# Allgemeines

|  |  |  |
| --- | --- | --- |
| Git-Projekt / Git clone | git@git.services.emea.dir:log/elastic.git |  |
|  |  |  |
|  |  |  |

# Vorbereitung

Zunächst sind einige Vorbereitungen auf der Umgebung zu treffen, um die Installation durchführen zu können:

1. Zunächst müssen die persönlichen SSH Keys auf die Zielmaschine kopiert werden nach /home/<username>/.ssh/<username>
2. Wechsel auf den Root User (sudo su)
3. Ausführen des Proxy Scripts (proxy\_on 🡪 Windows Credentials eingeben)
4. SSH-Setup für Git ausführen (eval $(ssh-agent -s);ssh-agent -s;ssh-add /home/<username>/.ssh/<username>, und mit dem Passwort des Private Keys bestätigen.
5. Installations-Script aus dem Git-Projekt auf die Maschine kopieren (liegt im Git-Projekt unter /logstash/install-logstash-forwarder.sh)

# Durchführen der Installation

Sind die Vorbereitungen abgeschlossen, kann mit der Installation begonnen werden:

1. Installations-Script ausführen (./install-logstash-forwarder.sh)
2. Die Installation erfolgt automatisch, es muss jedoch einmalig eine Bestätigung eingegeben werden („yes“). Es wird das Git-Projekt unter /tmp geklont, von hier aus wird die Installation ausgeführt.

Bricht die Installation mit der Meldung  
„Error: Execution of '/usr/bin/yum -d 0 -e 0 -y list logstash-forwarder' returned 1: Error: Cannot retrieve repository metadata (repomd.xml) for repository: logstashforwarder. Please verify its path and try again“   
ab, so muss sie nur erneut ausgeführt werden.

Bricht die Installation mit der Meldung  
Error: Could not run: Could not find file /tmp/elastic/logstash/puppet/manifests/install-logstash-forwarder.pp  
ab 🡪 siehe Troubleshooting (Git SSH Probleme)

# Nachträgliche Anpassung der Installation

Nach der Installation muss auf dem Host die Liste der Files, die vom logstash-forwarder überwacht werden, angepasst werden. Hierzu wie folgt vorgehen:

1. Den Service mit service logstash-forwarder stop anhalten
2. Die Date /etc/logstash-forwarder.conf mit einem Texteditor öffnen
3. In der Datei alle Blöcke unter „files“ löschen, die auf dem Server nicht überwacht werden sollen (z.B. den Block mit den „icinga“ logs)
4. Service mit service logstash-forwarder start starten und Logs unter /var/log/logstash-fowarder/logstash-forwarder.err prüfen

Nun ist zu prüfen, ob die Installation erfolgreich war:

1. Prüfen ob der Service läuft service logstash-forwarder status
2. Checken der Logs unter /var/log/logstash-fowarder/logstash-forwarder.err

# Troubleshooting

## HTTP Timeout

Tritt bei der Installation ein Timeout – insbesondere bei HTTP(s) Anfragen auf, so ist evtl. der HTTP Proxy nicht korrekt gesetzt.

1. Prüfen ob der Proxy gesetzt ist: via echo $http\_proxy
2. Ist diese Variable leer, so muss das Script proxy\_on ausgeführt werden. Es müssen die Windows-Credentials verwendet werden.
3. Achtung: Das Script muss nach sudo su erneut ausgeführt werden!

## Git SSH Probleme

Wird der SSH Agent nicht korrekt ausgeführt, so beendet sich die Installation mit der Meldung, dass Dateien nicht gefunden werden können, sowie der folgenden Git Meldung:

Permission denied (publickey).

In diesem Fall ist Schritt 4 der Vorbereitung (SSH-Setup) erneut auszuführen und die Installation erneut zu starten.