# Micro Focus Security ArcSight ArcSight Platform

Software Version: 21.1

## ArcSight Platform Release Notes

Document Release Date: July 2021
Software Release Date: May 2021

# Legal Notices

## Copyright Notice



# Support

## Contact Information

| | |
|---|---|
| **Phone** | A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information |
| **Support Web Site** | https://softwaresupport.softwaregrp.com/ |
| **ArcSight Product Documentation** | https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs |

# Contents


What's New ... 6
- Updates for ArcSight Command Center for Enterprise Security Manager ... 6
- Updates for ArcSight Intelligence ... 6
  - FIPS 140-2 Compliance ... 6
  - Cloud-native Deployment ... 7
  - Custom Model Support ... 7
  - Fusion User Management ... 7
- Updates for ArcSight Management Center ... 7
- Updates for ArcSight Recon ... 8
  - Cloud-native Deployment ... 8
  - Enhancements to Search in Recon ... 8
  - New Compliance Packs to Check for Data Compliance ... 8
- Introducing ArcSight SOAR ... 9
  - FIPS 140-2 Compliance ... 9
  - SOAR Licensing ... 9
  - Out of the Box Playbooks ... 9
  - MISP Threat Sharing Integration Capabilities ... 10
- Updates for ArcSight Fusion ... 10
  - FIPS 140-2 Compliance ... 10
  - Complete Integration with Platform Capabilities ... 10
  - Widget for Monitoring Database Health ... 10
- Updates for ArcSight Platform Installer ... 11
  - CDF 2021.02 ... 11
- Updates for ArcSight Transformation Hub ... 12

Technical Requirements ... 13

Downloading the ArcSight Platform Installation Files ... 13
- Understanding the Files to Download ... 13
- Downloading the Installation Files ... 16

Licensing Information ... 16

Known Issues ... 16
- Post Upgrade fusion-metadata-rethinkdb Pod May Go Into a Crash Loop ... 17
- Deploying Fusion in AWS Environment with a Load Balancer Requires Proxy Host Configuration ... 18
- Pods Might Not Run During Fusion Reinstall ... 19

Installation, Upgrade, or Adding Additional Capabilities Fails Due to Comma Character in On-Premises Docker Container Registry Admin Password ..... 19
CDF Management Portal Admin Password Change Fails to Update Registry Admin Password ..... 19
On Multi-master Non-root Install, itom-cdf-keepalived Pod Restarting and Suite Fails to Deploy ..... 20
After an Upgrade from the Patch Release, Error Returned: "Failed to upgrade. Internal Server Error." ..... 20
Accessing the CDF Management Portal Reconfigure Page ..... 20
Contacting Micro Focus ..... 21
Additional Documentation ..... 21
Send Documentation Feedback ..... 23

# Release Notes for the ArcSight Platform 21.1

## Thursday, July 8, 2021

ArcSight Platform 21.1 (the Platform) enables you to deploy a combination of security, user, and entity solutions into a single cluster within the Container Deployment Foundation (CDF) environment. The core services for this CDF environment, including the Dashboard and user management, are provided by a common layer called Fusion.

- ArcSight Command Center for Enterprise Security Manager 7.5.0
- ArcSight Intelligence 6.3.0
- ArcSight Management Center 3.0
- ArcSight Recon 1.2.0
- ArcSight SOAR 3.1.0
- ArcSight Fusion 1.3.0
- ArcSight Platform Installer 21.1
- ArcSight Transformation Hub 3.5.0
- Layered Analytics 1.2.0

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment** or **support** on this topic at the bottom of any page in the HTML version of the documentation posted at the ArcSight Platform Documentation page or the documentation pages for the included products.


- "What's New" on the next page
- "Technical Requirements" on page 13
- "Downloading the ArcSight Platform Installation Files" on page 13
- "Licensing Information" on page 16
- "Known Issues" on page 16
- "Contacting Micro Focus" on page 21

# What's New

The following sections outline the key features and functions provided in this release. For more information about these enhancements, please see the release notes for the specific product solution.

