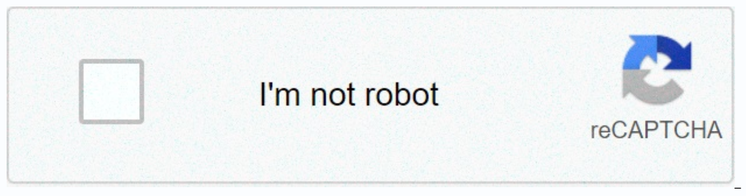

Continue

Arcsight logger upgrade guide

 Guides for Logger 6.6 / 6.6P1 Guides (only in case): Focus on a single version at time. (6.5 -> 6.6 -> 6.6P1) Create a configuration backup between each stepCheck release notes for update instructions. Depending on the version, you may need to upgrade the operating system if this is required, it should be performed before upgrading the logger (this is version-independent - the release notes should have the required information for each version)If the logger appliance, the OS upgrade file is located in the same location as the logger version on the support portal. (we provide the operating system updates for the appliance) For SW loggers, check the OS version for the version of the logger you are about to install and have your Linux administrator, upgrade the operating system before upgrading the logger, remember again to take Config back between this step)hope it helps. Advertising - Scroll to page 2 of 46 Ad Thank you for participating! * Your review is very important for improving the work of artificial intelligence, which forms the content of this project you read a free preview pages 8 to 13 are not displayed in this preview. You are reading a free preview pages 17 to 26 are not displayed in this preview. You are reading a free preview pages 31 to 42 are not displayed in this preview. 5 coment-rios 0 gostaram Estatsticas Notas Seja a primeira pessoa a gostar disto 1. Upgrade Guide ArcSight ESM 6.5c to 6.5c SP1 April 22, 2014 contact information revision s/phone A list of phone numbers is available on the HP ArcSight Technical Support page: solutions/software.html?compURI=1345981. URitMaVwpWI Support Website Protect 724 Community Date Product Version Description 4/22/2014 ArcSight ESM 6.5c SP1 New Guide to Upgrade from ESM 6.5c to 6.5c SP1 3. Confidential ESM Upgrade Guide 3 Content Chapter 1: Upgrade ESM 6.5c to 6.5c SP1 ..... 5 Summary ..... 5 Migration from Oracle-Based ESM 5.5 to 6.5c SP1 ..... 6 Upgrade Log Files ..... 6 Planning your upgrade ..... 7 Upgrade ESM 6.5c to 6.5c SP1 ..... 8 Untar the installation .tar file ..... 8 Stops all services ..... 8 Keep these TCP ports open ..... 8 Upgrading of the ESM ..... 9 To confirm that the upgrade was successful ..... 14 Post-Upgrade Tasks ..... 15 Chapter 2: Upgrading the ArcSight Console ..... 17 Chapter 3: Checking the status of existing content after upgrading ..... 19 Chapter 4: Upgrading ArcSight SmartConnectors ..... 23 Updating the Forwarding Connector ..... 23 Chapter 5: Updating the hierarchical or other multi-ESM installation to 6.5c SP1 ..... 25 Summary 25 Updating a hierarchical deployment ..... 25 Updating a peer-to-peer configuration ..... 26 Appendix A: Updating standard content ..... 27 Preparing existing content for upgrades ..... 27 configurations retained during upgrade ..... 27 configurations that need to be restored after the upgrade ..... 28 Backing up existing resources before upgrading ..... 28 Performing the upgrade ..... 29 Reviewing and restoring content after upgrading ..... 29 Checking and reapplying configurations ..... 29 Review of customized content ..... 29 4. Content 4 ESM Upgrade Guide Confidential fixation of invalid resources ..... 30 Index ..... 31 5. Confidential ESM Upgrade Manual 5 Chapter 1 Upgrade ESM 6.5c to 6.5c SP1 This document describes the steps required to upgrade the ESM software components from 6.5c to 6.5c SP1. The following topics are covered here: Summary The following upgrade paths are supported for this release: . ESM 6.5c to ESM 6.5c SP1 - ESM 6.5c Patch 1 (or later) to ESM 6.5c SP1 If you experience issues during the upgrade, please contact HP ArcSight Customer Support for help. Be sure to have the following handy while you go to Help Support: - the log files listed in the Upgrade Log Files section, the /opt/arcsight/manager/tmp/ arcsight_dump_system_tables.sql. <timestamp> Summary on page 5 Migration from Oracle-Based ESM 5.5 to 6.5c SP1 on page 6 Upgrade Log Files on page 6 Plan your upgrade on page 7 Upgrade ESM 6.5c to 6.5c SP1 on page 8 Post-Upgrade Tasks on Page 15 To Upgrade Your Operating System... To upgrade your red hat Linux 6.2 operating system to 6.4 or 6.5, do so only before upgrading your ESM installation to 6.5c SP1. RHEL 6.2 is no longer supported. You can upgrade from RHEL 6.4 to 6.5 after upgrading ESM 6.5c to ESM 6.5c SP1. 6. 1 Upgrade ESM 6.5c to 6.5c SP1 6 ESM Upgrade Guide Confidential Migration from Oracle-Based ESM 5.5 to 6.5c SP1 </timestamp>The following migration paths are used for this release: - ESM 5.5 to ESM 6.5c SP1 - ESM 5.5 P1 (or later) to 6.5c SP1 migration instructions can be found in the Document Migration of ESM Resources from Oracle to CORR Engine. Upgrade log files The following log files are generated during the upgrade: Suite Upgrade Logs: /opt/arcsight/upgradelogs/suite_upgrade.log - This log gives you an overview of the upgrade progress. This is the first protocol you should consult if the upgrade fails. /opt/arcsight/suite/logs/install/ ArcSight_ESM_6.5c_SUITE_Install_ .log<timestamp>Logger Upgrade Logs: /opt/arcsight/logger/current/arcsight/logger/logs/logs directory: - logger_init_driver.log - contains the logger upgrade overview .log - contains the upgrade status of the MySQL logger tables./arcsight/logger/postgressql_ upgrade .out - contains the loggers postgres tables Upgrade Edition Manager Upgrade Logs: - /opt/arcsight/manager/upgrade/out/ <timestamp>/logs/upgrade/ Directory: - server.upgrade.log - Manager Upgrade Log server.upgrade.std.log - Manager Upgrade Standard Edition The timestamp should match the timestamp when you upgraded. Each upgrade attempt (see below) will leave a log folder with the name of the timestamp at the moment. Be sure to use the correct one. ArcSight Web Upgrade Logs: ' /opt/arcsight/web/logs/default directory: ' webserver.log - ArcSight Web upgrade log ' webserver.std.log - ArcSight Web upgrade standard output ArcSight Services Upgrade Logs: '/opt/arcsight/services/logs directory: ' arcsight_services.log - contains information about starting and stopping services during the upgrade arcsight_services_async.log . 