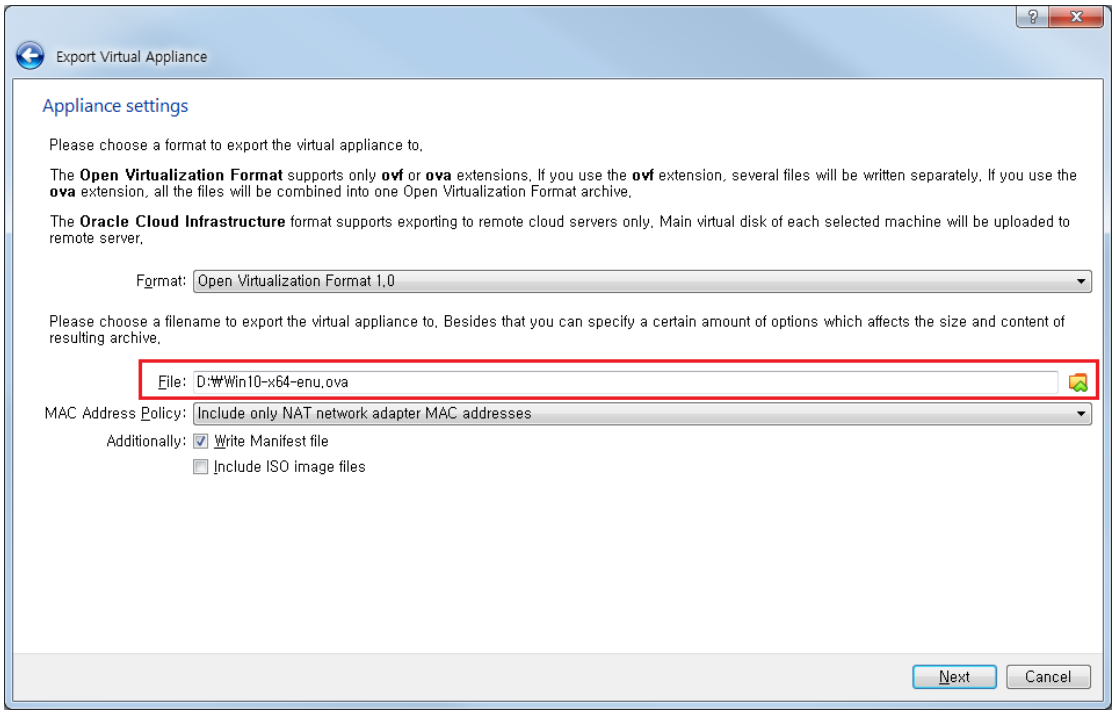
1. 关闭虚拟机，然后重新运行 Virtual Box。
2. 从菜单中选择**文件 > 导出虚拟机。**



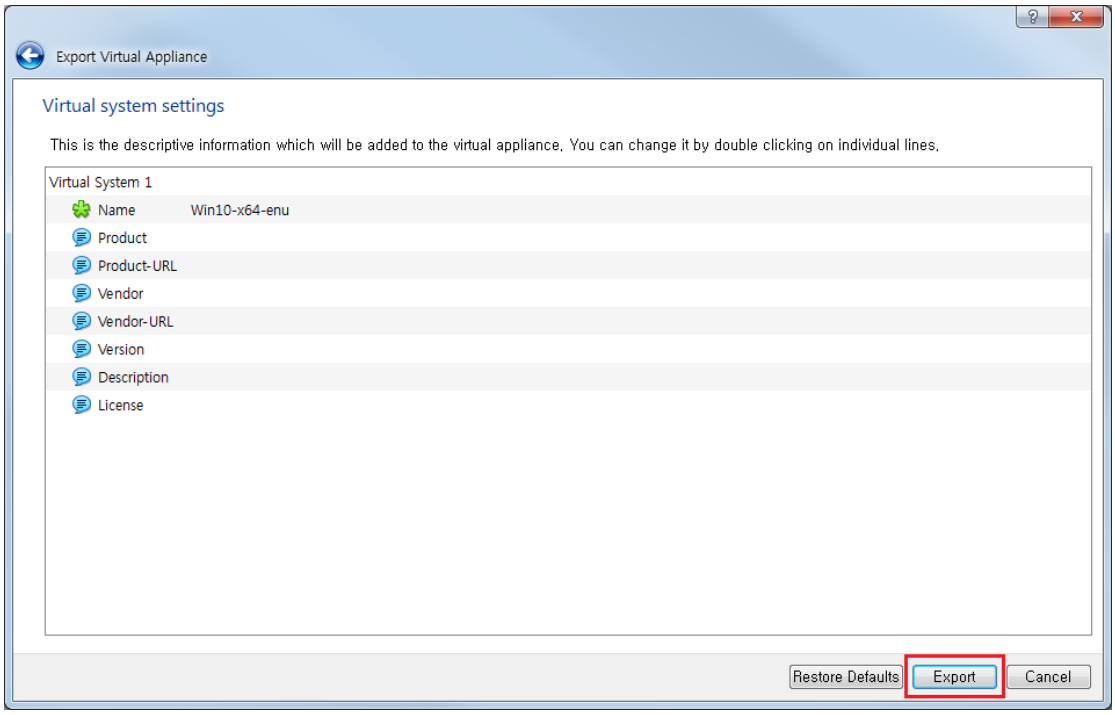
3. 选择要导出的虚拟机，然后单击**下一步。**



4. 在虚拟机设置的**文件**中输入要导出的虚拟机文件路径，然后单击**下一步**。



5. 确认虚拟机 1 的内容，然后单击**导出**。



6. 按 **Windows 键**或**开始菜单**，然后键入 cmd，将搜索命令提示符。右键单击命令提示符，然后选择“以管理员身份运行”。

7. 弹出管理员权限的 Windows PowerShell 窗口。输入以下命令，将导出文件的哈希值（MD5）保存到文件中。

```
C:\Windows\system32> certutil -hashfile <ova path> MD5 | find /i /v "md5"
| find /i /v "certutil" > <hash file name>
```

如果您在 PowerShell 中而不是在命令提示符中输入，请按如下输入。此时，请务必小心输入引号的类型。

```
PS C:\Windows\system32> certutil -hashfile <ova path> MD5 | find /i /v
`"md5"' | find /i /v `"certutil"' > <hash file name>
```

8. 将 ova 文件和生成的哈希文件上载到 MDS 服务器。

⚠注意

在步骤 7 中，**<ova path>**之后键入的 **MD5** 必须是大写。

More security,
More freedom

AhnLab, Inc.

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com

www.ahnlab.com

AhnLab MDS

AhnLab