Seqrite

Endpoint Protection

Disaster Recovery for EPP Server 8.4

www.seqrite.com

Copyright Information

Copyright © 2008–2024 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Protection is subject to the user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Disaster Recovery for EPP Server 8.4 ..... ***2***
Objective 2
Backup and Restore on Standalone IP to IP 2
Prerequisites 2
Backup Procedure 2
Installation of New Server 4
Restore Procedure 4
Migration from Distributed IP to IP/Hostname Installation 7
Install the 8.4 Server and Backup Data 7
Prepare for New Installation 7
Configure Nginx (if applicable) 8
Restore Data 8
Backup and Restore Folder Structure for 8.4 9
Restoration of SSR and Control Center 10
Restoration of SSR (Same Machine) 10
Restoration of SSR (Different Machine with Same IP/Hostname) 10
Restoration of Control Center (Same Machine or Different Machine) 11

Copyright © 2008–2024 Quick Heal Technologies Ltd.

Disaster Recovery for EPP Server 8.4

Objective

This guide provides step-by-step instructions for disaster recovery of SSR and Control Center through the backup and restore of EPSNG Server 8.4. It ensures that you can maintain your previous setup without data loss. It is recommended to perform backup and restore activities every 15 to 30 days.

Backup and Restore on Standalone IP to IP

Follow these steps if you have an 8.4 server installed on an Ubuntu machine and wish to back up and restore data on an EPSNG Server 8.4:
The backup and restore process covers server data such as:

- Policies and configurations
- Custom packages and admin settings
- Reports for all features
- Registered endpoints and patch management
- Roaming, DLP policies, UA, AD
- Client actions, groups, users, file sandbox
- 7.6 migrated clients, monthly and weekly reports, and FAM

Need to add the CRON on server machine as per requirement

```
0 0 15 * *
sh/opt/Seqrite_EndPoint_Security/ab.sh>>/opt/Seqrite_EndPoint_Security/backup_schedule.log
```

Execute the following command only once to run backup every 15 days or 30 days.

Command : `bash backup.sh`

Prerequisites

- Ensure that you have at least 1 GB of free disk space before starting the backup.
- Verify that all 8.4 prerequisites are met before installing the server.

Backup Procedure

1. **Prepare Backup Files**
    - Download the backup files from the following location: 8.4 Backup and Restore Files.

- Extract the ZIP file to access `run_backup.sh` and `backup_standalone.sh`.

2. **Copy Files to Server**
   - Place the extracted `run_backup.sh` and `backup_standalone.sh` files in the `/opt/Seqrite_EndPoint_Security/Backup` directory on your server.

3. **Set File Permissions**
   - Open a terminal and execute the following command to set the appropriate permissions for the backup files:

```
chmod 755 run_backup.sh backup_standalone.sh
```

4. **Perform the Backup**
   - Execute the backup script by running:

```
bash run_backup.sh 19
```

   - After completion, you will see a success message: Backup is completed.
   - The backup will generate `exportDump<Date_time>` and `MongoDump<Date_time>` directories in the `/opt/Seqrite_EndPoint_Security/Backup/` location.
5. **Copy Backup Data**
   - Transfer the `exportDump<Date_time>` and `MongoDump<Date_time>` directories to a safe location, such as another machine, NFS, shared drive, or removable disk, to protect against data loss.

Installation of New Server

Install EPSNG Server 8.4

- Install EPSNG Server 8.4 on the existing machine with the "Activate Later" option and perform basic configurations.
- Ensure all 8.4 installation prerequisites are met before proceeding.

Restore Procedure

1. **Prepare for Restore**
   - Obtain the backup folder from the removable drive, shared drive, or NFS and place it on the server machine.
2. **Transfer Backup Files**
   - Use Mobaxterm or another terminal application to connect to the server.
   - Navigate to the

```
/opt
```

   - directory and copy the backup files:

```
cd /opt
```

- Copy `exportDump<Date_time>` and `MongoDump<Date_time>`, along with `outputFilePath.txt` from the backup location to the `/opt` directory.

