IBM Expert Labs
Infrastructure expertise for
hybrid cloud and enterprise IT

Securing Your VIOS Server

Thomas Barlen
Senior Managing Consultant
IBM Power System Security
barlen@de.ibm.com

Agenda

- Basic Virtual I/O Server security configuration
- User management and authentication
- Audit and logging

Agenda

- Basic Virtual I/O Server security configuration
- User management and authentication
- Audit and logging

Introduction

- The Virtual I/O Server (VIOS) is a critical infrastructure component that provides resources to partitions that host business applications
- It is very important to properly protect the VIOS environment to prevent outages, data leakages, etc.
- The biggest problem is "*not doing anything to protect VIOS*" and "*always using padmin to log in to VIOS*"
  - No accountability
  - Issues cannot really be traced back to the source of the problem
  - Besides, only using padmin is using a shared user account, which violates all security regulations

Basic VIOS Security Setup

- VIOS comes with a standard command to set up security features after the initial setup
  - Command: **`viosecure`**
  - Command let's you set, change, and view security settings
- By default, after an initial install, no security levels are set
- **`viosecure`** performs two actions:
  - Applies security levels (low,medium,high or custom profiles)
    - Uses AIX Security Expert rules
    - Be careful with level high → Some services might not run anymore
  - Set up firewall rules

Basic VIOS viosecure command

- **`viosecure`** command syntax

```
Usage: viosecure  -level LEVEL [-apply]  [-rule ruleName] | [-outfile filename]
       viosecure  -view [ -actual | -latest ] [ -rule ruleName | -nonint ]
       viosecure  -file rulesFile
       viosecure  -changedRules
       viosecure  -undo
       viosecure  -firewall {on [[-force] -reload]| off} [-ip6]
       viosecure  -firewall {allow | deny} -port number [-interface ifname]
                  [-address IPaddress] [-timeout Timeout] [-remote] [-ip6]
       viosecure  -firewall view [-fmt delimiter] [-ip6]
```

Basic VIOS viosecure command – Security hardening

- The viosecure command provides a more convenient method to apply AIX Security Export rules
  - Can prompt for rules to apply

```
padmin@viosprod1:padmin> viosecure -level low

1. lls_maxage:Maximum age for password: Specifies the maximum number of weeks (13 weeks)
   that a password is valid
2. lls_maxexpired:Time to change password after the expiration: Specifies the maximum number
   of weeks to 8 weeeks, after maxage that an expired password can be changed by the user
3. lls_minlen:Minimum length for password: Specifies the minimum length of a password to 8
4. lls_minalpha:Minimum number of alphabetic chars: Specifies the minimum number of alphabetic
   characters in a password to 2
5. lls_minother:Minimum number of non-alphabetic chars: Specifies the minimum number of non-alphabetic
   characters in a password to 2
6. lls_mindiff:Minimum number of chars: Specifies the minimum number of characters required in a new
   password to 4, that were not in the old password
7. lls_histexpire:Password reset time: Specifies the number of weeks to 26 weeks, before a password
   can be reused
8. lls_histsize:Password reuse time: Specifies the number of previous passwords a user cannot resuse to 4
9. lls_pwdwarntime:Password expiration warning time: Specifies the number of days to 5 days, before the
   system issues a warning that a password change is required
10. lls_usrck:Check user definitions: Verifies the correctness of user definitions and fixes the errors
? 4
? a
Processedrules=1        Passedrules=1   PrereqFailedrules=0     Failedrules=0   Level=LLS
        Input file=/home/ios/security/viosecure.xml
```

Basic VIOS viosecure command – Security hardening (cont'd)

