



Configurez les options système SolidFire après le déploiement.

Element Software

NetApp
November 12, 2025

Sommaire

- Configurez les options système SolidFire après le déploiement. 1
 - Configurez les options système SolidFire après le déploiement. 1
 - Trouver plus d'informations 1
- Modifier les informations d'identification dans NetApp HCI et NetApp SolidFire 1
 - Trouver plus d'informations 5
- Modifier le certificat SSL par défaut du logiciel Element 5
 - Trouver plus d'informations 6
- Modifier le mot de passe IPMI par défaut des nœuds 6
 - Modifier le mot de passe IPMI par défaut des nœuds H410S 6
 - Modifier le mot de passe IPMI par défaut des nœuds H610S 7
 - Trouver plus d'informations 7

Configurez les options système SolidFire après le déploiement.

Configurez les options système SolidFire après le déploiement.

Une fois votre système SolidFire configuré, vous pouvez effectuer quelques tâches facultatives.

Si vous modifiez les identifiants du système, vous voudrez peut-être connaître l'impact sur les autres composants.

De plus, vous pouvez configurer les paramètres d'authentification multifactorielle, de gestion des clés externes et de sécurité FIPS (Federal Information Processing Standards). Il est également conseillé de mettre à jour vos mots de passe lorsque cela est nécessaire.

Trouver plus d'informations

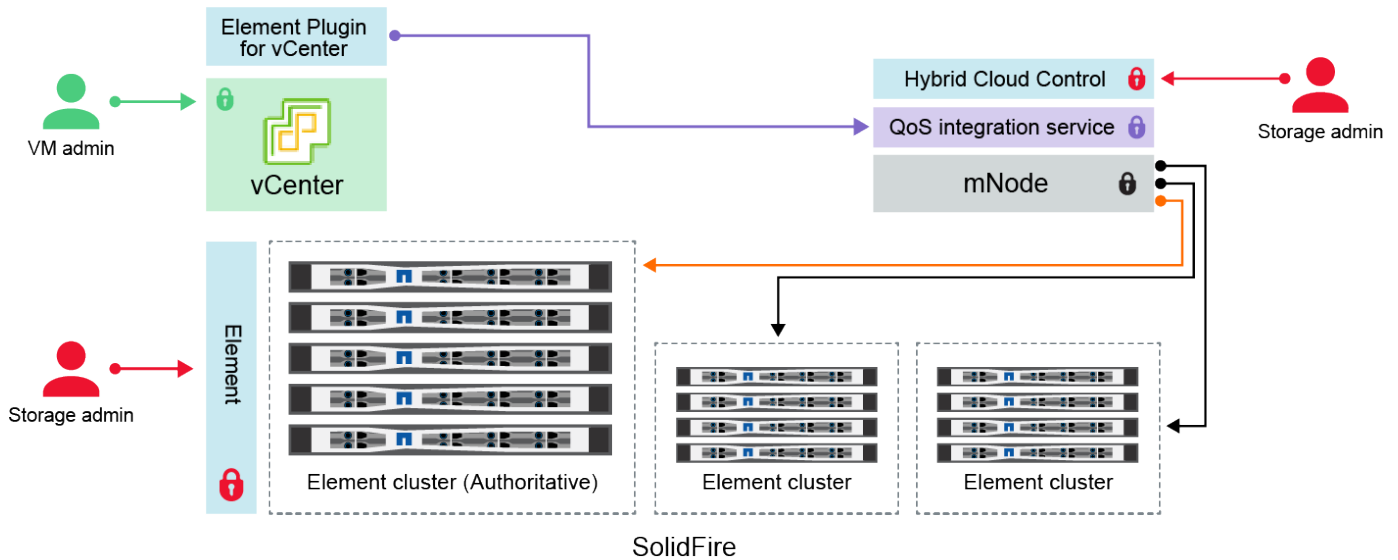
- ["Modifier les informations d'identification dans NetApp HCI et NetApp SolidFire"](#)
- ["Modifier le certificat SSL par défaut du logiciel Element"](#)
- ["Modifier le mot de passe IPMI des nœuds"](#)
- ["Activer l'authentification multifacteur"](#)
- ["Commencez la gestion des clés externes"](#)
- ["Créer un cluster prenant en charge les disques FIPS"](#)

Modifier les informations d'identification dans NetApp HCI et NetApp SolidFire

Selon les politiques de sécurité de l'organisation qui a déployé NetApp HCI ou NetApp SolidFire, la modification des identifiants ou des mots de passe fait généralement partie des pratiques de sécurité. Avant de modifier les mots de passe, vous devez prendre en compte l'impact sur les autres composants logiciels du déploiement.

