



部署后配置**SolidFire**系统选项 Element Software

NetApp
November 12, 2025

目录

- 部署后配置SolidFire系统选项 1
 - 部署后配置SolidFire系统选项 1
 - 查找更多信息 1
 - 更改NetApp HCI和NetApp SolidFire中的凭据 1
 - 查找更多信息 4
 - 更改 Element 软件的默认 SSL 证书 4
 - 查找更多信息 5
 - 更改节点的默认 IPMI 密码 5
 - 更改 H410S 节点的默认 IPMI 密码 5
 - 更改 H610S 节点的默认 IPMI 密码 6
 - 查找更多信息 6

部署后配置SolidFire系统选项

部署后配置SolidFire系统选项

设置好SolidFire系统后，您可能需要执行一些可选任务。

如果您更改了系统中的凭据，您可能需要了解这对其他组件的影响。

此外，您还可以配置多因素身份验证、外部密钥管理和联邦信息处理标准 (FIPS) 安全性的设置。您还应该在必要时更新密码。

查找更多信息

- ["更改NetApp HCI和NetApp SolidFire中的凭据"](#)
- ["更改 Element 软件的默认 SSL 证书"](#)
- ["更改节点的 IPMI 密码"](#)
- ["启用多重身份验证"](#)
- ["开始使用外部密钥管理"](#)
- ["创建支持 FIPS 驱动器的集群"](#)

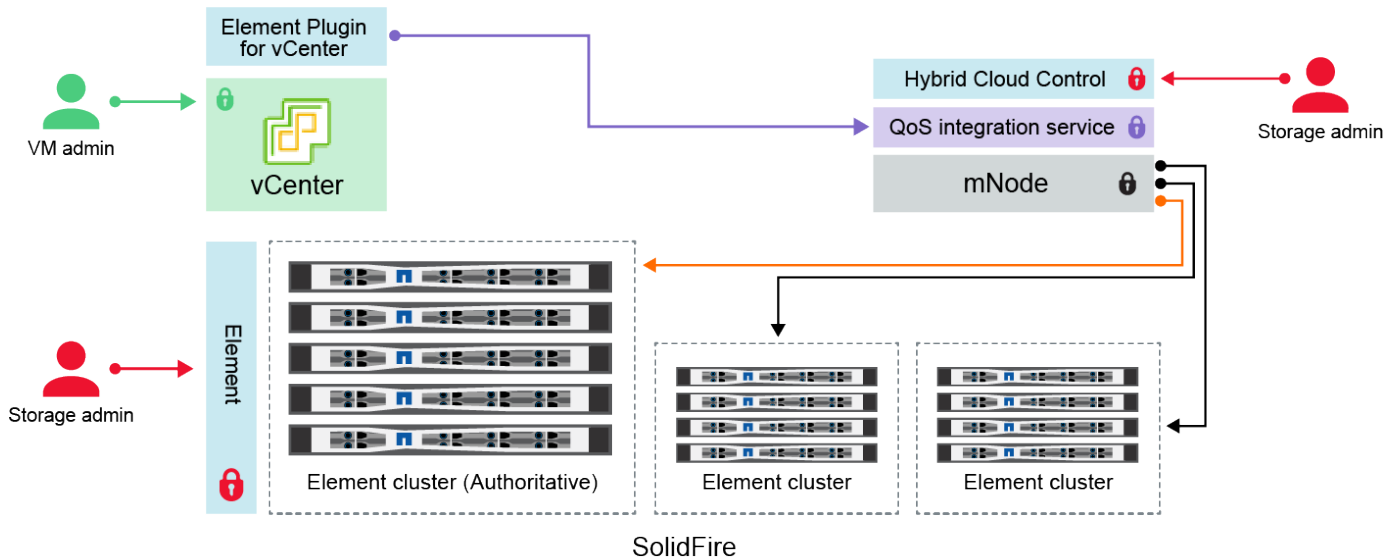
更改NetApp HCI和NetApp SolidFire中的凭据

根据部署NetApp HCI或NetApp SolidFire 的组织的安全策略，更改凭据或密码通常是安全实践的一部分。在更改密码之前，您应该了解此举对部署中其他软件组件的影响。

如果您更改NetApp HCI或NetApp SolidFire部署中某个组件的凭据，下表提供了有关对其他组件的影响的指导。

NetApp SolidFire组件交互

:



