Configuration des options du système SolidFire après le déploiement

Element Software

NetApp
October 01, 2024

Sommaire

Configuration des options du système SolidFire après le déploiement

Une fois le système SolidFire configuré, vous pouvez effectuer certaines tâches facultatives.

Si vous modifiez les informations d'identification dans le système, vous pouvez connaître l'impact sur les autres composants.

En outre, vous pouvez configurer les paramètres de l'authentification multifacteur, de la gestion externe des clés et de la sécurité FIPS (Federal information Processing Standards). Vous devez également examiner la mise à jour des mots de passe si nécessaire.

Trouvez plus d'informations

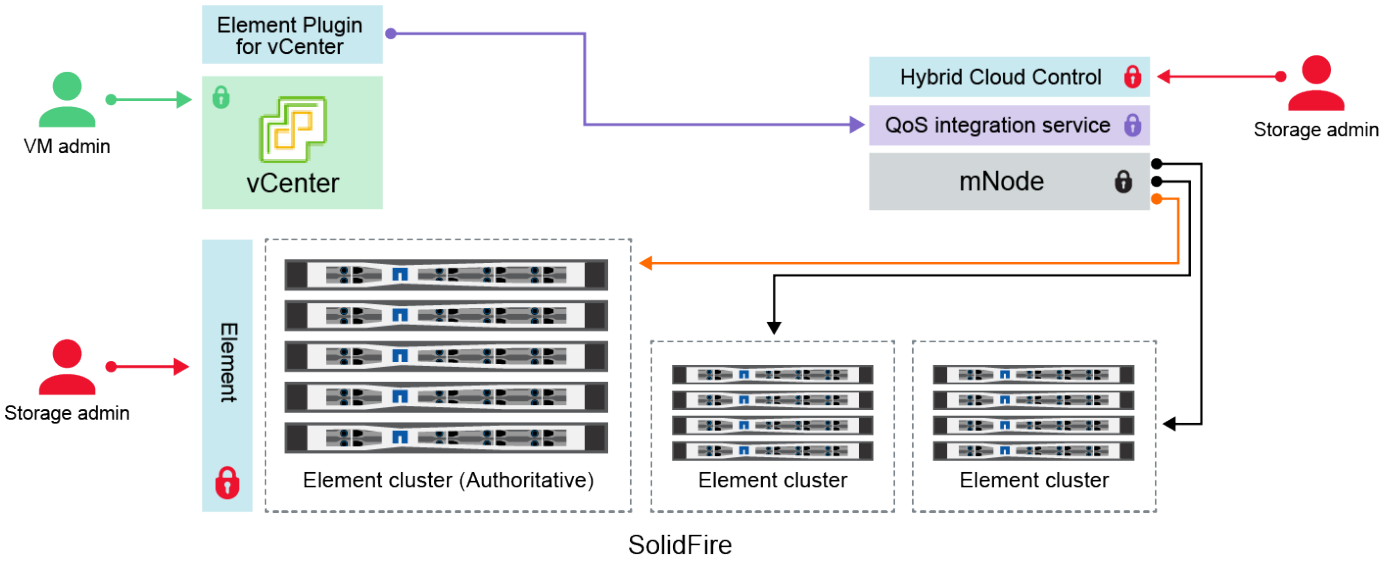
- "Modifiez les identifiants dans NetApp HCI et NetApp SolidFire"
- "Modifiez le certificat SSL par défaut du logiciel Element"
- "Modifiez le mot de passe IPMI pour les nœuds"
- "Activez l'authentification multifacteur"
- "Commencez par une gestion externe des clés"
- "Créez un cluster prenant en charge les disques FIPS"

Modifiez les identifiants dans NetApp HCI et NetApp SolidFire

Selon les politiques de sécurité établies dans l'entreprise qui ont déployé NetApp HCI ou NetApp SolidFire, il est souvent possible de modifier des identifiants ou des mots de passe. Avant de modifier les mots de passe, vous devez connaître l'impact sur les autres composants logiciels du déploiement.