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

Interactions entre les composants de NetApp SolidFire :



Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants de l'élément 	S'applique à : NetApp HCI et SolidFire Les administrateurs utilisent ces identifiants 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 informations d'identification de l'administrateur des clusters de stockage, connus sous le nom de <i>cluster faisant autorité</i> pour lesquels le mnode a été initialement configuré. Pour les clusters de stockage ajoutés ultérieurement à Hybrid Cloud Control, le mnode stocke en toute sécurité les informations d'identification de l'administrateur. Si les informations d'identification des clusters de stockage ajoutés ultérieurement sont modifiées, ces informations d'identification doivent également être mises à jour dans le mnode à l'aide de l'API mnode.	"Mettez à jour les mots de passe d'administrateur du cluster de stockage." - Mettez à jour les informations d'identification de l'administrateur du cluster de stockage dans le mnode en utilisant le "API modifyclusteradmin".

Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants d'authentification unique vSphere 	S'applique uniquement à : NetApp HCI Les administrateurs utilisent ces identifiants pour se connecter au client VMware vSphere. Lorsque vCenter fait partie de l'installation NetApp HCI, les informations d'identification sont configurées dans le moteur de déploiement NetApp comme suit : • nom_utilisateur@vsphere.local avec le mot de passe spécifié, et • administrateur@vsphere.local avec le mot de passe spécifié. Lorsqu'un vCenter existant est utilisé pour déployer NetApp HCI, les informations d'identification vSphere Single Sign-on sont gérées par les administrateurs VMware du service informatique.	"Mise à jour des identifiants vCenter et ESXi".
Identifiants du contrôleur de gestion de la carte mère (BMC) 	S'applique uniquement à : NetApp HCI Les administrateurs utilisent ces identifiants pour se connecter au BMC des nœuds de calcul NetApp dans un déploiement NetApp HCI. Le BMC assure la surveillance matérielle de base et offre des fonctionnalités de console virtuelle. Les informations d'identification BMC (parfois appelées <i>IPMI</i>) de chaque nœud de calcul NetApp sont stockées en toute sécurité sur le mnode dans les déploiements NetApp HCI. NetApp Hybrid Cloud Control utilise les informations d'identification BMC en tant que compte de service pour communiquer avec le BMC des nœuds de calcul lors des mises à niveau du firmware des nœuds de calcul. Lorsque les identifiants BMC sont modifiés, les identifiants des nœuds de calcul respectifs doivent également être mis à jour sur le mnode afin de conserver toutes les fonctionnalités de Hybrid Cloud Control.	• "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". • "Modifier les informations d'identification BMC sur le nœud de gestion".

Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants ESXi 	S'applique uniquement à : NetApp HCI Les administrateurs peuvent se connecter aux hôtes ESXi en utilisant soit SSH, soit l'interface DCUI locale 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 NetApp Deployment Engine. Les informations d'identification racine ESXi de chaque nœud de calcul NetApp sont stockées en toute sécurité sur le mnode dans les déploiements NetApp HCI. NetApp Hybrid Cloud Control utilise les informations d'identification d'un compte de service pour communiquer directement avec les hôtes ESXi lors des mises à niveau du firmware et des contrôles d'intégrité des nœuds de calcul. Lorsque les informations d'identification racine ESXi sont modifiées par un administrateur VMware, les informations d'identification des nœuds de calcul respectifs doivent être mises à jour sur le mnode pour conserver la fonctionnalité de contrôle du cloud hybride.	"Mise à jour des informations d'identification pour les hôtes vCenter et ESXi".
mot de passe d'intégration QoS 	S'applique à : NetApp HCI et, en option, SolidFire Non utilisé pour les connexions interactives des administrateurs. L'intégration QoS entre VMware vSphere et Element Software est activée via : • Module d'extension Element pour vCenter Server, et • Service QoS 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 SIOC du plug-in NetApp Element pour vCenter Server est également connu sous le nom de <i>mot de passe QoSSIOC</i>. Consultez l'article de la base de connaissances Element Plug-in pour vCenter Server.

