在部署后配置 SolidFire 系统选项

Element Software

NetApp
January 15, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/element-software-123/storage/task_post_deploy_credentials.html on January 15, 2024. Always check docs.netapp.com for the latest.

目录

在部署后配置 SolidFire 系统选项

设置 SolidFire 系统后，您可能需要执行一些可选任务。

如果更改系统中的凭据，您可能希望了解对其他组件的影响。

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。您还应根据需要查看更新密码。

了解更多信息

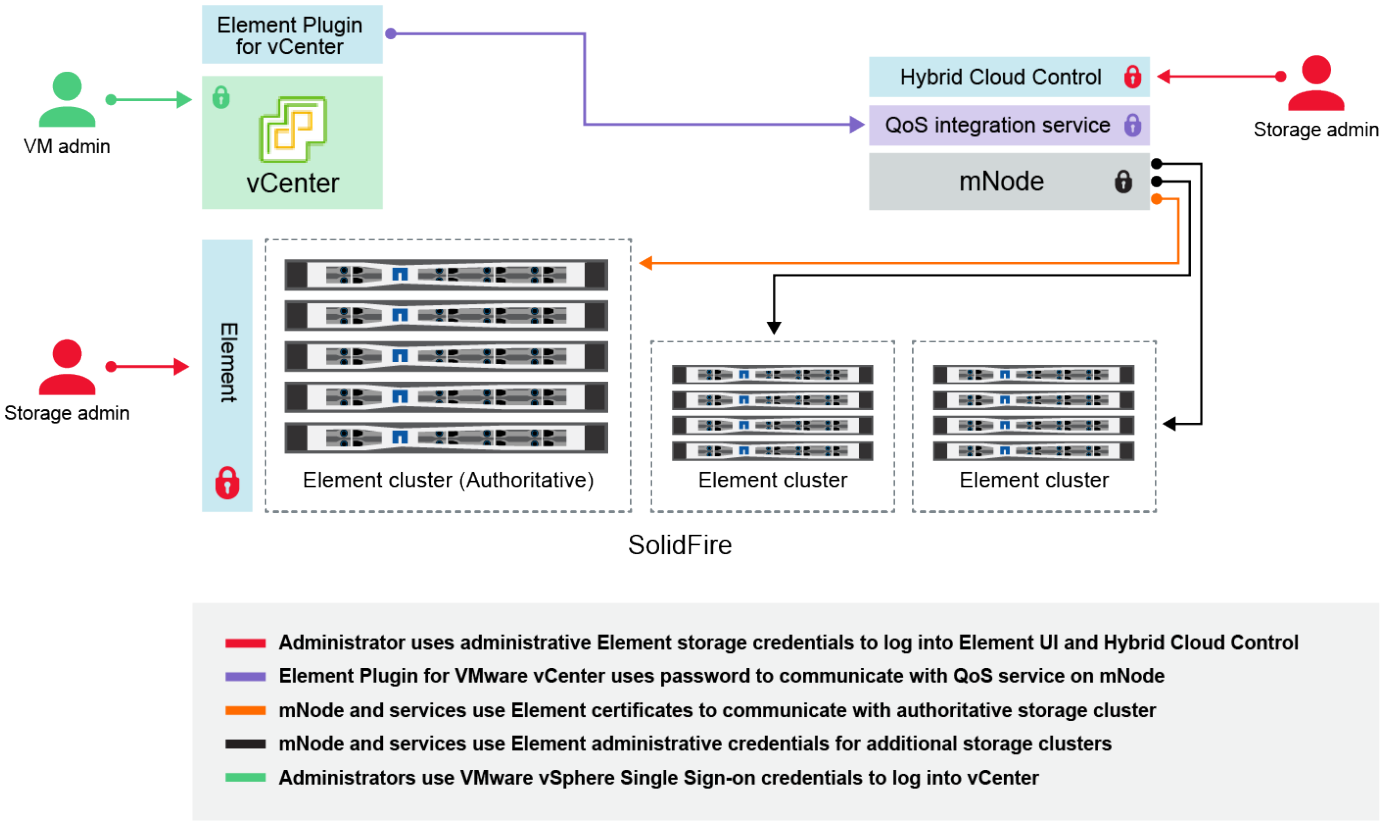
- "在 NetApp HCI 和 NetApp SolidFire 中更改凭据"
- "更改 Element 软件的默认 SSL 证书"
- "更改节点的 IPMI 密码"
- "启用多因素身份验证"
- "开始使用外部密钥管理"
- "创建支持 FIPS 驱动器的集群"