3. **Rename Backup Directories**
   - Rename

     ```
     exportDump<Date_time>
     ```

     to

     ```
     exportDump
     ```

     and

     ```
     MongoDump<Date_time>
     ```

     to

     ```
     MongoDump
     ```

     ```
     mv exportDump<Date_time> exportDump
     mv MongoDump<Date_time> MongoDump
     ```

4. **Prepare Restore Files**
   - Place `run_restore.sh`, `restore_standalone.sh`, and `backward_compatibility_8.4.js` in the `/opt` directory.
   - Set the appropriate permissions for these files:

     ```
     chmod 755 run_restore.sh restore_standalone.sh
     backward_compatibility_8.4.js
     ```

5. **Perform the Restore**
   - Execute the restore script by running:

     ```
     bash run_restore.sh 19
     ```

   - Wait for the completion message: `Restoration is Completed`.
6. **Activate Server**
   - Activate the server with the same key used for the previous 8.4 server installation.

7. **Verify Data**
    - Confirm that all previous data has been restored and is correctly loaded.
8. **Patch Management**

    If customer has the Patch management configured then
    - For same machine restoration, the patch management server will work as is.
    - For different machine restoration, we need to run the script: Post-upgrade, execute a script on the client.

        a. **Setup**:
            - Extract and place both files in the same location.

        b. **Execute Patch Management Script**:
            - Run the batch file with the parameter `{PM Server Path}` in admin mode using: `set_eps_guid.bat C:\Program Files\Seqrite\Seqrite Patch Management\Patch` `Server UUID`

              Note: Obtain the UUID with the command: `sudo dmidecode -q | grep -w UUID.` `Example UUID: 423a6fb9-faf2-2ef1-f164-cba48f87ed1c`

Copyright © 2008–2024 Quick Heal Technologies Ltd.

Migration from Distributed IP to IP/Hostname Installation

Install the 8.4 Server and Backup Data

1. **Install Server**:
   - Deploy the 8.4 server using the distributed method on CentOS.
2. **Generate Data for Backup**:
   - Ensure that all policies, configurations, custom packages, admin settings, and features such as registered endpoints, Patch Management, Roaming, DLP policy, UA, AD, Client actions, Groups, Users, File sandbox, 7.6 migrated client, monthly and weekly reports, and FAM are functioning correctly.
3. **Perform Data Mapping**:
   - Validate data through data mapping after restoration.
4. **Backup Data**:
   a. **Prepare Backup Scripts**:
      - Place `run_backup.sh` and `backup_standalone.sh` in the `/opt/Seqrite_EndPoint_Security/` directory.
      - Assign 755 permissions to both files.
   b. **Execute Backup**:
      - Run the command: `bash run_backup.sh 19`
   c. **Verify Backup**:
      - After completion, verify that `exportDump<Date_time>` and `MongoDump<Date_time>` folders are created in `/opt/Seqrite_EndPoint_Security/Backup/`.
   d. **Transfer Backup**:
      - Download the backup folder to another machine to ensure data safety in case of a machine crash.
5. **Shutdown**:
   - Shut down both the 8.4 server machine and the DB machine.

Prepare for New Installation

1. **Setup New Machines**:
   - Use two Ubuntu machines and assign the IP addresses of the previous 8.4 server and DB machine to the new machines for 8.4 installation.

Copyright © 2008–2024 Quick Heal Technologies Ltd.

