安全策略设置

项目 • 2023/03/18

适用范围

- Windows 10
- Windows 11

此参考主题介绍安全设置的常见方案、体系结构和过程。

安全策略设置是管理员在计算机上或多台设备上配置的规则，用于保护设备或网络上的资源。 本地组策略编辑器管理单元的安全设置扩展允许将安全配置定义为组策略对象 (GPO) 的一部分。 GPO 链接到 Active Directory 容器（如站点、域或组织单位），它们使你能够管理多个设备的安全设置，这些设备从加入域的任何设备。 安全设置策略用作整体安全实现的一部分，以帮助保护组织中的域控制器、服务器、客户端和其他资源。

安全设置可以控制：

- 对网络或设备的用户身份验证。
- 允许用户访问的资源。
- 是否在事件日志中记录用户或组的操作。
- 组中的成员身份。

若要管理多个设备的安全配置，可以使用以下选项之一：

- 编辑 GPO 中的特定安全设置。
- 使用"安全模板"管理单元创建包含要应用的安全策略的安全模板，然后将安全模板导入到 组策略 对象中。 安全模板是表示安全配置的文件，它可以导入到 GPO、应用于本地设备或用于分析安全性。

有关管理安全配置的详细信息，请参阅 管理安全策略设置。

本地组策略编辑器的安全设置扩展包括以下类型的安全策略：

- **帐户策略。** 这些策略在设备上定义;它们会影响用户帐户与计算机或域的交互方式。帐户策略包括以下类型的策略：
  - **密码策略。** 这些策略确定密码的设置，例如强制实施和生存期。 密码策略用于域帐户。
  - **帐户锁定策略。** 这些策略确定帐户被锁定到系统的条件和时间长度。 帐户锁定策略用于域或本地用户帐户。
  - **Kerberos 策略。** 这些策略用于域用户帐户;它们确定与 Kerberos 相关的设置，例如票证生存期和强制实施。

- **本地策略。** 这些策略适用于计算机，并包括以下类型的策略设置：

- **审核策略。** 指定控制安全事件记录到计算机上的安全日志的安全设置，并指定要记录 (成功、失败或两者) 的安全事件类型。

  > ⓘ **备注**
  >
  > 对于运行 Windows 7 及更高版本的设备，我们建议使用“高级审核策略配置”下的设置，而不是“本地策略”下的“审核策略设置”。

- **用户权限分配。** 指定在设备上具有登录权限或特权的用户或组

- **安全选项。** 指定计算机的安全设置，例如管理员和来宾帐户名称;访问软盘驱动器和 CD-ROM 驱动器;安装驱动程序;登录提示;等等。

- **具有高级安全性的 Windows 防火墙。** 使用有状态防火墙指定设置来保护网络上的设备，该防火墙允许确定允许哪些网络流量在设备和网络之间传递。
- **网络列表管理器策略。** 指定可用于配置网络在一个设备或多个设备上列出和显示方式的不同方面的设置。
- **公钥策略。** 除了某些证书路径和服务设置外，还指定用于控制加密文件系统、数据保护和 BitLocker 驱动器加密的设置。
- **软件限制策略。** 指定设置以标识软件并控制其在本地设备、组织单位、域或站点上运行的能力。
- **应用程序控制策略。** 指定设置，以根据文件的唯一标识控制哪些用户或组可以在组织中运行特定应用程序。
- **本地计算机上的 IP 安全策略。** 指定设置，以确保使用加密安全服务通过 IP 网络进行专用安全通信。 IPsec 建立从源 IP 地址到目标 IP 地址的信任和安全性。
- **高级审核策略配置。** 指定用于控制将安全事件记录到设备上的安全日志的设置。“高级审核策略配置”下的设置可以更好地控制要监视的活动，而不是“本地策略”下的“审核策略”设置。

Windows 版本和许可要求

下表列出了支持Windows 安全中心策略设置和审核的 Windows 版本：

Windows 专业版	Windows 企业版	Windows 专业教育版/SE	Windows 教育版
是	是	是	是

Windows 安全中心策略设置和审核许可证权利由以下许可证授予：

Windows 专业版/专业教育版/SE	Windows 企业版 E3	Windows 企业版 E5	Windows 教育版 A3	Windows 教育版 A5
是	是	是	是	是

有关 Windows 许可的详细信息，请参阅 Windows 许可概述。

基于策略的安全设置管理

用于组策略的安全设置扩展提供基于策略的集成管理基础结构，以帮助你管理和强制实施安全策略。

可以通过组策略和Active Directory 域服务 (AD DS) 来定义安全设置策略并将其应用于用户、组、网络服务器和客户端。 可以 (Microsoft Web (IIS) 服务器) 创建具有相同功能的一组服务器，然后使用组策略对象将常见安全设置应用于组。 如果以后将更多服务器添加到此组，则会自动应用许多常见安全设置，从而减少部署和管理工作。

使用安全设置策略的常见方案

安全设置策略用于管理安全性的以下方面：帐户策略、本地策略、用户权限分配、注册表值、文件和注册表访问控制列表 (ACL) 、服务启动模式等。

作为安全策略的一部分，可以使用专门为组织中的各种角色配置的安全设置策略（例如域控制器、文件服务器、成员服务器、客户端等）创建 GPO。

可以创建组织单位 (OU) 结构，根据设备的角色对设备进行分组。 使用 OU 是分离网络中不同角色的特定安全要求的最佳方法。 此方法还允许将自定义安全模板应用于每个服务器或计算机类。 创建安全模板后，为每个 OU 创建新的 GPO，然后将安全模板 (.inf 文件) 导入新 GPO。

将安全模板导入 GPO 可确保应用 GPO 的任何帐户在刷新组策略设置时自动接收模板的安全设置。 在工作站或服务器上，安全设置定期刷新，（随机偏移量最多为 30 分钟）;在域控制器上，如果应用的任何 GPO 设置发生更改，则每隔几分钟就会发生一次此过程。 无论是否发生任何更改，设置也会每 16 小时刷新一次。

> **备注**
>
> 这些刷新设置因操作系统版本而异，并且可以配置。

通过将基于 组策略 的安全配置与委派管理结合使用，可以确保将特定安全设置、权限和行为应用于 OU 中的所有服务器和计算机。 此方法可以轻松地使用将来所需的任何其他更改来更新多个服务器。

与其他操作系统技术的依赖关系

对于属于 Windows Server 2008 或更高版本域成员的设备，安全设置策略依赖于以下技术：

- **Active Directory 域服务 (AD DS)**

  基于 Windows 的目录服务 AD DS 在网络上存储有关对象的信息，并使此信息可供管理员和用户使用。 通过使用 AD DS，可以从单个位置查看和管理网络上的网络对象，并且用户可以使用单一登录访问允许的网络资源。

- **组策略**

  AD DS 中的基础结构，用于在运行 Windows Server 的设备上启用基于目录的配置管理用户和计算机设置。 通过使用组策略，可以定义用户组和计算机组的配置，包括策略设置、基于注册表的策略、软件安装、脚本、文件夹重定向、远程安装服务、Internet Explorer 维护和安全性。

- **域名系统 (DNS)**

  用于在 Internet 和专用 TCP/IP 网络上查找域名的分层命名系统。 DNS 提供用于将 DNS 域名映射到 IP 地址和将 IP 地址映射到域名的服务。 此服务允许用户、计算机和应用程序查询 DNS，以通过完全限定的域名而不是 IP 地址指定远程系统。

- **Winlogon**

  Windows 操作系统的一部分，提供交互式登录支持。 Winlogon 是围绕交互式登录模型设计的，该模型由三个组件组成：Winlogon 可执行文件、凭据提供程序和任意数量的网络提供程序。

- **设置**

  在干净安装或从早期版本的 Windows Server 升级期间，安全配置与操作系统设置过程交互。

- **安全帐户管理器 (SAM)**

  登录过程中使用的 Windows 服务。 SAM 维护用户帐户信息，包括用户所属的组。

- **本地安全机构 (LSA)**

  一个受保护的子系统，用于对用户进行身份验证并将其登录到本地系统。 LSA 还维护有关系统上本地安全的各个方面的信息，统称为系统的本地安全策略。

- **Windows Management Instrumentation (WMI)**

WMI 是 Microsoft Windows 操作系统的一项功能，是 Microsoft 实现Web-Based企业管理 (WBEM) ，这是开发用于访问企业环境中管理信息的标准技术的行业举措。 WMI 提供对托管环境中对象相关信息的访问。 通过 WMI 和 WMI 应用程序编程接口 (API) ，应用程序可以在公共信息模型 (CIM) 存储库和由各种类型的提供程序维护的动态信息中查询和更改静态信息。

- **策略 (RSoP) 的结果集**

  增强的组策略基础结构，它使用 WMI，以便更轻松地规划和调试策略设置。 RSoP 提供公共方法，用于公开扩展组策略在假设情况下将执行的操作，以及扩展在实际情况中执行的操作。 这些公共方法允许管理员轻松确定适用于用户或设备的策略设置组合，或者将应用于用户或设备。

- **服务控制管理器 (SCM)**

  用于配置服务启动模式和安全性。

- **注册表**

  用于配置注册表值和安全性。

- **文件系统**

  用于配置安全性。

- **文件系统转换**

  当管理员将文件系统从 FAT 转换为 NTFS 时，将设置安全性。

- **Microsoft 管理控制台 (MMC)**

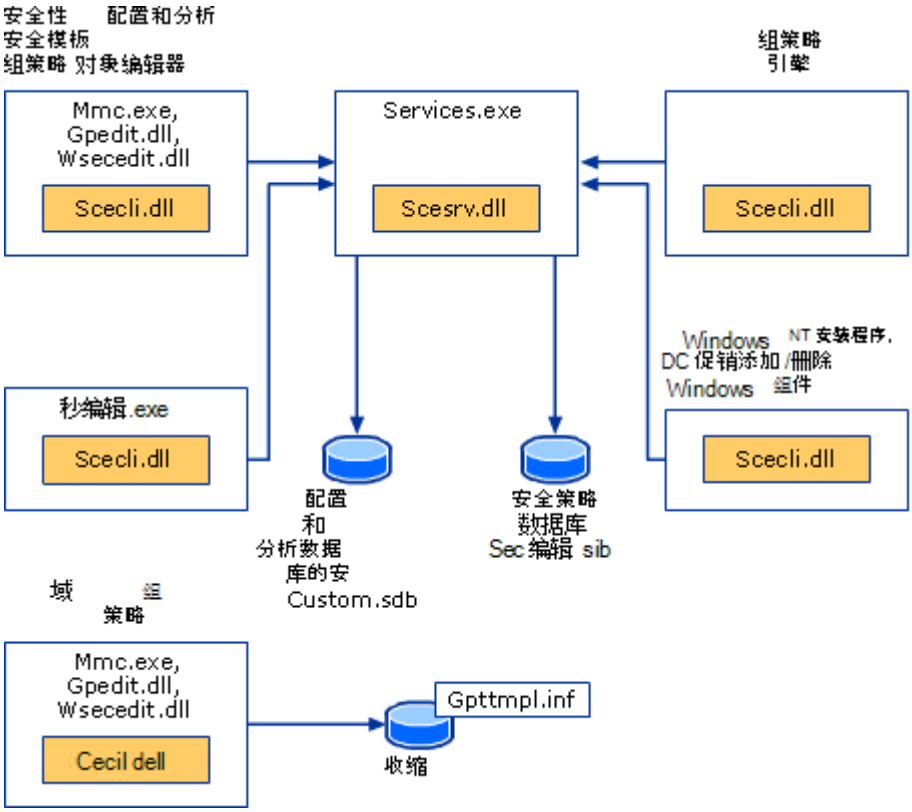
  安全设置工具的用户界面是本地组策略编辑器 MMC 管理单元的扩展。

安全设置策略和组策略

本地组策略编辑器的安全设置扩展是安全Configuration Manager工具集的一部分。 以下组件与安全设置相关联：配置引擎;分析引擎;模板和数据库接口层;设置集成逻辑;和 secedit.exe 命令行工具。 安全配置引擎负责处理运行该引擎的系统的安全配置编辑器相关安全请求。 分析引擎分析给定配置的系统安全性并保存结果。 模板和数据库接口层处理内部存储) 从模板或数据库 (读取和写入请求。 本地组策略编辑器的安全设置扩展处理来自基于域或本地设备的组策略。 安全配置逻辑与安装程序集成并管理系统安全性，以便干净安装或升级到更新的 Windows 操作系统。 安全信息存储在模板 (.inf 文件) 或 Secedit.sdb 数据库中。

下图显示了安全设置和相关功能。

安全设置策略和相关功能



- **Scesrv.dll**

  提供核心安全引擎功能。

- **Scecli.dll**

  提供安全配置引擎的客户端接口，并向 RSoP) (策略的结果集提供数据。

- **Wsecedit.dll**

  本地组策略编辑器的安全设置扩展。 scecli.dll加载到 wsecedit.dll 以支持安全设置用户界面。

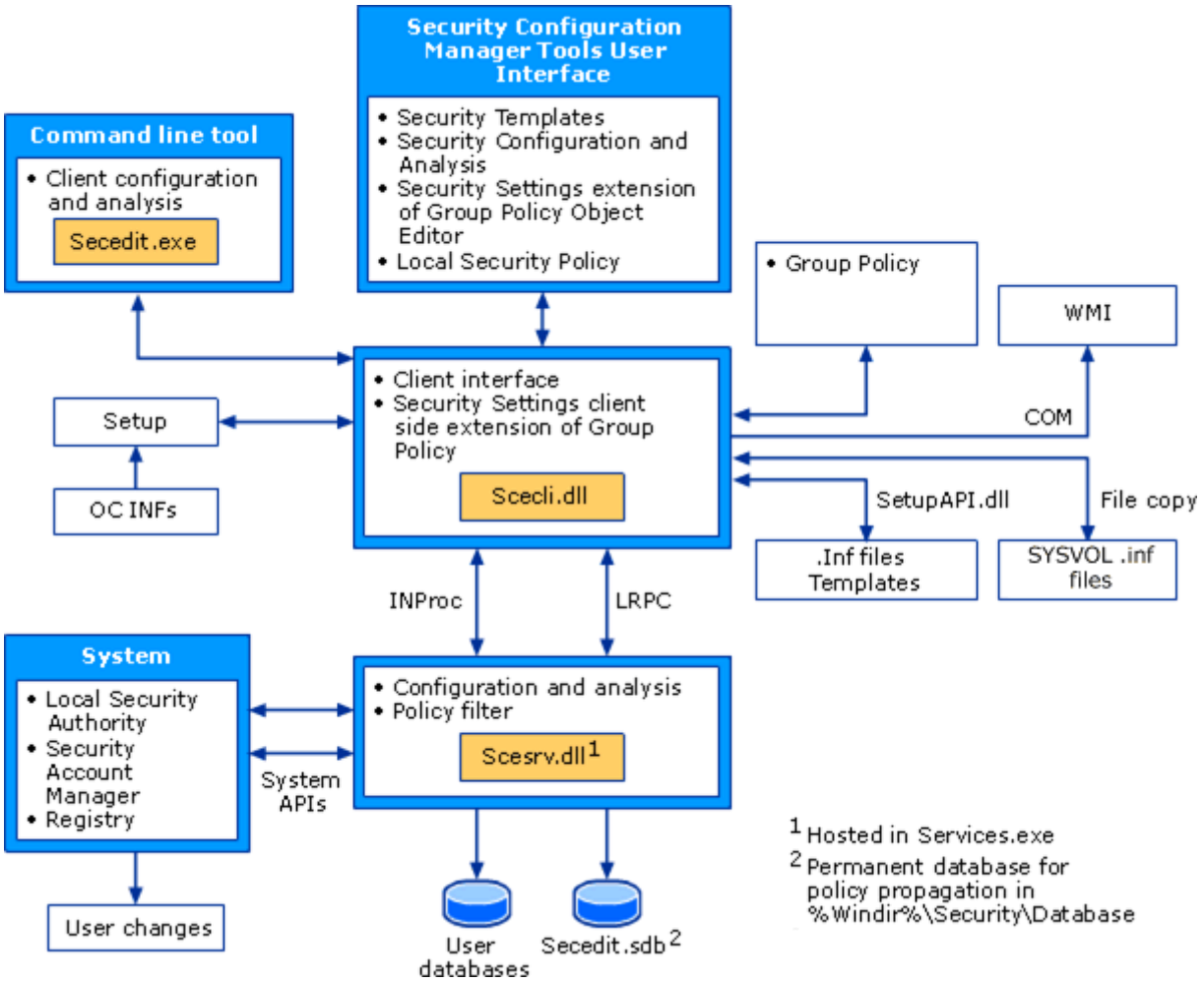
- **Gpedit.dll**

  本地组策略编辑器 MMC 管理单元。

安全设置扩展体系结构

本地组策略编辑器的安全设置扩展是安全Configuration Manager工具的一部分，如下图所示。

安全设置体系结构



安全设置配置和分析工具包括安全配置引擎，该引擎提供本地计算机 (非域成员) 以及基于组策略的安全设置策略配置和分析。 安全配置引擎还支持创建安全策略文件。 安全配置引擎的主要功能是scecli.dll和scesrv.dll。

以下列表介绍了安全配置引擎的这些主要功能以及其他安全设置相关功能。

- **scesrv.dll**

  此.dll文件托管在 services.exe 中，并在本地系统上下文中运行。 scesrv.dll提供核心安全Configuration Manager功能，例如导入、配置、分析和策略传播。

  Scesrv.dll通过调用相应的系统 API（包括 LSA、SAM 和注册表）来执行各种与安全相关的系统参数的配置和分析。

  Scesrv.dll公开导入、导出、配置和分析等 API。 它会检查请求是否通过 LRPC (Windows XP) 发出，如果不是，则调用失败。

  使用以下方法在部分安全设置扩展之间进行通信：
  - 组件对象模型 (COM) 调用
  - 本地远程过程调用 (LRPC)
  - 轻型目录访问协议 (LDAP)
  - Active Directory 服务接口 (ADSI)
  - 服务器消息块 (SMB)

- Win32 API
- Windows Management Instrumentation (WMI) 调用

在域控制器上，scesrv.dll接收对 SAM 和 LSA 所做的更改的通知，这些更改需要跨域控制器同步。 Scesrv.dll使用进程内scecli.dll模板修改 API 将这些更改合并到默认域控制器策略 GPO 中。 Scesrv.dll还会执行配置和分析操作。

- **Scecli.dll**

  此Scecli.dll是用于scesrv.dll的客户端接口或包装器。 scecli.dll加载到 Wsecedit.dll 以支持 MMC 管理单元。安装程序使用它来配置安装程序 API .inf 文件安装的文件、注册表项和服务的默认系统安全性和安全性。

  安全配置和分析用户界面的命令行版本secedit.exe使用scecli.dll。

  Scecli.dll实现组策略的客户端扩展。

  Scesrv.dll使用scecli.dll从 SYSVOL 下载适用的组策略文件，以便将组策略安全设置应用到本地设备。

  Scecli.dll将安全策略的应用程序记录到 WMI (RSoP) 。

  Scesrv.dll策略筛选器在对 SAM 和 LSA 进行更改时使用scecli.dll来更新默认域控制器策略 GPO。

- **Wsecedit.dll**

  组策略对象编辑器管理单元的安全设置扩展。 可以使用此工具在站点、域或组织单位的 组策略 对象中配置安全设置。 还可以使用安全设置将安全模板导入 GPO。

- **Secedit.sdb**

  此 Secedit.sdb 是用于策略传播的永久系统数据库，包括用于回滚的持久设置表。

- **用户数据库**

  用户数据库是管理员为配置或分析安全性而创建的系统数据库以外的任何数据库。

- **.Inf 模板**

  这些模板是包含声明性安全设置的文本文件。 在配置或分析之前，它们将加载到数据库中。 组策略安全策略存储在域控制器的 SYSVOL 文件夹中的 .inf 文件中，这些策略 (使用文件复制) 下载，并在策略传播期间合并到系统数据库中。

安全设置策略流程和交互

对于管理组策略的已加入域的设备，安全设置将与组策略一起处理。 并非所有设置都是可配置的。

组策略处理

当计算机启动且用户登录时，将按以下顺序应用计算机策略和用户策略：

1. 网络启动。 远程过程调用系统服务 (RPCSS) 和多个通用命名约定提供程序 (MUP) 启动。

2. 为设备获取组策略对象的有序列表。 该列表可能取决于以下因素：

    - 设备是否是域的一部分，因此，取决于通过 Active Directory 组策略。
    - 设备在 Active Directory 中的位置。
    - 组策略 对象的列表是否已更改。 如果组策略对象列表未更改，则不执行任何处理。

3. 应用计算机策略。 这些设置位于已收集列表中的“计算机配置”下。 此过程默认为同步过程，按以下顺序进行：本地、站点、域、组织单位、子组织单位等。 处理计算机策略时不显示任何用户界面。

4. 启动脚本运行。 默认情况下，这些脚本是隐藏和同步的;每个脚本必须在下一个脚本开始之前完成或超时。 默认超时为 600 秒。 可以使用多个策略设置来修改此行为。

5. 用户按 Ctrl+Alt+DEL 登录。

6. 验证用户后，将加载用户配置文件;它受有效的策略设置控制。

7. 为用户获取组策略对象的有序列表。 该列表可能取决于以下因素：

    - 用户是否是域的一部分，因此，取决于通过 Active Directory 组策略。
    - 是否启用了环回策略处理，如果是，则状态 (环回策略设置的“合并”或“替换”)。
    - 用户在 Active Directory 中的位置。
    - 组策略 对象的列表是否已更改。 如果组策略对象列表未更改，则不执行任何处理。

8. 应用用户策略。 这些设置是收集列表中的“用户配置”下的设置。 默认情况下，这些设置是同步的，按以下顺序进行：本地、站点、域、组织单位、子组织单位等。 处理用户策略时，不显示任何用户界面。

9. 登录脚本运行。 默认情况下，基于 组策略 的登录脚本是隐藏和异步的。 用户对象脚本最后运行。

10. 将显示由组策略规定的操作系统用户界面。

组策略对象存储

组策略 对象 (GPO) 是由全局唯一标识符 (GUID) 标识的虚拟对象，存储在域级别。 GPO 的策略设置信息存储在以下两个位置：

- **组策略 Active Directory 中的容器。**

  组策略容器是包含 GPO 属性的 Active Directory 容器，例如版本信息、GPO 状态以及其他组件设置列表。

- **(SYSVOL) 域的系统卷文件夹中组策略模板。**

  组策略模板是一个文件系统文件夹，其中包含由 .admx 文件指定的策略数据、安全设置、脚本文件和有关可供安装的应用程序的信息。 组策略模板位于域>\策略子文件夹中的 <SYSVOL 文件夹中。

GROUP_POLICY_OBJECT结构提供有关 GPO 列表中 GPO 的信息，包括 GPO 的版本号、指向指示 GPO Active Directory 部分的字符串的指针，以及指向指定 GPO 文件系统部分路径的字符串的指针。

组策略处理顺序

组策略设置按以下顺序进行处理：

1. **本地组策略对象。**

   运行从 Windows XP 开始的 Windows 操作系统的每个设备都有一个本地存储组策略对象。

2. **网站。**

   接下来将处理已链接到站点的任何组策略对象。 处理是同步的，按指定的顺序进行。

3. **域。**

   多个域链接组策略对象的处理是同步的，按指定的顺序处理。

4. **组织单位。**

   组策略首先处理链接到 Active Directory 层次结构中最高的组织单位的对象，然后组策略链接到其子组织单位的对象，依此类说。 最后，将处理链接到包含用户或设备的组织单位的组策略对象。

在 Active Directory 层次结构中的每个组织单位级别，可以链接一个、多个或任何组策略对象。 如果多个组策略对象链接到一个组织单位，则它们的处理是同步的，并且按指定的顺序进行。

此顺序意味着首先处理本地组策略对象，最后处理组策略链接到计算机或用户是直接成员的组织单位的对象，这将覆盖以前的组策略对象。

此顺序是默认处理顺序，管理员可以指定此订单的例外。 链接到站点、域或组织单位 (非本地组策略对象) 的组策略对象可针对该网站、域或组织单位设置为“**强制实施**”，以便无法重写其策略设置。 在任何站点、域或组织单位，都可以有选择地将组策略继承标记为“**块继承**”。 组策略始终应用设置为“**强制实施**”的对象链接，但无法阻止它们。 有关详细信息，请参阅组策略基础知识 - 第 2 部分：了解要应用哪些 GPO。

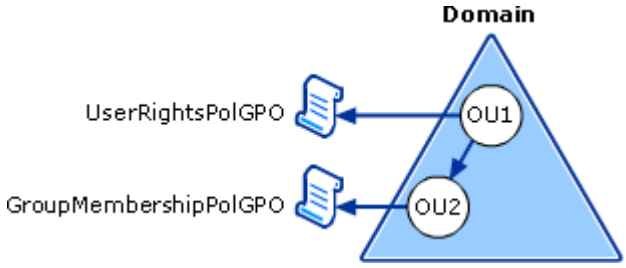
安全设置策略处理

在组策略处理的上下文中，安全设置策略按以下顺序进行处理。

1. 在组策略处理期间，组策略引擎确定要应用哪些安全设置策略。
2. 如果 GPO 中存在安全设置策略，组策略将调用安全设置客户端扩展。
3. 安全设置扩展从适当的位置（例如特定域控制器）下载策略。
4. 安全设置扩展根据优先规则合并所有安全设置策略。 处理根据本地、站点、域和组织单位 (OU) 组策略处理顺序，如前面“组策略处理顺序”部分所述。 如果多个 GPO 对给定设备有效，并且没有冲突的策略，则策略是累积的并合并的。

   此示例使用下图所示的 Active Directory 结构。 给定的计算机是 **GROUPMembershipPolGPO** GPO 链接到的 OU2 的成员。 此计算机还受 **UserRightsPolGPO** GPO 的约束，该 GPO 链接到层次结构中较高级别的 OU1。 在这种情况下，不存在任何冲突的策略，因此设备接收 **UserRightsPolGPO** 和 **GroupMembershipPolGPO** GPO 中包含的所有策略。

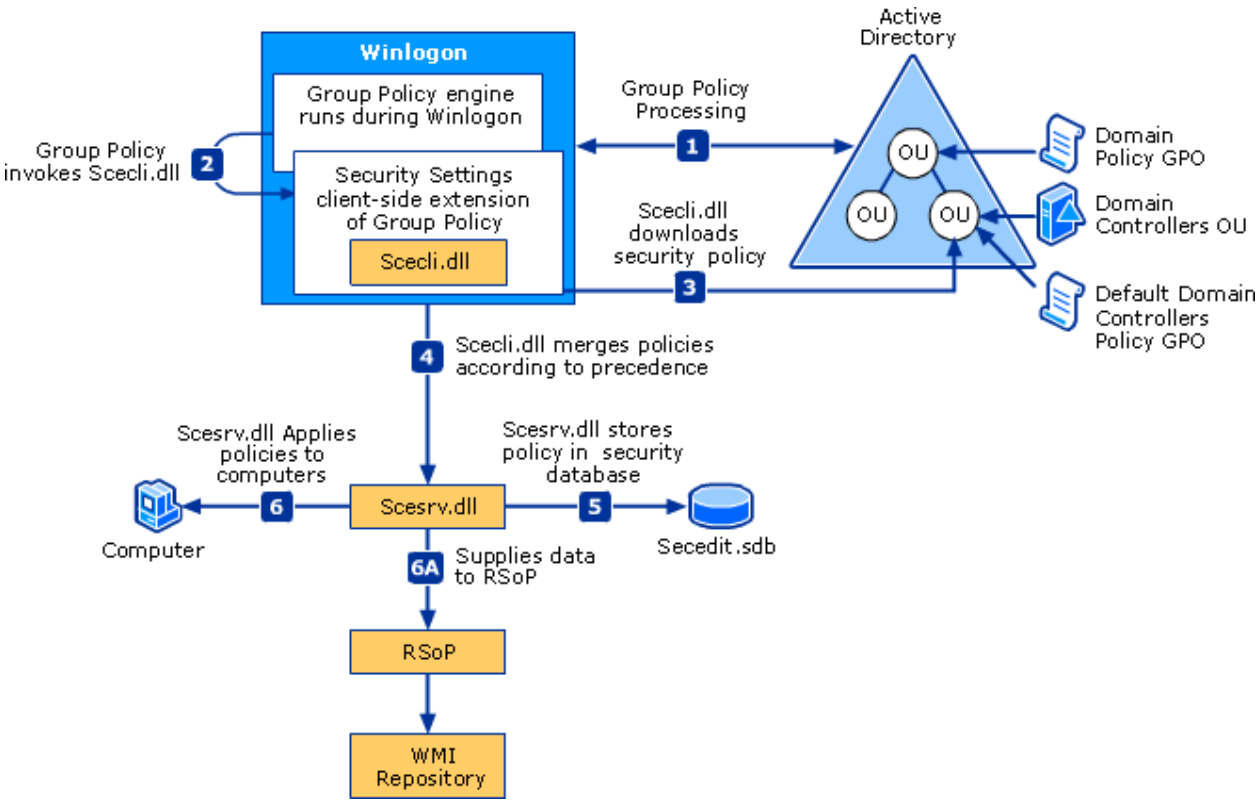
   多个 GPO 和安全策略的合并

5. 生成的安全策略存储在安全设置数据库 secedit.sdb 中。 安全引擎获取安全模板文件并将其导入到 secedit.sdb。

6. 安全设置策略将应用于设备。 下图演示了安全设置策略处理。

安全设置策略处理



在域控制器上合并安全策略

密码策略、Kerberos 和某些安全选项仅从域的根级别链接的 GPO 合并。 进行此合并是为了使这些设置在域中的所有域控制器之间保持同步。 合并了以下安全选项：

- 网络安全：在登录时间过期时强制注销
- 帐户: 管理员帐户状态
- 帐户: 来宾帐户状态
- 帐户: 重命名系统管理员帐户
- 帐户: 重命名来宾帐户

存在另一种机制，允许管理员使用净帐户进行的安全策略更改合并到默认域策略 GPO 中。 使用本地安全机构 (LSA) API 进行的用户权限更改将筛选到默认域控制器策略 GPO 中。

域控制器的特殊注意事项

如果应用程序安装在主域控制器上， (PDC) 操作主角色 (也称为灵活的单主操作或 FSMO) 并且应用程序对用户权限或密码策略进行了更改，则必须传达这些更改以确保跨域控制器进行同步。 Scesrv.dll会收到一条通知，指示安全帐户管理器 (SAM) 和 LSA 发生任何更

改，这些更改需要跨域控制器同步，然后使用scecli.dll模板修改 API 将更改合并到默认域控制器策略 GPO 中。

应用安全设置时

编辑安全设置策略后，在以下实例中链接到 组策略 对象的组织单位中的计算机上刷新设置：

- 重启设备时。
- 工作站或服务器上每 90 分钟一次，域控制器上每 5 分钟一次。 此刷新间隔是可配置的。
- 默认情况下，组策略传递的安全策略设置也每 16 小时 (960 分钟) 应用一次，即使 GPO 未更改也是如此。

安全设置策略的持久性

即使最初应用安全设置的策略中不再定义某个设置，安全设置也可以保留。

在以下情况下，安全设置可能会保留：

- 以前尚未为设备定义设置。
- 设置适用于注册表安全对象。
- 这些设置适用于文件系统安全对象。

通过本地策略或通过 组策略 对象应用的所有设置都存储在计算机上的本地数据库中。 每当修改安全设置时，计算机都会将安全设置值保存到本地数据库，该数据库保留已应用于计算机的所有设置的历史记录。 如果策略首先定义安全设置，然后不再定义该设置，则该设置将采用数据库中的上一个值。 如果数据库中不存在上一个值，则该设置不会还原为任何内容，并且仍按原样定义。 此行为有时称为“纹身”。

注册表和文件安全设置将保留通过 组策略 应用的值，直到该设置设置为其他值。

应用策略所需的权限

“应用组策略”和“读取”权限都需要将组策略对象的设置应用于用户或组和计算机。

筛选安全策略

默认情况下，所有 GPO 都具有“读取”和“应用”组策略“经过身份验证的用户组均允许”。 “经过身份验证的用户组”包括用户和计算机。 安全设置策略基于计算机。 若要指定哪些客户端计算机将或不会应用组策略 Object，可以拒绝它们对该组策略对象的“应用组策略”

或"读取"权限。 通过更改这些权限，可将 GPO 的范围限制为站点、域或 OU 中的一组特定计算机。

> **备注**
>
> 不要在域控制器上使用安全策略筛选，因为这会阻止向其应用安全策略。

迁移包含安全设置的 GPO

在某些情况下，你可能希望将 GPO 从一个域环境迁移到另一个环境。 两种最常见的方案是测试到生产迁移和生产到生产迁移。 GPO 复制过程对某些类型的安全设置有影响。

单个 GPO 的数据存储在多个位置和各种格式中;某些数据包含在 Active Directory 中，其他数据存储在域控制器上的 SYSVOL 共享上。 某些策略数据可能在一个域中有效，但在要向其复制 GPO 的域中可能无效。 例如，存储在安全策略设置中的安全标识符 (SID) 通常是特定于域的。 因此，复制 GPO 并不像获取文件夹并将其从一台设备复制到另一台设备那么简单。

以下安全策略可以包含安全主体，并且可能需要更多工作才能成功将它们从一个域移动到另一个域。

- 用户权限分配
- 受限组
- 服务
- 文件系统
- 注册表
- GPO DACL（如果选择在复制操作期间保留它）

若要确保正确复制数据，可以使用 组策略 管理控制台 (GPMC)。 当 GPO 从一个域迁移到另一个域时，GPMC 可确保正确复制所有相关数据。 GPMC 还提供迁移表，这些表可用于在迁移过程中将特定于域的数据更新为新值。 GPMC 隐藏了迁移 GPO 操作所涉及的大部分复杂性，并且它为执行 GPO 复制和备份等操作提供了简单可靠的机制。

本部分内容

主题	描述
管理安全策略设置	本文讨论在本地设备或整个中小型组织中管理安全策略设置的不同方法。
配置安全策略设置	介绍在本地设备、已加入域的设备和域控制器上配置安全策略设置的步骤。

主题	描述
安全策略设置参考	此安全设置参考提供了有关如何实现和管理安全策略的信息，包括设置选项和安全注意事项。

管理安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文讨论在本地设备或整个中小型组织中管理安全策略设置的不同方法。

安全策略设置应用作整体安全实现的一部分，以帮助保护组织中的域控制器、服务器、客户端设备和其他资源。

安全设置策略是在设备或多台设备上配置的规则，用于保护设备或网络上的资源。 本地组策略编辑器管理单元 (Gpedit.msc) 的安全设置扩展允许将安全配置定义为组策略对象 (GPO) 的一部分。 GPO 链接到 Active Directory 容器（如站点、域和组织单位），使管理员能够管理从加入域的任何设备中的多台计算机的安全设置。

安全设置可以控制：

- 对网络或设备的用户身份验证。
- 允许用户访问的资源。
- 是否在事件日志中记录用户或组的操作。
- 组中的成员身份。

有关每个设置的信息（包括说明、默认设置以及管理和安全注意事项），请参阅 安全策略设置参考。

若要管理多台计算机的安全配置，可以使用以下选项之一：

- 编辑 GPO 中的特定安全设置。
- 使用“安全模板”管理单元创建包含要应用的安全策略的安全模板，然后将安全模板导入到 组策略 对象中。 安全模板是一个表示安全配置的文件，它可以导入到 GPO，或应用于本地设备，或者可用于分析安全性。

设置管理方式的更改

随着时间的推移，引入了管理安全策略设置的新方法，其中包括新的操作系统功能和添加新设置。 下表列出了管理安全策略设置的不同方法。

工具或功能	说明和使用

工具或功能	说明和使用
安全策略管理单元	Secpol.msc MMC 管理单元设计为仅管理安全策略设置。
安全编辑器命令行工具	Secedit.exe 通过将当前配置与指定的安全模板进行比较来配置和分析系统安全性。
安全合规性管理器	工具下载 一个解决方案加速器，可帮助你规划、部署、操作和管理 Windows 客户端和服务器操作系统以及 Microsoft 应用程序的安全基线。
安全配置向导	Scw.exe SCW 是基于角色的工具，仅在服务器上可用：可以使用它创建一个策略，使所选服务器执行特定角色所需的服务、防火墙规则和设置。
安全 Configuration Manager工具	此工具集允许你为本地设备、组织单位或域创建、应用和编辑安全性。
组策略	Gpmc.msc 和 Gpedit.msc 组策略管理控制台使用 组策略 对象编辑器来公开本地安全选项，这些选项随后可以合并到 组策略 对象中，以便在整个域中分发。 本地组策略编辑器在本地设备上执行类似的功能。
软件限制策略 请参阅 管理软件限制策略	Gpedit.msc 软件限制策略 (SRP) 是一项基于组策略的功能，用于标识在域中的计算机上运行的软件程序，并控制这些程序运行的能力。
管理 AppLocker 请参阅 管理 AppLocker	Gpedit.msc 防止恶意软件 (恶意软件) 和不支持的应用程序影响环境中的计算机，并防止组织中的用户安装和使用未经授权的应用程序。

使用本地安全策略管理单元

本地安全策略管理单元 (Secpol.msc) 将本地策略对象的视图限制为以下策略和功能：

- 帐户策略
- 本地策略
- 高级安全 Windows 防火墙
- 网络列表管理器策略
- 公钥策略
- 软件限制策略
- 应用程序控制策略
- 本地计算机上的 IP 安全策略
- 高级审核策略配置

如果计算机已加入域，则可能会覆盖本地设置的策略。

本地安全策略管理单元是安全Configuration Manager工具集的一部分。 有关此工具集中的其他工具的信息，请参阅本主题中的使用安全Configuration Manager。

使用 secedit 命令行工具

secedit 命令行工具适用于安全模板，并提供六个主要功能：

- **Configure** 参数通过向错误服务器应用正确的安全模板来帮助解决设备之间的安全差异。
- **Analyze** 参数将服务器的安全配置与所选模板进行比较。
- **Import** 参数允许从现有模板创建数据库。 安全配置和分析工具也进行此克隆。
- **Export** 参数允许将设置从数据库导出到安全设置模板中。
- **通过 Validate** 参数，可以验证创建或添加到安全模板的每一行或任何文本行的语法。 此验证可确保如果模板无法应用语法，则模板不会出现问题。
- **Generate Rollback** 参数将服务器的当前安全设置保存到安全模板中，以便可用于将服务器的大部分安全设置还原到已知状态。 例外情况是，应用后，回滚模板不会更改最近应用的模板更改的文件或注册表项的访问控制列表条目。

使用安全合规性管理器

安全合规性管理器是一种可下载的工具，可帮助你规划、部署、操作和管理 Windows 客户端和服务器操作系统以及 Microsoft 应用程序的安全基线。 它包含一个完整的数据库，其中包含建议的安全设置、自定义基线的方法，以及以多种格式实现这些设置的选项，包括 XLS、GPO、Desired Configuration Management (DCM) 包或安全内容自动化协议 (SCAP) 。 安全合规性管理器用于将基线导出到环境，以自动执行安全基线部署和合规性验证过程。

使用安全合规性管理器管理安全策略

1. 下载最新版本。 可以在 Microsoft 安全基线 博客中找到详细信息。
2. 阅读此工具中包含的相关安全基线文档。
3. 下载并导入相关的安全基线。 安装过程逐步完成基线选择。
4. 在部署这些基线之前，打开“帮助”并按照如何自定义、比较或合并安全基线的说明进行操作。

使用安全配置向导

安全配置向导 (SCW) 指导你完成创建、编辑、应用或回滚安全策略的过程。 使用 SCW 创建的安全策略是一个.xml文件，应用后，该文件将配置服务、网络安全、特定注册表值

和审核策略。 SCW 是基于角色的工具：可以使用它创建策略，使所选服务器执行特定角色所需的服务、防火墙规则和设置。 例如，服务器可能是文件服务器、打印服务器或域控制器。

下面是使用 SCW 时的注意事项：

- SCW 禁用不必要的服务，并为 Windows 防火墙提供高级安全支持。
- 使用 SCW 创建的安全策略与安全模板不同，后者是扩展名为 .inf 的文件。 安全模板包含的安全设置比可以使用 SCW 设置更多的设置。 但是，可以在 SCW 安全策略文件中包括安全模板。
- 可以使用 组策略 部署使用 SCW 创建的安全策略。
- SCW 不会安装或卸载服务器执行角色所需的功能。 可以通过 服务器管理器 安装特定于服务器角色的功能。
- SCW 检测服务器角色依赖项。 如果选择服务器角色，则会自动选择依赖服务器角色。
- 运行 SCW 时，所有使用 IP 协议和端口的应用都必须在服务器上运行。
- 在某些情况下，必须连接到 Internet 才能使用 SCW 帮助中的链接。

> **备注**
>
> SCW 仅在 Windows Server 上可用，并且仅适用于服务器安装。

可以通过服务器管理器或运行scw.exe来访问 SCW。 向导将引导你完成服务器安全配置，以便：

- 创建可应用于网络上任何服务器的安全策略。
- 编辑现有安全策略。
- 应用现有安全策略。
- 回滚上次应用的安全策略。

安全策略向导根据服务器的角色配置服务和网络安全，并配置审核和注册表设置。

有关 SCW 的详细信息（包括过程），请参阅 安全配置向导。

使用安全Configuration Manager

使用安全Configuration Manager工具集，可以创建、应用和编辑本地设备、组织单位或域的安全性。

有关如何使用安全Configuration Manager的过程，请参阅安全Configuration Manager。

下表列出了安全Configuration Manager的功能。

安全Configuration Manager 工具	描述
安全配置和分析	在模板中定义安全策略。 这些模板可以应用于组策略或本地计算机。
安全模板	在模板中定义安全策略。 这些模板可以应用于组策略或本地计算机。
组策略的安全设置扩展	编辑域、站点或组织单位上的单个安全设置。
本地安全策略	编辑本地计算机上的单个安全设置。
Secedit	在命令提示符下自动执行安全配置任务。

安全配置和分析

安全配置和分析是一个 MMC 管理单元，用于分析和配置本地系统安全性。

安全分析

设备上的操作系统和应用的状态是动态的。 例如，可能需要暂时更改安全级别，以便立即解决管理或网络问题。 但是，这种更改通常无法反转。 这种不可逆的更改状态意味着计算机可能不再满足企业安全性的要求。

通过定期分析，可以跟踪并确保作为企业风险管理计划的一部分，每台计算机上的适当安全级别。 可以优化安全级别，最重要的是，检测系统随时间推移可能发生的任何安全漏洞。

使用安全配置和分析可以快速查看安全分析结果。 它提供当前系统设置的建议，并使用视觉标志或备注来突出显示当前设置与建议的安全级别不匹配的任何区域。 安全配置和分析还能够解决分析显示的任何差异。

安全配置

安全配置和分析还可用于直接配置本地系统安全性。 通过使用个人数据库，可以导入使用安全模板创建的安全模板，并将这些模板应用于本地计算机。 这些安全模板会立即使用模板中指定的级别配置系统安全性。

安全模板

使用 Microsoft 管理控制台的安全模板管理单元，可以为设备或网络创建安全策略。 它是一个单一入口点，可以考虑所有系统安全性。 安全模板管理单元不会引入新的安全参

数，它只是将所有现有安全属性组织到一个位置，以简化安全管理。

将安全模板导入组策略对象可同时配置域或组织单位的安全性，从而简化域管理。

若要将安全模板应用于本地设备，可以使用安全配置和分析或 secedit 命令行工具。

安全模板可用于定义：

- 帐户策略
  - 密码策略
  - 帐户锁定策略
  - Kerberos 策略
- 本地策略
  - 审核策略
  - 用户权限分配
  - 安全选项
- 事件日志：应用程序、系统和安全事件日志设置
- 受限组：安全敏感组的成员身份
- 系统服务：系统服务的启动和权限
- 注册表：注册表项的权限
- 文件系统：文件夹和文件的权限

每个模板都保存为基于文本的 .inf 文件。 使用此文件可以复制、粘贴、导入或导出部分或全部模板属性。 除 Internet 协议安全性和公钥策略外，所有安全属性都可以包含在安全模板中。

组策略的安全设置扩展

组织单位、域和站点链接到组策略对象。 使用安全设置工具，可以更改 组策略 对象的安全配置，进而影响多台计算机。 使用安全设置，可以根据修改的组策略对象，修改许多设备的安全设置，只需将一个设备加入域即可。

安全设置或安全策略是在设备或多台设备上配置的规则，用于保护设备或网络上的资源。 安全设置可以控制：

- 如何在网络或设备中对用户进行身份验证
- 用户有权使用的资源
- 是否在事件日志中记录用户或组的操作
- 组成员身份

可以通过两种方式更改多台计算机上的安全配置：

- 使用安全模板和安全模板创建安全策略，然后通过安全设置将模板导入到 组策略 对象。

- 使用安全设置更改一些选择设置。

本地安全策略

安全策略是影响设备上安全性的安全设置的组合。 可以使用本地安全策略来编辑本地设备上的帐户策略和本地策略

使用本地安全策略可以控制：

- 谁访问你的设备
- 用户有权在你的设备上使用哪些资源
- 是否在事件日志中记录用户或组的操作

如果本地设备已加入域，则需要从域的策略或你所属的任何组织单位的策略获取安全策略。 如果从多个源获取策略，则冲突将按以下优先级顺序解决。

1. 组织单位策略
2. 域策略
3. 站点策略
4. 本地计算机策略

如果使用本地安全策略修改本地设备上的安全设置，则直接修改设备上的设置。 因此，设置会立即生效，但这种效果可能只是暂时的。 设置实际上将在本地设备上保持有效，直到下次刷新组策略安全设置，从组策略收到的安全设置将覆盖本地设置（无论发生冲突）。

使用安全Configuration Manager

有关如何使用安全Configuration Manager的过程，请参阅安全Configuration Manager操作方法。 本节包含本主题中有关以下内容的信息：

- 应用安全设置
- 导入和导出安全模板
- 分析安全性并查看结果
- 解决安全差异
- 自动执行安全配置任务

应用安全设置

编辑安全设置后，在链接到 组策略 对象的组织单位的计算机上刷新这些设置：

- 重启设备时，将刷新该设备上的设置。
- 若要强制设备刷新其安全设置和所有组策略设置，请使用 gpupdate.exe。

将多个策略应用于计算机时策略的优先级

对于由多个策略定义的安全设置，将遵循以下优先级顺序：

1. 组织单位策略
2. 域策略
3. 站点策略
4. 本地计算机策略

例如，加入域的工作站将在发生冲突时由域策略覆盖其本地安全设置。 同样，如果同一工作站是组织单位的成员，则从组织单位的策略应用的设置将覆盖域和本地设置。 如果工作站是多个组织单位的成员，则立即包含该工作站的组织单位具有最高优先级。

> ⓘ **备注**
>
> 使用gpresult.exe了解将哪些策略应用于设备以及按何种顺序应用。
> 对于域帐户，只能有一个帐户策略，其中包括密码策略、帐户锁定策略和 Kerberos 策略。

安全设置中的持久性

即使最初应用安全设置的策略中不再定义某个设置，安全设置仍可能保留。

在以下情况下，安全设置中的持久性发生：

- 以前尚未为设备定义设置。
- 设置适用于注册表对象。
- 设置适用于文件系统对象。

通过本地策略或组策略对象应用的所有设置都存储在设备上的本地数据库中。 每当修改安全设置时，计算机都会将安全设置值保存到本地数据库，该数据库保留已应用于设备的所有设置的历史记录。 如果策略首先定义安全设置，然后不再定义该设置，则该设置将采用数据库中的上一个值。 如果数据库中不存在上一个值，则该设置不会还原为任何内容，并且仍按原样定义。 此行为有时称为“纹身”。

注册表和文件设置将保留通过策略应用的值，直到该设置设置为其他值。

基于组成员身份筛选安全设置

还可以通过拒绝用户或组在该组策略对象上应用组策略或读取权限来决定将或不会应用组策略对象，而不管他们登录到了哪个计算机。 应用组策略需要这两个权限。

导入和导出安全模板

安全配置和分析允许在数据库中导入和导出安全模板。

如果对分析数据库进行了任何更改，可以通过将这些设置导出到模板中来保存这些设置。 导出功能允许将分析数据库设置保存为新的模板文件。 然后，可以使用此模板文件来分析或配置系统，也可以将其导入到 组策略 对象。

分析安全性并查看结果

安全配置和分析通过将系统安全性的当前状态与 *分析数据库*进行比较来执行安全分析。 在创建过程中，分析数据库至少使用一个安全模板。 如果选择导入多个安全模板，数据库将合并各种模板并创建一个复合模板。 它按导入顺序解决冲突;导入的最后一个模板优先。

安全配置和分析使用可视标志指示问题，按安全区域显示分析结果。 它显示安全区域中每个安全属性的当前系统和基本配置设置。 若要更改分析数据库设置，请右键单击条目，然后单击“ **属性**”。

视觉对象标志	**含义**
红色 X	条目在分析数据库和系统上定义，但安全设置值不匹配。
绿色检查标记	条目在分析数据库中和系统上定义，并且设置值匹配。
问号	该条目未在分析数据库中定义，因此未分析。 如果未分析某个条目，则可能是在分析数据库中未定义该条目，或者运行分析的用户可能没有足够的权限在特定对象或区域上执行分析。
感叹 号	此项在分析数据库中定义，但在实际系统上不存在。 例如，可能有一个受限组，该组在分析数据库中定义，但在分析的系统上实际上不存在。
无突出显示	项未在分析数据库或系统上定义。

如果选择接受当前设置，则会修改基本配置中的相应值以匹配它们。 如果将系统设置更改为与基本配置匹配，则使用安全配置和分析配置系统时，更改将反映出来。

若要避免继续标记已调查并确定合理的设置，可以修改基本配置。 对模板的副本进行了更改。

解决安全差异

可以通过以下方法解决分析数据库和系统设置之间的差异：

- 如果确定本地系统安全级别由于该计算机的上下文 (或角色) 而有效，则接受或更改已标记或未包含在配置中的部分或全部值。 这些属性值随后在数据库中更新，并在单击“ **立即配置计算机**”时应用于系统。
- 如果确定系统不符合有效的安全级别，请将系统配置为分析数据库值。
- 将更适合该计算机角色的模板作为新的基本配置导入数据库，并将其应用于系统。对分析数据库的更改对数据库中存储的模板，而不是对安全模板文件进行更改。 仅当返回到安全模板并编辑该模板或将存储的配置导出到同一模板文件时，才会修改安全模板文件。

  应仅使用“**立即配置计算机**”来修改*不受*组策略设置影响的安全区域，例如本地文件和文件夹、注册表项和系统服务的安全性。 否则，当应用组策略设置时，它将优先于本地设置，例如帐户策略。

  通常，在分析基于域的客户端的安全性时，不要使用 “**立即配置计算机** ”，因为必须单独配置每个客户端。 在这种情况下，应返回到“安全模板”，修改模板，并将其重新应用到相应的组策略对象。

自动执行安全配置任务

通过在命令提示符处从批处理文件或自动任务计划程序调用 secedit.exe 工具，可以使用该工具自动创建和应用模板，并分析系统安全性。 还可以从命令提示符动态运行它。 如果有多个设备必须分析或配置安全性，并且需要在非工作时间执行这些任务，则Secedit.exe非常有用。

使用组策略工具

组策略是一种基础结构，允许你通过组策略设置和组策略首选项为用户和计算机指定托管配置。 对于仅影响本地设备或用户的组策略设置，可以使用本地组策略编辑器。 可以通过 组策略 管理控制台 (GPMC) 在Active Directory 域服务 (AD DS) 环境中管理组策略设置和组策略首选项。 组策略管理工具也包含在远程服务器管理工具包中，以便通过桌面管理组策略设置。

网络列表管理器策略

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

网络列表管理器策略是安全设置，可用于配置网络在一个设备或多个设备上列出和显示的不同方面。

若要为一台设备配置网络列表管理器策略，可以将 Microsoft 管理控制台 (MMC) 与 组策略 对象编辑器管理单元配合使用，并编辑本地计算机策略。 网络列表管理器策略位于 组策略 对象编辑器中的以下路径：**计算机配置 |Windows 设置 |安全设置 |网络列表管理器策略**

若要为许多计算机（例如 Active Directory 域中的所有域计算机）配置网络列表管理器策略，请按照组策略文档了解如何编辑所需对象的策略。 网络列表管理器策略的路径与上面列出的路径相同。

网络列表管理器策略的策略设置

为网络列表管理器策略提供了以下策略设置。 这些策略设置位于“组策略对象编辑器”的详细信息窗格中**的“网络名称”。**

身份不明的网络

此策略设置允许你为 Windows 无法识别的网络配置网络 **位置**，包括位置类型和用户权限，这些网络由于网络问题或操作系统从网络接收的网络信息中缺少可识别字符。 网络位置标识计算机连接到的网络类型，并自动为该位置设置相应的防火墙设置。 可以为此策略设置配置以下项：

- **位置类型。** 对于此项，可以使用以下选项：
  - **未配置。** 如果选择此选项，则此策略设置不会将位置类型应用于身份不明的网络连接。
  - **专用。** 如果选择此选项，此策略设置会将位置类型“专用”应用于未识别的网络连接。 专用网络（如家庭或工作网络）是一种位置类型，假定你信任网络上的其他计算机。 如果活动且身份不明的网络可能位于公共场所，请不要选择此项。

- **公共。** 如果选择此选项，此策略设置会将位置类型“公共”应用于未识别的网络连接。 公用网络（例如机场或咖啡店的无线网络）是一种位置类型，假定你不信任网络上的其他计算机。

- **用户权限。** 对于此项，可以使用以下选项：
  - **未配置。** 如果选择此选项，则此策略设置不会指定用户是否可以更改身份不明的网络连接的位置。
  - **用户可以更改位置。** 如果选择此选项，则此策略设置允许用户将身份不明的网络连接位置从“专用”更改为“公共”或“公共”更改为“专用”。
  - **用户无法更改位置。** 如果选择此选项，则此策略设置不允许用户更改身份不明的网络连接的位置。

标识网络

此策略设置允许你为处于临时状态的网络配置 **网络位置** ，而 Windows 则用于标识网络和位置类型。 网络位置标识计算机连接到的网络类型，并自动为该位置设置相应的防火墙设置。 可以为此策略设置配置以下项：

- **位置类型。** 对于此项，可以使用以下选项：
  - **未配置。** 如果选择此选项，则此策略设置不会将位置类型应用于正在由 Windows 标识的网络连接。
  - **专用。** 如果选择此选项，此策略设置会将位置类型“专用”应用于正在标识的网络连接。 专用网络（如家庭或工作网络）是一种位置类型，假定你信任网络上的其他设备。 如果活动且身份不明的网络可能位于公共场所，请不要选择此项。
  - **公共。** 如果选择此选项，此策略设置会将位置类型“公共”应用于正在由 Windows 标识的网络连接。 公用网络（例如机场或咖啡店的无线网络）是一种位置类型，假定你不信任网络上的其他设备。

所有网络

此策略设置允许指定 **用户权限** ，用于控制用户是否可以更改用户连接到的所有网络的网络名称、位置或图标。 可以为此策略设置配置以下项：

- **网络名称。** 对于此项，可以使用以下选项：
  - **未配置。** 如果选择此选项，此策略设置不会指定用户是否可以更改所有网络连接的网络名称。
  - **用户可以更改名称。** 如果选择此选项，用户可以更改他们连接到的所有网络的网络名称。
  - **用户无法更改名称。** 如果选择此选项，则用户无法更改其连接到的任何网络的网络名称。

- **网络位置。** 对于此项，可以使用以下选项：

- **未配置。** 如果选择此选项，则此策略设置不会指定用户是否可以更改所有网络连接的位置。
- **用户可以更改位置。** 如果选择此选项，则此策略设置允许用户将所有网络位置从“专用”更改为“公共”，或从“公共”更改为“专用”。
- **用户无法更改位置。** 如果选择此选项，则此策略设置不允许用户更改其连接到的任何网络的位置。

- **网络图标。** 对于此项，可以使用以下选项：
  - **未配置。** 如果选择此选项，则此策略设置不会指定用户是否可以更改所有网络连接的网络图标。
  - **用户可以更改图标。** 如果选择此选项，则此策略设置允许用户更改用户连接到的所有网络的网络图标。
  - **用户无法更改图标。** 如果选择此选项，则此策略设置不允许用户更改用户连接到的任何网络的网络图标。

配置安全策略设置

项目 • 2023/06/08 • 适用于: ✅ Windows 11, ✅ Windows 10

本文介绍在本地设备、已加入域的设备和域控制器上配置安全策略设置的步骤。 必须在本地设备上具有管理员权限，或者必须具有相应的权限才能更新域控制器上的组策略对象 (GPO) 才能执行这些过程。

当无法访问本地设置时，它指示 GPO 当前控制该设置。

使用本地安全策略控制台配置设置

1. 若要打开“本地安全策略”，请在 “**开始**” 屏幕上键入 **secpol.msc**，然后按 Enter。
2. 在控制台树的安全 **设置** 下，执行以下操作之一：

   - 选择“ **帐户策略**” 以编辑 **密码策略** 或 **帐户锁定策略。**
   - 选择“ **本地策略**” 以编辑 **审核策略**、 **用户权限分配**或 **安全选项。**

3. 在详细信息窗格中找到策略设置时，双击要修改的安全策略。
4. 修改安全策略设置，然后选择“ **确定**”。

> **备注**
>
> - 某些安全策略设置要求在设置生效之前重启设备。
> - 帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

使用本地组策略编辑器控制台配置安全策略设置

必须具有适当的权限才能安装和使用 Microsoft 管理控制台 (MMC) ，以及更新域控制器上的组策略对象 (GPO) 才能执行这些过程。

1. 打开“本地组策略编辑器” (gpedit.msc) 。
2. 在控制台树中，单击“**计算机配置**”，选择“**Windows 设置**”，然后选择“**安全设置**”。
3. 执行下列操作之一：

   - 选择“ **帐户策略**” 以编辑 **密码策略** 或 **帐户锁定策略。**
   - 选择“ **本地策略**” 以编辑 **审核策略**、 **用户权限分配**或 **安全选项。**

4. 在详细信息窗格中，双击要修改的安全策略设置。

> **备注**
>
> 如果尚未定义此安全策略，请选择“检查**定义这些策略设置**”框。

5. 修改安全策略设置，然后选择“ **确定**”。

> **备注**
>
> 如果要为网络上的许多设备配置安全设置，可以使用 组策略 管理控制台。

配置域控制器的设置

以下过程介绍如何仅为域控制器配置安全策略设置， (域控制器) 。

1. 若要打开域控制器安全策略，请在控制台树中，找到 *GroupPolicyObject [ComputerName]* 策略，依次单击“**计算机配置**”、“Windows **设置**”和“**安全设置**”。
2. 执行下列操作之一：
   - 双击“ **帐户策略**” 以编辑 **密码策略**、 **帐户锁定策略**或 Kerberos **策略**。
   - 选择“ **本地策略**” 以编辑 **审核策略**、 **用户权限分配**或 **安全选项**。
3. 在详细信息窗格中，双击要修改的安全策略。

> **备注**
>
> 如果尚未定义此安全策略，请选择“检查**定义这些策略设置**”框。

4. 修改安全策略设置，然后选择“ **确定**”。

> **重要**
>
> - 在将新创建的策略应用到网络之前，请始终在测试组织单元中测试该策略。
> - 通过 GPO 更改安全设置并单击“ **确定**”时，该设置将在下次刷新设置时生效。

相关文章

- 安全策略设置参考

安全策略设置参考

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

此安全设置参考提供了有关如何实现和管理安全策略的信息，包括设置选项和安全注意事项。

本参考重点介绍被视为安全设置的设置。 此参考仅检查 Windows 操作系统中的设置和功能，这些设置和功能可帮助组织保护其企业免受恶意软件威胁。 此参考中未介绍管理功能和无法配置的安全功能。

描述的每个策略设置都包含引用内容，例如详细说明设置、最佳做法、默认设置、操作系统版本之间的差异、策略管理注意事项以及安全注意事项，其中包括对漏洞、对策以及这些对策的潜在影响的讨论。

本部分内容

主题	描述
帐户策略	概述 Windows 中的帐户策略，并提供策略说明的链接。
审核策略	提供有关 Windows 中可用的基本审核策略的信息，以及指向每个设置的信息的链接。
安全选项	介绍本地 **安全策略的安全选项** 下的设置，并链接到有关每个设置的信息。
高级安全审核策略设置	提供有关 Windows 中可用的高级安全审核策略设置及其生成的审核事件的信息。
用户权限分配	提供有关 Windows 中可用的用户权限分配安全策略设置用户权限的概述和链接。