- View the applied rules

```
padmin@viosprod1:padmin> viosecure -view
prereqrrl_A3E0235C:Prereq rule for remote root login: Checks whether any non root user exists with privileges to
  login remotely
prereqtcb_A3E0235C:Prereq rule for TCB: Checks whether TCB is enabled or not
prereqsed_A3E0235C:Prereq rule for SED: Checks whether the machine has 64 bit kernel support or not
prereqnontcb_A3E0235C:Prereq rule for non-TCB: Checks whether the system is non TCB or not
prereqRSSSFull_A3E0235C:Prereq rule for RealSecure Server Sensor Full: This option is for the full version
  and has to be purchased.  Please visit www.iss.net to get more details.
prereqRSSSLite_A3E0235C:Prereq rule for RealSecure Server Sensor Lite: To use this option, please install
  ServerSensor.pkg
  from the Expansion Pack.
lls_minalpha_A3E0235C:Minimum number of alphabetic chars: Specifies the minimum number of alphabetic characters
  in a password to 2
prereqbinaudit_4B03D9CA:Prereq rule for binaudit: Checks whether auditing is running or not
prereqcde_4B03D9CA:Prereq rule for CDE: Checks whether CDE entry eixsts or not in /etc/inittab.
prereqnocde_4B03D9CA:Prereq rule for CDE: Checks whether CDE entry eixsts or not in /etc/inittab.


Press 'q' to quit or the enter key to continue
q
padmin@viosprod1:padmin>
```

Basic VIOS viosecure command – Security hardening (cont'd)

- Checking for compliance (changed rules)
  - Examples shows the check result when the minalpha attributes has been modified and does not match the security rule value anymore

```
padmin@viosprod1:padmin> viosecure -changedRules
Processing lls_minalpha_4B03D9CA : failed.
Processedrules=1        Passedrules=0   Failedrules=1   Level=LLS
        Input file=/etc/security/aixpert/core/appliedaixpert.xml

 User attribute minalpha, should have value 2, but it is 1


Processedrules=1        Passedrules=0   Failedrules=1   Level=LLS
        Input file=/etc/security/aixpert/core/appliedaixpert.xml
```

Basic VIOS viosecure command - Firewall

- The firewall is turned off by default
- If turned on, the default rules are applied, which allow the following traffic
  - ftp
  - ftp-data
  - ssh
  - web
  - https
  - rmc
  - cimom

Basic VIOS viosecure command – Firewall (cont'd)