Si vous modifiez les identifiants d'un composant d'un déploiement NetApp HCI ou NetApp SolidFire, le tableau suivant fournit des conseils sur l'impact sur les autres composants.

Interactions des composants NetApp SolidFire :



Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Informations d'identification d'élément 	**S'applique à**: NetApp HCI et SolidFire Les administrateurs utilisent ces informations d'identification pour se connecter à : • Interface utilisateur Element sur le cluster de stockage Element • Contrôle du cloud hybride sur le nœud de gestion (mNode) Lorsque Hybrid Cloud Control gère plusieurs clusters de stockage, il n'accepte que les identifiants d'administration des clusters de stockage, appelés « cluster qui fait autorité », pour lesquels le nœud a été initialement configuré. Pour les clusters de stockage ajoutés ultérieurement au contrôle du cloud hybride, mNode stocke en toute sécurité les informations d'identification d'administration. Si les informations d'identification des clusters de stockage ajoutés ultérieurement sont modifiées, les informations d'identification doivent également être mises à jour dans le mNode à l'aide de l'API mNode.	• "Mettre à jour les mots de passe d'administration du cluster de stockage." • Mettez à jour les informations d'identification de l'administrateur du cluster de stockage dans le nœud mNode à l'aide de "API modifyclusteradmin".

Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Identifiants d'authentification unique vSphere 	**S'applique à**: NetApp HCI seulement Les administrateurs utilisent ces informations d'identification pour se connecter au client VMware vSphere. Lorsque vCenter fait partie de l'installation de NetApp HCI, les identifiants sont configurés dans le moteur de déploiement NetApp comme suit : • nomutilisateur@vsphere.locusmabl avec le mot de passe spécifié, et • admin@vsphere.locks.com avec le mot de passe spécifié. Lorsqu'un vCenter existant est utilisé pour déployer NetApp HCI, les identifiants d'authentification unique vSphere sont gérés par les administrateurs IT VMware.	"Mettre à jour les identifiants vCenter et ESXi".
Informations d'identification du contrôleur BMC (Baseboard Management Controller) 	**S'applique à**: NetApp HCI seulement Les administrateurs utilisent ces identifiants pour se connecter au BMC des nœuds de calcul NetApp dans un déploiement NetApp HCI. Le contrôleur BMC propose des fonctions de base de surveillance du matériel et de console virtuelle. Les identifiants BMC (parfois appelés *IPMI*) pour chaque nœud de calcul NetApp sont stockés de manière sécurisée sur le nœud mNode dans les déploiements NetApp HCI. NetApp Hybrid Cloud Control utilise les identifiants BMC dans la capacité d'un compte de service pour communiquer avec le BMC dans les nœuds de calcul lors des mises à niveau du micrologiciel du nœud de calcul. Lorsque les informations d'identification BMC sont modifiées, les informations d'identification des nœuds de calcul respectifs doivent également être mises à jour sur mNode pour conserver toutes les fonctionnalités de contrôle du cloud hybride.	• "Configurez IPMI pour chaque nœud sur NetApp HCI". • Pour les nœuds H410C, H610C et H615C, "Modifier le mot de passe IPMI par défaut". • Pour les nœuds H410S et H610S, "Modifier le mot de passe IPM par défaut". • "Modifiez les informations d'identification BMC sur le nœud de gestion".

Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Identifiants ESXi 	**S'applique à**: NetApp HCI seulement Les administrateurs peuvent se connecter à des hôtes ESXi à l'aide de SSH ou de DCUI local avec un compte racine local. Dans les déploiements NetApp HCI, le nom d'utilisateur est « root » et le mot de passe a été spécifié lors de l'installation initiale de ce nœud de calcul dans le moteur de déploiement NetApp. Les identifiants root ESXi pour chaque nœud de calcul NetApp sont stockés en toute sécurité sur le nœud mNode dans les déploiements NetApp HCI. NetApp Hybrid Cloud Control utilise les identifiants se trouvant dans la capacité d'un compte de service pour communiquer avec les hôtes ESXi directement pendant les mises à niveau du firmware du nœud de calcul et les vérifications de l'état de santé. Lorsque les identifiants root ESXi sont modifiés par un administrateur VMware, les informations d'identification des nœuds de calcul respectifs doivent être mises à jour sur le nœud mNode pour conserver la fonctionnalité de contrôle du cloud hybride.	"Mettez à jour les informations d'identification pour les hôtes vCenter et ESXi".
Mot de passe d'intégration de la QoS 	**S'applique à**: NetApp HCI et optionnel en SolidFire Non utilisé pour les connexions interactives par les administrateurs. L'intégration de QoS entre VMware vSphere et Element Software s'effectue via : • Le plug-in Element pour vCenter Server, et • Service de qualité de service sur le mNode. Pour l'authentification, le service QoS utilise un mot de passe exclusivement utilisé dans ce contexte. Le mot de passe QoS est spécifié lors de l'installation initiale du plug-in Element pour vCenter Server, ou généré automatiquement lors du déploiement de NetApp HCI. Aucun impact sur les autres composants.	"Mettez à jour les informations d'identification QoSSIOC dans le plug-in NetApp Element pour vCenter Server". Le mot de passe NetApp Element Plug-in for vCenter Server SIOC est également appelé *QoSSIOC password*. Consultez l'article Element Plug-in for vCenter Server KB.

Type et icône d'informations d'identification	Utilisation par l'administrateur	Reportez-vous à ces instructions
Identifiants de l'appliance vCenter Service 	**S'applique à** : NetApp HCI uniquement si configuré par le moteur de déploiement NetApp Les administrateurs peuvent se connecter aux machines virtuelles de l'appliance vCenter Server. Dans les déploiements NetApp HCI, le nom d'utilisateur est « root » et le mot de passe a été spécifié lors de l'installation initiale de ce nœud de calcul dans le moteur de déploiement NetApp. Selon la version de VMware vSphere déployée, certains administrateurs du domaine d'authentification unique vSphere peuvent également se connecter à l'appliance. Aucun impact sur les autres composants.	Aucune modification requise.
Identifiants d'administrateur du nœud de gestion NetApp 	**S'applique à**: NetApp HCI et optionnel en SolidFire Les administrateurs peuvent se connecter aux ordinateurs virtuels de nœud de gestion NetApp pour obtenir des fonctions avancées de configuration et de dépannage. Selon la version du nœud de gestion déployée, la connexion via SSH n'est pas activée par défaut. Dans les déploiements NetApp HCI, l' utilisateur a spécifié le nom d'utilisateur et le mot de passe lors de l'installation initiale de ce nœud de calcul dans le moteur de déploiement NetApp. Aucun impact sur les autres composants.	Aucune modification requise.

Trouvez plus d'informations

- "Modifiez le certificat SSL par défaut du logiciel Element"
- "Modifiez le mot de passe IPMI pour les nœuds"
- "Activez l'authentification multifacteur"
- "Commencez par une gestion externe des clés"
- "Créez un cluster prenant en charge les disques FIPS"

Modifiez le certificat SSL par défaut du logiciel Element

Vous pouvez modifier le certificat SSL par défaut et la clé privée du nœud de stockage du cluster à l'aide de l'API NetApp Element.

Lors de la création d'un cluster logiciel NetApp Element, le cluster crée un certificat SSL unique et une clé privée auto-signés qui sont utilisés pour toutes les communications HTTPS via l'interface utilisateur d'Element,

l'interface utilisateur par nœud ou les API. Le logiciel Element prend en charge les certificats auto-signés ainsi que les certificats émis et vérifiés par une autorité de certification (AC) de confiance.

Vous pouvez utiliser les méthodes d'API suivantes pour obtenir plus d'informations sur le certificat SSL par défaut et apporter des modifications.

- **GetSSLCertificate**

  Vous pouvez utiliser le "Méthode GetSSLCertificate" pour récupérer des informations sur le certificat SSL actuellement installé, y compris tous les détails du certificat.