帐户策略

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

概述 Windows 中的帐户策略，并提供策略说明的链接。

使用 组策略 应用的所有帐户策略设置都在域级别应用。 默认值存在于密码策略设置、帐户锁定策略设置和 Kerberos 策略设置的内置默认域控制器策略中。 域帐户策略将成为作为域成员的任何设备的默认本地帐户策略。 如果在 Active Directory 域服务 (AD DS) 中的域级别以下的任何级别设置这些策略，则它们仅影响成员服务器上的本地帐户。

> **备注**
>
> 每个域只能有一个帐户策略。 帐户策略必须在默认域策略或链接到域根的新策略中定义，并且优先于默认域策略，该策略由域中的域控制器强制实施。 这些域范围的帐户策略设置 (密码策略、帐户锁定策略和 Kerberos 策略) 由域中的域控制器强制执行;因此，域控制器始终从默认域策略组策略对象 (GPO) 检索这些帐户策略设置的值。

唯一的例外是为组织单位定义另一个帐户策略， (OU) 。 OU 的帐户策略设置会影响 OU 中包含的任何计算机上的本地策略。 例如，如果 OU 策略定义的最长密码期限不同于域级帐户策略，则仅当用户登录到本地计算机时，才会应用并强制实施 OU 策略。 默认本地计算机策略仅适用于工作组或域策略中同时不适用 OU 帐户策略和域策略的计算机。

本部分内容

主题	描述
密码策略	Windows 的密码策略概述，以及指向每个策略设置的信息的链接。
帐户锁定策略	介绍帐户锁定策略设置，并链接到有关每个策略设置的信息。
Kerberos 策略	介绍 Kerberos 策略设置，并提供指向策略设置说明的链接。

相关主题

配置安全策略设置

密码策略

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

Windows 的密码策略概述，以及指向每个策略设置的信息的链接。

在许多操作系统中，对用户标识进行身份验证的最常见方法是使用密码或密码。 安全网络环境要求所有用户使用强密码，该密码至少包含 8 个字符，并且包含字母、数字和符号的组合。 这些密码有助于防止未经授权的用户使用手动方法或自动化工具猜测弱密码的用户帐户和管理帐户。 定期更改的强密码可降低成功密码攻击的可能性。

Windows 在 Windows Server 2008 R2 和 Windows Server 2008 中引入，支持精细密码策略。 此功能为组织提供了一种为域中不同用户组定义不同密码和帐户锁定策略的方法。 细化密码策略仅适用于用户对象 (或 inetOrgPerson 对象，而不是) 和全局安全组的用户对象。 有关详细信息，请参阅 AD DS Fine-Grained密码和帐户锁定策略分步指南。

若要对 OU 的用户应用细化密码策略，可以使用影子组。 影子组是一个全局安全组，在逻辑上映射到 OU 以强制实施精细密码策略。 将 OU 的用户添加为新创建的影子组的成员，然后将细化密码策略应用于此影子组。 可以根据需要为其他 OU 创建其他阴影组。 如果将用户从一个 OU 移动到另一个 OU，则必须更新相应阴影组的成员身份。

细化密码策略包括可在默认域策略中定义的所有设置的属性 (除 Kerberos 设置) 帐户锁定设置外。 指定细化密码策略时，必须指定所有这些设置。 默认情况下，只有域管理员组的成员可以设置细化的密码策略。 但是，还可以将设置这些策略的功能委托给其他用户。 域必须至少运行 Windows Server 2008 R2 或 Windows Server 2008 才能使用细化密码策略。 细化密码策略不能直接应用于组织单位 (OU) 。

可以通过适当的密码策略强制使用强密码。 有一些密码策略设置可以控制密码的复杂性和生存期，例如 **密码必须满足复杂性要求** 策略设置。

可以使用 组策略 管理控制台在以下位置配置密码策略设置：

计算机配置\Windows 设置\安全设置\帐户策略\密码策略

此组策略在域级别应用。 如果单个组需要不同的密码策略，请考虑使用细化的密码策略，如上所述。

以下主题介绍了密码策略实现和最佳做法注意事项、策略位置、服务器类型或 GPO 的默认值、操作系统版本的相关差异、安全注意事项 (包括每个设置) 的可能漏洞、可以采取的对策以及每个设置的潜在影响。

本部分内容

主题	描述
强制实施密码历史记录	介绍 **强制执行密码历史记录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
最长密码使用期限	介绍 **最长密码期限** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
最短密码使用期限	介绍 **最短密码期限** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
最短密码长度	介绍 **最小密码长度** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
密码必须符合复杂性要求	介绍 **密码必须满足复杂性要求** 安全策略设置的最佳做法、位置、值和安全注意事项。
用可还原的加密来存储密码	介绍 **使用可逆加密** 安全策略设置存储密码的最佳做法、位置、值和安全注意事项。

相关主题

- 配置安全策略设置

强制实施密码历史记录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **强制执行密码历史记录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

“**强制实施密码历史记录**策略”设置确定在重用旧密码之前必须与用户帐户关联的唯一新密码的数量。 密码重用是任何组织中的一个重要问题。 许多用户希望长时间对其帐户重复使用同一密码。 同一密码用于特定帐户的时间越长，攻击者通过暴力攻击确定密码的可能性就越大。 如果用户需要更改其密码，但他们可以重复使用旧密码，则良好的密码策略的有效性将大大降低。

为 “**强制实施密码历史记录**” 指定一个较低的数字可让用户持续重复使用相同的少量密码。 如果未同时设置 最短密码期限，用户可以根据需要在一行中多次更改其密码，以便重复使用其原始密码。

可能值

- 用户指定的数字从 0 到 24
- 未定义

最佳做法

- 将 “**强制实施密码历史记录** ”设置为“24”。 此设置将有助于缓解由密码重用导致的漏洞。
- 设置 最长密码期限 以在 60 到 90 天内使密码过期。 尝试使主要业务周期之间的密码过期，以防止工作丢失。
- 配置 最短密码期限 ，以便不允许立即更改密码。

位置

计算机配置\Windows 设置\安全设置\帐户策略\密码策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	已记住 24 个密码
默认域控制器策略	未定义
独立服务器默认设置	记住 0 个密码
域控制器有效默认设置	已记住 24 个密码
成员服务器有效默认设置	已记住 24 个密码
客户端计算机上有效的 GPO 默认设置	已记住 24 个密码

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

用户使用相同的密码的时间越长，攻击者通过暴力攻击确定密码的可能性就越大。 此外，只要密码保持不变，任何可能已泄露的帐户仍可被利用。 如果需要更改密码，但未阻止密码重用，或者用户不断重用一些密码，则良好密码策略的有效性将大大降低。

如果为此策略设置指定了较低的数字，则用户可以重复使用相同的少量密码。 如果未同时配置 最短密码期限 策略设置，则用户可能会反复更改其密码，直到他们可以重复使用其原始密码。

> **注意：** 帐户泄露后，简单的密码重置可能不足以限制恶意用户，因为恶意用户可能已修改了用户的环境，使密码在特定时间自动更改回已知值。 如果帐户已遭入侵，最好在所有受影响的系统还原到正常操作并验证它们不再遭到入侵后删除该帐户并向用户分配一个新帐户。

对策

将 “**强制密码历史记录** ”策略设置配置为 24 (最大设置) ，以帮助最大程度地减少由密码重用导致的漏洞数。

若要使此策略设置生效，还应为 “最短密码期限 ”和“ 密码最长期限 ”策略设置配置有效值。

潜在影响

将 “**强制密码历史记录** ”设置配置为 24 的主要影响是用户每次需要更改旧密码时都必须创建新密码。 如果要求用户将其密码更改为新的唯一值，则用户在某个位置写入密码以便不会忘记密码的风险会增加。 另一个风险是，用户可能会创建 (增量更改的密码，例如，password01、password02 等) 以促进记忆，但这些密码使攻击者更容易猜测。 此外，“最长密码期限 ”策略设置的值过低可能会增加管理开销，因为忘记密码的用户可能会要求技术支持频繁重置密码。

相关主题

- 密码策略

最长密码使用期限

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **最长密码期限** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

最长 **密码期限** 策略设置确定在系统要求用户更改密码之前 () 可以使用密码的时间段（以天为单位）。 可以将密码设置为在 1 到 999 之间的特定天数后过期，也可以通过将天数设置为 0 来指定密码永不过期。 如果 **最长密码期限** 在 1 到 999 天之间，则最短密码期限必须小于最长密码期限。 如果 **最长密码期限** 设置为 0， 则最短密码期限 可以是 0 到 998 天之间的任何值。

> **注意：** 将 **最长密码期限** 设置为 -1 等效于 0，这意味着它永不过期。 将其设置为任何其他负数等效于将其设置为 “**未定义**”。

可能值

- 用户指定的天数介于 0 到 999 之间
- 未定义

最佳做法

根据环境，将 “**最长密码期限** ”设置为 30 到 90 天之间的值。 这样，攻击者在泄露用户密码并有权访问网络资源的时间有限。

> **备注**
>
> Microsoft 建议的安全基线不包含密码过期策略，因为它不如新式缓解措施有效。 但是，未实施 Azure AD 密码保护、多重身份验证或其他密码猜测攻击新式缓解措施的公司应使此策略生效。

位置

计算机配置\Windows 设置\安全设置\帐户策略\密码策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	42 天
默认域控制器策略	未定义
独立服务器默认设置	42 天
域控制器有效默认设置	42 天
成员服务器有效默认设置	42 天
客户端计算机上有效的 GPO 默认设置	42 天

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置、如何实施对策，以及实现的可能负面影响。

漏洞

密码存在时间越长，遭受暴力攻击、攻击者获取有关用户的一般知识或共享密码的用户入侵的可能性就越大。 将 “**最长密码期限**” 策略设置配置为 0，以便用户永远不需要更改其密码，只要有效用户获得授权访问，恶意用户就会使用泄露的密码。

注意事项

强制密码更改是一种长期存在的安全做法，但目前的研究强烈表明密码过期具有负面影响。 有关详细信息，请参阅 Microsoft 密码指南。

将 “**最长密码期限** ”策略设置配置为适合组织业务要求的值。 例如，许多组织都有合规性或保险要求，要求密码的生命周期较短。 存在此类要求时，可以使用 “**最长密码期限**” 策略设置来满足业务需求。

潜在影响

如果 “**最长密码期限**” 策略设置太低，则用户需要经常更改其密码。 此类配置可能会降低组织中的安全性，因为用户可能会将其密码保存在不安全的位置或丢失密码。 如果此策略设置的值过高，则组织内的安全级别会降低，因为它允许潜在攻击者使用更多时间来发现用户密码或使用已泄露的帐户。

相关主题

- 密码策略

最短密码使用期限

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **最短密码期限** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

最短密码期限策略设置确定 (天数，) 用户更改密码之前必须使用密码。 可以将值设置为 1 到 998 天，也可以通过将天数设置为 0 来立即允许更改密码。 最短密码期限必须小于最长密码期限，除非最大密码期限设置为 0，指示密码永不过期。 如果最长密码期限设置为 0，则最短密码期限可以设置为 0 到 998 之间的任何值。

可能值

- 用户指定的天数介于 0 到 998 之间
- 未定义

最佳做法

Windows 安全基线 建议将 **最短密码期限** 设置为一天。

将天数设置为 0 允许立即更改密码。 不建议使用此设置。 通过将即时密码更改与密码历史记录相结合，某人可以反复更改密码，直到满足密码历史记录要求，然后再次重新建立原始密码。 例如，假设密码为“Ra1ny day！”，历史记录要求为 24。 如果最短密码期限为 0，则可以连续更改密码 24 次，直到最终更改回“Ra1ny day！”。 最短密码期限为 1 天会阻止此情况。

如果为用户设置了密码，并且希望该用户更改管理员定义的密码，则必须选中“**用户下次登录时必须更改密码**检查”框。 否则，用户将无法更改密码，直到 **最短密码期限**指定的天数。

位置

计算机配置\Windows 设置\安全设置\帐户策略\密码策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	1 天
默认域控制器策略	未定义
独立服务器默认设置	0 天
域控制器有效默认设置	1 天
成员服务器有效默认设置	1 天
客户端计算机上有效的 GPO 默认设置	1 天

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

用户可能有喜欢使用的密码，因为他们很容易记住，并且他们相信他们的密码选择是安全的，不会泄露。 遗憾的是，密码可能会遭到入侵，如果攻击者以特定个人用户帐户为目标，并且知道该用户的数据，则重用旧密码可能会导致安全漏洞。

若要解决密码重用问题，必须使用安全设置的组合。 将此策略设置与 “强制实施密码历史记录” 策略设置结合使用可防止轻松重用旧密码。 例如，如果配置“强制实施密码历史记录”策略设置以确保用户不能重复使用其最近 12 个密码中的任何一个，但未将 “**最短密码期限**” 策略设置配置为大于 0 的数字，则用户可以在几分钟内更改其密码 13 次，并重复使用其原始密码。 将此策略设置配置为大于 0 的数字，使“强制密码历史记录”策略设置生效。

对策

将 “**最短密码期限** ”策略设置配置为值 1 天。 用户应了解此限制，并联系技术支持以尽快更改密码。 如果将天数配置为 0，则允许立即更改密码，我们不建议更改。

潜在影响

如果为用户设置了密码，但希望该用户在首次登录时更改密码，则管理员必须选中“**用户下次登录时必须更改密码**检查”框，否则用户必须在第二天之前更改密码。

相关主题

- 密码策略

最短密码长度

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

本文介绍 **最小密码长度** 安全策略设置的建议做法、位置、值、策略管理和安全注意事项。

参考

最短密码长度策略设置确定可以构成用户帐户密码的最小字符数。 可以将值设置为 1 到 14 个字符，也可以通过将字符数设置为 0 来确定不需要密码。

可能值

- 用户指定的字符数介于 0 和 14 之间
- 未定义

最佳做法

将最小密码长度设置为至少 8。 如果字符数设置为 0，则无需密码。 在大多数环境中，建议使用八个字符的密码，因为它足够长，足以提供足够的安全性，并且仍然足够短，用户可以轻松记住。 目前不支持超过 14 的最小密码长度。 此值将有助于提供足够的防御来抵御暴力攻击。 增加复杂性要求有助于降低字典攻击的可能性。 有关详细信息，请参阅 密码必须满足复杂性要求。

允许短密码会降低安全性，因为使用对密码执行字典或暴力攻击的工具很容易破坏短密码。 要求使用长密码可能会导致密码键入错误，这可能会导致帐户锁定，并可能增加技术支持呼叫的量。

此外，要求使用长密码实际上可能会降低组织的安全性，因为用户可能更可能记下其密码以避免忘记密码。 但是，如果用户被教导他们可以使用通行短语 (句子，如“我想喝一个5美元的奶昔”)，他们应该更有可能记住。

位置

计算机配置\Windows 设置\安全设置\帐户策略\密码策略

默认值

下表列出了实际和有效的默认策略值。 默认值也会在策略的属性页上列出。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	七个字符
默认域控制器策略	未定义
独立服务器默认设置	零个字符
域控制器有效默认设置	七个字符
成员服务器有效默认设置	七个字符
客户端计算机上有效的 GPO 默认设置	零个字符

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

密码攻击类型包括字典攻击 (尝试使用常见字词和短语) 和暴力攻击 (尝试字符) 的每个可能组合。 此外，攻击者有时会尝试获取帐户数据库，以便他们可以使用工具来发现帐户和密码。

对策

将 “**最小密码长度**” 策略设置配置为值 8 或更多。 如果字符数设置为 0，则无需密码。

在大多数环境中，我们建议使用八个字符的密码，因为它足够长，可以提供足够的安全性，但不太难让用户轻松记住。 此配置提供足够的防御来抵御暴力攻击。 除了“**最小密码长度**”设置外，使用“密码必须满足复杂性要求”策略设置，有助于减少字典攻击的可能性。

> **备注**
>
> 作为建立安全法规的一部分，一些司法管辖区对密码长度制定了法律要求。

潜在影响

长密码的要求实际上可能会降低组织的安全性，因为用户可能会将信息留在不安全的位置或丢失信息。 如果需要长密码，则键入错误的密码可能会导致帐户锁定并增加技术支持呼叫量。 如果组织因密码长度要求而出现忘记密码的问题，请考虑向用户教授密码，这些通行短语通常更容易记住，并且由于字符组合数量较多，更难发现。

相关主题

- 密码策略

密码必须符合复杂性要求

项目 • 2023/06/08

适用范围

- Windows 11
- Windows 10

介绍 **密码必须满足复杂性要求** 安全策略设置的最佳做法、位置、值和安全注意事项。

参考

密码必须满足复杂性要求策略设置确定密码是否必须满足一系列强密码准则。 启用此设置后，需要密码才能满足以下要求：

1. 密码不能包含用户的 samAccountName (帐户名) 值或整个 displayName (Full Name 值) 。 这两项检查都不区分大小写。

   将完全检查 samAccountName，只是为了确定它是否是密码的一部分。 如果 samAccountName 的长度少于三个字符，则跳过此检查。 displayName 针对分隔符进行分析：逗号、句点、短划线或连字符、下划线、空格、井号和制表符。 如果找到这些分隔符中的任何一个，则将拆分 displayName，并且所有已分析部分 (令牌) 确认不包含在密码中。 将忽略短于三个字符的标记，并且不会检查令牌的子字符串。 例如，名称“Erin M. Hagens”拆分为三个标记：“Erin”、“M”和“Hagens”。 由于第二个标记只有一个字符长，因此将被忽略。 因此，此用户不能将密码包含“erin”或“hagens”作为密码中的任何一个子字符串。

2. 密码包含以下三个类别中的字符：

   - 欧洲语言的大写字母 (A 到 Z，带有音调符号、希腊语和西里尔文字符)
   - 欧洲语言的小写字母 (到 z，sharp-s，带有音调符号、希腊语和西里尔字符)
   - (0 到 9)
   - 非字母数字字符 (特殊字符) ： `(~!@#$%^&*_-+=`|\\(){}\[\]:;"'<>,.?/)` 欧元或英镑等货币符号不计入此策略设置的特殊字符。
   - 分类为字母字符但不是大写或小写的任何 Unicode 字符。 此组包含来自亚洲语言的 Unicode 字符。

更改或创建密码时，会强制实施复杂性要求。

Windows Server 密码复杂性要求中包含的规则是 的 `Passfilt.dll`一部分，不能直接修改这些规则。

启用后，默认Passfilt.dll可能会导致对锁定帐户进行更多技术支持调用，因为用户习惯于仅包含字母表中字符的密码。 但是，此策略设置足够宽松，所有用户都应该习惯它。

可以包含在自定义 `Passfilt.dll` 中的其他设置是使用非上行字符。 若要键入上行字符，请按住 SHIFT 键，然后按键盘 (数字行上的任意一个键，) 从 1 到 9 和 0。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

> **提示**
>
> 有关最新的最佳做法，请参阅 **密码指南** 。

将 “**密码必须满足复杂性要求** ”设置为“已启用”。 此策略设置与最小密码长度 8 相结合，可确保单个密码至少有 159，238，157，238，528 种不同的可能性。 此设置使暴力攻击变得困难，但仍不是不可能。

使用 ALT 键字符组合可能会大大增强密码的复杂性。 但是，要求组织中的所有用户遵守如此严格的密码要求可能会导致用户不满和过度工作的技术支持。 请考虑在组织中实施一项要求，要求使用范围从 0128 到 0159 的 ALT 字符作为所有管理员密码的一部分。 (超出该范围的 ALT 字符可以表示不会增加密码复杂性的标准字母数字字符。)

使用公开可用的工具，仅包含字母数字字符的短密码很容易泄露。 若要防止此漏洞，密码应包含其他字符和/或满足复杂性要求。

位置

`Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy`

默认值

下表列出了实际和有效的默认策略值。 默认值也会在策略的属性页上列出。

服务器类型或组策略对象 (GPO)	默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	已启用
默认域控制器策略	已启用
独立服务器默认设置	禁用
域控制器有效默认设置	已启用
成员服务器有效默认设置	已启用
客户端计算机上有效的 GPO 默认设置	禁用

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

仅包含字母数字字符的密码可通过多种公开可用的工具轻松发现。

对策

将 "**密码必须满足复杂性要求** "策略设置为 "*已启用* "，并建议用户在密码中使用各种字符。

当与 最小密码长度 8 结合使用时，此策略设置可确保单个密码的不同可能性数非常大，因此很难 (但暴力攻击可能) 成功。 (如果增加最小密码长度策略设置，则成功攻击所需的平均时间也会增加。)

潜在影响

如果保留密码复杂性的默认配置，则可能会对锁定的帐户进行更多技术支持调用，因为用户可能不习惯使用包含非字母字符的密码，或者他们可能无法在具有不同布局的键盘上输入包含重音字符或符号的密码。 但是，所有用户都应能够以最小的难度遵循复杂性要求。

如果组织具有更严格的安全要求，则可以创建允许使用任意复杂密码强度规则的文件的自定义版本 `Passfilt.dll` 。 例如，自定义密码筛选器可能需要使用非上行符号。 (上行符号是需要按住 SHIFT 键，然后按键盘数字行上的任意键（从 1 到 9 和 0）的符号。) 自定

义密码筛选器可能还会执行字典检查，以验证建议的密码是否不包含常见的字典单词或片段。

使用 ALT 键字符组合可能会大大增强密码的复杂性。 但是，这种严格的密码要求可能会导致更多的技术支持请求。 或者，组织可以考虑要求所有管理员密码使用 0128-0159 范围内的 ALT 字符。 此范围之外的 (ALT 字符可以表示不会增加密码复杂性的标准字母数字字符。)

相关文章

- 密码策略

用可还原的加密来存储密码

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **使用可逆加密** 安全策略设置存储密码的最佳做法、位置、值和安全注意事项。

参考

使用可逆加密策略存储密码设置为使用要求用户密码进行身份验证的协议的应用程序提供支持。 以可逆的方式存储加密的密码意味着可以解密加密的密码。 知识渊博的攻击者如果能够破坏此加密，则可以使用受攻击的帐户登录到网络资源。 因此，除非应用程序要求超过保护密码信息的需求，否则不要为域中的所有用户启用 **使用可逆加密的存储** 密码。

如果使用质询握手身份验证协议 (CHAP) 通过远程访问或 Internet 身份验证服务 (IAS) ，则必须启用此策略设置。 CHAP 是远程访问和网络连接使用的身份验证协议。 Internet Information Services (IIS) 中的摘要式身份验证还要求启用此策略设置。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

将 “**使用可逆加密存储密码** ”的值设置为“已禁用”。 如果在 IIS 中通过远程访问、IAS 或摘要式身份验证使用 CHAP，则必须将此值设置为 “**已启用**”。 在用户的基础上使用 组策略应用设置时，此设置会带来安全风险，因为它需要在 Active Directory 用户和计算机 中打开相应的用户帐户对象。

> **注意：** 除非业务要求超过保护密码信息的需求，否则不要启用此策略设置。

位置

计算机配置\Windows 设置\安全设置\帐户策略\密码策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	禁用
默认域控制器策略	禁用
独立服务器默认设置	禁用
域控制器有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机上有效的 GPO 默认设置	禁用

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

启用此策略设置允许操作系统以可能削弱整体安全性的格式存储密码。

对策

使用可逆加密策略设置禁用存储密码。

> **备注**
>
> 禁用策略设置后，默认情况下，仅使用单向加密存储新密码。 现有密码将使用可逆加密进行存储，直到更改。

潜在影响

如果组织通过远程访问、IAS 或 IIS 中的摘要式身份验证使用 CHAP，则必须将此策略设置配置为“已启用”。 通过逐个用户组策略应用设置时，此设置会带来安全风险，因为它需要在Active Directory 用户和计算机中打开相应的用户帐户对象。

相关主题

- 密码策略

帐户锁定策略

项目 • 2023/05/12

适用范围

- Windows 11
- Windows 10

介绍帐户锁定策略设置，并链接到有关每个策略设置的信息。

尝试登录系统时尝试使用多个不成功的密码的人可能是尝试通过试用和错误来确定帐户密码的恶意用户。 Windows 域控制器会跟踪登录尝试，可以通过在预设的时间段内禁用帐户来配置域控制器以响应此类潜在攻击。 帐户锁定策略设置控制此响应的阈值，以及达到阈值后要执行的操作。 可以在组策略管理控制台的以下位置配置帐户锁定策略设置：**计算机配置\策略\Windows 设置\安全设置\帐户策略\帐户锁定策略。**

以下主题介绍了每个策略设置的实现和最佳做法注意事项、策略位置、服务器类型或 组策略 Object (GPO) 的默认值、操作系统版本的相关差异以及 (安全注意事项，包括每个策略设置) 的可能漏洞、可以实施的对策以及实施对策的潜在影响。

> **备注**
>
> 通过在管理远程访问的服务器上编辑注册表，可以单独配置远程访问客户端的帐户锁定设置。 有关详细信息，请参阅 **如何配置远程访问客户端帐户锁定。**

Windows 版本和许可要求

下表列出了支持帐户锁定策略的 Windows 版本：

Windows 专业版	Windows 企业版	Windows 专业教育版/SE	Windows 教育版
是	是	是	是

帐户锁定策略许可证权利由以下许可证授予：

Windows 专业版/专业教育版/SE	Windows 企业版 E3	Windows 企业版 E5	Windows 教育版 A3	Windows 教育版 A5
是	是	是	是	是

有关 Windows 许可的详细信息，请参阅 Windows 许可概述。

本部分内容

主题	描述
帐户锁定阈值	介绍 **帐户锁定阈值** 安全策略设置的最佳做法、位置、值和安全注意事项。
帐户锁定持续时间	介绍 **帐户锁定持续时间** 安全策略设置的最佳做法、位置、值和安全注意事项。
在此后重置帐户锁定计数器	介绍安全策略设置 **后重置帐户锁定计数器** 的最佳做法、位置、值和安全注意事项。

相关主题

配置安全策略设置

帐户锁定持续时间

项目 • 2023/03/09

适用范围

- Windows 11
- Windows 10

介绍 **帐户锁定持续时间** 安全策略设置的最佳做法、位置、值和安全注意事项。

参考

帐户锁定持续时间策略设置确定锁定的帐户在自动解锁之前保持锁定状态的分钟数。 可用范围为 1 到 99，999 分钟。 值 0 指定帐户将被锁定，直到管理员显式解除锁定。 如果 **帐户锁定阈值** 设置为大于零的数字， **则帐户锁定持续时间** 必须大于或等于 重置帐户锁定计数器后的值。 此策略设置依赖于定义的 **帐户锁定阈值** 策略设置，并且它必须大于或等于在策略设置 后为重置帐户锁定计数器 指定的值。

可能值

- 用户定义的分钟数（从 0 到 99，999）
- 未定义

如果配置了 帐户锁定阈值 ，在指定的失败尝试次数之后，帐户将被锁定。如果 **帐户锁定持续时间** 设置为 0，则帐户将保持锁定状态，直到管理员手动将其解锁。

建议将 **帐户锁定持续时间** 设置为大约 15 分钟。 若要指定永远不会锁定帐户，请将 “**帐户锁定阈值** ”设置为 0。

位置

计算机配置\Windows 设置\安全设置\帐户策略\帐户锁定策略

默认值

下表列出了实际和有效的默认策略值。 默认值也会在策略的属性页上列出。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义

服务器类型或组策略对象 (GPO)	默认值
默认域控制器策略	未定义
独立服务器默认设置	不适用
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	不适用

安全注意事项

尝试登录计算机期间多次未成功提交密码可能表示攻击者尝试通过试用和错误来确定帐户密码。 Windows 和 Windows Server 操作系统可以跟踪登录尝试，你可以将操作系统配置为在指定次数的失败尝试后在预设的时间段内禁用帐户。 帐户锁定策略设置控制此响应的阈值，以及达到阈值后要执行的操作。

漏洞

如果攻击者滥用 帐户锁定阈值 策略设置并反复尝试使用特定帐户登录，则可以创建拒绝服务 (DoS) 条件。 配置帐户锁定阈值策略设置后，在指定的失败尝试次数后，帐户将被锁定。 如果将 “**帐户锁定持续时间**” 策略设置为 0，则帐户将保持锁定状态，直到你手动解锁它。

对策

将 **帐户锁定持续时间** 策略设置配置为适合你的环境的值。 若要指定帐户在手动解锁之前保持锁定状态，请将值配置为 0。 将 “**帐户锁定持续时间**” 策略设置配置为非零值时，自动猜测帐户密码的尝试将在此间隔内延迟，然后再对特定帐户恢复尝试。 将此设置与 帐户锁定阈值 策略设置结合使用会使自动密码猜测尝试更加困难。

潜在影响

将 **帐户锁定持续时间** 策略设置为 0 以便无法自动解锁帐户可能会增加组织技术支持收到的解锁错误锁定帐户的请求数。

相关主题

帐户锁定策略

帐户锁定阈值

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **帐户锁定阈值** 安全策略设置的最佳做法、位置、值和安全注意事项。

参考

帐户锁定阈值策略设置确定将导致用户帐户被锁定的失败登录尝试次数。 在重置锁定帐户或帐户锁定持续时间策略设置指定的分钟数过期之前，无法使用锁定 的帐户 。 可以将失败的登录尝试设置为 1 到 999 的值，也可以通过将值设置为 0 来指定永远不会锁定帐户。 如果 **帐户锁定阈值** 设置为大于零的数字， **则帐户锁定持续时间** 必须大于或等于 重置帐户锁定计数器后的值。

暴力破解密码攻击可以自动为任何或所有用户帐户尝试数千甚至数百万个密码组合。 限制可以执行的失败登录数几乎消除了此类攻击的有效性。 但是，请务必注意，可以在配置了帐户锁定阈值的域中执行拒绝服务 (DoS) 攻击。 恶意用户可以以编程方式尝试对组织中的所有用户进行一系列密码攻击。 如果尝试次数大于 **帐户锁定阈值**的值，攻击者可能会锁定每个帐户。

尝试解锁工作站失败可能会导致帐户锁定，即使 “交互式登录：要求域控制器身份验证才能解锁工作站 安全”选项处于禁用状态。 如果你输入登录时所用的相同密码，Windows 不需要联系域控制器进行解锁，但如果输入其他密码，Windows 必须联系域控制器，以防你从另一台计算机更改了密码。

可能值

可以针对 **帐户锁定阈值** 策略设置配置以下值：

- 从 0 到 999 的用户定义数字
- 未定义

由于在配置此值时和未配置此值时可能存在漏洞，因此组织应权衡其已识别的威胁以及他们试图缓解的风险。 有关这些设置的信息，请参阅本文中的 对策 。

最佳做法

选择的阈值是运营效率和安全性之间的平衡，具体取决于组织的风险级别。 为了允许用户错误并阻止暴力攻击， Windows 安全基线 建议将值 10 作为组织可接受的起点。

与其他帐户锁定设置一样，此值更像一个准则，而不是一个规则或最佳做法，因为没有“一个大小适合所有人”。有关详细信息，请参阅 配置帐户锁定。

此策略设置的实现取决于操作环境;威胁向量、部署的操作系统和已部署的应用。 有关详细信息，请参阅本文中的 实现注意事项 。

位置

计算机配置\Windows 设置\安全设置\帐户策略\帐户锁定策略

默认值

下表列出了实际和有效的默认策略值。 默认值也会在策略设置的属性页上列出。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	0 次无效登录尝试
默认域控制器策略	未定义
独立服务器默认设置	0 次无效登录尝试
域控制器有效默认设置	0 次无效登录尝试
成员服务器有效默认设置	0 次无效登录尝试
客户端计算机上有效的 GPO 默认设置	0 次无效登录尝试

策略管理

本部分介绍可用于帮助你管理此策略设置的功能和工具。

重启要求

无。 此策略设置的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

实现注意事项

此策略设置的实现取决于操作环境。 考虑威胁向量、部署的操作系统和部署的应用。 例如：

- 帐户被盗或 DoS 攻击的可能性取决于系统和环境的安全设计。 考虑到这些威胁的已知和感知风险，设置帐户锁定阈值。
- 在客户端、服务器和域控制器之间协商加密类型时，Kerberos 协议可以自动重试计入此策略设置中设置的阈值限制的帐户登录尝试。 在部署不同版本的操作系统的环境中，加密类型协商会增加。
- 并非环境中使用的所有应用都可以有效地管理用户尝试登录的次数。 例如，如果用户在运行应用时连接反复断开，则所有后续失败的登录尝试都会计入帐户锁定阈值。

有关帐户锁定的 Windows 安全基线建议的详细信息，请参阅 配置帐户锁定。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

> ⓘ **备注**
>
> 锁定阈值策略将同时应用于本地成员计算机用户和域用户，以便缓解"漏洞"中所述的问题。 但是，内置管理员帐户虽然是高特权帐户，但具有不同的风险配置文件，并被排除在此策略之外。 这可确保不存在管理员无法登录来修正问题的情况。 作为管理员，还有其他可用的缓解策略，例如强密码。 另请参阅 **附录 D：保护** Active Directory **中的**Built-In**管理员帐户**。

漏洞

暴力破解密码攻击可以使用自动方法尝试任何用户帐户的数百万个密码组合。 如果限制可以执行的失败登录尝试次数，则几乎可以消除此类攻击的有效性。 但是，可以在配置了帐户锁定阈值的域上执行 DoS 攻击。 攻击者可能以编程方式尝试对组织中的所有用户进行一系列密码攻击。 如果尝试次数大于帐户锁定阈值，攻击者可能能够锁定每个帐户，而无需任何特殊权限或在网络中进行身份验证。

> ⓘ **备注**
>
> 此策略设置无法应对脱机密码攻击。

对策

由于在配置此值和未配置此值时可能存在漏洞，因此定义了两个不同的对策。 组织应根据确定的威胁和想要缓解的风险来权衡这两者之间的选择。 两个对策选项是：

- 将 “**帐户锁定阈值** ”设置为 0。 此配置可确保帐户不会被锁定，并防止有意尝试锁定帐户的 DoS 攻击。 此配置还有助于减少技术支持呼叫，因为用户不会意外地将自己锁定在其帐户外。 因为它不会防止暴力攻击，因此仅当显式满足以下两个条件时，才应选择此配置：
  - 密码策略设置要求所有用户具有 8 个或更多字符的复杂密码。
  - 在环境中发生一系列登录失败时，将建立可靠的审核机制来提醒管理员。

- 将 **帐户锁定阈值** 策略设置配置为足够高的值，使用户能够在帐户锁定前多次意外错误键入其密码，但请确保暴力密码攻击仍会锁定帐户。

  Windows 安全基线 建议配置 10 次无效登录尝试的阈值，这可以防止意外的帐户锁定并减少技术支持呼叫次数，但不会阻止 DoS 攻击。

  使用此类型的策略必须附带解锁锁定帐户的过程。 每当需要帮助缓解系统受到攻击导致的大规模锁定时，必须能够实施此策略。

潜在影响

如果启用此策略设置，则锁定的帐户在管理员重置或帐户锁定持续时间到期之前不可用。 启用此设置可能会生成更多技术支持呼叫。

如果将 “**帐户锁定阈值** ”策略设置为 0，则如果未建立可靠的审核机制，恶意用户尝试使用暴力破解密码攻击发现密码，则可能无法检测到。

如果将此策略设置配置为大于 0 的数字，攻击者可以轻松锁定帐户名称已知的任何帐户。 考虑到除了访问网络之外，不需要其他凭据来锁定帐户，这种情况尤其危险。

相关主题

帐户锁定策略

在此后重置帐户锁定计数器

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍安全策略设置 **后重置帐户锁定计数器** 的最佳做法、位置、值和安全注意事项。

参考

策略设置 **后重置帐户锁定计数器** 确定在将失败登录尝试计数器重置为 0 之前用户无法登录时必须经过的分钟数。 如果 帐户锁定阈值 设置为大于零的数字，则此重置时间必须小于或等于 帐户锁定持续时间的值。

高设置的缺点是，如果用户因登录错误而超过帐户锁定阈值，则会长时间锁定自己。 用户可能会进行过多的技术支持呼叫。

可能值

- 用户定义的分钟数（从 1 到 99，999）
- 未定义

最佳做法

确定组织的威胁级别，并将其与支持人员对密码重置的支持成本进行平衡。 每个组织都有特定的要求。

Windows 安全基线 建议在策略设置为 15 **后将"重置帐户锁定计数器** "配置为 15，但与其他帐户锁定设置一样，此值与其说是规则或最佳做法，不如说是"一刀切"。有关详细信息，请参阅 配置帐户锁定。

位置

计算机配置\Windows 设置\安全设置\帐户策略\帐户锁定策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	不适用
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	不适用

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果用户多次键入密码错误，可能会意外地锁定自己的帐户。

对策

Windows 安全基线 建议在策略设置为 15 **后配置重置帐户锁定计数器** 。

潜在影响

如果未配置此策略设置，或者如果值配置为间隔太长，攻击者可能会多次尝试登录到每个用户的帐户并锁定其帐户，拒绝服务 (DoS) 攻击可能会成功，或者管理员可能必须手动解锁所有锁定的帐户。 如果将此策略设置配置为合理的值，用户可以在合理的时间内执行新的登录尝试，以在登录失败后进行登录，而不会使暴力攻击在高速上可行。 请确保通知用户用于此策略设置的值，以便他们等待锁定计时器过期，然后再呼叫技术支持。

相关主题

- 帐户锁定策略

Kerberos 策略

项目 • 2023/03/18

适用范围

- Windows 10

介绍 Kerberos 策略设置，并提供指向策略设置说明的链接。

Kerberos 版本 5 身份验证协议提供身份验证服务的默认机制，以及用户访问资源并对该资源执行任务所需的授权数据。 通过缩短 Kerberos 票证的生存期，可以降低合法用户的凭据被盗并被攻击者成功使用的风险。 但是，此票证生存期缩短也会增加授权开销。 在大多数环境中，不应更改这些设置。

这些策略设置位于 **\Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy** 中。

以下主题介绍了实现和最佳做法注意事项、策略位置、服务器类型或 GPO 的默认值、操作系统版本的相关差异、安全注意事项 (包括每个设置) 可能的设置漏洞、可以采取的对策，以及每个设置的潜在影响。

本部分内容

主题	描述
强制执行用户登录限制	介绍 **强制执行用户登录限制** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
服务票证最长寿命	介绍 **服务票证最长生存期** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
用户票证最长寿命	介绍 **用户票证最长生存期** 策略设置的最佳做法、位置、值、策略管理和安全注意事项。
用户票证续订最长寿命	介绍 **用户票证续订最长生存期** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
计算机时钟同步的最大容差	介绍 **计算机时钟同步安全的最大容错** 的最佳做法、位置、值、策略管理和安全注意事项

相关主题

- 配置安全策略设置

强制执行用户登录限制

项目 • 2023/03/18

适用范围

- Windows 10

介绍 **强制执行用户登录限制** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

“**强制用户登录限制**”策略设置确定 Kerberos V5 密钥分发中心 (KDC) 是否根据用户帐户的用户权限策略验证会话票证的每个请求。 验证会话票证的每个请求都是可选的，因为额外的步骤需要时间，并且可能会降低对服务的网络访问速度。

此组策略设置的可能值为：

- 已启用
- 禁用
- 未定义

最佳做法

- 如果禁用此策略设置，用户可能会获得他们无权使用的服务的会话票证。

  建议将 “**强制实施用户登录限制** ”设置为“已启用”。

位置

计算机配置\Windows 设置\安全设置\帐户策略\Kerberos 策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	已启用
默认域控制器策略	未定义

服务器类型或 GPO	默认值
独立服务器默认设置	不适用
DC 有效默认设置	启用
成员服务器有效默认设置	不适用
客户端计算机有效默认设置	不适用

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

组策略

客户端设备将在下一次计划的刷新成功组策略获取新设置。 但要让域控制器立即分配这些新设置，需要gpupdate.exe /force。 在本地设备上，安全配置引擎将在大约五分钟内刷新此设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果禁用此策略设置，用户可能会收到他们不再有权使用的服务的会话票证，因为权限在登录后被删除。

对策

启用 “**强制用户登录限制**” 设置。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- Kerberos 策略

服务票证最长寿命

项目 • 2023/03/18

适用范围

- Windows 10

介绍 **服务票证最长生存期** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

服务票证策略设置的最长生存期确定授予的会话票证可用于访问特定服务的最大分钟数。 该值必须为 10 分钟或更大，并且必须小于或等于 **服务票证最长生存期** 策略设置的值。

此组策略设置的可能值为：

- 用户定义的分钟数（从 10 到 99，999）或 0 (在这种情况下，服务票证不会) 过期。
- 未定义。

如果客户端在请求与服务器的连接时显示过期的会话票证，则服务器将返回错误消息。 客户端必须从 Kerberos V5 KDC 请求新的会话票证。 但是，在对连接进行身份验证后，会话票证是否仍然有效不再重要。 会话票证仅用于对与服务器的新连接进行身份验证。 如果对连接进行身份验证的会话票证在连接期间过期，则正在进行的操作不会中断。

如果此策略设置的值太高，用户可能能够在登录时间之外访问网络资源。 此外，其帐户已被禁用的用户可能可以使用在帐户被禁用之前颁发的有效服务票证继续访问网络服务。 如果该值设置为 0，则服务票证永不过期。

最佳做法

- 建议将 **服务票证的最大生存期** 设置为 **600** 分钟。

位置

计算机配置\Windows 设置\安全设置\帐户策略\Kerberos 策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	600 分钟
默认域控制器策略	未定义
独立服务器默认设置	不适用
DC 有效默认设置	600 分钟
成员服务器有效默认设置	不适用
客户端计算机有效默认设置	不适用

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

此策略设置在域控制器上配置。

组策略

客户端计算机将在下一次计划的刷新成功组策略获取新设置。 但要让域控制器立即分配这些新设置，需要gpupdate.exe /force。 在本地设备上，安全配置引擎将在大约五分钟内刷新此设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果将 “**服务票证的最大生存期**” 设置的值配置为过高，则用户可能能够在登录时间之外访问网络资源。 此外，帐户被禁用的用户可能继续使用在禁用其帐户之前颁发的有效服务票证访问网络服务。

对策

将 **服务票证的最大生存期** 设置为 600 分钟。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- Kerberos 策略

用户票证最长寿命

项目 • 2023/05/25

适用范围

- Windows 10

介绍 **用户票证最长生存期** 策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

用户票证最长生存期策略设置确定可以使用用户票证授予票证) 的最大 (时间（以小时为单位）。 当用户的票证授予票证过期时，必须请求一个新票证，或者必须续订现有票证。

此组策略设置的可能值为：

- 用户定义的小时数（从 0 到 99，999）
- 未定义

如果此策略设置的值太高，则用户可能能够在登录时间之外访问网络资源，或者帐户已被禁用的用户可能能够使用禁用其帐户之前颁发的有效服务票证继续访问网络服务。 如果该值设置为 0，则票证授予票证永不过期。

最佳做法

- 建议将 **用户票证的最大生存期** 设置为 10 小时。

位置

计算机配置\Windows 设置\安全设置\帐户策略\Kerberos 策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	10 小时
默认域控制器策略	未定义

服务器类型或 GPO	默认值
独立服务器默认设置	不适用
域控制器有效默认设置	10 小时
成员服务器有效默认设置	不适用
客户端计算机有效默认设置	不适用

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

此策略设置在域控制器上配置。

组策略

客户端设备将在下一次计划的刷新成功组策略获取新设置。 但要让域控制器立即分配这些新设置，需要gpupdate.exe /force。 在本地计算机上，安全配置引擎将在大约五分钟内刷新此设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果将“**用户票证的最大生存期**”设置的值配置为过高，用户可能能够在登录时间之外访问网络资源。 此外，帐户被禁用的用户可能继续使用在禁用其帐户之前颁发的有效用户

票证访问网络服务。 如果将此值配置为太低，则对 KDC 的票证请求可能会影响 KDC 的性能，并给 DoS 攻击提供机会。

对策

使用 4 到 10 小时之间的值 **配置用户票证的最大生存期** 设置。

潜在影响

从默认值减少此设置可降低票证授予票证用于访问用户无权访问的资源的可能性。 但是，它需要更频繁地向 KDC 请求代表用户授予票证。 大多数 KDC 可以支持 4 小时的值，而没有任何额外的负担。

相关主题

- Kerberos 策略

用户票证续订最长寿命

项目 • 2023/03/18

适用范围

- Windows 10

介绍 **用户票证续订最长生存期** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

“**用户票证续订最长生存期**”策略设置确定 (天) 可以续订用户票证授予票证的时间段。

此组策略设置的可能值为：

- 用户定义的天数（从 0 到 99，999）
- 未定义

最佳做法

- 如果此策略设置的值过高，用户可能能够续订旧用户票证授予票证。 如果值为 0，则票证授予票证永不过期。

  建议将 **用户票证续订的最大生存期** 设置为 7 天。

位置

计算机配置\Windows 设置\安全设置\帐户策略\Kerberos 策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	7 天
默认域控制器策略	未定义
独立服务器默认设置	不适用
域控制器有效默认设置	7 天

服务器类型或 GPO	默认值
成员服务器有效默认设置	不适用
客户端计算机有效默认设置	不适用

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

此策略设置在域控制器上配置。

组策略

客户端设备将在下一次计划的刷新成功组策略获取新设置。 但要让域控制器立即分配这些新设置，需要gpupdate.exe /force。 在本地设备上，安全配置引擎将在大约五分钟内刷新此设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果 “**用户票证续订的最长生存期**” 设置的值过高，则用户可能能够续订旧用户票证。

对策

将 **用户票证续订的最长生存期** 设置为 7 天。

潜在影响

7 (7) 天是默认配置。 更改默认配置是用户便利性和安全性之间的权衡。 较短的时间段要求用户更频繁地向 DC 进行身份验证，但不经常使用 DC 进行身份验证的远程用户可能会被锁定在服务中，直到他们重新进行身份验证。

相关主题

- Kerberos 策略

计算机时钟同步的最大容差

项目 • 2023/03/18

适用范围

- Windows 10

介绍 **计算机时钟同步最大容错** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定 Kerberos V5 在客户端时钟上的时间和提供 Kerberos 身份验证的域控制器上的时间之间的最大时差) (，以分钟为单位。

为了防止“重播攻击”，Kerberos v5 协议使用时间戳作为其协议定义的一部分。 若要使时间戳正常工作，客户端和域控制器的时钟需要尽可能同步。 换句话说，这两个设备必须设置为相同的时间和日期。 由于两台计算机的时钟通常不同步，因此可以使用此策略设置在客户端时钟和域控制器时钟之间建立 Kerberos 协议的最大可接受差异。 如果客户端计算机时钟与域控制器时钟之间的差异小于此策略中指定的最大时差，则两台设备之间的会话中使用的任何时间戳都被视为真实时间戳。

此组策略设置的可能值为：

- 用户定义的分钟数（从 1 到 99，999）
- 未定义

最佳做法

- 建议将 **计算机时钟同步的最大容差** 设置为 5 分钟。

位置

计算机配置\Windows 设置\安全设置\帐户策略\Kerberos 策略

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	5 分钟
默认域控制器策略	未定义
独立服务器默认设置	不适用
域控制器有效默认设置	5 分钟
成员服务器有效默认设置	不适用
客户端计算机有效默认设置	不适用

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

此策略设置在域控制器上配置。

组策略

客户端设备将在下一次计划的刷新成功组策略获取新设置。 但要让域控制器立即分配这些新设置，需要gpupdate.exe /force。 在本地设备上，安全配置引擎将在大约五分钟内刷新此设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

为了防止“重播攻击” (恶意用户或程序重新提交身份验证凭据以获取对受保护资源) 的访问权限的攻击，Kerberos 协议使用时间戳作为其定义的一部分。 若要使时间戳正常工作，需要密切同步客户端计算机和域控制器的时钟。 由于两台计算机的时钟通常不同步，因此管理员可以使用此策略在客户端计算机时钟和域控制器时钟之间建立 Kerberos 协议的最大可接受差异。 如果客户端计算机时钟与域控制器时钟之间的差异小于此设置中指定的最大时差，则两台计算机之间的会话中使用的任何时间戳都被视为真实时间戳。

对策

将 **计算机时钟同步的最大容错** 设置为 5 分钟。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- Kerberos 策略

审核策略

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

提供有关 Windows 中可用的基本审核策略的信息，以及指向每个设置的信息的链接。

安全设置 **\本地策略\审核策略下的安全审核策略** 设置为无法使用高级安全审核策略设置的客户端设备和服务器提供广泛的安全审核功能。

安全设置\本地策略\审核策略下的基本审核策略设置如下：

- 审核帐户登录事件
- 审核帐户管理
- 审核目录服务访问
- 审核登录事件
- 审核对象访问
- 审核策略更改
- 审核特权使用
- 审核进程跟踪
- 审核系统事件

相关主题

- 配置安全策略设置
- 安全审核

安全选项

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍本地 **安全策略的安全选项** 设置以及指向详细信息的链接。

安全选项包含以下安全策略设置分组，可用于配置本地计算机的行为。 其中一些策略可以包含在 组策略 对象中，并在组织中分发。

在设备上本地编辑策略设置时，仅影响该设备的设置。 如果在组策略对象 (GPO) 中配置设置，这些设置将应用于受该 GPO 约束的所有设备。

有关设置安全策略的信息，请参阅 配置安全策略设置。

本部分内容

文章	说明
帐户: 管理员帐户状态	介绍“ **帐户：管理员帐户状态** 安全策略”设置的最佳做法、位置、值和安全注意事项。
帐户: 阻止 Microsoft 帐户	介绍 **帐户：阻止** Microsoft **帐户** 安全策略设置的最佳做法、位置、值、管理和安全注意事项。
帐户: 来宾帐户状态	介绍 “**帐户：来宾帐户状态** ”安全策略设置的最佳做法、位置、值和安全注意事项。
帐户: 使用空密码的本地帐户只允许进行控制台登录	介绍有关**账户：限制使用空密码的本地账户只允许进行控制台登录**安全策略的最佳做法、位置、值和安全注意事项。
帐户: 重命名系统管理员帐户	此安全策略文章面向 IT 专业人员介绍了此策略设置的最佳做法、位置、值和安全注意事项。
帐户: 重命名来宾帐户	介绍“ **帐户：重命名来宾帐户** 安全策略”设置的最佳做法、位置、值和安全注意事项。
审核: 对全局系统对象的访问进行审核	介绍 **审核：审核全局系统对象** 访问安全策略设置的最佳做法、位置、值和安全注意事项。
审核: 对备份和还原权限的使用进行审核	介绍 **审核：审核备份和还原特权安全策略设置的使用情况的** 最佳做法、位置、值和安全注意事项。

文章	说明
审核: 强制审核策略子类别设置（Windows Vista 或更高版本）替代审核策略类别设置	介绍审核的最佳做法、位置、值和安全注意事项 **：强制审核策略子类别设置** (Windows Vista **或更高版本) 替代审核策略类别设置** 安全策略设置。
审核: 如果无法记录安全审核则立即关闭系统	介绍审核的最佳做法、位置、值、管理做法和安全注意事项 **：如果无法记录安全审核安全策略设置，请立即关闭系统** 。
DCOM: 使用安全描述符定义语言(SDDL)语法的计算机访问限制	介绍 DCOM 的最佳做法、位置、值和安全注意事项 **：安全描述符定义语言中的计算机访问限制** (SDDL) **语法** 策略设置。
DCOM: 使用安全描述符定义语言(SDDL)语法的计算机启动限制	介绍 DCOM 的最佳做法、位置、值和安全注意事项 **：安全描述符定义语言中的计算机启动限制** (SDDL) **语法** 安全策略设置。
设备: 允许在未登录的情况下弹出	介绍设备的最佳做法、位置、值和安全注意事项 **：允许注销而无需登录** 安全策略设置。
设备: 允许对可移动媒体进行格式化并弹出	介绍设备的最佳做法、位置、值和安全注意事项 **：允许格式化和弹出可移动媒体** 安全策略设置。
设备: 防止用户安装打印机驱动程序	介绍设备的最佳做法、位置、值和安全注意事项 **：阻止用户安装打印机驱动程序** 安全策略设置。
设备: 将 CD-ROM 的访问权限仅限于本地登录的用户	介绍设备的最佳做法、位置、值和安全注意事项 **：将** CD-ROM **访问限制为仅限本地登录用户** 的安全策略设置。
设备: 将软盘驱动器的访问权限仅限于本地登录的用户	介绍设备的最佳做法、位置、值和安全注意事项 **：将软盘访问限制为仅限本地登录用户** 的安全策略设置。
域控制器: 允许服务器操作者计划任务	介绍域控制器的最佳做法、位置、值和安全注意事项 **：允许服务器操作员计划任务** 安全策略设置。
域控制器: LDAP 服务器签名要求	介绍域控制器的最佳做法、位置、值和安全注意事项 **：**LDAP **服务器签名要求** 安全策略设置。
域控制器: 拒绝计算机帐户密码更改	介绍域控制器的最佳做法、位置、值和安全注意事项 **：拒绝计算机帐户密码更改** 安全策略设置。
域成员: 对安全通道数据进行数字加密或数字签名(始终)	介绍域成员的最佳做法、位置、值和安全注意事项 **：始终) 安全策略设置 (对安全通道数据进行数字加密或签名** 。
域成员: 对安全通道数据进行数字加密(如果可能)	介绍域成员的最佳做法、位置、值和安全注意事项 **：尽可能) 安全策略设置以数字方式加密安全通道数据** (。
域成员: 对安全通道数据进行数字签名(如果可能)	介绍域成员的最佳做法、位置、值和安全注意事项 **：尽可能 () 安全策略设置对安全通道数据进行数字签名** 。
域成员: 禁用计算机帐户密码更改	介绍域成员的最佳做法、位置、值和安全注意事项 **：禁用计算机帐户密码更改** 安全策略设置。

文章	说明
域成员: 计算机帐户密码最长使用期限	介绍 “**域成员：最大计算机帐户密码期限** ”安全策略设置的最佳做法、位置、值和安全注意事项。
域成员: 需要强(Windows 2000 或更高版本)会话密钥	介绍域成员的最佳做法、位置、值和安全注意事项 **：要求强 (Windows 2000 或更高版本) 会话密钥** 安全策略设置。
交互式登录: 锁定会话时显示用户信息	介绍交互式登录的最佳做法、位置、值和安全注意事项 **：在会话锁定安全策略设置时显示用户信息** 。
交互式登录: 不显示上次登录	介绍交互式登录的最佳做法、位置、值和安全注意事项 **：不显示上次登录** 的安全策略设置。
交互式登录: 不显示登录时的用户名	介绍交互式登录的最佳做法、位置、值和安全注意事项 **：不要在登录安全策略设置中显示用户名** 。
交互式登录: 无须按 Ctrl+Alt+Del	介绍交互式登录的最佳做法、位置、值和安全注意事项 **：不需要** CTRL+ALT+DEL 安全策略设置。
交互式登录: 计算机帐户锁定阈值	介绍交互式登录的最佳做法、位置、值、管理和安全注意事项 **：计算机帐户锁定阈值** 安全策略设置。
交互式登录: 计算机不活动限制	介绍交互式登录的最佳做法、位置、值、管理和安全注意事项 **：计算机不活动限制** 安全策略设置。
交互式登录: 试图登录的用户的消息文本	介绍交互式登录的最佳做法、位置、值、管理和安全注意事项 **：尝试登录安全策略设置的用户的消息文本** 。
交互式登录: 试图登录的用户的消息标题	介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：尝试登录安全策略设置的用户的消息标题** 。
交互式登录: 之前登录到缓存的次数(域控制器不可用时)	介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：如果域控制器) 安全策略设置不可用，(以前对缓存的登录次数** 。
交互式登录: 提示用户在过期之前更改密码	介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：提示用户在过期前更改密码** 安全策略设置。
交互式登录: 需要域控制器身份验证以对工作站进行解锁	介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：要求域控制器身份验证才能解锁工作站** 安全策略设置。
交互式登录：需要Windows Hello 企业版或智能卡	介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项：**需要**Windows Hello **企业版或智能卡**安全策略设置。
交互式登录: 智能卡移除行为	介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项：**智能卡删除行为**安全策略设置。
Microsoft 网络客户端：对通信进行数字签名（始终）	介绍 Microsoft 网络客户端的最佳做法、位置、值、策略管理和安全注意事项 **：对通信进行数字签名 (始终)** SMBv3 和 SMBv2 的安全策略设置。

文章	说明
Microsoft 网络客户端: 将未加密的密码发送到第三方 SMB 服务器	介绍 Microsoft 网络客户端的最佳做法、位置、值、策略管理和安全注意事项 **：将未加密的密码发送到第三方 SMB 服务器** 安全策略设置。
Microsoft 网络服务器: 暂停会话前所需的空闲时间数量	介绍 Microsoft 网络服务器的最佳做法、位置、值和安全注意事项 **：暂停会话安全策略设置之前所需的空闲时间量** 。
Microsoft 网络服务器: 尝试使用 S4U2Self 获取声明信息	介绍 Microsoft 网络服务器的最佳做法、位置、值、管理和安全注意事项 **：尝试 S4U2Self 获取声明信息安全** 策略设置。
Microsoft 网络服务器：对通信进行数字签名（始终）	介绍 Microsoft 网络服务器的最佳做法、位置、值、策略管理和安全注意事项 **：对通信进行数字签名 (始终)** SMBv3 和 SMBv2 的安全策略设置。
Microsoft 网络服务器: 登录时间过期后断开与客户端的连接	介绍 Microsoft 网络服务器的最佳做法、位置、值和安全注意事项 **：在登录时间过期时断开客户端连接** 安全策略设置。
Microsoft 网络服务器: 服务器 SPN 目标名称验证级别	介绍 Microsoft 网络服务器的最佳做法、位置和值、策略管理和安全注意事项 **：服务器 SPN 目标名称验证级别** 安全策略设置。
网络访问: 允许匿名 SID/名称转换	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：允许匿名 SID/名称转换** 安全策略设置。
网络访问: 不允许 SAM 帐户的匿名枚举	介绍网络访问的最佳做法、位置、值和安全注意事项 **：不允许匿名枚举 SAM 帐户** 安全策略设置。
网络访问: 不允许 SAM 帐户和共享的匿名枚举	介绍网络访问的最佳做法、位置、值和安全注意事项 **：不允许匿名枚举 SAM 帐户和共享** 安全策略设置。
网络访问: 不允许存储网络身份验证的密码和凭据	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：不允许存储用于网络身份验证安全策略设置的密码和凭据** 。
网络访问: 将 Everyone 权限应用于匿名用户	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：让每个人权限应用于匿名用户** 安全策略设置。
网络访问: 可匿名访问的命名管道	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：可以匿名访问的命名管道** 安全策略设置。
网络访问: 可远程访问的注册表路径	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：远程访问注册表路径** 安全策略设置。
网络访问: 可远程访问的注册表路径和子路径	介绍网络访问的最佳做法、位置、值和安全注意事项 **：远程访问注册表路径和子路径** 安全策略设置。
网络访问：限制匿名访问命名管道和共享	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：限制对命名管道和共享的匿名访问** 安全策略设置。
网络访问：限制允许远程调用 SAM 的客户端	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：限制允许对 SAM 安全策略设置进行远程调用的客户端** 。

文章	说明
网络访问：可匿名访问的共享	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项**：可以匿名访问的共享** 安全策略设置。
网络访问: 本地帐户的共享和安全模型	介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项**：本地帐户安全策略设置的共享和安全模型** 。
网络安全: 允许本地系统将计算机标识用于 NTLM	介绍网络安全的位置、值、策略管理和 **安全注意事项：允许本地系统将计算机标识用于** NTLM 安全策略设置。
网络安全: 允许 LocalSystem NULL 会话回退	介绍 **网络安全：允许** LocalSystem NULL **会话回退** 安全策略设置的最佳做法、位置、值和安全注意事项。
网络安全: 允许对此计算机的 PKU2U 身份验证请求使用联机标识	介绍网络安全的最佳做法、位置和值 **：允许对此计算机的** PKU2U **身份验证请求使用联机标识** 安全策略设置。
网络安全: 配置 Kerberos Win7 仅允许的加密类型	介绍网络安全的最佳做法、位置、值和安全注意事项 **：配置仅** Kerberos Win7 **安全策略设置允许的加密类型** 。
网络安全: 在下一次更改密码时不存储 LAN 管理器哈希值	介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：不要在下一个密码更改安全策略设置中存储** LAN Manager **哈希值** 。
网络安全: 在超过登录时间后强制注销	介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：在登录时间过期时强制注销** 安全策略设置。
网络安全: LAN 管理器身份验证级别	介绍 **网络安全：**LAN Manager **身份验证级别** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
网络安全: LDAP 客户端签名要求	此安全策略参考主题面向 IT 专业人员，介绍了此策略设置的最佳做法、位置、值、策略管理和安全注意事项。 此信息适用于至少运行 Windows Server 2008 操作系统的计算机。
网络安全: 基于 NTLM SSP 的(包括安全 RPC)客户端的最小会话安全	介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：基于** NTLM SSP **的最小会话安全性 (包括安全** RPC) **客户端** 安全策略设置。
网络安全: 基于 NTLM SSP 的(包括安全 RPC)服务器的最小会话安全	介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：基于** NTLM SSP **的最小会话安全性 (包括安全** RPC) **服务器** 安全策略设置。
网络安全: 限制 NTLM: 为 NTLM 身份验证添加远程服务器例外	介绍网络安全的最佳做法、位置、值、管理方面和安全注意事项**：限制** NTLM**：为** NTLM **身份验证安全策略设置添加远程服务器例外** 。
网络安全: 限制 NTLM: 添加此域中的服务器例外	介绍网络安全的最佳做法、位置、值、管理方面和安全注意事项**：限制** NTLM**：在此域安全策略设置中添加服务器例外** 。