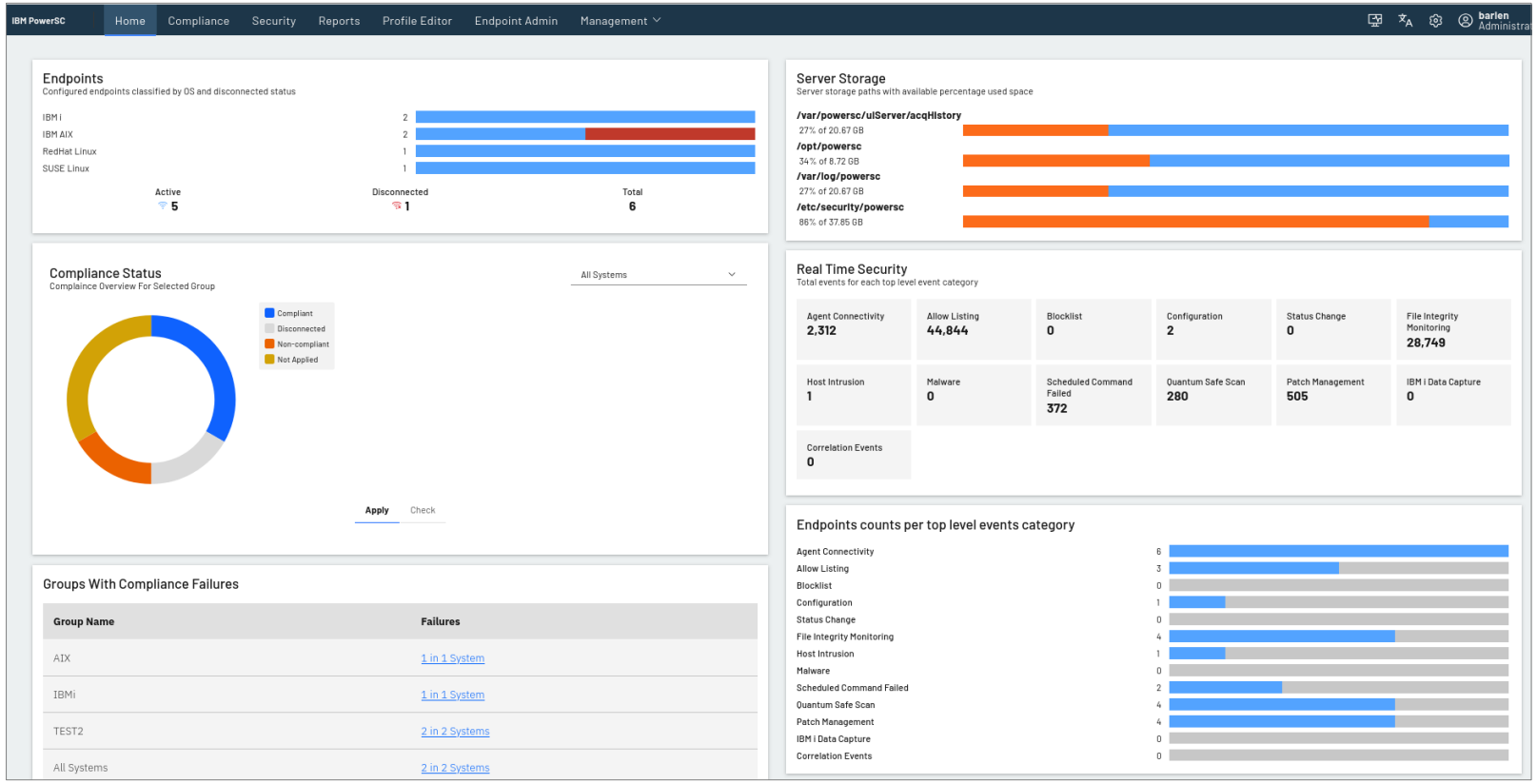
- Recommendations
  - Turn on the firewall (covers already commonly used VIOS ports)
  - If necessary allow other ports (by service name or port number)
    - If possible restrict by remote IP address

Example:
- Turn on firewall
- Allow communication to VIOS port 3211 from IP address 10.10.10.1

```
viosecure -firewall allow -port 3211 -address 10.10.10.1
```

Basic VIOS security

- IBM PowerSC provides also compliance profiles to harden VIOS and check for compliance
  - CIS V1 profile
  - CIS V2 level 1 profile
  - PCI V3 profile
  - Custom profiles



Agenda

- Basic Virtual I/O Server security configuration
- User management and authentication
- Audit and logging

User Management

- Recommendations
  - Do not use the padmin user for regular login
  - Create individual users for every person that has a need to work with the VIOS server
    - Assign proper Role-based Access Control (RBAC) roles to a user
    - VIOS comes with additional RBAC roles
      - Admin (Default if nothing is specified)
      - DEUser (Development Engineer)
      - PAdmin → provides access to **oem_setup_env** (equivalent permissions to user padmin)
      - RunDiagnostics
      - SRUser (Service Representative)
      - SYSAdm → provides **ONLY** access to **oem_setup_env**
      - ViewOnly (No change permissions)

User Management (cont'd)

- Creating a user with the IOS Command Line Interface command `mkuser`
  - Create a system administrator user ID. This assigns Admin as the default role.
    ```
    mkuser  barlen
    ```
  - Create a service representative (SR) user ID. This assigns SRUser as the default role.
    ```
    mkuser -sr barlen
    ```
  - Create a development engineer (DE) user ID. This assigns DEUser as the default role.
    ```
    mkuser -de barlen
    ```
  - Create users with varying access rights with the -attr flag by specifying roles and default_roles attributes. This assigns users with varying access rights, enabling them to access a varying set of commands.
    ```
    mkuser -attr roles=Admin,SYSAdm default_roles=Admin barlen
    ```

