Gamme Dell EMC Unity™ Secure Remote Services Requirements and Configuration

Version 5.x

Part Number: 302-002-573
June 2019
Rev. 07

DELL Technologies

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Contents

Préface :

Dans le cadre d'un effort d'amélioration, des révisions régulières des matériels et logiciels sont publiées. Par conséquent, il se peut que certaines fonctions décrites dans le présent document ne soient pas prises en charge par l'ensemble des versions des logiciels ou matériels actuellement utilisés. Pour obtenir les informations les plus récentes sur les fonctionnalités des produits, consultez les notes de mise à jour de vos produits. Si un produit ne fonctionne pas correctement ou ne fonctionne pas comme indiqué dans ce document, contactez un professionnel du support technique .

Obtenir de l'aide

Pour plus d'informations sur le support, les produits et les licences, procédez comme suit :

Informations sur les produits

Pour obtenir de la documentation sur le produit et les fonctionnalités ou les notes de mise à jour, rendez-vous sur la page de Documentation technique Unity à l'adresse dell.com/unitydocs.

Résolution des problèmes

Pour obtenir des informations relatives aux produits, mises à jour logicielles, licences et services, consultez le site Web du support (enregistrement obligatoire) à l'adresse dell.com/support. Une fois que vous êtes connecté, recherchez la page du produit appropriée.

1

Introduction

Ce chapitre présente la fonction EMC Secure Remote Services (ESRS).

Ce document traite des points suivants :

Sujets :

Benefits of ESRS

The embedded ESRS feature in Unity deployments provides a highly secure, remote connection between your Unity environment and Dell EMC. A connection that, once made, can unlock a wide range of benefits and services like:

- Automated health checks.
- 24x7 predictive wellness monitoring.
- Remote issue analysis and diagnosis.
- An enhanced Online Support experience with actionable, real-time data-driven insight into your global Dell EMC environment through the MyService360 dashboard.
- Remote delivery of Dell EMC's service and support.
- CloudIQ, a software-as-a-service cloud management dashboard that provides intelligent analytics about performance, capacity, and configuration for health-based reporting and remediation. ESRS must be enabled on your storage system to send data to CloudIQ.

About remote service options

Three remote service options are available by which to send storage system information to the Support Center for remote troubleshooting:

- Centralized ESRS
- Integrated ESRS (déploiements physiques uniquement) with one of the following types of remote service connectivity options:
  - Outbound/Inbound
  - Outbound only

A fourth option, Disabled, is available but not recommended. If you select this option, the Support Center will not receive notifications about issues with the storage system. You may need to collect system information manually to assist support representatives with troubleshooting and resolving problems with the storage system.

REMARQUE : Before you can configure ESRS, you must specify valid support credentials.

Centralized ESRS

Centralized ESRS runs on a gateway server. When you select this option, your storage system is added to other storage systems in an ESRS cluster. The cluster resides behind a single common (centralized) secure connection between Support Center servers and an off-array ESRS Gateway. The ESRS Gateway is the single point of entry and exit for all IP-based ESRS activities for the storage systems associated with the gateway.

The ESRS Gateway is a remote support solution application that is installed on one or more customer-supplied dedicated servers. The ESRS Gateway functions as a communication broker between the associated storage systems, Policy Manager (optional) and proxy servers (optional), and the Support Center. Connections to the Policy Manager and associated proxy

servers are configured through the ESRS Gateway interface along with add (register), modify, delete (unregister), and querying status capabilities that ESRS clients can use to register with the ESRS Gateway. You can configure a Primary and a Secondary Gateway for ESRS for high availability in the event that one of the gateways is inaccessible. Both gateways must reside on the same cluster to minimize disruption if one gateway fails over to the other.

For more information about ESRS Gateway and Policy Manager, go to the ESRS product page on Online Support (https://Support.EMC.com).

To configure your storage system to use Centralized ESRS, you only need to provide the IP address of the ESRS Gateway and ensure that port 9443 is open between the gateway and the storage system. Also, ensure that port 443 is open (outbound) for network traffic.

REMARQUE : Storage systems can only be added to the ESRS Gateway from Unisphere. If the storage system is added from the gateway server, it will appear to be connected, but will not successfully send system information.

Integrated ESRS (déploiements physiques uniquement)

REMARQUE : La disponibilité de cette fonction dépend de votre mise en œuvre.

Integrated ESRS runs directly on the storage system. When you select this option, you set up the storage system to use a secure connection between itself and the Support Center. You can select one of the following remote service connectivity options for Integrated ESRS:

- Outbound/Inbound, which is the default, from the storage system to the Support Center and from the Support Center to the storage system for remote access using https.
- Outbound only from the storage system to the Support Center using https.

When you select the Outbound/Inbound option, the storage system sets up a secure connection between itself and the Support Center. This option enables remote service connectivity capabilities for remote transfer to and remote transfer from the Support Center with the storage system. Configure the connection from the storage system to a Policy Manager (optional) and any associated proxy servers (optional) through either Unisphere or the CLI.

When you select the Outbound only option, the storage system sets up a secure connection between itself and the Support Center. This option enables remote service connectivity capability for remote transfer to the Support Center from the storage system.

To configure the storage system to use Integrated ESRS, you must:

1. Specify valid support credentials, otherwise, you cannot perform an ESRS readiness check or configure ESRS.
2. Run a readiness check (optional, but highly recommended).
3. If you skipped the readiness check, accept the license agreement for the feature.
4. Run the network check.

   REMARQUE : Several ports need to be allowed by your firewall/network setting for the network check and ESRS functionality. Ports 443 and 8443 are required for outbound connections while ports 80 and 443 are required for inbound connections. Also, if the settings that appear for the global proxy server need to be changed, edit the settings then run the network check.
5. For Outbound/Inbound remote service connectivity, you must specify the required customer contact data for the storage system if it has not been specified. This step is not applicable to Outbound only remote service connectivity.
6. Request an access code for verification through email (an extra level of authentication) and submit the access code for validation to continue the ESRS enabling process.
7. Check the status of the system's ESRS connection to the Support Center.
8. For Outbound/Inbound remote service connectivity, configure the Policy Manager (if an additional layer of security is required). The Policy Manager requires port 8090 (default) or the customer-specified port to be open for outgoing traffic. If it is configured to use SSL, port 8443 must be open.
9. Specify whether to send data to CloudIQ.

When Outbound only is the current ESRS configuration on the storage system, you can modify the proxy server information, if applicable, and change the remote service connectivity option to Outbound/Inbound. Changing the remote service connectivity option to Outbound/Inbound also requires you to specify the customer contact data for the storage system if it has not been specified and, if required, to configure the Policy Manager.

When Outbound/Inbound is the current ESRS configuration on the storage system, you can modify the proxy server information, if applicable, and the contact and system information. However, you cannot change the remote service connectivity option from Outbound/Inbound to Outbound only, that change is not supported.

Operational description

The ESRS feature provides an IP-based connection that enables Support to receive error files and alerts from your storage system, and to perform remote troubleshooting resulting in a fast and efficient time to resolution.

REMARQUE : It is strongly recommended that you enable the ESRS feature to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not enable ESRS, you may need to collect system information manually to assist Support with troubleshooting and resolving problems with your storage system. ESRS must be enabled on the system for data to be sent to CloudIQ.

