ArcSight Platform 20.11 Release Notes

December 2020

ArcSight Platform 20.11 (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. This release includes the following products:

- ArcSight Command Center for Enterprise Security Manager 7.4.0
- ArcSight Intelligence 6.2.0 - **NAME CHANGED!**
- ArcSight Recon 1.1.0
- ArcSight SOAR 3.0.0 - **NEW!**
- Transformation Hub 3.4.0

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 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?

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.

Introducing the ArcSight Platform Installer

The ArcSight Platform Installer provides an installation process that can automatically take care of all the prerequisites, software installations, and post-installation configurations for a new deployment. This tool provides configuration files applicable for single-node and multi-node setups. For more information about the ArcSight Platform Installer, see "Using ArcSight Platform Installer to Build Your Environment" in the *Administrator's Guide for ArcSight Platform*.

Introducing ArcSight SOAR

This release introduces ArcSight SOAR, which brings native security orchestration automation and response capabilities to the ArcSight family for faster security operations and enhanced operational efficiency. ArcSight SOAR is available free of charge to both new, and existing, customers of ArcSight ESM and ArcSight Recon. It is fully programmable and adaptable to meet security teams' unique needs, and enables multiple forms of automation, analyst augmentation, collaborative investigation and response through an intuitive interface.

ArcSight SOAR connects people, processes, and technology to help security engineers run day-to-day security operations efficiently. By providing tactical automation and orchestration through a single pane of glass, it enables SecOps teams to ramp up their output despite a growing cybersecurity skills gap and an increasing volume of complex attacks and alerts.

To access SOAR features in the ArcSight Platform environment, select **RESPOND** in the left navigation.

Updates for ArcSight Command Center for Enterprise Security Manager

This release of ArcSight Command Center includes the following enhancements:

- The MITRE Coverage view on the MITRE Dashboard is a customizable matrix that allows you to view any combination of the available data, such as attacks identified in the last two days or coverage that is installed but not enabled.
- You can now access and view session lists.
- You can now view the knowledge base articles associated with an event in an active channel.

For more information, see the *ArcSight Enterprise Security Manager 7.4 Release Notes*.

ArcSight Interset is now ArcSight Intelligence

In this release, ArcSight Interset SE changes its name to ArcSight Intelligence, and includes the following updates:

For more information, see the *ArcSight Intelligence 6.2 Release Notes*.

Support for New Devices

For the supported data types, Intelligence also provides support for new devices that provide relevant data to the Intelligence analytics models. For more information, see the "Adding Support for New Devices" section in the *Administrator's Guide for ArcSight Platform*.

Support for a New Data Type

Intelligence now supports the ingestion and analysis of the Repository data type. The following repository systems are supported: GitHub Enterprise 2.21.0, BitBucket Server 7.5.0, and Perforce 2020.1.

Integration with Enterprise Security Manager

Enterprise Security Manager (ESM) can now use risky users and alerts information provided by Intelligence to automatically populate Active Lists. This can be achieved by integrating Intelligence with ESM with the help of FlexConnectors. For more information, see the "Integrating Intelligence with Enterprise Security Manager" section in the *Administrator's Guide for ArcSight Platform*.

Integration with Fusion

The Fusion UI now includes an Entities at Risk link that allows direct navigation to the Intelligence UI. The Intelligence UI also includes a new Fusion link that takes users back to the Fusion UI. In the Fusion UI, you can create widgets that display the count of entities analyzed by Intelligence.

URL Compression and Encoding

For enhanced data security, Intelligence provides options to encode the Intelligence URL string. Based on your requirements, you can set the limit for the URL string length and then select a preferred URL encoding option. For more information, see the "Setting an Encoding Option for the URL" section in the *Administrator's Guide for ArcSight Platform*.

Updates for ArcSight Recon

This release provides the following updates in ArcSight Recon 1.1:

Enhancements to Search in Recon

This release enhances the Search function in Recon as follows:

- Enhanced Event Details panel
- Ability to configure preferences for search settings
- Ability to set an expiration time for searches
- Ability to choose from three types of timestamps

For more information, see the *ArcSight Recon 1.1 Release Notes*.

