

Backup der Konfigurationen von Netzwerkkomponenten

Inhalt

| | |
|--|----|
| Backup der Konfigurationen von Netzwerkkomponenten | 1 |
| 1. Einführung | 1 |
| 2. TFTP/FTP Server..... | 1 |
| 3. Cisco ASA Backup..... | 5 |
| 4. Backup des Juniper VPN-Konzentrators | 8 |
| 5. Backup eines Pulse Secure Servers | 9 |
| 6. Backup der F5 BIG-IP | 10 |

1. Einführung

Konfigurationen der Netzwerkkomponenten sollten nach jeder Änderung gesichert werden. Selbst bei Geräten, welche in einem Cluster oder redundant laufen, ist das Backup erforderlich, da Konfigurationsfehler auf das Standby-Gerät übertragen werden können.

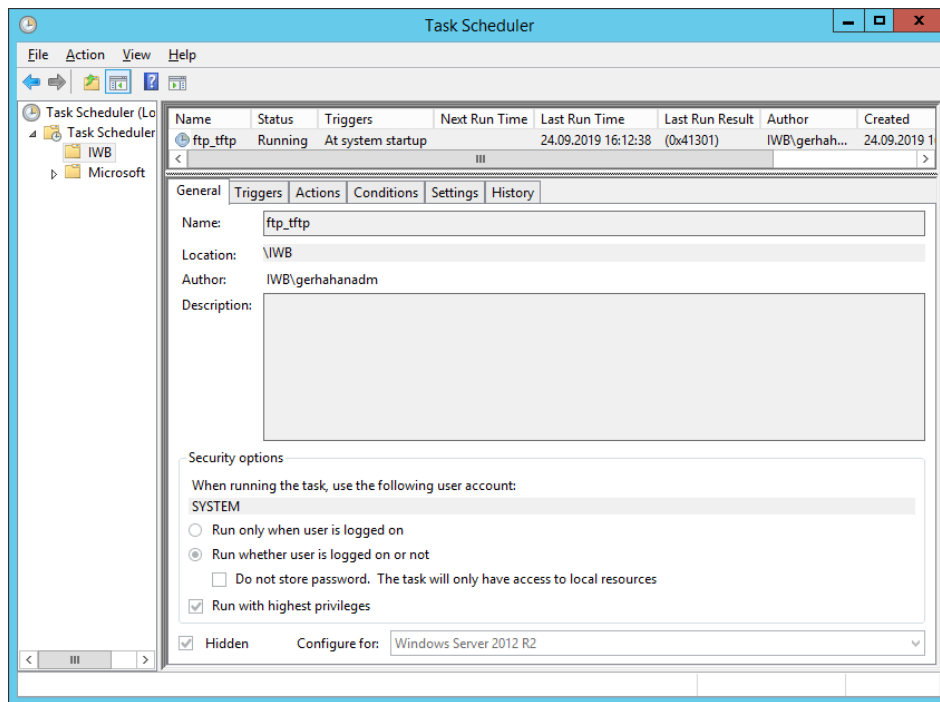
Alternativ zur Sicherung der Konfiguration nach einer Änderung kann die Sicherung ein Mal am Tag erfolgen.

Für das Backup der Konfigurationen sollten in erster Linie die Möglichkeiten der Geräte selbst genutzt werden, um so wenig wie möglich zusätzlichen Aufwand zu betreiben.