Type et icône d'identification	Utilisation par l'administrateur	Consultez ces instructions
Identifiants de l'appliance vCenter Service 	S'applique à : NetApp HCI uniquement s'il est configuré par NetApp Deployment Engine 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 vSphere Single Sign-on peuvent également se connecter à l'appliance. Aucun impact sur les autres composants.	Aucune modification nécessaire.
Identifiants d'administrateur du nœud de gestion NetApp 	S'applique à : NetApp HCI et, en option, SolidFire Les administrateurs peuvent se connecter aux machines virtuelles du nœud de gestion NetApp pour effectuer des configurations avancées et des dépannages. Selon la version du nœud de gestion déployée, la connexion via SSH n'est pas activée par défaut. Dans les déploiements NetApp HCI, le nom d'utilisateur et le mot de passe étaient spécifiés par l'utilisateur lors de l'installation initiale de ce nœud de calcul dans NetApp Deployment Engine. Aucun impact sur les autres composants.	Aucune modification nécessaire.

Trouver plus d'informations

- ["Modifier le certificat SSL par défaut du logiciel Element"](#)
- ["Modifier le mot de passe IPMI des nœuds"](#)
- ["Activer l'authentification multifacteur"](#)
- ["Commencez la gestion des clés externes"](#)
- ["Créer un cluster prenant en charge les disques FIPS"](#)

Modifier 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, celui-ci génère un certificat SSL (Secure Sockets Layer) auto-signé unique et une clé privée utilisés pour toutes les communications HTTPS via l'interface utilisateur 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 API suivantes pour obtenir plus d'informations sur le certificat SSL par défaut et y apporter des modifications.

- **Obtenir un certificat SSL**

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

- **Définir le certificat SSL**

Vous pouvez utiliser le "[Méthode SetSSLCertificate](#)" pour configurer les certificats SSL du cluster et par nœud avec le certificat et la clé privée que vous fournissez. Le système valide le certificat et la clé privée afin d'empêcher l'application d'un certificat invalide.

- **Supprimer le certificat SSL**

Le "[Méthode RemoveSSLCertificate](#)" Supprime le certificat SSL et la clé privée actuellement installés. Le cluster génère ensuite un nouveau certificat auto-signé et une nouvelle clé privée.



Le certificat SSL du cluster est automatiquement appliqué à tous les nouveaux nœuds ajoutés au cluster. Tout nœud retiré 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.

Trouver plus d'informations

- "[Modifier le certificat SSL par défaut du nœud de gestion](#)"
- "[Quelles sont les exigences relatives à la configuration de certificats SSL personnalisés dans Element Software ?](#)"
- "[Documentation logicielle SolidFire et Element](#)"
- "[Module d'extension NetApp Element pour vCenter Server](#)"

Modifier le mot de passe IPMI par défaut des nœuds

Vous pouvez modifier le mot de passe administrateur par défaut de l'interface de gestion de plateforme intelligente (IPMI) dès que vous disposez d'un accès IPMI distant au nœud. Vous pourriez vouloir faire cela s'il y a des mises à jour d'installation.

Pour plus de détails sur la configuration de l'accès IPM pour les nœuds, consultez "[Configurer IPMI pour chaque nœud](#)".

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

- Nœuds H410S
- Nœuds H610S

Modifier le mot de passe IPMI par défaut des 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 aurez besoin

Vous auriez dû configurer l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur web sur un ordinateur pouvant accéder au réseau IPMI et accédez à l'adresse IP IPMI du nœud.
2. Saisissez le nom d'utilisateur `ADMIN` et mot de passe `ADMIN` dans l'invite de connexion.
3. Une fois connecté, cliquez sur l'onglet **Configuration**.
4. Cliquez sur **Utilisateurs**.
5. Sélectionnez `ADMIN` utilisateur et cliquez sur **Modifier l'utilisateur**.
6. Cochez la case **Changer le mot de passe**.
7. Saisissez 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 ayant des mots de passe IPMI par défaut.

Modifier le mot de passe IPMI par défaut des 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 aurez besoin

Vous auriez dû configurer l'adresse IP IPMI pour chaque nœud de stockage.

Étapes

1. Ouvrez un navigateur web sur un ordinateur pouvant accéder au réseau IPMI et accédez à l'adresse IP IPMI du nœud.
2. Saisissez le nom d'utilisateur `root` et mot de passe `calvin` dans l'invite de connexion.
3. Une fois connecté, cliquez sur l'icône de navigation du menu en haut à gauche de la page pour ouvrir le panneau latéral.
4. Cliquez sur **Paramètres**.
5. Cliquez sur **Gestion des utilisateurs**.
6. Sélectionnez l'utilisateur **Administrateur** dans la liste.
7. Cochez la case **Changer 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 ayant des mots de passe IPMI par défaut.

Trouver plus d'informations

- ["Documentation logicielle SolidFire et Element"](#)
- ["Module d'extension NetApp Element pour vCenter Server"](#)

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.