文章	说明
网络安全: 限制 NTLM: 审核传入 NTLM 流量	介绍 **网络安全：限制** NTLM：**审核传入** NTLM **流量** 安全策略设置的最佳做法、位置、值、管理方面和安全注意事项。
网络安全: 限制 NTLM: 审核此域中的 NTLM 身份验证	介绍 **网络安全：限制** NTLM：**在此域安全策略设置中审核** NTLM **身份验证** 的最佳做法、位置、值、管理方面和安全注意事项。
网络安全: 限制 NTLM: 传入 NTLM 流量	介绍 **网络安全：限制** NTLM：**传入** NTLM **流量** 安全策略设置的最佳做法、位置、值、管理方面和安全注意事项。
网络安全: 限制 NTLM: 此域中的 NTLM 身份验证	介绍网络安全的最佳做法、位置、值、管理方面和安全注意事项：**在此域安全策略设置中限制** NTLM：NTLM **身份验证** 。
网络安全: 限制 NTLM: 到远程服务器的传出 NTLM 流量	介绍 **网络安全：限制** NTLM：**传出** NTLM **流量到远程服务器** 安全策略设置的最佳做法、位置、值、管理方面和安全注意事项。
恢复控制台: 允许自动管理登录	介绍恢复控制台的最佳做法、位置、值、策略管理和安全注意事项 ：**允许自动管理登录** 安全策略设置。
恢复控制台: 允许软盘复制并访问所有驱动器和所有文件夹	介绍恢复控制台的最佳做法、位置、值、策略管理和安全注意事项 ：**允许软盘复制并访问所有驱动器和文件夹** 安全策略设置。
关闭：允许系统关闭而无需打开 lg	介绍 **关闭：允许系统关闭而无需登录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
关机: 清除虚拟内存页面文件	介绍 **关闭：清除虚拟内存页文件** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。
系统加密: 为计算机上存储的用户密钥强制进行强密钥保护	介绍系统加密的最佳做法、位置、值、策略管理和安全注意事项：**对计算机安全策略设置中存储的用户密钥强制实施强密钥保护** 。
系统加密: 将 FIPS 兼容算法用于加密、哈希和签名	此安全策略参考主题面向 IT 专业人员，介绍了此策略设置的最佳做法、位置、值、策略管理和安全注意事项。
系统对象：非 Windows 子系统不要求区分大小写	介绍系统对象的最佳做法、位置、值、策略管理和安全注意事项：**要求非** Windows **子系统安全策略设置不区分大小写** 。
系统对象: 加强内部系统对象的默认权限(例如，符号链接)	介绍系统对象的最佳做法、位置、值、策略管理和安全注意事项：**加强内部系统对象的默认权限 (例如符号链接)** 安全策略设置。
系统设置: 可选子系统	介绍系统设置的最佳做法、位置、值、策略管理和安全注意事项：**可选子系统** 安全策略设置。
系统设置: 将 Windows 可执行文件中的证书规则用于软件限制策略	介绍系统设置的最佳做法、位置、值、策略管理和安全注意事项：**对软件限制策略安全策略设置使用** Windows **可执行文件上的证书规则** 。
用户帐户控制: 用于内置管理员帐户的管理员批准模式	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项：内置管理员帐户安全策略设置**的管理员审批模式。**

文章	说明
用户帐户控制: 允许 UIAccess 应用程序在不使用安全桌面的情况下提示提升权限	介绍用户帐户控制的最佳做法、位置、值和安全注意事项 **：允许 UIAccess 应用程序在不使用安全桌面安全策略设置的情况下提示提升** 。
用户帐户控制: 管理员批准模式中管理员的提升权限提示行为	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项：**管理员审批模式安全策略设置中管理员的提升提示行为。**
用户帐户控制: 标准用户的提升权限提示行为	介绍 **用户帐户控制：标准用户安全策略设置的提升提示的行为** 的最佳做法、位置、值、策略管理和安全注意事项。
用户帐户控制: 检测应用程序安装并提示提升权限	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：检测应用程序安装并提示提升** 安全策略设置。
用户帐户控制: 只提升签名并验证的可执行文件	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：仅提升经过签名和验证** 的安全策略设置的可执行文件。
用户帐户控制: 仅提升安装在安全位置的 UIAccess 应用程序	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：仅提升安装在安全位置安全策略设置中的 UIAccess 应用程序** 。
用户帐户控制: 以管理员批准模式运行所有管理员	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项：**在管理员审批模式安全策略设置中运行所有管理员。**
用户帐户控制: 提示提升权限时切换到安全桌面	介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：在提示提升安全策略设置时切换到安全桌面** 。
用户帐户控制: 将文件和注册表写入错误虚拟化到每用户位置	介绍 **用户帐户控制：将文件和注册表写入失败虚拟化到每个用户位置** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

相关文章

- 安全策略设置参考
- 安全策略设置

帐户: 管理员帐户状态

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍“ **帐户：管理员帐户状态** 安全策略”设置的最佳做法、位置、值和安全注意事项。

参考

此安全设置确定是启用或禁用本地管理员帐户。

以下条件会阻止禁用管理员帐户，即使禁用此安全设置也是如此。

1. 管理员帐户当前正在使用
2. 管理员组没有其他成员
3. 管理员组的所有其他成员包括：
   a. 禁用
   b. 在本地用户权限分配中列出拒绝登录

如果管理员帐户已禁用，则如果密码不符合要求，则无法启用该帐户。 在这种情况下，管理员组的其他成员必须重置密码。

可能值

- 已启用
- 禁用
- 未定义

默认情况下，此设置在域控制器上 **未定义** ，在独立服务器上 **为“已启用** ”。

最佳做法

- 在某些情况下，禁用管理员帐户可能会成为维护问题。 例如，在域环境中，如果构成连接的安全通道因任何原因而失败，并且没有其他本地管理员帐户，则必须在安全模式下重新启动计算机，以解决中断连接状态的问题。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	禁用

策略管理

在某些情况下，禁用管理员帐户可能会成为维护问题。 组织可能考虑禁用内置管理员帐户的原因包括：

- 对于某些组织来说，定期更改本地帐户的密码可能是一个令人生畏的管理挑战。
- 默认情况下，无论用户登录的失败尝试次数如何，都无法锁定管理员帐户。 帐户的这种开放状态使其成为暴力破解密码猜测攻击的主要目标。
- 此帐户具有已知安全标识符 (SID)。 一些非 Microsoft 工具允许通过指定 SID（而不是帐户名称）通过网络进行身份验证。 此身份验证方法意味着，即使重命名管理员帐户，恶意用户也可能使用 SID 发起暴力攻击。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全模式注意事项

在安全模式下启动设备时，仅当计算机未加入域且没有其他活动的本地管理员帐户时，才会启用禁用的管理员帐户。 在这种情况下，可以使用具有当前管理凭据的安全模式来访问计算机。 如果计算机已加入域，则不会启用禁用的管理员帐户。

如何访问禁用的管理员帐户

可以使用以下方法来访问已禁用的管理员帐户：

- 对于未加入域的计算机：禁用所有本地管理员帐户后，在本地或通过网络) 以安全模式 (启动设备，然后使用该计算机上默认本地管理员帐户的凭据登录。
- 对于已加入域的计算机：使用 psexec 启用默认本地管理员帐户，远程运行 **net user administrator /active： yes** 命令。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

无论内置管理员帐户的登录失败次数如何，都无法锁定，这使得它成为尝试猜测密码的暴力攻击的主要目标。 此外，此帐户具有众所周知的安全标识符 (SID) ，并且有一些非 Microsoft 工具允许使用 SID 而不是帐户名称进行身份验证。 因此，即使重命名管理员帐户，攻击者也可以使用 SID 登录来发起暴力攻击。 如果失败的登录次数超过其配置的最大数目，则属于管理员组成员的所有其他帐户都有锁定帐户的安全措施。

对策

禁用 “**帐户：管理员帐户状态** ”设置，以便在正常系统启动时无法使用内置管理员帐户。 如果很难为本地帐户维护定期密码更改计划，可以禁用内置管理员帐户，而不是依赖常规密码更改来保护它免受攻击。

潜在影响

如果禁用管理员帐户，则在某些情况下可能会出现维护问题。 例如，如果成员计算机与域控制器之间的安全通道因任何原因在域环境中失败，并且没有其他本地管理员帐户，则必须在安全模式下重启，以解决导致安全通道失败的问题。 如果当前管理员密码不符合密码要求，则无法在禁用管理员帐户后启用该帐户。 如果出现这种情况，管理员组的其他成员必须在管理员帐户上设置密码。

相关主题

安全选项

帐户: 阻止 Microsoft 帐户

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **帐户：阻止 Microsoft 帐户** 安全策略设置的最佳做法、位置、值、管理和安全注意事项。

参考

此设置阻止使用 “**设置**” 应用添加 Microsoft 帐户进行单一登录 (SSO) Microsoft 服务和某些后台服务的身份验证，或使用 Microsoft 帐户对其他应用程序或服务进行单一登录。 有关详细信息，请参阅 Microsoft 帐户。

如果启用此设置，则有两个选项：

- **用户无法添加 Microsoft 帐户** 意味着现有连接的帐户仍可以登录到设备 (并显示在登录屏幕上) 。 但是，用户无法使用 “**设置**” 应用来添加新的已连接帐户 (或) 将本地帐户连接到 Microsoft 帐户。
- **用户无法使用 Microsoft 帐户添加或登录** 意味着用户无法添加新的连接帐户 (或将本地帐户连接到 microsoft 帐户) 或通过 “**设置**”使用现有连接帐户。

如果禁用或未配置此策略 (建议) ，用户将能够将 Microsoft 帐户与 Windows 配合使用。

可能值

- 此策略已禁用
- 用户无法添加 Microsoft 帐户
- 用户无法使用 Microsoft 帐户添加或登录

默认情况下，此设置未在域控制器上定义，在独立服务器上禁用。

最佳做法

- 如果客户端计算机上禁用或未配置此策略设置，用户将能够使用其 Microsoft 帐户、本地帐户或域帐户来登录 Windows。 它还使用户能够将本地或域帐户连接到 Microsoft 帐户。 这种连接功能为用户提供了一个方便的选项。

- 如果需要限制组织中 Microsoft 帐户的使用，请单击“ **用户无法添加 Microsoft 帐户** ”设置选项，以便用户无法使用 “**设置**” 应用添加新的已连接帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置、如何实施对策，以及实现对策的可能负面后果。

漏洞

虽然 Microsoft 帐户受密码保护，但它们也有可能在企业外部进行更大的曝光。 此外，如果 Microsoft 帐户的所有者不容易区分，审核和取证将变得更加困难。

对策

通过限制 Microsoft 帐户的使用，在企业中仅需要域帐户。 单击“ **用户无法添加 Microsoft 帐户** ”设置选项，以便用户无法在设备上创建新的 Microsoft 帐户、将本地帐户切换到 Microsoft 帐户或将域帐户连接到 Microsoft 帐户。

潜在影响

在组织中建立对帐户的更大控制可以为你提供更安全的管理功能，包括密码重置过程。

相关主题

安全选项

帐户：来宾帐户状态 - 安全策略设置

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 “**帐户：来宾帐户状态** ”安全策略设置的最佳做法、位置、值和安全注意事项。

参考

“**帐户：来宾帐户状态**”策略设置确定是启用或禁用来宾帐户。 此帐户允许未经身份验证的网络用户以不带密码的来宾身份登录来访问系统。 未经授权的用户可以访问来宾帐户通过网络访问的任何资源。 此特权意味着，任何具有允许访问来宾帐户、来宾组或 Everyone 组的权限的网络共享文件夹都将通过网络进行访问。 这种可访问性可能会导致数据泄露或损坏。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

将 “**帐户：来宾帐户**”**状态** 设置为“已禁用”，以便内置来宾帐户不再可用。 所有网络用户必须进行身份验证，然后才能访问系统上的共享资源。 如果禁用了来宾帐户，并且 “网络访问：本地帐户的共享和安全模型 ”设置为“ **仅限来宾**”，则网络登录（例如 SMB 服务执行的登录）将失败。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

默认来宾帐户允许未经身份验证的网络用户以不带密码的来宾身份登录。 这些未经授权的用户可以访问来宾帐户通过网络访问的任何资源。 此功能意味着，任何具有允许访问来宾帐户、来宾组或 Everyone 组的权限的共享文件夹都可以通过网络进行访问，这可能会导致数据泄露或损坏。

对策

禁用 “**帐户：来宾帐户状态** ”设置，以便无法使用内置来宾帐户。

潜在影响

所有网络用户都必须经过身份验证，然后才能访问共享资源。 如果禁用来宾帐户，并且 “**网络访问：共享和安全模型** ”选项设置为 “**仅来宾**”，则网络登录（例如 Microsoft 网络服务器 (SMB 服务) 执行的登录）将失败。 此策略设置对大多数组织的影响不大，因为它是从 Windows Vista 和 Windows Server 2003 开始的默认设置。

相关主题

安全选项

帐户: 使用空密码的本地帐户只允许进行控制台登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍有关**账户：限制使用空密码的本地账户只允许进行控制台登录**安全策略的最佳做法、位置、值和安全注意事项。

参考

账户：限制适用空密码的本地账户只允许进行控制台登录策略设置确定是否允许具有空密码的本地帐户通过网络服务进行远程交互式登录，如远程桌面服务、Telnet 和文件传输协议 (FTP)。 如果启用此策略设置，则本地帐户必须具有非空密码才能用于从远程客户端执行交互式登录或网络登录。

此策略设置不会影响在控制台以物理方式执行的交互式登录或使用域帐户进行的登录。 使用远程交互式登录的非 Microsoft 应用程序可能会绕过此策略设置。 空密码严重威胁计算机安全，因此应通过公司策略和适当的技术措施禁止使用。 不过，如果能够创建新帐户的用户创建了一个已绕过基于域的密码策略设置的帐户，则该帐户可能具有空密码。 例如，用户可以生成独立的系统，创建一个或多个具有空密码的帐户，然后将计算机加入域。 该具有空密码的本地帐户仍可正常工作。 然后，知道帐户名称的任何人都可以使用具有空密码的帐户登录到系统。

不在物理安全位置的设备应始终对所有本地用户帐户强制实施强密码策略。 否则，对设备具有物理访问权限的任何人都可以使用没有密码的用户帐户登录。 此策略对于便携式设备尤为重要。

如果将此安全策略应用于所有人组，则任何人都将无法通过远程桌面服务登录。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 建议将**账户：限制使用空密码的本地账户只允许进行控制台登录**设为“已启用”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

通过 GPO 分发的策略优先于在加入域的计算机上本地配置的策略设置。 在域控制器上，使用 ADSI 编辑器或 dsquery 命令来确定有效的最小密码长度。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中不包含此策略，则可以使用本地安全策略管理单元在本地设备上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

空密码严重威胁计算机安全，因此应通过公司策略和适当的技术措施禁止使用。 从 Windows Server 2003 起，Active Directory 域的默认设置需要至少 7 个字符的复杂密码，而从 Windows Server 2008 开始，将需要至少 8 个字符。 但是，如果能够创建新帐户的用户绕过基于域的密码策略，则可以创建使用空密码的账户。 例如，用户可以生成独立计算机，使用空密码创建一个或多个帐户，然后将计算机加入域。 该具有空密码的本地帐户仍可正常工作。 知道这些未受保护帐户之一的名称的任何人都可以使用它进行登录。

对策

启用**帐户：使用空密码的本地帐户只允许进行控制台登录**设置。

潜在影响

无。 此非影响行为是默认配置。

相关主题

安全选项

帐户: 重命名系统管理员帐户

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

此安全策略参考主题面向 IT 专业人员，介绍了此策略设置的最佳做法、位置、值和安全注意事项。

参考

帐户：重命名管理员帐户策略设置确定不同的帐户名称是否与管理员帐户的安全标识符 (SID) 相关联。

由于管理员帐户存在于桌面版 (家庭版、专业版、企业版和教育版) 的所有Windows 10上，因此重命名该帐户会使攻击者稍微难以猜测此用户名和密码组合。

通过为“帐户”指定值来重命名 **管理员帐户：重命名管理员帐户** 策略设置。

可能值

- 用户定义的文本
- 未定义

最佳做法

- 请务必将新帐户名通知有权使用此帐户的用户。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	未定义
独立服务器默认设置	管理员
DC 有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

策略冲突注意事项

无。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中不包含此策略，则可以使用本地安全策略管理单元在本地设备上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

管理员帐户存在于桌面版Windows 10的所有版本上。 如果重命名此帐户，未经授权的人员猜测此特权用户名和密码组合会稍微困难一些。 从 Windows Vista 开始，安装操作系统的人员会指定一个帐户，该帐户是管理员组的第一个成员，并且具有配置计算机的完整权限，因此默认情况下，此对策将应用于新安装。 如果设备从以前版本的 Windows 升级，则保留名称为“管理员”的帐户，并保留以前安装中为该帐户定义的所有权限和特权。

无论攻击者使用错误密码多少次，都无法锁定内置管理员帐户。 此功能使管理员帐户成为尝试猜测密码的暴力攻击的热门目标。 此对策的值会降低，因为此帐户具有已知的 SID，并且有非 Microsoft 工具允许使用 SID 而不是帐户名称进行身份验证。 因此，即使重命名管理员帐户，攻击者也可以使用 SID 登录来发起暴力攻击。

对策

在 “**帐户：重命名管理员帐户** ”设置中指定新名称，以重命名管理员帐户。

潜在影响

必须向有权使用此帐户的用户提供新的帐户名称。 (此设置的指南假定管理员帐户未禁用。)

相关主题

安全选项

帐户：重命名来宾帐户 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍“ **帐户：重命名来宾帐户** 安全策略”设置的最佳做法、位置、值和安全注意事项。

参考

“**帐户：重命名来宾帐户**”策略设置确定不同的帐户名称是否与来宾帐户的安全标识符 (SID) 相关联。

可能值

- *用户定义的文本*
- 来宾

最佳做法

1. 对于不安全位置的设备，重命名帐户会使未经授权的用户更难猜到它。
2. 对于位于安全或受信任位置的计算机，将帐户名称保留为“来宾”可提供设备之间的一致性

位置

计算机配置\Windows 设置\安全设置

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	来宾
默认域控制器策略	来宾
独立服务器默认设置	来宾

服务器类型或 GPO	默认值
DC 有效默认设置	来宾
成员服务器有效默认设置	来宾
客户端计算机有效默认设置	*用户定义的文本*

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中不包含此策略，则可以使用本地安全策略管理单元在本地设备上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

从 Windows Server 2003 和 Windows XP Professional 开始，来宾帐户存在于所有 Windows 服务器和客户端操作系统版本中。 由于帐户名称是众所周知的，因此它为恶意用户提供了访问网络资源并尝试提升权限或安装软件的载体，这些软件可用于以后对系统的攻击。

对策

在 “**帐户：重命名来宾帐户** ”设置中指定新名称，以重命名来宾帐户。 如果重命名此帐户，未经授权的人员猜测此特权用户名和密码组合会稍微困难一些。

潜在影响

应该影响不大，因为默认情况下，来宾帐户在 Windows 2000 Server、Windows Server 2003 和 Windows XP 中处于禁用状态。 对于以后的操作系统，启用策略时 **，将来宾** 作为默认策略。

相关主题

安全选项

审核: 对全局系统对象的访问进行审核

项目 • 2023/05/25

适用范围

- Windows 10

介绍 **审核：审核全局系统对象** 访问安全策略设置的最佳做法、位置、值和安全注意事项。

参考

如果启用此策略设置，当设备创建系统对象（如互斥体、事件、信号灯和 MS-DOS® 设备）时，将应用默认系统访问控制列表 (SACL)。 如果还启用 "审核对象访问 审核"设置，则会审核对这些系统对象的访问。

全局系统对象也称为"基本系统对象"或"基命名对象"，是具有由创建它们的应用程序或系统组件为其分配名称的临时内核对象。 这些对象最常用于同步多个应用程序或复杂应用程序的多个部分。 由于这些对象具有名称，因此这些对象在范围内是全局的，因此对设备上的所有进程可见。 这些对象都具有安全描述符;但通常，它们没有 NULL SACL。 如果启用此策略设置并在启动时生效，则内核会在创建这些对象时为这些对象分配 SACL。

威胁是，如果保护不当，全局可见的命名对象可能由知道对象名称的恶意程序操作。 例如，如果同步对象（如互斥体）具有构造不佳的任意访问控制列表 (DACL)，则恶意程序可能会按名称访问该互斥体，并导致创建它的程序出现故障。 但是，发生这种情况的风险非常低。

启用此策略设置可能会生成大量安全事件，尤其是在繁忙的域控制器和应用程序服务器上。 这可能会导致服务器响应缓慢，并强制安全日志记录大量意义不大的事件。 对全局系统对象的访问进行审核是一项全有或全无事务：无法筛选哪些事件将被记录，哪些不记录。 即使组织具有资源来分析启用此策略设置时生成的事件，也不太可能具有源代码或每个命名对象用途的说明;因此，许多组织不太可能从启用此策略设置中受益。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 使用高级安全审核策略选项“高级安全审核策略设置\对象访问中的审核 内核对象”，以减少生成的不相关的审核事件数。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

当本地保存或通过组策略分发此策略的更改时，需要重启计算机，然后此策略才会生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

审计

若要审核访问全局系统对象的尝试，可以使用以下两个安全审核策略设置之一：

- 高级安全审核策略设置\对象访问中的审核内核对象

- "安全 设置"\"本地策略"\"审核策略"下的"审核对象访问"

如果可能，请使用"高级安全审核策略"选项来减少生成的不相关的审核事件数。

如果配置了 "审核内核对象" 设置，则会生成以下事件：

事件 ID	事件消息
4659	请求对象的句柄，意图删除。
4660	对象已删除。
4661	请求了对象的句柄。
4663	尝试访问对象。

如果配置了 "审核对象访问" 设置，则会生成以下事件：

事件 ID	事件消息
560	已授予对现有对象的访问权限。
562	对象的句柄已关闭。
563	尝试打开对象，意图将其删除。 **注意：** 当在 Createfile () 中指定FILE_DELETE_ON_CLOSE标志时，文件系统会使用此标志
564	已删除受保护的对象。
565	已向现有对象类型授予访问权限。
567	使用了与句柄关联的权限。 **注意：** 使用某些授予的权限创建句柄，（读取、写入等）。 使用句柄时，将为每个使用的权限生成最多一个审核。
569	授权管理器中的资源管理器尝试创建客户端上下文。
570	客户端尝试访问对象。 **注意：** 将为对象上的每次尝试操作生成事件。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果保护不当，全局可见的命名对象可能会被恶意软件使用对象名称来操作。 例如，如果同步对象（如互斥体）的任意访问控制列表 (DACL) 选择不当，则恶意软件可能会按名称访问该互斥体，并导致创建它的程序出现故障。 但是，发生此类事件的风险非常低。

对策

启用 “**审核：审核全局系统对象的访问权限** ”设置。

潜在影响

如果启用 “**审核：审核全局系统对象的访问权限** ”设置，可能会生成大量安全事件，尤其是在繁忙的域控制器和应用程序服务器上。 这种情况可能会导致服务器响应缓慢，并强制安全日志记录许多意义不大的事件。 只能启用或禁用此策略设置，无法从此设置中选择记录的事件。 即使是具有分析此策略设置生成的事件的资源的组织也不太可能具有源代码或每个命名对象的用途说明。 因此，大多数组织不太可能通过启用此策略设置而受益。 若要减少生成的审核事件数，请使用高级审核策略。

相关主题

- 安全选项

审核: 对备份和还原权限的使用进行审核

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **审核：审核备份和还原特权安全策略设置的使用情况的** 最佳做法、位置、值和安全注意事项。

参考

“**审核：审核备份和还原”权限使用**策略设置确定在配置“**审核权限**使用”策略设置时，是否审核所有用户权限（包括备份和还原）的使用。 启用这两个策略设置会为每个备份或还原的文件生成审核事件。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 将 “**审核：审核备份和还原”权限的使用** 设置为“已禁用”。 启用此策略设置可能会生成大量安全事件，这可能会导致服务器响应缓慢，并强制安全事件日志记录大量意义不大的事件。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

审计

启用此策略设置与 “**审核特权**”**使用** 策略设置将记录安全日志中正在行使的任何用户权限实例。 如果启用了 **审核特权使用** ，但 **审核：审核备份和还原权限的使用** 已禁用，则当用户备份或还原用户权限时，不会审核这些事件。

启用 “**审核特权使用** 策略”设置时启用此策略设置会为每个备份或还原的文件生成审核事件。 此设置可帮助你跟踪意外或恶意以未经授权的方式还原数据的管理员。

或者，可以使用高级审核策略 “审核敏感权限使用”，这有助于管理生成的事件数。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

使用备份和还原功能时，它会创建与备份目标相同的文件系统副本。 定期备份和还原卷是事件响应计划的重要组成部分。 但是，恶意用户可能会使用合法的备份副本来获取对信息的访问权限或模拟合法的网络资源来危害企业。

对策

启用 “**审核：审核备份和还原**”**权限的使用** 设置。 或者，通过配置 AutoBackupLogFiles 注册表项来实现自动日志备份。 如果在还启用 “审核权限使用 ”设置时启用此选项，则会为备份或还原的每个文件生成审核事件。 此信息可帮助你识别用于以未经授权的方式意外或恶意还原数据的帐户。 有关配置此密钥的详细信息，请参阅 事件日志密钥。

潜在影响

如果启用此策略设置，可能会生成大量安全事件，这可能会导致服务器响应缓慢，并强制安全事件日志记录许多意义不大的事件。 如果增加安全事件日志大小以减少系统关闭的可能性，则过大的日志文件可能会影响系统性能。

相关主题

- 安全选项

审核: 强制审核策略子类别设置（Windows Vista 或更高版本）替代审核策略类别设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍审核的最佳做法、位置、值和安全注意事项 **：强制审核策略子类别设置 (Windows Vista 或更高版本) 替代审核策略类别设置** 安全策略设置。

参考

可以使用审核策略子类别以更精确的方式管理审核策略。

有 40 多个审核子类别提供有关设备上活动的精确详细信息。 有关这些子类别的信息，请参阅 高级安全审核策略设置。

可能值

- 已启用
- 禁用

最佳做法

- 使设置保持启用状态。 此“已启用”状态有助于审核类别级别的事件，而无需修改策略。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

审计

若要使用子类别管理审核策略，而无需更改组策略，SCENoApplyLegacyAuditPolicy 注册表值会阻止从组策略和本地安全策略管理工具应用类别级审核策略。

如果此处设置的类别级别审核策略与当前生成的事件不一致，则原因可能是设置了此注册表项。

命令行工具

可以使用auditpol.exe从命令提示符显示和管理审核策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

在 Windows Vista 中引入审核子类别之前，很难在每系统或按用户级别跟踪事件。 较大的事件类别创建过多事件，因此很难找到需要审核的关键信息。

对策

根据需要启用审核策略子类别以跟踪特定事件。

潜在影响

如果在通过命令行工具启用此设置后，尝试使用 组策略 修改审核设置，则会忽略组策略审核设置，转而使用自定义策略设置。 若要使用 组策略 修改审核设置，必须先禁用 **SCENoApplyLegacyAuditPolicy** 密钥。

> **重要：** 对于可能会生成大量流量的审核设置，请非常谨慎。 例如，如果为所有 Privilege Use 子类别启用成功或失败审核，则生成的大量审核事件可能会使在安全事件日志中查找其他类型的条目变得困难。 此类配置也可能对系统性能产生重大影响。

相关主题

- 安全选项

审核: 如果无法记录安全审核则立即关闭系统

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍审核的最佳做法、位置、值、管理做法和安全注意事项 **：如果无法记录安全审核安全策略设置，请立即关闭系统** 。

参考

审核：如果无法记录安全审核，则立即关闭系统策略设置确定系统在无法记录安全事件时是否关闭。 此策略设置是受信任的计算机系统评估条件 (TCSEC) -C2 和通用条件认证的要求，以防止在审核系统无法记录这些事件时发生可审核事件。 Microsoft 已选择通过停止系统并在审核系统出现故障时显示“停止”消息来满足此要求。 如果出于任何原因无法记录安全审核，则启用此策略设置将停止系统。 通常，当安全审核日志已满时，无法记录事件，并且 **安全日志的 Retention 方法** 的值为 “**不覆盖事件 (手动清除日志)** 或 **按天覆盖事件**。

使用 **审核：如果无法记录安全审核** 设置为 “**已启用**”，则立即关闭系统，如果安全日志已满且无法覆盖现有条目，则会出现以下停止消息：

停止：C0000244 {Audit Failed}：尝试生成安全审核失败。

若要恢复，必须登录， (可选) 存档日志，清除日志，并根据需要重置此选项。

如果计算机无法将事件记录到安全日志中，在发生安全事件后，关键证据或重要的故障排除信息可能无法查看。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 根据安全审核要求，可以启用 “**审核：如果无法记录安全审核，请立即关闭系统** ”设置，以确保捕获安全审核信息以供审阅。 但是，启用此设置会增加记录的事件数。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。 启用此策略设置的管理负担可能很高，尤其是在同时 **将安全日志的保留方法** 设置为“ **不覆盖事件 (手动清除日志)** 的情况下。 此设置会 (备份操作员可能会拒绝备份或还原数据) 为拒绝服务威胁，因为如果服务器因登录事件和其他写入安全日志的安全事件而不知所措，服务器可能会被迫关闭。 此外，由于关闭不正常，因此可能会对操作系统、应用程序或数据造成无法弥补的损害。 尽管 NTFS 文件系统将保证在系统突然关闭期间将保持文件系统的完整性，但无法保证在系统重启时，每个应用程序的每个数据文件仍将处于可用状态。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

修改此设置可能会影响与客户端、服务和应用程序的兼容性。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果计算机无法将事件记录到安全事件日志中，在发生安全事件后，关键证据或重要的故障排除信息可能无法进行查看。 此外，攻击者可能会生成大量安全事件日志事件，以故意强制关闭。

对策

启用 “**审核：如果无法记录安全审核**”**设置，请立即关闭系统** ，以确保捕获安全审核信息以供审阅。

潜在影响

如果启用此策略设置，则管理负担可能很大，尤其是同时 **将安全日志的保留方法** 配置为 “**不覆盖事件** (手动清除日志) 。 此配置会导致否认威胁， (备份操作员可能会拒绝备份或还原数据) 成为拒绝服务 (DoS) 漏洞，因为服务器可能会因登录事件和写入安全事件日志的其他安全事件而被迫关闭。 此外，由于关闭是突然的，因此可能会对操作系统、应用程序或数据造成无法弥补的损害。 尽管 NTFS 文件系统在发生此类计算机关闭时保持其完整性，但不能保证在设备重启时，每个应用程序的每个数据文件仍将处于可用状态。

相关主题

- 安全选项

DCOM: 使用安全描述符定义语言(SDDL)语法的计算机访问限制

项目 • 2023/03/18

适用范围

- Windows 10

介绍 DCOM 的最佳做法、位置、值和安全注意事项 **：安全描述符定义语言中的计算机访问限制 (SDDL) 语法** 策略设置。

参考

通过此策略设置，可以定义其他计算机范围的控件，这些控件控制对设备上基于 DCOM) 的所有分布式组件对象模型 (。 这些控制限制设备上的调用、激活或启动请求。 考虑这些访问控制的一种简单方法是，在每次调用、激活或启动任何基于 COM 的服务器时，针对设备范围的访问控制列表 (ACL) 执行额外的访问检查。 如果访问检查失败，调用、激活或启动请求将被拒绝。 (此检查是针对特定于服务器的 ACL 运行的任何访问检查的补充。) 实际上，它提供了访问任何基于 COM 的服务器必须传递的最低授权标准。 此策略设置控制访问权限，以涵盖呼叫权限。

这些设备范围的 ACL 提供了一种方法来替代应用程序通过 CoInitializeSecurity 函数或特定于应用程序的安全设置指定的弱安全设置。 它们提供必须通过的最低安全标准，而不管特定服务器的设置如何。

这些 ACL 还为管理员提供了一个集中位置，用于设置适用于设备上所有基于 COM 的服务器的常规授权策略。

此策略设置允许你以两种不同的方式指定 ACL。 可以在 SDDL 中键入安全描述符，也可以向用户和组授予或拒绝本地访问和远程访问权限。 建议使用内置用户界面来指定要与此设置一起应用的 ACL 内容。 默认 ACL 设置因你运行的 Windows 版本而异。

可能值

- 组和特权的 SDDL 表示形式的*用户定义的输入*

  指定要授予权限的用户或组时，安全描述符字段将填充这些组和特权的安全描述符定义语言表示形式。 可以向用户和组授予本地访问和远程访问的显式“允许”或“拒绝”权限。

- 空

此值表示本地安全策略如何删除策略强制密钥。 此值删除策略，然后将其设置为“未定义”。 通过使用 ACL 编辑器清空列表，然后按“确定”来设置 Blank 值。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	空
默认域控制器策略	空
独立服务器默认设置	空
DC 有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

由于启用 DCOM：**安全描述符定义语言中的计算机访问限制** (SDDL) **语法** 策略设置，在配置此策略设置时，注册表设置优先于以前的注册表设置。 远程过程调用 (RPC) 服务检查“策略”部分中的新注册表项是否存在计算机限制，并且这些注册表项优先于 OLE 下的现有注册表项。 此优先级意味着以前现有的注册表设置不再有效，如果对现有设置进行更改，则不会更改用户的设备访问权限。 在配置用户和组列表时要小心谨慎。

如果由于 Windows 操作系统中的 DCOM 更改而拒绝管理员访问 DCOM 应用程序的权限，则管理员可以使用 **安全描述符定义语言中的 DCOM：计算机访问限制** (SDDL) **语法**

策略设置来管理对计算机的 DCOM 访问。 管理员可以使用此设置指定哪些用户和组可以本地和远程访问计算机上的 DCOM 应用程序。 此设置会将 DCOM 应用程序的控制还原给管理员和用户。 若要定义此设置，请在 **安全描述符定义语言中打开**“**DCOM：计算机访问限制**” **(SDDL) 语法** 设置，然后单击“ **编辑安全性**”。 指定要包含的用户或组，以及这些用户或组的计算机访问权限。 此信息定义 设置并设置相应的 SDDL 值。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

例如，许多 COM 应用程序包括一些特定于安全性的代码（，例如，调用 CoInitializeSecurity），但它们使用允许未经身份验证访问进程的弱设置。 管理员无法在不修改应用程序的情况下重写这些设置，以在早期版本的 Windows 中强制增强安全性。 攻击者可能会尝试通过 COM 调用攻击单个应用程序中的弱安全性。

此外，COM 基础结构包括远程过程调用服务 (RPCSS)，这是在计算机启动期间和之后运行的系统服务。 此服务管理 COM 对象和正在运行的对象表的激活，并为 DCOM 远程处理提供帮助程序服务。 它公开可远程调用的 RPC 接口。 由于某些基于 COM 的服务器允许未经身份验证的远程访问，因此任何人都可以调用这些接口，包括未经身份验证的用户。 因此，RPCSS 可能会受到使用远程、未经身份验证的计算机的恶意用户的攻击。

对策

若要保护单个基于 COM 的应用程序或服务，请将 **安全描述符定义语言中的 DCOM：计算机访问限制 (SDDL) 语法** 设置设置为适当的设备范围的 ACL。

潜在影响

Windows 在安装默认 COM ACL 时实现它们。 从默认值修改这些 ACL 可能会导致某些使用 DCOM 进行通信的应用程序或组件失败。 如果实现基于 COM 的服务器并覆盖默认安全设置，请确认 ACL 分配的应用程序特定调用权限是否为相应用户的正确权限。 否则，必须更改特定于应用程序的权限 ACL，以便为适当的用户提供激活权限，以便使用 DCOM 的应用程序和 Windows 组件不会失败。

相关主题

- 安全选项

DCOM: 使用安全描述符定义语言(SDDL)语法的计算机启动限制

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 DCOM 的最佳做法、位置、值和安全注意事项 **：安全描述符定义语言中的计算机启动限制 (SDDL) 语法** 安全策略设置。

参考

此策略设置类似于 安全描述符定义语言中的 DCOM：计算机访问限制 (SDDL) 语法 设置，因为它允许你定义更多计算机范围的控件，以控制对设备上所有基于 DCOM 的应用程序的访问。 但是，此策略设置中指定的 ACL 控制本地和远程 COM 启动请求 (无法访问设备上的) 请求。 考虑此访问控制的一种简单方法是，在每次启动任何基于 COM 的服务器时针对设备范围的 ACL 执行额外的访问检查。 如果访问检查失败，调用、激活或启动请求将被拒绝。 (此检查是针对特定于服务器的 ACL 运行的任何访问检查的补充。) 实际上，它提供了启动任何基于 COM 的服务器必须传递的最低授权标准。 安全描述符定义语言中的 DCOM：计算机访问限制 (SDDL) 语法策略设置的不同之处在于，它提供应用于尝试访问已启动的基于 COM 的服务器的最低访问检查。

这些设备范围的 ACL 提供了一种替代应用程序通过 CoInitializeSecurity 或特定于应用程序的安全设置指定的弱安全设置的方法。 它们提供必须通过的最低安全标准，而不管特定基于 COM 的服务器的设置如何。 这些 ACL 为管理员提供了一个集中位置，用于设置适用于所有基于 COM 的服务器的常规授权策略。 **安全描述符定义语言 (SDDL) 语法设置中的 DCOM：计算机启动限制**允许通过两种方式指定 ACL。 可以在 SDDL 中键入安全描述符，也可以向用户和组授予或拒绝本地访问和远程访问权限。 建议使用内置用户界面来指定要与此设置一起应用的 ACL 内容。 默认 ACL 设置因你运行的 Windows 版本而异。

可能值

- 空

  此值表示本地安全策略如何删除策略强制密钥。 此值删除策略，然后将其设置为“未定义”。 通过使用 ACL 编辑器清空列表，然后按“确定”来设置 Blank 值。

- 组和特权的 SDDL 表示形式的*用户定义的输入*

  指定要授予权限的用户或组时，安全描述符字段将填充这些组和特权的安全描述符定义语言表示形式。 可以向用户和组授予本地访问和远程访问的显式“允许”或“拒绝”权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	空
默认域控制器策略	空
独立服务器默认设置	空
DC 有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

由于此策略而创建的注册表设置优先于此区域中以前的注册表设置。 远程过程调用 (RPC) 服务 (RpcSs) 检查“策略”部分中的新注册表项，了解计算机限制;这些条目优先于 OLE 下的现有注册表项。

如果由于 Windows 操作系统中对 DCOM 所做的更改而被拒绝访问激活和启动 DCOM 应用程序，则此策略设置可用于控制 DCOM 激活和启动到设备。

可以使用 DCOM **：安全描述符定义语言中的计算机启动限制 (SDDL) 语法** 策略设置，指定哪些用户和组可以在本地和远程启动和激活设备上的 DCOM 应用程序。 此设置将 DCOM 应用程序的控制还原给管理员和指定用户。 若要定义此设置，请打开 “**安全描述符定义语言中的 DCOM：计算机启动限制 (SDDL) 语法** 设置”，然后单击“ **编辑安全性**”。 指定要包含的组以及这些组的设备启动权限。 此信息定义 设置并设置相应的 SDDL 值。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

例如，许多 COM 应用程序包括一些特定于安全性的代码 (，例如，调用 CoInitializeSecurity) ，但它们使用允许未经身份验证访问进程的弱设置。 如果不修改应用程序，则无法重写这些设置以强制在早期版本的 Windows 中增强安全性。 攻击者可能会尝试通过 COM 调用攻击单个应用程序中的弱安全性。

此外，COM 基础结构包括远程过程调用服务 (RPCSS) ，这是一种在计算机启动期间运行且始终在启动后运行的系统服务。 此服务管理 COM 对象和正在运行的对象表的激活，并为 DCOM 远程处理提供帮助程序服务。 它公开可远程调用的 RPC 接口。 由于某些基于 COM 的服务器允许未经身份验证的远程组件激活，因此任何人都可以调用这些接口，包括未经身份验证的用户。 因此，使用未经身份验证的远程计算机，恶意用户可能会攻击 RPCSS。

对策

若要保护单个基于 COM 的应用程序或服务，请将此策略设置设置为适当的计算机范围的 ACL。

潜在影响

Windows 在安装默认 COM ACL 时实现它们。 从默认值修改这些 ACL 可能会导致某些使用 DCOM 进行通信的应用程序或组件失败。 如果实现基于 COM 的服务器并覆盖默认安全设置，请确认 ACL 分配的特定于应用程序的启动权限包括对相应用户的激活权限。 否则，必须更改特定于应用程序的启动权限 ACL，以便为适当的用户提供激活权限，以便使用 DCOM 的应用程序和 Windows 组件不会失败。

相关主题

- 安全选项

设备: 允许在未登录的情况下弹出

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍设备的最佳做法、位置、值和安全注意事项 **：允许注销而无需登录** 安全策略设置。

参考

此策略设置启用或禁用用户无需登录即可从扩展坞中删除便携式设备的功能。 如果启用此策略设置，用户可以按固定的便携式设备的物理弹出按钮安全地取消停靠设备。 如果禁用此策略设置，用户必须登录才能接收取消停靠设备的权限。 只有具有 “**从扩展坞中删除计算机**” 权限的用户才能获得此权限。

> **注意：** 禁用此策略设置只会降低无法机械取消停靠的便携式设备的失窃风险。 用户可以物理删除可机械取消停靠的设备，无论他们是否使用 Windows 取消停靠功能。

启用此策略设置意味着对已放置在扩展坞中的设备具有物理访问权限的任何人都可以删除计算机并可能篡改计算机。 对于没有扩展坞的设备，此策略设置没有影响。 但是，对于在办公室时通常停靠的移动计算机的用户，此策略设置将有助于降低设备被盗或恶意用户获得对这些设备的物理访问权限的风险

可能值

- 已启用
- 禁用
- 未定义

最佳做法

建议禁用 “**设备：允许取消停靠而无需登录** ”策略设置。 已停靠其设备的用户必须先登录到本地控制台，然后才能取消连接其系统。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果启用此策略设置，对扩展坞中的便携式计算机具有物理访问权限的任何人都可以删除它们，并可能篡改它们。

对策

禁用 “**设备：允许取消停靠而无需登录** ”设置。

潜在影响

已将设备停靠的用户必须先登录到本地控制台，然后才能取消停靠其计算机。 对于没有扩展坞的设备，此策略设置没有影响。

相关主题

- 安全选项

设备: 允许对可移动媒体进行格式化并弹出

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍设备的最佳做法、位置、值和安全注意事项 ：**允许格式化和弹出可移动媒体** 安全策略设置。

参考

此策略设置确定允许谁格式化和弹出可移动媒体。

用户可以将可移动磁盘移动到具有管理用户权限的其他设备，然后获取任何文件的所有权，为自己分配完全控制权，以及查看或修改任何文件。 配置此策略设置的优势会因大多数可移动存储设备在按下按钮时弹出媒体而减弱。

可能值

- 管理员
- 管理员和高级用户
- 管理员和交互式用户 (不适用于 Windows Server 2008 R2 或 Windows 7 及更高版本)
- 未定义

最佳做法

- 建议将 “**允许**”**设置为格式化可移动媒体并将其弹出** 给 **管理员**。 只有管理员才能弹出 NTFS 格式的可移动媒体。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	管理员
DC 有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

用户可以将可移动磁盘上的数据移到具有管理权限的其他计算机上。 然后，用户可以获取任何文件的所有权，授予自己完全控制权，并查看或修改任何文件。 按下机械按钮时，大多数可移动存储设备弹出媒体会降低此策略设置的优势。

对策

配置 “**设备：允许格式化和弹出可移动媒体** ”设置给 **管理员**。

潜在影响

只有管理员可以格式化和弹出可移动媒体。 如果用户习惯使用可移动媒体进行文件传输和存储，则必须通知他们策略的更改。

相关主题

- 安全选项

设备: 防止用户安装打印机驱动程序

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍设备的最佳做法、位置、值和安全注意事项 **：阻止用户安装打印机驱动程序** 安全策略设置。

参考

若要将设备打印到网络打印机，必须在本地安装该网络打印机的驱动程序。 **设备：阻止用户安装打印机驱动程序**策略设置确定谁可以在添加网络打印机时安装打印机驱动程序。 将值设置为 “**已启用**”时，只有管理员和 Power Users 才能在添加网络打印机时安装打印机驱动程序。 将值设置为 **Disabled** 允许任何用户在添加网络打印机时安装打印机驱动程序。 此设置可防止无特权用户下载和安装不受信任的打印机驱动程序。

如果已配置了用于下载驱动程序的受信任路径，则此设置没有影响。 如果使用受信任的路径，打印子系统将尝试使用受信任路径下载驱动程序。 如果受信任路径下载成功，则代表任何用户安装驱动程序。 如果受信任的路径下载失败，则不会安装驱动程序，也不会添加网络打印机。

尽管在某些组织中，允许用户在自己的工作站上安装打印机驱动程序可能很合适，但这种想法并不适用于服务器。 在服务器上安装打印机驱动程序可能会导致系统不稳定。 只有管理员才应在服务器上拥有此用户权限。 恶意用户可能会故意尝试通过安装不适当的打印机驱动程序来破坏系统。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 建议将 “**设备：阻止用户安装打印机驱动程序**” 设置为“已启用”。 只有“管理”、“Power User”或“服务器操作员”组中的用户才能在服务器上安装打印机。 如果已启用此策略设置，但本地计算机上已存在网络打印机的驱动程序，则用户仍可以添加网络打印机。 此策略设置不会影响用户添加本地打印机的能力。

> **备注**
>
> 应用 2021 年 7 月 6 日更新 后，非管理员（包括委派的管理员组（如打印机操作员）无法将已签名和未签名的打印机驱动程序安装到打印服务器。 默认情况下，只有管理员才能将已签名和未签名的打印机驱动程序安装到打印服务器。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

在某些组织中，允许用户在自己的工作站上安装打印机驱动程序可能很合适。 但是，应仅允许管理员（而不是用户）在服务器上执行此操作，因为在服务器上安装打印机驱动程序可能会无意中导致计算机不稳定。 恶意用户可能会在故意试图损坏计算机时安装不适当的打印机驱动程序，或者用户可能会意外安装伪装成打印机驱动程序的恶意软件。

对策

启用 “**设备：阻止用户安装打印机驱动程序**” 设置。

潜在影响

只有管理员、Power Users 或服务器操作员组的成员才能在服务器上安装打印机。 如果启用此策略设置，但本地计算机上已存在网络打印机的驱动程序，则用户仍可添加网络打印机。

相关主题

- 安全选项

设备: 将 CD-ROM 的访问权限仅限于本地登录的用户

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍设备的最佳做法、位置、值和安全注意事项 **：将 CD-ROM 访问限制为仅限本地登录用户** 的安全策略设置。

参考

此策略设置确定本地用户和远程用户是否可以同时访问 CD。 如果启用此策略设置，则仅允许以交互方式登录的用户访问可移动 CD。 如果启用此策略设置，并且没有人以交互方式登录，则可以通过网络访问 CD。

启用此策略设置的安全优势很小，因为它仅在有人同时登录到系统的本地控制台时阻止网络用户访问驱动器。 此外，CD 驱动器不会自动作为网络共享驱动器提供;必须特意选择共享驱动器。 当管理员安装软件或从 CD-ROM 复制数据，并且不希望网络用户能够执行应用程序或查看数据时，这种共享设置非常重要。

如果启用此策略设置，当任何人登录到服务器的本地控制台时，通过网络连接到服务器的用户将无法使用安装在服务器上的任何 CD 驱动器。 启用此策略设置不适用于充当网络用户的 CD 自动存储盒的系统。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 最佳做法取决于 CD 驱动器的安全和用户可访问性要求。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

远程用户可能会访问包含敏感信息的已装载 CD。 此风险很小，因为 CD 驱动器不会自动作为共享驱动器提供;必须特意选择共享驱动器。 但是，你可以拒绝网络用户从服务器上的可移动媒体查看数据或运行应用程序的能力。

对策

启用 “**设备：将 CD-ROM 驱动器访问限制为仅本地登录用户** ”设置。

潜在影响

当任何人登录到服务器的本地控制台时，通过网络连接到服务器的用户无法使用服务器上安装的任何 CD 驱动器。 需要访问 CD 驱动器的系统工具将失败。 例如，卷影复制服务在初始化时尝试访问计算机上存在的所有 CD 和软盘驱动器，如果服务无法访问其中一个驱动器，则失败。 如果为备份作业指定了卷影副本，则此条件会导致Windows 备份工具失败。 使用卷影副本的任何非 Microsoft 备份产品也会失败。 此策略设置不适用于充当网络用户的 CD 自动存储盒的计算机。

相关主题

- 安全选项

设备: 将软盘驱动器的访问权限仅限于本地登录的用户

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍设备的最佳做法、位置、值和安全注意事项 **：将软盘访问限制为仅限本地登录用户**的安全策略设置。

参考

此策略设置确定本地和远程用户是否可以同时访问可移动软盘。 启用此策略设置仅允许以交互方式登录的用户访问可移动软盘。 如果启用此策略设置，并且没有人以交互方式登录，则可以通过网络访问软盘。

启用此策略设置的安全优势很小，因为它仅在有人同时登录到系统的本地控制台时阻止网络用户访问软盘驱动器。 此外，软盘驱动器不会自动作为网络共享驱动器提供;必须特意选择共享驱动器。 当你从软盘安装软件或复制数据时，这种共享设置变得非常重要，他们不希望网络用户能够执行应用程序或查看数据。

如果启用此策略设置，当有人登录到服务器的本地控制台时，通过网络连接到服务器的用户将无法使用安装在服务器上的任何软盘驱动器。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 最佳做法取决于 CD 驱动器的安全和用户可访问性要求。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

远程用户可能会访问包含敏感信息的已装载软盘。 此风险很小，因为软盘驱动器不会自动共享;管理员必须特意选择共享驱动器。 但是，你可以拒绝网络用户从服务器上的可移动媒体查看数据或运行应用程序的能力。

对策

启用 “**设备：将软盘访问限制为仅本地登录用户** ”设置。

潜在影响

当任何人登录到服务器的本地控制台时，通过网络连接到服务器的用户无法使用设备上安装的任何软盘驱动器。 需要访问软盘驱动器的系统工具会失败。 例如，卷影复制服务在初始化时尝试访问计算机上存在的所有 CD-ROM 和软盘驱动器，如果服务无法访问其中一个驱动器，则会失败。 如果为备份作业指定了卷影副本，则此条件会导致Windows 备份工具失败。 使用卷影副本的任何非 Microsoft 备份产品也会失败。

相关主题

- 安全选项

域控制器: 允许服务器操作者计划任务

项目 • 2023/03/18

适用范围

- Windows Server

介绍域控制器的最佳做法、位置、值和安全注意事项 **：允许服务器操作员计划任务** 安全策略设置。

参考

此策略设置确定服务器操作员是否可以使用 **at** 命令提交作业。 如果启用此策略设置，则服务器操作员通过 **at** 命令创建的作业在运行任务计划程序服务的帐户的上下文中运行。 默认情况下，该帐户是本地系统帐户。

> **注意：** 此安全选项设置仅影响 **at** 命令的计划程序工具。 它不会影响任务计划程序工具。

启用此策略设置意味着服务器操作员通过 **at** 命令创建的作业将在运行该服务的帐户的上下文中执行，默认情况下，即本地系统帐户。 这种与本地帐户的同步意味着服务器操作员可以执行本地系统帐户能够执行的任务，但服务器操作员通常无法执行，例如将其帐户添加到本地管理员组。

对于大多数组织来说，启用此策略设置的影响应该很小。 用户（包括服务器操作员组中的用户）仍可使用任务计划程序向导创建作业，但这些作业将在用户设置作业时用于进行身份验证的帐户上下文中运行。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 此策略的最佳做法取决于任务计划的安全和操作要求。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

命令行工具

at 命令安排在指定时间和日期在计算机上运行的命令和程序。 计划服务必须正在运行才能使用 **at** 命令。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

在本地系统帐户的上下文下运行的任务可能会影响特权级别高于计划任务的用户帐户的资源。

对策

禁用 **域控制器：允许服务器操作员计划任务** 设置。

潜在影响

对于大多数组织来说，影响应该很小。 (包括服务器操作员组中) 的用户仍可以通过任务计划程序管理单元创建作业。 但是，这些作业在用户设置作业时用于进行身份验证的帐户上下文中运行。

相关主题

- 安全选项

域控制器：LDAP 服务器通道绑定令牌要求

项目 • 2023/04/29

适用于:

- Windows Server

本文介绍域控制器的最佳做法、位置、值和安全注意事项 **：LDAP 服务器通道绑定令牌要求** 安全策略设置。

参考

此策略设置确定轻型目录访问协议 (LDAP) 服务器是否需要 LDAP 客户端协商通道绑定 (EPA) 。

未签名/未受保护的网络流量容易受到中间人攻击，其中入侵者捕获服务器和客户端设备之间的数据包，并在转发到客户端设备之前对其进行修改。 在 LDAP 服务器示例中，恶意用户可能导致客户端设备根据 LDAP 目录中的虚假记录做出决策。 可以通过实施强大的物理安全措施来保护网络基础结构来降低企业网络中的风险。 此外，实现 Internet 协议安全性 (IPsec) 身份验证标头模式（为 IP 流量提供相互身份验证和数据包完整性）可能会使所有类型的中间人攻击变得困难。

- 如果通道绑定设置为"始终"，则不支持通道绑定的 LDAP 客户端将被拒绝。
- 如果通道绑定在支持时设置为 ，则只会阻止不正确的通道绑定，并且不支持通道绑定的客户端可以继续通过 LDAP over TLS 进行连接。

使用 SASL 身份验证方法对用户进行身份验证时，CBT 或 EPA 与 TLS 会话一起使用。 SASL 表示使用 NTLM 或 Kerberos 进行用户身份验证。 LDAP 简单绑定 over TLS 不提供通道绑定令牌保护，因此不建议这样做。

可能值

- **从不**：不执行通道绑定验证。 这是所有尚未更新的服务器的行为。
- **支持时**：通过 TLS/SSL 连接进行身份验证时，播发对通道绑定令牌的支持的客户端必须提供正确的令牌;不播发此类支持和/或不使用 TLS/SSL 连接的客户端不受影响。 这是允许应用程序兼容性的中间选项。
- **始终**：所有客户端都必须通过 LDAPS 提供通道绑定信息。 服务器拒绝来自不这样做的客户端的 LDAPS 身份验证请求。

最佳做法

建议将 “**域控制器：LDAP 服务器通道绑定令牌要求** ”设置为 “**始终**”。 不支持 LDAP 通道绑定的客户端将无法对域控制器执行 LDAP 查询。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	无
成员服务器有效默认设置	无
客户端计算机有效默认设置	无

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

未签名/未受保护的网络流量容易受到中间人攻击。 在此类攻击中，入侵者捕获服务器和客户端设备之间的数据包，对其进行修改，然后将其转发到客户端设备。 关于 LDAP 服务器，攻击者可能导致客户端设备根据 LDAP 目录中的虚假记录做出决策。 为了降低组织网络中此类入侵的风险，可以实施强大的物理安全措施来保护网络基础结构。 还可以实现 Internet 协议安全性 (IPsec) 身份验证标头模式，该模式对 IP 流量执行相互身份验证和数据包完整性，使所有类型的中间人攻击变得困难。

对策

将 “**域控制器：LDAP 服务器通道绑定令牌要求** ”设置配置为 “**始终**”。

潜在影响

不支持 LDAP 通道绑定的客户端设备无法对域控制器运行 LDAP 查询。

相关文章

- 安全选项
- 安装 ADV190023 后的 LDAP 会话安全设置和要求
- Windows (KB4520412) 的 2020 LDAP 通道绑定和 LDAP 签名要求
- KB4034879：使用 LdapEnforceChannelBinding 注册表项使通过 SSL/TLS 进行 LDAP 身份验证更安全

域控制器: LDAP 服务器签名要求

项目 • 2023/03/18

适用范围

- Windows Server

本文介绍域控制器的最佳做法、位置、值和安全注意事项 **：LDAP 服务器签名要求** 安全策略设置。

参考

此策略设置确定轻型目录访问协议 (LDAP) 服务器是否需要 LDAP 客户端协商数据签名。

未签名的网络流量容易受到中间人攻击，其中入侵者捕获服务器和客户端设备之间的数据包，并在转发到客户端设备之前对其进行修改。 在 LDAP 服务器示例中，恶意用户可能导致客户端设备根据 LDAP 目录中的虚假记录做出决策。 可以通过实施强大的物理安全措施来保护网络基础结构来降低企业网络中的风险。 此外，实现 Internet 协议安全性 (IPsec) 身份验证标头模式（为 IP 流量提供相互身份验证和数据包完整性）可能会使所有类型的中间人攻击变得困难。

此设置不会影响通过 SSL (LDAP TCP/636) 进行 LDAP 简单绑定。

如果需要签名，则会拒绝不使用 SSL 的 LDAP 简单绑定 (LDAP TCP/389) 。

> **谨慎：** 如果将服务器设置为“需要签名”，则还必须设置客户端设备。 不设置客户端设备会导致与服务器的连接丢失。

可能值

- 无。 与服务器绑定不需要数据签名。 如果客户端计算机请求数据签名，则服务器支持它。
- 需要签名。 除非正在使用传输层安全性/安全套接字层 (TLS/SSL) ，否则必须协商 LDAP 数据签名选项。
- 未定义。

最佳做法

- 建议将 “**域控制器：LDAP 服务器签名要求** ”设置为 “**需要签名**”。 不支持 LDAP 签名的客户端将无法对域控制器执行 LDAP 查询。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	无
成员服务器有效默认设置	无
客户端计算机有效默认设置	无

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

未签名的网络流量容易受到中间人攻击。 在此类攻击中，入侵者捕获服务器和客户端设备之间的数据包，对其进行修改，然后将其转发到客户端设备。 关于 LDAP 服务器，攻击者可能导致客户端设备根据 LDAP 目录中的虚假记录做出决策。 为了降低组织网络中此类入侵的风险，可以实施强大的物理安全措施来保护网络基础结构。 还可以实现

Internet 协议安全性 (IPsec) 身份验证标头模式，该模式对 IP 流量执行相互身份验证和数据包完整性，使所有类型的中间人攻击变得困难。

对策

将 “**域控制器：LDAP 服务器签名要求** ”设置为 “**需要签名**”。

潜在影响

不支持 LDAP 签名的客户端设备无法对域控制器运行 LDAP 查询。

相关主题

- 安全选项

域控制器: 拒绝计算机帐户密码更改

项目 • 2023/03/18

适用范围

- Windows Server

介绍域控制器的最佳做法、位置、值和安全注意事项 **：拒绝计算机帐户密码更改** 安全策略设置。

参考

此策略设置启用或禁用阻止域控制器接受计算机帐户的密码更改请求。 默认情况下，加入域的设备每 30 天更改一次计算机帐户密码。 如果启用，域控制器将拒绝计算机帐户密码更改请求。

可能值

- **启用** 启用此设置后，域控制器无法接受对计算机帐户密码的任何更改。
- **禁用** 禁用此设置后，域控制器可以接受对计算机帐户密码的任何更改。
- **未定义** 与 Disabled 相同。

最佳做法

- 在域中的所有域控制器上启用此策略设置可防止域成员更改其计算机帐户密码。 这种防护反过来又会使这些密码容易受到攻击。 确保此设置符合域的整体安全策略。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

