

F5 LTM TMSH Base Config

Config with LDAP Auth

```
## =====
## Insert in TMSH "load sys config merge from-terminal"
## Finish with CTRL-D
## =====

# - NTP settings
# -----
sys ntp {
    servers { 1.2.3.4 4.3.2.1 }
    timezone Europe/Zurich
}

# - SNMP settings
# -----
sys snmp {
    agent-addresses { tcp6:161 udp6:161 }
    allowed-addresses { 127.0.0.0/255.0.0.0 1.2.3.4/255.255.255.0 4.3.2.1/255.255.255.0
5.4.3.2/255.255.255.0 }
    communities {
        mycommunity1 {
            community-name public
            source default
        }
        mycommunity2 {
            community-name public2
        }
    }
    disk-monitors {
        root {
            minspace 2000
            path /
        }
    }
}
```

```

    var {
        minspace 10000
        path /var
    }
}
process-monitors {
    bigd {
        process bigd
    }
    chmand {
        process chmand
    }
    httpd {
        max-processes infinity
        process httpd
    }
    mcpd {
        process mcpd
    }
    sod {
        process sod
    }
    tmm {
        max-processes infinity
        process tmm
    }
}
sys-contact contact@email.com
sys-location "Location of F5"
}

# - DNS settings
# -----
sys dns {
    name-servers { 1.2.3.4 4.3.2.1 }
    search { localhost corp.domain.com mgmt.domain.com domain.com }
}

# - LDAP-Access settings for AD
# -----

```

```

auth ldap system-auth {
    bind-dn CN=LDAPProxyUser,OU=Accounts,OU=OrgUnit,DC=domain,DC=com
    bind-pw <pw>
    login-attribute userPrincipalName
    port ldaps
    search-base-dn DC=domain,DC=com
    servers { dc.domain.com }
    ssl enabled
}

auth password-policy { }

auth remote-role {
    role-info {
        LDAP-Administrator {
            attribute memberOF=CN=GRP_F5Admins,OU=Groups,DC=domain,DC=com
            console tmsh
            line-order 1
            role administrator
            user-partition All
        }
        LDAP-ReadOnly {
            attribute memberOF=CN=GRP_F5ReadOnly,OU=Groups,DC=domain,DC=com
            line-order 2
            role guest
            user-partition All
        }
        LDAP-ReadOnly-FW-Admins {
            attribute memberOF=CN=GRP_FWAdmins,OU=Groups,DC=domain,DC=com
            line-order 4
            role guest
            user-partition All
        }
        LDAP-ReadOnly-FW-R0 {
            attribute memberOF=CN=GRP_FWReadOnly,OU=Groups,DC=domain,DC=com
            line-order 5
            role guest
            user-partition All
        }
    }
}

auth remote-user {

```

```
    default-partition Common
}
auth source {
    type active-directory
}

# - Local-User Einstellung
# -----
auth user admin {
    description "Admin User"
    password <pw>
    partition Common
    partition-access {
        all-partitions {
            role admin
        }
    }
    shell bash
}
auth user scriptuser {
    description "Script-User"
    password <pw>
    partition Common
    partition-access {
        all-partitions {
            role admin
        }
    }
    shell bash
}

# - Syslog
# -----
sys syslog {
    remote-servers {
        /Common/remotesyslog1 {
            host 1.2.3.4
            remote-port 514
        }
    }
}
```

Debugging AD/LDAP

If you need to Debug AD/LDAP Auth see the following guide:

<https://my.f5.com/manage/s/article/K15811>

You should see logs in /var/log/secure

Enable debugging log with

```
tmssh modify /auth ldap all debug enabled
```

Disable with:

```
tmssh modify /auth ldap all debug disabled
```

Config with RADIUS Auth

```
## =====
## Insert in TMSH "load sys config merge from-terminal"
## Finish with CTRL-D
## =====

# - NTP settings
# -----
sys ntp {
    servers { 1.2.3.4 4.3.2.1 }
    timezone Europe/Zurich
}

# - SNMP settings
# -----
sys snmp {
    agent-addresses { tcp6:161 udp6:161 }
    allowed-addresses { 127.0.0.0/255.0.0.0 1.2.3.4/255.255.255.0 4.3.2.1/255.255.255.0
5.4.3.2/255.255.255.0 }
    communities {
        mycommunity1 {
            community-name public
            source default
        }
    }
}
```

```

    mycommunity2 {
        community-name public2
    }
}
disk-monitors {
    root {
        minspace 2000
        path /
    }
    var {
        minspace 10000
        path /var
    }
}
process-monitors {
    bigd {
        process bigd
    }
    chmand {
        process chmand
    }
    httpd {
        max-processes infinity
        process httpd
    }
    mcpd {
        process mcpd
    }
    sod {
        process sod
    }
    tmm {
        max-processes infinity
        process tmm
    }
}
sys-contact contact@email.com
sys-location "Location of F5"
}

```

- DNS settings

```
# -----  
sys dns {  
    name-servers { 1.2.3.4 4.3.2.1 }  
    search { localhost corp.domain.com mgmt.domain.com domain.com }  
}  
  
# - RADIUS-Access settings  
# -----  
auth radius /Common/system-auth {  
    servers {  
        /Common/system_auth_name1  
        /Common/system_auth_name2  
    }  
}  
  
auth radius-server /Common/system_auth_name1 {  
    secret <secret>  
    server 1.2.3.4  
}  
  
auth radius-server /Common/system_auth_name2 {  
    secret <secret>  
    server 4.3.2.1  
}  
  
auth remote-role {  
    role-info {  
        /Common/LDAP-Administrator {  
            attribute F5-LTM-User-Info-1=adm  
            console tmsh  
            line-order 1  
            role administrator  
            user-partition All  
        }  
        /Common/LDAP-Guest {  
            attribute F5-LTM-User-Info-1=guest  
            line-order 2  
            role guest  
            user-partition All  
        }  
        /Common/LDAP-application-security-editor {  
            attribute F5-LTM-User-Info-1=wase  
            console tmsh  
            line-order 3
```

```

        role webapplicationsecurityeditor
        user-partition All
    }
}
auth remote-user {
    default-partition Common
}
auth source {
    type radius
}

# - Local-User Einstellung
# -----
auth user admin {
    description "Admin User"
    password <pw>
    partition Common
    partition-access {
        all-partitions {
            role admin
        }
    }
    shell bash
}
auth user scriptuser {
    description "Script-User"
    password <pw>
    partition Common
    partition-access {
        all-partitions {
            role admin
        }
    }
    shell bash
}

# - Syslog
# -----
sys syslog {
    remote-servers {

```



```
/Common/remotesyslog1 {  
    host 1.2.3.4  
    remote-port 514  
}
```

Revision #3

Created 17 March 2021 06:54:10

Updated 31 May 2024 14:32:21 by Peter Baumann