ESRS and security

ESRS employs multiple security layers throughout each step in the remote connectivity process to ensure that you and Support can use the solution with confidence:

- All notifications originate from your site—never from an outside source— and are kept secure through the use of Advanced Encryption Standard (AES)-256 bit encryption
- IP-based architecture integrates with your existing infrastructure and maintains the security of your environment
- Communications between your site and the Support Center are bilaterally authenticated using RSA® digital certificates
- Only authorized Customer Service professionals verified via two-factor authentication can download the digital certificates needed to view a notification from your site
- The optional ESRS v3 Policy Manager application, which is only applicable to Integrated ESRS with Outbound/Inbound connectivity, enables you to grant or restrict Support access based on your own unique guidelines and requirements, and includes a detailed audit log

ESRS management

You can manage ESRS using Unisphere, UEMCLI, or the REST API. You can enable or disable the service, change the settings for the global proxy server, set up a Policy Manager (déploiements physiques uniquement), and provide your Full-access support account credentials which are necessary for ESRS to work.

The storage system itself does not implement any policies. If you require more control over remote access to your storage system, you can use a Policy Manager (applicable to Integrated ESRS with Outbound/Inbound connectivity) to set authorization permissions. The Policy Manager software component can be installed on a customer-supplied server. It controls remote access to your devices, maintains an audit log of remote connections, and supports file transfer operations. You can control by whom, what, and when access to your storage system occurs. For more information about the Policy Manager, go to the Online Support website (https://support.emc.com/). After logging in, locate the applicable product page and search for the link to the specific ESRS product technical documentation.

The integrated ESRS feature (déploiements physiques uniquement) is embedded in the operating environment (OE) of the storage system as a managed service. La disponibilité de cette fonction dépend de votre mise en œuvre. The integrated implementation includes the High Availability (HA) feature, which provides monitoring of ESRS and is responsible for failing it over from the primary storage processor (SP) to the backup SP should the primary SP fail. HA is responsible for restarting ESRS if it fails. The OE is responsible for persisting the configuration and certificates that are needed for ESRS to work.

Centralized ESRS allows you to configure both a Primary gateway and a Secondary gateway to allow for high availability (HA) within the VE cluster on the network. If the primary gateway goes down, the Unity system will automatically fail over to the secondary gateway on the network for ESRS and Cloud IQ connectivity. Configuration of the primary gateway is mandatory, while configuration of the secondary gateway is optional.

REMARQUE : Once the Primary and Secondary gateway have been configured for Centralized ESRS, you cannot change the primary gateway to the secondary gateway. In order to do this, you must disable and then reenable Centralized ESRS with the appropriate gateway order.

ESRS is supported in full service mode (both SPs are in service mode). If you have already enabled ESRS, the system functions as configured. If you have not enabled ESRS, you can temporarily enable it. In this latter situation, the configuration will not persist once your storage system has recovered to normal operation.

ESRS communication

Access to a DNS server is required for ESRS to work.

By default, ESRS attempts to use a configured proxy server to communicate with Support Center back-end systems. If the proxy server is not available, ESRS attempts to bypass the proxy server and communicate directly to the Support Center back-end systems.

2

Conditions requises et configuration

Ce chapitre décrit les conditions requises pour la fonction ESRS et fournit une description du fonctionnement de la fonction. Ce chapitre décrit également les processus pour provisionner la fonction.

Ce document traite des points suivants :

Sujets :

Prerequisites for ESRS

As prerequisites for enabling ESRS on the storage system, you must have the following:

- Operating environment (OE) version 4.0 or later.
- At least one DNS server must be configured on the storage system.
- Unrestricted access to Support Center (https://support.emc.com/) over the Internet using HTTPS (for non-proxy environments).
- Online Support Full-access account (requires specific credentials that are associated with the site ID, which is associated with the system serial number).

  REMARQUE : If there is a problem with your Online Support account, Support personnel can help you configure ESRS using their RSA credentials.
- Do not use dynamic IP addresses (DHCP) for any components of the ESRS Gateway servers, Policy Manager servers, or managed devices.
- Network traffic over port 443 is required for ESRS functionality and is required for remote support personnel to perform many break/fix tasks using ESRS.
- SSL checking, certificate verification, and certificate proxying are not permitted for ESRS network traffic.

REMARQUE : If you use DHCP to assign IP addresses to any ESRS components (ESRS Gateway servers, Policy Manager servers, or managed devices), they must have static IP addresses. Leases for the IP addresses that those devices use cannot be set to expire. It is recommended that you assign static IP addresses to those devices you plan to have managed by ESRS.

Conditions requises pour Integrated ESRS

Les conditions suivantes sont liées à l'implémentation du support à distance sécurisé EMC (ESRS) uniquement :

- Le trafic réseau (HTTPS) doit être autorisé sur les ports 443 et 8443 (sortant) vers le Centre de support. L'échec de l'ouverture du port 8443 entraîne des répercussions importantes sur les performances (30 à 45 %). L'échec de l'ouverture des deux ports peut entraîner un retard dans la résolution des problèmes avec le terminal.
- Si l'implémentation d'ESRS inclut un Policy Manager pour plus de contrôle sur l'accès à distance au système de stockage, vous devez l'indiquer lors de la configuration d'ESRS.

  REMARQUE : Un Policy Manager s'applique uniquement au Support à distance sécurisé EMC intégré avec connectivité sortante/entrante.
- Si l'implémentation d'ESRS inclut un serveur proxy pour la connexion du système de système à Policy Manager, vous devez l'indiquer lors de la configuration d'ESRS.

Configuration requise pour Centralized ESRS

Les conditions suivantes sont uniquement liées à l'implémentation du support à distance sécurisé EMC centralisé :

- Le trafic réseau (HTTPS) doit être autorisé sur le port 9443 entre le système Unity et le serveur ESRS Gateway. En outre, le trafic réseau sur le port 443 est requis pour les fonctionnalités ESRS.
- La version de l'environnement d'exploitation du serveur de passerelle ESRS doit être la version 3.12.00.04 ou version ultérieure.

REMARQUE : N'ajoutez ou ne supprimez jamais de système Unity manuellement à partir d'un serveur ESRS Gateway. Pour ajouter ou supprimer un système de stockage à partir d'un serveur de passerelle, utilisez uniquement l'Assistant de configuration Unisphere ESRS.

Compte à accès complet au support en ligne Dell EMC

La configuration d'ESRS sur un système de stockage exige un compte actif avec accès complet sur le site Web de support en ligne Dell EMC. Ce compte associe des informations d'identification particulières à un domaine e-mail et une organisation spécifiques. Lorsque vous configurez ESRS sur le système de stockage, vous devez spécifier ces informations d'identification (nom d'utilisateur + mot de passe) afin d'activer le canal de communication ESRS pour le système.

Lors de la vérification de la préparation d'ESRS, vous pouvez recevoir un message indiquant que vos informations d'identification du support ne sont pas associées à un compte client. Cela peut indiquer que vous devez effectuer une mise à niveau à partir d'un compte à accès limité (Lite) vers un compte à accès complet. Reportez-vous aux étapes ci-dessous pour plus d'informations sur la mise à niveau vers un compte à accès complet. Dans le cas contraire, vous devrez peut-être contacter votre fournisseur de services pour des problèmes liés à l'enregistrement de vos informations d'identification du support.

REMARQUE : La prise en charge de l'accès complet est fourni uniquement pour les clients disposant d'un support en ligne directe.

Création d'un compte initial de support en ligne

Lorsque vous créez un compte initial de support en ligne, il est possible que lui soient rattachés des privilèges limités et qu'il ne soit pas associé à un profil de société. À moins que votre société possède un profil établi sur le site de Support en ligne, le compte est créé avec une adresse e-mail, un nom d'utilisateur et un mot de passe, mais sans affiliation à votre société. Lorsque vous créez le compte, vous recevez un e-mail de confirmation contenant un lien de validation. Vous pouvez cliquer sur le lien, vous connecter au site Web de support en ligne, activer votre compte et, s'il s'agit d'un compte à accès limité (appelé « Lite »), vous pouvez, si vous le souhaitez, demander sa mise à niveau pour que lui soient rattachés des privilèges d'accès complet.