引用的策略配置以下注册表值：

注册表 Hive：HKEY_LOCAL_MACHINE注册表路径：
\System\CurrentControlSet\Services\Netlogon\Parameters\

值名称：RefusePasswordChange

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	不适用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果在域中的所有域控制器上启用此策略设置，则域成员无法更改其计算机帐户密码，并且这些密码更容易受到攻击。

对策

禁用 **域控制器：拒绝计算机帐户密码更改** 设置。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

域成员: 对安全通道数据进行数字加密或数字签名(始终)

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍域成员的最佳做法、位置、值和安全注意事项 **：始终) 安全策略设置 (对安全通道数据进行数字加密或签名** 。

参考

此设置确定域成员发起的所有安全通道流量是否满足最低安全要求。 具体而言，它确定由域成员发起的所有安全通道流量是否都必须进行签名或加密。 无论是否协商所有其他安全通道流量的加密，通过安全通道传输的登录信息始终都是加密的。

以下策略设置确定是否可以使用无法对安全通道流量进行签名或加密的域控制器建立安全通道：

- 域成员: 对安全通道数据进行数字加密或数字签名(始终)
- 域成员: 对安全通道数据进行数字加密(如果可能)
- 域成员: 对安全通道数据进行数字签名(如果可能)

设置 **域成员：以数字方式加密或签名安全通道数据 (始终)** 为 “**启用**” ，可防止与无法对所有安全通道数据进行签名或加密的任何域控制器建立安全通道。

为了保护身份验证流量免受中间人攻击、重播攻击和其他类型的网络攻击，基于 Windows 的计算机通过 NetLogon 创建称为安全通道的信道。 这些通道对计算机帐户进行身份验证。 当远程用户连接到网络资源并且用户帐户存在于受信任的域中时，它们还会对用户帐户进行身份验证。 此身份验证称为直通身份验证，它允许运行已加入域的 Windows 的设备访问其域和任何受信任域中的用户帐户数据库。

若要启用 **域成员： (始终)** 成员工作站或服务器上的策略设置对安全通道数据进行数字加密或签名，成员所属的域中的所有域控制器必须能够对所有安全通道数据进行签名或加密。

启用 **域成员：对安全通道数据进行数字签名或签名 (始终)** 策略设置自动启用 域成员：尽可能) 策略设置对安全通道数据进行数字签名 (。

当设备加入域时，将创建一个计算机帐户。 连接到域后，设备会使用该帐户的密码在每次重启时使用域控制器为其域创建安全通道。 此安全通道用于执行 NTLM 直通身份验证和 LSA SID/名称查找等操作。 对在安全通道上发送的请求进行身份验证，并加密密码等敏感信息，但不会检查通道的完整性，并且并非所有信息都已加密。 如果系统设置为始终加密或签名安全通道数据，则无法使用无法对所有安全通道流量进行签名或加密的域控制器建立安全通道。 如果计算机配置为尽可能加密或签名安全通道数据，则可以建立安全通道，但会协商加密和签名级别。

可能值

- 已启用

  策略 域成员：在可能的情况下对安全通道数据进行数字签名（，无论其当前设置如何，都假定已启用）。 此启用可确保域成员尝试至少对安全通道流量进行签名。

- 禁用

  所有安全通道流量的加密和签名都与域控制器协商，在这种情况下，签名和加密的级别取决于域控制器的版本和以下策略的设置：

  1. 域成员: 对安全通道数据进行数字加密(如果可能)
  2. 域成员: 对安全通道数据进行数字签名(如果可能)

- 未定义

最佳做法

- 将 “**域成员：对安全通道数据进行数字加密或签名” (始终)** 设置为 “**已启用**”。
- 尽可能将 “域成员：对安全通道数据 (进行数字加密”) 设置为 “**已启用**”。
- 将 “域成员：对安全通道数据 (进行数字签名” （ 如果可能 ）) 设置为 “**已启用**”。

> **注意：** 可以启用策略设置 “域成员：尽可能对安全通道数据进行数字加密 () ”和 “域成员：尽可能对安全通道数据进行数字签名” () 支持这些策略设置的域中的所有设备上，而不会影响早期版本的客户端和应用程序。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	已启用
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

通过组策略分发此策略会覆盖本地安全策略设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当设备加入域时，将创建一个计算机帐户。 设备加入域后，每次重启时，都会使用该帐户的密码通过域控制器为其域创建安全通道。 在安全通道上发送的请求已经过身份验证，并加密密码等敏感信息，但不会对通道进行完整性检查，并且并非所有信息都已加密。 如果设备配置为始终加密或签名安全通道数据，但域控制器无法对安全通道数据的任何部分进行签名或加密，则计算机和域控制器无法建立安全通道。 如果设备配置为加密或签名安全通道数据，则可以尽可能建立安全通道，但会协商加密和签名级别。

对策

根据环境选择以下设置之一，将域中的计算机配置为加密或签名安全通道数据。

- **域成员: 对安全通道数据进行数字加密或数字签名(始终)**
- 域成员: 对安全通道数据进行数字加密(如果可能)
- 域成员: 对安全通道数据进行数字签名(如果可能)

潜在影响

安全通道的数字加密和签名是一个好主意，因为安全通道在发送到域控制器时会保护域凭据。

相关主题

- 安全选项

域成员: 对安全通道数据进行数字加密(如果可能)

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍域成员的最佳做法、位置、值和安全注意事项 **：尽可能) 安全策略设置以数字方式加密安全通道数据** (。

参考

此设置确定域成员发起的所有安全通道流量是否满足最低安全要求。 具体而言，它确定是否必须加密域成员发起的所有安全通道流量。 无论是否协商所有其他安全通道流量的加密，通过安全通道传输的登录信息始终都是加密的。

除了此策略设置，以下策略设置还确定是否可以使用无法对安全通道流量进行签名或加密的域控制器建立安全通道：

- 域成员: 对安全通道数据进行数字加密或数字签名(始终)
- 域成员: 对安全通道数据进行数字签名(如果可能)

设置 **域成员：以数字方式加密或签名安全通道数据 (始终)** 为 **“启用”** ，可防止与无法对所有安全通道数据进行签名或加密的任何域控制器建立安全通道。

为了保护身份验证流量免受中间人攻击、重播攻击和其他类型的网络攻击，基于 Windows 的计算机通过 NetLogon 创建称为安全通道的信道。 这些通道对计算机帐户进行身份验证。 当远程用户连接到网络资源并且用户帐户存在于受信任的域中时，它们还会对用户帐户进行身份验证。 此身份验证称为直通身份验证，它允许运行已加入域的 Windows 操作系统的计算机访问其域和任何受信任域中的用户帐户数据库。

启用 域成员：对安全通道数据进行数字签名或签名 (始终) 策略设置自动启用 **域成员：尽可能) 策略设置对安全通道数据进行数字签名** (。

当设备加入域时，将创建一个计算机帐户。 设备加入域后，每次重启时，都会使用该帐户的密码通过域控制器为其域创建安全通道。 此安全通道用于执行 NTLM 传递身份验证和 LSA SID/名称查找等操作。 对在安全通道上发送的请求进行身份验证，并加密密码等敏感信息，但不会检查通道的完整性，并且并非所有信息都已加密。 如果系统设置为始终加密或签名安全通道数据，则无法使用无法对所有安全通道流量进行签名或加密的域控

制器建立安全通道。 如果计算机配置为尽可能加密或签名安全通道数据，则可以建立安全通道，但会协商加密和签名级别。

可能值

- 已启用

  域成员将请求加密所有安全通道流量。 如果域控制器支持对所有安全通道流量进行加密，则将对所有安全通道流量进行加密。 否则，仅加密通过安全通道传输的登录信息。

- 禁用

  域成员不会尝试协商安全通道加密。

  > **注意：** 如果始终启用安全策略设置 “域成员：对安全通道数据进行数字加密或签名 (始终) ”，则会覆盖此设置。

- 未定义

最佳做法

- 将 “域成员：对安全通道数据进行数字加密或签名” (始终) 设置为 “**已启用**”。
- 尽可能将 “**域成员：对安全通道数据 (进行数字加密**”) 设置为 “**已启用**”。
- 将 “域成员：对安全通道数据 (进行数字签名” （ 如果可能 ）) 设置为 “**已启用**”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	已启用
独立服务器默认设置	启用
DC 有效默认设置	启用

服务器类型或 GPO	默认值
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

通过 组策略 分发此策略不会覆盖本地安全策略设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当设备加入域时，将创建一个计算机帐户。 加入域后，设备会在每次重启时使用该帐户的密码通过域控制器为其域创建安全通道。 在安全通道上发送的请求已经过身份验证，并加密密码等敏感信息，但不会对通道进行完整性检查，并且并非所有信息都已加密。 如果设备配置为始终加密或签名安全通道数据，但域控制器无法对安全通道数据的任何部分进行签名或加密，则计算机和域控制器无法建立安全通道。 如果计算机配置为尽可能加密或签名安全通道数据，则可以建立安全通道，但会协商加密和签名级别。

对策

根据环境选择以下设置之一，将域中的计算机配置为加密或签名安全通道数据：

- 域成员: 对安全通道数据进行数字加密或数字签名(始终)
- **域成员: 对安全通道数据进行数字加密(如果可能)**
- 域成员: 对安全通道数据进行数字签名(如果可能)

潜在影响

安全通道的数字签名是一个好主意，因为它可以在将域凭据发送到域控制器时保护这些凭据。

相关主题

- 安全选项

域成员: 对安全通道数据进行数字签名(如果可能)

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍域成员的最佳做法、位置、值和安全注意事项 **：尽可能 () 安全策略设置对安全通道数据进行数字签名** 。

参考

此设置确定域成员发起的所有安全通道流量是否满足最低安全要求。 具体而言，它确定是否必须对域成员发起的所有安全通道流量进行签名。 无论是否协商所有其他安全通道流量的加密，通过安全通道传输的登录信息始终都是加密的。

以下策略设置确定是否可以使用无法对安全通道流量进行签名或加密的域控制器建立安全通道：

- 域成员: 对安全通道数据进行数字加密或数字签名(始终)
- 域成员: 对安全通道数据进行数字加密(如果可能)
- 域成员: 对安全通道数据进行数字签名(如果可能)

设置 域成员：以数字方式加密或签名安全通道数据 (始终) 为 “**启用**” ，可防止与无法对所有安全通道数据进行签名或加密的任何域控制器建立安全通道。

为了保护身份验证流量免受中间人攻击、重播攻击和其他类型的网络攻击，基于 Windows 的计算机通过 NetLogon 创建称为安全通道的信道。 这些通道对计算机帐户进行身份验证。 当远程用户连接到网络资源并且用户帐户存在于受信任的域中时，它们还会对用户帐户进行身份验证。 此身份验证称为直通身份验证，它允许运行已加入域的 Windows 操作系统的计算机访问其域和任何受信任域中的用户帐户数据库。

启用 域成员：对安全通道数据进行数字签名或签名 (始终) 策略设置自动启用 **域成员：尽可能) 策略设置对安全通道数据进行数字签名** (。 当设备加入域时，将创建一个计算机帐户。 设备加入域后，每次重启时，都会使用该帐户的密码通过域控制器为其域创建安全通道。 此安全通道用于执行 NTLM 传递身份验证和 LSA SID/名称查找等操作。 对在安全通道上发送的请求进行身份验证，并加密密码等敏感信息，但不会检查通道的完整性，并且并非所有信息都已加密。 如果系统设置为始终加密或签名安全通道数据，则无法使用

无法对所有安全通道流量进行签名或加密的域控制器建立安全通道。 如果计算机配置为尽可能加密或签名安全通道数据，则可以建立安全通道，但会协商加密和签名级别。

可能值

- 已启用

  域成员将请求对所有安全通道流量进行签名。 如果域控制器支持对所有安全通道流量进行签名，则将对所有安全通道流量进行签名，这可确保在传输过程中不会被篡改。

- 禁用

  除非策略域成员：始终启用），否则不会协商签名：始终启用数字 加密或签名安全通道数据 (。

- 未定义

最佳做法

- 将 “域成员：对安全通道数据进行数字加密或签名” (始终) 设置为 “**已启用**”。
- 尽可能将 “域成员：对安全通道数据 (进行数字加密”) 设置为 “**已启用**”。
- 将 “**域成员：对安全通道数据 (进行数字签名”（ 如果可能 ）**) 设置为 “**已启用**”。

> **注意：** 可以在加入支持这些策略设置的域的所有设备上启用其他两个策略设置： 域成员：尽可能 () 和 **域成员对安全通道数据进行数字签名（（ 如果可能)** ），同时对支持这些策略设置的域的所有设备启用数字加密安全通道数据。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	已启用
独立服务器默认设置	启用

服务器类型或 GPO	默认值
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

通过 组策略 分发此策略不会覆盖本地安全策略设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当设备加入域时，将创建一个计算机帐户。 加入域后，设备会在每次重启时使用该帐户的密码通过域控制器为其域创建安全通道。 在安全通道上发送的请求已经过身份验证，并加密密码等敏感信息，但不会对通道进行完整性检查，并且并非所有信息都已加密。 如果设备配置为始终加密或签名安全通道数据，但域控制器无法对安全通道数据的任何部分进行签名或加密，则计算机和域控制器无法建立安全通道。 如果计算机配置为尽可能加密或签名安全通道数据，则可以建立安全通道，但会协商加密和签名级别。

对策

由于这些策略密切相关且根据环境有用，因此请根据需要选择以下设置之一，以配置域中的设备，以便尽可能加密或签名安全通道数据。

- 域成员: 对安全通道数据进行数字加密或数字签名(始终)

- 域成员: 对安全通道数据进行数字加密(如果可能)
- **域成员: 对安全通道数据进行数字签名(如果可能)**

潜在影响

安全通道的数字签名是一个好主意，因为安全通道在发送到域控制器时会保护域凭据。

相关主题

- 安全选项

域成员: 禁用计算机帐户密码更改

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍域成员的最佳做法、位置、值和安全注意事项 ：**禁用计算机帐户密码更改** 安全策略设置。

参考

域成员：禁用计算机帐户密码更改策略设置确定域成员是否定期更改其计算机帐户密码。 将其值设置为 Enabled 会阻止域成员更改计算机帐户密码。 将其设置为 Disabled 允许域成员更改由域成员的值指定的计算机帐户密码 ：最大计算机帐户密码期限 策略设置，默认情况下每 30 天一次。

默认情况下，属于域的设备需要每隔 30 天自动更改其帐户的密码。 不再能够自动更改其计算机密码的设备面临恶意用户确定系统域帐户密码的风险。 验证 “**域成员：禁用计算机帐户密码更改** ”选项是否设置为 “**已禁用**”。

可能值

- 已启用
- 禁用

最佳做法

1. 不要启用此策略设置。 计算机帐户密码用于在成员和域控制器之间以及域中的域控制器之间建立安全通道通信。 建立后，安全通道将传输做出身份验证和授权决策所需的敏感信息。

2. 请勿使用此策略设置来尝试支持使用相同计算机帐户的双启动方案。 如果要配置加入同一域的双启动安装，请为这两个安装指定不同的计算机名称。 此策略设置已添加到 Windows 操作系统，以帮助存储几个月后投入生产的预生成计算机的组织。 这些设备不必重新加入域。

3. 可以考虑在特定环境中使用此策略设置，例如以下环境：

- 非持久性虚拟桌面基础结构实现。 在此类实现中，每个会话都从只读基础映像启动。
- 对 OS 卷没有写入访问权限的嵌入式设备。

在任一情况下，正常操作期间进行的密码更改都将在会话结束后丢失。 强烈建议你为维护时段计划密码更改。 将密码更改添加到 Windows 在维护时段期间执行的更新和修改。 若要在特定 OS 卷上触发密码更新，请运行以下命令：

```
Nltest /sc_change_pwd:<AD DS domain name>
```

在此命令中， <AD DS 域名> 表示本地计算机的域。 有关维护时段和非持久性 VDI 实现的详细信息，请参阅针对虚拟桌面基础结构的优化Windows 10版本 1803 (VDI) 角色：VDI 优化原则：非持久性 VDI。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	禁用
默认域控制器策略	禁用
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

默认情况下，运行属于域的 Windows Server 的设备每隔特定天数（通常为 30 天）自动更改其帐户的密码。 如果禁用此策略设置，则运行 Windows Server 的设备将保留与其计算机帐户相同的密码。 无法自动更改其帐户密码的设备面临攻击者的风险，攻击者可能会确定计算机域帐户的密码。

对策

验证“**域成员：禁用计算机帐户密码更改**”设置是否配置为“**已禁用**”。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

域成员: 计算机帐户密码最长使用期限

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 “**域成员：最大计算机帐户密码期限** ”安全策略设置的最佳做法、位置、值和安全注意事项。

参考

域成员：最大计算机帐户密码期限策略设置确定域成员何时提交密码更改。

在基于 Active Directory 的域中，每个设备都有一个帐户和密码。 默认情况下，域成员每 30 天提交一次密码更改。 可以延长或缩短此间隔。 此外，可以使用 “**域成员：禁用计算机帐户密码更改** ”策略来完全禁用密码更改要求。 但是，在考虑此选项之前，请查看 域成员：禁用计算机帐户密码更改中所述的含义。

> ⓘ **重要**
>
> 显著增加密码更改间隔 (或禁用密码更改) 使攻击者有更多的时间对其中一个计算机帐户进行暴力破解密码猜测攻击。

有关详细信息，请参阅 计算机帐户密码过程 。

可能值

- 用户定义的天数介于 1 到 999 之间（含）
- 未定义

最佳做法

建议将 “**域成员：最长计算机帐户密码期限** ”设置为大约 30 天。 将该值设置为更少的天数可能会增加复制并影响域控制器。 例如，在 Windows NT 域中，计算机密码每 7 天更改一次。 额外的复制改动会影响具有许多计算机或站点之间链接缓慢的大型组织中的域控制器。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	30 天
DC 有效默认设置	30 天
成员服务器有效默认设置	30 天
客户端计算机有效默认设置	30 天

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

默认情况下，域成员每 30 天提交一次密码更改。 如果延长此间隔，使计算机不再提交密码更改，攻击者将有更多时间来进行暴力攻击来猜测一个或多个计算机帐户的密码。

对策

将 “**域成员：最长计算机帐户密码期限** ”设置为 30 天。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

域成员: 需要强(Windows 2000 或更高版本)会话密钥

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍域成员的最佳做法、位置、值和安全注意事项 **：要求强 (Windows 2000 或更高版本) 会话密钥** 安全策略设置。

参考

“**域成员：需要强 (Windows 2000 或更高版本) 会话密钥**”策略设置确定是否可以使用无法使用 128 位强会话密钥加密安全通道流量的域控制器建立安全通道。 启用此策略设置会阻止使用无法使用强密钥加密安全通道数据的任何域控制器建立安全通道。 禁用此策略设置允许 64 位会话密钥。

应尽可能利用这些更强的会话密钥来帮助保护安全通道通信免受窃听和会话劫持网络攻击。 窃听是一种黑客攻击形式，其中网络数据在传输过程中被读取或更改。 可以修改数据以隐藏或更改发件人的名称，也可以对其进行重定向。

可能值

- 已启用

  在成员工作站或服务器上启用时，成员所属的域中的所有域控制器都必须能够使用 128 位强密钥加密安全通道数据。 此功能意味着所有此类域控制器必须至少运行 Windows 2000 Server。

- 禁用

  允许使用 64 位会话密钥。

- 未定义。

最佳做法

- 建议将 “**域成员：需要强 (Windows 2000 或更高版本) 会话密钥** ”设置为“已启用”。 启用此策略设置可确保所有传出安全通道流量都需要强加密密钥。 禁用此策略设置

需要协商密钥强度。 仅当所有受信任域中的域控制器都支持强密钥时，才启用此选项。 默认情况下，此值处于禁用状态。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

|服务器类型或 GPO

默认值
默认域策略
默认域控制器策略
独立服务器默认设置
DC 有效默认设置
成员服务器有效默认设置
客户端计算机有效默认设置

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

滥用此策略设置是一个常见错误，可能会导致数据丢失或数据访问或安全性问题。

你将能够将不支持此策略设置的设备加入到域控制器启用了此策略设置的域。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

从 Windows 2000 开始，用于在域控制器和成员计算机之间建立安全通道通信的会话密钥要强得多。

应尽可能利用这些更强的会话密钥来帮助保护安全通道通信免受试图劫持网络会话和窃听的攻击。 (窃听是一种黑客攻击形式，其中网络数据在传输过程中被读取或更改。可以修改数据以隐藏或更改发送方，也可以重定向。)

对策

启用 **域成员：需要强 (Windows 2000 或更高版本) 会话密钥** 设置。

如果启用此策略设置，则所有传出安全通道流量都需要强加密密钥。 如果禁用此策略设置，则会协商关键强度。 仅当所有受信任域中的域控制器都支持强密钥时，才应启用此策略设置。 默认情况下，此策略设置处于禁用状态。

潜在影响

不支持此策略设置的设备无法加入域控制器已启用此策略设置的域。

相关主题

- 安全选项

交互式登录: 锁定会话时显示用户信息

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

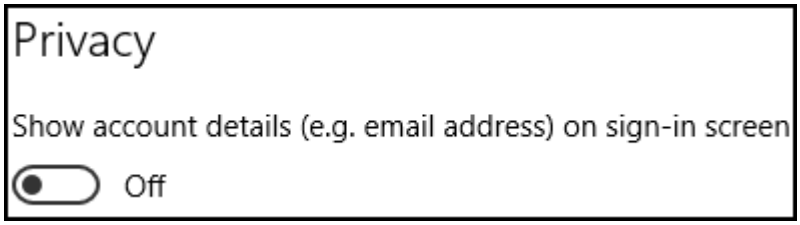
介绍交互式登录的最佳做法、位置、值和安全注意事项 **：在会话锁定安全策略设置时显示用户信息** 。

参考

此安全设置控制登录屏幕上是否与用户名一起显示电子邮件地址或域\用户名等详细信息。 对于运行 Windows 10 版本 1511 和 1507 (RTM) 的客户端，此设置的工作方式与以前版本的 Windows 类似。 但是，由于 Windows 10 版本 1607 中引入了新的**隐私**设置，因此此安全设置对这些客户端的影响不同。

从 Windows 10 版本 1607 开始的更改

从 Windows 10 版本 1607 开始，Windows 10添加了新功能，以默认隐藏用户名详细信息（如电子邮件地址），并能够更改默认值以显示详细信息。 此功能由**设置**>**帐户**>**登录选项**中的新**隐私**设置控制。 默认情况下，“隐私”设置处于关闭状态，这会隐藏详细信息。



交互式登录：在会话锁定时显示用户信息，组策略设置控制相同的功能。

此设置具有以下可能的值：

- **用户显示名称、域和用户名**

  对于本地登录，将显示用户的全名。 如果用户使用 Microsoft 帐户登录，则会显示用户的电子邮件地址。 对于域登录，将显示 domain\username。 此设置与启用 **隐私** 设置的效果相同。

- **仅限用户显示名称**

将显示锁定会话的用户的全名。 此设置与关闭 **隐私** 设置的效果相同。

- **不显示用户信息**

  不显示任何名称。 从 Windows 10 版本 1607 开始，不支持此选项。 如果选择此选项，则会改为显示锁定会话的用户的全名。 此项更改使此设置与新的 **隐私** 设置的功能保持一致。 若要不显示任何用户信息，请启用组策略设置“**交互式登录：不显示上次登录**”。

- **仅限域和用户名**

  仅对于域登录，将显示 domain\username。 **隐私**设置将自动打开并灰显。

- **空白**

  默认设置。 此设置将转换为“未定义”，但它将以与“仅用户显示名称”选项相同的方式 **显示用户全名**。 设置选项后，无法将此策略重置为空白或未定义。

Windows 10版本 1607 的修补程序

运行 Windows 10版本 1607 的客户端不会在登录屏幕上显示详细信息，即使选择了“**用户显示名称、域和用户名**”选项，因为“**隐私**”设置处于关闭状态。 如果“ **隐私**” 设置已打开，将显示详细信息。

无法批量更改客户端的 **隐私** 设置。 相反，将 KB 4013429 应用于运行 Windows 10 版本 1607 的客户端，使其行为与以前版本的 Windows 类似。 运行更高版本的Windows 10的客户端不需要修补程序。

有相关的组策略设置：

- **计算机配置\策略\管理模板\System\Logon\阻止用户在登录时显示帐户详细信息** 会阻止用户在登录屏幕上显示帐户详细信息。
- **计算机配置\Windows 设置\安全设置\本地策略\安全选项\不显示上次登录** 会阻止显示最后一个登录用户的用户名。
- **计算机配置\Windows 设置\安全设置\本地策略\安全选项\在登录时不显示用户名** 会阻止在 Windows 登录时和输入凭据后和桌面显示之前立即显示用户名。

与相关组策略设置交互

对于所有版本的 Windows 10，默认情况下仅显示用户显示名称。

如果启用了“**阻止用户在登录时显示帐户详细信息**”，则无论任何其他组策略设置如何，都只显示用户显示名称。 用户无法显示详细信息。

如果未启用“**阻止用户在登录时显示帐户详细信息**”，则可以设置“**交互式登录**”：**当会话锁定为“用户显示名称”、“域和用户名”**或“**域和用户名**”时显示用户信息，仅显示其他详细信息（如 domain\username）。 在这种情况下，运行Windows 10版本 1607 的客户端需要应用 KB 4013429。 用户无法隐藏其他详细信息。

如果未启用 “**阻止用户在登录时显示帐户详细信息** ”，并且启用了“ **不显示上次登录** ”，则不会显示用户名。

最佳做法

此策略的实现取决于所显示登录信息的安全要求。 如果运行存储敏感数据的计算机（监视器显示在不安全的位置），或者如果计算机具有远程访问的敏感数据，则显示登录用户的全名或域帐户名称可能会与整体安全策略相矛盾。

根据安全策略，可能还需要启用 交互式登录：不显示最后一个用户名 策略。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	**用户显示名称、域和用户名**
成员服务器有效默认设置	**用户显示名称、域和用户名**
客户端计算机上有效的 GPO 默认设置	**用户显示名称、域和用户名**

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当计算机在不安全区域中显示安全桌面时，可通过物理方式或通过远程连接查看监视器的任何人随时获取某些用户信息。 显示的用户信息可能包括域用户帐户名称或锁定会话的用户或上次登录的用户的完整名称。

对策

启用此策略设置后，操作系统可以隐藏某些用户信息，使其在设备启动后或在会话已使用 CTRL+ALT+DEL) 锁定时，在安全桌面 (上显示。 但是，如果使用 **切换用户** 功能，以便为每个登录用户显示登录磁贴，则会显示用户信息。

你可能还需要启用 交互式登录：不显示上次登录 策略，这将阻止 Windows 操作系统显示登录名和上次登录用户的登录磁贴。

相关主题

- 安全选项

交互式登录: 不显示上次登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值和安全注意事项 **：不显示上次登录** 的安全策略设置。 在Windows 10版本 1703 之前，此策略设置名为 **Interactive logon：不显示最后一个用户名。**

参考

此安全策略设置确定安全桌面上是否显示最后一个登录到设备的用户的名称。

如果启用此策略，则安全桌面上不会显示最后一个成功登录用户的全名，也不会显示用户的登录磁贴。 此外，如果使用 “**切换用户**” 功能，则不会显示全名和登录磁贴。 登录屏幕请求限定的域名 (或本地用户名) 和密码。

如果禁用此策略，将显示最后一个登录用户的全名，并显示用户的登录磁贴。 使用 **切换用户** 功能时，此行为相同。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

此策略的实现取决于所显示登录信息的安全要求。 如果你的设备存储敏感数据，监视器显示在不安全的位置，或者如果你的设备具有远程访问的敏感数据，则显示登录用户的全名或域帐户名称可能会与整体安全策略相矛盾。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	禁用
默认域控制器策略	禁用
独立服务器默认设置	禁用
域控制器有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机上有效的 GPO 默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

例如，有权访问控制台的攻击者 (具有物理访问权限的人或可以通过远程桌面会话主机) 连接到设备的人可以查看最后一个登录用户的姓名。 然后，攻击者可以尝试猜测密码、

使用字典或使用暴力攻击来尝试登录。

对策

启用 **交互式登录：不显示最后一个用户名** 设置。

潜在影响

用户在本地登录或登录域时，必须始终键入其用户名和密码。 不会显示所有登录用户的登录磁贴。

相关主题

- 安全选项

交互式登录: 不显示登录时的用户名

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10
- Windows Server 2019

介绍交互式登录的最佳做法、位置、值和安全注意事项 **：不要在登录安全策略设置中显示用户名** 。

参考

从 Windows 10 版本 1703 开始，Windows 10引入了新的策略设置。 此安全策略设置决定是否在登录期间显示用户名。 此设置仅影响 **“其他用户** ”磁贴。

如果已启用策略，并且用户以 **其他用户**身份登录，则登录期间不会显示该用户的全名。 在同一上下文中，如果用户在登录屏幕中键入其电子邮件地址和密码并按 **Enter**，则显示的文本“其他用户”保持不变，并且不再像以前版本的 Windows 10 那样替换为用户的名字和姓氏。 此外，如果用户输入其域用户名和密码并单击“ **提交**”，则在显示“开始”屏幕之前不会显示其全名。

如果禁用策略并且用户以 **其他用户**身份登录，则登录期间，“其他用户”文本将替换为该用户的名字和姓氏。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

此策略的实现取决于所显示登录信息的安全要求。 如果你的设备存储敏感数据，监视器显示在不安全的位置，或者如果你的设备具有远程访问的敏感数据，则显示登录用户的全名或域帐户名称可能会与整体安全策略相矛盾。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机上有效的 GPO 默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

例如，有权访问控制台的攻击者 (具有物理访问权限的人或可以通过远程桌面会话主机) 连接到设备的人可以查看最后一个登录用户的姓名。 然后，攻击者可以尝试猜测密码、使用字典或使用暴力攻击来尝试登录。

对策

启用 **交互式登录：登录时不显示用户名** 设置。

潜在影响

用户在本地登录或登录到域时，必须始终键入其用户名和密码。 不会显示所有登录用户的登录磁贴。

相关主题

- 安全选项

交互式登录: 无须按 Ctrl+Alt+Del

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值和安全注意事项 **：不需要 CTRL+ALT+DEL** 安全策略设置。

参考

此安全设置确定用户登录前是否需要按 Ctrl+ALT+DEL。

如果在设备上启用了此策略设置，则用户无需按 Ctrl+ALT+DEL 即可登录。

如果禁用此策略，则要求任何用户在登录到 Windows 操作系统 (之前按 CTRL+Alt+DEL，除非他们使用智能卡登录) 。

Microsoft 开发了此功能，使具有某些类型物理障碍的用户能够更轻松地登录到运行 Windows 操作系统的设备;但是，无需按 Ctrl+ALT+DELETE 组合键，用户容易受到试图截获其密码的攻击。 在用户登录之前需要 CTRL+Alt+DELETE 可确保用户在输入密码时通过受信任的路径进行通信。

恶意用户可能会安装类似于 Windows 操作系统的标准登录对话框的恶意软件，并捕获用户的密码。 然后，攻击者可以使用该用户拥有的任何级别的用户权限登录到受攻击的帐户。

> ⓘ **备注**
>
> 定义策略后，将创建**位于 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** 中的注册表值 **DisableCAD**。 若要还原此策略所做的更改，将其值设置为“**未定义**”是不够的，还需要删除此注册表值。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 建议将 “**禁用 CTRL+ALT+DEL 登录要求** ”设置为 “**未配置**”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

从 Windows Server 2008 和 Windows Vista 开始，如果禁用此策略，则需要 CTRL+Alt+DELETE 组合键才能进行身份验证。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

此设置使具有某些类型物理障碍的用户能够更轻松地登录到运行 Windows 操作系统的设备。 但是，如果用户不需要按 Ctrl+ALT+DEL，则他们容易受到试图截获其密码的攻击。 如果登录前需要 CTRL+ALT+DEL，则用户密码将通过受信任的路径进行通信。

如果启用此设置，攻击者可能会安装类似于 Windows 操作系统中标准登录对话框的恶意软件，并捕获用户的密码。 然后，攻击者将能够使用用户拥有的任何特权级别登录到受攻击的帐户。

对策

禁用 **交互式登录：不需要** CTRL+ALT+DEL 设置。

潜在影响

除非他们使用智能卡登录，否则用户必须同时按三个键，然后才能显示登录对话框。

相关主题

- 安全选项

交互式登录: 计算机帐户锁定阈值

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值、管理和安全注意事项 **：计算机帐户锁定阈值** 安全策略设置。

参考

从Windows Server 2012和Windows 8开始，**交互式登录：计算机帐户阈值**安全策略设置在启用了 BitLocker 的计算机上强制实施锁定策略，以保护操作系统卷。

使用安全设置，可以为导致使用 BitLocker 锁定设备的失败登录尝试次数设置阈值。 此阈值意味着，如果超过指定的最大登录失败尝试次数，设备将使受信任的平台模块 (TPM) 保护程序以及除 48 位恢复密码以外的任何其他保护程序失效，然后重新启动。 在设备锁定模式下，计算机或设备仅启动到启用触摸的 Windows 恢复环境 (WinRE) ，直到授权用户输入恢复密码以还原完全访问权限。

使用 Ctrl+Alt+Delete 或受密码保护的屏幕保护程序锁定的工作站或成员服务器上的失败密码尝试将计为登录尝试失败。

可能值

可以将 **无效登录尝试** 值设置为 1 到 999。 从 1 到 3 的值被解释为 4。 如果将值设置为 0 或留空，则由于此策略设置，计算机或设备永远不会被锁定。

最佳做法

将此策略设置与其他失败的帐户登录尝试策略结合使用。 例如，如果 “帐户锁定阈值 ”策略设置设置为 4，则将 “**交互式登录：计算机帐户锁定阈值** ”设置为 6 允许用户还原对资源的访问，而无需还原 BitLocker 锁定导致设备的访问。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

需要重启此策略的更改才能在本地保存或通过组策略分发时生效。

组策略

由于此策略设置是在 Windows Server 2012 和 Windows 8 中引入的，因此只能在包含此策略设置的那些设备上本地设置，但可以通过组策略设置和分发到运行支持 组策略 且已启用 BitLocker 的 Windows 操作系统的任何计算机。

设置此策略时，请考虑 帐户锁定阈值 策略设置，该设置确定将导致用户帐户被锁定的失败登录尝试次数。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

此策略设置有助于保护 BitLocker 加密设备免受攻击者试图暴力猜测 Windows 登录密码的侵害。 如果未设置，则攻击者可以尝试使用无数密码，前提是没有其他帐户保护机制。

对策

将此策略设置与其他失败的帐户登录尝试策略结合使用。 例如，如果 “帐户锁定阈值 ”策略设置设置为 4，则将 “**交互式登录：计算机帐户锁定阈值** ”设置为 6 允许用户还原对资源的访问，而无需还原 BitLocker 锁定导致设备的访问。

潜在影响

如果未设置，攻击者可能会使用暴力破解密码破解软件入侵设备。

如果设置得太低，工作效率可能会受到阻碍，因为如果不提供 48 位 BitLocker 恢复密码，被锁定的用户将无法访问设备。

相关主题

- 安全选项

交互式登录: 计算机不活动限制

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值、管理和安全注意事项 **：计算机不活动限制** 安全策略设置。

参考

从Windows Server 2012和Windows 8开始，Windows 使用安全策略设置"交互式登录：计算机非活动限制"来检测登录 (登录) 会话**的用户输入不活动。** 如果非活动时间超过此策略设置的非活动限制，则用户通过调用屏幕保护程序 (屏幕保护程序在目标计算机上) 处于活动状态来锁定会话。 可以通过启用组策略**用户配置\管理模板\控制面板\个性化\启用屏幕保护程序来激活屏幕保护程序。** 此策略设置允许使用 组策略 来控制锁定时间。

> ⓘ **备注**
>
> 如果配置了 "**交互式登录：计算机不活动限制** 安全策略"设置，则设备不仅在非活动时间超过非活动限制时锁定，而且当屏幕保护程序激活或屏幕因电源设置而关闭时也会锁定。

可能值

设备的自动锁定设置为处于非活动状态的运行秒，其范围为 0 (0) 到 599，940 秒 (166.65 小时) 。

如果计算机在设置为 0 (0) **后将被锁定** ，或者没有值 (空白) ，则会禁用策略设置，并且用户登录会话在任何非活动后都不会锁定。

最佳做法

根据设备的使用情况和位置要求设置用户输入处于非活动状态的时间。 例如，如果设备或设备位于公共区域，你可能希望设备在短时间处于非活动状态后自动锁定，以防止未经授权的访问。 但是，如果设备由个人或一组受信任的个人使用，例如在受限的制造区域中，则自动锁定设备可能会降低工作效率。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

在服务器上创建和链接组策略时，计算机配置\策略\Windows 设置\安全设置\本地策略\安全选项) (

默认值

下表列出了此策略的实际和有效的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

需要重启，此策略的更改在本地保存或通过组策略分发时生效。

组策略

由于此策略设置是在 Windows Server 2012 和 Windows 8 中引入的，因此只能在包含此策略设置的计算机本地设置，但可以通过组策略设置和分发到运行支持组策略的 Windows 操作系统的任何计算机。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当当前已登录的用户离开时，此策略设置有助于防止在未刻意锁定桌面的情况下未经授权访问你控制的设备。 在早于 Windows Server 2012 和 Windows 8 的版本中，桌面锁定机制在控制面板个性化设置的单个计算机上设置。

对策

使用安全策略设置“交互式登录：基于设备的使用情况和位置要求 **的计算机不活动限制** ”设置用户输入处于非活动状态的时间。

潜在影响

此安全策略设置可以限制对不安全计算机的未经授权的访问;但是，该要求必须与目标用户的工作效率要求相平衡。

相关主题

- 安全选项

交互式登录: 试图登录的用户的消息文本

项目 • 2023/03/18

适用于：

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值、管理和安全注意事项 **：尝试登录安全策略设置的用户的消息文本** 。

参考

交互式登录：尝试登录的用户的消息文本和交互式登录：尝试登录的用户的消息标题策略设置密切相关。

交互式登录：尝试登录的用户的消息文本 指定要在用户登录时向用户显示的文本消息。

交互式登录：尝试登录的用户的消息标题 指定要显示在包含文本消息的窗口的标题栏中的标题。 此文本通常用于法律原因，例如，警告用户不当使用公司信息的后果，或警告用户其操作可能会受到审核。

配置这些策略设置后，用户将看到一个对话框，然后才能登录到服务器控制台。

可能值

此设置的可能值为：

- 用户定义的文本
- 未定义

最佳做法

- 建议设置 **交互式登录：尝试登录的用户的消息文本** 类似于以下值之一：

    1. 未经适当授权继续是冒犯。
    2. 此系统仅限于授权用户。 尝试未经授权的访问的个人将被起诉。 如果未经授权，请立即终止访问。 单击“确定”以指示你接受此信息。

> ⓘ **重要**

> 标题或文本中显示的任何警告都应得到组织法律和人力资源部门的代表的批准。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍有助于管理此策略的不同要求。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

有两个与登录显示相关的策略设置：

- **交互式登录: 试图登录的用户的消息文本**
- 交互式登录: 试图登录的用户的消息标题

第一个策略设置指定在用户登录时向用户显示的文本消息，第二个策略设置指定文本消息窗口标题栏的标题。 许多组织出于法律目的使用此文本;例如，警告用户滥用公司信息的后果，或警告用户可能对其操作进行审核。

漏洞

用户通常不了解安全做法的重要性。 但是，在登录之前显示警告消息可能有助于防止攻击，方法是在恶意或不知情的用户之前警告其不当行为的后果。 它还可以通过在登录过程中通知员工适当的策略来帮助加强公司策略。

对策

配置 “**交互式登录：尝试登录的用户的消息文本** ”和 “交互式登录”：尝试登录设置的用户的消息标题 ，设置为组织的相应值。

潜在影响

用户可以在登录到服务器控制台之前在对话框中看到一条消息。

相关主题

- 安全选项

交互式登录: 试图登录的用户的消息标题

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：尝试登录安全策略设置的用户的消息标题** 。

参考

此安全设置允许指定显示在窗口标题栏中的标题，其中包含 **交互式登录：尝试登录的用户的消息标题。** 此文本通常用于法律原因，例如，警告用户不当使用公司信息的后果，或警告用户其操作可能受到审核。

交互式登录：尝试登录的用户的消息标题和交互式登录：尝试登录的用户的消息文本策略设置密切相关。 **交互式登录：尝试登录的用户的消息标题** 指定要在用户登录时显示的消息标题。 此文本通常用于法律原因，例如，警告用户不当使用公司信息的后果，或警告用户其操作可能会受到审核。

配置这些策略设置后，用户将在登录服务器控制台之前看到一个对话框。

可能值

- *用户定义的标题*
- 未定义

最佳做法

1. 建议为 **尝试登录的用户设置"交互式登录：消息标题** "的值类似于以下值：

   - 受限系统

     或

   - 警告：此系统仅限于授权用户。

2. 设置策略 交互式登录：尝试登录的用户的消息文本 ，以强化邮件标题的含义。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

有两个与登录显示相关的策略设置：

- 交互式登录: 试图登录的用户的消息文本
- **交互式登录: 试图登录的用户的消息标题**

第一个策略设置指定在用户登录时向用户显示的文本消息，第二个策略设置指定文本消息窗口标题栏的标题。 许多组织出于法律目的使用此文本;例如，警告用户滥用公司信息的后果，或警告用户可能对其操作进行审核。

漏洞

用户通常不了解安全做法的重要性。 但是，在登录之前显示具有相应标题的警告消息可能有助于防止攻击，方法是在恶意用户或未知情的用户之前警告其不当行为的后果。 它还可以通过在登录过程中通知员工适当的策略来帮助加强公司策略。

对策

配置 “交互式登录：尝试登录的用户的消息文本 ”和 “**交互式登录**”：**尝试登录设置的用户的消息标题** ，设置为组织的相应值。

> **备注**
>
> 显示的任何警告消息都应得到组织的法律和人力资源代表的批准。

潜在影响

用户可以在登录到服务器控制台之前在对话框中看到一条消息。

相关主题

- 安全选项

交互式登录: 之前登录到缓存的次数(域控制器不可用时)

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：如果域控制器) 安全策略设置不可用，(以前对缓存的登录次数 。**

参考

交互式登录：如果域控制器不可用，(之前对缓存的登录次数) 策略设置确定用户是否可以使用缓存的帐户信息登录到 Windows 域。 域帐户的登录信息可以缓存在本地，以便在后续登录时无法联系域控制器时，用户仍然可以登录。 此策略设置确定本地缓存其登录信息的唯一用户数。

如果域控制器不可用，并且缓存了用户的登录信息，则会提示用户显示以下消息：

无法联系域的域控制器。 你已使用缓存的帐户信息登录。 自上次登录以来对配置文件所做的更改可能不可用。

如果域控制器不可用，并且用户的登录信息未缓存，则会提示用户显示以下消息：

系统现在无法登录你，因为 *域名* 不可用。

此策略设置的值指示服务器在本地缓存其登录信息的用户数。 如果值为 10，则服务器将缓存 10 个用户的登录信息。 当第 11 个用户登录到设备时，服务器将覆盖最早的缓存登录会话。

访问服务器控制台的用户将在该服务器上缓存其登录凭据。 能够访问服务器的文件系统的恶意用户可以找到此缓存的信息，并使用暴力攻击来确定用户密码。 Windows 通过加密信息并在系统注册表中保留缓存的凭据（分布在多个物理位置）来缓解此类攻击。

> **备注**
>
> 缓存的帐户信息不会过期，但可能会被覆盖，如前所述。

可能值

- 从 0 到 50 的用户定义数字
- 未定义

最佳做法

Windows 安全基线不建议配置此设置。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	10 次登录
DC 有效默认设置	无效果
成员服务器有效默认设置	10 次登录
客户端计算机有效默认设置	10 次登录

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

策略冲突注意事项

无

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

分配给此策略设置的数字指示其登录信息由服务器在本地缓存的用户数。 如果数字设置为 10，则服务器将缓存 10 个用户的登录信息。 当第 11 个用户登录到设备时，服务器将覆盖最早的缓存登录会话。

访问服务器控制台的用户在该服务器上缓存其登录凭据。 能够访问服务器的文件系统的攻击者可以找到此缓存的信息，并使用暴力攻击来尝试确定用户密码。

为了缓解此类攻击，Windows 会加密信息并遮盖其物理位置。

对策

配置 **交互式登录：如果域控制器不可用，** ）设置为 0（这会禁用登录信息的本地缓存），则缓存 (的先前登录次数。 其他对策包括强制实施强密码策略和计算机的物理安全位置。

潜在影响

如果没有可用于对设备进行身份验证的域控制器，则用户无法登录到任何设备。 组织可以为最终用户计算机（尤其是移动用户）将此值配置为 2。 配置值 2 表示用户的登录信息仍位于缓存中，即使 IT 部门的成员最近登录到设备以执行系统维护也是如此。 此方法允许用户在未连接到组织的网络时登录到其计算机。

相关主题

- 安全选项

交互式登录：提示用户在过期前更改密码

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：提示用户在过期前更改密码** 安全策略设置。

参考

此策略设置确定何时警告用户其密码即将过期。 此警告使用户在当前密码过期之前有时间选择强密码，以避免失去系统访问权限。

可能值

- 用户定义的天数（从 0 到 999）
- 未定义

最佳做法

- 将用户密码配置为定期过期。 用户需要警告其密码即将过期，否则他们可能会被锁定在系统外。
- 设置 **交互式登录：提示用户在过期前将密码更改为** 五天。 如果密码过期日期为五天或更少天，则用户每次登录域时都会看到一个对话框。
- 将策略设置为零时，用户登录时不会显示密码过期警告。 在长时间运行的登录会话期间，会在密码过期的当天或密码已过期时收到警告。

位置

计算机配置\策略\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的默认值。 默认值也列在策略的属性页上。

服务器类型或组策略对象	默认值

服务器类型或组策略对象	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	五天
DC 有效默认设置	五天
成员服务器有效默认设置	五天
客户端计算机有效默认设置	五天

策略管理

本部分介绍可用于管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无。

组策略

使用组策略管理控制台配置此策略设置， (GPMC) 通过组策略对象 (GPO) 进行分发。 如果此策略未包含在分布式 GPO 中，可以通过本地安全策略管理单元在本地计算机上配置它。

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置、如何实施对策，以及对策的可能负面影响。

漏洞

如果用户密码在组织中配置为定期过期，则需要在过期前警告用户。 否则，它们可能会无意中被锁定到设备之外。

对策

配置 **交互式登录：提示用户在过期前将密码更改为** 五天。

潜在影响

当用户的密码配置为在 5 天或更短时间内过期时，用户会看到一个对话框，提示他们每次登录到域时更改其密码。

相关主题

- 安全选项

交互式登录: 需要域控制器身份验证以对工作站进行解锁

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项 **：要求域控制器身份验证才能解锁工作站** 安全策略设置。

参考

解锁锁定的设备需要登录信息。 对于域帐户， **“交互式登录：要求域控制器身份验证以解锁工作站** ”策略设置确定是否需要联系域控制器来解锁设备。 启用此策略设置需要域控制器对用于解锁设备的域帐户进行身份验证。 禁用此策略设置可让用户解锁设备，而无需计算机使用域控制器验证登录信息。 但是，如果 交互式登录：如果域控制器不可用，）设置为大于零的值，则以前对缓存 (的登录次数，则用户的缓存凭据将用于解锁系统。

设备将本地 (缓存到内存中，) 经过身份验证的任何用户的凭据。 设备使用这些缓存凭据对尝试解锁主机的任何人进行身份验证。

使用缓存凭据时，此身份验证过程之后，不会考虑或应用最近对帐户所做的任何更改（，例如用户权限分配、帐户锁定或被禁用的帐户）。 此结果不仅意味着用户权限不会更新，更重要的是，禁用的帐户仍能够解锁系统的控制台。

建议将 **“交互式登录：要求域控制器身份验证才能解锁工作站** ”设置为“已启用”，并将 “交互式登录”设置为“：如果域控制器不可用，则以前对缓存 (的登录次数) 设置为 0。 当用户锁定设备的主机或屏幕保护程序超时自动锁定时，仅当用户能够重新对域控制器进行身份验证时，才能解锁主机。 如果没有可用的域控制器，则用户无法解锁其设备。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 设置 **交互式登录：要求域控制器身份验证才能解锁工作站** ，并将其设置为“已启用”，并将 “交互式登录”设置为“：如果域控制器不可用， (以前对缓存的登录次数) 为 0。 当用户锁定设备的主机或屏幕保护程序超时自动锁定时，仅当用户能够重新对域控制器进行身份验证时，才能解锁主机。 如果没有可用的域控制器，则用户无法解锁其设备。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

默认情况下，设备在本地内存中缓存经过身份验证的任何用户的凭据。 设备使用这些缓存凭据对尝试解锁主机的任何人进行身份验证。 使用缓存凭据时，在对帐户进行身份验证后，不会考虑或应用最近对该帐户所做的任何更改（例如用户权限分配、帐户锁定或被禁用的帐户）。 用户权限不会更新，禁用的帐户仍能够解锁设备的控制台

对策

配置 **交互式登录：要求域控制器身份验证才能解锁工作站** 设置为“已启用”，并配置 “交互式登录”：如果域控制器不可用，) 设置为 0，则以前对缓存 (的登录次数 。

潜在影响

当设备上的主机被用户锁定或屏幕保护程序超时自动锁定时，仅当用户可以重新对域控制器进行身份验证时，才能解锁主机。 如果没有可用的域控制器，则用户无法解锁其工作站。 如果配置 交互式登录：如果域控制器不可用) 设置为 0，则以前对缓存 (的登录次数 ，则域控制器不可用的用户（（例如移动用户或远程用户) 无法登录）。

相关主题

- 安全选项

交互式登录：需要Windows Hello 企业版或智能卡

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10 版本 1703 或更高版本

介绍交互式登录的最佳做法、位置、值、策略管理和安全注意事项：**需要Windows Hello 企业版或智能卡**安全策略设置。

> **备注**
>
> 可能需要下载适用于 Windows 版本的 ADMX 模板才能应用此策略。

参考

交互式登录：需要Windows Hello 企业版或智能卡策略设置要求用户使用智能卡或 Windows Hello 企业版方法登录到设备。

要求用户使用复杂密码进行身份验证可增强网络安全，尤其是在用户必须定期更改其密码的情况下。 此要求降低了恶意用户能够通过暴力攻击猜测用户密码的可能性。 使用智能卡而不是密码进行身份验证可显著提高安全性，因为使用当今的技术，恶意用户几乎不可能模拟另一个用户。 需要个人标识号 (PIN 的智能卡) 提供双重身份验证：尝试登录的用户必须拥有智能卡并知道其 PIN。 捕获用户设备和域控制器之间的身份验证流量的恶意用户会发现解密流量很困难：即使他们这样做，当用户下次登录到网络时，将生成一个新的会话密钥，用于加密用户与域控制器之间的流量。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 将“**交互式登录：需要Windows Hello 企业版或智能卡**”设置为“已启用”。 所有用户必须使用智能卡登录到网络，或者使用Windows Hello 企业版方法。 此要求意味着

组织必须具有可靠的公钥基础结构 (PKI) ，并为所有用户提供智能卡和智能卡阅读器。 有关无密码身份验证的详细信息，请参阅Windows Hello 企业版概述。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表按服务器类型或组策略对象 (GPO) 列出了此策略的实际和有效默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 更改在本地保存或通过组策略分发时，无需重启设备即可生效。

策略冲突注意事项

无。

组策略

可以使用组策略管理控制台 (GPMC) 通过 GPO 进行分发来配置此策略设置。 如果此策略未包含在分布式 GPO 中，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可能很难让用户选择强密码，如果攻击者有足够的时间和计算资源，即使强密码也容易受到暴力攻击。

对策

对于有权访问包含敏感数据的计算机的用户，请向用户颁发智能卡或配置Windows Hello 企业版。 然后将“**交互式登录：需要Windows Hello 企业版或智能卡**”设置为“已启用”。

潜在影响

启用了此设置的设备的所有用户都必须使用智能卡或Windows Hello 企业版方法在本地登录。 组织必须具有可靠的公钥基础结构 (PKI) 、智能卡和智能卡读取器，或者已启用 Windows Hello 企业版。 这些要求是重大挑战，因为规划和部署这些技术需要专业知识和资源。 Active Directory 证书服务可用于实现和管理证书。 可以在客户端上使用自动用户和设备注册和续订。

相关文章

- 安全选项
- Windows Hello 企业版概述

交互式登录: 智能卡移除行为

项目 • 2023/04/12

适用范围

- Windows 11
- Windows 10

介绍交互式登录的建议做法、位置、值、策略管理和安全注意事项：**智能卡删除行为**安全策略设置。

参考

此策略设置确定从智能卡读取器中删除登录用户的智能卡时会发生什么情况。

如果使用智能卡进行身份验证，则在删除卡时，设备应自动锁定自身。 因此，如果用户在离开时忘记手动锁定其设备，恶意用户将无法获得访问权限。

如果在此策略设置的属性表中选择"**强制注销**"，则在删除智能卡时，用户会自动注销。 用户返回工作站时，必须重新插入智能卡并重新输入 PIN。

> ⓘ **备注**
>
> 此策略依赖于 **智能卡删除策略** 服务。 服务必须运行才能使策略生效，因此建议将服务的启动类型设置为 "**自动**"。

可能值

- 无操作
- 锁定工作站

  如果使用此设置，则在删除智能卡时，工作站会锁定。 因此，用户可以离开该区域，带着智能卡，并保持受保护的会话。

- 强制注销

  如果使用此设置，则在删除智能卡时，用户会自动注销。

- 如果远程桌面服务会话，则断开连接

如果使用此设置，删除智能卡会断开会话的连接，而不会注销用户。 因此，用户可以插入智能卡，稍后或在另一台配备阅读器的智能卡计算机上继续会话，而无需再次登录。 如果会话是本地会话，则此策略的工作方式与锁定工作站相同。

- 未定义

最佳做法

- 将“**交互式登录：智能卡删除行为**”设置为“**锁定工作站**”。 如果在此策略设置的属性表中选择“**锁定工作站**”，则在删除智能卡时，工作站将锁定。 因此，用户可以离开该区域，带着智能卡，并保持受保护的会话。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值，按服务器类型或组策略对象 (GPO) 。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	无操作
DC 有效默认设置	无操作
成员服务器有效默认设置	无操作
客户端计算机有效默认设置	无操作

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无

组策略

可以使用 组策略 管理控制台配置此策略设置， (要通过 GPO 分发的 GPMC) 。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

用户有时在离开工作站时忘记锁定工作站，从而允许恶意用户访问其设备。 如果使用智能卡进行身份验证，则在删除卡时，设备应自动锁定自身，以确保只有具有智能卡的用户才能使用这些凭据访问资源。

对策

将“**交互式登录：智能卡删除行为**”设置为“**锁定工作站**”。

如果为此策略设置选择“**锁定工作站**”，则删除智能卡时，设备将锁定。 用户可以离开该区域，带着智能卡，并仍保留受保护的会话。 此行为类似于要求用户在屏幕保护程序启动后在设备上恢复工作时登录的设置。

如果为此策略设置选择“**强制注销**”，则在删除智能卡时，用户会自动注销。 将设备部署为公共接入点（例如展台或其他类型的共享设备）时，此设置非常有用

潜在影响

如果选择“ **强制注销**”，则当用户返回工作站时，必须插入其智能卡并输入其 PIN。

相关主题

- 安全选项

Microsoft 网络客户端：对通信进行数字签名（始终）

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10
- Windows Server

本文介绍 Microsoft 网络客户端的最佳做法、位置、值、策略管理和安全注意事项 **：数字签名通信 (始终)** SMBv3 和 SMBv2 的安全策略设置。

> **ⓘ 备注**
>
> 本文介绍服务器消息块 (SMB) v2 和 v3 协议。 SMBv1 不安全，已在 Windows 中弃用。 从 Windows 10 版本 1709 和 Windows Server 版本 1709 开始，**默认情况下不会安装 SMBv1**。

> **ⓘ 重要**
>
> Microsoft 不建议使用以下组策略设置：
>
> - Microsoft **网络服务器**: **对通信进行数字签名(如果服务器允许)**
> - Microsoft **网络客户端**: **对通信进行数字签名(如果服务器允许)**
>
> 也不要使用 **EnableSecuritySignature** 注册表设置。
>
> 这些选项仅影响 SMBv1 行为。 它们可以有效地替换为 **数字签名通信 (始终)** 组策略设置或 **RequireSecuritySignature** 注册表设置。

参考

服务器消息块 (SMB) 协议为文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供了基础。 为了防止修改传输中的 SMB 数据包的“中间人”攻击，SMB 协议支持对 SMB 数据包进行数字签名。

在高安全性网络中实现数字签名有助于防止模拟客户端计算机和服务器，这称为“会话劫持”。滥用这些策略设置是可能导致数据访问失败的常见错误。

从 SMBv2 客户端和服务器开始， *可能需要签名*， 也可以 *不需要*签名。 如果启用此策略设置，SMBv2 客户端将对所有数据包进行数字签名。 另一个策略设置确定 SMBv3 和 SMBv2 服务器通信是否需要签名： Microsoft 网络服务器：对通信进行数字签名 (始终) 。

SMB 客户端和 SMB 服务器之间进行协商，以决定是否使用签名。 下表显示了 SMBv3 和 SMBv2 的有效行为。

客户端	**服务器 - 必需**	**服务器 - 不需要**
客户端 - 必需	签署	签署
客户端 - 不需要	已签名 [1]	未签名[2]

[1] 域控制器 SMB 流量
的默认值[2] 其他所有 SMB 流量的默认值

在 SMBv2 中提高了 SMB 签名的性能。 有关详细信息，请参阅 潜在影响。

可能值

- 已启用
- 禁用

最佳做法

启用 Microsoft **网络客户端：对通信进行数字签名 (始终)** 。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	**默认值**
默认域策略	禁用
默认域控制器策略	禁用
独立服务器默认设置	禁用

服务器类型或 GPO	默认值
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍可用于管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置、如何实施对策，以及对策的可能负面影响。

漏洞

会话劫持使用的工具允许有权访问与客户端设备或服务器相同的网络的攻击者中断、结束或窃取正在进行的会话。 攻击者可能会截获和修改未签名的 SMB 数据包，然后修改流量并转发流量，使服务器执行令人反感的操作。 或者，攻击者可以在合法身份验证后伪装成服务器或客户端计算机，并未经授权访问数据。

SMB 是许多版本的 Windows 操作系统都支持的资源共享协议。 它是许多新式功能（例如存储空间直通、存储副本和 SMB 直通）以及许多旧式协议和工具的基础。 SMB 签名对用户和托管数据的服务器进行身份验证。 如果任一方未能通过身份验证过程，则不会进行数据传输。

对策

启用 Microsoft **网络客户端：对通信进行数字签名 (始终)** 。

> ⓘ **备注**

可以保护所有网络流量的替代对策是通过 IPsec 实现数字签名。 有一些基于硬件的加速器用于 IPsec 加密和签名，可用于最大程度地减少对服务器的性能影响。 没有可用于 SMB 签名的此类加速器。

潜在影响

存储速度会影响性能。 源和目标上的更快的驱动器允许更多的吞吐量，这会导致更多的 CPU 使用率进行签名。 如果使用 1-Gb 以太网网络或较慢的存储速度与新式 CPU，则性能下降有限。 如果使用更快的网络（（例如 10 Gb）），则签名对性能的影响可能会更大。

相关文章

- 安全选项
- Microsoft 网络服务器：对通信进行数字签名（始终）

Microsoft 网络客户端: 将未加密的密码发送到第三方 SMB 服务器

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 Microsoft 网络客户端的最佳做法、位置、值、策略管理和安全注意事项 **：将未加密的密码发送到第三方 SMB 服务器** 安全策略设置。

参考

服务器消息块 (SMB) 协议为文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供了基础。 此策略设置允许或阻止 SMB 重定向程序将纯文本密码发送到身份验证期间不支持密码加密的非 Microsoft 服务器服务。

可能值

- 已启用

  允许服务器消息块 (SMB) 重定向程序将纯文本密码发送到身份验证期间不支持密码加密的非 Microsoft 服务器服务。

- 禁用

  服务器消息块 (SMB) 重定向程序仅向非 Microsoft SMB 服务器服务发送加密密码。 如果这些服务器服务不支持密码加密，身份验证请求将失败。

- 未定义

最佳做法

- 建议将 **Microsoft 网络客户端：发送未加密的密码以连接到第三方 SMB 服务器** 设置为“已禁用”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果启用此策略设置，服务器可以通过网络将纯文本密码传输到提供 SMB 服务的其他计算机。 这些其他设备可能不使用 Windows Server 2003 或更高版本中包含的任何 SMB 安全机制。