Ability to Create Storage Groups

This release gives you the ability to create **storage groups**, which allows you to partition the incoming events data and provide different retention periods based on query filters. Because you can set data retention policies per storage group, you can retain certain high volume events for a short time period and other important events for a longer time period.

The **query filter** enables you to associate a storage group with specific compliance requirements, business needs, or search activities. Recon uses the specified query filters to direct events to the correct storage group.

For more information, see the *ArcSight Recon 1.1 Release Notes*.

Updates for Transformation Hub

This release includes the following updates for Transformation Hub:

- Transformation Hub can now be deployed and configured in an Amazon Web Services (AWS) environment that leverages its cloud-native services and capabilities.
- A new silent install process for on-premises installations greatly simplifies the initial deployment of container-based ArcSight products and capabilities. The installer supports deployments from a simple, single node containing all capabilities to multi-node, high-availability deployment models. It installs and configures OS, storage, network, and other prerequisites and performs pre- and post-deployment resource and configuration checks. A minimum set of parameters are required, such as Master and Worker Node host names.
- Upgrades to Version 3.4.0 from prior Version 3.x releases and patches or hotfixes are supported in the native CDF Installer, using rolling upgrades through the Master and Worker Nodes in the cluster. If the cluster had been deployed with a high-availability deployment, the cluster will continue to process event streams while the upgrade proceeds from node-to-node.
- Support for the latest SmartConnector release, v8.1.0, is included. In addition to CEF and ESM_Binary formats, this release now supports emitting Avro-formatted event streams.
- New stream processor and Kafka Topics supporting Avro-formatted events are now available in Transformation Hub. ArcMC and Transformation Hub have been enhanced to enable routing of Avro streams and consumption of Avro events forwarded from ESM.
- Documentation is now available online, as HTML pages, supplemented by traditional PDF documents.
- The Container Deployment Foundation (CDF), Kubernetes and Docker components have been upgraded to CDF version 2020.08.

- Platform component version updates have been certified on RHEL 8.2, CentOS 8.2, with current releases of Azul Zulu Java runtime, PostgreSQL, 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.
- Miscellaneous bug fixes are also included. For more information, see the *Transformation Hub Release Notes*.

For more information, see the documentation for Transformation Hub 3.4.0.

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.

Downloading the ArcSight Platform Installation Files

You can download the installation packages for the products in the ArcSight Platform from the Micro Focus Downloads site. 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.

- "Understanding the Files to Download" on page 6
- "Downloading the Installation Files" on page 8

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

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 new ArcSight Platform Installer, and the ArcSight database.

	ESM Command Center	Intelligence	Recon	Transformation Hub
All Deployments – Metadata				
arcsight-installer-metadata-20.11.0.16.tar	✔	✔	✔	✔
All Deployments – Images				
esm-7.4.0.16.tar	✔			
fusion-1.2.0.16.tar	✔	✔	✔	
intelligence-6.2.0.16.tar		✔		
layered-analytics-1.1.0.16.tar	✔	✔		
recon-1.1.0.16.tar			✔	
soar-3.0.0.16.tar	✔		✔	
transformationhub-3.4.0.16.tar		✔	✔	✔
All Deployments – Dashboard Widgets				
soar-widgets-1.2.0.2.tar	✔		✔	
widget-sdk-3.2.5.tgz (*optional*)	✔	✔	✔	
On-premises Deployments				
cdf-2020.08.00153.20.11.0.5.zip	✔	✔	✔	✔
Cloud Deployments				
aws-byok-installer-2020.08.00153-20.11.0.5.zip				✔
cdf-byok-images-2020.08.00153-20.11.0.5.tar				✔
cdf-deployer-2020.08.00153-20.11.0.5.zip				✔

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

All Deployments - Metadata

File	Description
arcsight-installer-metadata-20.00.0.16.tar	Contains the core image of the CDF Management Portal.