User Management (cont'd)

- Example creating a user with three roles
  - Note: After the user is created, a .profile is copied into the user's home directory. Once the user logs in the first time, the .profile is replaced with a link to /usr/ios/cli/.profile

```
mkuser -attr roles=Admin,SYSAdm,ViewOnly \
   default_roles=ViewOnly barlen2
--------------------
Log in with user barlen2
barlen2@:barlen2> mkvdev
Access to run command is not valid.

barlen2@:barlen2> rmvdev
Access to run command is not valid.

barlen2@:barlen2> lsmap -vadapter vhost13
SVSA            Physloc                                     Client Partition ID
--------------- ------------------------------------------- ------------------
vhost13         U8286.42A.102F5FV-V2-C33                    0x00000014

VTD                   NO VIRTUAL TARGET DEVICE FOUND
```

User Management (cont'd)

- Example continues
  - User needs to perform changes and switches to the Admin role

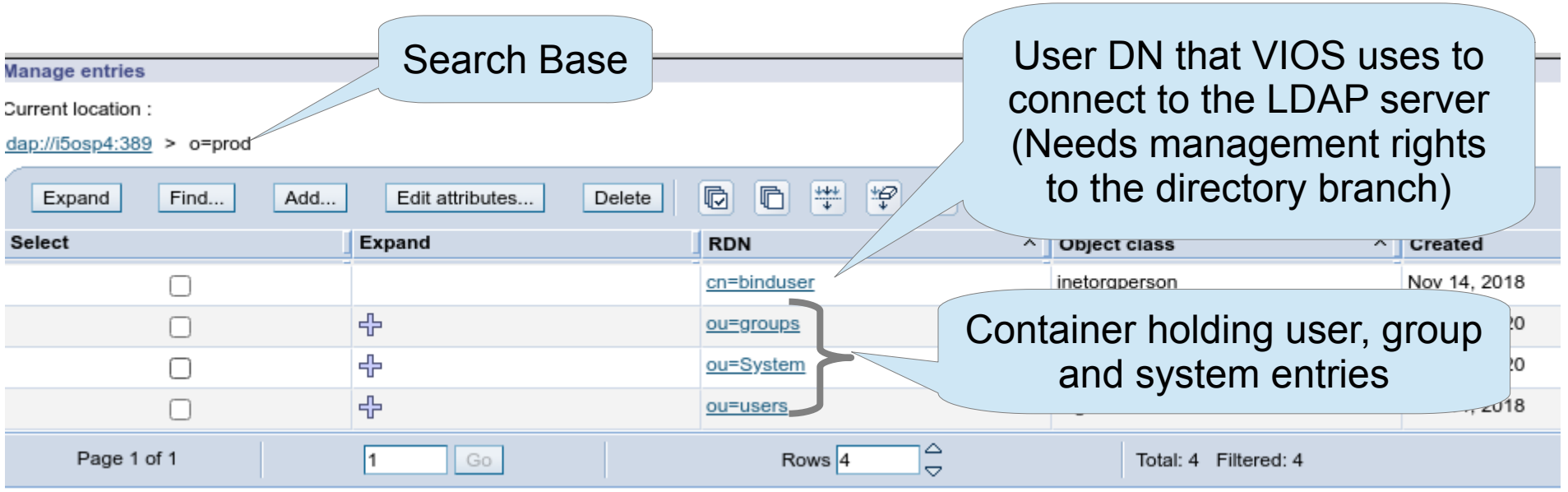
```
barlen2@:barlen2> rolelist -e
ViewOnly
barlen2@:barlen2> rolelist
Admin
SYSAdm
ViewOnly
barlen2@:barlen2> swrole Admin
barlen2's Password:
barlen2@:barlen2> mkvdev
rksh: mkvdev:  not found.
barlen2@:barlen2> ioscli mkvdev
Command requires one of the following options: -vdev -sea -lnagg -vlan -fbo

Usage: mkvdev  [-f] {-vdev TargetDevice | -dplc TDPhysicalLocationCode}
               {-vadapter VirtualServerAdapter |
               -aplc VSAPhysicalLocationCode} [-dev DeviceName]
...
```

