

Identity and Security Compliance Management

[Rogue Administration Use Case]

Patrick Holderness

pholderness@novell.com

About This Document

Each Utopia Demo will have two or three pieces of documentation, to be used as follows:

1. use this Quickstart to prepare for your demo meeting. It includes everything you need to know to get the right virtual machines started and ready to begin showing the solution. Use this quickstart if you are building the demo locally on your own hardware or if you are accessing a pre-built version on the Novell Online Demo System (NODS)
2. Once your demo virtual machines are started and at the right place you're ready to begin your demo. If you know the products and your customer's requirements then you can go ahead and deliver your own demo using the system. However if you would like further instructions then the Tutorial will give you a guide of how to drive the demo.
3. In some cases a third piece - a Sample Demo is provided, which gives an illustration of how the solution might be shown to a customer.

For online copies of all these documents please visit <http://www.novell.com/communities/demosystemsbook>

Demo Synopsis

When an identity attribute is changed by an administrator, not by Identity Manager, it is called rogue administration. Sentinel can capture such events and initiate appropriate actions.

In this implementation the SOAP integrator feature of Sentinel is used to initiate a workflow in the Identity Manager User Application. The workflow disables the perpetrator's account and notifies his/her manager of the activity.

Setup Instructions

Virtual Machines

ISM-IDV			
IP address	Memory	Disk Space	DVD #
172.17.2.91	2048 MB	8.78 GB	3a

ISM-W2008			
IP address	Memory	Disk Space	DVD #
172.17.2.93	1024 MB	19.3 GB	3d

ISM-SentinelRD			
IP address	Memory	Disk Space	DVD #
172.17.2.98	2048 MB	9.6 GB	3f

User ID's

u:root p:n0v3ll

u:administrator p:n0v3ll

u:uaadmin p:n0v3ll

u:rogueadmin p:n0v3ll

u:admin p:n0v3ll

Useful URLs

A Utopia folder listing useful URLs is available in the favorites on each machine referenced. The Identity Manager User Application must be used in conjunction with this demonstration.

<http://172.17.2.91:8080/IDM/jsps/login/Login.jsp>

<http://172.17.2.98:8080>

Preparing The Demo

- Start/resume ISM-SentinelRD.
- Once ISM-SentinelRD has started/resumed, login as administrator.
- Once logged in to ISM-SentinelRD, start Sentinel using the icon on the desktop.
- If this image has not been started within the past 10 days Add Partitions using the icon on the desktop.*
- Start/resume ISM-IDV.
- Once ISM-IDV has started/resumed, login as root
 - If integrating this machine for the first time see the note on configuring the Sentinel driver.*
- Start/resume ISM-W2008.
- Once ISM-W2008 has started/resumed, login as ad\administrator.
 - If integrating this machine for the first time see the note on installing a collector manager.*
- On ISM-SentinelRD
 - Login to Sentinel Control Center as admin by performing the following steps:
 - Using Firefox, access the Sentinel login page.
 - Click Applications
 - Click Launch Control Center
 - If integrating this machine for the first time see the note on configuring the ISM-W2008 event source.*


Notes / Issues

When provisioning the Compliance Management Platform demo on NODS these steps have already been performed. The following instructions apply only to a local copy of the Compliance Management Platform demo images.

Install a collector manager.

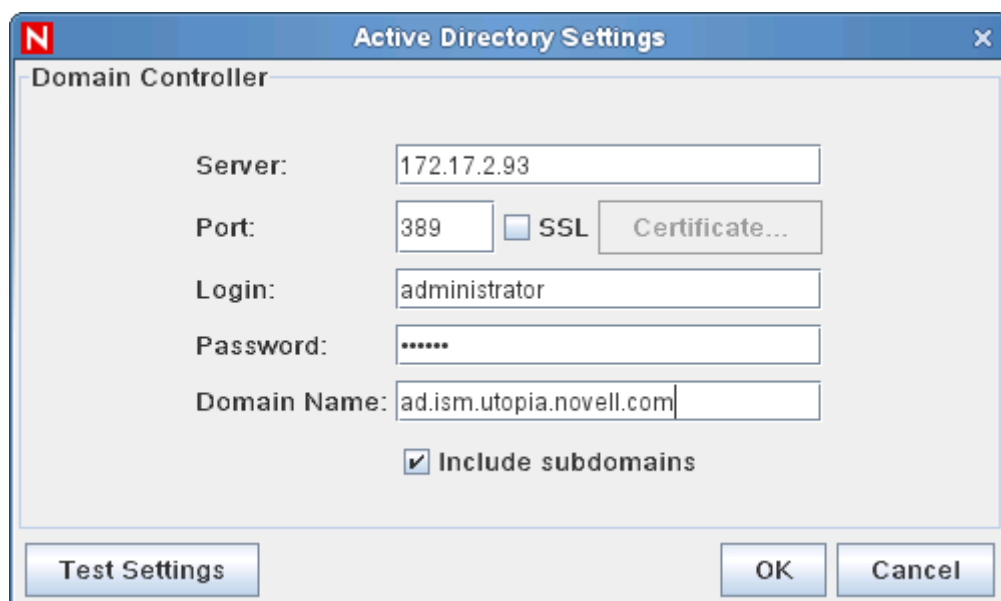
- Using a browser, go to <http://ism-sentinelrd:8080> and login as admin
- Click the Applications link
- Click Download Installer to download scm_installer.zip
- Unzip the scm_installer.zip file.
- The files are unzipped to a directory named disk1.
- Run disk1\setup.bat
- Select a language to proceed with the installation.
- Read the Welcome screen, then click Next.
- Accept the End User License Agreement, then click Next
- Specify C:\Novell\Sentinel6 as the installation location, then click Next.
- Keep the default Message bus port (61616)
- Change the Communication Server host name to ISM-SENTINELRD, then click Next
- Select Automatic Memory Configuration, then click Next
- Click Install
- Supply the collectormanager password (480ccb7460d3f8b0053235dc443b11e), then click Next
- Read the Security Warning, then click Accept Permanently
- Click Finish
- Select No, I will restart my computer at a later time, then click Finish
- Modify the properties of the Sentinel service using the Services console
- On the Log On tab select This account using ad\administrator for the username
- Type n0v3ll in the password and password confirmation text boxes, then click OK
- Read the privilege message, then click OK
- Click OK to dismiss the properties panel
- Start the Sentinel service