1 Upgrade ESM 6.5c to 6.5c SP1 Confidential ESM Upgrade Guide 7 Plan your upgrade - Important! Make sure your ESM 6.5c is fully functional and its archives are intact. If you have a problem with your ESM 6.5c system, contact HP ArcSight Customer Support before upgrading. • Both XFS and EXT4 file system formats are supported in ESM 6.5c SP1. After the upgrade, you will remain in the same file system format as you were before. ESM does not support switching file system formats. Before you begin updating your ESM, we recommend that you open a ticket with HP ArcSight Customer Support to test the upgrade with your system tables to determine if specific steps are required for your configuration. Run the resource validator (resvalidate) before providing customer support for your system tables. For more information about running Resvalidate, see Caution below. Resolve any invalid resources that are used by the resource validator before you send the system tables to support. When planning your deployment, take two weeks to plan results. When HP ArcSight Customer Support tests your upgrade</timestamp> </timestamp> </timestamp> run more smoothly. Standard system-supplied reaources are updated with new versions during the upgrade. If you have customized one of these resources, back it up to .arb files before upgrading. For more information, see Preparing existing content for upgrade on page 27. • Download the ArcSightESMSuite-xxxx.tar upgrade file from the HP SSO download site. The xxxx in the file name represents the build number. When you click the .tar file to download it, its checksum appears at the bottom of the page. After downloading the .tar file, calculate the checksum for the downloaded .tar file and make sure it matches the checksum provided on the download page. • Make sure you have at least 50 GB of free space in your /opt directory. • Make sure you have at least 3 GB of free space in your /tmp directory. If you have connectors older than version 4.8.1, ArcSight recommends that you update them to the latest version. You can now upgrade to ESM 6.5c SP1. Please note that once you start upgrading, you will not be able to reset to the previous version of ESM. Do not attempt to use the uninstall link, it will not work for an upgrade. If the upgrade fails, contact HP ArcSight Customer Support for assistance with the upgrade process. Run the resource validator (resvalidate) located in the /opt/arcsight/manager/bin/ directory in the ArcSight Manager directory to verify that the resources are working properly before the upgrade. This prevents you from assigning incorrect resources to the upgrade. Run the resource validation script as follows: First run: arcsight resvalidate Then run: arcsight resvalidate -persist false 8. 1 Upgrading ESM 6.5c to 6.5c SP1 8 ESM Upgrade Guide Confidential Upgrade ESM 6.5c to 6.5c SP1 Untar the Installation .tar File 1 Log in as user Arcsight. 2 If you downloaded the .tar file to a different system than the system where your ESM 6.5c installation is located, move the .tar file to the ESM 6.5c computer. 3 Check the integrity of the .tar file just to make sure it was not truncated or corrupted during the download. Run: md5sum -c ArcSightESMSuite-xxxx.tar.md5 4 Untar the ArcSightESMSuite-xxxx.tar File: tar xvf ArcSightESMSuite-xxxx.tar All Services Stop. To do this: 1 Switch users to root: su - root Enter the password for the user root when

prompted. 2 From the location where you are using the Removed file: ./stop_services.sh Keep these TCP ports open before upgrading ESM, open the following TCP ports on your system if they are not already open, and make sure that no other process uses these TCP ports. Open the following TCP ports for external inbound connections: 8443 9443 9000 The following TCP ports are used internally for cross-component communication by ESM. Make sure that they and NOT in use: 1976, 28001, 2812, 3306, 5555, 6005, 6009, 6443, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8766, 8808 8880, 8888, 8889, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9095, 9 090, 9123, 9124, 9999, 45450 • If you want to upgrade your operating system from Red Hat Linux 6.4 to 6.5, do so after upgrading to 6.5c SP1. • If you are upgrading from a remote system connected to the ESM system, let X-Windows run on your remote system. Use ssh -X to perform the upgrade. • Do not change environment variables. In particular, if logger environment variables such as ARCSIGHT_LOGGER_BASE, UPGRADE, and ARCSIGHT_BASE are changed, the upgrade may fail. 9. 1 Upgrading ESM 6.5c to 6.5c SP1 Confidential ESM Upgrade Guide 9 Upgrade ESM To update the components in your ESM 6.5c installation: 1 Sign in as a user Arcsight. 