对策

禁用 Microsoft **网络客户端：发送未加密的密码以连接到第三方 SMB 服务器** 设置。

潜在影响

某些较旧的应用程序可能无法通过 SMB 协议与组织中的服务器通信。

相关主题

- 安全选项

Microsoft 网络服务器: 暂停会话前所需的空闲时间数量

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 Microsoft 网络服务器的最佳做法、位置、值和安全注意事项 **：暂停会话安全策略设置之前所需的空闲时间量** 。

参考

每个服务器消息块 (SMB) 会话都会消耗服务器资源。 建立大量空会话将导致服务器速度变慢或可能失败。 恶意用户可能会重复建立 SMB 会话，直到服务器停止响应;此时，SMB 服务将变得缓慢或无响应。

Microsoft **网络服务器：暂停会话策略设置前所需的空闲时间量**确定在由于非活动而暂停会话之前必须在 SMB 会话中传递的连续空闲时间量。 可以使用此策略设置来控制设备何时挂起非活动 SMB 会话。 客户端设备活动恢复时，会自动重新建立会话。

可能值

- 用户定义的分钟数（从 0 到 99，999）。

  对于此策略设置，值 0 表示尽可能快地断开空闲会话的连接。 最大值为 99999 (每天 8 个营业时间) ，即 208 天。 实际上，此值禁用策略。

- 未定义

最佳做法

- 建议将此策略设置为 15 分钟。 影响不大，因为如果客户端恢复活动，SMB 会话将自动重新建立。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO 默认值
默认域策略
默认域控制器策略
独立服务器默认设置
DC 有效默认设置
成员服务器有效默认设置
客户端计算机有效默认设置

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

每个 SMB 会话都会消耗服务器资源，许多空会话会使服务器变慢或可能导致服务器失败。 攻击者可能会反复建立 SMB 会话，直到服务器的 SMB 服务变得缓慢或无响应。

对策

服务器上的默认行为在设计上缓解了此威胁。

潜在影响

影响不大，因为如果客户端计算机恢复活动，SMB 会话会自动重新建立。

相关主题

- 安全选项

Microsoft 网络服务器: 尝试使用 S4U2Self 获取声明信息

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 Microsoft 网络服务器的最佳做法、位置、值、管理和安全注意事项 **：尝试 S4U2Self 获取声明信息安全** 策略设置。

参考

此安全设置支持在尝试访问需要用户声明的文件共享之前运行 Windows 版本的客户端设备Windows 8。 此设置确定本地文件服务器是否会尝试使用 Kerberos Service-for-User-to-Self (S4U2Self) 功能从客户端的帐户域获取网络客户端主体的声明。 仅当文件服务器使用用户声明来控制对文件的访问，并且文件服务器将支持其帐户可能位于域中的客户端主体时，才应启用此设置，该域中的客户端计算机和域控制器在Windows 8或Windows Server 2012之前运行 Windows 版本。

启用后，此安全设置会导致 Windows 文件服务器检查经过身份验证的网络客户端主体的访问令牌，并确定是否存在声明信息。 如果没有声明，则文件服务器将使用 Kerberos S4U2Self 功能尝试联系客户端帐户域中Windows Server 2012域控制器，并为客户端主体获取启用声明的访问令牌。 可能需要启用声明的令牌才能访问应用了基于声明的访问控制策略的文件或文件夹。

如果禁用此设置，则 Windows 文件服务器不会尝试获取客户端主体的已启用声明的访问令牌。

可能值

- **默认**

  Windows 文件服务器将检查经过身份验证的网络客户端主体的访问令牌，并确定是否存在声明信息。

- **Enabled**

  与 **Default** 相同。

- **禁用**
- **未定义**

  与 Disabled 相同。

最佳做法

此设置应设置为 “**默认值** ”，以便文件服务器可以自动评估用户是否需要声明。 仅当存在包含用户声明的本地文件访问策略时，才应将此设置显式配置为 “**启用** ”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

仅当文件服务器使用用户声明来控制对文件的访问，并且文件服务器将支持其帐户可能位于域中的客户端主体时，才应启用此设置，该域中的客户端计算机和域控制器在Windows 8或Windows Server 2012之前运行 Windows 版本。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

无。 启用此策略设置可让你利用Windows Server 2012和Windows 8及更高版本中的功能（针对特定方案）使用启用了声明的令牌访问在 windows 操作系统上应用了基于声明的访问控制策略的文件或文件夹，然后再Windows Server 2012 和Windows 8。

对策

不适用。

潜在影响

无。

相关主题

- 安全选项

Microsoft 网络服务器：对通信进行数字签名（始终）

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10
- Windows Server

介绍 Microsoft 网络服务器的最佳做法、位置、值、策略管理和安全注意事项 **：对通信进行数字签名 (始终)** SMBv3 和 SMBv2 的安全策略设置。

> **ⓘ 备注**
>
> 本文介绍服务器消息块 (SMB) v2 和 v3 协议。 SMBv1 不安全，已在 Windows 中弃用。 从 Windows 10 版本 1709 和 Windows Server 版本 1709 开始，**默认情况下不会安装 SMBv1**。

> **ⓘ 重要**
>
> Microsoft 不建议使用以下组策略设置：
>
> - Microsoft **网络服务器**: **对通信进行数字签名(如果服务器允许)**
> - Microsoft **网络客户端**: **对通信进行数字签名(如果服务器允许)**
>
> 也不要使用 **EnableSecuritySignature** 注册表设置。
>
> 这些选项仅影响 SMBv1 行为。 它们可以有效地替换为 **数字签名通信 (始终)** 组策略设置或 **RequireSecuritySignature** 注册表设置。

参考

服务器消息块 (SMB) 协议为文件和打印共享以及许多其他网络操作（例如远程 Windows 管理）提供了基础。 为了防止修改传输中的 SMB 数据包的中间人攻击，SMB 协议支持 SMB 数据包的数字签名。

在高安全性网络中实现数字签名有助于防止模拟客户端计算机和服务器，这称为“会话劫持”。但是，滥用这些策略设置可能会导致数据访问失败。

从 SMBv2 客户端和服务器开始，可能需要签名，也可以不需要签名。 如果启用此策略设置，SMBv2 客户端将对所有数据包进行数字签名。 另一个策略设置确定 SMBv3 和 SMBv2 服务器通信是否需要签名： Microsoft 网络客户端：数字签名通信 (始终) 。

SMB 客户端和 SMB 服务器之间进行了协商，以决定是否有效使用签名。 下表包含 SMBv3 和 SMBv2 的有效行为。

客户端	**服务器 - 必需**	**服务器 - 不需要**
客户端 - 必需	签署	签署
客户端 - 不需要	已签名 [1]	未签名[2]

[1] 域控制器 SMB 流量
的默认值[2] 其他所有 SMB 流量的默认值

在 SMBv2 中提高了 SMB 签名的性能。 有关详细信息，请参阅 潜在影响。

可能值

- 已启用
- 禁用

最佳做法

启用 Microsoft **网络服务器：对通信进行数字签名 (始终)** 。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	**默认值**
默认域策略	禁用
默认域控制器策略	已启用
独立服务器默认设置	禁用
DC 有效默认设置	启用

服务器类型或 GPO	默认值
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

会话劫持使用的工具允许有权访问与客户端设备或服务器相同的网络的攻击者中断、结束或窃取正在进行的会话。 攻击者可能会截获和修改未签名的服务器消息块 (SMB) 数据包，然后修改流量并将其转发，以便服务器可能执行令人反感的操作。 或者，攻击者可以在合法身份验证后伪装成服务器或客户端设备，并未经授权访问数据。

SMB 是许多 Windows 操作系统支持的资源共享协议。 它是许多新式功能（例如存储空间直通、存储副本和 SMB 直通）以及许多旧式协议和工具的基础。 如果任一方未能通过身份验证过程，则不会进行数据传输。

对策

启用 Microsoft **网络服务器：对通信进行数字签名 (始终)** 。

> **备注**
>
> 可以保护所有网络流量的替代对策是使用 IPsec 实现数字签名。 可以使用基于硬件的加速器进行 IPsec 加密和签名，以尽量减少对服务器 CPU 的性能影响。 没有可用于 SMB 签名的此类加速器。

潜在影响

存储速度会影响性能。 源和目标上更快的驱动器允许更多的吞吐量，这会导致签名的 CPU 使用率增加。 如果使用 1 GB 以太网网络或较慢的存储速度与新式 CPU，则性能下降有限。 如果使用更快的网络（（例如 10 Gb）），则签名对性能的影响可能会更大。

相关文章

- 安全选项
- Microsoft 网络客户端：对通信进行数字签名（始终）

Microsoft 网络服务器：在登录时间过期时断开客户端连接

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 Microsoft 网络服务器的最佳做法、位置、值和安全注意事项 **：在登录时间过期时断开客户端连接** 安全策略设置。

参考

此策略设置启用或禁用在用户帐户的有效登录时间之外连接到本地设备的用户的强制断开连接。 它会影响 SMB 组件。 如果启用此策略设置，则客户端登录时间过期时，与 SMB 服务的客户端计算机会话将强制断开连接。 如果禁用此策略设置，则会在客户端设备的登录时间过期后维护已建立的客户端设备会话。

可能值

- 已启用

  当客户端设备的登录时间过期时，与 SMB 服务的客户端设备会话将强制断开连接。 如果组织中未使用登录小时数，则启用此策略设置将不起作用。

- 禁用

  在客户端设备的登录时间过期后，系统会维护已建立的客户端设备会话。

- 未定义

最佳做法

- 如果启用此策略设置，还应启用 网络安全：在登录时间过期时强制注销。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果组织为用户配置登录时间，则启用此策略设置是有意义的。 否则，在登录时间之外无权访问网络资源的用户可以继续使用这些资源与在允许时间内建立的会话。

对策

启用 Microsoft **网络服务器：在登录时间过期时断开客户端连接** 设置。

潜在影响

如果组织中未使用登录小时数，则此策略设置没有影响。 如果使用了登录时间，则现有用户会话在其登录时间到期时被强制终止。

相关主题

- 安全选项

Microsoft 网络服务器: 服务器 SPN 目标名称验证级别

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 Microsoft 网络服务器的最佳做法、位置和值、策略管理和安全注意事项 **：服务器 SPN 目标名称验证级别** 安全策略设置。

参考

此策略设置控制当客户端设备使用服务器消息块 (SMB) 协议建立会话时，具有共享文件夹或打印机的服务器对服务主体名称 (SPN) 执行的验证级别。 验证级别可帮助防止针对 SMB 服务 (称为 SMB 中继攻击) 的一类攻击。 此设置会影响 SMB1 和 SMB2。

使用 SMB 的服务器为其文件系统和其他资源（例如打印机）提供网络客户端设备的可用性。 大多数使用 SMB 的服务器使用 NT 域身份验证 (NTLMv1 和 NTLMv2) 和 Kerberos 协议来验证用户对资源的访问。

可能值

验证级别的选项包括：

- **关闭**

  SMB 服务器不需要或验证来自 SMB 客户端的 SPN。

- **接受（如果由客户端提供）**

  SMB 服务器将接受并验证 SMB 客户端提供的 SPN，如果会话与 SMB 服务器的 SPN 列表匹配，则允许建立会话。 如果 SPN 不匹配，则会拒绝该 SMB 客户端的会话请求。

- **从客户端需要**

  SMB 客户端必须在会话设置中发送 SPN 名称，并且提供的 SPN 名称必须与请求建立连接的 SMB 服务器匹配。 如果客户端设备未提供 SPN，或者提供的 SPN 不匹配，则会拒绝会话。

默认设置为“关”。

最佳做法

此设置会影响服务器 SMB 行为，应仔细评估和测试其实现，以防止中断文件和打印服务功能。

> **注意：** 所有 Windows 操作系统都支持客户端 SMB 组件和服务器端 SMB 组件。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	关闭
默认域控制器策略	关闭
独立服务器默认设置	关闭
域控制器有效默认设置	未实现验证级别检查
成员服务器有效默认设置	未实现验证级别检查
客户端计算机上有效的 GPO 默认设置	未实现验证级别检查

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

无。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

此策略设置控制客户端设备使用 SMB 协议建立会话时，具有共享文件夹或打印机的服务器对服务主体名称 (SPN) 执行的验证级别。 验证级别可帮助防止针对 SMB 服务器的一类攻击 (称为 SMB 中继攻击) 。 此设置将同时影响 SMB1 和 SMB2。

对策

有关适合你的环境的对策，请参阅上面的 **可能值** 。

潜在影响

所有 Windows 操作系统都支持客户端 SMB 组件和服务器端 SMB 组件。 此设置会影响服务器 SMB 行为，应仔细评估和测试其实现，以防止中断文件和打印服务功能。

由于 SMB 协议已广泛部署，因此将选项设置为 “**接受**”（**如果客户端提供** ）或 “**必需**” 将阻止某些客户端成功对环境中的某些服务器进行身份验证。

相关主题

- 安全选项

网络访问: 允许匿名 SID/名称转换

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：允许匿名 SID/名称转换** 安全策略设置。

参考

此策略设置启用或禁用匿名用户为其他用户请求安全标识符 (SID) 属性的功能。

如果启用此策略设置，用户可以使用已知的 Administrators SID 获取内置管理员帐户的真实名称，即使帐户已重命名也是如此。 然后，该用户可能会使用该帐户名称发起暴力破解密码猜测攻击。

滥用此策略设置是一个常见错误，可能会导致数据丢失或数据访问或安全性问题。

可能值

- 已启用

  匿名用户可以请求其他用户的 SID 属性。 了解管理员 SID 的匿名用户可以联系已启用此策略的计算机，并使用 SID 获取管理员的姓名。 此设置会影响 SID 到名称的转换和名称到 SID 的转换。

- 禁用

  防止匿名用户为其他用户请求 SID 属性。

- 未定义

最佳做法

- 将此策略设置为 Disabled，这是成员计算机上的默认值;因此，它不会对他们产生任何影响。 域控制器的默认值为 Enabled。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	启用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

操作系统版本差异

此设置的默认值在操作系统之间已更改，如下所示：

- 运行 Windows Server 2003 R2 或更早版本的域控制器上的默认值设置为“已启用”。
- 运行 Windows Server 2008 及更高版本的域控制器上的默认值设置为“禁用”。

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

修改此设置可能会影响与客户端计算机、服务和应用程序的兼容性。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果启用此策略设置，则具有本地访问权限的用户可以使用已知管理员的 SID 来了解内置管理员帐户的真实名称，即使它已重命名。 然后，该用户可以使用帐户名称发起密码猜测攻击。

对策

禁用 **网络访问：允许匿名 SID/名称转换** 设置。

潜在影响

“禁用”是成员设备上此策略设置的默认配置;因此，它对他们没有影响。 域控制器的默认配置为 Enabled。

相关主题

- 安全选项

网络访问: 不允许 SAM 帐户的匿名枚举

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值和安全注意事项 **：不允许匿名枚举 SAM 帐户** 安全策略设置。

参考

此策略设置确定将为与设备的匿名连接分配哪些其他权限。 Windows 允许匿名用户执行某些活动，例如枚举域帐户和网络共享的名称。 例如，当管理员想要授予不保持相互信任的受信任域中的用户访问权限时，此权限很方便。

此策略设置对域控制器没有影响。

滥用此策略设置是一个常见错误，可能会导致数据丢失或数据访问或安全性问题。

可能值

- 已启用
- 禁用

  管理员无法为设备匿名连接分配其他权限。 匿名连接将依赖于默认权限。

- 未定义

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突

即使启用了此策略设置，匿名用户也将有权访问具有显式包含内置组的资源，这些权限包括 Windows Server 2008 和 Windows Vista) 之前的系统上的 ANONYMOUS LOGON (。

组策略

此策略对域控制器没有影响。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

未经授权的用户可以匿名列出帐户名称，并使用这些信息执行社交工程攻击或尝试猜测密码。 社交工程攻击者试图以某种方式欺骗用户以获取密码或某种形式的安全信息。

对策

启用 **网络访问：不允许 SAM 帐户的匿名枚举** 设置。

潜在影响

无法通过单向信任向另一个域的用户授予访问权限，因为信任域中的管理员无法枚举另一个域中的帐户列表。 匿名访问文件和打印服务器的用户无法列出这些服务器上的共享网络资源;必须先对用户进行身份验证，然后才能查看共享文件夹和打印机的列表。

相关主题

- 安全选项

网络访问: 不允许 SAM 帐户和共享的匿名枚举

项目 • 2023/03/18

适用范围

- Windows 10

介绍网络访问的最佳做法、位置、值和安全注意事项 **：不允许匿名枚举 SAM 帐户和共享**安全策略设置。

参考

此策略设置确定将为与设备的匿名连接分配哪些其他权限。 Windows 允许匿名用户执行某些活动，例如枚举域帐户和网络共享的名称。 例如，当管理员想要授予不保持相互信任的受信任域中的用户访问权限时，此权限很方便。 但是，即使启用了此策略设置，匿名用户也将有权访问具有显式包含内置组 ANONYMOUS LOGON 的权限的资源。

此策略设置对域控制器没有影响。 滥用此策略设置是一个常见错误，可能会导致数据丢失或数据访问或安全性问题。

可能值

- 已启用
- 禁用

  管理员无法为设备匿名连接分配其他权限。 匿名连接将依赖于默认权限。 但是，未经授权的用户可以匿名列出帐户名称，并使用这些信息来尝试猜测密码或执行社交工程攻击。

- 未定义

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突

即使启用了此策略设置，匿名用户也将有权访问具有显式包含内置组的资源，这些权限包括 Windows Server 2008 和 Windows Vista) 之前的系统上的 ANONYMOUS LOGON (。

组策略

此策略对域控制器没有影响。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

未经授权的用户可以匿名列出帐户名称和共享资源，并使用这些信息来尝试猜测密码或执行社交工程攻击。

对策

启用 **网络访问：不允许匿名枚举 SAM 帐户和共享** 设置。

潜在影响

无法通过单向信任向另一个域的用户授予访问权限，因为信任域中的管理员无法枚举另一个域中的帐户列表。 匿名访问文件和打印服务器的用户无法列出这些服务器上的共享网络资源;必须先对用户进行身份验证，然后才能查看共享文件夹和打印机的列表。

相关主题

- 安全选项

网络访问: 不允许存储网络身份验证的密码和凭据

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：不允许存储用于网络身份验证安全策略设置的密码和凭据** 。

参考

此安全设置确定凭据管理器是否保存密码和凭据以供以后在获取域身份验证时使用。

可能值

- 已启用

  凭据管理器不会在设备上存储密码和凭据

- 禁用

  凭据管理器将在此计算机上存储密码和凭据，供以后用于域身份验证。

- 未定义

最佳做法

建议禁用 Windows 操作系统在不需要凭据的任何设备上缓存凭据的功能。 评估服务器和工作站以确定要求。 缓存凭据主要用于在与域断开连接时需要域凭据的笔记本电脑上使用。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	禁用
默认域控制器策略	禁用
独立服务器默认设置	禁用
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机上有效的 GPO 默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

当本地保存或通过组策略分发此策略的更改时，需要重启设备，然后此策略才会生效。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

登录设备时，用户可以访问缓存的密码。 虽然此信息听起来可能很明显，但如果用户在不知不觉中运行读取密码并将其转发给另一个未经授权的用户，则可能会出现问题。

> **注意：** 对于有效实施和管理企业防病毒解决方案以及合理的软件限制策略的组织来说，此攻击和其他涉及恶意软件攻击的成功机会将大大降低。

无论使用哪种加密算法来加密密码验证程序，都可以覆盖密码验证程序，以便攻击者可以验证程序所属的用户的身份进行身份验证。 因此，可能会覆盖管理员的密码。 此过程需要对设备进行物理访问。 存在可帮助覆盖缓存验证程序的工具。 借助其中一个实用工具，攻击者可以使用覆盖的值进行身份验证。

覆盖管理员的密码无助于攻击者访问使用该密码加密的数据。 此外，覆盖密码也无助于攻击者访问任何加密文件系统 (EFS) 属于该设备上的其他用户的数据。 覆盖密码无助于攻击者替换验证程序，因为基本密钥材料不正确。 因此，使用加密文件系统或使用数据保护 API (DPAPI) 加密的数据不会解密。

对策

启用 **网络访问：不允许存储用于网络身份验证的密码和凭据** 设置。

若要限制计算机上存储的缓存域凭据的数量，请设置 **cachedlogonscount** 注册表项。 默认情况下，操作系统会为每个唯一用户最近 10 个有效登录缓存验证程序。 此值可以设置为 0 到 50 之间的任何值。 默认情况下，所有版本的 Windows 操作系统都会记住 10 个缓存登录，Windows Server 2008 及更高版本除外，这些登录设置为 25。

当你尝试从基于 Windows 的客户端设备登录到域，并且域控制器不可用时，你不会收到错误消息。 因此，你可能没有注意到你使用缓存的域凭据登录。 可以通过 ReportDC 注册表项设置使用缓存域凭据的登录通知。

潜在影响

每当用户登录到其 Microsoft 帐户或域帐户无法访问的其他网络资源时，都强制键入密码。 此策略设置应该不会影响访问配置为允许其基于 Active Directory 的域帐户进行访问的网络资源的用户。

相关主题

- 安全选项

网络访问: 将 Everyone 权限应用于匿名用户

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：让每个人权限应用于匿名用户** 安全策略设置。

参考

此策略设置确定为与设备的匿名连接授予哪些其他权限。 如果启用此策略设置，匿名用户可以枚举域帐户和共享文件夹的名称，并执行某些其他活动。 此功能很方便，例如，当管理员想要向不保持相互信任的受信任域中的用户授予访问权限时。

默认情况下，为匿名连接创建的令牌不包括 Everyone SID。 因此，分配给 Everyone 组的权限不适用于匿名用户。

可能值

- 已启用

  Everyone SID 将添加到为匿名连接创建的令牌中，匿名用户可以访问已为其分配了 Everyone 组权限的任何资源。

- 禁用

  将从为匿名连接创建的令牌中删除 Everyone SID。

- 未定义

最佳做法

- 将此策略设置为 “**已禁用**”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

未经授权的用户可以匿名列出帐户名称和共享的资源，并使用这些信息来尝试猜测密码、执行社交工程攻击或发起 DoS 攻击。

对策

禁用 “**网络访问：允许每个人”权限应用于匿名用户** 设置。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

网络访问: 可匿名访问的命名管道

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 ：**可以匿名访问的命名管道** 安全策略设置。

参考

此策略设置确定哪些通信会话或管道具有允许匿名访问的属性和权限。

通过命名管道（如 COMNAP 和 LOCATOR）限制访问有助于防止对网络进行未经授权的访问。

可能值

- 用户定义的共享文件夹列表
- 未定义

最佳做法

- 将此策略设置为 null 值;即启用策略设置，但不要在文本框中输入命名管道。 此设置将禁用对命名管道的空会话访问，依赖于此功能或对命名管道的未经身份验证访问的应用程序将不再起作用。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	Netlogon、samr、lsarpc
独立服务器默认设置	Null
DC 有效默认设置	Netlogon、samr、lsarpc
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

若要使此策略设置生效，还必须启用 “网络访问：限制对命名管道和共享的匿名访问 ”设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以限制通过命名管道（如 COMNAP 和 LOCATOR）的访问，以帮助防止对网络进行未经授权的访问。 以下列表介绍了可用的命名管道及其用途。 这些管道在早期版本的 Windows 中被授予匿名访问权限，一些旧版应用程序仍可能使用它们。

命名管道	用途
COMNAP	名为管道的 SNABase。 系统网络体系结构 (SNA) 是最初为 IBM 大型机计算机开发的网络协议的集合。
COMNODE	名为管道的 SNA 服务器。

命名管道	用途
SQL\QUERY	SQL Server的默认命名管道。
SPOOLSS	打印后台处理程序服务的命名管道。
EPMAPPER	终结点映射器命名管道。
定位	名为管道的远程过程调用定位符服务。
TrlWks	名为管道的分布式链接跟踪客户端。
TrkSvr	名为管道的分布式链接跟踪服务器。

对策

配置 “**网络访问：可以匿名访问的命名管道** ”设置为 null 值 (启用此设置，但不在文本框中指定命名管道) 。

潜在影响

此配置禁用对命名管道的 null 会话访问，依赖于此功能或对命名管道的未经身份验证访问的应用程序不再有效。 在混合模式环境中，此结果可能会破坏 Windows Server 2003 域之间的信任。

相关主题

- 安全选项

网络访问: 可远程访问的注册表路径

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：远程访问注册表路径** 安全策略设置。

参考

此策略设置确定当应用程序或进程引用 WinReg 密钥以确定访问权限时可访问的注册表路径。

注册表是用于获取设备配置信息的数据库，其中大部分信息都是敏感的。 恶意用户可以使用注册表来促进未经授权的活动。 为了降低发生这种情况的风险，将在整个注册表中分配适当的访问控制列表 (ACL)，以帮助防止未经授权的用户访问。

若要允许远程访问，还必须启用远程注册表服务。

可能值

- 用户定义的路径列表
- 未定义

最佳做法

- 将此策略设置为 null 值;也就是说，启用策略设置，但不要在文本框中输入任何路径。 远程管理工具（如 Microsoft 基线安全分析器和Configuration Manager）需要远程访问注册表。 从可访问路径列表中删除默认注册表路径可能会导致这些和其他管理工具失败。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	请参阅以下注册表项组合
DC 有效默认设置	请参阅以下注册表项组合
成员服务器有效默认设置	请参阅以下注册表项组合
客户端计算机有效默认设置	请参阅以下注册表项组合

以下所有注册表项的组合适用于以前的设置：

1. System\CurrentControlSet\Control\ProductOptions
2. System\CurrentControlSet\Control\Server Applications
3. Software\Microsoft\Windows NT\CurrentVersion

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

攻击者可以使用注册表中的信息来促进未经授权的活动。 为了降低此类攻击的风险，在整个注册表中分配了合适的 ACL，以帮助防止未经授权的用户访问。

对策

将 “**网络访问：远程访问注册表路径** ”设置配置为 null 值 (启用此设置，但不要在文本框中输入任何路径) 。

潜在影响

远程管理工具 (如 Microsoft 基线安全分析器 (MBSA) 和Configuration Manager需要远程访问注册表，以正确监视和管理这些计算机。 如果从可访问路径列表中删除默认注册表路径，此类远程管理工具可能会失败。

> **注意：** 如果要允许远程访问，还必须启用远程注册表服务。

相关主题

- 安全选项

网络访问: 可远程访问的注册表路径和子路径

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值和安全注意事项 **：远程访问注册表路径和子路径** 安全策略设置。

参考

此策略设置确定当应用程序或进程引用 WinReg 密钥以确定访问权限时可以访问哪些注册表路径和子路径。

注册表是用于获取设备配置信息的数据库，其中大部分信息都是敏感的。 恶意用户可以使用它来促进未经授权的活动。 由于在整个注册表中分配的默认 ACL 具有相当严格的限制，并且有助于防止未经授权的用户访问，因此降低了发生这种情况的可能性。

若要允许远程访问，还必须启用远程注册表服务。

可能值

- 用户定义的路径列表
- 未定义

最佳做法

- 将此策略设置为 null 值;即启用策略设置，但不要在文本框中输入任何路径。 远程管理工具（如 Microsoft 基线安全分析器和Configuration Manager）需要远程访问注册表。 从可访问路径列表中删除默认注册表路径可能会导致这些和其他管理工具失败。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	请参阅以下注册表项组合
DC 有效默认设置	请参阅以下注册表项组合
成员服务器有效默认设置	请参阅以下注册表项组合
客户端计算机有效默认设置	请参阅以下注册表项组合

以下所有注册表项的组合适用于以前的设置：

1. System\CurrentControlSet\Control\Print\Printer
2. System\CurrentControlSet\Services\Eventlog
3. Software\Microsoft\OLAP Server
4. Software\Microsoft\Windows NT\CurrentVersion\Print
5. Software\Microsoft\Windows NT\CurrentVersion\Windows
6. System\CurrentControlSet\Control\ContentIndex
7. System\CurrentControlSet\Control\Terminal Server
8. System\CurrentControlSet\Control\Terminal Server\UserConfig
9. System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
10. Software\Microsoft\Windows NT\CurrentVersion\Perflib
11. System\CurrentControlSet\Services\SysmonLog

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

注册表包含敏感的设备配置信息，攻击者可以使用这些信息来促进未经授权的活动。 在整个注册表中分配的默认 ACL 是相当严格的，并且有助于保护注册表免受未经授权的用户访问，这一事实降低了此类攻击的风险。

对策

将 “**网络访问：远程访问注册表路径和子路径** ”设置为 null 值， (启用此设置，但不要在文本框中输入任何路径) 。

潜在影响

MBSA 和 Configuration Manager 等远程管理工具需要远程访问注册表才能正确监视和管理这些计算机。 如果从可访问路径列表中删除默认注册表路径，此类远程管理工具可能会失败。

> **注意：** 如果要允许远程访问，还必须启用远程注册表服务。

相关主题

- 安全选项

网络访问：限制匿名访问命名管道和共享

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10
- Windows 8.1
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：限制匿名访问命名管道和共享** 安全策略设置。

参考

此策略设置启用或禁用仅对网络访问中命名的共享文件夹和管道的匿名 **访问限制：可以匿名访问的命名管道** 和 网络访问：可以匿名访问的共享 设置。 此设置通过在注册表项中添加 Value 1 的 RestrictNullSessAccess 来控制对计算机上的共享文件夹的空会话访问 **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters**。 此注册表值打开或关闭 null 会话共享文件夹，以控制服务器服务是否限制未经身份验证的客户端对命名资源的访问。

空会话是一个弱点，可以通过环境中的设备上的各种共享文件夹加以利用。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 将此策略设置为“已启用”。 启用此策略设置会将未经身份验证的用户的空会话访问限制为 Null，这些服务器管道和共享文件夹除外，这些服务器管道和共享文件夹列在 **NullSessionPipes** 和 **NullSessionShares** 注册表项中。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

空会话是一个弱点，可以通过共享文件夹 (包括环境中设备上) 的默认共享文件夹。

对策

启用 “**网络访问：限制对命名管道和共享的匿名访问** ”设置。

潜在影响

可以启用此策略设置，将未经身份验证的用户的 null 会话访问限制为除 NullSessionPipes 和 NullSessionShares 条目中列出的服务器管道和共享文件夹以外的所有服务器管道和共享文件夹。

相关主题

- 安全选项

网络访问：限制允许远程调用 SAM 的客户端

项目 • 2023/03/18

适用范围

- Windows 10
- Windows 8.1
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

网络访问：限制允许远程调用 SAM 的客户端安全策略设置控制可以在本地安全帐户管理器 (SAM) 数据库和 Active Directory 中枚举用户和组的用户。 Windows 10版本 1607 首次支持此设置，Windows Server 2016 (RTM) ，可以在早期的 Windows 客户端和服务器操作系统上配置此设置。

本文介绍不同版本的 Windows 中此安全策略设置的默认值。 默认情况下，从 Windows 10 版本 1607 和 Windows Server 2016 开始的计算机比早期版本的 Windows 限制更严格。 此限制性特征意味着，如果混合使用计算机（例如同时运行 Windows Server 2016 和 Windows Server 2012 R2 的成员服务器），则运行Windows Server 2016的服务器可能无法在默认情况下枚举运行服务器的帐户Windows Server 2012 R2 成功。

本文还介绍了相关事件，以及如何在约束允许远程枚举用户和组的安全主体之前启用审核模式，以便环境在不影响应用程序兼容性的情况下保持安全。

> ⓘ **备注**
>
> 此策略的实现可能会影响运行 Microsoft Exchange 2016 或 Microsoft Exchange 2013 的服务器上的 **脱机通讯簿生成** 。

引用

SAMRPC 协议可使低特权用户在网络上的计算机中查询数据。 例如，用户可以使用 SAMRPC 枚举用户（包括本地或域管理员等特权帐户）或从本地 SAM 和 Active Directory 枚举组和组成员身份。 此信息可以提供重要的上下文，并且可以作为攻击者泄露域或网络环境的起始点。

为了减少该风险，可以配置**网络访问：限制允许远程调用 SAM 的客户端**安全策略设置，以强制安全帐户管理器 (SAM) 针对远程调用执行访问检查。 访问检查允许或拒绝所定义

的用户和组执行到 SAM 和 Active Directory 的远程 RPC 连接。

默认情况下，未定义 **网络访问：限制允许对 SAM 进行远程调用的客户端** 安全策略设置。 如果对其进行定义，则可以编辑默认安全描述符定义语言 (SDDL) 字符串，以明确允许或拒绝用户和组远程调用 SAM。 如果在定义策略后策略设置留空，则不会强制实施该策略。

从 Windows 10 版本 1607 和 Windows Server 2016 开始的计算机上的默认安全描述符只允许本地（内置）管理员组在非域控制器上远程访问 SAM，并允许每个人在域控制器上进行访问。 可以编辑默认安全描述符，以允许或拒绝其他用户和组，包括内置管理员。

运行早期 Windows 版本的计算机上的默认安全描述符不会限制对 SAM 的任何远程调用，但管理员可以编辑安全描述符以强制实施限制。 这种限制较少的默认值允许测试对现有应用程序启用限制的影响。

策略和注册表名称

	描述
策略名称	网络访问：限制允许远程调用 SAM 的客户端
位置	计算机配置 |Windows 设置 |安全设置 |本地策略 |安全选项
可能值	- 未定义 - 已定义，以及允许或拒绝使用 SAMRPC 远程访问本地 SAM 或 Active Directory 的用户和组的安全描述符。
注册表位置	`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\RestrictRemoteSam`
注册表类型	REG_SZ
注册表值	包含要部署的安全描述符 SDDL 的字符串。

组策略设置仅在运行 Windows Server 2016 或 Windows 10 版本 1607 或更高版本的计算机上可用。 这些计算机是使用用户界面 (UI) 配置此设置的唯一选项。

在运行早期版本的 Windows 的计算机上，需要直接编辑注册表设置或使用组策略首选项。 若要避免在这种情况下手动设置它，可以在运行 Windows Server 2016 或 Windows 10 版本 1607 或更高版本的计算机上配置 GPO 本身，并使它适用于 GPO 范围内的所有计算机，因为在安装相应的知识库后，每台计算机上都存在同一注册表项。

备注

此策略的实施方式与其他"网络访问"策略类似，因为在列出的注册表路径中有一个策略元素。 不存在本地策略与企业策略的概念；只有一个策略设置，以写入的策略设置为准。

例如，假设本地管理员使用本地安全策略管理单元 (Secpol.msc)（用于编辑同一注册表路径）将此设置配置作为本地策略的一部分。 如果企业管理员将此设置配置作为企业 GPO 的一部分，该企业 GPO 将覆盖同一注册表路径。

默认值

从 Windows 10 版本 1607 和 Windows Server 2016 开始，与早期版本的 Windows 相比，计算机具有硬编码和限制更严格的默认值。 不同的默认值有助于在最近的 Windows 版本默认更安全且较旧版本不会发生任何中断性行为更改的情况下取得平衡。 管理员可以测试对早期版本的 Windows 应用相同的限制是否会在生产环境中实现此安全策略设置之前，导致现有应用程序出现兼容性问题。

换言之，每个知识库文章中的修补程序都提供必要的代码和功能，但需要在安装修补程序后配置限制，因为默认情况下，在早期版本的 Windows 中安装修补程序后不会启用任何限制。

	默认 SDDL	转换的 SDDL	备注
Windows Server 2016 (或更高版本) 域控制器 (读取 Active Directory)	""	-	每个人都有保持兼容性的读取权限。
早期的域控制器	-	-	默认情况下不执行任何访问检查。

	默认 SDDL	转换的 SDDL	备注
Windows 10 版本 1607 (或更高版本) 非域控制器	`O:SYG:SYD:(A;;RC;;;BA)`	所有者： NTAUTHORITY/SYSTEM (WellKnownGroup) (S-1-5-18) 主要组： NTAUTHORITY/SYSTEM (WellKnownGroup) (S-1-5-18) DACL： - 修订：0x02 - 大小：0x0020 - 王牌计数：0x001 - Ace[00]---------- - Ace 类型：0x00 (ACCESS_ALLOWED_ACE_TYPE) Ace 大小：0x0018 继承标志：0x00 访问掩码：0x00020000 AceSid： BUILTIN\Administrators (Alias) (S-1-5-32-544) SACL：不存在	仅对本地（内置）管理员组成员授予 RC 访问（READ_CONTROL，也称为 STANDARD_RIGHTS_READ）。
早期的非域控制器	-	-	默认情况下不执行任何访问检查。

策略管理

本部分介绍了如何配置仅审核模式，如何分析在启用**网络访问：限制允许远程调用 SAM 的客户端**安全策略设置时记录的相关事件，以及如何配置事件限制以防止填满事件日志。

仅审核模式

仅审核模式将 SAMRPC 协议配置为针对当前配置的安全描述符执行访问检查，但如果访问检查失败，则不会使调用失败。 相反，将会允许调用，但是，如果已启用该功能，SAMRPC 会记录事件，描述会发生的情况。 此模式为管理员提供了在生产中启用策略之前测试其应用程序的方法。 默认情况下，仅审核模式未配置。 若要配置，请添加以下注册表设置。

注册表	详细信息

注册表	详细信息
路径	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
设置	RestrictRemoteSamAuditOnlyMode
数据类型	REG_DWORD
值	1
注意	无法使用预定义组策略设置添加或删除此设置。 如果需要，管理员可以创建自定义策略来设置注册表值。 无需重启，SAM 即可动态响应该注册表值中的更改。

相关事件

有相应的事件可以指示限制远程调用 SAM 的时间、尝试从 SAM 数据库读取的帐户等。 建议使用以下工作流识别因限制远程调用 SAM 可能会受到影响的应用程序：

1. 将事件日志转储到共享。
2. 右键单击“系统日志”，选择“ **筛选当前日志**”，并在“事件 ID”字段中指定 `16962-16969`。
3. 使用事件源 **Directory-Service-SAM** 查看下表中列出的事件 ID 16962 到 16969。
4. 确定哪些安全上下文在 SAM 数据库中枚举用户或组。
5. 对调用方设置优先级，确定是否应允许他们，然后将允许的调用方包括在 SDDL 字符串中。

事件 ID	事件消息文本	描述
16962	“正在使用默认安全描述符限制远程调用 SAM 数据库：%1.%n” %2 -“默认 SD 字符串：”	在缺少注册表 SDDL，从而导致回退到默认硬编码 SDDL 时发出事件（事件应包括默认 SDDL 的副本）。
16963	消息文本：“正在使用配置的注册表安全描述符限制远程调用 SAM 数据库：%1.%n” %1 -“注册表 SD 字符串：”	在从注册表（在启动或更改时）读取新 SDDL 并被视为有效时发出事件。 事件包括来源和已查询 SDDL 的副本。

事件 ID	事件消息文本	描述
16964	“注册表安全描述符格式不正确：%1.%n 正在使用默认安全描述符限制远程调用 SAM 数据库：%2.%n” %1 -“格式不正确的 SD 字符串：” %2 -“默认 SD 字符串：”	在注册表 SDDL 格式不正确，从而导致回退到默认硬编码 SDDL 时发出事件（事件应包括默认 SDDL 的副本）。
16965	消息文本：“远程调用 SAM 数据库已被拒绝。%n客户端 SID：%1%n 网络地址：%2%n” %1 -“客户端 SID：”%2 -“客户端网络地址”	拒绝访问远程客户端时发出事件。 事件应包括标识和客户端的网络地址。
16966	审核模式已启用 消息文本：“现已针对远程调用 SAM 数据库启用仅审核模式。 SAM 将为在正常模式下会被拒绝访问的客户端记录事件。 %n”	无论何时，在启用或禁用培训模式时（请参阅 16968）发出事件。
16967	审核模式已禁用 消息文本：“现已针对远程调用 SAM 数据库禁用仅审核模式。%n 了解详细信息”	无论何时，在启用或禁用培训模式时（请参阅 16968）发出事件。
16968	消息文本：“当前已针对远程调用 SAM 数据库启用仅审核模式。%n 以下客户端通常会被拒绝访问：%n客户端 SID：%1 来自网络地址：%2。 %n” %1 -“客户端 SID：” %2 -“客户端网络地址：”	当访问远程客户端会被拒绝，但由于启用培训模式而允许通过时，发出事件。 事件应包括标识和客户端的网络地址。
16969	消息文本：“%2 对 SAM 数据库的远程调用在过去 %1 秒限制窗口中被拒绝。%n ”%1 -“限制时段：” %2 -“已取消消息计数：”	由于在某些服务器上会导致事件日志换行的预期大容量，限制对于某些事件可能是必要的。 注意：启用审核模式时，不会限制事件。 具有大量低特权和匿名远程数据库查询的环境可能会看到大量记录在系统日志中的事件。 有关详细信息，请参阅设置限制部分。

对比尝试远程枚举帐户的安全上下文与默认安全描述符。 然后编辑安全描述符，以添加需要远程访问的帐户。

事件限制

忙碌的服务器可能使用与远程枚举访问检查相关的事件填满事件日志。 为了防止这种情况，默认情况下每 15 分钟记录一次拒绝访问的事件。 此时间段的长度由以下注册表值控制。

注册表路径	**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa**
设置	RestrictRemoteSamEventThrottlingWindow
数据类型	DWORD
值	秒
是否需要重启？	否
注意	**默认值为** 900 秒 (15 分钟) 。 限制使用从 0 开始并在限制时段内递增的抑制事件计数器。 例如，在过去 15 分钟内已取消 X 个事件。 在记录事件 16969 后会重启计数器。

重启要求

无需重启即可启用、禁用或修改 **网络访问：限制允许对 SAM 安全策略设置进行远程调用的客户端** ，包括仅审核模式。 更改在本地保存或通过组策略分发时，无需重启设备即可生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

SAMRPC 协议具有默认的安全状况，使低特权攻击者可能在网络上的计算机中查询对其进一步的黑客攻击和渗透计划至关重要的数据。

以下示例说明了攻击者利用远程 SAM 枚举的方式：

1. 低特权攻击者在网络上获得立足点。
2. 然后攻击者会查询网络上的所有计算机，以确定将高特权域用户配置为该计算机上的本地管理员的计算机。
3. 如果攻击者可以，然后在该计算机上找到允许接管该计算机的任何其他漏洞，攻击者随后可以蹲在计算机等待高特权用户登录，然后窃取或模拟这些凭据。

对策

你可以通过启用**网络访问：限制允许远程调用 SAM 的客户端**安全性策略设置和仅为明确允许访问的这些帐户配置 SDDL 减少此漏洞。

潜在影响

如果已定义策略，则管理员工具、脚本和以前枚举用户、组和组成员身份的软件可能会失败。 若要找出可能会受到影响的帐户，请在仅审核模式中测试此设置。

后续步骤

安全选项

网络访问：可匿名访问的共享

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 ：**可以匿名访问的共享**安全策略设置。

参考

此策略设置确定匿名用户可以访问哪些共享文件夹。

可能值

- 用户定义的共享文件夹列表
- 未定义

最佳做法

- 将此策略设置为 null 值。 应该影响不大，因为此 null 值是默认值。 所有用户都必须经过身份验证，然后才能访问服务器上的共享资源。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	未定义

服务器类型或 GPO	默认值
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

任何网络用户都可以访问列出的任何共享文件夹，这可能会导致敏感数据泄露或损坏。

对策

配置 “**网络访问：可以匿名访问的共享** ”设置为 null 值。

潜在影响

应该影响不大，因为此状态是默认配置。 只有经过身份验证的用户有权访问服务器上的共享资源。

相关主题

- 安全选项

网络访问: 本地帐户的共享和安全模型

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络访问的最佳做法、位置、值、策略管理和安全注意事项 **：本地帐户安全策略设置的共享和安全模型** 。

参考

此策略设置确定如何对使用本地帐户的网络登录进行身份验证。 如果将此策略设置配置为“经典”，则使用本地帐户凭据的网络登录会使用这些凭据进行身份验证。 如果将此策略设置配置为“仅来宾”，则使用本地帐户的网络登录会自动映射到来宾帐户。 经典模型提供对资源访问权限的精确控制，使你能够针对同一资源向不同用户授予不同类型的访问权限。 相反，“仅来宾”模型平等对待所有用户，并且他们都会获得对给定资源（可以是只读资源）的相同级别访问权限。

> **注意：** 此策略设置不会影响使用域帐户的网络登录。 此策略设置也不会影响通过 Telnet 或远程桌面服务等服务远程执行的交互式登录。 当设备未加入域时，此策略设置还会定制 Windows 资源管理器中的“**共享和安全**”选项卡，以对应于正在使用的共享和安全模型。

如果此策略设置的值为 “**仅来宾 - 本地用户**”，**则**可以通过网络访问你的设备的任何用户都以来宾用户权限进行身份验证。 此权限意味着他们可能无法写入共享文件夹。 尽管此限制确实提高了安全性，但授权用户无法访问这些系统上的共享资源。 如果值为 **Classic - 本地用户本身进行身份验证**，则本地帐户必须受密码保护;否则，任何人都可以使用这些用户帐户来访问共享的系统资源。

可能值

- 经典 - 本地用户以自己身份进行身份验证
- 仅限来宾 - 本地用户以来宾身份进行身份验证
- 未定义

最佳做法

1. 对于网络服务器，将此策略设置为 “**经典 - 本地用户**”**作为自身进行身份验证。**

2. 在最终用户系统上，将此策略设置为 “**仅来宾 - 本地用户身份验证为来宾**”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	经典 (本地用户以自身身份进行身份验证)
DC 有效默认设置	经典 (本地用户以自身身份进行身份验证)
成员服务器有效默认设置	经典 (本地用户以自身身份进行身份验证)
客户端计算机有效默认设置	经典 (本地用户以自身身份进行身份验证)

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

使用“仅来宾”模型时，任何可以通过网络向设备进行身份验证的用户都使用来宾权限执行此操作，这可能意味着他们对该设备上的共享资源没有写入访问权限。 尽管此限制确实提高了安全性，但授权用户更难访问这些计算机上的共享资源，因为这些资源的 ACL 必须包含访问控制条目 (ACE) 来宾帐户。 使用经典模型时，本地帐户应受密码保护。 否则，如果启用了来宾访问，任何人都可以使用这些用户帐户来访问共享的系统资源。

对策

对于网络服务器，请配置“**网络访问：本地帐户的共享和安全模型**”**设置为**“**经典 – 本地用户以自己身份进行身份验证**”。 在最终用户计算机上，将此策略设置配置为 “**仅来宾 – 本地用户以来宾身份进行身份验证**”。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

网络安全: 允许本地系统将计算机标识用于 NTLM

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的位置、值、策略管理和 **安全注意事项：允许本地系统将计算机标识用于 NTLM** 安全策略设置。

参考

当服务连接到运行 Windows Vista 或 Windows Server 2008 之前的 Windows 操作系统版本的设备时，作为本地系统运行并使用 SPNEGO (协商)（还原 NTLM）的服务将匿名进行身份验证。 在 Windows Server 2008 R2 和 Windows 7 及更高版本中，如果服务连接到运行 Windows Server 2008 或 Windows Vista 的计算机，则系统服务将使用计算机标识。

当服务使用设备标识进行连接时，支持签名和加密以提供数据保护。 (当服务匿名连接时，会创建系统生成的会话密钥，该密钥不提供保护，但它允许应用程序对数据进行签名和加密，而不会出错。匿名身份验证使用 NULL 会话，该会话与服务器不执行用户身份验证;因此，允许匿名访问。）

可能值

设置	Windows Server 2008 和 Windows Vista	至少 Windows Server 2008 R2 和 Windows 7
启用	作为使用 Negotiate 的本地系统运行的服务将使用计算机标识。 此值可能会导致 Windows 操作系统之间的某些身份验证请求失败并记录错误。	作为使用 Negotiate 的本地系统运行的服务将使用计算机标识。 此行为是默认行为。
禁用	作为本地系统运行的服务在还原为 NTLM 身份验证时使用 Negotiate 进行匿名身份验证。 此行为是默认行为。	作为本地系统运行的服务在还原为 NTLM 身份验证时使用 Negotiate 进行匿名身份验证。

设置	Windows Server 2008 和 Windows Vista	至少 Windows Server 2008 R2 和 Windows 7
两者都不是	作为本地系统运行的服务在还原为 NTLM 身份验证时使用 Negotiate 进行匿名身份验证。	作为使用 Negotiate 的本地系统运行的服务将使用计算机标识。 此行为可能会导致 Windows 操作系统之间的某些身份验证请求失败并记录错误。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	不适用
成员服务器有效默认设置	不适用
客户端计算机上有效的 GPO 默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突注意事项

策略 “网络安全：允许 LocalSystem NULL 会话回退”（如果已启用），将允许在系统服务尝试身份验证时使用 NTLM 或 Kerberos 身份验证。 此特权会以牺牲安全性为代价提高互

操作性的成功性。

Windows Server 2008 和 Windows Vista 的匿名身份验证行为与更高版本的 Windows 不同。 在这些系统上配置和应用此策略设置可能不会产生相同的结果。

组策略

可以通过使用要通过组策略对象 (GPO) 分发的组策略管理控制台 (GPMC) 来配置此策略设置。 如果分布式 GPO 中未包含此策略，则可以使用本地安全策略管理单元在本地计算机上配置此策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当服务连接到运行低于 Windows Vista 或 Windows Server 2008 版本的 Windows 的计算机时，作为本地系统运行并使用 SPNEGO (协商) 还原 NTLM 的服务将使用 NULL 会话。 在 Windows Server 2008 R2 和 Windows 7 及更高版本中，如果服务连接到运行 Windows Server 2008 或 Windows Vista 的计算机，则系统服务将使用计算机标识。

当服务与计算机标识连接时，支持签名和加密以提供数据保护。 当服务使用 NULL 会话进行连接时，会创建系统生成的会话密钥，该密钥不提供保护，但它允许应用程序对数据进行签名和加密，而不会出错。

对策

可以配置 “**网络安全：允许本地系统使用 NTLM 的计算机标识** ”安全策略设置，以允许使用 Negotiate 的本地系统服务在还原为 NTLM 身份验证时使用计算机标识。

潜在影响

如果未在 Windows Server 2008 和 Windows Vista 上配置此策略设置，则作为本地系统运行的服务将使用 NULL 会话，并还原早于 Windows Vista 或 Windows Server 2008 的 Windows 操作系统的 NTLM 身份验证。 从 Windows Server 2008 R2 和 Windows 7 开始，系统允许使用 Negotiate 的本地系统服务在还原为 NTLM 身份验证时使用计算机标识。

相关文章

- 安全选项

网络安全: 允许 LocalSystem NULL 会话回退

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **网络安全：允许 LocalSystem NULL 会话回退** 安全策略设置的最佳做法、位置、值和安全注意事项。

参考

此策略会影响运行 Windows Server 2008 R2 和 Windows 7 及更高版本的设备与运行早期版本的 Windows 操作系统的设备之间的身份验证过程中的会话安全性。 对于运行 Windows Server 2008 R2 和 Windows 7 及更高版本的计算机，作为本地系统运行的服务需要服务主体名称 (SPN) 才能生成会话密钥。 但是，如果 "网络安全：允许本地系统使用 NTLM 的计算机标识 "设置为"已禁用"，则作为本地系统运行的服务在将数据传输到运行早于 Windows Vista 或 Windows Server 2008 版本的服务器时，将回退到使用 NULL 会话身份验证。 NULL 会话不会为每个身份验证建立唯一的会话密钥;因此，它无法提供完整性或机密性保护。 " **网络安全：允许 LocalSystem NULL 会话回退** "设置确定是否允许请求使用会话安全性的服务使用已知密钥执行签名或加密功能以实现应用程序兼容性。

可能值

- **Enabled**

  当作为本地系统运行的服务使用 NULL 会话进行连接时，将创建系统生成的会话密钥，该密钥不提供任何保护，但允许应用程序对数据进行签名和加密，而不会出错。 这会增加应用程序兼容性，但会降低安全级别。

- **禁用**

  当作为本地系统运行的服务使用 NULL 会话进行连接时，会话安全性将不可用。 寻求加密或签名的调用将失败。 此设置更安全，但存在降低应用程序不兼容的风险。 使用设备标识而不是 NULL 会话的调用仍将完全使用会话安全性。

- 未定义。 如果未定义此策略，则默认值将生效。 此策略对于早于 Windows Server 2008 R2 和 Windows 7 的 Windows 操作系统版本启用，否则为"禁用"。

最佳做法

当服务与设备标识连接时，支持签名和加密以提供数据保护。 当服务使用 NULL 会话连接时，不会提供此级别的数据保护。 但是，你需要评估环境以确定支持的 Windows 操作系统版本。 如果启用此策略，某些服务可能无法进行身份验证。

此策略适用于 Windows Server 2008 和 Windows Vista (SP1 及更高版本) 。 当环境不再需要支持 Windows NT 4 时，应禁用此策略。 默认情况下，它在 Windows 7 和 Windows Server 2008 R2 及更高版本中处于禁用状态。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	不适用
成员服务器有效默认设置	不适用
客户端计算机上有效的 GPO 默认设置	不适用

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果此设置为“启用”，则当服务使用 NULL 会话进行连接时，将创建系统生成的会话密钥，该密钥不提供任何保护，但允许应用程序对数据进行签名和加密，而不会出错。 可能会公开要保护的数据。

对策

可以将计算机配置为将本地系统的计算机标识与“ **网络安全：允许本地系统使用 NTLM 的计算机标识**”策略。 如果这是不可能的，则此策略可用于防止数据在传输过程中公开（如果数据受已知密钥保护）。

潜在影响

如果启用此策略，将 NULL 会话与本地系统配合使用的服务可能无法进行身份验证，因为将禁止它们使用签名和加密。

相关主题

- 安全选项

网络安全: 允许对此计算机的 PKU2U 身份验证请求使用联机标识

项目 • 2023/03/09

适用范围

- Windows 11
- Windows 10

本文介绍网络安全的最佳做法、位置和值 **：允许对此计算机的 PKU2U 身份验证请求使用联机标识** 安全策略设置。

参考

在 Windows Server 2008 R2 和 Windows 7 中，协商安全支持提供程序 (SSP) 支持扩展 SSP Negoexts.dll。 Windows 操作系统将此扩展 SSP 视为身份验证协议。 它支持 Microsoft 的 SSP，包括 PKU2U。 还可以开发或添加其他 SSP。

当设备配置为使用联机 ID 接受身份验证请求时，Negoexts.dll在用于登录的计算机上调用 PKU2U SSP。 PKU2U SSP 获取本地证书并在对等计算机之间交换策略。 在对等计算机上对其进行验证时，元数据中的证书将发送到登录对等方进行验证。 它将用户的证书关联到安全令牌，然后登录过程完成。

> **备注**
>
> 通过凭据管理器具有标准用户凭据的帐户的任何人都可以链接联机 ID。

默认情况下，未在已加入域的设备上配置此策略。 此禁用将禁止联机标识从 Windows 7 到 Windows 10 版本 1607 向已加入域的计算机进行身份验证。 默认情况下，此策略在 Windows 10 版本 1607 及更高版本中处于启用状态。

可能值

- **已启用**：此设置允许使用联机 ID 建立对等关系的两个 (或更多) 计算机之间成功完成身份验证。 PKU2U SSP 获取本地证书并在对等设备之间交换策略。 在对等计算机上验证时，元数据中的证书将发送到登录对等方进行验证。 它将用户的证书关联到安全令牌，然后登录过程完成。

  > **备注**

> 默认情况下，PKU2U 在 Windows Server 上处于禁用状态。 如果禁用 PKU2U，则远程桌面从已加入混合 Azure AD 的服务器连接到已加入 Azure AD 的Windows 10设备或已加入混合 Azure AD 的域成员Windows 10设备失败。 若要解决此问题，请在服务器和客户端上启用 PKU2U。

- **已禁用**：此设置可防止使用联机 ID 向对等关系中的另一台计算机对用户进行身份验证。
- ***未设置***：未配置此策略会阻止使用联机 ID 对用户进行身份验证。 此选项是已加入域的设备上的默认选项。

最佳做法

在域中，应使用域帐户进行身份验证。 将此策略设置为“**已禁用**”，或者不将此策略配置为排除联机标识用于仅本地环境的身份验证。 对于已加入混合和 Azure AD 的环境，将此策略设置为“**已启用**”。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的有效默认值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	禁用
成员服务器有效默认设置	禁用
Windows 10版本 1607 之前客户端计算机上的有效 GPO 默认设置	禁用
客户端计算机上的有效 GPO 默认设置Windows 10版本 1607 及更高版本	已启用

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置、如何实施对策，以及对策的可能负面影响。

漏洞

启用此策略设置允许一台计算机上的用户帐户与联机标识（例如 Microsoft 帐户或 Azure AD 帐户）相关联。 如果该对等设备同样配置) 而不使用 Windows 登录帐户 (域或本地) ，则该帐户随后可以登录到对等设备 (。 此设置不仅有益，而且对于已加入 Azure AD 的设备来说是必需的，这些设备使用联机标识登录，并由 Azure AD 颁发证书。 此策略可能与 *仅本地* 环境无关，并且可能绕过已建立的安全策略。 但是，在使用 Azure AD 的混合环境中，它不会造成任何威胁，因为它依赖于用户的联机标识和 Azure AD 进行身份验证。

对策

将此策略设置为 *"已禁用"*，或者不为 *仅本地* 环境配置此安全策略。

潜在影响

如果未设置或禁用此策略，则 PKU2U 协议不会用于在对等设备之间进行身份验证，这会强制用户遵循域定义的访问控制策略。 此禁用是 *仅限本地* 环境中的有效配置。 某些角色/功能（（例如故障转移群集））不使用域帐户进行 PKU2U 身份验证，在禁用此策略时将停止正常运行。

如果在混合环境中启用此策略，则允许用户使用 Azure AD 颁发的证书及其在相应设备之间的联机标识进行身份验证。 此配置允许用户在此类设备之间共享资源。 如果未启用此策略，则无法与已加入 Azure AD 的设备建立远程连接。

修复/修正

此漏洞已于 2021 年 2 月 9 日在 CVE-2021-25195 安全更新中修复。

相关主题

- 安全选项

网络安全: 配置 Kerberos 允许的加密类型

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10
- Windows Server

介绍网络安全的最佳做法、位置、值和安全注意事项 **：配置 Kerberos 安全策略设置允许的加密类型** 。

参考

通过此策略设置，可以设置 Kerberos 协议允许使用的加密类型。 如果未选择，则不允许使用加密类型。 此设置可能会影响与客户端计算机、服务和应用程序的兼容性。 允许多个选择。

有关详细信息，请参阅 如果禁用 Kerberos 的 DES，则记录 KDC 事件 ID 16 或 27。

下表列出了并说明了允许的加密类型。

加密类型	说明和版本支持
DES_CBC_CRC	使用循环冗余检查函数使用密码块链接的数据加密标准 在 Windows 2000 Server、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 中受支持。 默认情况下，Windows 7、Windows 10、Windows 11、Windows Server 2008 R2 及更高版本的操作系统不支持 DES。
DES_CBC_MD5	使用 Message-Digest 算法 5 校验和函数进行加密块链接的数据加密标准 在 Windows 2000 Server、Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 中受支持。 默认情况下，Windows 7、Windows 10、Windows 11、Windows Server 2008 R2 及更高版本的操作系统不支持 DES。
RC4_HMAC_MD5	使用 Message-Digest 算法 5 校验和函数使用哈希消息身份验证代码的 Rivest 4 在 Windows 2000 Server、Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、Windows 10、Windows 11、Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2 中受支持。

加密类型	说明和版本支持
AES128_HMAC_SHA1	使用安全哈希算法的 128 位加密块中的高级加密标准与哈希消息身份验证代码 (1) 。 Windows 2000 Server、Windows XP 或 Windows Server 2003 不支持。 在 Windows Vista、Windows Server 2008、Windows 7、Windows 10、Windows 11、Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2 中受支持。
AES256_HMAC_SHA1	使用安全哈希算法的 256 位密码块中的高级加密标准与哈希消息身份验证代码 (1) 。 Windows 2000 Server、Windows XP 或 Windows Server 2003 不支持。 在 Windows Vista、Windows Server 2008、Windows 7、Windows 10、Windows 11、Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2 中受支持。
将来的加密类型	Microsoft 为可能实现的其他加密类型保留。

