IBM Security QRadar

Master Console

V0.11.0

备注

使用此信息及其支持的产品前，请阅读第 17 页的『声明』中的信息。

目录

Master Console 简介 v

Master Console 1

Master Console 中管理员的新增内容 1
Master Console V0.11.0 中的新增内容. 1
Master Console V0.10.0 中的新增功能. 1
Master Console V0.9.1 中的新增内容 2
Master Console V0.9.0 中的新增内容 2
Master Console V0.8.1 中的新增功能 2
Master Console 入门 3
受支持的环境 3
安装 Master Console V0.11.0. 5
安装 Master Console V0.10.0 或更早版本 5
打开 Master Console 5
为 Master Console 创建授权令牌 6
向 Master Console 添加部署 6
部署监视. 7
监视受管主机 8
监视攻击. 9
过滤攻击列表 11
用户管理 13
添加本地用户 13
编辑用户设置 13
除去本地用户 13
过滤用户列表 14
在 Master Console 中配置 Active Directory 和 LDAP 认证. 15

声明 17

商标 18
产品文档的条款和条件 18
IBM 在线隐私声明 19
隐私策略注意事项 20

© Copyright IBM Corp. 2015, 2016

Master Console 简介

IBM® Security QRadar® 管理员使用 Master Console 可查看与部署和主机有关的运行状况以及其他信息。

目标受众

本指南面向负责调查和管理网络安全的所有 QRadar 用户。 要使用本信息，您必须具有 QRadar 访问权，并了解贵企业的网络和联网技术。

技术文档

要在 Web 上查找 IBM Security QRadar 产品文档，包括所有翻译文档，请访问 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)。

有关如何在 QRadar 产品库中访问更多技术文档的信息，请参阅访问 IBM Security 文档技术说明 (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

与客户支持人员联系

有关与客户支持人员联系的信息，请参阅支持与下载技术说明 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

有关良好安全实践的声明

IT 系统安全性涉及通过预防、检测和应对企业内外的不当访问来保护系统和信息。不当访问可能会导致信息被篡改、销毁、盗用或滥用，并可能导致系统损坏或者被滥用，包括用于攻击他人。 没有任何 IT 系统或产品应该被认为绝对安全，并且没有任何单一产品、服务或安全措施在预防不当使用或访问方面完全有效。 IBM 的系统、产品和服务设计成合法的综合性安全途径的组成部分，这必定涉及额外的操作过程，并且可能需要其他系统、产品或服务才能实现最高效用。 IBM 不保证任何系统、产品或服务不受任何相关方的恶意或非法行为影响，也不保证能够使您的企业不受这些行为影响。

请注意：

使用本程序可能会涉及各种法律或法规，包括关于隐私、数据保护、雇佣以及电子通信和存储的法律或法规。IBM Security QRadar 只能用于合法目的并以合法方式使用。客户同意按照适用的法律、法规和政策使用本程序，并承担遵守适用的法律、法规和政策的所有责任。 被许可方表示它将获取或已获取允许合法使用 IBM Security QRadar 所需的任何许可、许可权或许可证。

© Copyright IBM Corp. 2015, 2016

Master Console

使用 Master Console 可监视 IBM Security QRadar 部署。

Master Console 对受管安全服务提供者 (MSSP) 环境非常有用。通过使用仪表板可同时监视多个部署。

以可视化方式表示运行数据（例如，CPU 使用率、网络和磁盘活动、内存使用情况以及事件和流的速率），使您更方便监视部署的运行状况。

集中式攻击管理视图按量级顺序显示所有部署中的攻击。向下钻取信息，然后登录特定 QRadar 部署，以获取有关攻击的更多信息。

Master Console 中管理员的新增内容

了解每个 Master Console 发行版中的新增功能部件。

Master Console V0.11.0 中的新增内容

Master Console V0.11.0 包含以下安装和设计上的更改：

安装

Master Console V0.11.0 会在您安装 QRadar V7.2.8 时一起安装。不提供单独下载。

导航改进

新的悬浮菜单使用文字代替了图标，使导航更为直观，便于您找到想要查看的页面。

Master Console V0.10.0 中的新增功能

Master Console V0.10.0 引入了租户和域感知以及对用户列表的搜索和过滤功能，并保留了未来升级中的区域划分信息等。

搜索和过滤 Master Console 用户

使用新的搜索栏，可构建文本和基于字段的查询，以过滤**用户管理**窗口上显示的 Master Console 用户列表。


了解更多有关过滤 Master Console 用户列表的信息...

租户和域感知

现在，Master Console 可显示有关为监视的每个部署所配置的租户和域的信息。单击**受管主机**页面上的**租户**选项卡，可查看每个租户的事件和流比率限制。


了解更多有关 QRadar 部署的信息...

© Copyright IBM Corp. 2015, 2016

改进对未来升级中区域划分信息的处理

若配置了第三方认证服务提供者，未来对 Master Console 进行升级时将保留区域划分设置。为充分利用这项改进，您必须在升级到 Master Console V0.10.0 时或在第一次配置第三方认证服务提供者时，将区域划分信息添加到`shiro.realms` 文件中。

 了解更多有关配置认证服务提供者的信息...

通过 YUM 软件包管理器安装 Master Console

现在，Master Console 是通过 Yellowdog Updater Modified (YUM) 命令进行安装的，该命令提供改进的依赖性检查和软件包管理功能。

 了解更多有关安装 Master Console 的信息...