2 Deploying Execution Permission to ArcSightESMSuite.bin File: chmod +x ArcSightESMSuite.bin 3 Upgrade: ./ArcSightESMSuite.bin 4 You will be prompted to confirm that you want to upgrade your existing ESM installation. Click Yes: Before the upgrade process begins, it checks to see if all upgrade requirements are met. If an error occurs at this point, correct the error and run the update file again. If you encounter errors after the start of the upgrade... Check the /opt/arcsight/upgradelogs/suite_upgrade.log file to see where the upgrade failed. If your log file does not contain the following line, you can fix the error that appears in the log file and retry the upgrade: Pre-upgrade tasks completed successfully. If the upgrade failed at any time after the pre-upgrade tasks, contact HP ArcSight Customer Support for help recovering from the bug and send them all /opt/arcsight/upgradelogs/*. Do not use the uninstall link, it will not work for upgrades. 10. 1 Upgrading ESM 6.5c to 6.5c SP1 10 ESM Upgrade Guide Confidential 5 Read through the introductory screen and click Next: The upgrade performs a pre-upgrade check of the redundant name to ensure that there are no duplicate resource names in the same group in your database. If duplicate names are found, an error is generated that causes the upgrade to stop. To resolve this: 1 Check the /opt/arcsight/upgradelogs/runcheckdupnames.txt file to determine which duplicate names are causing the conflict. 2 Resolve duplicate names manually. 3 Perform the upgrade Step 3 again. Please contact Customer Service via the HP SSO website for assistance. 11. 1 Upgrade ESM 6.5c to 6.5c SP1 Confidential ESM Upgrade Guide 11 6 Click the I accept the terms of the license agreement and then click Next. The button is not active until you scroll to the end of the license agreement. 7 Read the note and click Next: 12. 1 Upgrade ESM 6.5c to 6.5c SP1 12 ESM Upgrade Guide Confidential 8 Specify or select where you can like the link for the installation you want to create and click Next. 9 Check the settings and click Install. 11 Upgrade ESM 6.5c to 6.5c SP1 Confidential ESM Upgrade Guide 13 10 You will see the following progress bar: 11 Once the bits for all components have been copied, you will receive the following screen. Click Next: The upgrade is in silent mode, transmitting configurations, updating the schema, and updating the content. Before the upgrade process begins, the existing software components are backed up to the /opt/arcsight directory: manager.preUpgradeBackup -services.preUpgradeBackup -suite.preUpgradeBackup-Web.preUpgradeBackup-Backup-Backup///arcsight/logger/BLxxxx, where xxxx is the logger version number. 1. 1 Upgrade ESM 6.5c to 6.5c SP1 14 ESM Upgrade Guide Confidential . See the Upgrade Log Files section on page 6 for log files generated during the upgrade. The system tables are exported to /opt/arcsight/manager/tmp/arcsight_dump_system_tables.sql. <t imestamp=>For the Postgres dump, see /opt/arcsight/logger/current/arcsight/logger/user/logger/esm 65c.postgres. <timestamp>.dump 12 The installer will show you progress when the components are installed and the upgrade begins. 13 You will see the Upgrade Complete screen once the upgrade is complete. Click Done. 14 Important! Make sure that you run the following as a user root: su - root Enter the root password when prompted. /opt/arcsight/manager/bin/setup_services.sh 15 Follow the steps after the upgrade, which are listed in the Post-Upgrade Tasks section on page 15. To confirm that the upgrade was successful, you can check the /opt/arcsight/upgradelogs/suite_upgrade.log file that displays the error in the event of a failed upgrade. You can review the update summary report and logs to see if the manager has been successfully updated. The upgrade summary report applies only to the manager and cannot delete the dump file until the upgrade is complete and approved as good. You will need it to be restored in the event of a failed upgrade. 1. 1 Upgrade ESM 6.5c to 6.5c SP1 Confidential ESM Upgrade Guide 15 found in the Manager <ARCSIGHT_HOME>/upgrade/out/<time_stamp>/summary.html. If the upgrade is successful, you should see the following in the /opt/arcsight/upgradelogs/suite_upgrade.log: Upgrade completed successfully. Make sure that you verify that all components are available by running the following command: Status all you should see a response similar to the following: aps service is available arcsight_web service is available, the service is available logger_httpd service is available, logger_servers service is available logger_web service is available that the mysqld service is available.</time_stamp> </ARCSIGHT_HOME> </timestamp> </t> is another good way to check a successful upgrade: Build versions: esm:6.5.1.xxxx.0(BExxxx) storage:BLxxxxx Run the following command to check the RPM versions: rpm -qa|grep arcsight You have upgraded to ESM 6.5c SP1. Make sure you update the existing console. See Upgrade the ArcSight console on page 17. Tasks after the upgrade After you confirm that the upgrade was successful, you can perform the tasks in this section. To use the Forwarding connector, download the installation files for this and install them manually. To do this, you can find the forwarding connector documents. The NetFlow Monitoring content is triggered by NetFlow events from the following SmartConnectors that are not currently installed with ESM 6.5c SP1. ArcSight IP Flow SmartConnector - ArcSight QoSient ARGUS SmartConnector If you are upgrading to ESM 6.5c SP1, if you want to use the NetFlow Monitoring content, you must install and configure these SmartConnectors. For more information about getting smart connectors, contact your HP ArcSight sales representative. 