Rhel 6 package

9.17. Package Group Selection Now that you have made most of the choices for your installation, you are ready to confirm the default package selection or customize packages for your system. The Installation Defaults screen appears with the default package details set for your Red Hat Enterprise Linux installation. This screen varies depending on the version of Red Enterprise Linux you are installing. If you installed Red Hat Enterprise Linux in text mode, you can't make package selection. The installer automatically selects packages only in the base and basic groups. These packages are sufficient to ensure that the system is operational at the end of the installation process, ready to install updates and new packages. To change the package selection, complete the installation, then use the Add/Remove software application to make unwanted changes. By default, Red Hat Enterprise Linux installation loads a selection of software that is suitable for a system deployed as a core server. Note that this installation does not include a graphical setting. To include a selection of appropriate software for other roles, click the radio button corresponding to one of the following options: Basic Server This option provides a basic installation of Red Enterprise Linux for use on a server. Database Server This option provides the MySQL database with PostgreSQL. This web server option provides the Apache web server. Desktop This option provides OpenOffice.org suite productivity, graphical tools like the GIMP, and multimedia applications. This Software Development Workstation Option provides the necessary tools to compile software on your Red Enterprise Linux system. Minimal this option provides only the bulk packages to run Red Hat Enterprise Linux. A minimal installation provides the basis for single-purpose server or desktop devices and maximize performance and security on such an installation. To customize your package set further, select the Customize now option on the screen. Click Next to take you to the Selection Group Package screen. 9.17.1. Install from Additional Repositories You can define additional repositories to increase the software available to your system during installation. A repository is a network location that stores software packages along with the metadata that describes them. Many of the software packages used in Red Hat Enterprise Linux require other software to be installed. The installer uses the metadata to ensure that these requirements are met for each piece of software you choose for installation. The basic options are: The ClusteredStorage repository includes packages for storage groups using the Global Red File System (GFS). The HighAvailability repository includes packages for high-availability clustering (also known as blinkers failover) using the Available Red Service components. Repositatory loadbalans include packages for cluster using Linux Virtual Server (LVS). The Exquisite Hat Enterprise Linux 6 repositatory is automatically selected for you. It contains the complete collection of software that was released as Red Enterprise Linux 6, with the various pieces of software in the versions that were current at the time of release. To include software from extra repositories, select Add additional software repositories and provide the location of the repository. To edit an existing software repository software, select the storage from the list and then select Modify Repository. If you change the repository information during a non-network installation, such as from a Red Hat Enterprise Linux DVD, the installer installation prompts you for network configuration information. If you select Add additional software repositories, the Edit Storage dialog appears. Provide a Repository name and URL of Repository for where it is. Once you've located a mirror, determine the URL to use, find the directory on the mirror that has a directory named reboot. Once you provide information for an additional repository, the installer reads the package metadata on the network. Software that is specifically marked is then included in the group package selection system. If you choose Return from the package selection screen, any extra repository data you can enter lost. This allows you to effectively cancel extra repositories. Currently there is no way to cancel only one repositatory once entered. I would like to know how to do this via the internet, something similar to CentO's official search