Configure the Sentinel driver.

- Copy `/opt/novell/sentinel6_rd_x86-64/jre64/lib/security/jssecacerts` from ISM-SentinelIRD to `/opt/novell/eDirectory/lib64/nds-modules/jre/lib/security` on ISM-IDV
- Restart eDirectory
- Using Firefox access the Novell iManager bookmark and login as admin
- Click Identity Manager Overview
- Click the search  button
- Click driverset1
- Edit the Driver Configuration properties of the SentinelIRD driver
- Type `ssl://172.17.2.98:61616` in the Broker URL text box
- Supply the collectormanager password (480ccbf7460d3f8b0053235dc443b11e) in both the Broker Password and Reenter Broker Password text boxes, then click OK
- Start the SentinelIRD driver
- Download http://www.novell.com/communities/files/rogue_administration_designer_artifacts.zip
- Unzip `rogue_administration_designer_artifacts.zip`
- Launch Designer
- Right click Directory Abstraction Layer, then click Import from File
- Read the warning on overwriting existing files, then click OK
- Specify `DAL_Entity_User.xml`, then click OK
- Deploy the User entity
- Right click Provisioning Request Definitions, then click import from File
- Read the warning on overwriting existing files, then click OK
- Specify `Rogue_Administration_Activity.xml`, then click OK
- Deploy the `Rogue_Administration_Activity` PRD found in the Accounts category
- Exit Designer

Configuring the ISM-W2008 event source.

- Click Event Source Management, then click Live View
- Right click the newly installed Collector Manager, then click Add Collector
- Click Add More, then click Next
- Browse to
`/opt/novell/sentinel6_rd_x86-64/content/Microsoft_Active-Directory-and-Windows_6.1r5.clz.zip`
- Click Open, then click Next
- Read the update warning, then click Next
- Click Finish
- Click Active Directory 2008, then click Next
- Click Next at the Select Collector Script dialog
- Click Next at the Configure Collector Property dialog
- Check Run, then click Finish
- Right click the newly installed collector, then click Add Connector
- Click Install More Connectors
- Click Next at the Plugin Import Type dialog
- Browse to `/opt/novell/sentinel6_rd_x86-64/content/wms_connector.zip`
- Click Open, then click Next
- Read the update warning, then click Next
- Click Finish
- Click WMS, then click Next
- Click Configure Active Directory Settings and set according to this image (Password=n0v3ll)



Active Directory Settings

Domain Controller

Server: 172.17.2.93

Port: 389 SSL Certificate...

Login: administrator

Password: *****

Domain Name: ad.ism.utopia.novell.com

Include subdomains

Test Settings OK Cancel

- Click OK, then click Next
- At the Service Installation dialog use ad\administrator for the Login Name and n0v3ll for the Password
- Click Install Service
- Click Finish (Do not click run until you have verified that the WMS service has started on ISM-W2008)
- Right click the newly installed connector, then click Add Event Source
- Choose Select from Active Directory, then click Populate List
- Select ISM-W2008, then click Next
- Click Next at the Connection Mode (Advanced) dialog
- Click Finish
- Verify that the WMS service is running on ISM-W2008, then right click the newly created event source and click Start

Where next?

- Visit our documentation site at <http://www.novell.com/communities/demosystemsbook> and navigate to the demo you are preparing
- Watch the Tutorial for your demo.
- Watch the Sample Demo if one is provided.
- In case of any issues please post your query to the support forum at <http://forums.novell.com/novell-product-support-forums/utopia/>