16. 1 Upgrade ESM 6.5c to 6.5c SP1 16 ESM Upgrade Guide Confidential . File resources are not handled properly during the ESM upgrade. This results in unallocated file resources after the upgrade. For example, the .art files are created as new file resources in ESM 6.5c, and the resources receive new version IDs during the upgrade. The original files are stored in the file resource under the Unassigned folder. To work around this issue, you can safely delete the unassigned .art files after an upgrade because they are duplicates. The upgrade preserves custom speed templates by adding the .previous file extension and replaces the original file with an uncustomized version. To restore your customized version, simply delete the new file and change the name of your customized version by removing the .previous file extension. For example, if you customized the email.vm file, there are two files after the upgrade is complete: email.vm and email.vm.previous. Your customizations are in the second one that is not in use. To restore your customized version, delete email.vm and rename email.vm.previous to email.vm. If you have customized the Cases user interface for the existing 6.x environment, the customizations are not automatically copied during the upgrade. The upgrade creates backups of multiple files and places them in preUpgradeBackup folders. Most of them will be restored correctly after the upgrade. in this version some do not. The workaround is to manually restore it after the upgrade as follows: a copy label_strings_en.properties and resource_strings_en.properties at /opt/arcsight/manager.preUpgradeBackup/i18n/common to /opt/arcsight/manager/i18n/common. b Copy caseui.xml at /opt/arcsight/manager.preUpgradeBackup/config to /opt/arcsight/manager/config. c If a custom case detail mapping is case detail mapping, audit events exist, copy case.properties to /opt/arcsight/manager.preUpgradeBackup/config/audit to /opt/arcsight/manager/config/audit. d Restart the manager for these changes to take effect. If the *_en.properties file does not exist under /opt/arcsight/manager.preUpgradeBackup/i18n/common, copy the *.properties file. If present, copy *_en.properties. For other locales, copy the file *_<locale>.properties. 17. Confidential ESM Upgrade Guide 17 Chapter 2 Upgrade of the ArcSight Console The ArcSight Console Upgrade Process should be performed on all ArcSight Console instances that connect to the manager running on the upgraded system. 1 Exit the ArcSight console when it is running. 2 Download the appropriate installation file for your platform from the HP SSO download website. The xxxx in the file name represents the console build number: ArcSight-6.5.1.xxxx.0-Console-Win.exe - ArcSight-6.5.1.xxxx.0-Console-Linux.bin - ArcSight-6.5.1.xxxx.0-Console-MacOSX.zip 3 If you downloaded the 6.5c SP1 Console installation file to another computer, you want to transfer it to the computer on which you want to install the console. 4 Run the installation file that is appropriate for your platform: - On Windows: Double-click ArcSight-6.5.1.xxxx.0-Console-Win.exe - On Macintosh: Unzip the following file: ArcSight 6.5.1.xxxx.0-Console-MacOSX.zip and double-click the installer. On Linux: Run the following command. ./ArcSight-6.5.1.xxxx.0-Console-Linux.bin To install in console mode, run the following command using the shell prompt, and then follow the instructions in the window. ./ArcSight-6.5.1.xxxx.0-Console-Linux.bin -i console step through the screens of the installation wizard. In particular, enter values as described below for the following wizard screens: • Introduction - Read the introduction and click Next. License Agreement - The I accept the terms of the license agreement will be disabled until you read Contract 18 and scroll to the end of the agreement. 2 Upgrade ArcSight Console 18 ESM Upgrade Guide Confidential Text. After reading the text, click the I accept the terms of the license agreement, and then click Next. • Special notification - Read the notification and click Next. • Select Installation Folder - Enter a path for 6.5c SP1 that is different from the location where <ARCSIGHT_HOME>where the existing console is installed. Select Shortcut Folder (on Windows) or LinkFolder (under UNIX) - Specify or select where to create the ArcSight console icon, such as.B in an existing program filegroup or on the desktop on Windows. Click Next. • Pre-installation summary - Check the settings and click Install. After you go through the installation wizard, the configuration wizard starts automatically. 5 The console installer prompts you,</ARCSIGHT_HOME> </locale> </locale> and gives you the ability to copy your existing settings to the new console. Settings such as connection information, including the Manager host name or IP address and port number, and authentication information, including authentication type. Select Yes, I want to transfer the settings and click Next. 6 You will be prompted to enter the location of your previous console installation. Click Next. 7 For more information about the remaining screens, see the ESM Installation and Configuration Guide for installing a console using the Installation Wizard. 8 Start the ArcSight console. 