2. **Install 8.4**:
    - Install 8.4 with the Active Later option and perform basic configurations.
    - **For IP-based Installation**: Proceed with the next steps.
    - **For Hostname-based Installation**: Ensure that the server machine hostname is configured with an FQDN. If not, follow the additional steps below:

Configure Nginx (if applicable)

Run Nginx Configuration Clean up Script:

a. **Prerequisites**:
- Ensure Nginx is installed (it will be installed with the EPSNG setup).

b. **Installation**:
- Download `modify_nginx.sh` and make it executable with `chmod +x modify_nginx.sh.`

c. **Usage**:
- Execute the script with `bash modify_nginx.sh.`

Restore Data

1. **Restore Data**:

a. **Prepare Restoration**:
- Copy `exportDump<Date_time>` and `MongoDump<Date_time>,` along with `outputFilePath.txt` from the backup folder to `/opt.`
- Rename `exportDump<Date_time>` and `MongoDump<Date_time>` to `exportDump` and `MongoDump`, respectively.

b. **Prepare Restoration Scripts**:
- Place `run_restore.sh`, `restore_standalone.sh,` and `backward_compatibility_8.2.js` in the `/opt` directory.
- Assign 755 permissions to all these files.
- Note: Although the script is named backward compatibility, `backward_compatibility_8.2.js` is actually a forward compatibility script.

c. **Execute Restoration**:
- Run `bash run_restore.sh 19.`

2. **Activate Server**:
    - Activate the server using the same key used for the previous 8.4 server.
    - **Troubleshooting**: If activation fails, reset the AFG flag in the activation DB.

3. **Validate Restoration**:
    - Perform data mapping and verify that the data from the previous 8.4 server has been restored without loss.
4. **Patch Management**:
   Post-upgrade, execute a script on the client. The 8.1 patch server will function the same as the 8.4 server.
   a. **Setup**:
      - Extract and place both files in the same location.

   b. **Execute Patch Management Script**:
      - Run the batch file with the parameter `{PM Server Path}` in admin mode using: `set_eps_guid.bat C:\Program Files\Seqrite\Seqrite Patch Management\Patch` `Server UUID`
      - **Note**: Obtain the UUID with the command: `sudo dmidecode -q | grep -w UUID.` `Example UUID: 423a6fb9-faf2-2ef1-f164-cba48f87ed1c`

Backup and Restore Folder Structure for 8.4

8.4_to_8.4_backup_restore:

- **Standalone**:
    - backup_standalone.sh
    - backup_standalone_instruction.txt
    - backward_compatibility_8.4.js
    - restore_standalone.sh
    - run_backup.sh
    - run_restore.sh

Restoration of SSR and Control Center

Restoration of SSR (Same Machine)

1. Ensure backup data is available.
2. Install the SSR restoration software.
3. Run the restoration script.
4. In the activation database, modify the existing SSR ID for the SSR being restored in the `Slave_tns` file. Append a string to the ID to facilitate activation, as activation will not proceed with the same SSR ID without modification.
5. Activate the SSR using the same key.
6. The SSR should be restored successfully.

Restoration of SSR (Different Machine with Same IP/Hostname)

1. Update the new machine's IP address or hostname to reflect the previous SSR machine's configuration.
2. Install the SSR restoration software on the new machine with the same IP address or hostname.
3. Run the restoration script.
4. In the activation database, modify the existing SSR ID for the SSR being restored in the `Slave_tns` file. Append a string to the ID to facilitate activation.
5. Obtain the installation number of the new machine using the command: `sudo dmidecode -q | grep -w UUID`
6. Retrieve the MAC address of the new machine.
7. Update the `Slave_tns` file with the new installation number and MAC address for the SSR being restored.
8. In the Control Center database, update the `SiteOnboardingCollectionInfo` table with the new installation number for the existing SSR entry.
9. Activate the SSR using the same key.
10. The SSR should be restored successfully.

Copyright © 2008–2024 Quick Heal Technologies Ltd.

Restoration of Control Center (Same Machine or Different Machine)

1. For backup and restore of Control Center the procedure will be same as Backup and Restore on Standalone IP to IP.
2. Install the Control Center restoration software.
3. Run the restoration script.
4. Activate the Control Center using the same key.
5. The Control Center should be restored and ready for use.