REMARQUE : Les privilèges de compte à accès limité sont suffisants pour enregistrer des systèmes de stockage et leur attribuer des licences. En revanche, vous ne pouvez pas configurer ESRS pour un système de stockage à l'aide d'un compte qui ne dispose que de privilèges d'accès limité.

Mise à niveau vers des privilèges d'accès complet

Si votre compte de support en ligne a été initialement activé avec des privilèges à accès limité, vous pouvez formuler une demande pour que lui soient rattachés des privilèges d'accès complet.

Si votre organisation possède déjà un profil de société sur le site Web de support en ligne, vous pouvez être invité à sélectionner votre ID de site (emplacement) dans la liste des ID proposés, après quoi vous serez associé à votre société et pourrez configurer le service ESRS sur votre système de stockage.

Pour créer un nouveau profil client sur le site Web de support en ligne, vous devez fournir les informations suivantes :

Informations requises	Description
Relations avec Dell EMC	Indiquez si votre organisation est un partenaire, fournisseur ou client de produits Dell EMC.
Identifiant du site (physique)	Sélectionnez un identifiant de site existant (si vous en avez déjà créé un pour votre organisation) ou sélectionnez votre organisation dans une base de données de profils d'organisation.

REMARQUE : L'adresse e-mail associée au compte initial à accès limité devient le domaine e-mail d'entreprise associé au nouveau profil client.

Si vous avez fourni les informations requises sur votre société lors de la validation de votre compte à accès limité, votre demande sera traitée sous 24 à 48 heures. Vous recevrez alors un e-mail pour confirmer la mise à niveau et l'attribution au compte de privilèges d'accès complet. L'e-mail contient un lien de validation sur lequel vous devez cliquer pour vous connecter et activer les privilèges d'accès complet sur le système de support en ligne.

Après avoir activé des privilèges d'accès complet pour votre support en ligne, vous pouvez utiliser les informations d'identification du compte pour configurer la fonction ESRS sur les systèmes de stockage associés à votre organisation.

Mode de configuration du Support à distance sécurisé EMC (ESRS)

Dans Unisphere, vous pouvez configurer le support à distance pour un système de stockage en utilisant l'une des méthodes suivantes :

- Assistant Configuration initiale—Assistant pour configurer l'ensemble des paramètres du système de stockage qui est exécuté la première fois que vous accédez au système avec Unisphere.
- Page Présentation—Service pour le système de stockage accessible à partir d'Unisphere (**Système** > **Service** > **Présentation**).
- ESRS—Page des paramètres ESRS accessible à partir de Unisphere (**Paramètres** > **Configuration du support**).
- UEMCLI—Interface de ligne de commande qui inclut des commandes que vous pouvez exécuter sur un système via une invite depuis un hôte Microsoft Windows ou UNIX/Linux pour configurer les paramètres ESRS. Pour obtenir des informations sur les commandes CLI associées à ESRS, reportez-vous au *Guide d'utilisation de l'interface de ligne de commande Unisphere*.
- Serveur d'API REST Unisphere Management—Interface de l'application qui peut recevoir des demandes des API REST pour configurer les paramètres ESRS. Pour plus d'informations sur l'API REST Unisphere Management, reportez-vous au *Guide de programmation avec l'API REST Unisphere Management*.

Pour déterminer l'état de la fonction ESRS, dans Unisphere, accédez à **Système** > **Service** > **Présentation**. ESRS est activé lorsqu'une coche apparaît dans un cercle vert sous **Services à distance sécurisés EMC**.

Lorsque vous activez la fonction ESRS sur un système de stockage, configurez les paramètres suivants :

REMARQUE : Vous devez spécifier des informations d'identification du support valides (nom d'utilisateur et mot de passe associés à un compte de Support en ligne actif doté des privilèges d'accès complet) pour être en mesure de configurer ESRS.

- ESRS—Type du support à distance sécurisé EMC (ESRS), centralisé ou intégré (avec connectivité sortante/entrante ou sortante uniquement), que le système de stockage utilisera. Bien que vous puissiez désactiver la fonction ESRS, cela n'est pas recommandé.
- Contrat de licence (Support à distance sécurisé EMC intégré uniquement)—Les conditions générales d'utilisation du Support à distance sécurisé EMC (ESRS) doivent être acceptées afin de configurer et d'utiliser le Support à distance sécurisé EMC intégré.
- Vérification réseau (facultative, les paramètres n'apparaissent que pour le Support à distance sécurisé EMC intégré)—Valide la préparation du réseau pour la configuration d'ESRS et, le cas échéant, permet de modifier les informations du serveur proxy global :
  - Protocole : protocole permettant de communiquer avec un serveur proxy utilisé pour le canal de communication. Les options disponibles sont HTTP sur le port 3128 (port par défaut) et SOCKS (protocole par défaut) sur le port 1080 (port par défaut).

    REMARQUE : La sélection du protocole SOCKS ou HTTP ajoute automatiquement le port par défaut associé à l'adresse du serveur proxy. Si nécessaire, vous pouvez spécifier un port différent via Unisphere, ou des commandes UEMCLI ou REST.
  - Adresse du serveur proxy : adresse réseau à associer au trafic du serveur proxy global.

    REMARQUE : La modification de la sélection du protocole après avoir spécifié une adresse IP change automatiquement le port ajouté à la valeur par défaut du protocole, à moins qu'un port autre que le port par défaut ait été spécifié via des commandes UEMCLI ou REST.
  - Informations d'identification : nom d'utilisateur et mot de passe d'un compte utilisé pour accéder au système de serveur proxy.

- Informations de contact et d'emplacement du système (les paramètres n'apparaissent que pour le Support à distance sécurisé EMC intégré avec connectivité sortante/entrante)—Informations modifiables que le Support utilisera pour répondre à vos problèmes.
- Vérification par email—Demande de code d'accès puis authentification de l'adresse email.
- Informations relatives au Policy Manager (facultatives, les paramètres n'apparaissent que pour le Support à distance sécurisé EMC intégré avec connectivité sortante/entrante)—Informations relatives au Policy Manager pour le canal de communication ESRS :
  - Protocole : protocole permettant de communiquer avec un système Policy Manager utilisé pour le canal de communication ESRS.
  - Adresse du serveur proxy : adresse réseau et numéro de port à associer au trafic du serveur de règles.
- Informations sur le serveur proxy associé au Policy Manager (facultatives, les paramètres n'apparaissent que pour le Support à distance sécurisé EMC intégré avec connectivité sortante/entrante)—Si un Policy Manager est utilisé, serveur proxy utilisé par le Policy Manager pour la fonction ESRS :
  - Protocole : protocole utilisé pour communiquer avec un serveur proxy utilisé par le Policy Manager.
  - Adresse du serveur proxy : adresse réseau et numéro de port à associer au serveur proxy utilisé par le serveur de règles.
  - Informations d'identification : nom d'utilisateur et mot de passe d'un compte utilisé pour accéder au serveur proxy utilisé par le Policy Manager.
- Envoyer des données à CloudIQ (la case à cocher n'apparaît que pour le Support à distance sécurisé EMC intégré et elle est cochée par défaut. Décochez la case pour désactiver l'envoi de données à CloudIQ [non recommandé])—CloudIQ est un tableau de bord SaaS pour la gestion du Cloud qui offre une analytique intelligente sur les performances, la capacité et la configuration afin de proposer un reporting sur l'état du système et les mesures correctives.

  REMARQUE : CloudIQ est activé par défaut lorsque le support ESRS centralisé est activé. Pour désactiver ou réactiver CloudIQ pour le support ESRS centralisé, dans Unisphere, accédez à **Paramètres** > **Configuration du support** > **CloudIQ**.