可能值

加密类型选项包括：

- DES_CBC_CRC
- DES_CBC_MD5
- RC4_HMAC_MD5
- AES128_HMAC_SHA1
- AES256_HMAC_SHA1
- 将来的加密类型

  从 Windows 7 和 Windows Server 2008 R2 版本开始，Microsoft 为可能实现的其他加密类型保留这些选项。

最佳做法

分析环境以确定支持哪些加密类型，然后选择满足该评估条件的类型。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	默认 OS 设置适用，默认情况下不支持 DES 套件。
成员服务器有效默认设置	默认 OS 设置适用，默认情况下不支持 DES 套件。
客户端计算机上有效的 GPO 默认设置	默认 OS 设置适用，默认情况下不支持 DES 套件。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

Windows Server 2008 R2、Windows 7 和 Windows 10 不支持 DES 加密套件，因为有更强的加密套件可用。 若要启用与非 Windows 版本的 Kerberos 协议的 Kerberos 互操作性，可以启用这些套件。 但是，这样做可能会在运行 Windows Server 2008 R2、Windows 7 和 Windows 10 的计算机上打开攻击途径。 还可以为运行 Windows Vista 和 Windows Server 2008 的计算机禁用 DES。

对策

不要配置此策略。 此禁用将强制运行 Windows Server 2008 R2、Windows 7 和 Windows 10 的计算机使用 AES 或 RC4 加密套件。

潜在影响

如果未选择任何加密类型，则运行 Windows Server 2008 R2、Windows 7 和 Windows 10 的计算机在与运行非 Windows 版本的 Kerberos 协议的计算机连接时，可能会出现 Kerberos 身份验证失败。

如果选择任何加密类型，则会降低 Kerberos 身份验证加密的有效性，但会改进与运行旧版 Windows 的计算机的互操作性。 Kerberos 协议的当代非 Windows 实现支持 RC4 和

AES 128 位和 AES 256 位加密。 大多数实现（包括 MIT Kerberos 协议和 Windows Kerberos 协议）都已弃用 DES 加密。

相关文章

- 安全选项

网络安全: 在下一次更改密码时不存储 LAN 管理器哈希值

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：不要在下一个密码更改安全策略设置中存储 LAN Manager 哈希值** 。

参考

此策略设置确定是否阻止 LAN 管理器在下次更改密码时存储新密码的哈希值。 哈希值是应用加密算法后密码的表示形式，该算法对应于算法指定的格式。 若要解密哈希值，必须确定加密算法，然后反向加密算法。 与加密更强的 NTLM 哈希相比，LAN 管理器哈希相对较弱，容易受到攻击。 由于 LM 哈希存储在安全数据库中的本地设备上，因此，如果安全数据库安全帐户管理器 (SAM) 受到攻击，密码可能会遭到入侵。

当攻击者攻击 SAM 文件时，他们可能会获得对用户名和密码哈希的访问权限。 攻击者可以使用密码破解工具来确定密码是什么。 他们有权访问此信息后，可以通过模拟用户来使用它来访问网络上的资源。 启用此策略设置不会阻止这些类型的攻击，但会使它们更加困难。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 将“**网络安全”设置为“启用”，不要在下次密码更改时存储 LAN Manager 哈希值。**
- 要求所有用户在下次登录到域时设置新密码，以便删除 LAN 管理器哈希。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

寻求访问用户名和密码哈希的攻击者可能会针对 SAM 文件。 此类攻击使用特殊工具来发现密码，然后可用于模拟用户并访问网络上的资源。 启用此策略设置无法阻止这些类型的攻击，因为 LAN 管理器哈希比 NTLM 哈希弱得多，但这些攻击要成功要困难得多。

对策

启用 **网络安全：在下一个密码更改设置时不要存储 LAN 管理器哈希值** 。 要求所有用户在下次登录到域时设置新密码，以便删除 LAN 管理器哈希。

潜在影响

某些非 Microsoft 应用程序可能无法连接到系统。

相关主题

- 安全选项

网络安全: 在超过登录时间后强制注销

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：在登录时间过期时强制注销** 安全策略设置。

参考

此安全设置确定是否在用户帐户的有效登录时间之外断开连接到本地设备的用户的连接。 此设置会影响服务器消息块 (SMB) 组件。

此策略设置不适用于管理员帐户，但它的行为与帐户策略相同。 对于域帐户，只能有一个帐户策略。 帐户策略必须在默认域策略中定义，并且由构成域的域控制器强制实施。 域控制器始终从默认域策略组策略对象 (GPO) 拉取帐户策略，即使有其他帐户策略应用于包含域控制器的组织单位也是如此。 默认情况下，加入域的工作站和服务器 (例如，成员设备) 也为其本地帐户接收相同的帐户策略。 但是，通过为包含成员设备的组织单位定义帐户策略，成员设备的本地帐户策略可以不同于域帐户策略。 Kerberos 设置不会应用于成员设备。

可能值

- 已启用

  启用后，此策略会导致客户端与 SMB 服务器的客户端会话在客户端登录时间过期时强制断开连接。

- 禁用

  禁用后，此策略允许在客户端的登录时间过期后继续建立的客户端会话。

- 未定义

最佳做法

- 将 “**网络安全：登录时间过期时强制注销** ”设置为“已启用”。 当用户的登录时间过期时，成员服务器上的 SMB 会话将终止，并且用户将无法登录到系统，直到其下一个计划的访问时间开始。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	禁用
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果禁用此策略设置，用户可以在其分配的登录时间之外保持与计算机的连接。

对策

启用 “**网络安全：登录时间过期时强制注销**” 设置。 此策略设置不适用于管理员帐户。

潜在影响

当用户的登录时间过期时，SMB 会话会终止。 在下一个计划访问时间开始之前，用户无法登录到设备。

相关文章

- 安全选项

网络安全: LAN 管理器身份验证级别

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **网络安全：LAN Manager 身份验证级别** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定用于网络登录的质询或响应身份验证协议。 LAN Manager (LM) 包括 Microsoft 提供的客户端计算机和服务器软件，允许用户在单个网络上将个人设备链接在一起。 网络功能包括透明文件和打印共享、用户安全功能和网络管理工具。 在 Active Directory 域中，Kerberos 协议是默认身份验证协议。 但是，如果出于某种原因未协商 Kerberos 协议，Active Directory 将使用 LM、NTLM 或 NTLM 版本 2 (NTLMv2) 。

LAN Manager 身份验证包括 LM、NTLM 和 NTLMv2 变体，它是在运行 Windows 操作系统的所有客户端设备执行以下操作时用于对运行 Windows 操作系统的所有客户端设备进行身份验证的协议：

- 加入域
- 在 Active Directory 林之间进行身份验证
- 基于早期版本的 Windows 操作系统对域进行身份验证
- 从 Windows 2000 开始，向未运行 Windows 操作系统的计算机进行身份验证
- 对不在域中的计算机进行身份验证

可能值

- 发送 LM & NTLM 响应
- 发送 LM & NTLM - 使用 NTLMv2 会话安全性（如果协商）
- 仅发送 NTLM 响应
- 仅发送 NTLMv2 响应
- 仅发送 NTLMv2 响应。 拒绝 LM
- 仅发送 NTLMv2 响应。 拒绝 LM & NTLM
- 未定义

网络安全：LAN Manager 身份验证级别设置确定用于网络登录的质询/响应身份验证协议。 此选项会影响客户端使用的身份验证协议级别、计算机协商的会话安全级别以及服

务器接受的身份验证级别。 下表标识了策略设置，介绍了设置，并标识了在相应注册表设置中使用的安全级别（如果选择使用注册表来控制此设置而不是策略设置）。

设置	描述	注册表安全级别
发送 LM & NTLM 响应	客户端设备使用 LM 和 NTLM 身份验证，并且从不使用 NTLMv2 会话安全性。 域控制器接受 LM、NTLM 和 NTLMv2 身份验证。	0
发送 LM & NTLM - 使用 NTLMv2 会话安全性（如果协商）	客户端设备使用 LM 和 NTLM 身份验证，如果服务器支持，则它们使用 NTLMv2 会话安全性。 域控制器接受 LM、NTLM 和 NTLMv2 身份验证。	1
仅发送 NTLM 响应	客户端设备使用 NTLMv1 身份验证，如果服务器支持 NTLMv2 会话安全性，则使用 NTLMv2 会话安全性。 域控制器接受 LM、NTLM 和 NTLMv2 身份验证。	2
仅发送 NTLMv2 响应	客户端设备使用 NTLMv2 身份验证，如果服务器支持 NTLMv2 会话安全性，则使用 NTLMv2 会话安全性。 域控制器接受 LM、NTLM 和 NTLMv2 身份验证。	3
仅发送 NTLMv2 响应。 拒绝 LM	客户端设备使用 NTLMv2 身份验证，如果服务器支持 NTLMv2 会话安全性，则使用 NTLMv2 会话安全性。 域控制器拒绝接受 LM 身份验证，它们将仅接受 NTLM 和 NTLMv2 身份验证。	4
仅发送 NTLMv2 响应。 拒绝 LM & NTLM	客户端设备使用 NTLMv2 身份验证，如果服务器支持 NTLMv2 会话安全性，则使用 NTLMv2 会话安全性。 域控制器拒绝接受 LM 和 NTLM 身份验证，它们仅接受 NTLMv2 身份验证。	5

最佳做法

- 最佳做法取决于特定的安全和身份验证要求。

策略位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

注册表位置

HKLM\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel

默认值

下表列出了此策略的实际和有效的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	仅发送 NTLMv2 响应
DC 有效默认设置	仅发送 NTLMv2 响应
成员服务器有效默认设置	仅发送 NTLMv2 响应
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

修改此设置可能会影响与客户端设备、服务和应用程序的兼容性。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

在 Windows 7 和 Windows Vista 中，此设置未定义。 在 Windows Server 2008 R2 及更高版本中，此设置配置为 **仅发送 NTLMv2 响应**。

对策

将 “**网络安全：LAN 管理器身份验证级别** ”设置配置为 “**仅发送 NTLMv2 响应**”。 当所有客户端计算机都支持 NTLMv2 时，Microsoft 和许多独立组织强烈建议使用此级别的身份验证。

潜在影响

不支持 NTLMv2 身份验证的客户端设备无法在域中进行身份验证，无法使用 LM 和 NTLM 访问域资源。

相关主题

- 安全选项

网络安全: LDAP 客户端签名要求

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

此安全策略参考主题面向 IT 专业人员，介绍了此策略设置的最佳做法、位置、值、策略管理和安全注意事项。 此信息适用于至少运行 Windows Server 2008 操作系统的计算机。

参考

此策略设置确定代表发出 LDAP BIND 请求的客户端设备请求的数据签名级别。 以下列表中介绍了数据签名的级别：

- **无。** LDAP BIND 请求使用调用方指定的选项发出。
- **协商签名。** 如果传输层安全性/安全套接字层 (TLS/SSL) 尚未启动，则除了调用方指定的选项外，还会使用 LDAP 数据签名选项集启动 LDAP BIND 请求。 如果已启动 TLS/SSL，则使用调用方指定的选项启动 LDAP BIND 请求。
- **需要签名。** 此级别与 **协商签名**相同。 但是，如果 LDAP 服务器的中间 saslBindInProgress 响应未指示需要 LDAP 流量签名，则调用方将返回 LDAP BIND 命令请求失败的消息。

滥用此策略设置是一个常见错误，可能会导致数据丢失或数据访问或安全性问题。

可能值

- 无
- 协商签名
- 需要签名
- 未定义

最佳做法

- 将 “**网络安全：LDAP 客户端签名要求** ”和 “**域控制器：LDAP 服务器签名要求** ”设置为 “**需要签名**”。 若要避免使用未签名的流量，请将客户端和服务器端设置为要求签名。 不设置任一端将阻止客户端计算机与服务器通信。 这种防护可能导致许多功能失败，包括用户身份验证、组策略和登录脚本。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	协商签名
DC 有效默认设置	协商签名
成员服务器有效默认设置	协商签名
客户端计算机有效默认设置	协商签名

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

修改此设置可能会影响与客户端设备、服务和应用程序的兼容性。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

未签名的网络流量容易受到中间人攻击，其中入侵者捕获客户端计算机和服务器之间的数据包，对其进行修改，然后将其转发到服务器。 对于 LDAP 服务器，这种易感性意味着攻击者可能导致服务器根据 LDAP 查询中的错误或更改的数据做出决策。 若要降低网络中的此风险，可以实施强大的物理安全措施来保护网络基础结构。 此外，如果需要通过 IPsec 身份验证标头对所有网络数据包进行数字签名，则可以使所有类型的中间人攻击变得困难。

对策

将 “**网络安全：LDAP 客户端签名要求** ”设置为 “**需要签名**”。

潜在影响

如果将客户端配置为需要 LDAP 签名，则它可能无法与不需要对请求进行签名的 LDAP 服务器通信。 若要避免此问题，请确保“ **网络安全：LDAP 客户端签名要求** ”和 “**域控制器：LDAP 服务器签名要求** ”设置都设置为“ **需要签名**”。

相关主题

- 安全选项

网络安全: 基于 NTLM SSP 的(包括安全 RPC)客户端的最小会话安全

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：基于 NTLM SSP 的最小会话安全性 (包括安全 RPC) 客户端** 安全策略设置。

参考

此策略设置允许客户端设备要求协商 128 位加密或 NTLMv2 会话安全性。 这些值取决于“**网络安全：LAN 管理器身份验证级别**”**策略** 设置值。

可能值

- 要求 NTLMv2 会话安全性

  如果未协商 NTLMv2 协议，连接将失败。

- 需要 128 位加密

  如果未协商强加密 (128 位) ，连接将失败。

最佳做法

设置此策略的做法取决于安全要求。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	需要 128 位加密
DC 有效默认设置	需要 128 位加密
成员服务器有效默认设置	需要 128 位加密
客户端计算机有效默认设置	需要 128 位加密

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略冲突

此安全策略的设置取决于 “**网络安全：LAN 管理器身份验证级别**”**策略** 设置值。 有关此策略的信息，请参阅 网络安全：LAN 管理器身份验证级别。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可能会公开使用 NTLM 安全支持提供程序 (NTLM SSP) 的网络流量，使已获得网络访问权限的攻击者可以制造中间人攻击。

对策

启用所有可用于 **网络安全的选项：基于 NTLM SSP 的最小会话安全性 (包括安全 RPC) 客户端策略** 设置。

潜在影响

强制实施这些设置的客户端设备无法与不支持这些设置的旧服务器通信。

相关主题

- 安全选项

网络安全: 基于 NTLM SSP 的(包括安全 RPC)服务器的最小会话安全

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的最佳做法、位置、值、策略管理和 **安全注意事项：基于 NTLM SSP 的最小会话安全性 (包括安全 RPC) 服务器** 安全策略设置。

参考

此策略设置允许客户端设备要求协商 128 位加密或 NTLMv2 会话安全性。 这些值取决于 网络安全：LAN Manager 身份验证级别 策略设置值。

为此策略设置设置所有这些值将有助于防止使用 NTLM 安全支持提供程序 (NTLM SSP) 的网络流量被已获取同一网络的恶意用户公开或篡改。 也就是说，这些设置有助于防止中间人攻击。

可能值

- 需要 128 位加密。 如果未协商强加密 (128 位) ，连接将失败。
- 需要 NTLMv2 会话安全性。 如果未协商 NTLMv2 协议，连接将失败。
- 未定义。

最佳做法

- 启用可用于此安全策略的所有值。 不支持这些策略设置的旧版客户端设备将无法与服务器通信。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	需要 128 位加密
DC 有效默认设置	需要 128 位加密
成员服务器有效默认设置	需要 128 位加密
客户端计算机有效默认设置	需要 128 位加密

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

策略依赖项

此安全策略的设置取决于 “网络安全：LAN 管理器身份验证级别 ”设置值。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可能会公开使用 NTLM 安全支持提供程序 (NTLM SSP) 的网络流量，使已获得网络访问权限的攻击者可以制造中间人攻击。

对策

启用所有可用于 **网络安全的选项：基于 NTLM SSP 的最小会话安全性 (包括安全 RPC) 服务器** 策略设置。

潜在影响

不支持这些安全设置的较旧客户端设备无法与设置此策略的计算机通信。

相关主题

- 安全选项

网络安全: 限制 NTLM: 为 NTLM 身份验证添加远程服务器例外

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的最佳做法、位置、值、管理方面和安全注意事项 **：限制 NTLM：为 NTLM 身份验证安全策略设置添加远程服务器例外** 。

参考

“ **网络安全：限制 NTLM：为 NTLM 身份验证添加远程服务器例外** ”策略设置允许创建允许客户端设备使用 NTLM 身份验证的远程服务器的例外列表，前提是配置了 “网络安全：限制 NTLM： 将 NTLM 流量传出到远程服务器 ”策略设置。

如果配置此策略设置，则可以定义允许客户端设备使用 NTLM 身份验证的远程服务器列表。

如果未配置此策略设置，则不会应用任何例外，并且如果 网络安全：限制 NTLM：向远程服务器的传出 NTLM 流量 已启用，则来自客户端设备的 NTLM 身份验证尝试将失败。

列出应用程序用作命名格式的 NetBIOS 服务器名称，每行一个。 若要确保出现异常，所有应用程序使用的名称必须位于列表中。 单个星号 (*) 可以在字符串中的任何位置用作通配符。

可能值

- 用户定义的远程服务器列表

  输入允许客户端使用 NTLM 身份验证的远程服务器列表时，将定义并启用策略。

- 未定义

  如果未通过定义服务器列表来配置此策略设置，则策略是未定义的，不会应用任何异常。

最佳做法

1. 首先强制实施 “网络安全：限制 NTLM：审核传入 NTLM 流量 ”或 “网络安全：限制 NTLM：在此域策略设置中审核 NTLM 身份验证 ”，然后查看操作事件日志以了解这些身份验证尝试涉及哪些服务器，以便可以决定要豁免的服务器。

2. 设置服务器例外列表后，强制实施 “网络安全：限制 NTLM：审核传入 NTLM 流量 ”或 “网络安全：限制 NTLM：在此域策略设置中审核 NTLM 身份验证 ”，然后在设置策略以阻止 NTLM 流量之前再次查看操作事件日志。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

通过 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置设置为“**未配置**”，将应用本地设置。

审计

查看操作事件日志，查看服务器异常列表是否按预期运行。 此设备上的审核和阻止事件记录在 **应用程序和服务日志**\Microsoft\Windows\NTLM 中的操作事件日志中。

没有安全审核策略可以配置为查看此策略的输出。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果已确定不应使用 NTLM 身份验证协议从客户端设备到任何远程服务器，因为需要使用更安全的协议（如 Kerberos），则可能有一些客户端应用程序仍在使用 NTLM。 如果是这样，并且你已将 “网络安全：限制 NTLM：向远程服务器传出 NTLM 流量 ”设置为任何拒绝选项，则这些应用程序将失败，因为来自客户端计算机的出站 NTLM 身份验证流量将被阻止。

如果定义了允许客户端设备使用 NTLM 身份验证的服务器例外列表，则 NTLM 身份验证流量将继续在这些客户端应用程序和服务器之间流动。 然后，服务器容易受到利用 NTLM 中安全漏洞的任何恶意攻击。

对策

使用 网络安全：限制 NTLM：以仅审核模式传出到远程服务器的 NTLM 流量 时，可以通过查看哪些客户端应用程序向环境中的远程服务器发出 NTLM 身份验证请求来确定。 评估后，必须逐个确定 NTLM 身份验证是否仍至少满足安全要求。 如果没有，则必须升级客户端应用程序才能使用 NTLM 身份验证以外的其他方法。

潜在影响

为此策略设置定义服务器列表将启用来自使用这些服务器的客户端应用程序的 NTLM 身份验证流量，并且此流量可能会导致安全漏洞。

如果未定义此列表，并且启用了 网络安全：限制 NTLM：传出到远程服务器的 NTLM 流量 ，则使用 NTLM 的客户端应用程序将无法对以前使用的那些服务器进行身份验证。

相关主题

- 安全选项

网络安全: 限制 NTLM: 添加此域中的服务器例外

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍网络安全的最佳做法、位置、值、管理方面和安全注意事项 **：限制 NTLM：在此域安全策略设置中添加服务器例外** 。

参考

" **网络安全：限制 NTLM：在此域中添加服务器例外** "策略设置允许在此域中创建一个服务器例外列表，如果"网络安全：限制此域中的 NTLM： NTLM 身份验证 "策略设置中设置了任一拒绝选项，则允许客户端设备使用 NTLM 直通身份验证。

如果配置此策略设置，则可以在此域中定义允许客户端设备使用 NTLM 身份验证的服务器列表。

如果未配置此策略设置，则不会应用任何例外，并且如果启用了 **网络安全：限制 NTLM：此域中的 NTLM 身份验证** ，则域中的所有 NTLM 身份验证尝试都将失败。

将 NetBIOS 服务器名称列出为命名格式，每行一个。 单个星号 (*) 可以在字符串中的任何位置用作通配符。

可能值

- 用户定义的服务器列表

  在此域中输入允许客户端使用 NTLM 身份验证的服务器列表时，将定义并启用策略。

- 未定义

  如果未通过定义服务器列表来配置此策略设置，则策略是未定义的，不会应用任何异常。

最佳做法

1. 首先强制实施 **网络安全：限制 NTLM：在此域策略设置中审核 NTLM 身份验证** ，然后查看操作事件日志以了解这些身份验证尝试中涉及哪些域控制器，以便可以决定要免除哪些服务器。
2. 设置服务器例外列表后，强制实施 “**网络安全：限制 NTLM：在此域中审核 NTLM 身份验证**” 策略设置，然后在设置策略以阻止 NTLM 流量之前再次查看操作事件日志。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 在本地保存或通过组策略分发时，此策略的更改无需重启即可生效。

组策略

通过 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。

审计

查看操作事件日志，查看服务器异常列表是否按预期运行。 此计算机上的审核和阻止事件记录在 **应用程序和服务日志\Microsoft\Windows\NTLM** 中的操作事件日志中。

没有安全审核策略可以配置为查看此策略的输出。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果确定不应在域中使用 NTLM 身份验证协议，因为需要使用更安全的协议（如 Kerberos），则域中可能仍存在一些 NTLM 身份验证流量。 如果是这样，并且你将此 域中的“网络安全：网络安全：限制 NTLM： NTLM 身份验证 ”设置为任何拒绝选项，则任何 NTLM 身份验证请求都将失败，因为传递成员服务器将阻止 NTLM 请求。

如果在此域中定义了允许客户端计算机使用 NTLM 直通身份验证的服务器例外列表，则 NTLM 身份验证流量将继续在这些服务器之间流动，这使得它们容易受到利用 NTLM 中安全漏洞的任何恶意攻击。

对策

在仅审核模式下 **使用此域中的“网络安全：限制 NTLM：NTLM”身份验证** 时，可以通过查看哪些客户端应用程序向直通身份验证服务器发出 NTLM 身份验证请求来确定。 评估后，必须逐个确定 NTLM 身份验证是否仍至少满足安全要求。

潜在影响

为此策略设置定义服务器列表将启用这些服务器之间的 NTLM 身份验证流量，这可能会导致安全漏洞。

如果未定义此列表，并且已启用 **网络安全：限制 NTLM：此域中的 NTLM 身份验证** ，则 NTLM 身份验证将在之前使用的域中的那些直通服务器上失败

相关主题

- 安全选项

网络安全: 限制 NTLM: 审核传入 NTLM 流量

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **网络安全：限制 NTLM：审核传入 NTLM 流量** 安全策略设置的最佳做法、位置、值、管理方面和安全注意事项。

参考

网络安全 **：限制 NTLM：审核传入 NTLM 流量** 策略设置允许审核传入 NTLM 流量。

在 组策略 内启用此审核策略时，它会在分发该组策略的任何服务器上强制实施。 这些事件将记录在 **应用程序和服务日志**\Microsoft\Windows\NTLM 中的操作事件日志中。 使用审核事件收集系统可帮助你更高效地收集事件进行分析。

在服务器上启用此策略时，只会记录发到该服务器的身份验证流量。

启用此审核策略时，其工作方式与 网络安全：限制 NTLM：传入 NTLM 流量 策略相同，但它实际上不会阻止任何流量。 因此，可以有效地使用它来了解环境中的身份验证流量，当准备好阻止该流量时，可以启用“网络安全：限制 NTLM：传入 NTLM 流量”策略设置，然后选择“ **拒绝所有帐户** ”或“ **拒绝所有域帐户** ”。

可能值

- 禁用

  设置此策略的服务器不会记录传入 NTLM 流量的事件。

- 为域帐户启用审核

  设置此策略的服务器将仅记录域中的帐户的 NTLM 直通身份验证请求事件，当 “网络安全：限制 NTLM：传入 NTLM 流量 ”策略设置为 “**拒绝所有域帐户**”时，才会阻止这些帐户。

- 为所有帐户启用审核

设置此策略的服务器将记录所有 NTLM 身份验证请求的事件，当 “网络安全：限制 NTLM： 传入 NTLM 流量 ”策略设置为 “**拒绝所有帐户**”时，将阻止这些请求。

- 未定义

  未定义的此状态与 “**禁用**”相同，并且不对 NTLM 流量进行审核。

最佳做法

根据环境和测试持续时间，定期监视日志大小。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 在本地保存或通过组策略分发时，此策略的更改无需重启即可生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。

审计

查看操作事件日志，查看此策略是否按预期运行。 此计算机上的审核和阻止事件记录在**应用程序和服务日志\Microsoft\Windows\NTLM** 中的操作事件日志中。 使用审核事件收集系统可帮助你更高效地收集事件进行分析。

没有安全审核事件策略可以配置为查看此策略的输出。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

NTLM 和 NTLMv2 身份验证容易受到各种恶意攻击，包括 SMB 中继、中间人攻击和暴力攻击。 减少和消除环境中的 NTLM 身份验证会强制 Windows 操作系统使用更安全的协议，例如 Kerberos 版本 5 协议或不同的身份验证机制（如智能卡）。

漏洞

启用此策略设置将通过日志记录来显示网络或域中哪些服务器和客户端计算机处理 NTLM 流量。 如果 NTLM 身份验证流量遭到入侵，则这些设备的标识可能以恶意方式使用。 策略设置不会阻止或缓解任何漏洞，因为它仅用于审核目的。

对策

在生产环境中启用此策略设置时，限制对日志文件的访问。

潜在影响

如果未启用或配置此策略设置，则不会记录 NTLM 身份验证流量信息。 如果启用此策略设置，则只会执行审核功能;不会实现任何安全增强功能。

相关主题

- 安全选项

网络安全: 限制 NTLM: 审核此域中的 NTLM 身份验证

项目 • 2023/03/18

适用范围

- Windows Server

介绍 **网络安全：限制 NTLM：在此域安全策略设置中审核 NTLM 身份验证** 的最佳做法、位置、值、管理方面和安全注意事项。

参考

“ **网络安全：限制 NTLM：在此域中审核 NTLM 身份验证** ”策略设置允许你审核该域中的域控制器 NTLM 身份验证。

在域控制器上启用此策略设置时，只会记录发到该域控制器的身份验证流量。

启用此审核策略时，其工作方式与网络安全 **：限制 NTLM：此域策略设置中的 NTLM 身份验证** 相同，但它实际上不会阻止任何流量。 因此，可以有效地使用它来了解发到域控制器的身份验证流量，在准备好阻止该流量时，可以启用 “**网络安全：在此域策略中限制 NTLM：NTLM 身份验证**” 设置，并选择“ **拒绝域帐户到域服务器**”、“ **域服务器拒绝**”或“**域帐户拒绝**”。

可能值

- **禁用**

  设置此策略的域控制器不会记录传入 NTLM 流量的事件。

- **为域服务器启用域帐户**

  当 NTLM 身份验证被拒绝时，设置此策略的域控制器将记录域中帐户的 NTLM 身份验证登录尝试的事件，因为 “**网络安全：在此域中限制 NTLM： 此域中的 NTLM 身份验证** ”策略设置为 “**拒绝域帐户到域服务器**”。

- **为域帐户启用**

  当 NTLM 身份验证被拒绝时，域控制器将记录使用域帐户的 NTLM 身份验证登录尝试的事件 **，因为“网络安全：在此域中限制 NTLM： NTLM 身份验证**” 策略设置已**针对域帐户设置为“拒绝”**。

- **为域服务器启用**

  当 NTLM 身份验证被拒绝时，域控制器会将 NTLM 身份验证请求的事件记录到域中的所有服务器，因为“ **网络安全：在此域中限制 NTLM：NTLM 身份验证** ”策略设置设置为 “**拒绝域服务器**”。

- **全部启用**

  设置此策略的域控制器将记录传入 NTLM 流量的所有事件。

最佳做法

根据环境和测试持续时间，定期监视操作事件日志大小。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 在本地保存或通过组策略分发时，此策略的更改无需重启即可生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。

审计

查看操作事件日志，查看此策略是否按预期运行。 此计算机上的审核和阻止事件记录在 **应用程序和服务日志\Microsoft\Windows\NTLM** 中的操作事件日志中。 使用审核事件收集系统可帮助你更高效地收集事件进行分析。

没有安全审核事件策略可以配置为查看此策略的输出。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

NTLM 和 NTLMv2 身份验证容易受到各种恶意攻击，包括 SMB 重播、中间人攻击和暴力攻击。 减少和消除环境中的 NTLM 身份验证会强制 Windows 操作系统使用更安全的协议，例如 Kerberos 版本 5 协议或不同的身份验证机制（如智能卡）。

漏洞

启用此策略设置将通过日志记录显示网络或域内的哪些设备处理 NTLM 流量。 如果 NTLM 身份验证流量遭到入侵，则这些设备的标识可能以恶意方式使用。 策略设置不会阻止或缓解任何漏洞，因为它仅用于审核目的。

对策

在生产环境中启用此策略设置时，限制对日志文件的访问。

潜在影响

如果未启用或配置此策略设置，则不会记录 NTLM 身份验证流量信息。 如果启用此策略设置，则只会执行审核功能;不会实现任何安全增强功能。

相关主题

- 安全选项

网络安全: 限制 NTLM: 传入 NTLM 流量

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **网络安全：限制 NTLM：传入 NTLM 流量** 安全策略设置的最佳做法、位置、值、管理方面和安全注意事项。

参考

使用 “**网络安全：限制 NTLM：传入 NTLM 流量** ”策略设置，可以拒绝或允许来自客户端计算机、其他成员服务器或域控制器的传入 NTLM 流量。

可能值

- **全部允许**

  服务器将允许所有 NTLM 身份验证请求。

- **拒绝所有域帐户**

  服务器将拒绝域登录的 NTLM 身份验证请求，向客户端设备返回 NTLM 阻止的错误消息，并记录错误，但服务器将允许本地帐户登录。

- **拒绝所有帐户**

  服务器将拒绝来自所有传入流量的 NTLM 身份验证请求， (域帐户登录还是本地帐户登录) ，将 NTLM 阻止的错误消息返回给客户端设备，并记录错误。

- 未定义

  未定义的此状态与 “**全部允许**”相同，服务器将允许所有 NTLM 身份验证请求。

最佳做法

如果选择” **拒绝所有域帐户** ”或 “**拒绝所有帐户**”，则会限制传入成员服务器的 NTLM 流量。 最好设置 “**网络安全：限制 NTLM：审核传入 NTLM 流量** ”策略设置，然后查看操作日志，了解对成员服务器进行了哪些身份验证尝试，以及哪些客户端应用程序正在使用 NTLM。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 在本地保存或通过组策略分发时，此策略的更改无需重启即可生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。

审计

查看操作事件日志，查看此策略是否按预期运行。 此计算机上的审核和阻止事件记录在 **应用程序和服务日志**\Microsoft\Windows\NTLM 中的操作事件日志中。

没有可以配置为查看此策略的事件输出的安全审核事件策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

NTLM 和 NTLMv2 身份验证容易受到各种恶意攻击，包括 SMB 重播、中间人攻击和暴力攻击。 减少和消除环境中的 NTLM 身份验证会强制 Windows 操作系统使用更安全的协议，例如 Kerberos 版本 5 协议或不同的身份验证机制（如智能卡）。

漏洞

仅当服务器处理 NTLM 请求时，才会发生对 NTLM 身份验证流量的恶意攻击，这些攻击会导致服务器遭到入侵。 如果这些请求被拒绝，将消除对 NTLM 的暴力攻击。

对策

如果确定不应在网络中使用 NTLM 身份验证协议，因为需要使用更安全的协议（如 Kerberos），则可以选择此安全策略设置提供的多个选项之一来限制 NTLM 的使用。

潜在影响

如果配置此策略设置，则许多 NTLM 身份验证请求可能会在网络中失败，这可能会降低工作效率。 通过此策略设置实现此更改之前，请设置 “**网络安全：限制 NTLM：审核传入 NTLM 流量** 到同一选项，以便可以查看日志中的潜在影响，执行服务器分析，并创建要从此策略设置” 网络安全：限制 NTLM：在此域中添加服务器例外”的服务器例外列表。

相关主题

- 安全选项

网络安全: 限制 NTLM: 此域中的 NTLM 身份验证

项目 • 2023/03/18

适用范围

- Windows Server

介绍网络安全的最佳做法、位置、值、管理方面和安全注意事项 ：**在此域安全策略设置中限制 NTLM：NTLM 身份验证** 。

参考

此域策略设置中的"网络安全：限制 NTLM： NTLM 身份验证"允许你从此域控制器拒绝或允许域中的 NTLM 身份验证。 此策略设置不会影响到此域控制器的交互式登录。

可能值

- **禁用**

  域控制器将允许域内的所有 NTLM 直通身份验证请求。

- **拒绝域帐户到域服务器**

  域控制器将拒绝使用此域中所有服务器的帐户进行的所有 NTLM 身份验证登录尝试。 NTLM 身份验证尝试将被阻止，并且将返回 NTLM 阻止错误，除非服务器名称位于 "**网络安全：限制 NTLM：在此域策略设置中添加服务器例外** "列表中。

  如果用户连接到其他域，则可以使用 NTLM，具体取决于是否已在这些域上设置了任何"限制 NTLM"策略。

- **域帐户的拒绝**

  只有域控制器会拒绝来自域帐户的所有 NTLM 身份验证登录尝试，并且将返回 NTLM 阻止错误，除非服务器名称位于 "**网络安全：限制 NTLM：在此域策略中添加服务器例外** "设置中的异常列表中。

- **域服务器的拒绝**

  域控制器将拒绝对域中所有服务器的 NTLM 身份验证请求，并将返回 NTLM 阻止错误，除非服务器名称位于 "**网络安全：限制 NTLM：在此域策略中添加服务器例外**"

设置中的 例外列表中。 如果配置了此策略设置，则未加入域的服务器不会受到影响。

- **全部拒绝**

  域控制器将拒绝来自其服务器及其帐户的所有 NTLM 直通身份验证请求，并返回 NTLM 阻止的错误，除非服务器名称位于 **网络安全：限制 NTLM：在此域策略设置中添加服务器例外** 列表中。

- 未定义

  域控制器将允许部署策略的域中的所有 NTLM 身份验证请求。

最佳做法

如果选择任何拒绝选项，则会限制传入域的 NTLM 流量。 首先，设置 “**网络安全：限制 NTLM：在此域中审核 NTLM 身份验证** ”策略设置，然后查看操作日志以了解对成员服务器进行的身份验证尝试。 然后，可以使用 “网络安全：限制 NTLM：在此域中添加服务器例外 ”策略设置，将这些成员服务器名称添加到服务器例外列表。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未配置
默认域控制器策略	未配置
独立服务器默认设置	未配置
域控制器有效默认设置	未配置
成员服务器有效默认设置	未配置
客户端计算机有效的默认设置	未配置

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 在本地保存或通过组策略分发时，此策略的更改无需重启即可生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。 该策略仅适用于域控制器。

审计

查看操作事件日志，查看此策略是否按预期运行。 此计算机上的审核和阻止事件记录在 **应用程序和服务日志\Microsoft\Windows\NTLM** 中的操作事件日志中。

没有安全审核事件策略可以配置为查看此策略的输出。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

NTLM 和 NTLMv2 身份验证容易受到各种恶意攻击，包括 SMB 重播、中间人攻击和暴力攻击。 减少和消除环境中的 NTLM 身份验证会强制 Windows 操作系统使用更安全的协议，例如 Kerberos 版本 5 协议或不同的身份验证机制（如智能卡）。

漏洞

仅当服务器或域控制器处理 NTLM 请求时，才会对 NTLM 身份验证流量进行恶意攻击，从而导致服务器或域控制器遭到入侵。 如果拒绝这些请求，则消除此攻击途径。

对策

如果确定不应在网络中使用 NTLM 身份验证协议，因为需要使用更安全的协议（如 Kerberos 协议），则可以选择此安全策略设置提供的多个选项之一来限制域中的 NTLM 使用。

潜在影响

如果配置此策略设置，域内的许多 NTLM 身份验证请求可能会失败，这可能会降低工作效率。 在通过此策略设置实现此更改之前，请将 “**网络安全：限制 NTLM：审核此域中的 NTLM 身份验证** ”设置为同一选项，以便你可以查看日志中的潜在影响，执行服务器分

析，并使用网络安全创建要从此策略设置中排除的服务器例外列表 ： 限制 NTLM：在此域中添加服务器例外。

相关主题

- 安全选项

网络安全: 限制 NTLM: 到远程服务器的传出 NTLM 流量

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **网络安全：限制 NTLM：传出 NTLM 流量到远程服务器** 安全策略设置的最佳做法、位置、值、管理方面和安全注意事项。

> **备注**
>
> 有关配置要远程访问的服务器的详细信息，请参阅 **远程桌面 - 允许访问你的电脑。**

参考

“ **网络安全：限制 NTLM：向远程服务器传出 NTLM 流量** ”策略设置允许拒绝或审核从运行 Windows 7、Windows Server 2008 或更高版本的计算机到运行 Windows 操作系统的任何远程服务器的传出 NTLM 流量。

> **警告：** 修改此策略设置可能会影响与客户端计算机、服务和应用程序的兼容性。

可能值

- **全部允许**

  设备可以使用 NTLM 身份验证对远程服务器的标识进行身份验证，因为没有任何限制。

- **全部审核**

  向远程服务器发送 NTLM 身份验证请求的设备记录每个请求的事件。 此事件允许你标识从客户端设备接收 NTLM 身份验证请求的服务器。

- **全部拒绝**

  设备无法使用 NTLM 身份验证对远程服务器的任何标识进行身份验证。 可以使用 “网络安全：限制 NTLM：为 NTLM 身份验证添加远程服务器例外 ”策略设置来定义

允许客户端设备在拒绝其他服务器时使用 NTLM 身份验证的远程服务器列表。 此设置还会在发出身份验证请求的设备上记录事件。

- 未定义

  未定义的此状态与 “**全部允许**”相同，在部署策略时，设备将允许所有 NTLM 身份验证请求。

最佳做法

如果选择“ **全部拒绝**”，则客户端设备无法使用 NTLM 身份验证对远程服务器进行身份验证。 首先，选择“ **全部审核** ”，然后查看操作事件日志，了解这些身份验证尝试涉及哪些服务器。 然后，可以使用 “网络安全：限制 NTLM：为 NTLM 身份验证添加远程服务器例外 ”策略设置，将这些服务器名称添加到服务器例外列表。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

重启要求

无。 在本地保存或通过组策略分发时，此策略的更改无需重启即可生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。

审计

查看操作事件日志，查看此策略是否按预期运行。 此计算机上的审核和阻止事件记录在 **应用程序和服务日志\Microsoft\Windows\NTLM** 中的操作事件日志中。

没有可以配置为查看此策略的事件输出的安全审核事件策略。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

NTLM 和 NTLMv2 身份验证容易受到各种恶意攻击，包括 SMB 中继、中间人攻击和暴力攻击。 减少和消除环境中的 NTLM 身份验证会强制 Windows 操作系统使用更安全的协议，例如 Kerberos 版本 5 协议或不同的身份验证机制（如智能卡）。

漏洞

仅当服务器或域控制器处理 NTLM 请求时，才会对 NTLM 身份验证流量进行恶意攻击，导致服务器或域控制器遭到入侵。 如果拒绝这些请求，则消除此攻击途径。

对策

如果确定不应在网络中使用 NTLM 身份验证协议，因为需要使用更安全的协议（如 Kerberos），则可以从多个选项中进行选择，以将 NTLM 的使用限制为服务器。

潜在影响

如果将此策略设置配置为拒绝所有请求，则向远程服务器发出的大量 NTLM 身份验证请求可能会失败，这可能会降低工作效率。 通过此策略设置实现此限制之前，请选择“ **全部审核** ”，以便可以查看日志中的潜在影响，执行服务器分析，并使用 “网络安全：限制 NTLM：为 NTLM 身份验证添加远程服务器例外 ”创建要从此策略设置中排除的服务器例外列表。

相关主题

- 安全选项

恢复控制台: 允许自动管理登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍恢复控制台的最佳做法、位置、值、策略管理和安全注意事项 ：**允许自动管理登录**安全策略设置。

参考

此策略设置确定在授予对设备的访问权限之前是否必须提供内置管理员帐户密码。 如果启用此设置，则内置管理员帐户会自动登录到恢复控制台中的计算机;无需密码。

在对无法重启的系统进行故障排除和修复时，恢复控制台非常有用。 但是，启用此策略设置以便用户可以自动登录到控制台是危险的。 任何人都可以转到服务器，通过断开电源来关闭服务器，重新启动服务器，从“**重启**”菜单中选择“**恢复控制台**”，然后完全控制服务器。

可能值

- 已启用

  内置管理员帐户会自动登录到恢复控制台上的计算机;无需密码

- 禁用

  不允许自动管理登录。

- 未定义

  不允许自动管理登录。

最佳做法

- 将 **恢复控制台：允许自动管理登录** 设置为 “**已禁用**”。 此设置要求用户输入用户名和密码才能访问恢复控制台帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置

策略冲突

无。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

当必须对未启动的设备进行故障排除和修复时，恢复控制台非常有用。 但是，允许自动登录到恢复控制台可以让某人完全控制服务器。

对策

禁用 **恢复控制台：允许自动管理登录** 设置。

潜在影响

用户必须输入用户名和密码才能访问恢复控制台。

相关主题

- 安全选项

恢复控制台: 允许软盘复制并访问所有驱动器和所有文件夹

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍恢复控制台的最佳做法、位置、值、策略管理和安全注意事项 **：允许软盘复制和访问所有驱动器和文件夹** 安全策略设置。

参考

此策略设置启用或禁用恢复控制台 SET 命令，该命令允许设置以下恢复控制台环境变量。

- **AllowWildCards。** 启用对某些命令的通配符支持，例如 DEL 命令。
- **AllowAllPaths。** 允许访问设备上的所有文件和文件夹。
- **AllowRemovableMedia。** 允许将文件复制到可移动媒体，例如软盘。
- **NoCopyPrompt。** 取消在覆盖现有文件之前通常显示的提示。

你可能会忘记删除包含敏感数据或恶意用户随后可能窃取的应用程序的可移动媒体（如 CD 或软盘）。 或者，使用恢复控制台后，可能会意外地将启动磁盘留在计算机中。 如果设备出于任何原因重新启动，并且 BIOS 已配置为在硬盘驱动器之前从可移动媒体启动，则服务器将从可移动磁盘启动。 此启动会导致服务器的网络服务不可用。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 将 “**恢复控制台：允许软盘复制和访问驱动器和文件夹**” 设置为 “**已禁用**”。 使用恢复控制台启动服务器并使用内置管理员帐户登录的用户将无法将文件和文件夹复制到软盘。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。

策略冲突

无。

命令行工具

启用此安全选项可使恢复控制台 SET 命令可用，以便设置以下恢复控制台环境变量：

- AllowWildCards：为某些命令启用通配符支持（，例如 DEL 命令）。
- AllowAllPaths：允许访问设备上的所有文件和文件夹。
- AllowRemovableMedia：允许将文件复制到可移动媒体，例如软盘。
- NoCopyPrompt：覆盖现有文件时不提示。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可能导致系统重启到恢复控制台的攻击者可能会窃取敏感数据，并且不会留下审核或访问跟踪。

对策

禁用 **恢复控制台：允许软盘复制和访问驱动器和文件夹** 设置。

潜在影响

通过恢复控制台启动服务器并使用内置管理员帐户登录的用户无法将文件和文件夹复制到软盘。

相关主题

- 安全选项

关机: 允许系统在未登录的情况下关闭

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **关闭：允许系统关闭而无需登录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定是否可以在不登录 Windows 的情况下关闭设备。 启用后，Windows 的登录屏幕上提供了 “**关闭**” 选项。 如果禁用此设置，则会从屏幕中删除 “**关机**” 选项。 若要使用 选项，用户必须在设备上成功登录并具有 “**关闭系统** ”用户权限。

在本地访问控制台的用户可以关闭系统。 攻击者或被误导的用户可以使用远程桌面服务连接到服务器，然后关闭服务器或重启服务器，而无需标识自己。 恶意用户还可能通过重启或关闭服务器，从本地控制台引发临时拒绝服务条件。

可能值

- 已启用

  关闭命令在登录屏幕上可用。

- 禁用

  “关闭”选项将从登录屏幕中删除。 用户必须具有 “**关闭系统** ”用户权限才能执行关闭。

- 未定义

最佳做法

1. 在服务器上，将此策略设置为 “**已禁用**”。 必须登录到服务器才能关闭或重启它们。
2. 在客户端设备上，将此策略设置为 “**已启用**”。 使用用户权限分配策略“关闭 **系统**”定义有权关闭或重启这些用户的列表。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

有关用户权限分配策略的信息，请参阅关闭系统。

安全注意事项

本部分介绍：

- 攻击者如何利用功能或其配置。
- 如何实施对策。
- 实施对策的可能负面后果。

漏洞

可以在本地访问主机的用户可以关闭设备

有权访问本地控制台的攻击者可能会重启服务器，这将导致临时 DoS 条件。 攻击者还可以关闭服务器，使其所有应用程序和服务不可用。

对策

禁用 “**关闭：允许系统关闭而无需登录** ”设置。

潜在影响

必须登录服务器才能将其关闭或重启。

相关文章

- 安全选项

关机: 清除虚拟内存页面文件

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **关闭：清除虚拟内存页文件** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定在设备关闭时是否清除虚拟内存分页文件。 虚拟内存支持在不使用内存页时使用系统分页文件将内存页交换到磁盘。 在正在运行的设备上，此分页文件由操作系统独占打开，并且受到很好的保护。 但是，配置为允许其他操作系统启动的设备应验证系统分页文件是否已在设备关闭时清除。 此确认可确保可能放置在分页文件中的进程内存中的敏感信息对在关闭后直接访问分页文件的未授权用户不可用。

保留在实际内存中的重要信息可能会定期写入分页文件。 此定期写入操作可帮助设备处理多任务函数。 对已关闭的服务器具有物理访问权限的恶意用户可以查看分页文件的内容。 攻击者可以将系统卷移动到其他计算机，然后分析分页文件的内容。 此过程非常耗时，但它可能会公开从 RAM 缓存到分页文件的数据。 有权物理访问服务器的恶意用户可以通过从其电源中拔出服务器来绕过此对策。

可能值

- 已启用

  系统正常关闭时，系统会清除系统分页文件。 此外，此策略设置强制计算机在便携式设备上禁用休眠时清除休眠文件 (hiberfil.sys) 。

- 禁用

- 未定义

最佳做法

- 将此策略设置为 “**已启用**”。 此策略设置会导致 Windows 在系统关闭时清除分页文件。 根据分页文件的大小，此过程可能需要几分钟时间才能完全关闭系统。 在具有大型分页文件的服务器上，关闭服务器的这种延迟尤其明显。 对于具有 2 GB (GB)

RAM 和 2 GB 分页文件的服务器，此设置可为关闭过程添加超过 30 分钟。 对于某些组织，这种停机时间违反了其内部服务级别协议。 在环境中实施此对策时要小心。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

保留在实际内存中的重要信息可能会定期写入分页文件，以帮助 Windows 处理多任务函数。 对已关闭的服务器具有物理访问权限的攻击者可以查看分页文件的内容。 攻击者可以将系统卷移动到其他设备，然后分析分页文件的内容。 尽管此过程非常耗时，但它可能会公开从随机访问内存 (RAM) 缓存到分页文件的数据。

> **谨慎：** 有权物理访问设备的攻击者可以通过从其电源中拔出计算机来绕过此对策。

对策

启用 “**关闭：清除虚拟内存页文件** ”设置。 此配置会导致操作系统在设备关闭时清除分页文件。 完成此过程所需的时间取决于页面文件的大小。 由于该过程会多次覆盖页面文件使用的存储区域，因此设备可能需要几分钟时间才能完全关闭。

潜在影响

关闭和重启设备需要更长的时间，尤其是在具有大型分页文件的设备上。 对于具有 2 GB (GB) RAM 和 2 GB 分页文件的设备，此策略设置可能会使关闭过程增加 30 分钟以上。 对于某些组织，这种停机时间违反了其内部服务级别协议。 因此，在环境中实施此对策之前，请谨慎行事。

相关主题

- 安全选项

系统加密: 为计算机上存储的用户密钥强制进行强密钥保护

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍系统加密的最佳做法、位置、值、策略管理和安全注意事项 **：对存储在计算机安全策略设置上的用户密钥强制实施强密钥保护** 。

参考

此策略设置确定用户是否可以在没有密码的情况下使用私钥，例如其安全/多用途 Internet 邮件扩展 (S/MIME) 密钥。

配置此策略设置，使用户每次使用密钥 (时都必须提供密码，以及域密码) 使得恶意用户访问本地存储的用户密钥更加困难，即使攻击者控制了用户的设备并确定其登录密码也是如此。

可能值

- **存储和使用新密钥时不需要用户输入**
- **首次使用密钥时，系统会提示用户**
- **用户每次使用密钥时都必须输入密码**
- 未定义

最佳做法

- 将此策略设置为 “**用户每次使用密钥时必须输入密码**”。 用户每次访问存储在其计算机上的密钥时都必须输入其密码。 例如，如果用户使用 S/MIME 证书对其电子邮件进行数字签名，则每次发送已签名的电子邮件时，将强制输入该证书的密码。 对于某些组织来说，使用此值导致的开销可能过高，但首次 **使用密钥时**，系统会提示用户将值设置为最小值。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
DC 有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果用户的帐户遭到入侵或用户的设备无意中处于不安全状态，恶意用户可以使用为用户存储的密钥来访问受保护的资源。

对策

配置 **系统加密：对计算机上存储的用户密钥强制强密钥保护** 设置为 “**用户必须在每次使用密钥时输入密码**”，以便用户在每次使用密钥时都必须提供不同于其域密码的密码。 此配置使攻击者更难访问本地存储的用户密钥，即使攻击者控制了用户的计算机并确定登录密码也是如此。

潜在影响

用户每次访问存储在其设备上的密钥时都必须键入其密码。 例如，如果用户使用 S/MIME 证书对其电子邮件进行数字签名，则每次发送已签名的电子邮件时，他们必须键入该证书的密码。 对于某些组织，使用此配置所涉及的开销可能过高。 此设置至少应设置为 **首次使用密钥时提示用户**。

相关主题

- 安全选项

系统加密: 将 FIPS 兼容算法用于加密、哈希和签名

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

此安全策略参考主题面向 IT 专业人员，介绍了此策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

联邦信息处理标准 (FIPS) 140 是一种安全实现，旨在认证加密软件。 Windows 实施这些经过认证的算法以满足加密模块的要求和标准，供美国联邦政府的部门和机构使用。

TLS/SSL

此策略设置确定 TLS/SSL 安全提供程序是否仅支持符合 FIPS 的强密码套件（称为 TLS_RSA_WITH_3DES_EDE_CBC_SHA），这意味着提供程序仅支持将 TLS 协议作为客户端计算机和服务器（如果适用）。 它仅使用三重数据加密标准 (3DES) 加密算法进行 TLS 流量加密，仅使用 Rivest-Shamir-Adleman (RSA) 公钥算法进行 TLS 密钥交换和身份验证，仅使用安全哈希算法版本 1 (SHA-1) 哈希算法满足 TLS 哈希要求。

加密文件系统 (EFS)

对于 EFS 服务，此策略设置支持 3DES 和高级加密标准 (AES) 加密算法，用于加密 NTFS 文件系统支持的文件数据。 为了加密文件数据，默认情况下，EFS 在 Windows Server 2003、Windows Vista 及更高版本中使用高级加密标准 (AES) 算法和 256 位密钥，并在 Windows XP 中使用 DESX 算法。

远程桌面服务 (RDS)

如果使用的是远程桌面服务，则仅当支持 3DES 加密算法时，才应启用此策略设置。

BitLocker

对于 BitLocker，需要在生成任何加密密钥之前启用此策略设置。 启用此策略时，在 Windows Server 2012 R2 和 Windows 8.1 及更高版本上创建的恢复密码与 Windows Server 2012 R2 和 Windows 8.1 之前的操作系统上的 BitLocker 不兼容;BitLocker 将阻止在这些系统上创建或使用恢复密码，因此应改用恢复密钥。 此外，如果数据驱动器受密

码保护，则提供密码后，符合 FIPS 标准的计算机可以访问该驱动器，但该驱动器将为只读。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

我们建议希望符合 FIPS 140-2 的客户研究他们可能使用的应用程序和协议的配置设置，以确保其解决方案能够配置为在 WINDOWS 在 FIPS 140-2 批准的模式下运行时使用 WINDOWS 提供的 FIPS 140-2 验证加密。

有关 Microsoft 建议的配置设置的完整列表，请参阅 Windows 安全基线。 有关 Windows 和 FIPS 140-2 的详细信息，请参阅 FIPS 140 验证。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

操作系统版本差异

启用此设置后，加密文件系统 (EFS) 服务仅支持用于加密文件数据的三重 DES 加密算法。 默认情况下，EFS 的 Windows Vista 和 Windows Server 2003 实现使用高级加密标准 (AES) 和 256 位密钥。 Windows XP 实现使用 DESX。

启用此设置后，BitLocker 会生成适用于以下版本的恢复密码或恢复密钥：

操作系统	适用性
Windows 10、Windows 8.1和 Windows Server 2012 R2	在这些操作系统上创建恢复密码时，不能在此表中列出的其他系统上使用恢复密码。
Windows Server 2012 和 Windows 8	在这些操作系统上创建恢复密钥时，还可以在此表中列出的其他系统上使用恢复密钥。
Windows Server 2008 R2 和 Windows 7	在这些操作系统上创建恢复密钥时，还可以在此表中列出的其他系统上使用恢复密钥。
Windows Server 2008 和 Windows Vista	在这些操作系统上创建恢复密钥时，还可以在此表中列出的其他系统上使用恢复密钥。

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

使用 组策略 设置和部署此策略优先于本地设备上的设置。 如果组策略设置为“**未配置**”，将应用本地设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以启用此策略设置，以确保设备使用可用于数字加密、哈希和签名的最强大的算法。 使用这些算法可以最大程度地降低未经授权的用户泄露数字加密或签名数据的风险。

对策

启用 **系统加密：使用符合 FIPS 的算法进行加密、哈希和签名** 设置。

潜在影响

启用此策略设置的客户端设备无法通过数字加密或签名协议与不支持这些算法的服务器进行通信。 不支持这些算法的网络客户端无法使用需要这些算法的服务器进行网络通信。 例如，许多基于 Apache 的 Web 服务器未配置为支持 TLS。 如果启用此设置，还必须将 Internet Explorer® 配置为使用 TLS。 此策略设置还会影响用于远程桌面协议 (RDP) 的加密级别。 远程桌面连接工具使用 RDP 协议与运行终端服务的服务器和配置为进行远程控制的客户端计算机进行通信;如果两个设备未配置为使用相同的加密算法，RDP 连接将失败。

相关主题

- 安全选项

系统对象：非 Windows 子系统不要求区分大小写

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍系统对象的最佳做法、位置、值、策略管理和安全注意事项 **：要求非 Windows 子系统安全策略设置不区分大小写** 。

参考

此策略设置确定是否对所有子系统强制实施不区分大小写。 Microsoft Win32 子系统不区分大小写;但是，内核支持区分大小写的其他子系统，例如 UNIX (POSIX) 的可移植操作系统接口。 启用此策略设置会强制所有目录对象、符号链接和输入/输出 (I/O) 对象（包括文件对象）不区分大小写。 禁用此策略设置不允许 Win32 子系统区分大小写。

由于 Windows 不区分大小写，但 POSIX 子系统支持区分大小写，因此如果未强制实施此策略设置，则子系统的用户可能会创建一个与另一个文件同名但大写字母组合不同的文件。 当用户尝试使用普通 Win32 工具访问这些文件时，该约定可能会使用户感到困惑，因为只有一个文件可用。

可能值

- 已启用

  对所有目录对象、符号链接和 IO 对象（包括文件对象）强制实施不区分大小写。

- 禁用

  不允许 Win32 子系统区分大小写。

- 未定义

最佳做法

- 将此策略设置为 “**已启用**”。 将强制所有子系统观察不区分大小写。 但是，这种不敏感可能会使熟悉基于 UNIX 的操作系统之一并习惯于区分大小写的操作系统的用户感到困惑。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

由于 Windows 不区分大小写，但 POSIX 子系统支持区分大小写，如果启用此策略设置失败，该子系统的用户可能会创建与另一个文件同名但大小写字母组合不同的文件。 当用户尝试从普通 Win32 工具访问此类文件时，这种情况可能会使用户感到困惑，因为只有一个文件可用。

对策

启用 **系统对象：要求对非 Windows 子系统设置不区分大小写** 。

潜在影响

所有子系统都被迫观察不区分大小写。 此配置可能会使熟悉任何区分大小写的基于 UNIX 的操作系统的用户感到困惑。

相关主题

- 安全选项

系统对象：加强内部系统对象的默认权限，（例如符号链接）

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍系统对象的最佳做法、位置、值、策略管理和安全注意事项 ：**（增强内部系统对象的默认权限，例如符号链接）** 安全策略设置。

参考

此策略设置确定对象的默认自由访问控制列表 (DACL) 的强度。 Windows 维护共享系统资源的全局列表，例如 MS-DOS 设备名称、互斥体和信号灯。 进程使用此列表来查找和共享对象。 使用默认 DACL 创建每种类型的对象，该 DACL 指定谁可以使用哪些权限访问对象。 启用此策略设置可增强默认 DACL，并允许不是管理员的用户读取而不是修改他们未创建的共享对象。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 建议将此策略设置为 “**已启用**”。

位置

计算机配置\Windows 设置\安全设置\ 本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

默认情况下启用此策略设置，以防止与硬链接或符号链接一起使用的已知漏洞。 硬链接是文件系统中的实际目录条目。 使用硬链接时，文件系统中的相同数据可以通过不同的文件名引用。 符号链接是一个文本文件，它们提供指向文件的指针，该文件被操作系统解释为另一个文件或目录的路径。。 由于符号链接是单独的文件，因此它们可以独立于目标位置存在。 如果删除符号链接，则其目标位置不受影响。 禁用此设置后，恶意用户可能会通过创建类似于系统自动创建的临时文件的链接（如按顺序命名的日志文件）来销毁数据文件，但它指向恶意用户想要消除的数据文件。 当系统使用该名称写入文件时，数据将被覆盖。 启用 **系统对象：加强内部系统对象 (的默认权限，例如符号链接)** 可阻止攻击者通过不允许攻击者写入未创建的对象来利用创建具有可预测名称的文件的程序。

对策

启用 **系统对象：加强全局系统对象的默认权限 (例如符号链接)** 设置。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

系统设置: 可选子系统

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍系统设置的最佳做法、位置、值、策略管理和安全注意事项 **：可选子系统** 安全策略设置。

参考

此策略设置确定哪些子系统支持应用程序。 可以使用此安全设置指定环境所需的任意数量的子系统。

子系统引入了一种安全风险，它与可能跨登录保留的进程相关。 如果用户启动进程然后注销，则登录到系统的下一个用户可能会访问上一个用户启动的进程。 此模式很危险，因为第一个用户启动的进程可以保留该用户的系统用户权限;因此，第二个用户使用该过程执行的任何操作都是使用第一个用户的用户权限执行的。 这种权限滚动更新使得很难跟踪创建流程和对象的人员，这对于事后事件取证至关重要。

可能值

- 用户定义的子系统列表
- 未定义

最佳做法

- 将此策略设置设置为 null 值。 默认值为 **POSIX**，因此依赖于 POSIX 子系统的应用程序将不再运行。 例如，Microsoft Services for UNIX 3.0 安装 POSIX 子系统的更新版本。 对于使用适用于 UNIX 3.0 的服务的任何服务器，在 组策略 中重置此策略设置。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	Posix
DC 有效默认设置	Posix
成员服务器有效默认设置	Posix
客户端计算机有效默认设置	Posix