Alias is not working when switching roles
You need to create a .kshrc for the user with aliases, etc. and add the following line to the .profile

```
export ENV=/home/$USER/.kshrc
```

User Management LDAP

- If you have many VIOS partitions, it is recommended to define the users in a central LDAP-based directory server
- VIOS can be configured to authenticate users against an LDAP directory
- Create LDAP directory base structure in the LDAP directory server before setting up the LDAP client in VIOS



User Management LDAP (cont'd)

- The VIOS mkldap command requires at least one user and one group entry in the LDAP directory to complete the configuration
  - You can export current users and groups to an LDIF file and then strip down the exported data and import the entries into the LDAP directory server

```
sectoldif -d o=prod -S rfc2307aix > user.ldif
....vi...
dn: ou=Users,o=prod
ou: Users
objectClass: organizationalUnit

dn: uid=default,ou=Users,o=prod
uid: default
objectClass: aixauxaccount
objectClass: shadowaccount
.... leave all groups in there and at least one user ...
ldapadd -c -h i5osp4 -D cn=administrator -w <password> -f user.ldif
Operation 0 adding new entry ou=Users,o=prod
Operation 1 adding new entry uid=default,ou=Users,o=prod
Operation 2 adding new entry uid=daemon,ou=Users,o=prod
...
Operation 28 adding new entry cn=system,ou=Groups,o=prod
Operation 29 adding new entry cn=staff,ou=Groups,o=prod
```

User Management LDAP (cont'd)

- Create the VIOS LDAP client configuration

```
barlen@viosprod1:barlen> mkldap -host i5osp4,172.17.17.40
  -bind cn=binduser,o=prod -passwd <password>
  -base o=prod -auth ldap_auth

barlen@viosprod1:barlen> mkuser -ldap tomadm
Changing password for "tomadm"
tomadm's Old password:
tomadm's New password:
Enter the new password again:



barlen@viosprod1:barlen> lsuser tomadm
tomadm roles=Admin default_roles=Admin account_locked=false expires=0 histexpire=0
histsize=0 loginretries=0 maxage=0 maxexpired=-1
maxrepeats=8 minage=0 minalpha=1 mindiff=0 minlen=0 minother=0 pwdwarntime=330
registry=LDAP SYSTEM=LDAP
```

User Management LDAP (cont'd)

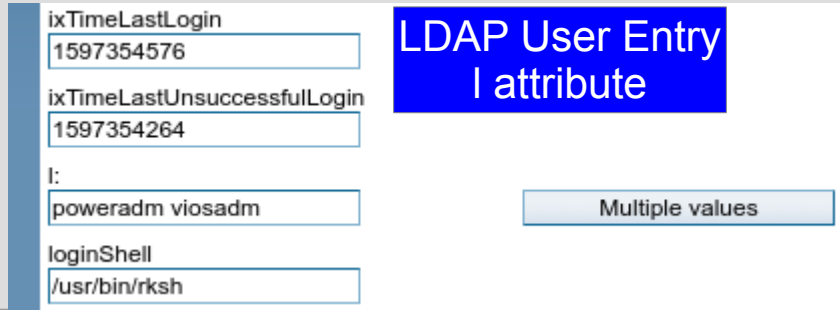
- Further configuration for centralized VIOS user management
  - Automatically create a user's home directory when logging in the first time

```
barlen@viosprod1:barlen> oem_setup_env

barlen@viosprod1:barlen> chsec -f /etc/security/login.cfg -s usw -a mkhomeatlogin=true

If you want to manage all users from the LDAP directory and not via the mkuser command,
change the default authentication to LDAP or compat mode
chsec -f /etc/security/user -s default -a SYSTEM="LDAP or compat"
```