在 NetApp HCI 和 NetApp SolidFire 中更改凭据

根据部署 NetApp HCI 或 NetApp SolidFire 的组织中的安全策略，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，您应了解此部署对其他软件组件的影响。

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

NetApp SolidFire 组件交互
：



凭据类型和图标	管理员使用情况	请参见以下说明
Element 凭据	• 适用场景 *： NetApp HCI 和 SolidFire 管理员可以使用这些凭据登录到： • 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，它仅接受存储集群的管理员凭据，即最初为 mnode 设置的 *authoritative cluster* 。对于稍后添加到 Hybrid Cloud Control 的存储集群， mnode 会安全地存储管理员凭据。如果更改了随后添加的存储集群的凭据，则还必须使用 mnode API 在 mnode 中更新这些凭据。	• "更新存储集群管理员密码。" • 使用更新 mnode 中的存储集群管理员凭据 "modifyclusteradmin API"。
vSphere 单点登录凭据	• 适用场景 *： 仅限 NetApp HCI 管理员可以使用这些凭据登录到 VMware vSphere Client 。如果 vCenter 是 NetApp HCI 安装的一部分，则凭据会在 NetApp 部署引擎中配置如下： • 使用指定密码 username@vsphere.local ，和 • 使用指定密码 administrator@vsphere.local 。使用现有 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"。

凭据类型和图标	管理员使用情况	请参见以下说明
基板管理控制器（BMC）凭据	• 适用场景 *：仅限 NetApp HCI 管理员可以使用这些凭据登录到 NetApp HCI 部署中 NetApp 计算节点的 BMC 。BMC 可提供基本的硬件监控和虚拟控制台功能。 每个 NetApp 计算节点的 BMC （有时称为 *ipmi* ）凭据都安全地存储在 NetApp HCI 部署中的 mnode 上。在计算节点固件升级期间， NetApp Hybrid Cloud Control 使用服务帐户容量中的 BMC 凭据与计算节点中的 BMC 进行通信。 更改 BMC 凭据后，还必须在 mnode 上更新相应计算节点的凭据，以保留所有 Hybrid Cloud Control 功能。	• "为 NetApp HCI 上的每个节点配置 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"。 • "更改管理节点上的 BMC 凭据"。
ESXi 凭据	• 适用场景 *：仅限 NetApp HCI 管理员可以使用 SSH 或本地 DCUI 使用本地 root 帐户登录到 ESXi 主机。在 NetApp HCI 部署中，用户名为 "root" ，密码是在 NetApp 部署引擎中首次安装该计算节点期间指定的。 每个 NetApp 计算节点的 ESXi 根凭据都安全地存储在 NetApp HCI 部署中的 mnode 上。在计算节点固件升级和运行状况检查期间， NetApp Hybrid Cloud Control 使用服务帐户容量中的凭据直接与 ESXi 主机进行通信。 如果 VMware 管理员更改了 ESXi 根凭据，则必须在 mnode 上更新相应计算节点的凭据，才能保留 Hybrid Cloud Control 功能。	"更新 vCenter 和 ESXi 主机的凭据"。
QoS 集成密码	• 适用场景 *： NetApp HCI ，在 SolidFire 中可选 不用于管理员交互式登录。 VMware vSphere 与 Element 软件之间的 QoS 集成可通过以下方式实现： • 适用于 vCenter Server 的 Element 插件，和 • mnode 上的 QoS 服务。 对于身份验证， QoS 服务使用在此上下文中专用的密码。QoS 密码是在首次安装适用于 vCenter Server 的 Element 插件期间指定的，或者在 NetApp HCI 部署期间自动生成的。 不会对其他组件造成影响。	"在适用于 vCenter Server 的 NetApp Element 插件中更新 QoSSIOC 凭据"。 适用于vCenter Server SIOC的NetApp Element 插件密码也称为_QoSSIOC密码_。 查看 {url-peak} [适用于vCenter Server的Element插件知识库文章^。