改进的数据验证和消息

重新设计的**添加部署**、**编辑部署**和**用户管理**窗口在您管理部署和用户帐户时，为您提供改进的数据验证和信息消息。

Master Console V0.9.1 中的新增内容

Master Console V0.9.1 包含用于修订"部署"窗口刷新率的更新，以及用于确保 Master Console 使用更高版本 IBM Security QRadar 的更新。

Master Console V0.9.0 中的新增内容

Master Console V0.9.0 引入了搜索和过滤攻击功能，除去了对 Microsoft Internet Explorer 10 的支持。

搜索和过滤攻击

使用新的搜索栏，可构建基于文本和字段的查询，以过滤在合并的攻击列表上出现的攻击。  了解更多...

受支持的浏览器更新

此发行版删除了对 Microsoft Internet Explorer 10 的浏览器支持。  了解更多...

Master Console V0.8.1 中的新增功能

Master Console V0.8.1 引入了本地用户管理和对 Active Directory 与 LDAP 安全提供程序的支持。

用户管理

您可以授予和控制本地用户对 Master Console 的访问权。升级到 Master Console V0.8.1 或更高版本后，所有现有 QRadar 用户都将作为本地用户迁移到 Master Console。您可以在 Master Console 中管理用户，包括添加用户和更改密码。  了解更多...。

安全提供程序集成

您可以使用现有 Active Directory 或 LDAP 安全基础结构来配置用户认证。  了解更多...

Master Console 入门

安装 Master Console 以监视 IBM Security QRadar 部署中的所有 QRadar 主机的运行状况和系统。

受支持的环境

安装和使用 Master Console 之前，请验证环境中是否有受支持的硬件和软件。

硬件需求

Master Console 在 QRadar 3105 设备上运行。

安装 Master Console 之前，请确认虚拟或物理设备是否符合以下硬件规范：

表 *1. QRadar 3105* 设备概述

描述	值
处理器	8
界面	两个 10/100/1000 Base-T 网络监视界面 一个 10/100/1000 Base-T QRadar 管理界面 一个 10/100 Base-T 集成管理模块界面 两个 10 Gbps SFP + 端口
内存	64 GB 8x 8 GB 1600 MHz RDIMM
存储器	9 x 3.5 英寸 1 TB 7.2 千转/分钟 NL SAS、共 9 TB、6.2 TB 可用 (Raid 5)
电源	750 瓦双冗余交流电源
规格	29.5 英寸长 x 17.7 英寸宽 x 2.4 英寸高

软件需求

要托管 Master Console，您必须使用 8500 激活密钥 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 来安装 IBM Security QRadar。无需单独的许可证密钥。

您可以使用 Master Console 来监视 QRadar Log Manager 部署，但集中式攻击管理视图为空。集中式攻击管理视图仅对监视攻击的系统（如 QRadar SIEM）显示攻击。

托管 Master Console 所需的 QRadar 版本可能不同于 Master Console 可监视的 QRadar 版本。在安装 Master Console 前，请复审下表中的软件需求。

表 2. *Master Console* 的软件需求

Master Console 版本	**安装**	**监控**	**受支持的浏览器**
Master Console V0.11.0*	与 QRadar V7.2.8 一起安装。 IBM Fix Central 上不提供 Master Console V0.11.0 的单独下载。	监视 QRadar V7.2.8 or V7.2.7	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome（最新版本）
Master Console V0.10.0	在 QRadar V7.2.7 上安装。	监视 QRadar V7.2.6 or V7.2.7	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome（最新版本）
Master Console V0.9.1	在 QRadar V7.2.6 或 V7.2.7 上安装。	监视 QRadar V7.2.6 or V7.2.7	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome（最新版本）
Master Console V0.9.0	在 QRadar V7.2.6 上安装。	监视 QRadar V7.2.6 or V7.2.7	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome（最新版本）
Master Console V0.8.1	在 QRadar V7.2.5 或 V7.2.6 上安装。	监视 QRadar V7.2.5 or V7.2.6	Microsoft Internet Explorer 11 Microsoft Internet Explorer 10 Mozilla Firefox 38 Extended Support Release Google Chrome（最新版本）
* 产品支持仅限于已发布的最新版本的 Master Console。			

有关安装 QRadar 的更多信息，请参阅 *IBM Security QRadar Users Guide*。

安装 Master Console V0.11.0

使用 8500 激活密钥 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 安装 IBM Security QRadar V7.2.8 时，会自动安装 Master Console。Master Console V0.11.0 不提供单独下载。

有关安装 QRadar 的更多信息，请参阅 *IBM Security QRadar Users Guide*。

安装 Master Console V0.10.0 或更早版本

使用 8500 激活密钥 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 安装 IBM Security QRadar V7.2.5 或更高版本后，会自动安装 Master Console。无需单独的许可证密钥。有关安装 QRadar 的更多信息，请参阅 *IBM Security QRadar Users Guide*。

您可以从 IBM Fix Central 下载最新的 Master Console 功能部件和增强功能。

开始之前

请确保作为安装位置的设备符合必需的最低硬件规范。有关更多信息，请参阅第 3 页的『受支持的环境』。

您必须具有文件复制软件程序（如 WinSCP），以将 Master Console 修订包文件从本地系统复制到 QRadar 设备。

关于此任务

第一次更新到 Master Console V0.8.1 或更高版本时，此更新过程会从 QRadar 控制台导入用户。导入时将覆盖所有现有 Master Console 用户（包括管理员）的密码，并将它们设置为在 QRadar 控制台上设置的密码。导入过程仅发生一次。以后更新 Master Console 时将不导入用户或覆盖密码。