## Updates for ArcSight Command Center for Enterprise Security Manager

For information about ESM updates, see the *ArcSight Enterprise Security Manager (ESM) 7.5 Release Notes*.

## Updates for ArcSight Intelligence

This release includes the following updates for Intelligence:

- FIPS 140-2 Compliance
- "Cloud-native Deployment" on the next page
- Custom Model Support
- Fusion User Management

For more information on the Intelligence release updates, see the *ArcSight Intelligence 6.3 Release Notes*.

### FIPS 140-2 Compliance

ArcSight Intelligence is now FIPS 140-2 compliant. Currently, all sub-components in the Intelligence architecture operate in the FIPS 140-2 mode. For all sub-components, the FIPS 140-2 mode is always enabled and you do not have the option to disable it.

For more information, see "Using ArcSight Platform and Products in FIPS Mode" in the *Administrator's Guide for ArcSight Platform*.

## Cloud-native Deployment

You can now deploy and configure Intelligence in the following cloud environments:

- **Azure** - Leverages the capabilities of the Microsoft Azure cloud platform.
- **Amazon Web Services (AWS)** - Leverages its cloud-native services and capabilities.

For more information, see "Setting Up Your Azure Deployment Architecture" and "Setting Up Your Deployment Architecture (Amazon Web Services)" in the *Administrator's Guide for ArcSight Platform*.

## Custom Model Support

Intelligence provides support for custom machine learning (ML) models. This feature enables you to enhance Intelligence with models that provide analytics tailored to your unique environments. It also provides a method for extending Intelligence analytics to address new use cases such as the detection of new patterns of unusual behavior. You can also customize the alert template associated with a custom model. An alert template provides a way to describe an anomaly in the Intelligence UI by using the textual information provided as part of the alert template's metadata.

For more information, see "Enabling Custom Model Support" in the *Administrator's Guide for ArcSight Platform*.

## Fusion User Management

You now use Fusion to create users and assign relevant roles and permissions for the users to access Intelligence.

# Updates for ArcSight Management Center

This release includes the following updates for ArcMC:

- ArcMC can now be deployed into the containerized ArcSight Suite as a component of the Fusion capability. This is the recommended model for Recon and Intelligence, supporting new deployments only, not upgrades from prior ArcMC releases.
- Integration with the AutoPass License Server.
- Supports the management of standalone Management Centers, Connectors, Transformation Hub, and Logger.
- Cloud Native Deployment into AWS and Azure.
- Miscellaneous bug fixes are also included.

For more information on the ArcMC release updates, see the *ArcSight Management Center Release Notes*.

# Updates for ArcSight Recon

This release includes the following updates for Recon:

- "Cloud-native Deployment" below
- "Enhancements to Search in Recon" below
- "New Compliance Packs to Check for Data Compliance" below

For more information on the Recon 1.2 release updates, see the *ArcSight Recon 1.2 Release Notes*.

## Cloud-native Deployment

You can now deploy and configure Recon in the following cloud environments:

- **Azure** - Leverages the capabilities of the Microsoft Azure cloud platform.
- **Amazon Web Services (AWS)** - Leverages its cloud-native services and capabilities.

For more information, see "Setting Up Your Azure Deployment Architecture" and "Setting Up Your Deployment Architecture (Amazon Web Services)" in the *Administrator's Guide for ArcSight Platform*.

For more information on the Recon 1.2 release updates, see the *ArcSight Recon 1.2 Release Notes*.

## Enhancements to Search in Recon

This release enhances the Search function in Recon as follows:

- Ability to Include Logger Data
- Schedule Searches to Run at Specific Intervals
- Enhancements to Fieldsets
- Query Auto-suggests Fields to Include

For more information on the Recon 1.2 release updates, see the *ArcSight Recon 1.2 Release Notes*.

## New Compliance Packs to Check for Data Compliance

This release provides three Compliance Packs to help you comply with a broad set of legal and governmental regulations that require your enterprise to organize and manage sensitive data

and institute a strong IT governance program. These packs support the following standards:

- General Data Product Regulation (GDPR)
- IT Governance - ISO 27002
- PCI DSS

# Introducing ArcSight SOAR

This release includes the following updates for SOAR:

- "FIPS 140-2 Compliance" below
- SOAR Licensing
- Out Of the Box Playbooks
- MISP Threat Sharing Integration Capabilities

For more information on the SOAR release updates, see the *ArcSight SOAR 3.1 Release Notes*.

