# 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/<user>/.ssh/<user>
2. Ausführen des Proxy Scripts (proxy\_on 🡪 Windows Credentials eingeben)
3. SSH-Setup für Git ausführen:  
   eval $(ssh-agent -s);ssh-agent -s;  
   ssh-add home/<user>/.ssh/<user>  
   und mit dem Passwort des Private Keys bestätigen.
4. In das Home-Verzeichnis wechseln und dort das Git-Projekt klonen:   
   git clone git@git.services.emea.dir:log/elastic.git
5. Ggf. In den Dateien

/home/<user>/elastic/logstash/install-logstash.sh  
/home/<user>/elastic/logstash/puppet/manifests/install-logstash.pp

die Pfade anpassen.

1. Nun sind alle benötigten Firewall-Freischaltungen einzutragen.

🡪 Siehe hierzu Dokument „elasticsearch - overview.docx“

1. Die SSL-Zertifikate müssen von Hand auf die Maschine kopiert werden. Hierzu folgende Dateien kopieren:

* logforwarder.key (Private Key) 🡪 /etc/ssl
* logforwarder.crt (Zertifikat inkl. Chain) 🡪 /etc/ssl/certs

# Durchführen der Installation

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

1. Wechsel in das Verzeichnis /home/<user>/elastic/logstash
2. Installations-Script ausführen:  
   ./install-logstash.sh
3. Die Installation erfolgt ab hier automatisch.

# Nachträgliche Anpassung der Installation

Zunächst ist zu prüfen, ob die Installation erfolgreich war.

1. Prüfen ob alle Services laufen

service logstash status

1. Checken der Logs unter /var/log/logstash/\*

# 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!