- **SetSSLCertificate**

  Vous pouvez utiliser "Méthode SetSSLCertificate"pour définir les certificats SSL de cluster et par nœud sur le certificat et la clé privée que vous fournissez. Le système valide le certificat et la clé privée pour empêcher l'application d'un certificat non valide.

- **RemoveSSLCertificate**

  "Méthode RemoveSSLCertificate"Supprime le certificat SSL et la clé privée actuellement installés. Le cluster génère alors un nouveau certificat auto-signé et une nouvelle clé privée.

> Le certificat SSL de cluster est automatiquement appliqué à tous les nouveaux nœuds ajoutés au cluster. Tout nœud supprimé du cluster revient à un certificat auto-signé et toutes les informations de certificat et de clé définies par l'utilisateur sont supprimées du nœud.

Trouvez plus d'informations

- "Modifiez le certificat SSL par défaut du nœud de gestion"
- "Quelles sont les exigences relatives à la définition de certificats SSL personnalisés dans Element Software ?"
- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"

Modifiez le mot de passe IPMI par défaut pour les nœuds

Vous pouvez modifier le mot de passe administrateur par défaut de l'interface IPMI (Intelligent Platform Management interface) dès que vous disposez d'un accès IPMI à distance au nœud. Vous pouvez le faire si des mises à jour d'installation sont disponibles.

Pour plus d'informations sur la configuration de l'accès IPM pour les nœuds, reportez-vous à la section "Configurez IPMI pour chaque nœud".

Vous pouvez modifier le mot de passe IPM pour ces nœuds :

- Nœuds H410S
- Nœuds H610S

Modifiez le mot de passe IPMI par défaut pour les nœuds H410S

Vous devez modifier le mot de passe par défaut du compte administrateur IPMI sur chaque nœud de stockage dès que vous configurez le port réseau IPMI.

Ce dont vous avez besoin

Vous devez avoir configuré l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur Web sur un ordinateur qui peut atteindre le réseau IPMI et naviguez jusqu'à l'adresse IP IPMI du nœud.
2. Entrez le nom d'utilisateur `ADMIN` et le mot de passe `ADMIN` dans l'invite de connexion.
3. Lorsque vous vous connectez, cliquez sur l'onglet **Configuration**.
4. Cliquez sur **utilisateurs**.
5. Sélectionnez `ADMIN` l'utilisateur et cliquez sur **Modifier l'utilisateur**.
6. Cochez la case **Modifier le mot de passe**.
7. Entrez un nouveau mot de passe dans les champs **Mot de passe** et **confirmer le mot de passe**.
8. Cliquez sur **Modifier**, puis sur **OK**.
9. Répétez cette procédure pour tous les autres nœuds H410S avec mots de passe IPMI par défaut.

Modifiez le mot de passe IPMI par défaut pour les nœuds H610S

Vous devez modifier le mot de passe par défaut du compte administrateur IPMI sur chaque nœud de stockage dès que vous configurez le port réseau IPMI.

Ce dont vous avez besoin

Vous devez avoir configuré l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur Web sur un ordinateur qui peut atteindre le réseau IPMI et naviguez jusqu'à l'adresse IP IPMI du nœud.
2. Entrez le nom d'utilisateur `root` et le mot de passe `calvin` dans l'invite de connexion.
3. Lorsque vous vous connectez, cliquez sur l'icône de navigation dans le menu en haut à gauche de la page pour ouvrir le tiroir de la barre latérale.
4. Cliquez sur **Paramètres**.
5. Cliquez sur **gestion des utilisateurs**.
6. Sélectionnez l'utilisateur **Administrateur** dans la liste.
7. Activez la case à cocher **Modifier le mot de passe**.
8. Saisissez un nouveau mot de passe fort dans les champs **Mot de passe** et **confirmer le mot de passe**.
9. Cliquez sur **Enregistrer** en bas de la page.
10. Répétez cette procédure pour tous les autres nœuds H610S avec mots de passe IPMI par défaut.

Trouvez plus d’informations

- "Documentation SolidFire et Element"
- "Plug-in NetApp Element pour vCenter Server"