## FIPS 140-2 Compliance

ArcSight SOAR is now FIPS 140-2 compliant. Currently, all sub-components in the SOAR architecture operate in the FIPS 140-2 mode. For all sub-components, the FIPS 140-2 mode is always enabled and you do not have the option to disable it.

For more information, see "Using ArcSight Platform and Products in FIPS Mode" in the *Administrator's Guide for ArcSight Platform*.

## SOAR Licensing

In addition to **ESM** and **Recon** users, **ArcSight Intelligence** users are now entitled to use SOAR without an extra license.

ArcSight SOAR also supports non-autopass ESM licenses. Customers using ESM version 6.11 and later can also use the SOAR capability.

## Out of the Box Playbooks

ArcSight SOAR provides out of the box playbook library, which can be used as templates. Customers can customize and use playbooks prepared by Micro Focus experts.

For more information on out of the box playbooks, see the ArcSight SOAR 3.1 User Guide.

## MISP Threat Sharing Integration Capabilities

ArcSight SOAR is integrated with MISP Threat Sharing and provides both threat intelligence sharing and enrichment for artifacts capabilities.

# Updates for ArcSight Fusion

This release includes the following updates for Fusion:

- "FIPS 140-2 Compliance" below
- Complete Integration with Platform Capabilities
- Widget for Monitoring Database Health

## FIPS 140-2 Compliance

ArcSight Fusion is now FIPS 140-2 compliant. Currently, all sub-components in the Fusion architecture operate in the FIPS 140-2 mode. For all sub-components, the FIPS 140-2 mode is always enabled and you do not have the option to disable it.

For more information, see "Using ArcSight Platform and Products in FIPS Mode" in the *Administrator's Guide for ArcSight Platform*.

## Complete Integration with Platform Capabilities

Fusion now provides a complete integration with the consoles for **ESM Command Center** and **ArcSight SOAR**. Also, this release incorporates **ArcSight Management Center** (ArcMC) within the Fusion capability. Users can access the ArcMC console to manage and monitor ArcSight infrastructure components, which is particularly useful when you have a large deployment of ArcSight connectors.

## Widget for Monitoring Database Health

The **Database Cluster Node Status** widget helps SOC managers and IT administrators monitor the state of the nodes that host the database. This widget displays the state of each node in the database cluster. It also raises awareness that the number of nodes that are down can affect the resiliency of the database cluster.

To use this widget, you must have a capability that requires the ArcSight Database.

# Updates for ArcSight Platform Installer

This release includes the following updates for the platform installer:

- Cloud-native Deployment
- CDF 2021.02
- Platform Installers

## Cloud-native Deployment

You can now deploy and configure Recon, Intelligence, ArcSight Management Center (ArcMC), and Fusion in the following cloud environments:

- **Azure** - Leverages the capabilities of the Microsoft Azure cloud platform.
- **Amazon Web Services (AWS)** - Leverages its cloud-native services and capabilities.

This option offers the following benefits:

- Cloud-native deployments into vendor supplied Kubernetes/Docker service environments require deployment of Worker Nodes only.
- Reduces the number of nodes deployed, which may reduce costs.
- Enables the cloud vendor to manage and upgrade their service environment on their schedule, not on ArcSight release boundaries.
- In prior releases, Transformation Hub was the only cloud-native deployment option.

For more information, see "Setting Up Your Azure Deployment Architecture" and "Setting Up Your Deployment Architecture (Amazon Web Services)" in the *Administrator's Guide for ArcSight Platform*.

## CDF 2021.02

- The Container Deployment Foundation (CDF), Kubernetes, Docker and AutoPass components have been upgraded to CDF version 2021.02, the latest CDF release.
- Platform component version updates have been certified on RHEL 8.2 and 7.9, and CentOS 8.2 and 7.9.
- Master Nodes can now be added to a pre-deployed cluster using the CDF Management Portal and ArcSight provided scripts.