凭据类型和图标	管理员使用情况	请参见以下说明
vCenter Service Appliance 凭据	• NetApp 部署引擎 *： 仅在 NetApp HCI 部署引擎设置的情况下才支持适用场景 管理员可以登录到 vCenter Server 设备虚拟机。在 NetApp HCI 部署中，用户名为 "root" ，密码是在 NetApp 部署引擎中首次安装该计算节点期间指定的。根据部署的 VMware vSphere 版本，vSphere Single Sign-On 域中的某些管理员也可以登录到设备。 不会对其他组件造成影响。	无需更改。
NetApp 管理节点管理员凭据	• 适用场景 *： NetApp HCI ，在 SolidFire 中可选 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，默认情况下不会启用通过 SSH 登录。 在 NetApp HCI 部署中，用户在 NetApp 部署引擎中首次安装该计算节点期间指定了用户名和密码。 不会对其他组件造成影响。	无需更改。

了解更多信息

- "更改 Element 软件的默认 SSL 证书"
- "更改节点的 IPMI 密码"
- "启用多因素身份验证"
- "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 证书和专用密钥。

创建 NetApp Element 软件集群时，集群会创建一个唯一的自签名安全套接字层（ SSL ）证书和专用密钥，用于通过 Element UI ，每节点 UI 或 API 进行所有 HTTPS 通信。Element 软件支持自签名证书以及由可信证书颁发机构（ 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 证书的详细信息并进行更改。

- * GetSSLCertificate *

  您可以使用 "GetSSLCertificate方法" 检索有关当前安装的SSL证书的信息、包括所有证书详细信息。

- * 设置 SSLCertificate *

您可以使用 "SetSSLCertificate方法" 将集群和每节点SSL证书设置为您提供的证书和专用密钥。系统会验证证书和专用密钥，以防止应用无效证书。

- * 删除 SSLCertificer*

  。 "RemoveSSLCertificate方法" 删除当前安装的SSL证书和专用密钥。然后，集群将生成新的自签名证书和专用密钥。

> 集群 SSL 证书会自动应用于添加到集群中的所有新节点。从集群中删除的任何节点都会还原为自签名证书，并且所有用户定义的证书和密钥信息都会从该节点中删除。

了解更多信息

- "更改管理节点的默认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"
- "适用于 vCenter Server 的 NetApp Element 插件"

更改节点的默认 IPMI 密码

您可以在对节点具有远程 IPMI 访问权限后立即更改默认的智能平台管理接口（ Intelligent Platform Management Interface ， IPMI ）管理员密码。如果存在任何安装更新，您可能需要执行此操作。

有关为节点配置 IPM 访问的详细信息，请参见 "为每个节点配置 IPMI"。

您可以更改以下节点的 IPM 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，应尽快更改每个存储节点上 IPMI 管理员帐户的默认密码。

您需要的内容

您应该已为每个存储节点配置 IPMI IP 地址。

步骤

1. 在可以访问 IPMI 网络的计算机上打开 Web 浏览器，然后浏览到此节点的 IPMI IP 地址。
2. 在登录提示符处输入用户名 `admin` 和密码 `admin` 。
3. 登录后，单击 * 配置 * 选项卡。
4. 单击 * 用户 * 。
5. 选择 `admin` user ，然后单击 * 修改用户 * 。

6. 选中 * 更改密码 * 复选框。
7. 在 * 密码 * 和 * 确认密码 * 字段中输入新密码。
8. 单击 * 修改 * ，然后单击 * 确定 * 。
9. 对具有默认 IPMI 密码的任何其他 H410S 节点重复此操作步骤。

更改 H610S 节点的默认 IPMI 密码

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

您需要的内容

您应该已为每个存储节点配置 IPMI IP 地址。

步骤

1. 在可以访问 IPMI 网络的计算机上打开 Web 浏览器，然后浏览到此节点的 IPMI IP 地址。
2. 在登录提示符处输入用户名 `root` 和密码 `calvin` 。
3. 登录后，单击页面左上角的菜单导航图标以打开边栏抽屉。
4. 单击 * 设置 * 。
5. 单击 * 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. 在 * 密码 * 和 * 确认密码 * 字段中输入新的强密码。
9. 单击页面底部的 * 保存 * 。
10. 对具有默认 IPMI 密码的任何其他 H610S 节点重复此操作步骤。

了解更多信息

- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

版权信息

版权所有 © 2024 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。