SSH

Cyberworld

从使用SSH密钥迁移到无密钥的即时访问降低编排工具访问风险

SSH零信任解决方案

目录

引言

在当今典型的企业环境中，手动执行日常任务会消耗时间和金钱，还容易出错。拥有大型环境的企业通常使用自动化编排工具（例如 Ansible、Puppet 和 BMC TrueSight）来简化软件配置、配置管理和应用程序部署。

编排工具虽然有助于简化大型环境中的任务，但是会使环境复杂化，因为它们使用 SSH 密钥作为访问凭据。

在本文档中，我们会分析编排工具的固有风险，以及如何通过从使用SSH密钥迁移到无密钥的即时访问来解决这些风险。

编排工具通常使用 SSH 密钥来访问目标

编排工具利用控制节点来管理日常任务。控制节点管理目标清单节点，以便自动执行标准任务，例如配置调配新系统、部署软件和管理更新。

为了确保所使用的通信通道的安全性并验证变更请求的真实性，编排工具使用SSH密钥作为访问凭据。在大型环境中，这相当于每次加入新目标时都需要配置SSH密钥，配置的SSH密钥还需要定期轮换。定期轮换数千个密钥方能满足监管要求。

然而，SSH密钥依赖于公钥加密技术，这是比密码更安全的访问凭据，但也存在重大的固有风险。例如：

- SSH 密钥提供轻松的横向移动和特权提升。
- SSH 密钥可以轻松复制。
- SSH 密钥永不过期且无法集中撤销。

随着时间的推移，在大型环境中管理SSH密钥会成为一种负担，因为管理数千个甚至数百万个SSH密钥会非常耗时且占用大量资源。

通过迁移到无密钥的即时短暂访问来降低SSH密钥的风险

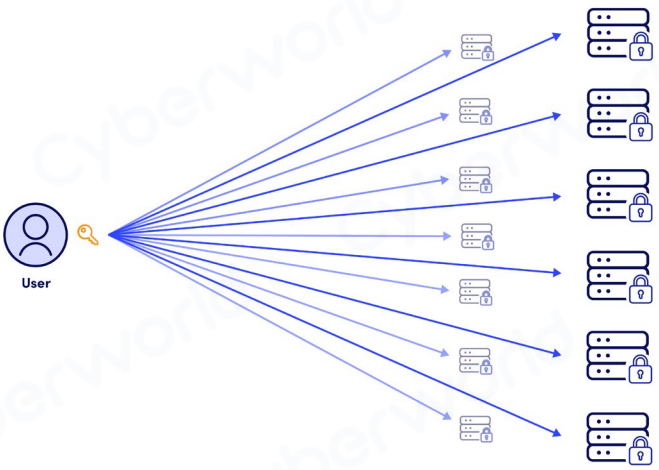
针对上述风险和挑战都有一个解决方案——**从使用SSH密钥迁移到使用由临时、短期证书支持的无密钥即时访问。**