过程

1. 从 Fix Central (http://www.ibm.com/support/fixcentral) 下载 Master Console 修订包。
2. 使用软件程序（如 WinSCP）将 Master Console 修订包复制到已安装 Master Console 的 QRadar 主机。
3. 使用 SSH 以 root 用户身份登录已复制 Master Console 软件修订的 QRadar 主机。
4. 通过输入以下命令停止 Tomcat 服务：

   ```
   service tomcat stop
   ```

5. 在 QRadar 设备的控制台窗口中，输入以下命令来安装 Master Console：

   ```
   yum -y install masterconsole-<version#>.rpm
   ```

6. 通过输入以下命令重新启动 Tomcat 服务：

   ```
   service tomcat start
   ```

结果

Master Console 已安装，并且 QRadar 设备上的服务已重新启动。

打开 Master Console

安装 Master Console 后，使用 QRadar 控制台的 IP 地址打开 Master Console。

开始之前

请确保已使用 8500 激活密钥 (3L0C3S-2M0F3Q-6B1N0W-5N737F) 安装 QRadar。

关于此任务

第一次更新到 Master Console V0.8.1 或更高版本时，此更新过程会从 QRadar 控制台导入用户。导入时将覆盖所有现有 Master Console 用户（包括管理员）的密码，并将它们设置为在 QRadar 控制台上设置的密码。导入过程仅发生一次。以后更新 Master Console 时将不导入用户或覆盖密码。

过程

1. 打开 Web 浏览器并输入以下 URL：

   `https://IP_address`

   IP_address 是安装 Master Console 的 QRadar 主机的 IP 地址。
2. 登录 Master Console。

   如果您是首次登录 Master Console，请使用系统上的管理员帐户和 root 用户密码。

下一步做什么

要添加想监视的 QRadar 部署，请参阅『向 Master Console 添加部署』。

为 Master Console 创建授权令牌

必须创建授权令牌以使 Master Console 能够连接到 IBM Security QRadar 部署。

过程

1. 在**管理员**选项卡的**系统配置**下，单击**已授权服务**。
2. 单击**添加已授权服务**，然后配置参数。
   a. 在**服务名称**字段中，输入服务的名称。 名称长度可达 255 个字符。
   b. 在**用户角色**菜单中，选择**管理员**。

      分配给已授权服务的用户角色决定了此服务在 QRadar 中可访问的功能。Master Console 的授权令牌必须具有**管理员**用户角色。
   c. 在**安全概要文件**菜单中，选择**管理员**。

      安全概要文件决定了此服务在 QRadar 中可访问的网络和日志源。Master Console 的授权令牌必须具有**管理员**安全概要文件。
   d. 在**到期日期**字段中，选择要使令牌到期的日期，或单击**无期限**复选框。
3. 单击**创建服务**，然后记录令牌值。

向 Master Console 添加部署

Master Console 管理员必须添加要监视的 IBM Security QRadar 部署。

开始之前

- 您必须拥有授权令牌。有关更多信息，请参阅『为 Master Console 创建授权令牌』。

- 如果您的组织需要安全的 SSL，请确保在 Master Console 中所有要监视的 QRadar 部署上，将不可信 SSL 证书替换为自签名证书或可信证书。
- 仅 QRadar 管理员可以添加、编辑或除去对 Master Console 的 QRadar 部署。

过程

1. 要添加部署，请单击屏幕右上角的**添加**。
2. 输入部署名称。
3. 输入控制台 IP 地址或主机名。
4. 输入授权令牌。
5. 单击**添加部署**。
6. 如果要使用不安全的 SSL 添加部署，并且您的组织不需要安全的 SSL，请选中**忽略不安全的 SSL** 复选框，然后单击**添加部署**。

部署监视

Master Console 以图形方式表示每个连接到 Master Console 的 IBM Security QRadar 部署的运行状况和运行数据（被称为部署卡）。