## Platform Installers

- Improved DNS pre-checking validation prior to starting install.
- Install tool now sets the node labels during installation in a way such that they automatically appear properly in the CDF Management Portal.
- Uninstall command (--cmd …) is now available to users, ensuring and enabling cleanup of previously installed resources and database.
- Enhanced database node pre-checking validation, allowing for pre-definition of all database nodes. At least one database node must be available and online for the install to proceed.
- For new NFS mounts, installer now secures the mounts automatically, negating the need for manual hardening of a freshly provisioned NFS.
- Layer2 network connectivity is generally required. A new pre-check validates its presence. If it is not found, use the vxlan backend property for flannel.
- Better documented certificate management procedures, including the vault used for signing certs for consumers/producers.
- The install-config-template.yaml is renamed to install-config-doc.yaml to clarify the purpose of this file. Text within the file is improved to make it easier to find the info needed to successfully complete the installation, such as a description of the suite configuration parameters.
- The interset-hdfs-namenode suite config parameter is automatically set by arcsight-install tool to make the installation easier and less prone to error.

# Updates for ArcSight Transformation Hub

This release includes the following updates for Transformation Hub:

- Transformation Hub now requires Fusion to be deployed. This enables log in to Transformation Hub's Kafka Manager using Fusion's Single Sign-on capability.
- Platform component version updates have been certified on RHEL 7.9/8.2 and CentOS 7.9/8.2, with current releases of Azul Zulu Java runtime, Apache Kafka Client, and the Confluent platform (which includes Apache Kafka, Schema Registry and ZooKeeper).
- Component libraries include current vulnerability compliance, and ciphers are up-to-date. Static cipher suites have been removed.
- Miscellaneous bug fixes are also included.

For more information on Transformation Hub release updates, see the *Transformation Hub Release Notes*.

# Technical Requirements

For more information about the software and hardware requirements required for a successful deployment, see the *Technical Requirements for ArcSight Platform*.

These *Technical Requirements* include guidance for the size of your environment based on expected workload. Micro Focus recommends the tested platforms listed in this document.

Customers running on platforms not provided in this document or with untested configurations will be supported until the point Micro Focus determines the root cause is the untested platform or configuration. According to the standard defect-handling policies, Micro Focus will prioritize and fix issues we can reproduce on the tested platforms.

# Downloading the ArcSight Platform Installation Files

You can download the installation packages for the products in the ArcSight Platform from the Micro Focus Downloads website. The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

Micro Focus provides several options for deploying products in your environment. For more information about deploying a product, see the *Administrator's Guide for ArcSight Platform*.


- "Understanding the Files to Download" below
- "Downloading the Installation Files" on page 16


## Understanding the Files to Download

You can download the following installation packages. You only need one copy of each file, regardless of the products that you intend to deploy. For example, the Transformation Hub-based files are available with the ESM, Intelligence, and Recon software downloads, but you only need to download the files once. The Transformation Hub file set includes the packages for the CDF installer, the ArcSight Platform Installer, and the ArcSight database.

| | ESM Command Center | Intelligence | Recon | Transformation Hub |
|---|---|---|---|---|
| **All Deployments – Metadata** | | | | |
| arcsight-installer-metadata-21.1.0.9.tar | ✔ | ✔ | ✔ | ✔ |
| **All Deployments – Images** | | | | |
| esm-7.5.0.9.tar | ✔ | | | |
| fusion-1.3.0.9.tar | ✔ | ✔ | ✔ | ✔ |
| intelligence-6.3.0.9.tar | | ✔ | | |
| layered-analytics-1.2.0.9.tar | ✔ | ✔ | | |
| recon-1.2.0.9.tar | | | ✔ | |
| soar-3.1.0.9.tar | ✔ | | ✔ | |
| transformationhub-3.5.0.9.tar | | ✔ | ✔ | ✔ |
| **All Deployments – Dashboard Widgets** | | | | |
| soar-widgets-1.2.0.2.tar | ✔ | | ✔ | |
| widget-sdk-3.2.12.tgz (*optional*) | ✔ | ✔ | ✔ | |
| **On-premises Deployments** | | | | |
| arcsight-platform-installer-21.1.0.9.zip | ✔ | ✔ | ✔ | ✔ |
| **Cloud Deployments** | | | | |
| arcsight-platform-cloud-installer-21.1.0.9.zip | | ✔ | ✔ | ✔ |