Serveur proxy (Support à distance sécurisé EMC intégré uniquement)

Les paramètres du serveur proxy pour le système ont déjà été configurés dans le cadre de la configuration initiale du système. Vérifiez ces paramètres lors de la configuration d'une implémentation Integrated ESRS et apportez les modifications nécessaires.

Policy Manager (Support à distance sécurisé EMC intégré avec connectivité sortante/entrante uniquement)

Si le système de stockage utilise un Policy Manager pour définir des autorisations, vous devez l'indiquer lors de la configuration d'ESRS. Si le Policy Manager est amené à utiliser un serveur proxy pour se connecter à votre système de stockage, vous devez également l'indiquer lors de la configuration d'ESRS. Si le serveur proxy du Policy Manager exige une authentification (SOCKS est uniquement pris en charge avec une authentification), vous devez également l'indiquer lors de la configuration d'ESRS et fournir des informations d'identification de connexion pour le serveur proxy. Vous devez fournir à la fois un nom d'utilisateur et un mot de passe à des fins d'authentification.

Pour plus d'informations sur Policy Manager, consultez le *Guide des opérations Secure Remote Services Policy Manager* sur le site Web de support (https://Support.EMC.com).

3

Configurer le support à distance à l'aide de Unisphere

Ce chapitre décrit les processus permettant de provisionner la fonction ESRS à l'aide de l'interface Unisphere.

Ce document traite des points suivants :

Sujets :

Configurer le support à distance

Prérequis

Si votre environnement informatique requiert que le système de stockage se connecte via un serveur proxy, vérifiez la configuration du serveur proxy avant de continuer en passant en revue la page **Paramètres** > **Configuration du support** > **Serveur proxy**.

À propos de cette tâche

Pour configurer le support à distance à l'aide de Unisphere, procédez comme suit :

Étapes

1. Sélectionnez l'icône **Paramètres**, puis sélectionnez **Configuration du support**.
2. Si vos informations d'identification ne sont pas déjà spécifiées, sélectionnez **Informations d'identification du Support** pour spécifier vos informations d'identification de support, votre nom d'utilisateur et votre mot de passe. Sinon, passez à l'étape suivante.

   Si vous ne spécifiez pas les informations d'identification du support valides, vous ne pourrez pas configurer le support à distance sécurisé EMC, afficher des informations sur les contrats de support, ni accéder aux pages de produits du support en ligne.
3. Sélectionnez **Services à distance sécurisés EMC**.

   Il est recommandé d'exécuter une vérification de préparation avant de configurer ESRS pour déterminer si ESRS peut être configuré. Pour contourner la vérification de la préparation, il suffit de cliquer sur **Configurer** et d'accéder à l'étape 6.
4. Cliquez sur **Vérification de la préparation**.
5. Dans **Vérification de la préparation d'ESRS**, sélectionnez l'option ESRS que vous préférez utiliser.

Option	Description
Integrated (déploiements physiques uniquement)	Avant l'exécution de la vérification de la préparation, le contrat de licence utilisateur final ESRS (EULA ESRS) doit être accepté. Une fois le contrat de licence accepté, cliquez sur **Suivant** pour exécuter la vérification. **REMARQUE :** Une fois le contrat de licence accepté, il n'apparaît plus.
Centralized	Avant l'exécution de la vérification de disponibilité, la version minimale requise du logiciel de la passerelle du serveur s'affiche, et l'adresse réseau de la passerelle doit être saisie. Après la saisie de l'adresse réseau de la passerelle, cliquez sur **Suivant** pour exécuter la vérification.

Après l'exécution de la vérification de disponibilité, l'une des opérations suivantes se produit :

- Si aucune erreur n'est détectée, un cercle vert avec une coche et un message de réussite s'affichent. Cliquez sur **Configurer ESRS** puis accédez à l'étape 6 pour poursuivre la configuration d'ESRS, ou cliquez sur **Fermer** pour revenir aux **Paramètres** d'ESRS et poursuivre la configuration ultérieurement.
- Si des erreurs apparaissent, vous devez soit résoudre les problèmes et cliquer sur **Nouvelle vérification** pour assurer la configuration d'ESRS, soit cliquer sur **Fermer** et résoudre les problèmes plus tard.

6. Dans **Configurer ESRS**, spécifiez les informations sur les options ESRS appropriées.

Option	Description
Support centralisé : surveillance avec une configuration des services ESRS centralisés	a. Spécifiez l'**adresse réseau de passerelle principale** du serveur ESRS Gateway qui est utilisé pour se connecter à EMC et assurez-vous que le port 9443 est ouvert entre le serveur Gateway et le système de stockage. **REMARQUE :** Les informations d'identification RSA peuvent être utilisées pour les configurations de passerelle principale sans compte de support client. Cela permet de configurer un support à distance sécurisé EMC centralisé, tandis que les informations d'identification du compte de support sont créées et validées sur le back-end. b. Vous pouvez également saisir **adresse réseau de passerelle secondaire** pour la haute disponibilité (HA) ESRS. La deuxième passerelle doit être configurée dans le même cluster HA ESRS que **l'adresse réseau de la passerelle principale**. **REMARQUE :** Si les informations d'identification RSA ont été utilisées pour la passerelle principale, elles doivent également être fournies pour effectuer la configuration d'une passerelle secondaire. **REMARQUE :** CloudIQ est activé par défaut lorsque le support ESRS centralisé est activé. Pour désactiver ou réactiver CloudIQ pour Centralized ESRS, dans Unisphere, accédez à **Paramètres** > **Configuration du support** > **CloudIQ**.
Support intégré : surveillance avec ce client ESRS intégré au système de stockage (déploiements physiques uniquement)	La disponibilité de cette fonction dépend de votre mise en œuvre. Vous devez passer par le processus de configuration d'ESRS et accepter les conditions générales d'utilisation d'ESRS. Vous pouvez choisir la connectivité sortante uniquement ou sortante/entrante avec votre fournisseur de services à distance et si vous souhaitez envoyer des données à CloudIQ. L'utilisation de Policy Manager et des serveurs proxy est facultative et applicable uniquement lorsque vous sélectionnez les services ESRS intégrés avec la connectivité sortante/entrante. Une fois sélectionnée, vous pouvez configurer un Policy Manager et les paramètres du serveur proxy. **REMARQUE :** (Les conditions générales d'utilisation d'ESRS n'apparaissent pas après leur acceptation dans le cadre de la procédure de vérification de la préparation.)
Ne pas activer les services distants	Il n'est pas recommandé de ne pas activer les services à distance. L'activation des Services à distance accélère le diagnostic des problèmes et leurs délais de résolution.

Étapes suivantes

Testez toujours la connectivité après la configuration d'ESRS. Ce processus vérifie que la connexion fonctionne et qu'elle permet à EMC Enterprise de reconnaître le système et de mettre à jour son état qui ne sera plus Inconnu. Cliquez sur **Tester** à l'un des emplacements suivants :

- **Tableau de bord** > **Système** > **Service** sous **EMC Secure Remote Services**
- **Paramètres** > **Configuration du support** > **EMC Secure Remote Services**

Si vous devez modifier (réapprovisionner) les informations relatives à la configuration d'ESRS, sélectionnez **Modifier**. L'assistant **Configurer ESRS** s'affiche pour vous permettre d'apporter les modifications nécessaires.

REMARQUE : Si l'état affiché est toujours **En cours de transition** et ne change pas après quelques minutes (temps nécessaire au test de connectivité), contactez le Support en ligne.

Configurer les Services à distance sécurisés EMC intégrés (déploiements physiques uniquement)

Prérequis

La fonction **ESRS intégrés** est sélectionnée dans les **Services à distance sécurisés EMC (ESRS)** et l'assistant **Configurer ESRS** apparaît à l'écran.