您可以在"按严重性部署"页面上查看部署卡。为帮助您快速确定需要注意的部署，将部署卡分成三组：**临界**、**警告**和**良好**。

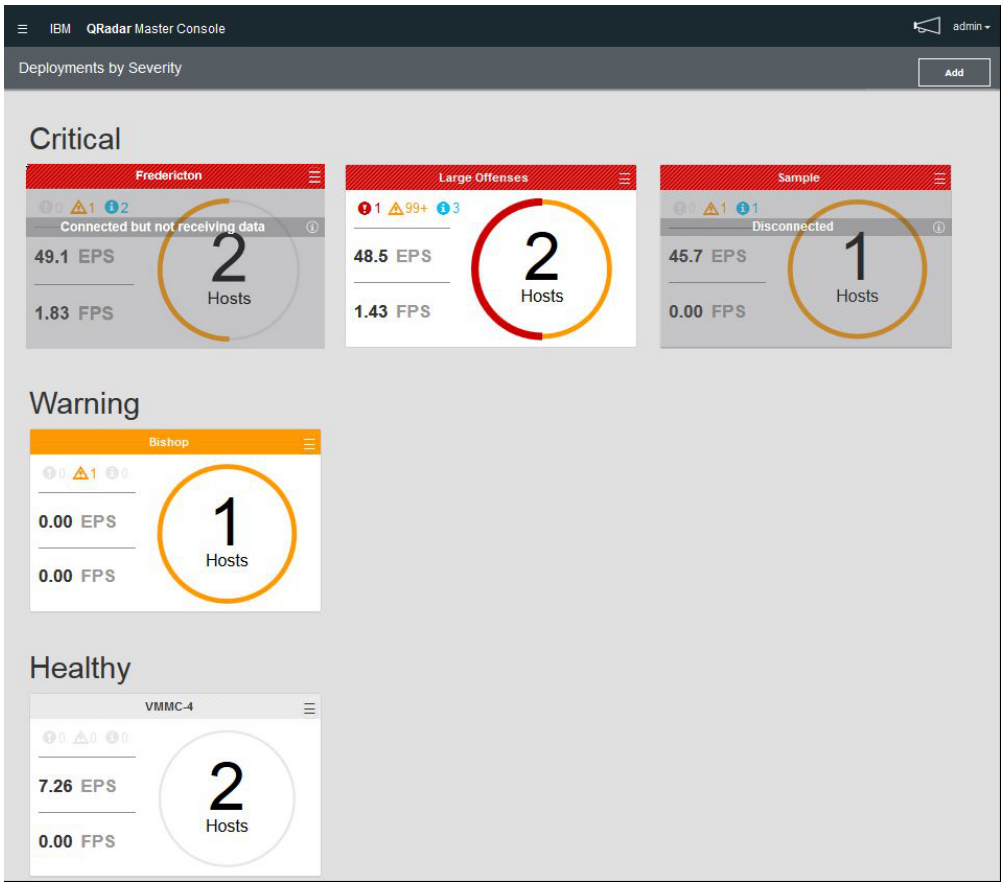

图 *1. Master Console* 中的部署卡

每个部署卡都显示以下信息：

- 部署中受管主机的数量。
- 部署状态，以圆圈的颜色表示。例如，如果部署有 2 个受管主机，且其中 1 个处于临界状态，那么圈住数字 2 的圆圈一半为红色。
- 过去 15 分钟内的临界、警告和参考系统通知的数量。
- 事件和流的速率，前 15 分钟测量的平均值。

Master Console 无法连接到部署时，此部署卡显示**已断开连接**。该状态意味着可能已关闭部署。部署显示为**已连接但未接收数据**时，授权令牌可能已撤销或已到期。

您可以在部署卡上执行以下操作：

- 单击部署卡以打开**受管主机**视图。
- 单击"汉堡包"() 图标，以编辑部署详细信息或断开部署与 Master Console 的连接。
- 部署显示**已断开连接**或**已连接但未接收数据**时，请单击部署卡上的信息图标，以查看上次接收数据的时间。