2. TFTP/FTP Server

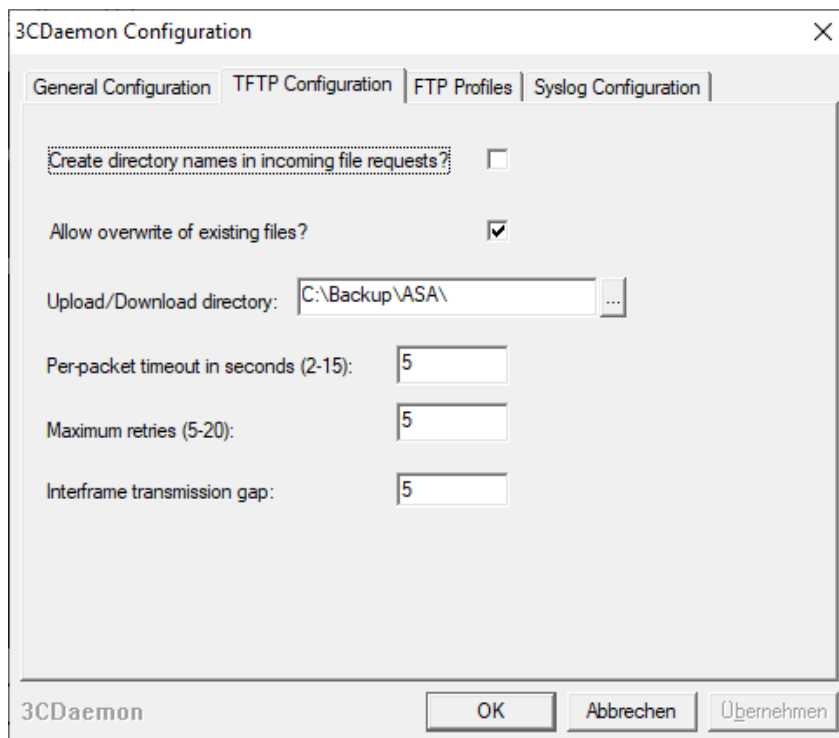
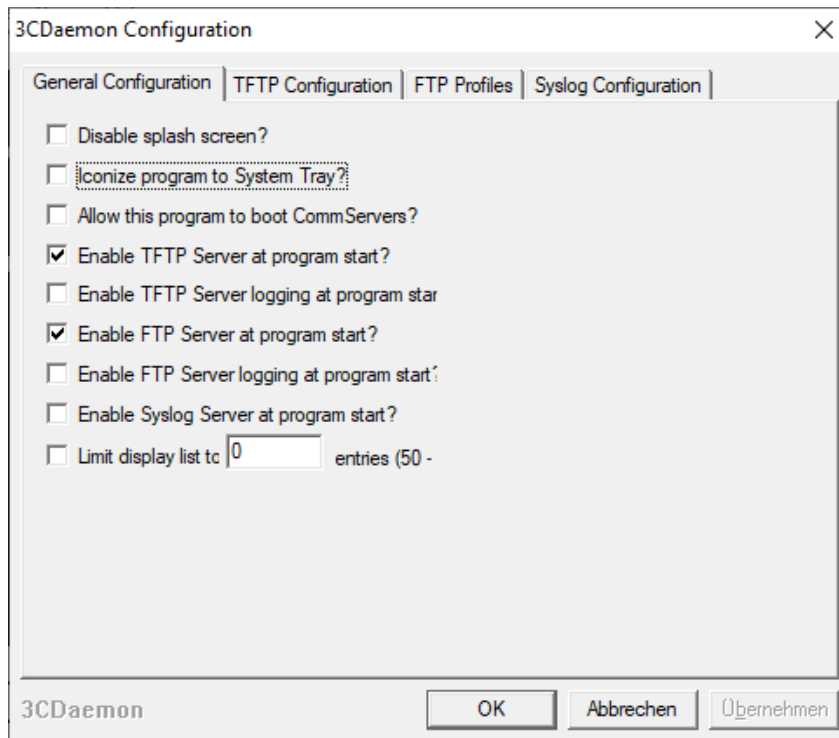
Zur Übertragung der Daten sind ein TFTP- und ein FTP-Server erforderlich. In diesem Fall wird das Programm 3C Daemon verwendet. Der von Microsoft mitgelieferte tftp-Service lässt nur Lesen von Daten zu, und ist deshalb nicht geeignet.

Das Programm kann über den Task Scheduler bei jedem Start auf einem Microsoft-Server gestartet werden. Der Microsoft eigene FTP-Service muss gestoppt sein.