À propos de cette tâche

Pour effectuer la configuration des Services à distance sécurisés EMC intégrés, procédez comme suit :

Étapes

1. Acceptez les conditions générales d'utilisation d'ESRS.

   Les conditions générales d'utilisation d'ESRS doivent être acceptées avant de pouvoir configurer et utiliser les Services à distance sécurisés EMC intégrés.

   REMARQUE : Si le contrat de licence a été accepté pendant la vérification de la préparation, avant de configurer ESRS, le contrat de licence ne réapparaît pas.

2. Lancez une vérification du réseau. Si un serveur proxy a été configuré pour le système de stockage, vous pouvez apporter des modifications, si nécessaire, en cliquant sur l'icône représentant un crayon en regard **Se connecter via un serveur proxy**, puis renseignez les informations appropriées dans la boîte de dialogue qui s'affiche.

   REMARQUE : Les modifications effectuées sur cette page s'appliquent aux paramètres de proxy global du système de stockage.

   Après avoir envoyé la page Vérification réseau et saisi les détails du serveur, des tests réseau sont effectués pour vérifier la connectivité entre le périphérique et le nœud principal. Si vous avez sélectionné les services ESRS intégrés avec la connectivité sortante/entrante, les serveurs GAS (Global Access Servers) sont également inclus dans les tests de réseau. La connectivité réseau entre ESRS et tous les serveurs EMC back-end est vérifiée. En cas d'échec des tests, ce qui signifie que le périphérique ne peut pas se connecter à certains ou à tous les serveurs back-end, les résultats s'affichent en haut de la page de l'assistant. Dans ce cas, vérifiez que les hôtes et les ports (443 et 8443) du pare-feu appropriés sont ouverts pour les serveurs back-end. Tous les tests doivent être concluants. Vous êtes chargé de résoudre les problèmes liés au pare-feu et serveur proxy ayant un impact sur la connectivité avec l'infrastructure ESRS.

3. Vérifiez les coordonnées des clients. (Cette vérification n'apparaît et ne s'applique que lorsque vous avez sélectionné les services ESRS intégrés avec la connectivité sortante/entrante.)

   Pour ajouter ou modifier les coordonnées des clients, cliquez sur l'icône représentant un crayon en regard de **Coordonnées** et fournissez les informations appropriées dans la boîte de dialogue qui s'affiche. Ces informations sont nécessaires pour poursuivre la configuration d'ESRS. Vérifiez l'exactitude des informations, car le Support les utilise pour répondre à vos problèmes.

4. Effectuez la procédure de vérification par e-mail.

   Cette étape ajoute un niveau d'authentification supplémentaire et permet de vérifier que vous êtes l'utilisateur approprié et autorisé à activer ESRS sur le système de stockage.

   a. Sélectionnez **Envoyer le code d'accès** pour effectuer une demande de code d'accès.

      Le code d'accès généré est un code PIN à 8 chiffres valable 30 minutes à partir du moment où il a été généré. L'assistant doit être exécuté durant cette période. Si vous resélectionnez **Envoyer le code d'accès** pendant les 30 minutes de procédure, le code précédent sera automatiquement invalidé, et vous devrez utiliser le code le plus récent.

      Le code d'accès est ensuite envoyé à l'adresse e-mail associée aux informations d'identification du compte de support. Un message s'affiche en haut de la page pour vous inviter à consulter votre messagerie électronique.

   b. Dans le champ **Code d'accès**, saisissez le code d'accès que vous avez reçu par e-mail.

      Si vous rencontrez des problèmes au cours de cette procédure de vérification par e-mail ou au niveau de la configuration du compte de support, le personnel de support peut sélectionner l'option **Alternative pour le personnel de support uniquement** et utiliser ses propres informations d'identification RSA, auquel cas la procédure de vérification par e-mail sera ignorée.

      Si les informations d'identification du support RSA sont utilisées, la deuxième fenêtre pop-up s'affichera, afin d'inviter le personnel du support technique à saisir à nouveau les informations d'identification du support RSA.

5. (Facultatif, ne s'applique que lorsque vous avez sélectionné le support à distance sécurisé EMC intégré.) Si votre système de stockage utilise un Policy Manager pour définir des autorisations, sélectionnez **Policy Manager** et renseignez les

informations appropriées pour le Policy Manager. Si le Policy Manager utilise un serveur proxy, sélectionnez **Utiliser le serveur proxy pour Policy Manager** et renseignez les informations correspondant au serveur proxy. Si vous n'allez pas utiliser de Policy Manager, passez à l'étape 6.
La boîte de dialogue **Policy Manager** s'affiche. Si vous utilisez le Policy Manager, il doit être installé et opérationnel. Il est recommandé d'utiliser une connexion SSL de niveau élevé.

6. La case **Envoyer des données à CloudIQ** est cochée (activée) par défaut. Décochez la case pour désactiver l'envoi de données à CloudIQ (non recommandé).

   CloudIQ peut être activé ou désactivé à la fin de la configuration ESRS via **Paramètres** > **Configuration du support** > **CloudIQ**.

   Une fois ESRS correctement configuré, les certificats adéquats sont installés, ESRS est provisionné et enregistré dans le Centre de support, et la page **Résultats** s'affiche.
7. Vérifiez le panneau **Présentation** de la page **Service** (**Tableau de bord** > **Système** > **Service**) pour afficher l'état de la connexion ESRS.

Étapes suivantes

Testez toujours la connectivité après la configuration d'ESRS. Ce processus vérifie que la connexion fonctionne et qu'elle permet à EMC de reconnaître le système et de mettre à jour son état actuel qui ne sera plus Inconnu. Cliquez sur **Tester** à l'un des emplacements suivants :

- **Tableau de bord** > **Système** > **Service** sous **EMC Secure Remote Services**
- **Paramètres** > **Configuration du support** > **EMC Secure Remote Services**

REMARQUE : Si l'état affiché est toujours en cours de transition et ne change pas après 20 minutes (temps nécessaire au test de connectivité), contactez le Support.

REMARQUE : Policy Manager peut être configuré ou modifié après la configuration d'ESRS en cliquant sur **Modifier**, sur la page **Paramètres** > **Configuration du support** > **EMC Secure Remote Services**.

Si vous devez modifier (réapprovisionner) les informations relatives à la configuration d'ESRS, sélectionnez **Modifier**. L'assistant **Configurer ESRS** s'affiche pour vous permettre d'apporter les modifications nécessaires.

- Pour les services ESRS intégrés avec la connectivité sortante uniquement :
  - Si un serveur proxy a été configuré pour le système de stockage, vous pouvez apporter des modifications, si nécessaire, en cliquant sur l'icône représentant un crayon en regard **Se connecter via un serveur proxy**, puis renseignez les informations appropriées dans la boîte de dialogue qui s'affiche.
  - Vous pouvez modifier le type de support à distance sécurisé EMC sur intégré (connectivité sortante/entrante) ou centralisé, puis spécifier les informations applicables.
- Pour les services ESRS intégrés avec la connectivité sortante/entrante :
  - Si un serveur proxy a été configuré pour le système de stockage, vous pouvez apporter des modifications, si nécessaire, en cliquant sur l'icône représentant un crayon en regard **Se connecter via un serveur proxy**, puis renseignez les informations appropriées dans la boîte de dialogue qui s'affiche.
  - Le panneau d'informations **Vérifier les coordonnées et l'emplacement du système** dans l'Assistant ESRS est activé avec une option de modification (icône représentant un crayon) en regard des **Informations de contact** et des **Informations système**. Les informations relatives au système peuvent être mises à jour à l'exception du numéro d'identifiant du site.
  - Vous pouvez modifier le type de support à distance sécurisé EMC et le faire passer d'intégré (connectivité sortante/entrante) à centralisé et spécifier les informations applicables.