监视受管主机

使用"受管主机"页面来查看所有连接到单一部署的受管主机的系统通知、系统内存和 CPU 使用情况统计信息。

为帮助您快速确定需要注意的受管主机，在受管主机卡的顶部用颜色进行标示：红色指示**临界**状态，黄色指示**警告**状态，灰色指示**良好**状态。

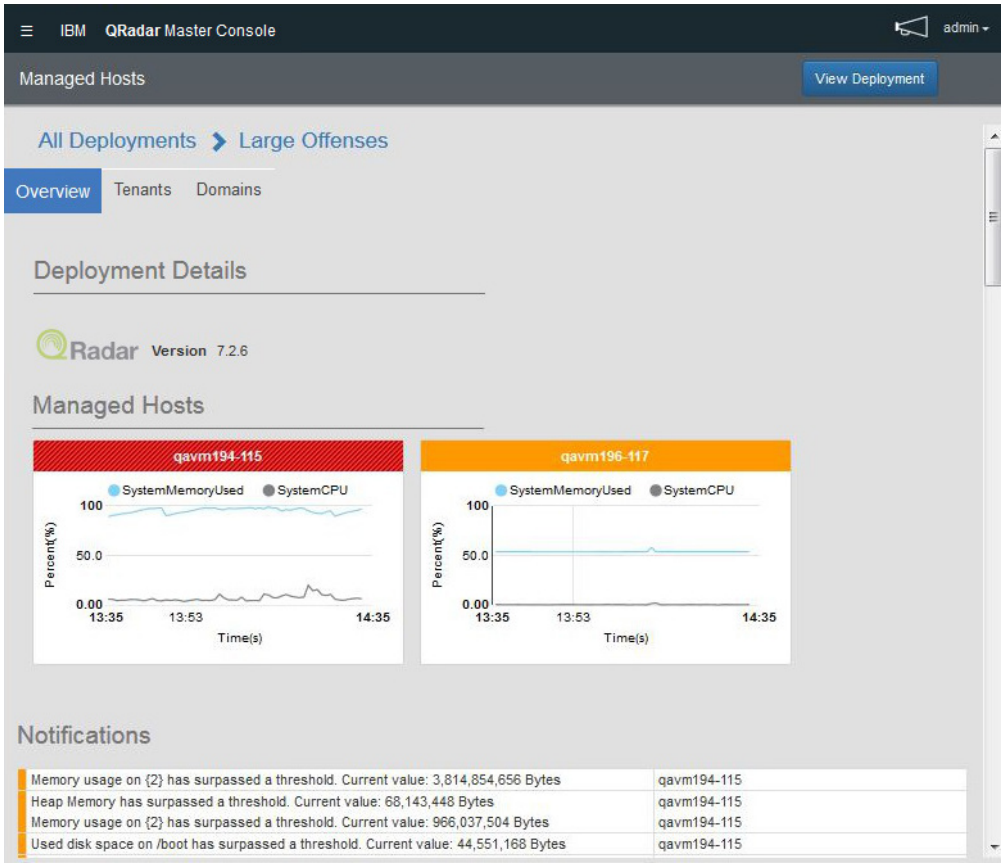

图 2. *Master Console* 中的"受管主机"页面

过程

1. 要查看"受管主机"页面，请单击"按严重性部署"页面上的部署卡。
2. 在"受管主机"页面上，可执行以下操作：
   a. 单击**查看部署**，以登录 QRadar 部署。
   b. 单击**租户**和**域**选项卡，以查看有关在部署中配置的租户和域的信息。
   c. 将鼠标悬停于受管主机图形上，以查看有关图形度量的更多信息。
   d. 要在受管主机图形上隐藏某个度量，请单击该度量的用颜色标示的图标。例如，要在图形上隐藏**系统 CPU** 度量，请单击**系统 CPU** 旁边的灰色圆圈。
   e. 要查看有关主机的运行数据（例如，CPU 和内存使用情况、网络和磁盘读写以及事件和流的速率），请单击受管主机卡。

监视攻击

使用 Master Console 从多个 IBM Security QRadar 部署中监视攻击。所有部署中的攻击都显示在单一列表中，其中最重要的攻击显示在顶部。

关于此任务

攻击卡按以下顺序排序：量级、部署和最近更新时间。

量级是攻击的相对重要性的指示符。量级根据相关性、严重性和可信性值计算。

- 相关性决定攻击对网络产生的影响。例如，端口打开时相关性就高。

- 可信性指示攻击的完整性，是由日志源中配置的可信性评级决定的。多个源报告同一事件会提高可信性。
- 严重性指示源造成的威胁，与目标如何准备应对攻击有关。

量级具有决定攻击卡颜色的数字值。将鼠标悬停于攻击卡上用颜色标示的条上，以查看量级编号。

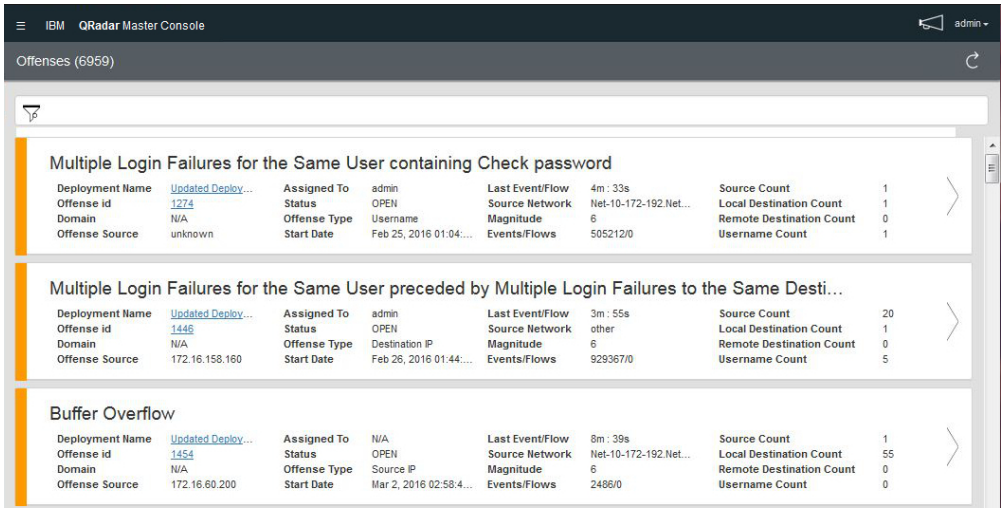

图 3. *Master Console* 中的部署卡

攻击卡显示以下信息：

表 3. 攻击卡信息

参数	描述
攻击标识	指向攻击摘要的链接。
攻击源	攻击源信息取决于攻击类型。 例如，如果**攻击类型**为源 IP，那么**攻击源**字段显示创建攻击的事件源的 IP 地址。如果**攻击类型**为目标 IP，那么**攻击源**字段显示事件的目标 IP 地址。
分配给	如果未分配用户对攻击进行调查，那么您可以将攻击分配给 QRadar 中的用户。有关将攻击分配给 QRadar 的更多信息，请参阅 *IBM Security QRadar Users Guide*。
状态	缺省情况下，过滤器只显示打开的攻击。
攻击类型	由创建攻击的规则决定。 例如，如果攻击类型为**日志源事件**，那么生成攻击的规则将使基于事件检测设备的事件互相关联。
开始日期	指定与攻击关联的第一个事件或流的日期和时间。
最后的事件/流	指定针对攻击、类别、源 IP 地址或目标 IP 地址观察最后的事件或流以来耗用的时间。
源网络	指定尝试破坏网络上组件安全的设备的网络。
事件/流	指定与源 IP 地址、目标 IP 地址、事件名称、用户名、MAC 地址、日志源、主机名、端口、日志源、ASN 地址、IPv6 地址、规则、ASN、应用程序、网络或类别关联的事件或流的数量。

表 3. 攻击卡信息 (续)