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

POSIX 子系统是一个电气和电子工程师协会， (IEEE) 标准，用于定义一组操作系统服务。 如果服务器支持使用该子系统的应用程序，则需要 POSIX 子系统。

POSIX 子系统引入了一种安全风险，该风险与可能会跨登录保留的进程相关。如果用户启动进程然后注销，则登录计算机的下一个用户可能会访问上一个用户的进程。 此辅助功能将允许第二个用户使用第一个用户的权限对进程执行操作。

对策

将 “**系统设置：可选子系统**”**设置** 配置为 null 值。 默认值为 POSIX。

潜在影响

依赖于 POSIX 子系统的应用程序不再运行。 例如，Microsoft Services for UNIX (SFU) 安装所需的 POSIX 子系统的更新版本，因此必须为使用 SFU 的任何服务器在 组策略 中重新配置此设置。

相关主题

- 安全选项

系统设置: 将 Windows 可执行文件中的证书规则用于软件限制策略

项目 • 2023/04/12

适用范围

- Windows 11
- Windows 10

介绍系统设置的最佳做法、位置、值、策略管理和安全注意事项 **：对软件限制策略安全策略设置使用 Windows 可执行文件上的证书规则 。**

参考

此策略设置确定在启用软件限制策略以及用户或进程尝试使用.exe文件扩展名运行软件时是否处理数字证书。 此安全设置启用或禁用证书规则 (这是一种软件限制策略) 。 使用软件限制策略，可以基于与软件关联的数字证书创建允许或禁止运行 Microsoft Authenticode® 签名软件的证书规则。 若要在软件限制策略中运行证书规则，必须启用此安全设置。

可能值

- 已启用
- 禁用
- 未定义

最佳做法

- 将此策略设置为 “**已启用**”。 启用证书规则会导致软件限制策略检查证书吊销列表 (CRL) ，以确保软件的证书和签名有效。 启动已签名程序时，此设置可能会降低系统性能。 可以通过编辑所需 GPO 中的软件限制策略来禁用 CRL。 在“**受信任的发布服务器属性**”对话框中，清除“**发布服务器**”和“**时间戳**”检查框。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果不使用软件限制策略，用户和设备可能会接触到可能包含恶意软件的未授权软件。

对策

启用 **系统设置：对 Windows 可执行文件使用证书规则进行软件限制策略** 设置。

潜在影响

如果启用证书规则，软件限制策略检查证书吊销列表 (CRL) 验证软件的证书和签名是否有效。 此检查过程可能会在已签名程序启动时对性能产生负面影响。 若要禁用此功能，可

以在相应的 GPO 中编辑软件限制策略。 在“**受信任的发布服务器属性**”对话框中，清除“**发布服务器**”和“**时间戳**”检查框。

相关主题

- 安全选项

用户帐户控制: 用于内置管理员帐户的管理员批准模式

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项：**内置管理员帐户安全策略设置的管理员审批模式。**

参考

此策略设置确定内置管理员帐户管理员审批模式的行为。 启用管理员审批模式后，本地管理员帐户的功能类似于标准用户帐户，但它能够提升权限，而无需使用其他帐户登录。 在此模式下，任何需要特权提升的操作都将显示一个提示，允许管理员允许或拒绝特权提升。 如果未启用管理员审批模式，则内置管理员帐户默认以完全管理权限运行所有应用程序。 默认情况下，管理员审批模式设置为“**禁用**”。

> ⓘ **备注**
>
> 如果计算机从以前版本的 Windows 操作系统升级，并且管理员帐户是计算机上唯一的帐户，则内置管理员帐户将保持启用状态，并且也会启用此设置。

可能值

- 已启用

  内置管理员帐户以管理员审批模式登录，以便任何需要特权提升的操作都显示一个提示，为管理员提供允许或拒绝特权提升的选项。

- 禁用

  如果未启用管理员审批模式，则内置管理员帐户默认以完全管理权限运行所有应用程序

最佳做法

- 建议不要在客户端计算机上启用内置管理员帐户，而是改用标准用户帐户和用户帐户控制 (UAC)。 如果要启用内置管理员帐户来执行管理任务，出于安全原因，还应启用管理员审批模式。 请参阅 UAC-管理员-Approval-Mode-for-the-built-in-Administrator-account

  若要启用管理员审批模式，还必须配置本地安全策略设置：用户帐户控制：管理员审批模式下管理员的提升提示行为，在**安全桌面上提示同意**，然后单击“确定”。

> ⓘ **备注**
>
> 启用管理员审批模式后，若要激活设置，必须先登录和注销。或者，可以从提升的命令提示符执行 **gpupdate /force**。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

UAC 功能尝试缓解的风险之一是在用户或管理员不知道其活动的情况下，在提升的凭据下运行的恶意软件。 恶意程序的攻击途径是发现管理员帐户的密码，因为该用户帐户是为所有 Windows 安装创建的。 为了解决此风险，至少在运行 Windows Vista 的计算机中禁用内置管理员帐户。 在至少运行 Windows Server 2008 的计算机中，已启用管理员帐户，并且必须在管理员首次登录时更改密码。 在至少运行 Windows Vista 的计算机的默认安装中，如果计算机未加入域，则你创建的第一个用户帐户具有本地管理员的等效权限。

对策

启用**用户帐户控制：如果已启用内置管理员帐户，则为内置管理员帐户设置管理员审批模式。**

潜在影响

每当程序请求提升特权时，系统都提示使用本地管理员帐户登录的用户同意。

相关主题

- 安全选项

用户帐户控制: 允许 UIAccess 应用程序在不使用安全桌面的情况下提示提升权限

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值和安全注意事项 **：允许 UIAccess 应用程序在不使用安全桌面安全策略设置的情况下提示提升** 。

参考

此安全设置控制用户界面辅助功能 (UIAccess 或 UIA) 程序是否可以自动禁用标准用户使用的提升提示的安全桌面。

> **注意：** 此设置不会更改管理员的 UAC 提升提示的行为。

Background

用户界面特权隔离 (UIPI) 在 Windows 子系统中实施限制，以防止低特权应用程序发送消息或在较高特权进程中安装挂钩。 允许高特权应用程序将消息发送到特权较低的进程。 UIPI 不会干扰或更改具有相同特权 (或完整性) 级别的应用程序之间的消息行为。

Microsoft UI 自动化 是支持 Windows 操作系统中的辅助功能要求的当前模型。 支持可访问用户体验的应用程序控制用户的其他 Windows 应用程序的行为。 当自动化客户端计算机和服务器上的所有应用程序都以标准用户 (即在中等完整性级别) 运行时，UIPI 限制不会干扰 Microsoft UI 自动化模型。

但是，有时，管理用户可能会在管理员审批模式下以基于 UAC 的提升权限运行应用程序。 Microsoft UI 自动化无法在无法绕过 UIPI 实施的限制的情况下，在桌面上驱动提升的应用程序的 UI 图形。 UI 自动化程序可以使用 UIAccess 跨特权级别绕过 UIPI 限制。

如果应用程序在请求权限时显示 UIAccess 属性，则应用程序会声明绕过 UIPI 限制以跨特权级别发送消息的要求。 在启动具有 UIAccess 权限的应用程序之前，设备将实现以下策略检查。

1. 应用程序必须具有一个数字签名，该签名可以使用与本地计算机上的受信任的根证书颁发机构存储关联的数字证书进行验证。

2. 应用程序必须安装在只能由管理员写入的本地文件夹中，例如 Program Files 目录。 UI 自动化应用程序允许的目录包括：
   a. %ProgramFiles% 及其子目录。
   b. %WinDir% 及其子目录，但由于标准用户具有写入访问权限而排除的几个子目录除外。

结果行为

启用此设置后，UIAccess 程序（（包括 Windows 远程协助））可以自动禁用安全桌面作为提升提示。 除非你还禁用了提升提示，否则提示将显示在交互式用户的桌面上，而不是显示在安全桌面上。 在 Windows 远程协助会话期间，这些提示还会显示在远程管理员的桌面视图上，远程管理员可以提供相应的提升凭据。

如果禁用此设置，则只能由交互式桌面的用户禁用安全桌面，或者通过禁用 用户帐户控制：在提示提升设置时切换到安全桌面 ，默认情况下启用此设置。

可能值

- 已启用

  UIA 程序可以针对提升提示自动禁用安全桌面，除非你还禁用了提升提示，否则提示将显示在交互式用户的桌面上，而不是显示在安全桌面上。 在 Windows 远程协助会话期间，远程管理员的桌面视图上也会显示提示，远程管理员可以提供适当的提升凭据。

- 禁用

  安全桌面只能由交互式桌面的用户禁用，也可以通过禁用 **用户帐户控制：在提示提升策略设置时切换到安全桌面** 。

最佳做法

- 最佳做法取决于安全策略和远程操作要求。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

策略交互

如果计划启用此设置，还应查看 用户帐户控制的效果：标准用户的提升提示行为 设置。 如果将其配置为 “**自动拒绝提升请求**”，则不会向用户显示提升请求。 如果禁用此设置，则只能由交互式桌面的用户禁用安全桌面，或者通过禁用 用户帐户控制：在提示提升设置时切换到安全桌面 ，默认情况下启用此设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

UIA 程序旨在代表用户与 Windows 和应用程序进行交互。 此设置允许 UIA 程序绕过安全桌面以提高在某些情况下的可用性，但它允许提升请求出现在常规交互式桌面而不是安全桌面上。 这种请求出现会增加恶意程序截获 UI 和应用程序之间传输的数据的风险。 由于 UIA 程序必须能够响应有关安全问题的提示（例如 UAC 提升提示），因此 UIA 程序必须高度信任。 若要被视为受信任，UIA 计划必须经过数字签名。 默认情况下，只能从以下受保护路径运行 UIA 程序：

- ..\Program Files\ (和子文件夹)
- ..\Program Files (x86) \ (和子文件夹，仅限 64 位版本的 Windows)
- ..\Windows\System32\

用户帐户控制可以禁用位于受保护路径的要求 ：仅提升安装在安全位置中的 UIAccess 应用程序 设置。 尽管此设置适用于任何 UIA 程序，但它主要用于某些 Windows 远程协助方案。

对策

禁用 **用户帐户控制：允许 UIAccess 应用程序在不使用安全桌面设置的情况下提示提升** 。

潜在影响

如果用户请求管理员的远程协助，并且远程协助会话已建立，则提升提示将显示在交互式用户的安全桌面上，并且管理员的远程会话将暂停。 若要避免在提升请求期间暂停远程管理员的会话，用户可以在设置远程协助会话时选择“允许 IT 专家响应用户帐户控制提示”检查框。 但选中此检查框需要交互式用户响应安全桌面上的提升提示。 如果交互式用户是标准用户，则用户没有允许提升所需的凭据。

相关主题

- 安全选项

用户帐户控制: 管理员批准模式中管理员的提升权限提示行为

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项：**管理员审批模式安全策略设置中管理员的提升提示行为。**

参考

此策略设置确定具有管理凭据的帐户的提升提示行为。

可能值

- **提升而不提示**

  假定管理员将允许需要提升的操作，并且不需要更多同意或凭据。

  注意 选择 “**提升而不提示**” 可最大程度地减少 UAC 提供的保护。 建议不要选择此值，除非管理员帐户受到严格控制，并且操作环境高度安全。

- **在安全桌面上提示输入凭据**

  当操作需要特权提升时，系统会在安全桌面上提示用户输入特权用户名和密码。 如果用户输入了有效的凭据，则操作会以用户的最高可用权限继续执行。

- **在安全桌面上提示同意**

  当操作需要特权提升时，系统会在安全桌面上提示用户选择 “**允许**” 或“ **拒绝**”。 如果用户选择 “**允许**”，则以用户的最高可用权限继续操作。*

- **提示输入凭据**

  需要特权提升的操作会提示管理员键入用户名和密码。 如果管理员输入了有效的凭据，则操作将继续具有适用的权限。

- **同意提示**

需要特权提升的操作会提示管理员选择 “**允许**” 或“ **拒绝**”。 如果管理员选择 “**允许**”，则操作会以管理员的最高可用权限继续执行。

- **非 Windows 二进制文件的同意提示**

  此同意提示是默认的。 当非 Microsoft 应用程序的操作需要特权提升时，系统会在安全桌面上提示用户选择 “**允许**” 或“ **拒绝**”。 如果用户选择 “**允许**”，则操作会以用户的最高可用权限继续执行。

*如果已启用内置管理员帐户并配置了管理员审批模式，则还必须在**安全桌面上配置**“**提示同意**”选项。 还可以通过在搜索框中键入 **UAC** ，从用户帐户控制中配置此选项。 在“用户帐户控制设置”对话框中，将滑块控件设置为“ **仅当应用尝试更改我的计算机时通知我 (默认)** 。

> ⓘ **备注**
>
> 启用管理员审批模式后，若要激活设置，必须先登录和注销。或者，可以从提升的命令提示符执行 **gpupdate /force**。

最佳做法

- 选择选项 “**提升而不提示**” 可最大程度地减少 UAC 提供的保护。 建议不要选择此值，除非管理员帐户受到严格控制，并且操作环境高度安全。
- 建议不要在客户端计算机上启用内置管理员帐户，而是改用标准用户帐户和用户帐户控制 (UAC) 。 如果要启用内置管理员帐户来执行管理任务，出于安全原因，还应启用管理员审批模式。 有关详细信息，请参阅 UAC-管理员-Approval-Mode-for-the-Built-in-Administrator-account

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	非 Windows 二进制文件的同意提示

服务器类型或 GPO	默认值
DC 有效默认设置	非 Windows 二进制文件的同意提示
成员服务器有效默认设置	非 Windows 二进制文件的同意提示
客户端计算机有效默认设置	非 Windows 二进制文件的同意提示

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

UAC 功能尝试缓解的风险之一是在用户或管理员不知道其活动的情况下，在提升的凭据下运行的恶意软件。 此设置可提高管理员对提升权限操作的意识，并允许管理员在程序尝试提升权限时阻止恶意程序提升其权限。

对策

将“**用户帐户控制：管理员审批模式下管理员的提升提示行为**”设置配置为“**提示同意**”。

潜在影响

管理员应注意，当所有二进制文件都尝试运行时，系统会提示他们同意。

相关主题

- 安全选项

用户帐户控制: 标准用户的提升权限提示行为

项目 • 2023/04/12

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：标准用户安全策略设置的提升提示的行为** 。

此策略设置确定标准用户的提升提示行为。

可能值

- **自动拒绝提升请求**

  此选项在标准用户尝试执行需要特权提升的操作时返回拒绝 *访问* 错误消息。 大多数以标准用户身份运行桌面的组织都配置此策略以减少技术支持呼叫。

- **在安全桌面上提示输入凭据**

  当操作需要特权提升时，系统会在安全桌面上提示用户输入不同的用户名和密码。 如果用户输入了有效的凭据，则操作将继续具有适用的权限。

- **提示输入凭据**

  需要特权提升的操作会提示用户键入管理用户名和密码。 如果用户输入了有效的凭据，则操作将继续具有适用的权限。 这是默认值。

最佳做法

1. 将 **标准用户的用户帐户控制：提升提示行为** 配置为 **自动拒绝提升请求。** 此设置要求用户使用管理帐户登录才能运行需要特权提升的程序。
2. 作为安全最佳做法，标准用户不应了解管理密码。 但是，如果用户同时具有标准帐户和管理员级帐户，请在 **安全桌面上设置“凭据提示”** ，以便用户不会选择始终使用其管理员帐户登录，并且会改变其行为以使用标准用户帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	在安全桌面上提示输入凭据
DC 有效默认设置	在安全桌面上提示输入凭据
成员服务器有效默认设置	在安全桌面上提示输入凭据
客户端计算机有效默认设置	在安全桌面上提示输入凭据

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

所有审核功能都集成到组策略中。 可以在 组策略 管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

UAC 功能尝试缓解的风险之一是恶意程序在提升的凭据下运行，而用户或管理员不知道其活动。 此设置使用户意识到程序需要使用提升的权限操作，并且用户必须提供程序管

理凭据才能运行。

对策

将 **标准用户的用户帐户控制：提升提示行为** 配置为 **自动拒绝提升请求。** 此设置要求用户使用管理帐户登录才能运行需要特权提升的程序。 作为安全最佳做法，标准用户不应了解管理密码。 但是，如果用户同时具有标准帐户和管理员级帐户，我们建议 **在安全桌面上设置“凭据提示”** ，以便用户不会选择始终使用其管理员帐户登录，并且会改变其行为以使用标准用户帐户。

潜在影响

用户必须提供管理密码才能使用提升的权限运行程序。 在确定受影响的程序并修改标准操作过程以支持最低特权操作时，此影响可能会导致 IT 人员负载增加。

相关主题

- 安全选项

用户帐户控制: 检测应用程序安装并提示提升权限

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：检测应用程序安装并提示提升** 安全策略设置。

参考

此策略设置确定整个系统的应用程序安装检测行为。 某些软件可能会在获得运行权限后尝试自行安装。 用户可能会授予程序运行的权限，因为程序受信任。 然后，系统会提示用户安装未知组件。 此安全策略提供了另一种方法来识别和停止这些尝试的软件安装，以免造成损害。

可能值

- **Enabled**

  检测到需要特权提升才能安装的应用程序安装包，并提示用户输入管理凭据。

- **禁用**

  不会检测到需要特权提升才能安装的应用程序安装包，并且不会提示用户输入管理凭据。

最佳做法

1. 当企业运行利用委托安装技术（如 组策略 Software Install (GPSI) 或 Configuration Manager）的标准用户桌面时，安装程序检测是不必要的。 因此，可以将此安全策略设置为 “**已禁用**”。
2. 启用 **用户帐户控制：检测应用程序安装并提示提升** 设置，因此标准用户在安装软件之前必须提供管理凭据。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

某些恶意软件可能会在获得运行权限后尝试自行安装，例如，具有受信任的应用程序 shell 的恶意软件。 用户可能会授予程序运行的权限，因为程序受信任。 然后，系统会提示用户安装未知组件。 此策略提供了在软件造成损害之前捕获软件的另一种方法。

对策

启用 **用户帐户控制：检测应用程序安装并提示提升** 设置。

潜在影响

用户必须提供管理密码才能安装程序。

相关主题

- 安全选项

用户帐户控制: 只提升签名并验证的可执行文件

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：仅提升经过签名和验证** 的安全策略设置的可执行文件。

参考

此策略设置在请求特权提升的任何交互式应用程序上强制实施公钥基础结构 (PKI) 签名检查。 可以控制允许在本地计算机的受信任发布者存储中通过证书填充运行的应用。

受信任的发布者是计算机用户已选择信任的证书颁发者，该颁发者具有已添加到受信任发布者的存储的证书详细信息。

Windows 维护证书存储中的证书。 这些存储可以由文件系统或注册表中的容器表示，也可以作为物理存储（如智能卡）实现。 证书存储与计算机对象相关联，或者由在该计算机上具有安全上下文和配置文件的不同用户拥有。 此外，服务可以具有证书存储。 证书存储通常包含许多证书，这些证书可能来自许多不同的证书颁发机构 (CA)。 启动证书路径发现后，Windows 会尝试查找证书的颁发 CA，并生成受信任的根证书的证书路径。 中间证书作为应用程序协议的一部分包含在应用程序协议中，或者从组策略或通过 AIA) 扩展中指定的颁发机构信息访问 (URL 选取。 生成路径时，将验证路径中的每个证书是否与各种参数（例如名称、时间、签名、吊销状态和其他约束）有关。

可能值

- **Enabled**

  在允许其运行之前，强制对给定可执行文件执行 PKI 证书链验证。

- **禁用**

  在允许运行给定可执行文件之前，不强制实施 PKI 证书链验证。

最佳做法

- 最佳做法取决于你的安全和性能目标。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	禁用
DC 有效默认设置	禁用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 此策略的更改在本地保存或通过组策略分发时，无需重启计算机即可生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

知识产权、个人信息和其他机密数据通常由计算机上的应用程序操作，并且需要提升的凭据才能访问信息。 用户和管理员本质上信任与这些信息源一起使用的应用程序，并提供其凭据。 如果其中一个应用程序被看起来与受信任的应用程序相同的恶意应用程序所取代，则机密数据可能会泄露，并且用户的管理凭据也会泄露。

对策

启用 **用户帐户控制：仅提升已签名和验证的可执行文件。**

潜在影响

启用此设置需要具有 PKI 基础结构，并且企业管理员已使用允许应用程序的证书填充受信任的发布者存储区。 某些较旧的应用程序未签名，并且无法在使用此设置强化的环境中使用它们。 在实现此设置之前，应在预生产环境中仔细测试应用程序。 控制安装在桌面上的应用程序和加入域的硬件应提供类似的保护，使其免受此设置所解决的漏洞的影响。 此外，此设置提供的保护级别并不保证将找到所有恶意应用程序。

相关主题

- 安全选项

用户帐户控制: 仅提升安装在安全位置的 UIAccess 应用程序

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：仅提升安装在安全位置安全策略设置中的 UIAccess 应用程序 。**

参考

此策略设置强制要求通过在其应用清单中标记 UIAccess=true 来请求以 *UIAccess* 完整性级别运行的应用必须驻留在文件系统上的安全位置。 相对安全的位置仅限于以下目录：

- \Program Files\ 包括子目录
- \Windows\system32\
- \Program Files (x86) \ ，包括 64 位 Windows 版本的子目录

> **注意：**无论此安全设置的状态如何，Windows 都会在请求使用 UIAccess 完整性级别运行的任何交互式应用程序上强制实施 PKI 签名检查。

Background

用户界面特权隔离 (UIPI) 在 Windows 子系统中实施限制，以防止低特权应用程序发送消息或在较高特权进程中安装挂钩。 允许高特权应用程序将消息发送到特权较低的进程。 UIPI 不会干扰或更改具有相同特权 (或完整性) 级别的应用程序之间的消息行为。

Microsoft UI 自动化 是支持 Windows 操作系统中的辅助功能要求的当前模型。 旨在支持可访问用户体验的应用程序控制用户的其他 Windows 应用程序的行为。 当自动化客户端计算机和服务器上的所有应用程序都以标准用户 (即在中等完整性级别) 运行时，UIPI 限制不会干扰 Microsoft UI 自动化模型。

但是，有时，管理用户可能会在管理员审批模式下以基于 UAC 的提升权限运行应用程序。 Microsoft UI 自动化无法在无法绕过 UIPI 实施的限制的情况下，在桌面上驱动提升的应用程序的 UI 图形。 UI 自动化程序可以使用 UIAccess 跨特权级别绕过 UIPI 限制。

如果应用程序在请求权限时显示 UIAccess 属性，则应用程序会声明绕过 UIPI 限制以跨特权级别发送消息的要求。 在启动具有 UIAccess 权限的应用程序之前，设备将实现以下策

略检查。

1. 应用程序必须具有一个数字签名，该签名可以使用与本地设备上的受信任的根证书颁发机构存储关联的数字证书进行验证

2. 应用程序必须安装在只能由管理员写入的本地文件夹中，例如 Program Files 目录。UI 自动化应用程序允许的目录包括：
   a. %ProgramFiles% 及其子目录。
   b. %WinDir% 及其子目录，但由于标准用户具有写入访问权限而排除的几个子目录除外。

可能值

- **Enabled**

  仅当应用程序位于文件系统中的安全位置时，应用程序才能从 UIAccess 完整性开始。

- **禁用**

  应用程序可以从 UIAccess 完整性开始，即使它不驻留在文件系统中的安全位置。

最佳做法

- 将此策略设置为“**启用**”，以允许位于指定安全目录中的应用程序使用 UIAccess 完整性运行。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用

服务器类型或 GPO	默认值
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

安全注意事项

本部分介绍：

- 攻击者如何利用功能或其配置。
- 如何实施对策。
- 反措施实施可能产生的负面后果。

漏洞

当应用程序从标准用户提升到管理员的权限时，UIAccess 完整性允许应用程序绕过用户界面特权隔离 (UIPI) 限制。 启用此设置后，在其清单中将 UIAccess 标志设置为 true 的应用程序可以与在更高特权级别运行的应用程序交换信息，例如登录提示和特权提升提示。需要此功能才能支持辅助功能，例如将用户界面传输到替代表单的屏幕阅读器。 但大多数应用程序不需要它。 使用 UIAccess 权限启动的进程具有以下功能：

- 设置前景窗口。
- 使用 SendInput 函数驱动任何应用程序窗口。
- 通过使用低级别挂钩、原始输入、GetKeyState、GetAsyncKeyState 和 GetKeyboardInput，对所有完整性级别使用读取输入。
- 设置日志挂钩。

- 使用 AttachThreadInput 将线程附加到更高的完整性输入队列。

对策

启用 **用户帐户控制：仅提升安装在安全位置设置中的 UIAccess 应用程序** 。

潜在影响

如果请求 UIAccess 的应用程序满足 UIAccess 设置要求，则至少运行 Windows Vista 操作系统的计算机启动应用程序，并能够绕过大多数 UIPI 限制。 如果应用程序不符合安全限制，则启动应用程序时没有 UIAccess 权限，并且它只能与相同或较低特权级别的应用程序交互。

相关文章

- 安全选项

用户帐户控制: 以管理员批准模式运行所有管理员

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

本文介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项：**在管理员审批模式安全策略设置中运行所有管理员。**

参考

此策略设置确定整个系统的所有用户帐户控制 (UAC) 策略的行为。 此设置是打开或关闭 UAC 的设置。

可能值

- **Enabled**

  管理员审批模式和所有其他 UAC 策略都依赖于启用此选项。 更改此设置需要重启系统。

- **禁用**

  管理员审批模式和所有相关 UAC 策略处于禁用状态。

  > ⓘ **备注**
  >
  > 如果此安全设置配置为“**禁用**”，Windows 安全中心应用会通知用户操作系统的整体安全性已降低。

最佳做法

- 启用此策略以允许所有其他 UAC 功能和策略正常运行。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

当本地保存或通过组策略分发此策略的更改时，必须重启计算机，然后此策略才会生效。

组策略

所有审核功能都集成到组策略中。 可以在域、站点或组织单位的组策略管理控制台或本地安全策略管理单元中配置、部署和管理这些设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

此设置将打开或关闭 UAC。 如果未打开此设置，则不使用 UAC，并且计算机上不存在依赖于 UAC 的任何安全优势和风险缓解措施。

对策

启用 **用户帐户控制：将所有用户（包括管理员）作为标准用户设置运行** 。

潜在影响

用户和管理员必须了解如何使用 UAC 提示并调整其工作习惯以使用最低特权操作。

相关主题

- 安全选项

用户帐户控制: 提示提升权限时切换到安全桌面

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍用户帐户控制的最佳做法、位置、值、策略管理和安全注意事项 **：在提示提升安全策略设置时切换到安全桌面** 。

参考

此策略设置确定提升请求是在交互式用户桌面上还是安全桌面上提示。

安全桌面显示登录 UI，并限制功能和对系统的访问，直到满足登录要求。

安全桌面与用户桌面的主要区别在于，仅允许作为 SYSTEM 运行的受信任进程在此处运行 (也就是说，) 用户的权限级别不会运行任何进程。 还必须通过整个链信任从用户桌面访问安全桌面的路径。

可能值

- **Enabled**

  默认情况下，所有提升请求都转到安全桌面。

- **禁用**

  所有提升请求都转到交互式用户桌面。

最佳做法

- 启用 **用户帐户控制：在提示提升设置时切换到安全桌面。** 安全桌面通过在仅受信任的系统进程可访问的受保护内存部分中显示凭据对话框来帮助防止输入和输出欺骗。

位置

计算机配置\Windows 设置\安全设置\本地策略\安全选项

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

提升提示对话框可能会受到欺骗，导致用户向恶意软件透露其密码。 通过隐藏实际光标并将其替换为偏移量，使光标实际指向“ **允许**” 按钮，可以欺骗鼠标光标。

对策

启用 **用户帐户控制：在提示提升设置时切换到安全桌面。** 安全桌面通过在仅受信任的系统进程可访问的受保护内存部分中显示凭据对话框来帮助防止输入和输出欺骗。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

用户帐户控制: 将文件和注册表写入错误虚拟化到每用户位置

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **用户帐户控制：将文件和注册表写入失败虚拟化到每个用户位置** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置启用或禁用将早期应用程序的写入失败重定向到注册表和文件系统中定义的位置。 此功能可缓解以前以管理员身份运行的应用程序，并将运行时应用程序数据写入 %ProgramFiles%、%Windir%\system32 或 HKEY_LOCAL_MACHINE\Software\。

对于至少运行 Windows Vista 的设备上的应用程序，可以禁用此功能，因为它不必要。

可能值

- **Enabled**

  设置此值有助于将应用程序写入失败的运行时重定向到文件系统和注册表的已定义用户位置。

- **禁用**

  将数据写入受保护位置的应用程序失败。

最佳做法

1. 如果运行不符合 Windows Vista 的应用程序，请启用此安全策略，以防止这些较旧的应用程序将数据写入不安全的位置。
2. 如果至少只运行符合 Windows Vista 的应用程序，则不需要此功能，因此可以禁用此策略。

位置

\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

默认值

下表列出了此策略的实际和有效的默认值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	启用
DC 有效默认设置	启用
成员服务器有效默认设置	启用
客户端计算机有效默认设置	启用

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

重启要求

无。 当在本地保存或通过组策略分发对此策略进行的更改时，这些更改无需重启设备即可立即生效。

组策略

所有审核功能都集成到组策略中。 可以在组策略管理控制台 (GPMC) 或本地安全策略管理单元中配置、部署和管理这些设置， (OU) 。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

早期的应用程序可能不会将数据写入安全位置。

对策

启用 “**用户帐户控制：将文件和注册表写入失败虚拟化到每个用户位置**” 设置。

潜在影响

无。 此无影响状态是默认配置。

相关主题

- 安全选项

Windows 10的高级安全审核策略设置

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

提供有关 Windows 中可用的高级安全审核策略设置及其生成的审核事件的信息。

安全 **设置\高级审核策略配置下的安全审核策略** 设置可以通过跟踪精确定义的活动来帮助组织审核与重要业务相关和安全相关规则的合规性，例如：

- 组管理员修改了包含财务信息的服务器上的设置或数据。
- 已定义组中的员工已访问重要文件。
- 正确的系统访问控制列表 (SACL) 应用于计算机或文件共享上的每个文件和文件夹或注册表项，以防范未检测到的访问。

可以通过本地设备上的本地安全策略管理单元 (secpol.msc) 或使用 组策略 访问这些审核策略设置。

这些高级审核策略设置允许仅选择要监视的行为。 可以排除对你而言很少或无关的行为的审核结果，或创建过多日志条目的行为。 此外，由于可以使用域组策略对象应用安全审核策略，因此可以相对简单地修改、测试审核策略设置并将其部署到所选用户和组。

有关详细信息，请参阅 高级安全审核策略。

用户权限分配

项目 • 2023/03/18

适用范围

- Windows 10
- Windows 11

提供有关 Windows 中可用的用户权限分配安全策略设置用户权限的概述和链接。 用户权限控制用户登录系统的方法。 用户权限在本地设备级别应用，并且允许用户在设备或域中执行任务。 用户权限包括登录权限和权限。 登录权限控制有权登录设备的人员及其登录方式。 用户权限控制对计算机和域资源的访问，并且可以覆盖已针对特定对象设置的权限。 用户权限在“**用户权限分配**”项下的组策略中管理。

每个用户权限都有一个常量名称和一个与之关联的组策略名称。 在日志事件中引用用户权限时，将使用常量名称。 可以在组策略管理控制台 (GPMC) 计算机**配置\Windows 设置\安全设置\本地策略\用户权限分配**下的以下位置配置用户权限分配设置，或使用本地组策略编辑器 (gpedit.msc) 在本地设备上配置用户权限分配设置。

有关设置安全策略的信息，请参阅 配置安全策略设置。

下表链接到每个安全策略设置，并提供每个设置的常量名称。 设置说明包含参考信息、配置策略设置的最佳做法、默认值、操作系统版本之间的差异以及策略管理和安全性的注意事项。

组策略设置	常量名称
作为受信任的调用方访问凭据管理器	SeTrustedCredManAccessPrivilege
从网络访问此计算机	SeNetworkLogonRight
作为操作系统的一部分运行	SeTcbPrivilege
将工作站添加到域	SeMachineAccountPrivilege
为进程调整内存配额	SeIncreaseQuotaPrivilege
允许本地登录	SeInteractiveLogonRight
允许通过远程桌面服务登录	SeRemoteInteractiveLogonRight
备份文件和目录	SeBackupPrivilege
跳过遍历检查	SeChangeNotifyPrivilege
更改系统时间	SeSystemtimePrivilege

组策略设置	常量名称
更改时区	SeTimeZonePrivilege
创建页面文件	SeCreatePagefilePrivilege
创建令牌对象	SeCreateTokenPrivilege
创建全局对象	SeCreateGlobalPrivilege
创建永久共享对象	SeCreatePermanentPrivilege
创建符号链接	SeCreateSymbolicLinkPrivilege
调试程序	SeDebugPrivilege
拒绝从网络访问这台计算机	SeDenyNetworkLogonRight
拒绝作为批处理作业登录	SeDenyBatchLogonRight
拒绝以服务身份登录	SeDenyServiceLogonRight
拒绝本地登录	SeDenyInteractiveLogonRight
拒绝通过远程桌面服务登录	SeDenyRemoteInteractiveLogonRight
信任计算机和用户帐户可以执行委派	SeEnableDelegationPrivilege
从远程系统强制关机	SeRemoteShutdownPrivilege
生成安全审核	SeAuditPrivilege
身份验证后模拟客户端	SeImpersonatePrivilege
增加进程工作集	SeIncreaseWorkingSetPrivilege
提高计划优先级	SeIncreaseBasePriorityPrivilege
加载和卸载设备驱动程序	SeLoadDriverPrivilege
将页锁定在内存	SeLockMemoryPrivilege
作为批处理作业登录	SeBatchLogonRight
作为服务登录	SeServiceLogonRight
管理审核和安全日志	SeSecurityPrivilege
修改对象标签	SeRelabelPrivilege
修改固件环境值	SeSystemEnvironmentPrivilege
获取同一会话中的其他用户的模拟令牌	SeDelegateSessionUserImpersonatePrivilege

组策略设置	常量名称
执行批量维护任务	SeManageVolumePrivilege
配置文件单个进程	SeProfileSingleProcessPrivilege
配置文件系统性能	SeSystemProfilePrivilege
从扩展坞中移除计算机	SeUndockPrivilege
替换进程级令牌	SeAssignPrimaryTokenPrivilege
还原文件和目录	SeRestorePrivilege
关闭系统	SeShutdownPrivilege
同步目录服务数据	SeSyncAgentPrivilege
取得文件或其他对象的所有权	SeTakeOwnershipPrivilege

相关主题

- 安全策略设置参考

作为受信任的调用方访问凭据管理器

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文介绍 **访问凭据管理器作为受信任的调用方** 安全策略设置的建议做法、位置、值、策略管理和安全注意事项。

参考

凭据管理器在备份和还原期间使用 **“访问凭据管理器作为受信任的调用方** ”策略设置。 任何帐户都不应具有此特权，因为它仅分配给 Winlogon 服务。 如果将此权限授予其他实体，则用户的已保存凭据可能会泄露。

常量：SeTrustedCredManAccessPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 不要从默认值修改此策略设置。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表显示了服务器类型或 组策略 Object (GPO) 的默认值。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义

服务器类型或 GPO	默认值
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

如果向某个帐户授予此用户权限，该帐户的用户可能会创建一个应用程序，该应用程序调用凭据管理器并返回其他用户的凭据。

对策

不要将 **访问凭据管理器定义为凭据管理器** 以外的任何帐户的受信任调用方策略设置。

潜在影响

无。 未定义 是默认配置。

相关主题

用户权限分配

从网络访问此计算机 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Azure Stack HCI

介绍 **从网络安全策略设置访问此计算机的** 最佳做法、位置、值、策略管理和安全注意事项。

> ⚠ **警告**
>
> 如果运行 Windows Server 或 Azure Stack HCI 故障转移群集，请不要从网络策略设置中删除 “**访问此计算机** ”中的“经过身份验证的用户”。 这样做可能会导致意外的生产中断。 这是因为用于运行群集服务的本地用户帐户 CLIUSR。 CLIUSR 不是本地管理员组的成员，如果删除了“经过身份验证的用户组”，群集服务将没有足够的权限来正常运行或正常启动。

参考

“ **从网络访问此计算机**” 策略设置确定哪些用户可以从网络连接到设备。 许多网络协议都需要此功能，包括基于 SMB) 协议 (服务器消息块、NetBIOS、通用 Internet 文件系统 (CIFS) 和组件对象模型 Plus (COM+) 。

用户、设备和服务帐户通过显式或隐式地向已授予此用户权限的安全组添加或删除来获取或失去 “**从网络访问此计算机** ”用户权限。 例如，用户帐户或计算机帐户可以显式添加到自定义安全组或内置安全组，也可以由 Windows 隐式添加到计算安全组，例如域用户、经过身份验证的用户或企业域控制器。 默认情况下，在默认域控制器中定义计算组（例如“经过身份验证的用户”）和域控制器的企业域控制器组时，用户帐户和计算机帐户将被授予“**从网络访问此计算机**”用户权限) 对象 组策略 (GPO) 。

常量：SeNetworkLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 在桌面设备或成员服务器上，仅向用户和管理员授予此权限。
- 在域控制器上，仅向经过身份验证的用户、企业域控制器和管理员授予此权限。
- 在故障转移群集上，请确保已将此权限授予经过身份验证的用户。
- 此设置包括 “**每个人** ”组，以确保向后兼容。 Windows 升级后，在验证所有用户和组已正确迁移后，应删除 “**所有人** ”组，并改用 “**经过身份验证的用户组** ”。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

GPO 的服务器类型	默认值
默认域策略	未定义
默认域控制器策略	每个人、管理员、经过身份验证的用户、企业域控制器、Windows 2000 之前的兼容访问
独立服务器默认设置	每个人、管理员、用户、备份操作员
域控制器有效默认设置	每个人、管理员、经过身份验证的用户、企业域控制器、Windows 2000 之前的兼容访问
成员服务器有效默认设置	每个人、管理员、用户、备份操作员
客户端计算机有效的默认设置	每个人、管理员、用户、备份操作员

策略管理

修改此用户权限时，以下操作可能会导致用户和服务遇到网络访问问题：

- 删除企业域控制器安全组

- 删除经过身份验证的用户组或允许用户、计算机和服务帐户通过网络连接到计算机的显式组
- 删除所有用户和计算机帐户

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以从设备连接到网络的用户可以访问他们有权访问的目标设备上的资源。 例如，用户需要 “**从网络访问此计算机** ”用户权限才能连接到共享打印机和文件夹。 如果将此用户权限分配给“ **所有人** ”组，则组中的任何人都可以读取这些共享文件夹中的文件。 这种情况不太可能出现，因为默认安装至少为 Windows Server 2008 R2 或 Windows 7 创建的组不包括 “**所有人** ”组。 但是，如果设备已升级，并且原始设备将 **Everyone** 组作为其定义的用户和组的一部分包含在其中，则该组将作为升级过程的一部分进行转换，并存在于设备上。

对策

将 “**从网络访问此计算机** ”用户权限限制为仅那些需要访问计算机的用户和组。 例如，如果将此策略设置配置为 “**管理员** ”和“ **用户组** ”，则登录到域的用户可以访问从域中的服务器共享的资源（如果 **域用户组** 的成员包含在本地 **用户组** 中）。

> **注意** 如果使用 IPsec 来帮助保护组织中的网络通信，请确保为包含计算机帐户的组授予此权限。 此权限是成功进行计算机身份验证所必需的。 将此权限分配给 **经过身份验证的用户** 或 **域计算机** 符合此要求。

潜在影响

如果删除所有用户的域控制器上的 “**从网络访问此计算机** ”用户权限，则任何人都无法登录到域或使用网络资源。 如果在成员服务器上删除此用户权限，则用户无法通过网络连接到这些服务器。 如果已安装可选组件（如 ASP.NET 或 Internet Information Services (IIS) ），则可能需要将此用户权限分配给这些组件所需的其他帐户。 请务必验证授权用户是否为访问网络所需的设备分配了此用户权限。

如果运行 Windows Server 或 Azure Stack HCI 故障转移群集，请不要从网络策略设置中删除“访问此计算机”中的“经过身份验证的用户”。 这样做可能会导致意外的生产中断。 此中断是由于用于运行群集服务的本地用户帐户 CLIUSR 造成的。 CLIUSR 不是本地管理员组的成员，如果删除“经过身份验证的用户组”，群集服务将没有足够的权限来正常运行或正常启动。

相关主题

用户权限分配

作为操作系统的一部分运行

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍作为操作系统安全策略设置 **一部分的 Act** 的最佳做法、位置、值、策略管理和安全注意事项。

参考

作为操作系统策略设置的一部分的 Act 确定进程是否可以假定任何用户的标识，从而获得对用户有权访问的资源的访问权限。 通常，只有低级别身份验证服务需要此用户权限。 默认情况下，可能的访问权限不限于与用户关联的内容。 调用进程可能会请求向访问令牌添加任意额外特权。 调用过程还可能生成一个访问令牌，该令牌不提供用于系统事件日志中的审核的主要标识。

常量：SeTcbPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 不要将此权限分配给任何用户帐户。 仅将此用户权限分配给受信任的用户。
- 如果服务需要此用户权限，请将服务配置为使用本地系统帐户登录，该帐户本质上包含此用户权限。 不要创建单独的帐户并向其分配此用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效的默认设置	未定义

策略管理

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

作为操作系统用户权限的一部分的 Act 功能非常强大。 具有此用户权限的用户可以完全控制设备并擦除其活动的证据。

对策

将 Act **作为操作系统用户权限的一部分** 限制为尽可能少的帐户，在典型情况下甚至不应将其分配给管理员组。 当服务需要此用户权限时，请将服务配置为使用本地系统帐户登录，该帐户本质上包括此权限。 不要创建单独的帐户并向其分配此用户权限。

潜在影响

应该影响不大或没有影响，因为本地系统帐户以外的任何帐户很少需要 Act **作为操作系统** 用户权限的一部分。

相关主题

用户权限分配

将工作站添加到域

项目 • 2023/03/18

适用范围

- Windows Server

介绍将 **工作站添加到域** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以将设备添加到特定域。 要使它生效，必须分配它，以便它至少应用于一个域控制器。 分配有此用户权限的用户最多可向域添加 10 个工作站。 将计算机帐户添加到域允许设备参与基于 Active Directory 的网络。

常量：SeMachineAccountPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 配置此设置，以便仅允许 IT 团队的授权成员将设备添加到域。

位置

计算机配置\Windows 设置\安全设置\用户权限分配\

默认值

默认情况下，此设置允许对域控制器上的经过身份验证的用户进行访问，并且不会在独立服务器上定义。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	经过身份验证的用户
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

如果用户具有组织单位 (OU) 或目录中的计算机容器的“创建计算机对象”权限，则用户还可以将计算机加入域。 分配有此权限的用户可以将无限数量的设备添加到域，无论他们是否具有 “**将工作站添加到域**” 用户权限。

此外，通过“ **将工作站添加到域** ”用户权限创建的计算机帐户将“域管理员”作为计算机帐户的所有者。 通过计算机容器上的权限创建的计算机帐户使用创建者作为计算机帐户的所有者。 如果用户对容器具有权限，并且还具有 “**将工作站添加到域** ”用户权限，则会根据计算机容器权限而不是用户权限添加设备。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

此策略具有以下安全注意事项：

漏洞

“ **将工作站添加到域** ”用户权限存在中度漏洞。 具有此权限的用户可以将设备添加到以违反组织安全策略的方式配置的域。 例如，如果你的组织不希望其用户对其设备具有管理权限，用户可以在其计算机上安装 Windows，然后将计算机添加到域。 用户知道本地管理员帐户的密码，可以使用该帐户登录，然后将个人域帐户添加到本地管理员组。

对策

配置此设置，以便仅允许 IT 团队的授权成员将计算机添加到域。

潜在影响

对于从未允许用户设置自己的计算机并将其添加到域的组织，此对策没有影响。 对于允许部分或所有用户配置其自己的设备的组织，此对策将强制组织为这些过程建立正式流程。 它不会影响现有计算机，除非这些计算机已从中删除，然后将其添加到域。

相关主题

- 用户权限分配

为进程调整内存配额

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍调整进程安全策略设置的 **内存配额** 的最佳做法、位置、值、策略管理和安全注意事项。

参考

此特权确定谁可以更改进程可以使用的最大内存。 此权限对于基于组或用户的系统优化非常有用。

此用户权限在默认域控制器组策略对象 (GPO) 以及工作站和服务器的本地安全策略中定义。

常量：SeIncreaseQuotaPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

1. 将进程用户权限 **的"调整内存配额** "限制为仅需要调整内存配额以执行其作业的用户。
2. 如果用户帐户需要此用户权限，则可以将其分配给本地计算机帐户，而不是域帐户。

位置

计算机配置\Windows 设置\安全设置\用户权限分配\

默认值

默认情况下，管理员、本地服务和网络服务组的成员具有此权限。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	管理员 本地服务 网络服务
默认域控制器策略	管理员 本地服务 网络服务
独立服务器默认设置	管理员 本地服务 网络服务
域控制器有效默认设置	管理员 本地服务 网络服务
成员服务器有效默认设置	管理员 本地服务 网络服务
客户端计算机有效默认设置	管理员 本地服务 网络服务

策略管理

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**调整进程内存配额**” 权限的用户可以减少可用于任何进程的内存量，这可能会导致业务关键型网络应用程序变慢或失败。 恶意用户可能使用此权限来启动拒绝服务 (DoS) 攻击。

对策

将 “**调整进程用户权限的内存配额** ”限制为需要其执行作业的用户，例如维护数据库管理系统的应用程序管理员或管理组织目录及其支持基础结构的域管理员。

潜在影响

未将用户限制为具有有限权限的角色的组织可能会发现很难实施这种对策。 此外，如果已安装可选组件（如 ASP.NET 或 IIS），则可能需要 **将“调整进程内存配额** ”用户权限分配给这些组件所需的其他帐户。 IIS 要求将此权限显式分配给 IWAM_<ComputerName>、网络服务和服务帐户。 否则，此对策应该不会对大多数计算机产生影响。 如果用户帐户需要此用户权限，则可以将其分配给本地计算机帐户，而不是域帐户。

相关主题

- 用户权限分配

允许本地登录 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 “**允许本地登录** ”安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以在设备上启动交互式会话。 用户必须具有此用户权限才能通过基于 Windows 的成员设备或域控制器上运行的远程桌面服务会话登录。

> **注意：** 如果具有 “**允许通过远程桌面服务登录**” 权限，则没有此权限的用户仍然可以在设备上启动远程交互式会话。

常量：SeInteractiveLogonRight

可能值

- 用户定义的帐户列表
- 未定义

默认情况下，以下组的成员在工作站和服务器上具有此权限：

- 管理员
- 备份运算符
- 用户

默认情况下，以下组的成员在域控制器上具有此权限：

- 帐户操作员
- 管理员
- 备份运算符
- 打印运算符
- 服务器操作员

最佳做法

1. 将此用户权限限制为必须登录到设备控制台的合法用户。
2. 如果有选择地删除默认组，则可以限制分配给组织中特定管理角色的用户的能力。

位置

计算机配置\策略\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	帐户操作员 管理员 备份运算符 打印运算符 服务器操作员
独立服务器默认设置	管理员 备份运算符 用户
域控制器有效默认设置	帐户操作员 管理员 备份运算符 打印运算符 服务器操作员
成员服务器有效默认设置	管理员 备份运算符 用户
客户端计算机有效默认设置	管理员 备份运算符 用户

策略管理

无需重启设备即可实现此更改。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

修改此设置可能会影响与客户端、服务和应用程序的兼容性。 从默认域控制器的策略中删除成员设备和域中域控制器上的组件和程序使用的服务帐户时，请谨慎。 删除登录到域中成员设备的控制台的用户或安全组，或删除本地安全帐户管理器中定义的服务帐户 (SAM) 成员设备或工作组设备的数据库时，也请谨慎。 如果要授予用户帐户在本地登录到域控制器的能力，则必须使该用户成为已具有 “**允许登录本地** 系统”权限的组的成员，或授予该用户帐户的权限。 域中的域控制器共享默认域控制器组策略对象 (GPO) 。 向帐户授予 “**允许本地登录** ”权限时，即允许该帐户在本地登录到域中的所有域控制器。 如果 GPO 的 “**允许本地登录** ”设置中列出了“用户组”，则所有域用户可以在本地登录。 “用户”内置组包含“域用户”作为成员。

组策略

组策略设置按以下顺序通过 GPO 应用，这将在下一组策略更新时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**允许本地登录** ”用户权限的任何帐户都可以登录到设备的控制台。 如果不将此用户权限限制为必须登录到计算机控制台的合法用户，则未经授权的用户可以下载并运行恶意软件以提升其权限。

对策

对于域控制器，请将 “**仅允许本地登录** ”用户权限分配给管理员组。 对于其他服务器角色，除了管理员之外，还可以选择添加备份操作员。 对于最终用户计算机，还应将此权限分配给用户组。 或者，可以将“帐户操作员”、“服务器操作员”和“来宾”等组分配给 “**拒绝本地登录** ”用户权限。

潜在影响

如果删除这些默认组，则可以限制分配给环境中特定管理角色的用户的功能。 如果已安装可选组件（如 ASP.NET 或 IIS），则可能需要将 “**允许本地登录** ”用户权限分配给这些组件所需的其他帐户。 IIS 要求将此用户权限分配给 IUSR_<*ComputerName*> 帐户。 应确认委托的活动不会受到对 **允许登录本地** 用户权限分配所做的任何更改的不利影响。

相关主题

- 用户权限分配

允许通过远程桌面服务登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 “**允许通过远程桌面服务登录** ”安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户或组可以通过远程桌面服务连接访问远程设备的登录屏幕。 用户可以与特定服务器建立远程桌面服务连接，但无法登录到同一服务器的控制台。

常量：SeRemoteInteractiveLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 若要控制谁可以打开远程桌面服务连接并登录到设备，请将用户添加到远程桌面用户组或从中删除用户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，Administrators 组的成员在域控制器、工作站和服务器上具有此权限。 远程桌面用户组在工作站和服务器上也具有此权限。 下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
域控制器本地安全策略	管理员
独立服务器默认设置	管理员 远程桌面用户
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员 远程桌面用户
客户端计算机有效默认设置	管理员 远程桌面用户

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

组策略

若要使用远程桌面服务成功登录到远程设备，用户或组必须是远程桌面用户或管理员组的成员，并被授予 “**允许通过远程桌面服务登录** ”权限。 用户可以与特定服务器建立远程桌面服务会话，但无法登录到同一服务器的控制台。

若要排除用户或组，可以将 “**通过远程桌面服务拒绝登录**” 用户权限分配给这些用户或组。 但是，使用此方法时要小心，因为可能会为允许通过 **远程桌面服务** 登录用户权限访问的合法用户或组创建冲突。

有关详细信息，请参阅 拒绝通过远程桌面服务登录。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略设置按以下顺序通过 GPO 应用，这将在下一组策略更新时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**允许通过远程桌面服务登录** ”用户权限的任何帐户都可以登录到设备的远程控制台。 如果不将此用户权限限制为必须登录到计算机主机的合法用户，则未经授权的用户可以下载并运行恶意软件来提升其权限。

对策

对于域控制器，请仅将 “**允许通过远程桌面服务登录**” 用户权限分配给“管理员”组。 对于其他服务器角色和设备，请添加远程桌面用户组。 对于已启用远程桌面 (RD) 会话主机角色服务且未在应用程序服务器模式下运行的服务器，请确保只有必须远程管理计算机的授权 IT 人员属于这些组。

> **谨慎：** 对于在应用程序服务器模式下运行的 RD 会话主机服务器，请确保只有需要访问服务器的用户才具有属于远程桌面用户组的帐户，因为默认情况下，此内置组具有此登录权限。

或者，可以将 “**通过远程桌面服务拒绝登录**” 用户权限分配给帐户操作员、服务器操作员和来宾等组。 但是，使用此方法时要小心，因为可能会阻止对合法管理员的访问，这些管理员也属于具有 “**通过远程桌面服务拒绝登录** ”用户权限的组。

潜在影响

从其他组中删除 “**允许通过远程桌面服务登录** ”用户权限 (或这些默认组中的成员身份更改) 可能会限制在你的环境中执行特定管理角色的用户的能力。 应确认委托的活动不会受到不利影响。

相关主题

- 用户权限分配

备份文件和目录 - 安全策略设置

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

本文介绍 **备份文件和目录** 安全策略设置的建议做法、位置、值、策略管理和安全注意事项。

参考

此用户权限确定哪些用户可以绕过文件和目录、注册表和其他永久性对象权限，以便备份系统。 仅当应用程序尝试通过 NTFS 备份应用程序编程接口 (API 通过 NTBACKUP.EXE 等工具) 访问时，此用户权限才有效。 否则，将应用标准文件和目录权限。

此用户权限类似于向在系统上的所有文件和文件夹上选择的用户或组授予以下权限：

- 遍历文件夹/执行文件
- 列出文件夹/读取数据
- 读取属性
- 读取扩展属性
- 读取权限

工作站和服务器上的默认值：

- 管理员
- 备份运算符

域控制器上的默认值：

- 管理员
- 备份运算符
- 服务器操作员

常量：SeBackupPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

1. 将 **备份文件和目录** 用户权限限制为必须备份组织数据作为日常工作职责的一部分的 IT 团队成员。 由于无法确保用户正在备份数据、窃取数据或复制要分发的数据，因此只能将此用户权限分配给受信任的用户。
2. 如果备份软件在特定服务帐户下运行，则只有这些帐户 (而不是 IT 人员) 应拥有备份文件和目录的用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此权限授予工作站和服务器上的管理员和备份操作员。 在域控制器上，管理员、备份操作员和服务器操作员具有此权限。

下表列出了服务器类型或 组策略 Object (GPO) 的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	管理员 备份运算符 服务器操作员
独立服务器默认设置	管理员 备份运算符
域控制器有效默认设置	管理员 备份运算符 服务器操作员
成员服务器有效默认设置	管理员 备份运算符
客户端计算机有效默认设置	管理员 备份运算符

策略管理

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过 GPO 按以下顺序应用，这将在下一组策略更新时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以将设备中的数据备份到单独的媒体的用户可以将媒体带到具有管理权限的非域计算机，然后还原数据。 他们可以获取文件的所有权，并查看数据集中包含的任何未加密数据。

对策

将 **备份文件和目录** 用户权限限制为必须备份组织数据作为日常工作职责的一部分的 IT 团队成员。 如果使用在特定服务帐户下备份数据的软件，则只有这些帐户（，而不是 IT 员工) 应有权备份文件和目录。

潜在影响

用户有权备份文件和目录的组成员身份的更改可能会限制分配给环境中特定管理角色的用户的能力。 确认授权管理员仍可备份文件和目录。

相关主题

- 用户权限分配

跳过遍历检查

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

> 在比较 Windows 10 版本 中了解有关每个 Windows 版本支持哪些特性和功能的详细信息。

介绍 **绕过遍历** 检查安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户 (或代表用户帐户执行操作的进程，) 有权在 NTFS 文件系统或注册表中导航对象路径，而无需检查遍历文件夹的特殊访问权限。 此用户权限不允许用户列出文件夹的内容。 它仅允许用户遍历文件夹以访问允许的文件或子文件夹。

常量：SeChangeNotifyPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

1. 如果要阻止用户看到他们无权访问的任何文件夹或文件，请使用基于访问的枚举。
2. 在大多数情况下，请使用此策略的默认设置。 如果更改设置，请通过测试验证意向。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 经过身份验证的用户 所有人 本地服务 网络服务 Windows 2000 之前的兼容访问
独立服务器默认设置	管理员 备份运算符 用户 所有人 本地服务 网络服务
域控制器有效默认设置	管理员 经过身份验证的用户 所有人 本地服务 网络服务 Windows 2000 之前的兼容访问
成员服务器有效默认设置	管理员 备份运算符 用户 所有人 本地服务 网络服务
客户端计算机有效默认设置	管理员 备份运算符 用户 所有人 本地服务 网络服务

策略管理

文件和文件夹的权限通过文件系统访问控制列表的相应配置进行控制，(ACL)。 遍历文件夹的功能不会向用户提供任何读取或写入权限。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

“**绕过遍历检查**”设置的默认配置是允许所有用户绕过遍历检查。 文件和文件夹的权限是通过文件系统访问控制列表 (ACL) 的适当配置来控制的，因为遍历文件夹的功能不会向用户提供任何读取或写入权限。 如果配置权限的管理员不了解此策略设置的工作原理，则默认配置可能导致出现问题的唯一方案是。 例如，管理员可能期望无法访问文件夹的用户无法访问任何子文件夹的内容。 这种情况不太可能出现，因此，这种脆弱性的风险很小。

对策

关注安全性的组织可能希望从具有 “**绕过遍历检查** 用户”权限的组列表中删除“每个人”组。 对遍历分配进行显式控制是限制对敏感信息的访问的有效方法。 还可以使用基于访问的枚举。 如果使用基于访问的枚举，则用户看不到他们无权访问的任何文件夹或文件。 有关此功能的详细信息，请参阅 基于访问的枚举。

潜在影响

Windows 操作系统和许多应用程序的设计预期是，任何能够合法访问计算机的人都将拥有此用户权限。 因此，建议在对生产系统进行此类更改之前，彻底测试 **对“绕过遍历检查** 用户”分配所做的任何更改。 具体而言，IIS 要求将此用户权限分配给网络服务、本地服务、IIS_WPG、IUSR_<*ComputerName*> 和 IWAM_<*ComputerName*> 帐户。 (还必须通过用户组中的成员身份将其分配给 ASPNET 帐户。) 建议将此策略设置保留为其默认配置。

相关主题

- 用户权限分配

更改系统时间 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **更改系统时间** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以调整设备内部时钟上的时间。 此权限允许计算机用户更改与事件日志、数据库事务和文件系统中的记录关联的日期和时间。 执行时间同步的进程也需要此权限。 此设置不会影响用户更改系统时间的时区或其他显示特征的能力。 有关分配更改时区权限的信息，请参阅 更改时区。

常量：SeSystemtimePrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 将 “**更改系统时间** 用户权限”限制为需要更改系统时间的合法用户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，管理员和本地服务组的成员在工作站和服务器上拥有此权限。 管理员、服务器操作员和本地服务组的成员在域控制器上拥有此权限。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 服务器操作员 本地服务
独立服务器默认设置	管理员 本地服务
DC 有效默认设置	管理员 服务器操作员 本地服务
成员服务器有效默认设置	管理员 本地服务
客户端计算机有效默认设置	管理员 本地服务

策略管理

本部分介绍可帮助你管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以更改计算机上的时间的用户可能会导致一些问题。 例如：

- 事件日志条目上的时间戳可能不准确
- 创建或修改的文件和文件夹上的时间戳可能不正确
- 属于域的计算机可能无法自行进行身份验证
- 尝试从时间不准确的设备登录到域的用户可能无法进行身份验证。

此外，由于 Kerberos 身份验证协议要求请求方和验证器在管理员定义的倾斜期内同步其时钟，因此更改设备时间的攻击者可能导致该计算机无法获取或授予 Kerberos 协议票证。

在大多数域控制器、成员服务器和最终用户计算机上，这些类型事件的风险得到缓解，因为 Windows 时间服务以以下方式自动与域控制器同步时间：

- 所有桌面客户端设备和成员服务器都使用身份验证域控制器作为其入站时间伙伴。
- 域中的所有域控制器都指定主域控制器 (PDC) 仿真器操作主机作为其入站时间伙伴。
- 所有 PDC 模拟器操作主机在其入站时间伙伴的选择中都遵循域的层次结构。
- 域根目录中的 PDC 模拟器操作主机对组织具有权威性。 因此，建议将此计算机配置为与可靠的外部时间服务器同步。

如果攻击者能够更改系统时间，然后停止 Windows 时间服务或将其重新配置为与不准确的时间服务器同步，则此漏洞会更加严重。

对策

将 “**更改系统时间** 用户权限”限制为需要更改系统时间的合法用户，例如 IT 团队成员。

潜在影响

应该没有影响，因为大多数组织的时间同步应该针对属于该域的所有计算机完全自动化。 不属于域的计算机应配置为与外部源（如 Web 服务）同步。

相关主题

- 用户权限分配

更改时区 - 安全策略设置

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **更改时区** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以调整设备用于显示本地时间的时区，其中包括设备的系统时间加上时区偏移量。