Die Funktion des FTP-Servers kann mit einer Monitoring Software, zum Beispiel Check_MK überwacht werden.

Konfiguration des 3C Daemon Programms



Der TFTP-Server wird nur für die Cisco Firewalls verwendet.

Einrichtung des FTP-Servers.

3CDaemon Configuration

General Configuration | TFTP Configuration | FTP Profiles | Syslog Configuration

anonymous
F5 BigIP_BU
Juniper_BU
Pulse_BU

User Info
Profile Name: F5 BigIP_BU
Set/Change user's password

User Directory: C:\Backup\F5 BigIP\ ...

This user can:
 Login
 Download
 Upload
 Delete Files
 Overwrite files
 Rename files
 Make Directories

Save Profile
Delete Highlighted Profile

To add a profile: Enter the new information into the form then press "Save Profile"
To edit a profile: Highlight the profile, make your changes, then press "Save Profile"
To delete a profile: Highlight the profile to delete, then press "Delete Profile"

3CDaemon OK Abbrechen Übernehmen

3CDaemon Configuration

General Configuration | TFTP Configuration | FTP Profiles | Syslog Configuration

anonymous
F5 BigIP_BU
Juniper_BU
Pulse_BU

User Info
Profile Name: Juniper_BU
Set/Change user's password

User Directory: C:\Backup\Juniper\ ...

This user can:
 Login
 Download
 Upload
 Delete Files
 Overwrite files
 Rename files
 Make Directories

Save Profile
Delete Highlighted Profile

To add a profile: Enter the new information into the form then press "Save Profile"
To edit a profile: Highlight the profile, make your changes, then press "Save Profile"
To delete a profile: Highlight the profile to delete, then press "Delete Profile"

3CDaemon OK Abbrechen Übernehmen

3CDaemon Configuration

General Configuration | TFTP Configuration | FTP Profiles | Syslog Configuration

anonymous
F5 BigIP_BU
Juniper_BU
Pulse_BU

User Info
Profile Name: Pulse_BU
Set/Change user's password

User Directory: C:\Backup\Pulse\ ...

This user can:
 Login
 Download
 Upload
 Delete Files
 Overwrite files
 Rename files
 Make Directories

Save Profile
Delete Highlighted Profile

To add a profile: Enter the new information into the form then press "Save Profile"
To edit a profile: Highlight the profile, make your changes, then press "Save Profile"
To delete a profile: Highlight the profile to delete, then press "Delete Profile"

3CDaemon OK Abbrechen Übernehmen

3. Cisco ASA Backup

Wenn die Konfigurationen der Cisco-ASA-Firewalls über das Tool Cisco Prime Infrastruktur gesichert werden, wird nur die System-Konfiguration automatisch gesichert. Verfügen die Firewalls über mehrere Context-Konfigurationen, sind für deren Sicherung extra Massnahmen zu ergreifen.

Eine Möglichkeit bestünde darin, weitere Firewalls pro Context in dem Tool Cisco Prime zu kreieren. Hier wird ein anderer Weg vorgeschlagen.

Mit einem CLI-Script werden auf den ASA-Firewalls die Context-Konfigurationen abgefragt und auf den TFTP-Server kopiert.

Das Script wird mit Hilfe des Terminal-Programms «teraterm» ausgeführt.

```
; sample macro of Tera Term
; Backup Konfigurationsdateien ASA
; Erstellen eines Containers mit allen Firewalls
strdim cfg 20 ;maximale Anzahl der Konfigurationen auf einer Firewall
strdim asa 15 ;maximale Anzahl Firewalls
asa[0]='alle'
asa[1]='ASA001'
asa[2]='ASA002'
asa[3]='192.168.100.100'
    erste=1 ;erstes Backup
    letzte=3 ;letztes Backup

for i erste letzte

;erstellen des Namens der Backup-Datei
    xasa=asa[i]
    getdate xdatum
    gettime xtime
    strconcat xasa '_'
    strconcat xasa xdatum
    ;strconcat xasa xtime
;mit Gerät verbinden
    msg = asa[i]
    strconcat msg ' /ssh /2 /auth=password /user=xxxxxxx /passwd=yyyyyyyyy'
    pause 1
    connect msg
    testlink ;testen der Verbindung
    if result=0 goto ende2
    wait '>'
    sendln 'ena'
    wait 'Password:'
    sendln 'zzzzzzzzzz'
    wait '#'
    sendln 'changeto system'
    wait '#'
```

```
;Konfigurationen feststellen und im Container cfg speichern
```