User Management LDAP (cont'd)

- If you do not further restrict access for LDAP users, all users in the configured search base can log in to all VIOS server that have this specific search base (i.e. ou=Users,o=prod)
- There are multiple ways to restrict access for LDAP users for a partition
  - Use the account attributes `hostsallowedlogin` or `hostsdeniedlogin`
  - Use NetGroups
  - Use filter attributes in the user search base (shown in this example)

```
Edit file /etc/security/ldap/ldap.cfg and locate the line with the user search base
userbasedn:ou=Users,o=prod

Append a search filter to the user base DN, i.e. only users
userbasedn:ou=Users,o=prod??(|(l=*poweradm*)(l=*viosadm*))
```



Kerberos Authentication

- VIOS can also be configured as a Kerberos client
- Kerberos authentication is supported for:
  - SSH
  - Telnet
  - FTP
- Requires an active Kerberos (KDC, such as Microsoft AD) server in the network
  - Register Service Principal Names (SPNs) for the VIOS servers in the KDC
    - SSH / Telnet: host/fqdn@KERBEROS.REALM
    - FTP: ftp/fqdn@KERBEROS.REALM
- Use the `mkkrb5clnt` command to configure Kerberos for the VIOS server
- Add SPNs to local VIOS krb5.keytab file or get the file from the KDC administrator

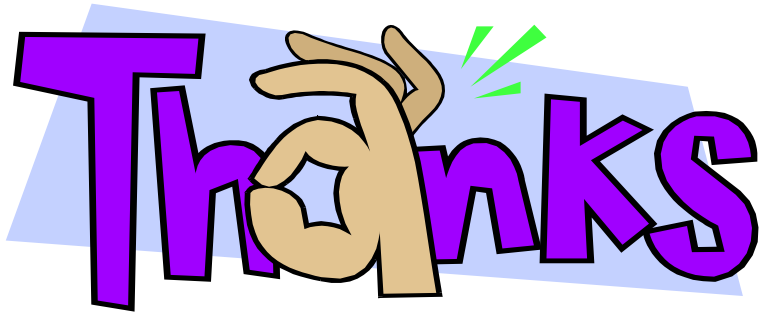
Agenda

- Basic Virtual I/O Server security configuration
- User management and authentication
- Audit and logging

Auditing and Logging

- Security policies as well as regulations typically mandate logging of various events, such as:
  - Successful and failed login attempts
  - User and group management tasks
  - Privileged user actions
- VIOS provides the same auditing and logging capabilities than a regular AIX environment
- Syslog by default logs *.info events to /var/log/syslog
  - No other events are logged
  - VIOS syslog.conf can also be configured to send events to a remote syslog server (recommended)
- The viosecure command can set up the audit subsystem in bin mode
  - Example: `viosecure -level medium -rule mls_binaudit`
    - Low: Turns on audit classes **general** for all users (root also has classes **tcpip** and **aixpert**)
    - Medium: Turns on audit classes **general, tcpip** for all users (root also has classes **SRC** and **aixpert**)
    - High: Turns on audit classes **general, SRC, cron, tcpip** for all users (root also has classes **mail, ipsec, lvm,** and **aixpert**)
- Manual changes can be made to the audit configuration to turn on role-based auditing (limits number of events)

Thanks



Thomas Barlen
Senior Managing Consultant
barlen@de.ibm.com

IBM Expert Labs

Visit us online

https://www.ibm.com/products/expertlabs

Expert Labs

Infrastructure expertise to help you build the foundation for today's hybrid cloud and enterprise IT data centers.

IBM Expert Labs helps you deploy the building blocks of a next-generation IT infrastructure that empowers your business.

- Solve business challenges
- Gain new skills
- Apply industry best practices

Contact us today to see how we can help empower your business.

Systems-Expert-Labs@ibm.com