9 After you upgrade a console to 6.5c SP1: a You can view the updated default content b All SmartConnectors connect to the manager on the ESM system. c The manager receives events from the SmartConnectors. If you don't see any event viewers in the console at first, select the All Active Channels/ArcSight System/Core/Live channel to view real-time events. DO NOT install the 6.5c SP1 console in the same location as the existing console. Installing in a different location prevents the installer from overwriting your existing configuration so that you can migrate settings from it. Be sure to select the <ARCSIGHT_HOME>current directory of your previous installation. 19. Confidential ESM Upgrade Guide 19 Chapter 3 Reviewing the status of existing content after the upgrade After the upgrade is complete, ensure that all your content has been successfully transferred to the 6.5c SP1 structures. Manually correct any content that has been migrated to an unwanted location or whose conditions are no longer valid. • Under Unassigned e.V., check for resources. Enable the Unassigned group in the resource tree for all resource types. The unassigned groups in each resource type contain all resources created by the customer that reside in a 6.5c system group. If you find resources in it, move them to other custom groups accordingly. HP recommends that you do not move these resources to Standard ArcSight content groups because they will be moved back to the Unassigned group for future upgrades. • Restore customizations to standard content resources. Default content is a group of system-provided resources that are updated with new versions during the upgrade. If you customized one of these system-provided resources, your customizations were overwritten during the upgrade. Set your configurations by importing the backed-up .arb files that you saved before the upgrade. • Check if assets are disabled under . The Disabled group in the asset resource structure is dynamic, which means that it queries the manager every two minutes for assets to be disabled. After the upgrade, verify that items have been disabled and moved to the Disabled group in the Assets resource tree. If so, check the disabled asset to see why it has been disabled and fix it accordingly. For </ARCSIGHT_HOME> </ARCSIGHT_HOME> If an asset's IP address is outside the scope of the updated zone, either expand the scope of the zone or assign the resource to another zone. You can also delete an object that has been disabled when it is no longer needed (click the asset on the right and select Delete). If, for existing assets, two assets in the same zone have the same host name or IP address, one of them becomes invalid after the ESM upgrade to 6.5c SP1. This can occur with assets whose host names are Fully Qualified Domain Name (FQDN) of the asset. In 6.5c SP1, only the host name is extracted from the FQDN and used when comparing the two assets. For example.B two assets have FQDNs myhost.mycompany.com and myhost.mycompany.us.com, only the myhost value is used to compare them, and their domain names are ignored. Because the host name is the same, these two assets are considered conflicting assets, and one of them becomes invalid. If you want to override this and use the FQDN instead, set the following property in the server.properties file: 20. 3 Check the status of existing content after upgrading 20 ESM Upgrade Guide Confidential asset.lookup.hostname.resolve.without.domain=true . User resource. Only the system user has access permissions to the Resource Structure /All Users. Therefore, any users or groups that you created in /All Users in the previous installation are now available under Custom User Groups. After the upgrade, make sure that the user ACLs are correct and remain valid, depending on how standard ArcSight content is organized for 6.5c SP1. For example, administrator access should only be granted to people who have permission to work with system-level content, such as.B for ArcSight System and ArcSight Administration. Update user ACLs manually. • Zone resource. Verify that zones became invalid during the upgrade process. • Fixed zones that you want to keep but were invalidated during the upgrade. • Make sure that the items assigned to the den zones that were moved or invalidated during the upgrade maintain their connections to the appropriate 6.0c zones. • Delete any invalid zones that you no longer want to keep. If you have made adjustments to the existing default zones, manually edit the new resource to restore the customizations you made in the appropriate 6.5c SP1 zone. Do not import the old zone. • Repair invalid resources. During the upgrade process, the resource validator identifies all resources that are upgrade (conditions that no longer work). Review the update summary report in the <ARCSIGHT_HOME>/upgrade/out//summary of the<time_stamp>Manager.html to find invalid resources and resolve their conditions accordingly. Customer-created content related to standard ArcSight content has changed significantly and may not work</time_stamp> </ARCSIGHT_HOME> </ARCSIGHT_HOME> Expected. An example would be a rule that uses an ArcSight system filter whose conditions have been changed so that the rule matches more events than you expect, or does not match the events you expect. Another example is a floating average data monitor whose threshold has been changed. To verify that the resources you rely on are working as