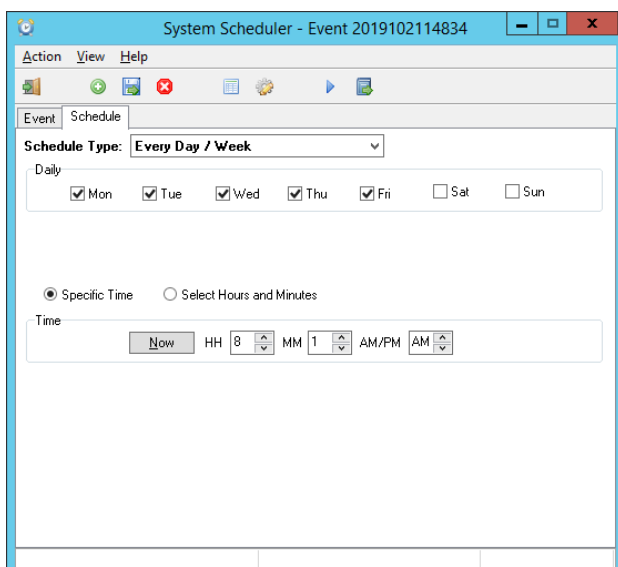
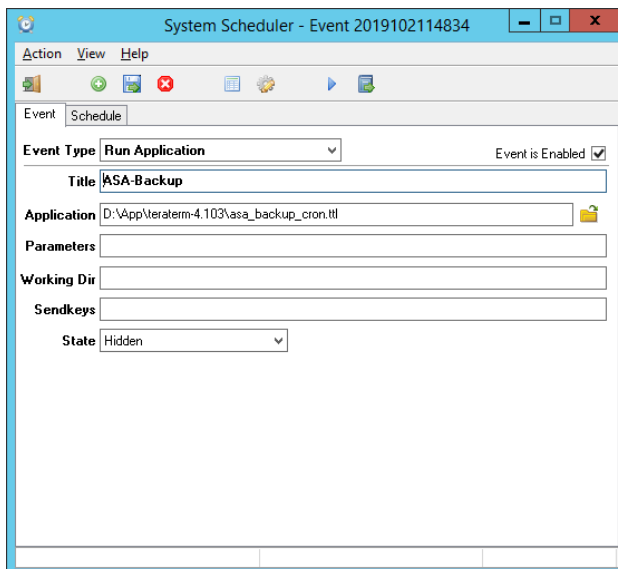
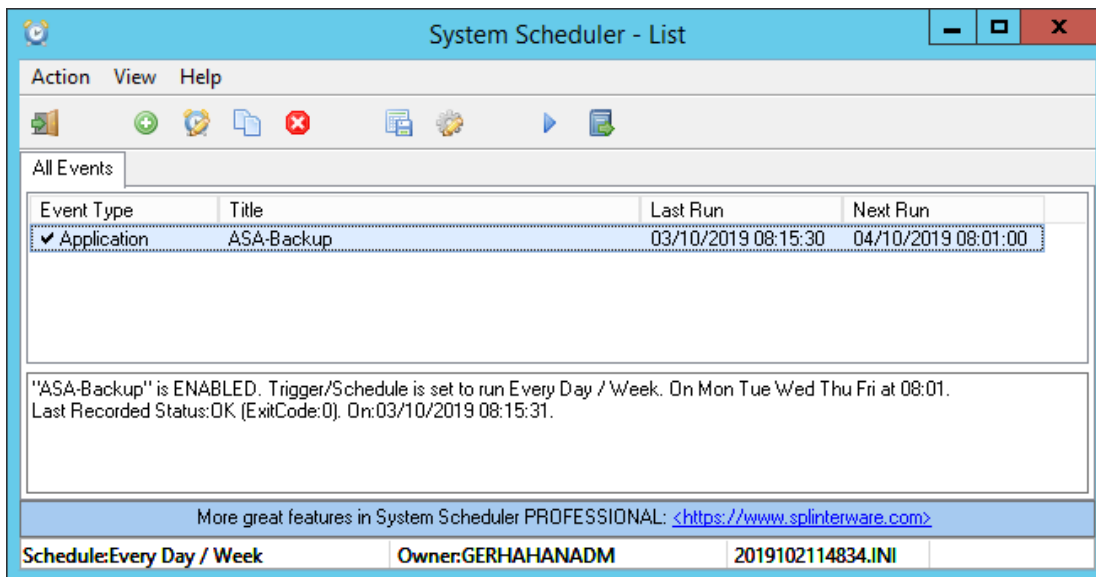
```
    sendln 'dir *.cfg'  
    j=0  
    :loop1  
        recvln  
        strlen inputstr  
        if result>47 then  
            strremove inputstr 1 48  
            cfg[j]=inputstr  
            if j<20 then  
                j=j+1  
            endif  
        endif  
    strscan inputstr 'total'  
    if result=0 goto loop1
```

```
;Konfigurationen auf den tftp-Server sichern
```

```
    :loop2  
        j=j-1  
        if j=-1 goto ende1  
        msg = 'copy '  
        strconcat msg cfg[j]  
        strconcat msg ' tftp://192.168.200.001/'  
        strconcat msg xasa  
        strconcat msg '_'  
        strconcat msg cfg[j]  
        sendln msg  
        sendln  
        ;stop  
    goto loop2  
    :ende1  
    sendln 'ex'  
:ende2  
next  
:ende
```