凭证类型和图标	管理员使用情况	请参阅这些说明
元素凭证 	适用范围： NetApp HCI和SolidFire 管理员使用以下凭据登录： - Element 存储集群上的 Element 用户界面 - 管理节点（mnode）上的混合云控制 当 Hybrid Cloud Control 管理多个存储集群时，它只接受存储集群的管理员凭据，即最初设置 mnode 的_权威集群_。对于之后添加到混合云控制的存储集群，mnode 安全地存储管理员凭据。如果后续添加的存储集群的凭证发生更改，则还必须使用 mnode API 在 mnode 中更新凭证。	请参阅这些说明 "更新存储集群管理员密码。" - 使用以下命令更新 mnode 中的存储集群管理员凭据："修改集群管理员 API"。
vSphere 单点登录凭据 	适用范围： 仅限NetApp HCI 管理员使用这些凭据登录 VMware vSphere Client。当 vCenter 作为NetApp HCI安装的一部分时，凭据在NetApp部署引擎中配置如下： - 使用指定的密码，以 <code>username@vsphere.local</code> 用户名登录，并 <code>administrator@vsphere.local</code> 使用指定的密码。当使用现有的 vCenter 部署NetApp HCI时，vSphere 单点登录凭据由 IT VMware 管理员管理。	"更新 vCenter 和 ESXi 凭据"。

凭证类型和图标	管理员使用情况	请参阅这些说明
基板管理控制器 (BMC) 凭证 	适用范围：仅限NetApp HCI 管理员使用这些凭证登录到NetApp HCI部署中NetApp计算节点的BMC。BMC提供基本的硬件监控和虚拟控制台功能。 在NetApp HCI部署中，每个NetApp计算节点的BMC（有时称为IPMI）凭据安全地存储在 mnode 上。NetApp Hybrid Cloud Control 使用BMC凭证作为服务帐户，在计算节点固件升级期间与计算节点中的BMC进行通信。 当BMC凭证更改时，mnode 上相应计算节点的凭证也必须更新，以保留所有混合云控制功能。	请参阅这些说明 • "在NetApp HCI上为每个节点配置 IPMI"。 • 对于 H410C、H610C 和 H615C 节点，"更改默认 IPMI 密码"。 • 对于 H410S 和 H610S 节点，"更改默认 IPM 密码"。 • "在管理节点上更改BMC凭据"。
ESXi凭证 	适用范围：仅限NetApp HCI 管理员可以使用 SSH 或本地 DCUI 和本地 root 帐户登录到 ESXi 主机。在NetApp HCI部署中，用户名是"root"，密码是在NetApp 部署引擎中首次安装该计算节点时指定的。 在NetApp HCI部署中，每个NetApp计算节点的 ESXi 根凭据都安全地存储在 mnode 上。NetApp Hybrid Cloud Control 使用服务帐户的凭据，在计算节点固件升级和运行状况检查期间直接与 ESXi 主机通信。 当 VMware 管理员更改 ESXi 根凭据时，必须在 mnode 上更新相应计算节点的凭据，以保留混合云控制功能。	"更新 vCenter 和 ESXi 主机的凭据"。
QoS集成密码 	适用范围：NetApp HCI和SolidFire中的可选组件 不用于管理员交互式登录。 VMware vSphere 和 Element Software 之间的 QoS 集成通过以下方式实现： • 适用于 vCenter Server 的 Element 插件，以及 • 在 mnode 上提供 QoS 服务。 为了进行身份验证，QoS 服务使用一个仅用于此上下文的密码。QoS 密码是在 vCenter Server 的 Element 插件初始安装期间指定的，或者是在NetApp HCI部署期间自动生成的。 对其他部件无影响。	"更新NetApp Element vCenter Server 插件中的 QoSSIOC 凭据"。 NetApp Element Plug-in for vCenter Server SIOC 密码也称为 QoSSIOC 密码。 请查看https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Plugin_for_vCenter_server/mNode_Status_shows_as_'Network_Down'_or_'Down'_in_the_mNode_Settings_tab_of_the_Element_Plugin_for_vCenter_(VCP)[vCenter Server Element插件知识库文章^]。

凭证类型和图标	管理员使用情况	请参阅这些说明
vCenter Service Appliance 凭据 	适用范围：仅限通过NetApp部署引擎设置的NetApp HCI。 管理员可以登录到 vCenter Server 设备虚拟机。在NetApp HCI部署中，用户名是“root”，密码是在NetApp部署引擎中首次安装该计算节点时指定的。根据部署的 VMware vSphere 版本，vSphere 单点登录域中的某些管理员也可以登录到该设备。 对其他部件无影响。	无需更改。
NetApp管理节点管理员凭据 	适用范围： NetApp HCI和SolidFire中的可选组件 管理员可以登录到NetApp管理节点虚拟机进行高级配置和故障排除。根据部署的管理节点版本，默认情况下未启用通过 SSH 登录。 在NetApp HCI部署中，用户名和密码是由用户在NetApp部署引擎中首次安装该计算节点时指定的。 对其他部件无影响。	无需更改。