To understand the files that you might need for your ArcSight Platform deployment, review the descriptions in the following table:

| File Type | File Name | Description |
|---|---|---|
| All Deployments - Metadata | arcsight-installer-metadata-21.1.0.9.tar | Contains metadata for deployment of the CDF Management Portal. |
| All Deployments - Images | esm-7.5.0.9.tar | Contains the images for deploying ESM Command Center. |
| | fusion-1.3.0.9.tar and arcsight-fusion-1.3.0-license.txt | Contains the images for deploying the Fusion capability. |
| | intelligence-6.3.0.9.tar | Contains the images for deploying Intelligence. |
| | layered-analytics-1.2.0.9.tar | Contains the images for deploying the Layered Analytics capability. |
| | recon-1.2.0.9.tar | Contains the images for deploying the Recon capability. |
| | soar-3.1.0.9.tar and enterprise-security--esm--arcsight-soar-3.1-license.txt | Contains the images for deploying the SOAR capability. |
| | transformationhub-3.5.0.9.tar | Contains the images for deploying Transformation Hub. |
| All Deployments - Dashboard Widgets | soar-widgets-1.2.0.2.tar | Contains the widgets that display SOAR-based data in the Dashboard. |
| | widget-sdk-3.2.5.tgz | Optional Provides the Widget Software Development Kit (the Widget SDK) that enables you to build new widgets or modify existing widgets for deployed applications such as ESM and Intelligence. |
| On-premises Deployments | arcsight-platform-installer-21.1.0.9.zip | Contains files for installing the infrastructure where you want to deploy capabilities, including the following content:<br>• CDF installer<br>• ArcSight Database installer - db-installer_x.x.x.x.tar.gz<br>• Configuration files for the ArcSight Installation Tool and its example scripts<br>You can find this file under Transformation Hub on the Software Downloads page. |
| Cloud Deployments | arcsight-platform-cloud-installer-21.1.0.9.zip | Contains the installation files for deploying capabilities to Amazon Web Services and Azure. |

## Downloading the Installation Files

To download and verify the signature of the downloaded files:

1. Log in to the computer where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the Micro Focus Downloads website along with their associated signature files (.sig). Micro Focus provides a digital public key that is used to verify that the software you downloaded from the Micro Focus software entitlement site is indeed from Micro Focus and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the Micro Focus Code Signing site. If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact Micro Focus Customer Support.
4. Begin the installation. For more information, see "Using the ArcSight Platform Installer" in the *Administrator's Guide for ArcSight Platform*.

# Licensing Information

For information about activating a new license, see "Installing Your License Keys" in the *Administrator's Guide for ArcSight Platform*.

# Known Issues

We are currently researching the following issues that are common to all capabilities that you can deploy in the ArcSight Platform.

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.


- "Post Upgrade fusion-metadata-rethinkdb Pod May Go Into a Crash Loop " on the next page
- "Deploying Fusion in AWS Environment with a Load Balancer Requires Proxy Host Configuration" on page 18

- "Pods Might Not Run During Fusion Reinstall" on page 19
- "Installation, Upgrade, or Adding Additional Capabilities Fails Due to Comma Character in On-Premises Docker Container Registry Admin Password" on page 19
- "CDF Management Portal Admin Password Change Fails to Update Registry Admin Password" on page 19
- "On Multi-master Non-root Install, itom-cdf-keepalived Pod Restarting and Suite Fails to Deploy" on page 20
- After Upgrade from Patch, Error Message Returned: Failed to upgrade Internal Server Error
- "Accessing the CDF Management Portal Reconfigure Page" on page 20


# Post Upgrade fusion-metadata-rethinkdb Pod May Go Into a Crash Loop

**Issue:**Kubernetes at times creates two instances of the fusion-metadata-rethinkdb pod, and allow one to run and delete the other. This causes one pod to hold the mount location and the other to fail and go into a crash loop.