Zu beachten ist, dass beim Einloggen auf den ASAs ein Schlüssel benötigt wird. Dieser wird einmal vom Programm teraterm erstellt, muss bestätigt werden und ist dann automatisch gültig. Sollte ein neuer Schlüssel erforderlich sein, ist das Login manuell zu starten und die Erzeugung des Schlüssels wieder zu bestätigen.

Da das Programm teraterm nicht vom Windows Task Scheduler gestartet werden kann, wird das Programm System Scheduler verwendet.



4. Backup des Juniper VPN-Konzentrators

Um den VPN Konzentrador SRX345 so zu konfigurieren, dass er seine derzeit aktive Konfiguration auf einen Archivierungsserver überträgt, werden folgende Anweisungen auf der Hierarchieebene [Systemarchivierungskonfiguration bearbeiten] ausgeführt:

```
[edit system archival configuration]
archive-sites {
ftp://username<:password>@host-address<:port>/url-path;
}
transfer-interval interval;
```

Um das Gerät so zu konfigurieren, dass die aktuell aktive Konfiguration regelmäßig an einen Archivstandort übertragen wird, ist die Anweisung für das Übertragungsintervall auf der Hierarchieebene [Systemarchivierungskonfiguration bearbeiten] hinzuzufügen:

```
[edit system archival configuration]
transfer-interval interval;
```

Das Intervall wird in Minuten angegeben. Die Befehle lauten:

```
set system archival configuration transfer-interval 1440
set system archival configuration archive-sites ftp://Juniper_BU:xxxxxx@192.168.200.001/
```

(wobei xxxxxx das Passwort für den ftp-Account „Juniper_BU“ ist.)