page. When you started Automation Basics Advanced Subject Release Note Change in development 3.2.0 – April 27, 2020 3.1.0 – June 27, 2019 3.0.1 - May 24, 2019 3.0.0 - April 18, 2019 2.10.4 - March 15, 2019 2.10.3 - March 06, 2019 2.9.3 – 06 March 2019, 2019 2.10.2 - February 21, 2019 2.10.1 - 19 December 2018 2.10.0 - 1 December 3, 2018 2.9.1 - October 03, 2018 2.9.0 – September 16 , 2018 2.8.1 - July 18, 2018 2.8.0 - July 10, 2018 2.7.2 - May 16, 2018 2.7.1 – April 20, 2019 - May 16, 2018 2.7.1 – April 20, 2018 2.7.0 - April 12, 2018 2.6.0 - January 19, 2018 2.5.1 - 14 December 2017 2.5.0 - October 25, 2017 2.4.1 – September 12, 12, 2017 2017 2.4.0 - August 23, 2017 2.3.2 - July 28, 2017 2.3.1 – July 07 2017 2.3.0 - June 19, 2017 2.2.1 – April 3, 2017 2.2.0 – February 27 , 2017 2.1.1 - 16 December 2016 2.1.0 - December 05 , 2016 2.0.1 - September 30, 2016 2.0.0 – August 31, 2016 1.6.0 - August 8, 2016 1.5.1 - July 13, 2016 1.5.0 – June 24, 2016 1.4.0 – April 18, 2016 1.3.2 – February 12, 12, 2016 2016 1.3.1 - January 25, 2016 1.3.0 – January 22, 2016 1.2.0 - December 07, 2015 1.1 1 - November 13, 2015 1.0 - October 27, 2015 0.13.2 - September 09, 2015 0.13.1 - August 28 , 2015 0.13.0 - August 24, 2015 0.12.2 - August 11 , 2015 0.12.1 - July 31, 2015 0.12.0 - July 20, 2015 0.11.6 - July 2, 2015 0.11.5 - July 1, 2015 2015 0.11.4 - June 30, 2015 0.11.3 - June 16, 2015 0.11.2 - June 2015 12, 2015 0.11.11 - 8 June 2015 0.11.0 – June 5, 2015 v.9.2 – May – May - 2015 v0.9.1 – May 12, 2015 v0.9.0 – April 29, 2015 v0.8.3 – March 23, 2015 v0.8.2 - March 10, 2015 v0.8.1 – 10 March 10, 2015 v0.8.0 - 2 March 2, 2015, 2015 v0.7 – January 16, 2015 v0.6.0 – December 8, 2014 v0.5.1 – November 3rd, 201 4 Upgrade Note Roadmap 3.3 Other Security Release Stories Report a Vulnerability How to Vulnerability Handle StackStorm Note the document you are currently reading is for version 3.2.0. Click here to view documentation for the latest stable version. If you're just looking for a quick one-liner installation, check the top-level guide installed. If you need a customized installation, use this guide for step-by-step instructions for installing StackStorm on one system as per the Reference deployment. Please check the supported versions and system requirements. RHEL 6 cannot ship with lebffi-wash package, which is a dependency for StackStorm. If that is the case, set up the server repositatory – Optional, follow the instructions in . Or, get a version of libffi-devel compatible with the libffi version installed. For example: ~$rpm -qa libffif-3.0.5-3.2.el6.x86_64 sudden localinstall -y ftp://rpmfind.net/linux/centos/6.9/os/x86_64/Packages/libffi-devel-3.0.5-3.2.el6.x86_64.rpm Use a service such as find the necessary RPM. If your system has SELinux in Supplement mode, please follow these instructions to adjust SELinux policies. This is necessary for successful installation. If you're not happy with these rules, you may want to tweak them according to your safety practices. First check if SELinux is in Enforce mode: If before the command returns 'Enfose', then run the following commands: # SELINUX management tool, not available for some minimum sudo yum installation install -y policycoreutils-python # Allow network access for nginx setsebool -httpd_can_network_connect P<3> <7> 1 Note If you see messages such as SELinux: Couldn't scroll down policy, meaning you are trying to adjust policy configuration when seLinux is disabled. You can ignore this error. Note the versions currently supported in MongoDB are 3.4 and 4.0. This is the version installed by the install script. MongoDB 4.0 is installed by default on Ubuntu 18.04 and RHEL/CentOS8. MongoDB 3.6 is also supported by StackStorm >=3.0.0, but we have observed some performance with MongoDB 3.6 so the default version that is installed on Ubuntu Xenial (16.04) and EL7 (CentOS 7 and RHEL 7) is still 3.4. Install MongoDB, rabitMQ, and PostgreSQL: sudo yum -y install # Add keys and breaks for latest MongoDB (3.4) sudo rpm -import sudo sh -c cat <EOT> /etc/yum.repos.d/mongodb-org-1 3.4.rest [mongodb-org-3.4] name=MongoDB Repository baseurl = 1</EOT>gpgkey= EOT sudo yum -y install crudini sudo yum -y install mongodb-org sudo um -y install rabbitmq -server sudo service start sudo service rabbitmq -server start sudo chkconfig mongod on sudo chkconfig rabitmq -server on # Install and configure posts 9.4. Based on the OS type, install redhat one or center' center. # RHEL: if grep -q Red Hat/etc/redhat-release; Then sudo yum -y localinstall female #CentOS: if green -q CentOS/etc/redhat-release; Then sudo yum -y localinstall fido yum -to install postgresql94-server postgresql94-contribute postgresql94-devel# Initialize PostgreSQL postgresql service-9.4 forbidden # Make the local connection use an MD password -encrypted for sed sudo authentication -i /s/\(host.