**Workaround:**Follow these steps:

1. Execute this command to scale down the replica count of the rethinkdb pod to 0:

```
kubectl scale --replicas=0 deployment fusion-metadata-rethinkdb -n $(
kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
```

2. Execute this command to scale up the replica count of the rethinkdb pod to 1:

```
kubectl scale --replicas=1 deployment fusion-metadata-rethinkdb -n $(
kubectl get namespaces | grep arcsight | cut -d ' ' -f1)
```

3. Execute this command to restart all pods:

```
kubectl delete pods -n $( kubectl get namespaces | grep arcsight | cut -d
' ' -f1) --all
```

You may wait for all Pods to come up.

# Deploying Fusion in AWS Environment with a Load Balancer Requires Proxy Host Configuration

**Issue:**In AWS Deployments with Application Load Balancers (ALB), OSP authentication between Fusion and other ArcSight capabilities may fail. (OCTCR33I164044)

**Workaround:**Add proxyPort, proxyTls and proxyDomain information to the Fusion tenant configuration file tenantcfg.xml on the NFS server as in the snippet below, where external-access-host is the ALB's host name

arcsight-nfs/arcsight-volume/sso/default/WEB-INF/conf/current/default/tenantcfg.xml

```
<Tenant
        xmlns="uri.osp.xml.config.05.2015"
        id="default"
displayName="Hercules Tenant"
       >

       <HTTPInterface
              id="default-http-domain"
              displayName="Hercules HTTP"
              path="/osp"
              port="${HTTP_INTERFACE_PORT:443}"
              tls="${HTTP_INTERFACE_SSL:true}"
              domainName="${HTTP_INTERFACE_DOMAIN}"
              cookieDomain="${HTTP_INTERFACE_DOMAIN}"
              proxyPort="443"
              proxyTls="true"
              proxyDomain="{--external-access-host}"
              />

       <HTTPInterface
              id="default-http-ip"
              displayName="Hercules HTTP"
              path="/osp"
              port="${HTTP_INTERFACE_PORT:443}"
              tls="${HTTP_INTERFACE_SSL:true}"
              ipAddress="${HTTP_INTERFACE_IP}"
              cookieDomain="${HTTP_INTERFACE_IP}"
              proxyPort="443"
              proxyTls="true"
              proxyDomain="{--external-access-host}"
              />
```

# Pods Might Not Run During Fusion Reinstall

**Issue:** After you undeploy the Fusion capability and then redeploy Fusion into the same cluster, pods might remain in CrashLoopBackOff or PodInitializing status. The root cause of the issue is that the redeploy causes the system to forget the password for the rethinkdb database. (OCTCR33I112042)

**Workaround:** Delete all the files in the NFS folder before redeploying Fusion: arcsight-nfs/arcsight-volume/investigate/search/rethinkdb/hercules-rethinkdb-0. This will cause the rethinkdb database to be automatically recreated when Fusion is redeployed.

# Installation, Upgrade, or Adding Additional Capabilities Fails Due to Comma Character in On-Premises Docker Container Registry Admin Password

**Issue:** For on-premises deployments, if the Docker container registry-admin password includes a comma (,) character, the image upload phase fails due to a bug in the container registry. The registry-admin password is initially set to the same password as the admin user for the CDF Management Portal during installation. However, later changing the CDF Management Portal admin password does not change the registry-admin password because it is managed separately. (INST-2464)

**Workaround:** Log in to the master node console and use the /opt/arcsight/kubernetes/scripts/updateLocalRegistryInfo.sh script to change the registry-admin password to a new one that does not include the restricted comma character.