    REMARQUE : Une fois le support à distance sécurisé EMC intégré configuré pour la connectivité entrante/sortante, il ne peut pas être redéfini sur la connectivité sortante uniquement.

4

Configurer le support à distance à l'aide de l'interface de ligne de commande

Ce chapitre décrit les processus permettant de provisionner la fonction ESRS à l'aide d'UEMCLI. Pour obtenir une documentation complète de ces commandes et des commandes associées, consultez le *Guide d'utilisation de l'interface de ligne de commande Unisphere*.

Ce document traite des points suivants :

Sujets :

Overview of configuring Remote Support using the CLI

Users have the option to provision Integrated ESRS with the UEMCLI.

Prérequis

This topic provides an overview of the chronological steps required for configuring ESRS using the CLI. Refer to the subsequent sections of this chapter for the detailed command usage and examples for each of these steps.

Étapes

1. Optionally, configure the use of a proxy server with the `/sys/support/config set` command.
2. Set the Customer Contact Data Information using the `/sys/info set` command.
3. Set your support account credentials using the `sys/support/account set` command.
4. Enable and configure the type of ESRS you want to use:
   a. For Centralized ESRS:
      i. Enable ESRS and configure settings using the `/sys/support/esrsc set` command.
      ii. Check the network connectivity from the primary or secondary Centralized ESRS gateway to the Dell EMC servers using the `/sys/support/esrsc checkNetwork` command.
      iii. After Centralized ESRS is enabled, test the configuration by sending a test Call Home to Dell EMC using the `/sys/support/esrsc test`command.
   b. For Integrated ESRS:
      i. Check that the support account associated with your system is configured and ready for ESRS connectivity using the `/sys/support/esrsi checkSupportAccountReadiness` command.
      ii. Check the network connectivity from the Integrated ESRS client to the Dell EMC servers using the `/sys/support/esrsi checkNetwork` command.
      iii. Enable ESRS and configure settings using the `/sys/support/esrsi set` command. This command allows you to accept the EULA and select the type of Integrated ESRS--one-way or two-way.
      iv. Optionally request an access code to be sent to the email account user using the `/sys/support/esrsi requestAccessCode` command.

REMARQUE : The access code is for additional verification purposes and expires after 30 minutes.

v. If you requested an access code, validate the access code you received using the `/sys/support/esrsi validateAccessCode -accessCode` command.

vi. Test the ESRS configuration using the `/sys/support/esrsi test`command.

5. Optionally, configure the Policy Manager and policy proxy server attributes using the `/sys/support/esrsi/policymgr set` command.

Configurer ou modifier les paramètres de support et de serveur proxy

Modifier les attributs de configuration du support.

Format

```
/sys/support/config set [-enableSupportProxy {yes | no }] [-supportProxyAddr <value>]
[-supportProxyPort <value>] [-supportProxyUser <value> {-supportProxyPasswd <value> |-
supportProxyPasswdSecure}] [-supportProxyProtocol {http | socks}] [-autoUpdateContracts
{yes | no}] [-enableCloudMgmt {yes | no}]
```

Qualificateurs d'action

Qualificateur	Description
`-enableSupportProxy`	Indique si le serveur proxy doit être activé ou désactivé. Les valeurs autorisées sont les suivantes : • `yes` • `no`
`-supportProxyAddr`	Spécifier le nom ou l'adresse IP du serveur proxy des services de support.
`-supportProxyPort`	Spécifier le port du serveur proxy des services de support.
`-supportProxyUser`	Spécifier le nom d'utilisateur d'un compte sur le serveur proxy des services de support.
`-supportProxyPasswd`	Spécifier le mot de passe du compte du serveur proxy des services de support.
`-supportProxyPasswdSecure`	Spécifie le mot de passe en mode sécurisé : l'utilisateur est invité à saisir le mot de passe.
`-supportProxyProtocol`	Spécifier le protocole utilisé pour les communications avec le serveur proxy du support. Les valeurs autorisées sont les suivantes : • `http` • `socks` **REMARQUE :** Les valeurs sont sensibles à la casse.
`-autoUpdateContracts`	Spécifier si le système doit mettre automatiquement à jour sa liste de contrats de service une fois par semaine. Les valeurs autorisées sont les suivantes : • `yes` • `no` **REMARQUE :** Les valeurs sont sensibles à la casse.
`-enableCloudMgmt`	Spécifiez si l'envoi de données à CloudIQ est activé sur le système. Les valeurs autorisées sont les suivantes : • `yes` • `no` **REMARQUE :** Les valeurs sont sensibles à la casse.

Exemple

La commande suivante spécifie les paramètres du serveur proxy des services de support :

```
uemcli /sys/support/config set -supportProxyAddr 10.0.0.1 -supportProxyPort 8080
-supportProxyUser user1 -supportProxyPasswd password123 -supportProxyProtocol http
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Configurer ou modifier les informations de contact du système

Saisir ou modifier les attributs du système et des informations de contact.

Format

```
/sys/info set [-location <value>] [-contactFirstName <value>] [-contactLastName <value>] [-
contactEmail <value>] [-contactPhone <value>] [-contactMobilePhone <value>]
```

Qualificateurs d'action

Qualificateur	Description
-location	Spécifiez un nom d'emplacement mis à jour.
-contactEmail	Spécifiez la nouvelle adresse e-mail du contact du système.
-contactPhone	Spécifiez le nouveau numéro de téléphone du contact du système.
-contactMobilePhone	Spécifiez le nouveau numéro de téléphone portable du contact du système.
-contactFirstName	Spécifiez le nouveau prénom du contact du système.
-contactLastName	Spécifiez le nouveau nom du contact du système.

Exemple

La commande suivante modifie les informations suivantes du système :

- Prénom du contact
- Nom du contact
- E-mail du contact
- N° de téléphone du contact
- Emplacement système
- Numéro de téléphone portable du contact

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/info set -contactFirstName Zach
-contactLastName Arnold -contactEmail something@someemail.com -contactPhone 1233456789
-location here -contactMobilePhone 987654321
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Configurer ou modifier les informations d'identification du support

Configurer ou modifier les attributs d'informations d'identification du compte de support associé à votre système.

Format

```
/sys/support/account set -user <value> {-passwd <value> | -passwdSecure}
```

Qualificateurs d'action

Qualificateur	Description
`-user`	Spécifiez le nom d'utilisateur du compte de support.
`-passwd`	Spécifiez le nouveau mot de passe du compte de support.
`-passwdSecure`	Spécifier le mot de passe en mode sécurisé : l'utilisateur est invité à saisir le mot de passe.

Exemple

La commande suivante spécifie le nouveau mot de passe du compte de support :

`uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account set -user user1 -passwd Password123`

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Configure Centralized ESRS with the Unisphere CLI

The following sections describe how to configure and test Centralized ESRS using the CLI.

Activez ou modifiez Centralized ESRS

Activez ou modifiez la configuration de Centralized ESRS.

Format

```
/sys/support/esrsc set -enable { yes | no } [ -address <value> ] [ -port <value>] [-
secondAddress <value>] [-secondPort <value>]
```

Qualificateurs d'action

Qualificateur	Description
`-enable`	Indiquez si le Centralized ESRS doit être activé ou désactivé. Les valeurs autorisées sont les suivantes : • `yes` • `no`

Qualificateur	Description
	REMARQUE : Si ESRS est désactivé, les autres paramètres ne peuvent pas être modifiés.
-address	Spécifie l'adresse IP du serveur Centralized ESRS VE auquel la connexion doit s'effectuer.
-port	Spécifie le numéro de port à utiliser pour se connecter au Centralized ESRS.
-secondAddress	Spécifiez le nom du réseau ou l'adresse IP du serveur Centralized ESRS VE secondaire.
-secondPort	Spécifie le numéro de port à utiliser pour se connecter au serveur Centralized ESRS VE principal. **REMARQUE :** La passerelle secondaire doit se trouver dans le même cluster que la passerelle principale.

Exemple 1

La commande suivante spécifie les paramètres du Centralized ESRS :

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc set -enable yes -address 10.10.22.22

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Exemple 2

L'exemple suivant configure Centralized ESRS VE avec une passerelle secondaire pour la haute disponibilité.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc set –enable yes –address 10.10.22.22 –secondAddress 10.10.22.32

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Vérifier la connexion réseau des services ESRS intégrés

Vérifiez la connectivité réseau des services ESRS centralisés avant de configurer ESRS.

Vérifiez la connectivité réseau à partir des services Centralized ESRS sur les serveurs Dell EMC. En cas d'échec, les services intégrés ESRS ne peuvent pas être activés.

Format