5. Backup eines Pulse Secure Servers

The screenshot shows the Pulse Connect Secure web interface. The top navigation bar includes 'Pulse Connect Secure', 'Help | Guidance | Switch to New UI | Sign Out'. A left sidebar contains a menu with categories: System, Authentication, Administrators, Users, and Maintenance. The main content area is titled 'Archiving > Archiving Servers' and has three tabs: 'Archiving Servers', 'Local Backups', and 'Pulse Collaboration'. Below the tabs is an introductory text: 'You can schedule automatic archiving of log data, system configuration, and user accounts. To do so, specify an FTP accessible location for the data, an FTP account to use, and the specific schedule for each type of archived data.' Below this is the 'Archive Settings' section with the following fields: 'Archive Server' (192.168.200.001), 'Destination Directory' (/), 'Username' (Pulse_BU), 'Password' (masked with dots), and 'Method' (radio buttons for SCP and FTP, with FTP selected). A note next to the Archive Server field states: 'Name or IP address. Please make sure that the server is reachable via management port.'

Das Backup des Pulse Secure Servers wird auf der GUI eingestellt.

This screenshot shows the 'Archive Settings' configuration page. It features several sections with checkboxes and scheduling options: 'Archive client-side log uploads' (unchecked), 'Archive system configuration' (checked), 'Archive user accounts' (unchecked), 'Archive XML configuration' (checked), 'Archive Debug Log' (unchecked), and 'Archive Periodic SnapShots' (unchecked). The 'Archive system configuration' and 'Archive XML configuration' sections include a weekly schedule (Sun-Sat) and two scheduling options: 'Every hour (00:00am till 11:00pm)' and 'Specified Time: 10:00 PM'. A text box for 'Password for configuration file:' is present below the system configuration section. At the bottom, there is a 'Save Changes' button.

6. Backup der F5 BIG-IP

Auf der BIG-IP müssen die Backup-Dateien der Konfiguration erst mit dem Befehl «save» erstellt werden.

```
save /sys ucs <path to save ucs file>
```

Die erstellten Dateien werden auf den FTP-Server übertragen und anschliessend auf dem Gerät gelöscht. Zu diesem Zweck wurde das folgende Script ftpg.sh im Verzeichnis «config» erstellt.

```
#!/bin/bash
#Zeitstempel
DATETIME=$( date '+%Y-%m-%d_%H-%M' )
#Dateibezeichnung
HOSTNAME=$(uname -n | cut -f 1 -d ".")
UCS_FILENAME="${DATETIME}_${HOSTNAME}"
SCF_FILENAME="${DATETIME}_${HOSTNAME}"
#erzeugen der Backup-Dateien
cd /config
tmsh save /sys config
tmsh save /sys ucs /var/tmp/${UCS_FILENAME}.ucs
tmsh save sys config file /var/tmp/${SCF_FILENAME}.scf
#FTP-Script
echo user F5_BigIP_BU xxxxxxxx> ftps.txt          #xxxxxx ist das Passwort auf dem FTP Server
echo bin >> ftps.txt
echo put /var/tmp/${SCF_FILENAME}.scf.tar ${SCF_FILENAME}.scf.tar >> ftps.txt
echo put /var/tmp/${SCF_FILENAME}.scf ${SCF_FILENAME}.scf >> ftps.txt
echo put /var/tmp/${UCS_FILENAME}.ucs ${UCS_FILENAME}.ucs >> ftps.txt
echo quit >> ftps.txt

#FTP Backup
ftp -inv 192.168.200.001 < ftps.txt

#Delete files that are older than 1 days
find /var/tmp/*.tar -mtime +1 -type f -delete
find /var/tmp/*.scf -mtime +1 -type f -delete
find /var/tmp/*.ucs -mtime +1 -type f -delete
```

(Nicht vergessen das Skript ausführbar zu machen: `chmod u+x`)

Das Script ftpg.sh automatisch ausführen: `crontab -e`
und folgende Zeile mit «a» einfügen und mit «:wq» speichern
(min h d m w script)

```
30 1 * * * /config/ftphg.sh
```