Introduction to Sentinel 7 Lab

NIQ22 **Novell Training Services** www.novell.com

ATT LIVE 2012 LAS VEGAS

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

U.S.A.

www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Exercise 1-1 Install the Sentinel 7 appliance

This lab demonstrates how to install the Sentinel 7 Server Appliance for VMWare™ Server.
The files providing the appliance have been extracted already and were made available within VMWare Workstation.
Ask the instructor if you need help.

Configuring Sentinel 7 during first start

Start the virtual server called *sentinel_server*

1. If not started first load VMWare
2. Within VMWare Workstation start the VM called **sentinel_server**
3. In the following screen select a the language (English US) and press "Next"
4. Select the keyboard layout (English US) and press "Next".
5. In the following screens select yes to accept the license agreement and press "Next".

   There will be two license agreements. One for the OS and one for Sentinel 7 itself!

6. **Set or accept the hostname and the domain and press "Next".**
7. On the following screen make sure to select "Network Interface" before you click "Next".

   Configure the network interface to use 172.17.5.99 as the IP Address and /16 as the Subnet-Mask as shown on the next page and press "Next"

   If you are done with the configuration in this screen press "Next" for three times.

8. Configure the correct time settings and press "Next"
9. Set "novell" as the password for the user root and press "Next".
10. After this press "Next" again on the screen providing information on the minimum requirements for the installation.
11. Set "novell" as the password for the user admin and press "Next".

    After pressing "Next" the setup is compeeted an the Sentinel 7 services are started. This can take a few minutes.

    Even if you see the following lines on the screen wait for a couple of minutes before trying to login to the appliance.

12. **On the host start Firefox (or IE) and enter https://172.17.5.99:8443 for the URL.**
    You will have to trust the certificate provided. If you see the login you completed the lab.

(End of Exercise)

Exercise 2-1 Logging into the Web UI

Users can log into the web UI.

Logging into the Web UI

Log into the web UI:
1. From the host desktop select the firefox icon from the quick launch tray in the lower left hand corner of the screen.

In the address field of the browser type the address of the secure port of the Sentinel server:

https://172.17.5.99:8443

When the Sentinel login appears, enter the following user name and password:

Username: admin
Password: novell

2. In the top left of the web UI select the **Collection** icon.

What is the EPS rate over the last minute?

3. Select the next icon, **Storage**

How much, and what percentage of space is currently being used?
How much space is currently available ?
What is the current usage rate per day?
How much space will be needed over the next 90 days?

4. Select the **Routing** icon next.

Are any events being routed to another Sentinel system?

5. Select the **Users** icon.

What users currently exist on the system?
What groups?
What can users that belong to the Administrator role do?

6. Select **Search Setup** next.

What other servers are being looked at when a distributed search is performed?

Exercise 2-2 Logging into the Sentinel Control Center

Users can log into the Sentinel Control Center.

Logging into the Sentinel Control Center

If you have logged out of the web UI, follow step 1 to log back in.
Log into the web UI:
1. From the host desktop select the firefox icon from the quick launch tray in the lower left hand corner of the screen.

In the address field of the browser type the address of the secure port of the Sentinel server:

https://172.17.5.99:8443

When the Sentinel login appears, enter the following user name and password:

Username: admin
Password: novell

2. In the top right of the web UI select the **Applications** icon.

In the center of the screen there are 2 downloads available. **Sentinel Control Center** and **Solution Designer**.
Select **Launch Control Center**

3. When the Sentinel Control Center has launch and prompts for a password, use the following:

Username: admin
Password: novell

4. Select the **Active view** tab.

In the last 30 seconds, approximately how many events from any event source was of Severity 4?

5. Select the **Incident** icon.

In the Incidents viewer, how many incidents are currently in an open state?

6. Select **iTRAC** next.

At what point in the workflow ConditionalTransitionExample is the incident from the previous example? (it will be highlighted in red)

(End of Exercise)