参数	描述
源计数	指定与该类别中的攻击关联的源 IP 地址的数量。如果源 IP 地址与五个不同的低级别类别中的攻击关联，那么只计算一次源 IP 地址。

过程

1. 单击左上角的"汉堡包"图标 ()，然后单击**攻击**。
2. 单击攻击卡上的箭头链接，以登录部署并打开攻击摘要。
3. 要查看隐藏或关闭的攻击，请单击过滤器  图标，然后选中要查看的攻击的复选框。

   与应用的过滤器相匹配的攻击的数量显示在页眉上。
4. 单击刷新图标以更新列出的攻击。

相关任务:

第 5 页的『打开 Master Console』
安装 Master Console 后，使用 QRadar 控制台的 IP 地址打开 Master Console。

过滤攻击列表

创建搜索查询来过滤合并的攻击列表中出现的攻击卡。例如，您可以过滤攻击列表，以仅显示分配给一个人的攻击，或仅显示针对单一部署的攻击。

关于此任务

使用**攻击**视图上的全文本搜索字段，能够快速找到关闭的或精确匹配的攻击，并以等级顺序显示。您可以创建查询以查找一个字、字的一部分、有特定顺序的多个字或有其他任何顺序的多个字。您可以在攻击卡上的所有数据字段中搜索数据，也可以通过指定要搜索的标识符来缩小搜索范围。

全文本搜索功能基于 Apache Lucene 搜索引擎。搜索不区分大小写。要使用单一字符通配符进行搜索，请使用 ? 符号。要使用多个字符通配符进行搜索，请使用 * 符号。

您可以通过指定要搜索攻击卡上的哪些字段来缩小搜索范围。下表显示了攻击卡上字段的字段标识：

表 4. 用于在攻击卡上搜索数据的字段标识

攻击卡描述	字段标识
攻击描述	description
部署名称	deployment_name
攻击标识	offense_id
域	domain_id
攻击源	offense_source
分配给	assigned_to
状态	status

表 4. 用于在攻击卡上搜索数据的字段标识 (续)

攻击卡描述	字段标识
攻击类型	offense_type 不能使用通配符搜索 offense_type。必须在查询中指定完全匹配文本。
开始日期	start_time
最后的事件/流	last_updated_time
源网络	source_network
量级	magnitude
事件/流	event_count flow_count
源计数	source_count
本地目标计数	local_destination_count
远程目标计数	remote_destination_count
用户名计数	username_count

过程

1. 单击左上角的"汉堡包"图标 ()，然后单击**攻击**。
2. 在搜索字段中，输入针对要搜索的文本的搜索查询。
   - 要搜索攻击卡上出现的任何数据，请在搜索框中输入该文本。
   - 要搜索特定字段中的数据，请输入字段标识，后跟冒号和要查询的术语。
   - 要转义特殊字符，请在搜索查询中以下特殊字符前加 \:

     `+ - && || ! ( ) { } [ ] ^ " ~ * ? : \`

   搜索查询示例:

   下表显示了可用于搜索攻击卡上数据的查询示例:

表 5. *Master Console* 搜索表达式

描述	搜索查询
搜索任何字段中有 text 或 test 的攻击。	te?t
搜索有 test、tests 或 tester 的攻击。	test*
搜索任何字段中有 password 的攻击。	*password*
搜索量级评级为 2、3 或 4 的攻击。	magnitude:[2 to 4]
搜索量级评级为 3 或 5 的攻击。	magnitude:(3 OR 5)
搜索攻击类型与 Event Name 相同的攻击。	offense_type: "Event Name"
搜索过去 10 天内更新的攻击。	last_update_time:[NOW-10DAYS to NOW]
搜索来自 Bishop 部署且量级为 3 的攻击。	deployment_name:Bishop AND magnitude:3

3. 要查看隐藏或关闭的攻击，请单击过滤器图标 ()，然后选中要查看的攻击的复选框。

与应用的过滤器相匹配的攻击的数量显示在页眉上。

用户管理

直接在 Master Console 中管理 Master Console 用户。

第一次更新到 Master Console V0.8.1 或更高版本时，此更新会从 QRadar 控制台导入用户。导入过程仅发生一次。以后更新 Master Console 时将不导入用户。初始导入后，直接从 Master Console 管理所有用户帐户。

添加本地用户

安装 Master Console 并更新到最新版本后，管理员可直接在 Master Console 中添加新用户。

过程

1. 单击左上角的"汉堡包"图标 ()，然后单击**设置**。
2. 单击**用户管理**。
3. 在"用户管理"窗口的右上角，单击**添加**以打开"添加用户"窗口。
4. 输入新用户的信息。
5. 如果新用户是管理员，请单击**安全管理员**复选框。
6. 单击**添加用户**。

编辑用户设置

更改设置，例如 Master Console 中本地用户的用户密码。

关于此任务

在 IBM Security QRadar 中更改的本地用户密码不会自动应用到 Master Console。必须编辑用户设置，并在 Master Console 中更改密码。

您不能在 Master Console 中更改 LDAP 和 Active Directory 密码。

过程

1. 单击左上角的"汉堡包"图标 ()，然后单击**设置**。
2. 单击**用户管理**。
3. 在要编辑的用户的卡上，单击"汉堡包"菜单  图标。
4. 选择**编辑用户**。
5. 在编辑用户窗口上修改用户信息。
6. 单击**编辑用户**以保存您的更改。

除去本地用户

如果用户不再需要访问，请从 Master Console 中除去本地用户。

过程

1. 单击左上角的"汉堡包"图标 ()，然后单击**设置**。
2. 单击**用户管理**，以查看所有本地用户的卡。
3. 在要编辑的用户的卡上，单击"汉堡包"菜单  图标。
4. 选择**除去用户**。
5. 在确认窗口中，单击**除去用户**。