```
/sys/support/esrsc checkNetwork -address <value> [-port <value>]
```

Qualificateur d'action

Qualificateur	Description
-address	Tapez l'adresse IP des services ESRS VE centralisés.
-port	Tapez le numéro de port utilisé pour les services ESRS VE centralisés.

Exemple

Cet exemple montre à quel moment les services ESRS centralisés échouent à établir la connectivité réseau.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc checkNetwork -address 10.100.10.7

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x6400be8

The centralized ESRS network connectivity check failed. Please check your firewall
configuration and whether the centralized ESRS server is operating normally. (Error
Code:0x6400be8)
```

Tester les ESRS centralisés

Une fois l'ESRS centralisé déjà configuré, vous pouvez utiliser cette commande pour tester la connexion entre votre système et la base de données ESRS. Pendant que la commande `checkNetwork` vérifie votre connectivité de réseau local, cette commande `test` vérifiera la connexion à Dell EMC.

Format

```
/sys/support/esrsc test
```

Exemple 1

L'exemple suivant montre les résultats de l'exécution de cette commande lorsque l'ESRS centralisé n'est pas encore configuré.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc test

```
Operation failed. Error code: 0x6400c06
 Not supported since Centralized Secure Remote Support is not enabled. (Error
Code:0x6400c06)
```

Exemple 2

L'exemple suivant montre quand cette commande est exécutée avec succès.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc test

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

REMARQUE : Une opération réussie indique que le test a été exécuté avec succès, pas que la connexion elle-même a réussi. En d'autres termes, il indique qu'un Call Home a été envoyé, mais n'indique pas s'il a été reçu par le serveur ESRS. Pour vérifier l'état du test réel, connectez-vous à service 360 pour afficher les demandes de service (SR) récentes. Si le Call Home a été reçu par le serveur ESRS, le test de connexion apparaîtra comme un Call Home SR automatiquement fermé.

Configure Integrated ESRS with the Unisphere CLI

The following sections describe how to configure and test Integrated ESRS using the CLI.

Vérifier la préparation des informations d'identification de support pour ESRS intégré

Avant de configurer ESRS, vérifiez que les informations d'identification du compte de support configurées pour votre système sont correctement enregistrées dans la base de données du support en ligne.

Format

```
/sys/support/esrsi checkSupportAccountReadiness
```

Exemple

L'exemple suivant montre que la commande s'exécute correctement, puisque les informations d'identification de prise en charge sont correctement configurées.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkSupportAccountReadiness

```
Storage system address: 10.0.0.1
Storage system port: 443
HTPS connection

Operation completed successfully.
```

Activer ou modifier Integrated ESRS

Activer ou modifier la configuration Integrated ESRS

Format

```
/sys/support/esrsi set {-enable {yes|no}|-acceptEula yes|-type {oneWay|twoWay}}
```

Qualificateurs d'action

Qualificateur	Description
`-enable`	Indiquer si ESRS doit être activé, réactivé ou désactivé. Les valeurs autorisées sont les suivantes : • `yes` • `no` **REMARQUE :** Si ESRS est désactivé, les autres paramètres ne peuvent pas être modifiés.
`-acceptEula`	Spécifie si vous souhaitez accepter la licence d'utilisateur. La valeur valide est : • `yes` **REMARQUE :** Si les CGU ESRS ne sont pas acceptées, aucun élément ne peut être configuré pour l'Integrated ESRS.
`-type`	Spécifie le type d'Integrated ESRS à utiliser. Les valeurs autorisées sont les suivantes : • `oneWay` (sortant uniquement) • `twoWay` (sortant/entrant) (par défaut)

Exemple

La commande suivante active Integrated ESRS, accepte le contrat EULA et définit le type de Integrated ESRS :

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi set -enable yes -acceptEula yes -type oneWay

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Vérifier la connexion réseau Integrated ESRS

Vérifiez la connectivité réseau à partir du client Integrated ESRS vers les serveurs d'EMC. En cas d'échec, Integrated ESRS ne peut pas être activé.

Format

```
/sys/support/esrsi checkNetwork
```

Exemple

La commande suivante affiche la connectivité réseau pour Integrated ESRS :

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkNetwork

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x6400bc8
 Remote Support cannot be enabled at this time, because the system cannot contact some
required EMC servers: esrghoprd02.emc.com:443/8443,esrghoprd03.emc.com:8443/443. Please
refer to online help for this error code to resolve the issue. (Error Code:0x6400bc8)
```

Demander un code d'accès pour Integrated ESRS

Demander un code d'accès pour Integrated ESRS Ce code d'accès peut être envoyé par e-mail à l'utilisateur du compte e-mail. Ce code d'accès sera valide pendant 30 minutes uniquement. Ce processus ajoute un niveau d'authentification supplémentaire et permet de vérifier que vous êtes l'utilisateur approprié et autorisé à activer ESRS sur le système de stockage.

Format

```
/sys/support/esrsi requestAccessCode
```

Exemple

La commande suivante envoie une demande de code d'accès dans le cadre du processus de vérification par e-mail d'Integrated ESRS :

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi requestAccessCode

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

1:     Recipient email address = sxxxxxxxxxx@mail.com
```

Valider un code d'accès pour Integrated ESRS

Valider le code d'accès pour Integrated ESRS qui a été envoyé par e-mail à l'utilisateur du compte de messagerie. Le code d'accès reçu sera valide pendant 30 minutes uniquement.

Format

```
/sys/support/esrsi validateAccessCode -accessCode <value>
```

Exemple

La commande suivante affiche la réponse à la validation du code d'accès de la procédure de vérification par e-mail :

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi validateAccessCode -accessCode 76507252

```
Storage system address: 10.0.0.1
Storage system port: 443
HTPS connection

Operation completed successfully.
```

Tester l'ESRS intégré

Une fois l'ESRS intégré déjà configuré, vous pouvez utiliser cette commande pour tester la connexion entre votre système et la base de données ESRS. Pendant que la commande `checkNetwork` vérifie votre connectivité de réseau local, cette commande `test` vérifiera la connexion à Dell EMC.

Format

```
/sys/support/esrsi test
```

Exemple 1

L'exemple suivant montre les résultats de l'exécution de cette commande lorsque l'ESRS intégré n'est pas encore configuré.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi test

```
Operation failed. Error code: 0x6400bad
 Not supported since Integrated Secure Remote Support is not enabled. (Error
Code:0x6400bad)
```

Exemple 2

L'exemple suivant montre quand cette commande peut être exécutée avec succès.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi test

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

REMARQUE : Une opération réussie indique que le test a été exécuté avec succès, pas que la connexion elle-même a réussi. En d'autres termes, il indique qu'un Call Home a été envoyé, mais n'indique pas s'il a été reçu par le serveur ESRS.

Pour vérifier l'état du test réel, connectez-vous à service 360 pour afficher les demandes de service (SR) récentes. Si le Call Home a été reçu par le serveur ESRS, le test de connexion apparaîtra comme un Call Home SR automatiquement fermé.