All Deployments - Images

File	Description
esm-7.4.0.16.tar	Contains the images for deploying ESM Command Center.
fusion-1.2.0.16.tar	Contains the images for deploying the Fusion capability.
intelligence-6.2.0.16.tar	Contains the images for deploying Intelligence.
layered-analytics-1.1.0.16.tar	Contains the images for deploying the Layered Analytics capability.
recon-1.1.0.16.tar	Contains the images for deploying the Recon capability.
soar-3.0.0.16.tar	Contains the images for deploying the SOAR capability.
transformationhub-3.4.0.16.tar	Contains the images for deploying Transformation Hub.

All Deployments - Dashboard Widgets

File	Description
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

You can find this file under **Transformation Hub** on the Software Downloads page.

File	Description
cdf-2020.08.00153.20.11.0.5.zip	Contains files for installing the infrastructure where you want to deploy capabilities, including the following content: ◆ CDF installer ◆ ArcSight Database installer - `db-installer_3.3.0-2.tar.gz` ◆ Configuration files for the ArcSight Installation Tool and its example scripts

Cloud Deployments

File	Description
aws-byok-installer-2020.08.00153-20.11.0.5.zip	Contains the installation files for deploying Transformation Hub to AWS.
cdf-byok-images-2020.08.00153-20.11.0.5.tar	Contains the images for deploying Transformation Hub to the cloud.
cdf-deployer-2020.08.00153-20.11.0.5.zip	Contains files needed for a cloud deployment.

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:

   `cd <download_directory>`

   For example:

   `cd /opt`
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 the *Administrator's Guide for ArcSight Platform*.
5. After completing the installation or upgrade, continue to "Additional Installation and Upgrade Steps" on page 9.

Additional Installation and Upgrade Steps

After completing a new installation or upgrade to this release, you must perform the following procedure to ensure that the Watchdog service does not generate erroneous NotOK files each hour. This action changes a SQL command within the `watchdog.sh` file. (`HERC-10152`)

1. Log in to the database node1.
2. Change to the `/opt/arcsight-database/scripts` directory:

   ```
   cd /opt/arcsight-database/scripts
   ```

3. Run the following command:

   ```
   sed -i '/^run_sql_command/c\run_sql_command "select cluster from
   investigation_scheduler.stream_clusters" /dev/null > /dev/null 2>&1'
   watchdog.sh
   ```

Licensing Information

For information about activating a new license, see 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.

Disk Requirement for CDF Upgrade

Issue: While upgrading CDF, the system cannot complete the upgrade due to limited disk space. `(OCTCR33|118004)`

Workaround: Prepare 20% disk space of `/opt/arcsight/kubernetes` with additional 10 GB free space under `/opt/arcsight/kubernetes`. For example, `/opt/arcsight/kubernetes` has 427.30 GB free space; however, you need 2543.27 GB free space to perform the upgrade. The workaround is as follows:

1. On a worker node, run the following to delete th-arcsight-avro topic:
   - `ZKProcess=\`docker ps -a | grep k8s_zookeeper | awk '{print $1}'\``
   - `docker exec -it $ZKProcess kafka-topics --zookeeper localhost --delete --topic th-arcsight-avro`

2. To ensure the disk space is freed up, enter the following:
   - `cd /opt/arcsight/k8s-hostpath-volume/th/kafka`
   - Repeat `du -shk th-arcsight-avro*` until you see something similar to `8 th-arcsight-avro-*`
3. Create topic:
   - `THWeb=`kubectl get pods --all-namespaces | grep th-web | awk '{print $1, $2}'``
   - `kubectl delete pods -n $THWeb`

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 following folder before redeploying Fusion: <*NFS directory*>/vol/arcsight/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.

Cannot Import Users from Enterprise Security Manager

Issue: When you attempt to import users from ArcSight Enterprise Security Manager, you will receive a 406 HTTPS Error if either of the following conditions is true:

- You attempt to import the users by using the IP address of the ESM server
- You enter the FQDN (fully qualified domain name) for the ESM server, but either the port or admin credentials are incorrect `(HERC-9941)`

Solution: Ensure that you specify a valid FQDN for the ESM server, as well as the correct port and admin credentials.

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/