过滤用户列表

创建搜索查询来过滤用户管理页面上显示的 Master Console 用户列表。例如，您可以过滤用户列表以仅显示处于活动状态的用户，或过滤用户列表以仅显示具有管理员安全概要文件的用户。

关于此任务

使用用户管理页面上的全文本搜索字段，能够快速找到关闭的或与搜索条件精确匹配的用户。全文本搜索功能基于 Apache Lucene 搜索引擎。要使用单一字符通配符进行搜索，请使用问号 (?)。要使用多个字符通配符进行搜索，请使用星号 (*)。您可以通过指定要搜索的用户字段来缩小搜索范围。

过程

1. 单击左上角的"汉堡包"图标 ()，然后单击**设置**。
2. 单击**用户管理**。
3. 在搜索字段中，输入针对要搜索的文本的搜索查询。
   - 要搜索自由格式文本，请在搜索框中输入该文本。在自由格式搜索中，必须使用完整词。不能使用词的一部分或通配符。
   - 要搜索特定字段中的数据，请输入后跟冒号的字段标识，然后输入要查询的术语。

   搜索查询示例：

   下表显示了可用于搜索用户数据的查询示例：

表 6. 用户数据搜索表达式

描述	搜索字符串
在**用户名**字段中搜索文本。	`name:John`
搜索唯一的登录名。该字段中的搜索区分大小写。	`login:Coop1`
搜索电子邮件地址。 您必须提供完整的电子邮件地址。不能通过电子邮件地址的一部分进行搜索。	`email:coop1@ca.ibm.com`
搜索系统上当前处于活动状态的用户。	`status:ACTIVE`
搜索所有具有管理特权的用户。	`role_name:admin`

表 6. 用户数据搜索表达式 (续)

描述	搜索字符串
搜索在过去 14 天内修改了概要文件的用户。	last_modified:[NOW-14DAYS TO NOW]

在 Master Console 中配置 Active Directory 和 LDAP 认证

第一次配置 Microsoft Active Directory 或 LDAP 认证服务提供者时，必须将区域划分信息添加到 /opt/qradar/masterconsole/conf/shiro.realms 文件中。

如果您最近升级到了 Master Console V0.10.0，那么必须手动从 shiro.ini 备份文件中将区域划分信息复制到 /opt/qradar/masterconsole/conf/shiro.realms 文件中。未来升级 Master Console 时将保留区域划分信息。

开始之前

请确保 shiro.ini.<timestamp> 备份文件存在于 /opt/qradar/masterconsole/conf/ 目录。如果不存在，请创建此备份文件。

请复查认证服务器上的配置。根据您配置的认证服务提供者的类型，可能需要提供以下参数值：

表 7. 认证参数描述

参数	描述
searchBase	在其中组织用户的 Active Directory 或 LDAP 目录的根目录。
searchFilter	用于查找 Active Directory 或 LDAP 用户的上下文。帐户是大多数服务器使用的缺省对象类，但是根据特定的 Active Directory 或 LDAP 服务器配置，此条目可能有所不同。
groupAttribute	标识 Active Directory 或 LDAP 用户所属的用户组。
groupRolesMap	Active Directory 或 LDAP 组到 Apache Shiro 角色的映射。
userDnTemplate	从 Active Directory 或 LDAP 服务器检索用户的 DN 模板。
contextFactory.url	Active Directory 或 LDAP 服务器 IP 地址和端口号。
principalSuffix	指定主体后缀，以简化用户必须指定的登录信息。 例如，用户可以创建名为 canada 的用户主体后缀，并输入 username@canada，而不需要输入 username@this.is.my.long.domain.name.in.canada.com。

过程

1. 将目录更改为 /opt/qradar/masterconsole/conf/。
2. 复制 shiro.realms 文件：

   ```
   cp shiro.realms.default shiro.realms
   ```

3. 打开 shiro.realms 文件。
4. 要配置 Microsoft Active Directory，请执行以下步骤：
   a. 查找以下部分并将示例值替换为适用于认证环境的值：

   ```
   # ----------------------------------------------------------------------------
   # following section is for configuring ActiveDirectory realm. Replace example
   # values before add to securityManager.realm
   ```

```
# ------------------------------------------------------------------------
adRealm = org.apache.shiro.realm.activedirectory.ActiveDirectoryRealm
adRealm.url = ldap://{ad_server}:389
adRealm.groupRolesMap = "CN=the_users,CN=Users,DC=department,DC=company,DC=com":"admin"
adRealm.searchBase = "DC=department,DC=company,DC=com"
adRealm.systemUsername= user_name
adRealm.systemPassword= password
adRealm.principalSuffix= @company.com
```

b. 将 $adRealm 添加到 securityManager.realms 条目：

```
securityManager.realms = $localRealm, $adRealm
```

5. 要配置 LDAP，请执行以下步骤：

a. 查找以下部分并将示例值替换为适用于认证环境的值：

```
#------------------------------------------------------------------------
# following section is for configuring OpenLdap realm. Replace example
# values before add to securityManager.realm
#------------------------------------------------------------------------
ldapRealm = com.ibm.si.mc.security.shiro.realm.LdapRealm
ldapRealm.searchBase = "dc=company,dc=com"
ldapRealm.searchFilter = (&(objectClass=account)(uid={0}))
ldapRealm.groupAttribute = ou
ldapRealm.groupRolesMap = "Manager":"admin"
ldapRealm.userDnTemplate = uid={0},dc=company,dc=com
ldapRealm.contextFactory.url = ldap://{ldap_server}:389
```

b. 将 $ldapRealm 添加到 securityManager.realms 条目：

```
securityManager.realms = $localRealm, $ldapRealm
```