SSH零信任解决方案是一个全面的管理机密和访问的平台，为自动化工具已在使用的现有访问凭据和新访问提供迁移路径。所有这些都按照大型 IT 环境所要求的效率完成。

您可以使用短期证书，而不是使用SSH密钥作为自动化工具（例如Ansible）的默认访问凭据。下面是使用 Ansible 的传统访问和现代无密钥访问的示例比较。

传统 Ansible 访问

在默认情况下，Ansible 使用 SSH 密钥来实现对所管理节点的访问。这些凭据的分发和配置必须在 Ansible 运行之前完成。



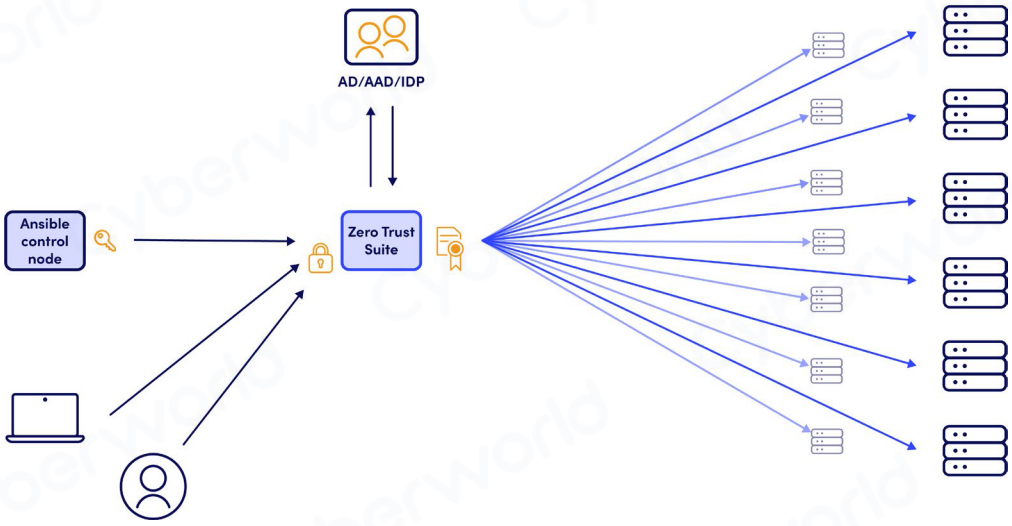
借助Ansible等编排工具提供的SSH密钥，用户可以访问数千台服务器。

现代无密钥访问

SSH密钥依赖于公钥加密技术，与密码等其他常设凭据相比，它们在安全性方面更胜一筹。易用性也是SSH密钥如此广泛使用的原因之一。然而，这种广泛的使用也加剧了SSH密钥的固有风险，并增加了维护需求。

代替SSH密钥，可行的解决方案是将密钥替换为短期证书，在需要时生成，可即时访问。与 SSH 密钥相比：

- **证书身份验证不需要在目标节点上配置访问凭据。**
- **只有在验证请求访问的用户身份后，才会授予访问权限。**
- **生成的访问授予证书有效期为几分钟，如果凭据被导出并随后被泄露，该证书就无法使用。**



利用 SSH 零信任套件进行无密钥访问。
Ansible 等编排工具使用 SSH 密钥连接到零信任套件。
用户（人和机器）也连接到零信任套件，该套件通过与 AD/AAD/IDP 集成来验证其角色。
零信任套件利用短期证书连接到数千台服务器。

从使用SSH密钥到短期证书的迁移过程被设计为完全自动化，并且对于使用SSH访问的最终用户或应用程序来说是透明的。自动化旨在发现和创建使用SSH密钥访问的清单，并识别SSH密钥及其信任关系。它会自动执行任何必要的配置，以促进从长期访问凭据迁移到使用短期证书。在单一管理平台下，一切都清晰可见。此过程的透明度保证无需修改现有基础架构、脚本或集成。

为什么要使用 SSH 零信任套件进行无密钥访问?

1. 通过基于角色的访问控制 (RBAC) 降低 SSH 访问风险	
传统访问	无密钥访问
使用SSH客户端或服务器应用程序访问节点不提供应用RBAC的能力。拥有访问凭据的任何人都可以使用它们，直到凭据被明确轮换或删除。	借助零信任套件，企业可以根据选择的单点事实(SPOT)自动应用访问规则，例如AD或首选身份提供商。 零信任套件会立即调整高度动态环境中的加入者、离开者、移动者流程，并在参数不满足时结束正在进行的连接。
2. 通过消除目标上的密码和密钥管理需求，显著降低配置开销，支持不可变架构范例	
传统访问	无密钥访问
机器对机器的SSH访问通常使用长期凭据，例如SSH密钥和密码，以满足自动化、配置和监察等需求。 新的访问凭据需要在目标节点上显式配置，并且可能有数十万个，特别是在授予自动化工具访问权限的情况下。	零信任套件默认使用短期证书，无需在目标服务器上配置和随后轮换SSH密钥或密码。 短期证书访问背后的技术本质上促进了不可变架构范例。此访问仅需要对目标节点进行初始配置（可以在部署期间执行），以便与选择作为凭据颁发者的证书颁发机构建立信任。
3. 使用即时凭据降低未经授权的访问风险	
传统访问	无密钥访问
使用常设凭据进行SSH访问的传统风险缓解涉及这些凭据的定期轮换，通常跨越整个资产。	零信任套件完全消除了长期凭据，从而降低了与SSH密钥和密码泄露相关的风险。
4. 完全控制所有 SSH 访问	
传统访问	无密钥访问
通常，企业控制的唯一SSH访问是交互式访问。然而，大约80%的SSH连接发生在机器之间，例如自动化和监察。	借助零信任套件，可以实现受控访问关闭并避免常见的安全问题，例如PAM旁路。

此外，SSH连接旨在提供的安全性与总体隐私相结合。 虽然需要安全性和隐私性，但它们也为对手提供了在传统监察技术不透明的节点上执行操作的掩护。数据泄露、建立连接持久性或未经授权的修改就会变得微不足道且难以检测。

仅此一点就增加了企业的风险暴露。

零信任套件提供对SSH连接发起的活动的透明视图。它提供了全面审核和监察连接、应用白名单规则以及记录整个会话的能力。

它还可以应用操作窗口和审批流程，利用四眼原则，甚至按需终止正在进行的连接。