*all.*all.*127.0.0.1\/32.*)\ident/1md5/ /var/lib/pgsql/pgsql/9.4/data/pg_hba.conf sudo sed -i s /s/(host.*all.*:1\/128.**)ident/\1md5 //var/lib/pgsql/9.4/data/pg_hba.conf # Start Postgre Service sudo postgresql service-9.4 start sudo chkconfig postgresql-9.4 on the following script will detect your platform and architecture and configure the appropriate StackStorm reputability. It will also add the GPG key used for package signing. curl -s | sudo bash sudo yum install -y st2 st2 est2mistral If you don't run RabitMQ, MongoDB or PostgreSQL on the same system, or have changed their default, please adjust the following settings: RabbitMQ connection of / etc/st2/st2.conf and /etc/mistral/mistral.conf MonDB at /etc/st2/st2.conf PostgreSQL in /etc/mistral/mistral.conf We see the configuration document for more information. The key-value store allows users to store encrypted values (secrets). These are stored using symmetric encryption (AES256). Pou jenere yon kle crypto, kouri komandman sa yo: DATASTORE_ENCRYPTION_KEYS_DIRECTORY =/elatriye DATASTORE_ENCRYPTION_KEY_PATH/st2/st2/st2=${DATASTORE_ENCRYPTION_KEYS_DIRECTORY}/datastore_key.json sudo mkdir -p ${DATASTORE_ENCRYPTION_KEYS_DIRECTORY} sudo st2-jenere-senm kripto-kle-chemen ${DATASTORE_ENCRYPTION_KEY_PATH} # Asire ou ke selman st2 itilizate ka li strp nan chgrp sudo sudo ${DATASTORE_ENCRYPTION_KEYS_DIRECTORY} sudo chmod o-r {{DATASTORE_ENCRYPTION_KEYS_DIRECTORY} sudo xNUMX} st2rp $ {DATASTORE_ENCRYPTION_KEY_PATH} toudo chmod o-r $ {DATASTORE_ENCRYPTION_KEY_PATH} # mete chemen nan dosye a kle nan konfigirasyon an sudo krudini -mete / elatriye / st2 / st2/st2.confyvalue encryption_key_path $ {DATASTORE_ENCRYPTION_KEY_PATH} sudo st2ctl rekomanse-eleman st2api kouri komandman sa yo yo mete kanpe baz done a Mistral PostgreSQL: # Kreye Mistral DB nan PostgreSQL chat << EHD | toudo -u postgres psql CREATE MISTRAL ROLE AND CREATE LOGIN ENCRYPTED PASSWORD 'StackStorm'; CREATE DATABASE Mistral Property EHD # Enstole Mistral Mistral tab, elatriye /opt / stackstorm / mistral / bin / mistral-db-jere -config-file /etc/mistral/mistral.confgrade tet # Enskri mises aksyon / opt / stackstorm / mistral / bin / mistral-db-jere-config-file /elatriye / mistral /mistral.confulate | grep -v -e openstack -e keystone -e ironicclient Nan kouri lokal yo ak aleka aksyon koki, StackStorm sevi ak yon itilizate sistem espesyal (pa stanley default). Pou aksyon linux, SSH yo itilize. Nou rekomande pou konfigirasyon piblik kle ki baze sou SSH akse sou tout gen tout anime aleka. Nou rekomande tou konfigirasyon SSH akse nan lokalhost pou ko kouri egzanp ak tes. Kreye StackStorm sistem itilizate, pemet modpas toudo, epi mete kanpe akse nan lokalhost pou ke Aksyon SSH ki baze sou ka teste lokalman. You will need elevated privileges to do this: # Create an SSH system user (default 'stanley' user may already exist) sudo useradd stanley sudo mkdir -p /home/stanley/.ssh sudo chmod 0700 /home/stanley/.ssh # Generate ssh keys sudo ssh-keygen -f /home/stanley/.ssh/stanley_rsa -P # Authorize key-based access sudo sh -c 'cat /home/stanley/.ssh/stanley_rsa.pub >> /home/stanley/.ssh/authorized_keys' sudo chown -R stanley:stanley /home/stanley/.ssh # Enable passwordless sudo sudo sh -c 'echo stanley ALL=(ALL) NOPASSWD: SETENV: ALL >> /etc/sudoers.d/st2' sudo chmod 0440 /etc/sudoers.d/st2 # Make sure 'Defaults requiretty' is disabled in '/etc/sudoers' sudo sed -i -r s/^Defaults\s+\+?requiretty/# Defaults +requiretty/g /etc/sudoers Configure SSH access and enable passwordless sudo on the remote hosts which StackStorm will be running remote actions on via SSH. Le li sevi avek kle a piblik ki te pwodwi nan etap anvan an, swiv enstriksyon yo nan Configured SSH. Pou kontwole Windows bwat, configured akse pou Windows kouri. Si ou ap itilize yon itilizate diferan, oswa chemen nan kle SSH yo, ou pral bezwen chanje seksyon sa a nan / elatriye / st2 / st2.conf: [system_user] itilizate = stanley ssh_key_file = / kay / stanley / ssh / stanley_rsa Komanse sevis: Detekte Enskri, reg ak aksyon: komandman sa yo pral teste enstalasyon StackStorm ou. They should all complete successfully: st2 --version st2 -h # List the actions from a 'core' pack st2 action list --pack=core # Run a local shell command st2 run core.local -- date -R # See the execution results st2 execution list # Fire a remote comand via SSH (Requires passwordless SSH) st2 run core.remote hosts='localhost' -- uname -a # Install a pack st2 pack install st2 Use the supervisor script to manage StackStorm services: sudo st2ctl start|stop|status|restart|restart-component|reload|clean At this point you have a minimal working installation, and can happily play with StackStorm: follow the Quick Start tutorial, deploy the examples, explore and install packs from StackStorm Exchange. Men, pa gen okenn ke kontan san yo pa yon UI Entenet, pa gen okenn sekirite san yo pa SSL oswa otantifikasyon, pa gen okenn plezi san chatOps, e pa gen okenn lajan san yo pa Ekstrem composer. It's over! Deployment of reference uses a file-based authentication for simplicity. See Authentication to configure and use PAM or LDAP authentication authentication. To set up authentication with file-based provider: Create a user with a password: # Install htpassw utility if you don't have it sudo yum - to install httpd-tool # Create a user file in a password file. htpasswd -bs/etc/st2/htpasswd st2admin '' Enable and configure authentication of /etc/st2/st2.conf:[auth]#... allow = True backend = flat_file backend_kwargs = { file_path : / etc / st2 / htpasswd } #... Restart the st2apipi service: sudo st2ctl restart - Component st2api Authenticate, and check that it works: # Login - you will push for password (default ') st2 login st2admin # Check that it works st2 list NGINX used to serve static file WebUI, redirect HTTP to HTTPS, provide SSL termination, and reverse-proxy st2auth and st2api Point API. To set it up: install the st2web and nginx package, generate certificates or set your existing certificates under /etc/ssl/st2, and configure nginx and StackStorm to supplied site configuration st2.conf. StackStorm depends on version of Nginx >=1.7.5. RHEL has in older version in the package repositories, so you will need to add the official Nginx repository: # Add key and rest for the latest stable nginx sudo rpm --import sudo sh -c cat <EOT>/etc/yum.repos.d/nginx.rest [nginx] name=nginx repo baseurl= nginxs/rhel/\$releasever/x86_64/gpgcheck=1 enabled=1 EOT#Ensure that EPEL rest is not used for nginx sudo sed -i 's/^\(enabled=1\)$/exclude=nginx\1/g'/etc/yum.repos.d/epel.rest# Install sudo sudo yum install -y nginx # Install st2web sudo yum install -y st2web # Generate the self-signed certificate or your place existing certificate under /etc/ssl/st2 sudo mkdir -p /etc/ssl/st2 sudo openssl req -x509 -newkey rsa:2048-keyout /etc/ssl/st2/st2.key -out /etc/ssl/st2/st2.crt\ -days 365 -nodes -subj /C=US/ST=California/L=Palo Alto/O=StackStorm/OU=Information\Technology/CN=$(hostname) # and Copy enable the supplied nginx config file sudo cp /usr/share/doc/st2/conf/nginx/st2.conf/ets/nginx/conf.d/ # Disable default_server setup of existing / etc / nginx / nginx.conf sudo s s/s/default_server/g'/etc/nginx/conf.d/default.conf nginx service restart nginx sudo chkconfig nginx on if you modified port, or url path in the nginx configuration, make the corresponding change in the st2web configuration of /opt/stackstorm/static/webui/config.js. Use your browser to connect to https://${ST2_HOSTNAME} and connect to the WebUI. If you are trying to access the API from the box and you have configured nginx according to the following instructions, use https://${EXTERNAL_IP}/api/v1/${REST_ENDPOINT}. For example: curl -X GET-H 'Connection: keep-alive' -H 'User-Agent: manual/curl' -H 'Accept-encoding: gzip, deflate' -H */* - H 'X-Auth-Token: <YOUR_TOKEN>' amp;lt;/YOUR_TOKEN> </EOT> </EOT> you can connect to REST break points with https://${EXTERNAL_IP}/auth/v1/${AUTH_ENDPOINT}. You can view the real REST point for a resource by adding an option --debug to provide the CLI command for the appropriate resource. For example, to see the End plugin for Get action, Invoke: If you already run a Hubot instance, you can install the hubot-stackstorm plugin and configure stackStorm environment variables, as described below. Otherwise, the easiest way to enable StackStorm ChatOps is to use the est2chatops package. Validate that the mansion package is installed, and a notification rule is enabled: #Ensure mansion pack is in place ls/opt/stackstorm/pack/castle# Create notification rule if not yet allow st2 rule to get