6. 保存 /opt/qradar/masterconsole/conf/shiro.realms 文件。
7. 输入以下命令，将区域划分信息添加到 shiro.ini 文件：

```
/opt/qradar/masterconsole/bin/generateShiroIni.py
```

8. 使用以下命令重新启动 Tomcat 服务器：

```
service tomcat restart
```

下一步做什么

通过使用 Microsoft Active Directory 或 LDAP 认证登录到 Master Console，以对配置进行测试。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在所有国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或默示只能使用 IBM 产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档所述内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。 您可以用书面形式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

International Business Machines Corporation"按现状"提供本出版物，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关非侵权、适销和适用于某种特定用途的保证。 某些管辖区域在某些交易中不允许免除明示或默示的保证。 因此本条款可能不适用于您。

此信息可能包含技术上或印刷上的错误。 将对此信息进行定期的更改；这些更改将编入该出版物的新修订版中。 IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是此 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系：

© Copyright IBM Corp. 2015, 2016

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

引用的性能数据和客户示例仅用于演示目的。实际性能结果可能根据特定配置和运行条件的不同而不同。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息包含日常业务运作所使用的数据和报表的示例。 为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。 所有这些名字都是虚构的，若现实生活中的人物和业务企业与此相似，纯属巧合。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上的 "Copyright and trademark information"获取。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

产品文档的条款和条件

根据下列条款和条件授予对这些出版物的使用许可权。

适用性

这些条款和条件是对 IBM Web 站点的任何使用条款的补充。

个人使用

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 明确许可，您不得分发、显示这些出版物或其中部分出版物，也不得制作其演绎作品。

商业使用

您只能在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

权利

除非本许可权中明确授予，否则不得授予对这些出版物或其中包含的任何信息、数据、软件或其他知识产权的任何许可权、许可证或权利，无论明示的还是默示的。

当 IBM 认定本出版物的使用损害了其利益时，或确定上述指示信息未被正确遵守时，IBM 保留随时撤消此处授予的许可权的权利。

只有您完全遵循所有适用的法律和法规，包括所有的美国出口法律和法规，您才可以下载、出口或再出口该信息。

IBM 对这些出版物的内容不作任何保证。这些出版物"按现状"提供，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关适销性、非侵权和适用于某种特定用途的保证。

IBM 在线隐私声明

IBM 软件产品，包括软件即服务解决方案（"软件产品"），可使用 cookie 或其他技术收集产品使用信息、帮助改善最终用户体验、定制与最终用户的交互或用于其他用途。 在许多情况下，软件产品不收集个人可标识信息。 部分软件产品可帮助您收集个人可标识信息。 如果该软件产品使用 cookie 来收集个人可标识信息，那么有关该产品使用 cookie 的具体信息如下所述。

根据部署的配置，"软件产品" 可能使用会话 cookie 来收集每个用户的会话 ID，以用于会话管理和认证用途。 可以禁用 cookie，但是这也将删除 cookie 启用的功能。

如果为此软件产品部署的配置提供您以客户身份通过 cookie 或其他技术从最终用户收集个人可标识信息的功能，那么您应该查找关于适用于此类数据收集的所有法律的您自己的合法建议（包括声明和许可）。

有关使用各种技术（包括 cookie）来达到这些目的的更多信息，请参阅 IBM 隐私策略 (http://www.ibm.com/privacy) 和 IBM 在线隐私声明 (http://www.ibm.com/privacy/details) 中标题为"Cookies, Web Beacons and Other Technologies"的部分，以及"IBM Software Products and Software-as-a-Service Privacy Statement"(http://www.ibm.com/software/info/product-privacy)。

隐私策略注意事项

IBM 软件产品（包括软件即服务解决方案，以下简称为"软件产品"）可使用 cookie 或其他技术收集产品使用信息、帮助改善最终用户体验、定制与最终用户的交互或用于其他用途。 在许多情况下，软件产品不收集个人可标识信息。 部分软件产品可帮助您收集个人可标识信息。 如果该软件产品使用 cookie 来收集个人可标识信息，那么有关该产品使用 cookie 的具体信息如下所述。

根据部署的配置，"软件产品" 可能使用会话 cookie 来收集每个用户的会话 ID，以用于会话管理和认证用途。 可以禁用 cookie，但是这也将删除 cookie 启用的功能。

如果为此软件产品部署的配置提供您以客户身份通过 cookie 或其他技术从最终用户收集个人可标识信息的功能，那么您应该查找关于适用于此类数据收集的所有法律的您自己的合法建议（包括声明和许可）。

有关使用各种技术（包括 cookie）来达到这些目的的更多信息，请参阅 IBM 隐私策略 (http://www.ibm.com/privacy) 和 IBM 在线隐私声明 (http://www.ibm.com/privacy/details) 中标题为"Cookies, Web Beacons and Other Technologies"的部分，以及"IBM Software Products and Software-as-a-Service Privacy Statement"(http://www.ibm.com/software/info/product-privacy)。

Printed in China