expected, perform the following checks: . Send events that you know should trigger the content through the system by using the Play with Rules feature. For more information about this feature and how to improve it for 6.5c SP1, see the online Help topic Checking Rules with Events. • Check the active Live or All Events channel to verify that the correlation event is raised and verify that the data monitors you create return the expected output based on the test events you are sending. • Ensure that notifications are sent to recipients in your notification destinations as expected. • Verify that the lists you created to support your content are collecting the playback with rule data as expected. • Outdated resources and resource groups Some of the ESM 6.0c resources and resource groups have been deprecated, meaning they are no longer needed. Resources are deprecated for several reasons: The resource was product-specific or vendor-specific. The resource was inefficient or presented marginal value (e.B. a collection of 10 reports was really a report with nine small variations). 21. 3 Checking the status of existing content after upgrading Confidential ESM Upgrade Guide 21 - New 6.5c SP1 features achieve the same goal more efficiently. During the upgrade, stale resources are moved to a separate deprecated group for this resource type. The resources that are moved to them retain the hierarchy they had in their original ESM 6.5c form. Resources that have been moved to this folder are still active, so if you rely on one of these resources, they will still exist and work. If you no longer need the stale resources, you can safely delete them after the upgrade. If you still need an outdated resource, you can move it back to an active resource tree and change its conditions as needed, and clear the Obsolete check box to repair erroneous references. After upgrading to ESM 6.5c SP1, you can use the Find Resources feature to generate a list of outdated resources: 1 to Edit > Find resources. 2 In the Search query field, enter the keyword out of date and press Enter. If you have created resources that relate to an outdated resource, or if you have modified an outdated resource to point to a resource that is not deprecated, some connections may be interrupted during the upgrade. If you still need to use the deprecated resource, resolve the broken reference by re-entering the deprecated resource to the resource tree and change the conditions as needed. HP no longer supports stale resources, so if you want to restore an outdated resource, you are responsible for maintaining it. HP also recommends that you verify that the new 6.5c SP1 resources meet the same goal more efficiently. 22. 3 Checking the status of existing content after upgrading 22 ESM Upgrade Guide Confidential 23. Confidential ESM Upgrade Guide 23 Chapter 4 Upgrade From ArcSight SmartConnectors SmartConnectors SmartConnectors must run version 4.8.1 or later. However, HP strongly recommends that you update all connectors to the latest available version. Download installation files according to your SmartConnector platforms. Use the .aup file for remote updating. Follow these steps to update SmartConnectors: 1 Identify any SmartConnectors that you want to update. 2 If you downloaded the SmartConnector installation file to another computer, transfer it to your SmartConnector computer. 3 Run the SmartConnector installation file. 4 Follow the installation wizard screens to update your SmartConnector. 5 Repeat Step 3 and Step 4 for each SmartConnector you identified in step 1. ESM provides the ability to remotely update the SmartConnectors with the .aup file. For detailed instructions on how to remotely upgrade SmartConnectors, refer to the SmartConnector User's Guide. For an overview of the SmartConnector installation and configuration process, see the SmartConnector User's Guide. For complete installation instructions for a specific SmartConnector, see the configuration guide for that connector. The product-specific configuration guide contains specific device configuration information, installation parameters, and device event mappings to ESM fields. For updating the Forwarding Connector, see the ArcSight Forwarding Connector Configuration Guide for instructions on how to update the Forwarding Connector. If FIPS mode is enabled for the Forwarding Connector when updating the Forwarding Connector, you do not need to re-import the Manager certificate when forwarding the connector. 24. 4 Upgrade of ArcSight SmartConnector 24 ESM Upgrade Guide Confidential 25. Confidential ESM Upgrade Guide 25 Chapter 5 Upgrading hierarchical or other multi-ESM installation to 6.5c SP1 This chapter describes the method for upgrading a multi-ESM deployment from 6.5c to 6.5c SP1. Summary In a multi-ESM deployment, two or more ESMs are deployed in one of the following configurations: - In a - Data from one or more source ESMs is routed to a central ESM. In a high-availability (failover) configuration, there is an alternate instance of an ESM in standby that can be applied when the active ESM is unavailable. In a peer-to-peer configuration, data is sent from a SmartConnector to more than one independent ESM for redundancy. The process of updating in a multi-ESM deployment is similar to upgrading in a single ESM deployment. However, they update the target ESMs first, and then the components connected to them, followed by the standby or source ESMs. ArcSight forwarding connectors may not be updated until the corresponding ESMs have been updated. Forwardconnectors must be the version that came with ESM or the latest version. Update a hierarchical deployment To update a hierarchical deployment, follow these steps, starting with the target ESM. 1 Update any SmartConnectors that are not running a current version. For best results, use version 4.8.1 or later. 