查找更多信息

- ["更改 Element 软件的默认 SSL 证书"](#)
- ["更改节点的 IPMI 密码"](#)
- ["启用多重身份验证"](#)
- ["开始使用外部密钥管理"](#)
- ["创建支持 FIPS 驱动器的集群"](#)

更改 Element 软件的默认 SSL 证书

您可以使用NetApp Element API 更改集群中存储节点的默认 SSL 证书和私钥。

创建NetApp Element软件集群时，该集群会创建一个唯一的自签名安全套接字层 (SSL) 证书和私钥，用于通过 Element UI、每个节点的 UI 或 API 进行的所有 HTTPS 通信。Element 软件支持自签名证书以及由受信任的证书颁发机构 (CA) 颁发和验证的证书。

您可以使用以下 API 方法获取有关默认 SSL 证书的更多信息并进行更改。

- 获取**SSL**证书

您可以使用["GetSSLCertificate 方法"](#)检索有关当前已安装的 SSL 证书的信息，包括所有证书详细信息。

- 设置**SSL**证书

您可以使用["SetSSLCertificate 方法"](#)将集群和每个节点的 SSL 证书设置为您提供的证书和私钥。系统会对证

书和私钥进行验证，以防止应用无效证书。

- 移除**SSL**证书

这"[RemoveSSLCertificate 方法](#)"移除当前已安装的 SSL 证书和私钥。然后，集群会生成一个新的自签名证书和私钥。



集群 SSL 证书会自动应用于添加到集群中的所有新节点。从集群中移除的任何节点都将恢复为自签名证书，并且所有用户定义的证书和密钥信息都将从该节点中删除。

查找更多信息

- "[更改管理节点默认 SSL 证书](#)"
- "[在 Element Software 中设置自定义 SSL 证书有哪些要求？](#)"
- "[SolidFire和 Element 软件文档](#)"
- "[NetApp Element vCenter Server 插件](#)"

更改节点的默认 IPMI 密码

只要您拥有对节点的远程 IPMI 访问权限，即可更改默认的智能平台管理接口 (IPMI) 管理员密码。如果安装有任何更新，您可能需要执行此操作。

有关配置节点 IPMI 访问权限的详细信息，请参阅"[为每个节点配置 IPMI](#)"。

您可以更改以下节点的 IPMI 密码：

- H410S节点
- H610S节点

更改 H410S 节点的默认 IPMI 密码

配置 IPMI 网络端口后，应立即更改每个存储节点上 IPMI 管理员帐户的默认密码。

你需要什么

您应该为每个存储节点配置 IPMI IP 地址。

步骤

1. 在能够访问 IPMI 网络的计算机上打开网页浏览器，并浏览到节点的 IPMI IP 地址。
2. 请输入用户名 `ADMIN` 和密码 `ADMIN` 在登录提示符中。
3. 登录后，点击“配置”选项卡。
4. 点击“用户”。
5. 选择 `ADMIN` 用户并点击*修改用户*。
6. 选中“更改密码”复选框。
7. 请在“密码”和“确认密码”字段中输入新密码。

8. 点击“修改”，然后点击“确定”。
9. 对其他所有使用默认 IPMI 密码的 H410S 节点重复此过程。

更改 H610S 节点的默认 IPMI 密码

配置 IPMI 网络端口后，应立即更改每个存储节点上 IPMI 管理员帐户的默认密码。

你需要什么

您应该为每个存储节点配置 IPMI IP 地址。

步骤

1. 在能够访问 IPMI 网络的计算机上打开网页浏览器，并浏览到节点的 IPMI IP 地址。
2. 请输入用户名 `root` 和密码 `calvin` 在登录提示符中。
3. 登录后，点击页面左上角的菜单导航图标，打开侧边栏抽屉。
4. 点击“设置”。
5. 点击“用户管理”。
6. 从列表中选择*管理员*用户。
7. 启用“更改密码”复选框。
8. 请在“密码”和“确认密码”字段中输入新的、强密码。
9. 点击页面底部的“保存”。
10. 对其他所有使用默认 IPMI 密码的 H610S 节点重复此过程。

查找更多信息

- ["SolidFire和 Element 软件文档"](#)
- ["NetApp Element vCenter Server 插件"](#)

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。