# CDF Management Portal Admin Password Change Fails to Update Registry Admin Password

**Issue:** For on-premises deployments, the registry-admin password is initially set to the same password as the admin user for the CDF Management Portal during installation. However, later changing the CDF Management Portal admin password does not change the registry-admin password because it is managed separately. The registry-admin password is used during upgrades and when adding capabilities to an existing cluster during the phase of image upload. (INST-2464)

**Workaround:** Log in to the master node console and use the /opt/arcsight/kubernetes/scripts/updateLocalRegistryInfo.sh script to change the registry-admin password.

# On Multi-master Non-root Install, itom-cdf-keepalived Pod Restarting and Suite Fails to Deploy

**Issue**: If sudo installing a multi-master cluster through the arcsight-install tool, you will notice all capability pods are marked as pending, and `itom-cdf-keepalived` pod is existing only in single replica and crashing. In additon, the `kubectl get nodes` command returns all of your worker nodes in a NotReady stats. If the sudo installation for multi-master was executed manually via install.sh, you will notice only the `itom-cdf-keepalived` pod in single replica count and crashing, even before you try to deploy the capabilities.

**Workaround:** Use `kubectl edit ds/itom-cdf-keepalived -n kube-system` to edit the daemonset definition of `cdf-keepalived.` Locate the "nodeSelector" section and change its value (make sure to honor the spacing) to master: "true". Save and exit as a normal vi session. Make sure `command kubectl get ds/itom-cdf-keepalived -n kube-system` returns now the current/desired replica count of 3.

# After an Upgrade from the Patch Release, Error Returned: "Failed to upgrade. Internal Server Error."

After upgrading to 21.1 from the 20.11 patch release, in some cases, the error message may be returned in the upgrade's final stages: "Failed to Upgrade. Internal Server Error." The issue can also be detected in logs if some resources are not upgraded. If encountering this, delete the old upgrade pod and then run the following command:
`kubectl delete deployment suite-upgrade-pod-arcsight-installer -n `kubectl get namespaces | grep arcsight-installer | awk ' {print $1}`

Then run the upgrade again.

# Accessing the CDF Management Portal Reconfigure Page

**Issue**: At times, you may not be able to access the CDF Management Portal Reconfigure page. For example, this issue may occur when you are trying to perform an upgrade.

**Workaround:** Follow these steps:

1. Verify the status of the nginx-ingress-controller DaemonSet :

   ```
   NS=$(kubectl get namespaces | awk '/arcsight/{print $1}')kubectl get
   daemonset nginx-ingress-controller -n $NS
   ```

2. Create a new nginx-ingress-controller.yaml file:

```
cd ${K8S_HOME}kubectl get daemonset nginx-ingress-controller -n `kubectl
get namespaces | grep arcsight-installer | awk '{print $1}'` -o yaml >
```

```
nginx-ingress-controller.yaml
```

3. Ensure that the saved nginx-ingress-controller.yaml file exist in the `${K8S_HOME}`home directory (`/opt/arcsight/kubernetes`) and contains definitions in yaml format.
4. Delete the current nginx-ingress-controller configuration:

```
kubectl delete -f ./nginx-ingress-controller.yaml
```

5. Apply the new nginx-ingress-controller configuration:

```
kubectl apply -f ./nginx-ingress-controller.yaml
```

6. Wait until the nginx-ingress-controller pods are up and running:

```
kubectl get pods -n $NS | grep nginx-ingress-controllerkubectl get pods -n
$NS --watch | grep nginx-ingress-controller
```

7. Verify the nginx-ingress-controller controller daemonset status:

```
kubectl get daemonset nginx-ingress-controller -n $NS
```

8. To continue to upgrade deployed capabilities, see "Accepting the Certificate" in the *Administrator's Guide for ArcSight Platform*.

# Contacting Micro Focus

For specific product issues, contact Micro Focus Support.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos.
- The Micro Focus Community pages.

# Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- *Administrator's Guide for ArcSight Platform*, which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in

the containerized platform.

- *User's Guide for Fusion 1.3 in the ArcSight Platform*, which is embedded in the product to provide both context-sensitive Help and conceptual information.
- Product Support Lifecycle Policy, which provides information on product support policies.

# Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on ArcSight Platform Release Notes (ArcSight Platform 21.1)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!