2 Stop all services on the current ESM. 3 Follow the instructions in Upgrade ESM 6.5c to 6.5c SP1 on page 5 to upgrade your ESM 6.5c to 6.5c SP1. 4 Once ESM 6.5c SP1 is running, follow the instructions in the ArcSight Console upgrade on page 17 to update all associated consoles. 5 Update the forwarding connector associated with this ESM to create ArcSight-7.0.1.6992.0-SuperConnector-to<platform><extension>. 26. 5 Upgrading the hierarchical or other multi-ESM installation to 6.5c SP1 26 ESM Upgrade Guide Confidential If the Forwarding Connector is connected to more than one target ESM, update all of these ESMs before upgrading the Forwarding Connector. Repeat this process until all ESMs and forwarding connectors are updated at each hierarchy level. Update a peer-to-peer configuration To update a setup where SmartConnectors send data directly to more than one ESM—that is, two or more ESMs are peers—follow the upgrade process described in the upgrade technical note that applies to your upgrade path to one of the ESMs, followed by the other ESMs. 27. Confidential Examples and BookBuilding Procedures Upgrade Guide 27 Appendix A Upgrade Standard Content This chapter covers the following topics. Preparing existing content for upgrade Most of the standard content requires no configuration or special preparation for the upgrade. Update preparation is recommended only for content that has been configured and for which the configuration is not retained after the upgrade. Configurations retained during the upgrade The following resource configurations are retained during the upgrade process. These resources do not require recovery after the upgrade. • Asset modeling for network assets, including: - Assets and asset groups and their settings - Asset categories, apply to assets and asset groups, vulnerabilities applied to assets, user-value zones, smart zones, users and user groups, reports, notification plans, and priority settings - Preparing existing content for upgrade to page 27 Performing the upgrade on page 29 Review and restore content after upgrading to page 29</extension> </platform> </platform> In the version you are upgrading to, it is moved to a folder in the resource tree called Deprecated during the upgrade. Example: All Rules/Arcsight System/Obsolete. If you are using this deprecated resource, move it to your own group after the upgrade. 28. Upgrading standard content 28 samples and BookBuilding Procedures Upgrade Guide Confidential configurations that require post-upgrade recovery The following resource configurations require post-upgrade recovery. • Any standard content resources that you have modified, including active lists—All custom content or special changes that are not already described in this document (including customizations made by Professional Services) Back up existing resources before upgrading. To support the process of reconfiguring resources that need to be reused after the upgrade, back up the resources that you identify in post-upgrade configurations on page 28 and export them to a package. After the upgrade, you can re-import the package and use the existing resources as a reference to restore configurations in the updated environment. To create a backup of the resources that need to be restored after the upgrade: 1 Create a new group under your personal group for each resource type (filter, rule, active list). Provide a name that identifies the content. Right-click your group name and select New Group. 2 Copy the resources to the new group. Repeat this process for each type of resource you want to back up. Select the resources you want to back up and drag them to the backup folder that you created in step 1. In the Drag and Drop Options dialog box, select Copy. 3 Export the backup groups to a package. • In the Navigator panel, right-click your group name and select New Package. In the Package Editor, in the Inspect/Edit panel, name the package to identify the content. Select the group you created in step 1, right-click and select Add to package. Select your new package and click OK. Right-click your package name and select Export Package to Bundle. Only active list attributes, such as TTL and description, are not retained during the upgrade. All entries that have been removed from an original active list will be restored during the upgrade. All added to an active list are retained during the upgrade. Before you back up existing resources, run the resource validator (resvalidate.sh) that is in the manager's bin scripts in the ESM Manager, <ARCSIGHT_HOME>to verify that the resources are working properly before the upgrade. This prevents you from assigning incorrect resources to the upgrade. During the upgrade process, the content is automatically run through a resource validator (see Fixing Invalid Resources on page 30). Copy and paste configurations from the old resources to the new one instead of backing up </ARCSIGHT_HOME> </ARCSIGHT_HOME> copy and paste configurations from the old resources into the new ones one at a time. This procedure ensures that you maintain your configurations without overriding the improvements provided in the upgrade. 