常量：SeTimeZonePrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

无。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 用户

服务器类型或 GPO	默认值
独立服务器默认设置	管理员 用户
域控制器有效默认设置	管理员 用户
成员服务器有效默认设置	管理员 用户
客户端计算机有效默认设置	管理员 用户

策略管理

无需重启设备即可使此策略设置生效。

此用户权限分配帐户的任何更改将在下次帐户登录时生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

更改时区表示很少的漏洞，因为系统时间不受影响。 此设置仅允许用户显示其首选时区，同时与不同时区的域控制器同步。

对策

由于系统时间不受此设置影响，因此不需要采取对策。

潜在影响

无。

相关主题

- 用户权限分配

创建页面文件 - 安全策略设置

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **创建页面文件** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

Windows 将硬盘驱动器的一部分指定为称为页面文件的虚拟内存，或者更具体地说，指定为pagefile.sys。 它用于补充计算机的随机访问内存 (RAM) ，以提高常用程序和数据的性能。 尽管文件在浏览时处于隐藏状态，但你可以使用系统设置对其进行管理。

此策略设置确定哪些用户可以创建和更改页面文件的大小。 它确定用户是否可以在“**系统属性**”对话框的“**高级**”选项卡上的“**性能选项**”框中指定特定驱动器的页面文件大小，或者通过使用内部应用程序接口 (API) 。

常量：SeCreatePagefilePrivilege

可能值

- 用户定义的帐户列表
- 管理员

最佳做法

- 将 “**创建页面文件** ”用户权限限制为“管理员”，这是默认值。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，管理员组的成员具有此权限。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	管理员
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以更改页面文件大小的用户可能会使其变小，或者将文件移动到高度碎片化的存储卷，这可能会导致设备性能降低。

对策

将 “**创建页面文件** ”用户权限限制为 Administrators 组的成员。

潜在影响

无。 将此权限限制为 Administrators 组的成员是默认配置。

相关主题

- 用户权限分配

创建令牌对象

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **创建令牌对象** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定进程可用于创建令牌的帐户，以及当进程使用 NtCreateToken () 或其他令牌创建 API 时，该进程可用于获取对本地资源的访问权限的帐户。

当用户登录到本地设备或通过网络连接到远程设备时，Windows 会生成用户的访问令牌。 然后，系统会检查令牌以确定用户权限的级别。 撤销权限时，将立即记录更改，但更改不会反映在用户的访问令牌中，直到用户下次登录或连接。

常量：SeCreateTokenPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 此用户权限由操作系统在内部使用。 除非有必要，否则不要将此用户权限分配给本地系统以外的用户、组或进程。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

此用户权限由操作系统在内部使用。 默认情况下，它不会分配给任何用户组。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	本地系统
成员服务器有效默认设置	本地系统
客户端计算机有效默认设置	本地系统

策略管理

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

> **谨慎：** 授予此用户权限的用户帐户对系统拥有完全控制权，这可能导致系统遭到入侵。 强烈建议不要将此权限分配给任何用户帐户。

Windows 检查用户的访问令牌以确定用户权限的级别。 当用户登录到本地设备或通过网络连接到远程设备时，将生成访问令牌。 撤销权限时，将立即记录更改，但更改不会反映在用户的访问令牌中，直到用户下次登录或连接。 能够创建或修改令牌的用户可以更改计算机上任何帐户的访问权限级别（如果他们当前已登录）。 他们可以升级其特权或创建 DoS 条件。

对策

不要将 **创建令牌对象** 用户权限分配给任何用户。 需要此用户权限的进程应使用已包含它的本地系统帐户，而不是分配了此用户权限的单独用户帐户。

潜在影响

无。 “未定义”是默认配置。

相关主题

- 用户权限分配

创建全局对象

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **创建全局对象** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以创建可供所有会话使用的全局对象。 如果用户没有此用户权限，则仍可以创建特定于其自己的会话的对象。

全局对象是一个对象，可供任意数量的进程或线程使用，甚至这些进程或线程未在用户的会话中启动。 远程桌面服务在其进程中使用全局对象来促进连接和访问。

常量：SeCreateGlobalPrivilege

可能值

- 用户定义的帐户列表
- 下面列出的默认帐户

最佳做法

- 不要将此权限分配给任何用户帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，管理员组的成员具有此权限，受支持版本的 Windows 上的本地服务和网络服务帐户也具有此权限。 包含服务是为了与早期版本的 Windows 向后兼容。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 本地服务 网络服务 服务
独立服务器默认设置	管理员 本地服务 网络服务 服务
域控制器有效默认设置	管理员 本地服务 网络服务 服务
成员服务器有效默认设置	管理员 本地服务 网络服务 服务
客户端计算机有效默认设置	管理员 本地服务 网络服务 服务

策略管理

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

用户帐户需要 “**创建全局对象** ”用户权限才能在远程桌面会话中创建全局对象。 用户仍然可以创建会话规范对象，而无需分配此用户权限。 分配此权限可能会面临安全风险。

默认情况下， **管理员** 组成员、系统帐户和服务控制管理器启动的服务分配有 “**创建全局对象**” 用户权限。 添加到 **远程桌面** 用户组的用户也具有此用户权限。

对策

当非管理员需要使用远程桌面访问服务器时，请将用户添加到 **远程桌面用户组** ，而不是向他们分配此用户权限。

潜在影响

无。 “未定义”是默认域策略配置。

相关主题

- 用户权限分配

创建永久共享对象

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **创建永久共享对象** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此用户权限确定进程可以使用哪些帐户通过对象管理器创建目录对象。 目录对象包括 Active Directory 对象、文件和文件夹、打印机、注册表项、进程和线程。 具有此功能的用户可以创建永久共享对象，包括设备、信号灯和互斥体。 此用户权限对于扩展对象命名空间的内核模式组件很有用。 由于在内核模式下运行的组件本质上具有分配给它们的此用户权限，因此无需专门分配它。

常量：SeCreatePermanentPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 拥有 “**创建永久共享对象**” 用户权限的用户可以创建新的共享对象并向网络公开敏感数据。 因此，请勿将此权限分配给任何用户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下， **LocalSystem** 是唯一具有此权限的帐户。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	LocalSystem
成员服务器有效默认设置	LocalSystem
客户端计算机有效默认设置	LocalSystem

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

拥有 “**创建永久共享对象**” 用户权限的用户可以创建新的共享对象并向网络公开敏感数据。

对策

不要将 “**创建永久共享对象**” 用户权限分配给任何用户。 需要此用户权限的进程应使用已包含此用户权限的系统帐户，而不是单独的用户帐户。

潜在影响

无。 “未定义”是默认配置。

相关主题

- 用户权限分配

创建符号链接

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **创建符号链接** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此用户权限确定用户是否可以从其登录的设备创建符号链接。

符号链接是指向另一个名为目标的文件系统对象的文件系统对象。 符号链接对用户是透明的。 链接显示为普通文件或目录，用户或应用程序可以以完全相同的方式处理它们。 符号链接旨在帮助迁移和应用程序与 UNIX 操作系统的兼容性。 Microsoft 实现了与 UNIX 链接一样的功能的符号链接。

> ⚠ **警告**
>
> 此权限应仅授予受信任的用户。 符号链接可能会暴露应用程序中的安全漏洞，这些安全漏洞不是用来处理这些漏洞的。

常量：SeCreateSymbolicLinkPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 只有受信任的用户才应获得此用户权限。 符号链接可能会暴露应用程序中的安全漏洞，这些安全漏洞不是用来处理这些漏洞的。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，管理员组的成员具有此权限。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍可用于帮助你管理此策略的不同功能和工具。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

- 本地策略设置
- 网站策略设置
- 域策略设置
- OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

命令行工具

此设置可以与符号链接文件系统设置结合使用，该设置可使用命令行工具操作，以控制设备上允许的符号链接类型。 有关详细信息，请在命令提示符处键入 `fsutil behavior set symlinkevaluation /?` 。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

拥有 “**创建符号链接**” 用户权限的用户可能会无意或恶意地向系统公开符号链接攻击。 符号链接攻击可用于更改对文件的权限、损坏数据、销毁数据或作为 DoS 攻击。

对策

不要将 “**创建符号链接**” 用户权限分配给标准用户。 将此权限限制为受信任的管理员。 可以使用 **fsutil** 命令建立符号链接文件系统设置，该设置控制可在计算机上创建的符号链接类型。

潜在影响

无。 未定义 是默认配置。

相关主题

- 用户权限分配

调试程序

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **调试程序** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以附加到或打开任何进程，甚至是他们不拥有的进程。 调试自己的应用程序的开发人员不需要此用户权限。 调试新系统组件的开发人员需要此用户权限。 此用户权限提供对敏感和关键操作系统组件的访问权限。

常量：SeDebugPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 仅将此用户权限分配给受信任的用户以减少安全漏洞。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，管理员组的成员具有此权限。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍了可用于帮助管理此策略的功能和工具。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

调试 **程序** 用户权限可用于从系统内存中捕获敏感设备信息，或者访问和修改内核或应用程序结构。 某些攻击工具利用此用户权限提取哈希密码和其他专用安全信息或插入恶意软件。 默认情况下， “**调试程序** ”用户权限仅分配给管理员，这有助于缓解此漏洞的风险。

对策

删除不需要 **调试程序** 用户权限的所有用户和组的帐户。

潜在影响

如果撤销此用户权限，则任何人都无法调试程序。 但是，通常情况下，在生产设备上很少需要此功能。 如果出现需要在生产服务器上调试应用程序的问题，可以将服务器暂时移动到其他组织单位，(OU)，并将**调试程序**用户权限分配给该 OU 的单独组策略。

相关主题

- 用户权限分配

拒绝从网络访问这台计算机

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **拒绝从网络安全策略设置访问此计算机的** 最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定阻止哪些用户通过网络访问设备。

常量：SeDenyNetworkLogonRight

可能值

- 用户定义的帐户列表
- 来宾

最佳做法

- 由于所有Active Directory 域服务程序都使用网络登录进行访问，因此在域控制器上分配此用户权限时请谨慎。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，在域控制器和独立服务器上，此设置为 Guest。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	来宾
独立服务器默认设置	来宾
域控制器有效默认设置	来宾
成员服务器有效默认设置	来宾
客户端计算机有效默认设置	来宾

策略管理

本部分介绍可用于帮助你管理此策略的功能和工具。

无需重启设备即可使此策略设置生效。

如果用户帐户受这两个策略的约束，则此策略设置将取代 “**从网络访问此计算机** ”策略设置。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以通过网络登录到设备的用户可以枚举帐户名称、组名称和共享资源的列表。 有权访问共享文件夹和文件的用户可以通过网络进行连接，并可能查看或修改数据。

对策

将 “**拒绝从网络用户访问此计算机** ”权限分配给以下帐户：

- 匿名登录
- 内置本地管理员帐户
- 本地来宾帐户
- 所有服务帐户

此列表的一个重要例外是用于启动必须通过网络连接到设备的服务的任何服务帐户。 例如，假设你配置了一个可供 Web 服务器访问的共享文件夹，并且通过网站显示该文件夹中的内容。 可能需要允许运行 IIS 的帐户从网络使用共享文件夹登录到服务器。 如果出于法规合规性考虑，必须配置处理敏感信息的服务器和工作站，则此用户权限有效。

> **备注**
>
> 如果在 Windows 服务的登录属性中配置了服务帐户，则需要域控制器的网络登录权限才能正确启动。

潜在影响

如果为其他帐户配置 “**拒绝从网络访问此计算机** ”用户权限，则可以限制分配给环境中特定管理角色的用户的功能。 应验证委派的任务是否没有受到负面影响。

相关主题

- 用户权限分配

拒绝作为批处理作业登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文介绍 **拒绝作为批处理作业安全** 策略设置登录的建议做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定通过使用批处理队列工具在将来自动计划和启动作业来阻止哪些帐户登录。 使用任务计划程序启动计划作业的任何帐户都需要能够使用批处理队列工具登录。

常量：SeDenyBatchLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

1. 分配此用户权限时，请彻底测试效果是否为预期效果。
2. 在域中，在适用的 组策略 对象 (GPO) 上修改此设置。
3. **拒绝作为批处理作业登录** 会阻止管理员或操作员使用其个人帐户来计划任务。 当该人员过渡到其他职位或职责时，此限制有助于业务连续性。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的功能和工具。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

此策略设置可能与“ **以批处理作业身份登录**” 设置冲突，并否定该设置。

组策略

在已加入域的设备（包括域控制器）上，域策略可能会覆盖此策略，这会阻止你修改本地策略设置。

例如，若要在域控制器上配置任务计划程序，检查组策略管理控制台中两个域控制器策略和域策略 GPO 的“设置”选项卡， (GPMC) 。 验证“ **拒绝作为批处理作业登录** ”设置中不存在目标帐户。

用户权限分配，并在 “**作为批处理作业登录**” 设置中正确配置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 **批量作业用户登录** 权限的帐户可用于计划可能消耗过多计算机资源并导致拒绝服务条件的作业。

对策

将 “**以批处理作业身份拒绝登录** ”用户权限分配给本地来宾帐户。

潜在影响

如果将 “**拒绝登录**”**作为批处理作业** 用户权限分配给其他帐户，则可以拒绝向分配了特定管理角色的用户执行所需作业活动的能力。 确认委托的任务不会受到不利影响。

相关主题

- 用户权限分配

拒绝以服务身份登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文介绍 **拒绝作为服务登录** 安全策略设置的建议做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定阻止哪些用户登录到设备上的服务应用程序。

服务是在没有用户界面的系统后台运行的应用程序类型。 它提供核心操作系统功能，例如 Web 服务、事件日志记录、文件服务、打印、加密和错误报告。

常量：SeDenyServiceLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

1. 分配此用户权限时，请彻底测试效果是否为预期效果。
2. 在域中，在适用的 组策略 对象 (GPO) 上修改此设置。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍可用于帮助你管理此策略的功能和工具。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

在已加入域的设备（包括域控制器）上，域策略可能会覆盖此策略，这会阻止你修改本地策略设置。

此策略设置可能与“ **以服务身份登录**” 设置冲突，并否定该设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

可以登录到服务应用程序的帐户可用于配置和启动新的未经授权的服务，例如键盘记录程序或其他恶意软件。 由于只有具有管理权限的用户才能安装和配置服务，并且已具有该访问权限级别的攻击者可以使用系统帐户将服务配置为运行，因此指定对策的优势有所降低。

对策

建议不要将 “**拒绝以服务身份登录** ”用户权限分配给任何帐户。 此配置是默认配置。 对安全性有强烈关注的组织在确定永远不需要登录到服务应用程序时，可能会将此用户权限分配给组和帐户。

潜在影响

如果将 **拒绝登录作为服务** 用户权限分配给特定帐户，则服务可能无法启动，并可能导致拒绝服务条件。

相关主题

- 用户权限分配

拒绝本地登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **拒绝本地登录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定阻止哪些用户直接在设备的控制台登录。

常量：SeDenyInteractiveLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

1. 将 “**拒绝本地登录** ”用户权限分配给本地来宾帐户，以限制可能未经授权的用户访问。
2. 结合 “**允许本地登录** ”策略设置测试对此策略设置的修改，以确定用户帐户是否受这两种策略的约束。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

如果将此策略设置应用于“每个人”组，则任何人都无法在本地登录。

组策略

如果用户帐户受这两个策略的约束，则此策略设置将取代 “**允许本地登录** ”策略设置。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

任何能够在本地登录的帐户都可用于在设备的控制台登录。 如果此用户权限不仅限于必须登录到设备控制台的合法用户，则未经授权的用户可能会下载并运行提升其用户权限的恶意软件。

对策

将 “**拒绝本地登录** ”用户权限分配给本地来宾帐户。 如果已安装可选组件（如 ASP.NET），则可能需要将此用户权限分配给这些组件所需的其他帐户。

潜在影响

如果将 “**拒绝本地登录** ”用户权限分配给其他帐户，则可以限制分配给环境中特定角色的用户的能力。 但是，应将此用户权限显式分配给配置了 Web 服务器角色的设备上的 ASPNET 帐户。 应确认委托的活动不会受到不利影响。

相关主题

- 用户权限分配

拒绝通过远程桌面服务登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **拒绝通过远程桌面服务登录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定阻止哪些用户通过远程桌面服务通过远程桌面连接登录到设备。 用户可以与特定服务器建立远程桌面连接，但无法登录到该服务器的控制台。

常量：SeDenyRemoteInteractiveLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 若要控制谁可以打开远程桌面连接并登录到设备，请将用户帐户添加到远程桌面用户组或从中删除用户帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

Remote System 属性控制远程桌面服务 (**允许或阻止与计算机) 的远程连接**和远程协助 (**允许远程协助连接到此计算机**) 的设置。

组策略

如果用户帐户受这两个策略的约束，则此策略设置将取代 “允许通过远程桌面服务登录 ” 策略设置。

组策略设置按以下顺序应用。 在下一次更新组策略时，它们会覆盖本地设备上的设置。

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. 组织单位策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

任何有权通过远程桌面服务登录的帐户都可用于登录到设备的远程控制台。 如果此用户权限不仅限于需要登录到计算机控制台的合法用户，则恶意用户可能会下载并运行提升其用户权限的软件。

对策

将 “**拒绝通过远程桌面服务登录** ”用户权限分配给内置本地来宾帐户和所有服务帐户。 如果已安装可选组件（如 ASP.NET），则可能需要将此用户权限分配给这些组件所需的其他帐户。

潜在影响

如果将 “**通过远程桌面服务拒绝登录**” 用户权限分配给其他组，则可以限制分配给环境中特定管理角色的用户的能力。 具有此用户权限的帐户无法通过远程桌面服务或远程协助连接到设备。 应确认委托的任务不会受到负面影响。

相关主题

- 用户权限分配

信任计算机和用户帐户可以执行委派

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍启用对委派安全策略设置信任 **计算机和用户帐户** 的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以在用户或计算机对象上设置 “**受信任的委派** ”设置。 安全帐户委派允许连接到多个服务器，每次服务器更改都会保留原始客户端的身份验证凭据。 委托身份验证是客户端和服务器应用程序在具有多个层时使用的一项功能。 它允许面向公众的服务使用客户端凭据对应用程序或数据库服务进行身份验证。 若要实现此配置，客户端和服务器必须在受信任的委派帐户下运行。

只有具有 “**启用对委派信任的计算机和用户帐户**” 凭据的管理员才能设置委派。 域管理员和企业管理员具有此凭据。 允许用户信任委派的过程取决于域的功能级别。

授予此权限的用户或计算机对象必须对帐户控制标志具有写入访问权限。 在设备 (或在用户上下文) 下运行的服务器进程（受信任的委派）可以使用客户端的委派凭据访问另一台计算机上的资源。 但是，客户端帐户必须对 对象上的帐户控制标志具有写入访问权限。

常量：SeEnableDelegationPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 没有理由将此用户权限分配给属于域的成员服务器和工作站上的任何人，因为它在这些上下文中没有意义。 它仅在域控制器和独立设备上相关。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍可帮助你管理此策略的功能、工具和指南。

修改此设置可能会影响与客户端、服务和应用程序的兼容性。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

此用户权限在默认域控制器组策略对象 (GPO) 以及工作站和服务器的本地安全策略中定义。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

> ⓘ **备注**

可 **在此处**找到有关配置策略的详细信息。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

滥用 **启用计算机和用户帐户信任委派** 用户权限可能会允许未经授权的用户模拟网络上的其他用户。 攻击者可能利用此特权获取对网络资源的访问权限，并难以确定安全事件后发生的情况。

对策

仅当明确需要计算机和用户帐户的功能时，才应分配“ **启用可信任的计算机和用户帐户** ”用户权限。 分配此权限时，应调查约束委派的使用以控制委托帐户可以执行的操作。 默认情况下，在域控制器上，此权限分配给管理员组。

> **注意：** 没有理由将此用户权限分配给属于域的成员服务器和工作站上的任何人，因为它在这些上下文中没有意义。 它仅在域控制器和独立计算机上相关。

潜在影响

无。 未定义 是默认配置。

相关主题

- 用户权限分配

从远程系统强制关机

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **强制从远程系统** 安全策略设置强制关闭的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定允许哪些用户从网络上的远程位置关闭设备。 此设置允许管理员组的成员或特定用户管理计算机 (从远程位置重启) 等任务。

常量：SeRemoteShutdownPrivilege

可能值

- 用户定义的帐户列表
- 管理员

最佳做法

- 将此用户权限显式限制为管理员组的成员或其他需要此功能的已分配角色，例如非管理操作人员。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器上的管理员和服务器操作员，以及独立服务器上的管理员。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 服务器操作员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员 服务器操作员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

必须在正在远程访问的计算机上应用此策略设置。

组策略

此用户权限在默认域控制器组策略对象 (GPO) 以及工作站和服务器的本地安全策略中定义。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

任何可以关闭设备的用户都可能导致出现拒绝服务情况。 因此，应严格限制此用户权限。

对策

将 “**强制关闭”从远程系统** 用户权限限制为“管理员”组的成员或需要此功能的其他已分配角色，例如非管理操作人员。

潜在影响

在域控制器上，如果从“服务器操作员”组中删除 “**强制关闭远程系统** ”用户权限，则可以限制分配给环境中特定管理角色的用户的功能。 确认委托的活动没有受到不利影响。

相关主题

- 用户权限分配

生成安全审核

项目 • 2023/05/25

适用范围

- Windows 11
- Windows 10

介绍 **生成安全审核** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定进程可以使用哪些帐户在安全事件日志中生成审核记录。 本地安全机构子系统服务 (LSASS) 将事件写入日志。 可以使用安全事件日志中的信息来跟踪未经授权的设备访问。

常量：SeAuditPrivilege

可能值

- 用户定义的帐户列表
- 本地服务
- 网络服务

最佳做法

- 由于如果帐户遭到入侵，审核日志可能成为攻击途径，因此请确保只有本地服务和网络服务帐户分配了 “**生成安全审核** ”用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器和独立服务器上的本地服务和网络服务。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	本地服务 网络服务
独立服务器默认设置	本地服务 网络服务
域控制器有效默认设置	本地服务 网络服务
成员服务器有效默认设置	本地服务 网络服务
客户端计算机有效默认设置	本地服务 网络服务

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

滥用此用户权限可能会导致生成许多审核事件、隐藏攻击证据或导致拒绝服务 (DoS) 如果启用了 “审核：无法记录安全审核时立即关闭系统 ”安全策略设置，则 DoS) 。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

恶意用户可能会使用可以写入安全日志的帐户来填充该日志中毫无意义的事件。 如果计算机配置为根据需要覆盖事件，恶意用户可以使用此方法删除其未经授权活动的证据。 如果计算机配置为在无法写入安全日志时关闭，并且计算机未配置为自动备份日志文件，则此方法可用于创建 DoS 条件。

对策

确保只有本地服务和网络服务帐户分配了 “**生成安全审核** ”用户权限。

潜在影响

无。 默认配置是限制对本地服务和网络服务帐户的 “**生成安全审核** ”用户权限。

相关主题

- 用户权限分配

身份验证后模拟客户端

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **身份验证后模拟客户端** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定允许哪些程序模拟用户或其他指定帐户并代表用户进行操作。 如果这种类型的模拟需要此用户权限，则未经授权的用户无法使客户端连接 (例如，通过远程过程调用 (RPC) 或命名管道) 到他们创建的模拟该客户端的服务。 (此类操作可能会将未经授权的用户的权限提升到管理或系统级别。)

模拟是线程在与拥有线程的进程上下文不同的安全上下文中运行的能力。 模拟旨在满足客户端/服务器应用程序的安全要求。 在客户端的安全上下文中运行时，服务在某种程度上"是"客户端。 其中一个服务的线程使用表示客户端凭据的访问令牌来获取对客户端有权访问的对象的访问权限。 模拟的主要原因是导致针对客户端标识执行访问检查。 使用客户端标识进行访问检查可能会导致访问受到限制或扩展，具体取决于客户端有权执行的操作。

由服务控制管理器启动的服务具有默认添加到其访问令牌的内置服务组。 由 COM 基础结构启动并配置为在特定帐户下运行的 COM 服务器也将服务组添加到其访问令牌。 因此，这些进程在启动时会直接分配此用户。

常量：SeImpersonatePrivilege

可能值

- 用户定义的帐户列表
- 默认值
- 未定义

最佳做法

- 如果存在以下任何条件，用户可以模拟访问令牌：
  - 正在模拟的访问令牌适用于此用户。

- 此会话中的用户使用显式凭据登录到网络以创建访问令牌。
- 请求的级别小于“模拟”，例如“匿名”或“标识”。

由于这些因素，用户通常不需要分配此用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器和独立服务器上的管理员、本地服务、网络服务和服务。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	管理员 本地服务 网络服务 服务
独立服务器默认设置	管理员 本地服务 网络服务 服务
域控制器有效默认设置	管理员 本地服务 网络服务 服务
成员服务器有效默认设置	管理员 本地服务 网络服务 服务
客户端计算机有效默认设置	管理员 本地服务 网络服务 服务

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 **身份验证后模拟客户端** 用户权限的攻击者可能会创建服务，误导客户端连接到服务，然后模拟该计算机以提升攻击者对设备的访问权限级别。

对策

在成员服务器上，确保只有管理员和服务组 (本地服务、网络服务和服务组) 在向其分配身份验证用户权限 **后具有模拟客户端** 。

潜在影响

在大多数情况下，此配置没有影响。 如果已安装可选组件（如 ASP.NET 或 IIS），则可能需要在 **身份验证后将模拟客户端** 的用户权限分配给这些组件所需的其他帐户，例如 IUSR_<*ComputerName*>、IIS_WPG、ASP.NET 或 IWAM_<*ComputerName*>。

在 IIS 7.0 及更高版本中， (IUSR) 的内置帐户将替换 IUSR_MachineName 帐户。 此外，名为 IIS_IUSRS 的组将替换IIS_WPG组。 由于 IUSR 帐户是内置帐户，因此 IUSR 帐户不再

需要密码。 IUSR 帐户类似于网络或本地服务帐户。 有关详细信息，请参阅 IIS 7.0 及更高版本的默认权限和用户权限。

相关主题

- 用户权限分配

增加进程工作集

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 “**增加进程工作集** ”安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以增加或减小进程的工作集的大小。 进程的工作集是当前在物理 RAM 中对进程可见的内存页集。 这些页面是常驻的，可供应用程序使用，而不会触发页面错误。 最小和最大工作集大小会影响进程的虚拟内存分页行为。

常量：SeIncreaseWorkingSetPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 应让用户知道，如果用户修改此安全设置，则可能会出现不良性能问题。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，标准用户具有此权限。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	用户
独立服务器默认设置	用户
域控制器有效默认设置	用户
成员服务器有效默认设置	用户
客户端计算机有效默认设置	用户

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

增加进程的工作集大小会减少可供系统其余部分使用的物理内存量。

对策

提高用户对增加进程工作集的影响以及如何识别其系统在更改此设置时受到不利影响的意识。

潜在影响

无。 默认配置允许标准用户增加进程的工作集。

相关主题

- 用户权限分配

提高计划优先级

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **提高计划优先级** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户帐户可以增加进程的基优先级类。 在优先级类中增加相对优先级不是特权操作。 操作系统随附的管理工具不需要此用户权限，但软件开发工具可能需要此权限。

具体而言，此安全设置确定哪些帐户可以使用对另一个进程具有写入属性访问权限的进程，以提高分配给其他进程的运行优先级。 具有此权限的用户可以通过任务管理器用户界面更改进程的计划优先级。

常量：SeIncreaseBasePriorityPrivilege

可能值

- 用户定义的帐户列表
- 未定义
- 管理员

最佳做法

- 保留默认值作为唯一负责控制进程计划优先级的帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

分配有此用户权限的用户可以将进程的计划优先级提高到"实时"，这将为所有其他进程留出很少的处理时间，并可能导致拒绝服务条件。

对策

验证是否只有管理员和窗口管理器组已为其分配了 "**增加计划优先级** "用户权限。

潜在影响

无。 默认配置是将 "**提高计划优先级** 用户权限"限制为"管理员"组和"窗口管理器"组的成员。

> ⚠ **警告**
>
> 如果从"**增加计划优先级**"用户权限中删除"**窗口管理器**"\"**窗口管理器组**"，则某些应用程序和计算机无法正常工作。 特别是，INK 工作区在统一内存体系结构 (UMA) 笔记本电脑和台式计算机上无法正常运行，这些计算机运行Windows 10版本 1903 (或更高版本) 并使用 Intel GFX 驱动程序。

在受影响的计算机上，当用户在 INK 工作区（例如 Microsoft Edge、 Microsoft PowerPoint 或 Microsoft OneNote 使用的工作区）上绘制时，屏幕会闪烁。 发生闪烁的原因是与墨迹书写相关的进程反复尝试使用Real-Time优先级，但权限被拒绝。

相关主题

- 用户权限分配
- 提高Windows Server 2012及更早版本的计划优先级

加载和卸载设备驱动程序

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **加载和卸载设备驱动程序** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以动态加载和卸载设备驱动程序。 如果设备上的 driver.cab 文件中已存在新硬件的已签名驱动程序，则不需要此用户权限。 设备驱动程序作为高特权代码运行。 Windows 支持即插即用规范，这些规范定义计算机如何检测和配置新添加的硬件，然后自动安装设备驱动程序。 在即插即用之前，用户需要在将设备附加到设备之前手动配置设备。 此模型允许用户插入硬件，然后 Windows 搜索相应的设备驱动程序包，并自动将其配置为正常工作，而不会干扰其他设备。

由于设备驱动程序软件就像是操作系统的一部分一样运行，可以不受限制地访问整个计算机，因此，仅允许已知和授权的设备驱动程序至关重要。

常量：SeLoadDriverPrivilege

可能值

- 用户定义的帐户列表
- 默认值
- 未定义

最佳做法

- 由于存在潜在的安全风险，请勿将此用户权限分配给不希望接管系统的任何用户、组或进程。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器上的管理员和打印操作员，以及独立服务器上的管理员。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 打印运算符
独立服务器默认设置	管理员
域控制器有效默认设置	管理员 打印运算符
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

设备驱动程序作为高特权代码运行。 拥有 **加载和卸载设备驱动程序** 用户权限的用户可能会无意中安装伪装成设备驱动程序的恶意软件。 管理员应注意并仅安装具有已验证数字签名的驱动程序。

> **注意：** 必须具有此用户权限或本地管理员组的成员才能安装本地打印机的新驱动程序或管理本地打印机并为双面打印等选项配置默认值。

对策

不要将 “**加载和卸载设备驱动程序** ”用户权限分配给成员服务器上的管理员以外的任何用户或组。 在域控制器上，不要将此用户权限分配给除域管理员以外的任何用户或组。

潜在影响

如果从“打印操作员”组或其他帐户中删除 “**加载和卸载设备驱动程序** ”用户权限，则可以限制分配给环境中特定管理角色的用户的功能。 应确保委托的任务不会受到负面影响。

相关主题

- 用户权限分配

将页锁定在内存

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **锁定内存中页** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些帐户可以使用进程将数据保留在物理内存中，从而防止计算机将数据分页到磁盘上的虚拟内存。

通常，在 Windows 上运行的应用程序可以协商更多的物理内存，为了响应请求，应用程序开始将数据从 RAM（（如数据缓存））移动到磁盘。 将可分页内存移动到磁盘时，更多的 RAM 可用，供操作系统使用。

为应用程序) 的特定帐户 (用户帐户或进程帐户启用此策略设置可防止对数据进行分页。 因此，Windows 在压力下可以回收的内存量受到限制。 此限制可能导致性能下降。

> ⓘ **备注**
>
> 通过配置此策略设置，Windows 操作系统的性能将有所不同，具体取决于应用程序是在 32 位还是 64 位系统上运行，以及它们是否是虚拟化映像。 早期版本和更高版本的 Windows 操作系统的性能也会有所不同。

常量：SeLockMemoryPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

最佳做法取决于平台体系结构和在这些平台上运行的应用程序。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**在内存中锁定页**” 用户权限的用户可以将物理内存分配给多个进程，这可能会为其他进程保留很少或没有 RAM，并导致拒绝服务条件。

对策

不要将 “**锁定内存页**” 用户权限分配给任何帐户。

潜在影响

无。 未定义 是默认配置。

相关主题

- 用户权限分配

作为批处理作业登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文介绍作为 **批处理作业安全** 策略设置登录的建议做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些帐户可以使用批处理队列工具（如任务计划程序服务）登录。 使用“添加计划任务向导”计划以特定用户名和密码运行的任务时，会自动为该用户分配“ **以批处理作业身份登录** ”用户权限。 当计划时间到达时，任务计划程序服务将用户作为批处理作业（而不是交互式用户）登录，并且任务在用户的安全上下文中运行。

常量：SeBatchLogonRight

可能值

- 用户定义的帐户列表
- 默认值
- 未定义

最佳做法

- 出于安全原因，将此权限分配给特定用户时，请使用自由裁量权。 在大多数情况下，默认设置已足够。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置适用于域控制器和独立服务器上的管理员、备份操作员和性能日志用户。

下表列出了实际和有效的默认策略值。 默认值也会在策略的属性页上列出。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 备份运算符 性能日志用户
独立服务器默认设置	管理员 备份运算符 性能日志用户
域控制器有效默认设置	管理员 备份运算符 性能日志用户
成员服务器有效默认设置	管理员 备份运算符 性能日志用户
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

当用户计划任务时，任务计划程序会自动授予此权限。 若要替代此行为，请使用 “拒绝登录”作为批处理作业 “用户权限分配”设置。

组策略设置按以下顺序应用，这将在下一组策略更新时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置。 它介绍了如何应用对策以及对策的可能消极后果。

漏洞

以 **批处理作业用户身份登录** 权限存在一个低风险漏洞，允许非管理员执行类似于管理员的功能。 如果未相应地评估、理解和限制，攻击者可以轻松利用此潜在攻击途径来破坏系统、凭据和数据。 对于大多数组织，默认设置就足够了。 默认情况下，本地管理员组的成员具有此权限。

对策

如果希望允许为特定用户帐户运行计划任务，则允许计算机自动管理此用户权限。 如果不想以这种方式使用任务计划程序，请仅为本地服务帐户配置 “**以批处理作业用户身份登录** ”。

对于 IIS 服务器，请在本地配置此策略，而不是通过基于域的组策略设置，以便可以确保本地 IUSR_<*ComputerName*> 和 IWAM_<*ComputerName*> 帐户具有此用户权限。

潜在影响

如果使用基于域的组策略设置配置“**作为批处理作业登录**”设置，则计算机无法将用户权限分配给任务计划程序中用于计划作业的帐户。 如果安装可选组件（如 ASP.NET 或 IIS），则可能需要将此用户权限分配给这些组件所需的其他帐户。 例如，IIS 要求将此用户权限分配给 IIS_WPG 组以及 IUSR_<*ComputerName*>、ASPNET 和 IWAM_<*ComputerName*> 帐户。 如果此用户权限未分配给此组和这些帐户，则 IIS 无法运行某些正常运行所需的 COM 对象。

相关主题

- 用户权限分配

作为服务登录

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

本文介绍“ **作为服务登录**” 安全策略设置的建议做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些服务帐户可以将进程注册为服务。 在服务帐户下运行进程可以避免人工干预。

常量：SeServiceLogonRight

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 尽量减少授予此用户权限的帐户数。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器上的“网络服务”和“独立服务器上的网络服务”。

下表列出了实际和有效的默认策略值。 策略的属性页还列出了默认值。

服务器类型或 GPO	默认值
默认域策略	未定义

服务器类型或 GPO	默认值
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	网络服务
成员服务器有效默认设置	网络服务
客户端计算机有效默认设置	网络服务

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

如果用户帐户受这两个策略的约束，则 **策略设置**“**拒绝作为服务登录** ”将取代此策略设置。

组策略设置按以下顺序应用，这将在下一组策略更新时覆盖本地设备上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

安全注意事项

本部分介绍攻击者如何利用某个功能或其配置。 它解释了对策。 它解决了对策的可能消极后果。

漏洞

“ **以服务身份登录**” 用户权限允许帐户启动计算机中连续运行的网络服务或服务，即使没有人登录控制台也是如此。 风险降低，因为只有具有管理权限的用户才能安装和配置服务。 已达到该访问权限级别的攻击者可以将服务配置为使用本地系统帐户运行。

对策

根据定义，网络服务帐户具有 “**以服务身份登录**” 用户权限。 此权限不是通过组策略设置授予的。 尽量减少授予此用户权限的其他帐户的数量。

潜在影响

在大多数计算机上，默认情况下， “**以服务身份登录** ”用户权限仅限于本地系统、本地服务和网络服务内置帐户，并且没有负面影响。 但是，如果你有可选组件（如 ASP.NET 或 IIS），则可能需要将用户权限分配给这些组件所需的其他帐户。 IIS 要求向 ASPNET 用户帐户显式授予此用户权限。

相关主题

- 用户权限分配

管理审核和安全日志

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍管理审核和安全日志安全策略设置的最佳做法、位置、值 、**策略管理和** 安全注意事项。

参考

此策略设置确定哪些用户可以为单个资源（例如文件、Active Directory 对象和注册表项）指定对象访问审核选项。 这些对象 (SACL) 指定其系统访问控制列表。 分配有此用户权限的用户还可以查看和清除安全登录事件查看器。 有关对象访问审核策略的详细信息，请参阅 审核对象访问。

常量：SeSecurityPrivilege

可能值

- 用户定义的帐户列表
- 管理员
- 未定义

最佳做法

1. 从组中删除此权限之前，请调查应用程序是否依赖于此权限。
2. 通常，不需要将此用户权限分配给管理员以外的组。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置是域控制器和独立服务器上的管理员。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

除非使用本地组策略编辑器、组策略管理控制台 (GPMC) 或 Auditpol 命令行工具启用它们，否则不会对对象访问执行审核。

有关对象访问审核策略的详细信息，请参阅 审核对象访问。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**管理审核和安全日志** ”用户权限的任何人都可以清除安全日志，以清除未授权活动的重要证据。

对策

确保只有本地管理员组具有 “**管理审核和安全日志** ”用户权限。

潜在影响

默认配置是将 **管理审核和安全日志** 用户权限限制为本地管理员组。

> **警告：** 如果已向本地管理员组以外的组分配此用户权限，则删除此用户权限可能会导致其他应用程序出现性能问题。 从组中删除此权限之前，请调查应用程序是否依赖于此权限。

相关主题

- 用户权限分配

修改对象标签

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **修改对象标签** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此权限确定哪些用户帐户可以修改对象（例如文件、注册表项或其他用户拥有的进程）的完整性标签。 在用户帐户下运行的进程可以将该用户拥有的对象的标签修改为没有此权限的较低级别。

完整性标签由 Windows Server 2008 和 Windows Vista 中引入的 Windows 完整性控件 (WIC) 功能使用。 WIC 通过将六个可能标签中的一个分配给系统上的对象来防止低完整性进程修改较高完整性的进程。 尽管 WIC 完整性级别类似于 NTFS 文件和文件夹权限（它们是对对象的自由裁量控制），但 WIC 完整性级别是由操作系统实施和强制实施的强制控制。 以下列表描述了从最低到最高的完整性级别：

- **可信** 匿名登录的进程的默认分配。
- **低** 与 Internet 交互的进程的默认分配。
- **中** 标准用户帐户和任何未显式指定为较低或更高完整性级别的对象的默认分配。
- **高** 请求使用管理权限运行的管理员帐户和进程的默认分配。
- **系统** Windows 内核和核心服务的默认分配。
- **安装** 由安装程序用于安装软件。 计算机上仅安装受信任的软件非常重要，因为分配有安装程序完整性级别的对象可以安装、修改和卸载所有其他对象。

常量：SeRelabelPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 不要授予任何组此用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置在域控制器和独立服务器上未定义。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	未定义
成员服务器有效默认设置	未定义
客户端计算机有效默认设置	未定义

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**修改对象标签** ”用户权限的任何人都可以更改文件或进程的完整性级别，使其提升或降低到可由较低完整性进程删除的地步。 这两种状态之一有效地绕过了 Windows 完整性控件提供的保护，使系统容易受到恶意软件的攻击。

如果恶意软件设置为提升的完整性级别（如受信任的安装程序或系统），则管理员帐户没有足够的完整性级别从系统中删除程序。 在这种情况下，强制使用 “**修改对象标签** ”权限，以便可以重新标记对象。 但是，重新标记必须通过使用与尝试重新标记的对象相同或更高级别完整性的进程进行。

对策

不要授予任何组此权限。 如有必要，请在受约束的时间段内对受信任的个人实施它，以响应特定的组织需求。

潜在影响

无。 未定义 是默认配置。

相关主题

- 用户权限分配

修改固件环境值

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **修改固件环境值** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定谁可以修改固件环境值。 固件环境值是存储在非基于 x86 的计算机的非易失性 RAM 中的设置。 设置的效果取决于处理器。

在基于 x86 的计算机上，唯一可以通过分配此用户权限修改的固件环境值是 “**上次已知良好配置**” 设置，它只能由系统修改。

在基于 Itanium 的计算机上，启动信息存储在非易失性 RAM 中。 必须向用户分配此用户权限，才能运行bootcfg.exe，并使用“**系统属性**”的“**高级**”选项卡上的“**启动和恢复**”功能更改**默认操作系统**设置。

固件环境值的确切设置由启动固件确定。 这些值的位置也由固件指定。 例如，在基于 UEFI 的系统上，NVRAM 包含指定系统启动设置的固件环境值。

在所有计算机上，安装或升级 Windows 都需要此用户权限。

常量：SeSystemEnvironmentPrivilege

可能值

- 用户定义的帐户列表
- 管理员
- 未定义

最佳做法

- 确保仅为本地管理员组分配了 “**修改固件环境值** ”用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置是域控制器和独立服务器上的管理员。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

此安全设置不会影响谁可以修改系统环境值和用户环境值，这些值显示在“**系统属性**”的“**高级**”选项卡上。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

分配了“**修改固件环境值**”用户权限的任何人都可以配置硬件组件的设置，使其失败，这可能导致数据损坏或拒绝服务条件。

对策

确保仅为本地管理员组分配了“**修改固件环境值**”用户权限。

潜在影响

从 **修改固件环境值** 用户权限中删除本地管理员组可能会导致 BitLocker 驱动器加密功能无法操作。

相关主题

- 用户权限分配

执行批量维护任务

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **执行卷维护任务** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以执行卷或磁盘管理任务，例如对现有卷进行碎片整理、创建或删除卷以及运行磁盘清理工具。

分配此用户权限时请谨慎。 具有此用户权限的用户可以浏览磁盘，并将中的文件扩展到包含其他数据的内存。 打开扩展文件后，用户可能能够读取和修改获取的数据。

常量：SeManageVolumePrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 确保仅为本地管理员组分配了 “**执行卷维护任务** ”用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置是域控制器和独立服务器上的管理员。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
DC 有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

分配有 “**执行卷维护任务**” 用户权限的用户可以删除卷，这可能导致数据丢失或拒绝服务条件。 此外，磁盘维护任务还可用于修改磁盘上的数据，例如可能导致特权提升的用户权限分配。

对策

确保仅为本地管理员组分配了 “**执行卷维护任务** ”用户权限。

潜在影响

无。 默认配置是将 “**执行卷维护任务**” 用户权限限制为本地 Administrators 组。

相关主题

- 用户权限分配

配置文件单个进程

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **配置文件单进程** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以查看应用程序进程的示例性能。 通常，你不需要此用户权限来使用操作系统中包含的性能报告工具。 但是，如果将系统的监视器组件配置为通过 Windows Management Instrumentation (WMI) 收集数据，则需要此用户权限。

常量：SeProfileSingleProcessPrivilege

可能值

- 用户定义的帐户列表
- 管理员
- 未定义

最佳做法

- 不应向单个用户授予此权限。 应仅针对监视其他程序的受信任应用程序授予该权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置是域控制器和独立服务器上的管理员。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值

服务器类型或组策略对象 (GPO)	默认值
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置按以下顺序通过 组策略 对象应用，这将在下一组策略更新时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

配置文件单进程用户权限存在一个中等漏洞。 具有此用户权限的攻击者可以监视计算机的性能，以帮助识别他们可能想要直接攻击的关键进程。 攻击者可以确定计算机上运行

的进程，以便确定可能需要避免的对策，例如防病毒软件或入侵检测系统。 它们还可以标识登录到计算机的其他用户。

对策

确保仅为本地管理员组分配“ **配置文件单进程**” 用户权限。

潜在影响

如果从 Power Users 组或其他帐户中删除 **配置文件单进程** 用户权限，则可以限制分配给环境中特定管理角色的用户的能力。 应确保委托的任务不会受到负面影响。

相关主题

- 用户权限分配

配置文件系统性能

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

此安全策略参考主题面向 IT 专业人员，介绍了 **配置文件系统性能** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定哪些用户可以使用 Windows 性能监视工具来监视系统进程的性能。

常量：SeSystemProfilePrivilege

可能值

- 用户定义的帐户列表
- 管理员
- 未定义

最佳做法

- 确保仅为本地管理员组分配 **配置文件系统性能** 用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器和独立服务器上的管理员和 NT SERVICE\WdiServiceHost。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

根据你的 Windows 版本和环境，如果你在使用管理员帐户时遇到访问错误，则可能需要将此用户权限添加到本地系统帐户或本地服务帐户。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

配置文件系统性能用户权限构成中度漏洞。 具有此用户权限的攻击者可以监视计算机的性能，以帮助识别他们可能想要直接攻击的关键进程。 攻击者还可以确定计算机上处于活动状态的进程，以便确定要避免的对策，例如防病毒软件或入侵检测系统。

对策

确保仅为本地管理员组分配 **配置文件系统性能** 用户权限。

潜在影响

无。 默认配置是将 **配置文件系统性能** 用户权限限制为本地管理员组。

相关主题

- 用户权限分配

从扩展坞中删除计算机 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **从扩展坞中删除计算机** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定用户是否可以在不登录的情况下从其扩展坞取消停靠便携式设备。 此策略设置仅影响涉及便携式计算机及其扩展坞的方案。

如果将此用户权限分配给 (的帐户，或者如果用户是) 分配的组的成员，则用户必须先登录，然后才能从其扩展坞中删除便携式设备。 否则，作为安全措施，从扩展坞中删除设备后，用户将无法登录。 如果未分配此策略，则用户可以在不登录的情况下从其扩展坞中删除便携式设备，然后能够在未连接状态下启动并登录到设备。

常量：SeUndockPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 仅将此用户权限分配给允许使用便携式设备的帐户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

尽管此可移植设备方案通常不适用于服务器，但默认情况下，此设置是域控制器和独立服务器上的管理员。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**从扩展坞中删除计算机** ”用户权限的任何人都可以登录，然后从扩展坞中删除便携式设备。 如果未定义此设置，则其效果与向所有人授予此权限的效果相同。 但是，实施此对策的价值会因以下因素而降低：

- 如果攻击者可以重启设备，他们可以在 BIOS 启动后、操作系统启动之前将其从扩展坞中删除。
- 此设置不会影响服务器，因为它们通常未安装在扩展坞中。
- 攻击者可能同时窃取设备和扩展坞。
- 用户可以物理删除可机械取消停靠的设备，无论他们是否使用 Windows 取消停靠功能。

对策

确保仅为本地管理员组和设备分配的用户帐户分配了 “**从扩展坞中删除计算机** ”用户权限。

潜在影响

默认情况下，仅向本地管理员组的成员授予此权限。 必须根据需要显式授予其他用户帐户此用户权限。 如果组织的用户不是其便携式设备上的本地管理员组的成员，则如果他们不首先关闭设备，则无法从扩展坞中删除其便携式设备。 因此，你可能希望将 “**从扩展坞中删除计算机**” 权限分配给可移植设备的本地用户组。

相关主题

- 用户权限分配

替换进程级令牌

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **替换进程级令牌** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些父进程可以替换与子进程关联的访问令牌。

具体而言，“**替换进程级令牌** ”设置确定哪些用户帐户可以调用 CreateProcessAsUser () 应用程序编程接口 (API) 以便一个服务可以启动另一个服务。 使用此用户权限的进程的示例是任务计划程序，其中用户权限扩展到可由任务计划程序管理的任何进程。

访问令牌是描述进程或线程的安全上下文的对象。 令牌中的信息包括与进程或线程关联的用户帐户的标识和特权。 使用此用户权限时，代表此用户帐户运行的每个子进程都将将其访问令牌替换为进程级令牌。

常量：SeAssignPrimaryTokenPrivilege

可能值

- 用户定义的帐户列表
- 违约
- 未定义

最佳做法

- 对于成员服务器，请确保只有本地服务和网络服务帐户具有 “**替换进程级令牌** ”用户权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置为域控制器和独立服务器上的网络服务和本地服务。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	网络服务 本地服务
独立服务器默认设置	网络服务 本地服务
域控制器有效默认设置	网络服务 本地服务
成员服务器有效默认设置	网络服务 本地服务
客户端计算机有效默认设置	网络服务 本地服务

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**替换进程级令牌** ”权限的用户如果知道用户的凭据，则可以以其他用户身份启动进程。

对策

对于成员服务器，请确保只有本地服务和网络服务帐户具有 “**替换进程级令牌** ”用户权限。

潜在影响

在大多数计算机上，将 **替换进程级令牌** 用户权限限制为本地服务和网络服务内置帐户是默认配置，并且不会造成负面影响。 但是，如果已安装可选组件（如 ASP.NET 或 IIS），则可能需要将 “**替换进程级令牌** ”用户权限分配给其他帐户。 例如，IIS 要求向 Service、Network Service 和 IWAM_<*ComputerName*> 帐户显式授予此用户权限。

相关主题

- 用户权限分配

还原文件和目录 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **还原文件和目录** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定哪些用户在还原备份的文件和目录时可以绕过文件、目录、注册表和其他永久性对象权限，并确定哪些用户可以将有效的安全主体设置为对象的所有者。

向此用户授予对帐户的权限类似于向该帐户授予对系统上所有文件和文件夹的以下权限：

- **遍历文件夹/执行文件**
- **写**

常量：SeRestorePrivilege

可能值

- 用户定义的帐户列表
- 违约
- 未定义

最佳做法

- 具有此用户权限的用户可以覆盖注册表设置、隐藏数据并获取系统对象的所有权，因此仅将此用户权限分配给受信任的用户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此权限授予域控制器上的管理员、备份操作员和服务器操作员组，以及独立服务器上的管理员和备份操作员组。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或组策略对象 (GPO)	默认值
默认域策略	
默认域控制器策略	管理员 备份运算符 服务器操作员
独立服务器默认设置	管理员 备份运算符
域控制器有效默认设置	管理员 备份运算符 服务器操作员
成员服务器有效默认设置	管理员 备份运算符
客户端计算机有效默认设置	管理员 备份运算符

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置按以下顺序通过 组策略 对象应用，这将在下一组策略更新时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 “**还原文件和目录**” 用户权限的攻击者可以将敏感数据还原到计算机并覆盖较新的数据，这可能导致重要数据丢失、数据损坏或拒绝服务条件。 攻击者可能会使用包含恶意软件的版本覆盖合法管理员或系统服务使用的可执行文件，以授予自己提升的权限、泄露数据或安装提供设备持续访问权限的程序

> **注意：** 即使配置了以下对策，攻击者也可以将数据还原到由攻击者控制的域中的计算机。 因此，组织必须仔细保护用于备份数据的媒体。

对策

确保仅向本地管理员组分配 “**还原文件和目录**” 用户权限，除非组织已明确定义备份和还原人员的角色。

潜在影响

如果从“备份操作员”组和其他帐户中删除 “**还原文件和目录** ”用户权限，则不是本地管理员组成员的用户无法加载数据备份。 如果将还原备份委托给组织中的一部分 IT 员工，则应验证此更改不会对组织人员完成其工作的能力产生负面影响。

相关主题

- 用户权限分配

关闭系统 - 安全策略设置

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **关闭系统** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此安全设置确定在本地登录到设备的用户是否可以关闭 Windows。

关闭域控制器会使域控制器无法执行处理登录请求、处理组策略设置以及响应轻型目录访问协议 (LDAP) 查询等操作。 关闭已分配有操作主机角色（也称为灵活的单一主机操作或 FSMO 角色）的域控制器可以禁用关键域功能。 例如，处理新密码的登录请求，这些请求由主域控制器 (PDC) 模拟器主机完成。

需要 “**关闭系统** 用户”权限才能启用休眠支持、设置电源管理设置以及取消关机。

常量：SeShutdownPrivilege

可能值

- 用户定义的帐户列表
- 违约
- 未定义

最佳做法

1. 确保只有管理员和备份操作员在成员服务器上具有 “**关闭系统** ”用户权限。 只有管理员才对域控制器拥有用户权限。 删除这些默认组可能会限制分配给环境中特定管理角色的用户的能力。 确保其委托的任务不会受到负面影响。
2. 关闭域控制器的功能应限制为少数受信任的管理员。 即使系统关闭需要能够登录到服务器，也应注意允许关闭域控制器的帐户和组。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置是域控制器上的管理员、备份操作员、服务器操作员和打印操作员，以及独立服务器上的管理员和备份操作员。

下表列出了最新受支持的 Windows 版本的实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	管理员 备份运算符 服务器操作员 打印运算符
独立服务器默认设置	管理员 备份运算符
域控制器有效默认设置	管理员 备份运算符 服务器操作员 打印运算符
成员服务器有效默认设置	管理员 备份运算符
客户端计算机有效默认设置	管理员 备份运算符 用户

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启计算机即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

此用户权限与 **从远程系统强制关闭**的效果不同。 有关详细信息，请参阅 强制从远程系统关闭。

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

关闭域控制器的功能应限制为少数受信任的管理员。 尽管 "**关闭系统** 用户"权限需要能够登录到服务器，但应注意允许关闭域控制器的帐户和组。

域控制器关闭后，它无法处理登录请求、处理组策略设置，以及响应轻型目录访问协议 (LDAP) 查询。 如果关闭具有操作主机角色的域控制器，则可以禁用关键域功能，例如处理由 PDC 主服务器执行的新密码的登录请求。

对于其他服务器角色，尤其是非管理员有权登录到服务器的角色（例如 RD 会话主机服务器），必须从没有合法理由重启服务器的用户中删除此用户权限。

对策

确保仅为管理员和备份操作员组分配了"关闭成员服务器上的 **系统** 用户"权限。 并确保仅向 Administrators 组分配域控制器上的用户权限。

潜在影响

从 "**关闭系统** "用户权限中删除这些默认组的影响可能会限制环境中分配的角色的委派能力。 确认委托的活动没有受到不利影响。

相关文章

- 用户权限分配

同步目录服务数据

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍 **同步目录服务数据** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户和组有权同步所有目录服务数据，而不管对象和属性的保护如何。 使用 ldap 目录同步 (dirsync) 服务时需要此权限。 域控制器本身具有此用户权限，因为同步过程在域控制器上的 **系统** 帐户上下文中运行。

常量：SeSyncAgentPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 确保未为帐户分配 **同步目录服务数据** 用户权限。 只有域控制器需要此特权，它们本身就具有此权限。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，不会在域控制器和独立服务器上定义此设置。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	默认值

服务器类型或 GPO	默认值
默认域策略	未定义
默认域控制器策略	未定义
独立服务器默认设置	未定义
域控制器有效默认设置	启用
成员服务器有效默认设置	禁用
客户端计算机有效默认设置	禁用

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置
3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

同步目录服务数据用户权限会影响域控制器，（只有域控制器才能）同步目录服务数据。域控制器本身具有此用户权限，因为同步过程在域控制器上的 **系统** 帐户上下文中运行。

具有此用户权限的攻击者可以查看目录中存储的所有信息。 然后，他们可以使用其中一些信息来促进更多攻击或公开敏感数据，例如直接电话号码或物理地址。

对策

确保未为帐户分配 **同步目录服务数据** 用户权限。

潜在影响

无。 未定义 是默认配置。

相关主题

- 用户权限分配

取得文件或其他对象的所有权

项目 • 2023/03/18

适用范围

- Windows 11
- Windows 10

介绍获取 **文件或其他对象的所有权** 安全策略设置的最佳做法、位置、值、策略管理和安全注意事项。

参考

此策略设置确定哪些用户可以获取设备中任何安全对象的所有权，包括 Active Directory 对象、NTFS 文件和文件夹、打印机、注册表项、服务、进程和线程。

每个对象都有一个所有者，无论对象是驻留在 NTFS 卷还是 Active Directory 数据库中。 所有者控制如何对 对象设置权限以及向谁授予权限。

默认情况下，所有者是创建对象的人员或进程。 所有者始终可以更改对对象的权限，即使他们被拒绝对对象的所有访问也是如此。

常量：SeTakeOwnershipPrivilege

可能值

- 用户定义的帐户列表
- 未定义

最佳做法

- 分配此用户权限可能会面临安全风险。 由于对象的所有者拥有对它们的完全控制，因此仅将此用户权限分配给受信任的用户。

位置

计算机配置\Windows 设置\安全设置\本地策略\用户权限分配

默认值

默认情况下，此设置是域控制器和独立服务器上的管理员。

下表列出了实际和有效的默认策略值。 默认值也列在策略的属性页上。

服务器类型或 GPO	**默认值**
默认域策略	未定义
默认域控制器策略	管理员
独立服务器默认设置	管理员
域控制器有效默认设置	管理员
成员服务器有效默认设置	管理员
客户端计算机有效默认设置	管理员

策略管理

本部分介绍有助于管理此策略的功能、工具和指南。

无需重启设备即可使此策略设置生效。

帐户所有者下次登录时，对帐户的用户权限分配所做的任何更改将生效。

所有权可以通过以下方式获取：

- 管理员。 默认情况下，管理员组被授予 “**获取文件或其他对象的所有权** ”用户权限。
- 对对象拥有 “**获取所有权** ”用户权限的任何人或任何组。
- 具有 “**还原文件和目录**” 用户权限的用户。

可以通过以下方式转移所有权：

- 如果其他用户是当前所有者访问令牌中定义的组的成员，则当前所有者可以向其他用户授予“ **获取所有权** ”用户权限。 用户必须拥有所有权才能完成转移。
- 管理员可以获取所有权。
- 拥有 “**还原文件和目录**” 用户权限的用户可以双击“ **其他用户和组** ”，然后选择要向其分配所有权的任何用户或组。

组策略

设置通过组策略对象 (GPO) 按以下顺序应用，这将在下一次更新组策略时覆盖本地计算机上的设置：

1. 本地策略设置
2. 网站策略设置

3. 域策略设置
4. OU 策略设置

当本地设置灰显时，它指示 GPO 当前控制该设置。

安全注意事项

本部分介绍攻击者如何利用一项功能或其配置，如何实施对策，以及对策实施可能产生的负面后果。

漏洞

具有 **获取文件或其他对象的所有权用户权限的任何用户** 都可以控制任何对象，而不管该对象的权限如何，然后对其进行任何更改。 此类更改可能会导致数据泄露、数据损坏或拒绝服务条件。

对策

确保只有本地管理员组具有 **获取文件或其他对象的所有权** 用户权限。

潜在影响

无。 默认配置是将 “**获取文件或其他对象的所有权** ”用户权限限制为本地管理员组。

相关主题

- 用户权限分配

Windows 安全中心

以零信任原则为核心，可保护数据并随时随地访问，从而使你受到保护、高效工作。

零信任和 Windows

概述

概述

硬件安全性

概述

概述

概念

受信任的平台模块

Windows Defender System Guard 固件保护

System Guard 安全启动和 SMM 保护支持

基于虚拟化的代码完整性保护

内核 DMA 保护

操作系统安全性

概述

概述

概念

受信任启动

加密和数据保护

Windows 安全基线

虚拟专用网络指南

Windows Defender 防火墙

病毒和威胁防护

应用程序安全性

概述

概述

概念

应用程序控制和基于虚拟化的保护

应用程序控制

应用程序防护

Windows 沙盒

Microsoft Defender SmartScreen

适用于 Windows 的 S/MIME

用户安全性和安全标识

概述

概述

概念

Windows Hello 企业版

Windows 10 凭据盗窃缓解

保护域凭据

Windows Defender Credential Guard

丢失或忘记的密码

访问控制

智能卡

云服务

概念

移动设备管理

Azure Active Directory

你的 Microsoft 帐户

OneDrive

家庭安全

安全基础

概述

概述

参考

Microsoft 安全开发生命周期

Microsoft Bug Bounty

通用标准认证

美国联邦信息处理标准 (FIPS) 140 验证

隐私控制

参考

Windows 和隐私合规性