chaptos.notify || rule st2 create / opt / stack / pack / chatops / regulations / notify_hubot.yaml Add NodeJS v10 reputable: curl -sL | sudo-E bash – Install the st2chatops packages: sudo yum install -y st2chatops review with the editor /opt/stackstorm/castle/st2chatops.env configuration file point it to your StackStor installation and the chat service you are using. At a minimum, you should generate an API key and set ST2_API_KEY the variable. By default st2api and st2auth are expected to be on the same host. If that's not the case, please update ST2_API variables ST2_AUTH_URL or just point to the correct host and ST2_HOSTNAME. The instance configuration uses Slack. To set this up, go to the cornea of Slack web admin, create a bot, and copy the authentication token in HUBOT_SLACK_TOKEN. If you are using a different chat service, set the corresponding environment variable under the Chat Service Environment Adapter section at st2chatops.env: Slack, HipChat, Flowdock, IRC, Mattermost, RocketChat, XMPP. Starting the service: st2chatops sudo service start # Ensure it will start on the boot sudo chkconfig st2chatops on Reload st2 package to ensure that the chatops.notify rule is recorded: sudo stct2l reload-register -All this! Go to your chat room and start ChatOps-ing. Read more in the ChatOps section. By default, when MongoDB, RabbitMQ and PostgreSQL are installed, they have authentication disabled or used a default static password. As such, after you have installed the services you should configure them and enable authentication and simulated password product randomly. NB: If you use the StackStorm installation script, this is done automatically for you. Configuring authorization and passwords for these services is from topics that the application has for this document. For more information refer to the links below: After you enable authentication for these components, you'll also need to update StackStorm services to use the new settings. This means editing the following configuration options: StackStorm - / etc / st2 / st2.conf database.username – MongoDB database user name. database.password – Password database MongoDB. messaging.url - RabbitMQ transport url(amqp://<username>: @:@:<password><hostname>5672) Mistral -</hostname></password></username>database.connection - PostgreSQL string database (postgresql + psycopg2://<username><password>@<hostname>mistral) transport_url - RabbitMQ transport url (rabbit://<username>:@:@<password><hostname>5672) Besides, you are strongly encouraged to follow these best practices to run network services: Ensure communication between the encrypted services. Enable SSL/TLS for Mongodb, RabitMQ, and PostgresQL. Configure services to only listen on localhost, and where necessary, their internal IP addresses. There is usually no need for most services used by StackStorm (MongoDB, RabbitMQ, PostgresQL) to be available on a public IP address. Configure a firewall and set up a whitelist. The firewall should only be allowed access by these users and systems that need access to these services. API and Author Services usually need to be accessible to your users, but other dependent services such as MongoDB, RabbitMQ and PostgreSQL do not do so. These should not be directly accessible by users, and only StackStorm components should be allowed to speak to them. Where possible, you should also use other network-based isolation and security features such as DMZs. The steps mentioned above are especially important for distributing production deployment where StackStorm components are running on multiple servers. Extreme Workflow Composite adds 24/7 priority support, Workflow Designer (a graphical tool for workflow creation/editing), RBAC and LDAP StackStorm. It is deployed as an additional package set on top of StackStorm. You'll need an Extreme Workflow subscription to compose with a license key to access the Extreme Repositories Workflow. To learn more about Extreme Workflow Composite Check out Product Pages. To request a quote, or to obtain an evaluation license, Sales contacts don't complete the form . To install Extreme Composer Workflow, replace ${EWC_LICENSE_KEY} in the below order with the key you received when registering or purchasing, and running the following commands: # Set up the Extreme Access Workflow composer, install Enterprise Package and configure RBAC curl -SSL -O amp;amp;gt; chmod+x install.sh ./install.sh --username=st2admin --password='' --license=${EWC_LICENSE_KEY} What's Next?