Configurer ou modifier les paramètres du Policy Manager et du serveur proxy

Configurez ou modifiez les attributs de Policy Manager et du serveur proxy.

Format

```
/sys/support/esrsi/policymgr set [ -enable { yes | no } ] [ -address <value> ] [ -port
<value> ] [ -protocol { http | https } ] [ sslStrength { high | medium | low } ] [ -
enableProxy { yes | no } ] [ -proxyAddr <value> ] [ -proxyPort <value> ] [ -proxyUser
<value> { -proxyPasswd <value> | -proxyPasswdSecure } ] [ -proxyProtocol { http | socks } ]
```

Qualificateurs d'action

Qualificateur	Description
`-enable`	Indique si ESRS Policy Manager doit être activé ou désactivé. Les valeurs autorisées sont les suivantes : • `yes` • `no` **REMARQUE :** Si ESRS Policy Manager est désactivé, les autres paramètres de Policy Manager ne peuvent pas être modifiés.
`-address`	Spécifie l'adresse du Policy Manager à configurer pour Integrated ESRS.
`-port`	Spécifie le numéro de port du serveur Policy Manager à configurer pour Integrated ESRS.
`-protocol`	Spécifie le protocole à utiliser par le serveur de Policy Manager.
`-sslStrength`	Spécifie la sécurité SSL d'ESRS Policy Manager (s'applique uniquement lorsque le protocole est HTTPS). Les valeurs autorisées sont les suivantes : • `high` • `medium` • `low`
`-enableProxy`	Spécifie l'activation du proxy de Policy Manager. Les valeurs autorisées sont les suivantes : • `yes` • `no` **REMARQUE :** Si ESRS Policy Manager est désactivé, les autres paramètres de serveur proxy de Policy Manager ne peuvent pas être modifiés.
`-proxyAddr`	Spécifie l'adresse de serveur du proxy de Policy Manager.
`-proxyPort`	Spécifie le numéro de port du serveur proxy de Policy Manager.
`-proxyUser`	Spécifie le nom d'utilisateur du compte sur le serveur proxy du Policy Manager.
`-proxyPasswd`	Spécifie le mot de passe du compte sur le serveur proxy du Policy Manager.
`-proxyProtocol`	Spécifie le protocole à utiliser par le serveur proxy du Policy Manager.

Exemple

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi/policymgr set -enable no

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

5

Troubleshooting

The service command **svc_esrs_ve** allows the user to perform basic tasks on ESRS VE, such as checking the status of the service and network or cleaning up the configuration. For more information, refer to the *Dell EMC Unity™ Service Commands Technical Notes* document.

This chapter provides information about the probable causes of problems that you may encounter when enabling and running the ESRS feature and the recommended actions to take to resolve them.

Topics include:

Sujets :

ESRS ne peut pas être activé.

Lorsqu'il n'est pas possible d'activer la fonction ESRS, envisagez les causes possibles suivantes et les interventions susceptibles de résoudre le problème.

Tableau 1. Résolution de problèmes - Impossible d'activer la fonction ESRS.

Cause probable	Intervention recommandée
Vous avez peut-être fourni des informations d'identification de connexion non valides ou vous n'avez pas procédé à la mise à niveau vers un compte de support à accès complet. Pour activer votre compte initial avec informations d'identification à accès complet, comptez un maximum de 48 heures.	Vérifiez les éléments suivants : • Les informations d'identification que vous avez spécifiées correspondent aux informations d'identification utilisées pour enregistrer le système de stockage sur le site Web de support. • Vos informations de compte ont été mises à niveau vers un compte de support à accès complet (utilisateur enregistré avec accès au site où réside le système de stockage installé). **REMARQUE :** Vous pouvez vérifier si vos informations d'identification sont valides en vous connectant au site Web de support (https://Support.EMC.com). Si vous n'avez pas encore enregistré votre système de stockage, faites-le maintenant. Si vous ne pouvez toujours pas accéder au site, envoyez un e-mail à l'adresse support@emc.com
Il se peut que vous ayez fourni des informations d'identification de connexion valides mais qu'elles ne soient pas associées à votre identifiant de site où le système de stockage est situé. Dans les systèmes de support, un identifiant de site est créé pour chaque site de votre organisation où des produits EMC ont été installés.	Vérifiez vos identifiants de site sur le site Web de support en ligne : 1. Connectez-vous au support en ligne avec vos informations d'identification. 2. Sélectionnez **Centre de maintenance**. 3. Sur la page Centre de maintenance, sous la zone Sites et contrats, cliquez sur **Administrer un site**. 4. Vérifiez que le site où le système de stockage est installé figure dans la liste Mes sites. **REMARQUE :** Vous pouvez également rechercher un site et l'ajouter à la liste Mes sites. Si un ID de site n'est pas disponible ou si l'ID de site correct n'est pas répertorié, vous devez informer votre responsable de compte local afin d'en effectuer la demande. Si un partenaire effectue

Tableau 1. Résolution de problèmes - Impossible d'activer la fonction ESRS. (suite)

Cause probable	Intervention recommandée
	l'installation, celui-ci doit soumettre la demande au groupe Install Base ou à son responsable de compte. Si le système Unity est répertorié sous l'ID de site incorrect, reportez-vous à l'article *KB 489840* pour plus d'informations sur la modification de l'ID de site qui est associé au système.

Utilisation des informations d'identification RSA pour configurer ESRS

Dans certains cas, les informations d'identification du support client n'ont pas été entièrement configurées ou validées sur les serveurs de support back-end. Dans les versions 4.x, cela empêche de configurer ESRS. Le personnel de support peut, qu'il soit sur site ou via un appel distant, saisir ses informations d'identification RSA pour contourner l'exigence d'un compte de support client entièrement configuré.

La fonction ESRS a signalé un problème de connexion

Lorsque la fonction ESRS a cessé de fonctionner, envisagez les causes possibles suivantes et les interventions susceptibles de résoudre le problème.

Tableau 2. Résolution de problèmes - la fonction ESRS est déconnectée.

Cause probable	Intervention recommandée
Le serveur DNS n'est pas opérationnel ou n'existe pas.	Effectuez ce qui suit : 1. Vérifiez que le nom du serveur DNS défini dans Unisphere est saisi correctement. 2. Activez SSH, connectez-vous à l'aide du compte de maintenance et utilisez la commande ping pour vous assurer que la communication entre le système de stockage et l'adresse IP du serveur DNS fonctionne correctement. 3. Utilisez l'outil **Nslookup** sur l'un des noms d'hôte ESRS pour vérifier que le serveur DNS peut y apporter une résolution correcte. S'il ne peut pas, ou si le serveur DNS ne peut pas être détecté, contactez votre administrateur réseau.
Un Policy Manager est configuré mais n'est pas joignable.	Vérifiez si le Policy Manager est en ligne. Dans Unisphere, accédez à **Paramètres** > **Configuration du support** > **EMC Secure Remote Service** et vérifiez que les paramètres de protocole, de port, de nom réseau/adresse IP du Policy Manager sont correctement configurés.
La connexion ESRS est fonctionnelle, mais vous ne pouvez pas établir de sessions à distance. Il est possible que le serveur Global Access (GAS) ne soit pas joignable. Les serveurs GAS sont utilisés pour les sessions à distance uniquement.	Effectuez ce qui suit : • Si la connexion inclut un serveur proxy client, assurez-vous que ce dernier est joignable. • Vérifiez que les hôtes et les ports (443 et 8443) du pare-feu appropriés sont ouverts pour EMC.
Un système configuré avec une implémentation ESRS Centralized rencontre des problèmes avec le protocole HTTP persistant et n'apparaît pas comme connecté.	Vérifiez que le port 9443 est ouvert pour permettre les appels REST API à partir du système de stockage vers ESRS Gateway.