29. An upgrade standard content samples and BookBuilding Procedures Upgrade Guide 29 Perform the upgrade After exporting a copy of the configured resources to a backup package, you can perform the upgrade process. For more information, see Updating ESM 6.5c to 6.5c SP1 on page 5 for upgrade procedures. Review and restore content after the upgrade is complete, perform the following checks to ensure that all content has been successfully transferred to the new environment. Review and reapply configurations Review and restore standard content after the upgrade. 1 Make sure that your configured resources, which are listed in the Preserve Configurations section during the upgrade on page 27, have retained their configurations as expected. 2 Configure the resources that can be recovered. re-import the package that you created in Save Existing Resources before upgrading on page 28. b Copy the configured configurations copied in the package and paste the configurations into the new resources that were installed with the upgrade. Copying your configurations one at a time instead of overwriting the new resources with the old ones ensures that you keep your configurations without overriding the improvements provided with the updated content. Review ingese content It is possible that updates to the default content when the default content is updated will cause the resources you create will not work intentionally. For example, a rule may be triggered too often or not at all if it uses a filter in which conditions have changed. To verify that the resources you rely on are working as expected, check the following: Send events that you know to trigger the content through the system by using the Play with Rules feature. For more information about this feature, see the ArcSight Console User's Guide. • Check live events. Check the active Live or All Events channel to ensure that the correlation event has been raised. Verify that the data monitors you create return the expected output based on the test events you are sending. • Check the notification targets. Make sure that sent to the recipients in your notification destinations as expected. • Check active lists. Verify that any active lists that you have created to support your content are collecting playback with rule data as expected. • Repair invalid resources. During the upgrade process, the resource validator identifies all resources that are invalidated during the upgrade (conditions that no longer work). Find invalid resources and resolve their conditions accordingly. For more information about invalid resources, see Fix Resources, below. 30. An Upgrade Standard Content 30 Samples and BookBuilding Procedures Upgrade Guide Confidential Fixation Invalid Resources During the upgrade process, the content runs through a resource validator that verifies that the values expressed in the resource condition statement continue to apply to the resource in the new format, and that all resources on which it depends are still present and valid. The resource validator runs on any resource that contains a condition statement or populates the asset model, such as.B: Active Channel Filters - Data Monitors - Rules - Reports - Query Reports and Schedules - Asset and Asset Ranges - Zones It is possible that during the upgrade the condition statement for a resource that you have created or modified will become invalid. For example, if the schema of an active list provided by ArcSight changes from one version to another, and a resource you create reads entries from that list, the condition statement in the resource you created no longer matches the schema of the active list, and the logic is invalid. If the installer performs the resource validation check and finds an invalid resource, the report it generates at the end of the upgrade determines why the resource is invalid. The Upgrade Installer: - Saves the reason why the resource was found invalid in the database so that you can generate a list of invalid resources that you can use later to manually resolve the issues. • Disables the resource so that it does not attempt to evaluate live events in their invalid state. 31. Confidential ESM Upgrade Guide 31 A Access Control Lists (ACLs) 20 Assets, disabled 19 C Cases UI customizations 16 console upgrade 17 Content verification status after upgrade 19D Disk memory, free 7 E EXT4 File System 7 F File Systems 7 Forwarding Connector 15 H Hierarchical Upgrade 25 I Invalid Resources 20, 30 L Log Files 6 LogsSight Arc Services Upgrade 6 ArcSight Web Upgrade 6 Logger Upgrade 6 Manager Upgrade 6 Upgrade 6 Suite 6 M Migration Paths 6 Multi-ESM Deployment 25 O Operating System Upgrade 5P Peer-to-Peer Upgrade 26 Ports to Keep Open 8 After Upgrade Tasks 15 Reputation Security Monitor 15 R Reputation Security Monitor 15 Resources Validator 7 Resources, outdated 20 resources, invalid 20 resources, unassigned 19 RHEL upgrade 5 S SmartConnectors 23 default content 27T TCP ports 8 U-upgrade backup directories 13 before upgrade 7 confirm if successful 14 confirm upgrade successfully 14 invalid resources 30 paths 5 tasks 15 after upgrade prepare for upgrade 27 prerequisites 7 29 Summary 5 Check Customer Content 29 Upgrade ArcSight Console 17 Forwarding Connector 23 SmartConnectors 23 with X-Windows 8 V Speed Templates 16 Index 32. 32 ESM Upgrade Guide Confidential X XFS File System 7 Z Zones 20 20 20