Deltek INSIGHT 2014

Tech Titans: Lock it down, securing your Costpoint 7 deployments

Drew Roman, IT Solutions Director
WJ Technologies L.L.C.

GC-518

OPTIMIZE YOUR POTENTIAL

Deltek INSIGHT 2014

Agenda

OPTIMIZE
YOUR POTENTIAL

Agenda

- Overview
- The Basics of Secure Deployment
- Database
- Application tier
- Web Tier
- Network
- Changes in Costpoint 7
- Questions

Deltek INSIGHT 2014

Overview

OPTIMIZE
YOUR POTENTIAL

Overview

- There is no such thing as a truly secure computer system, only more or less secure
- Security starts with the proper mindset
- The techniques covered today are only a few of the steps you can take to make your system more secure
- Security is a constantly moving target, please do not take what is covered today and think that it is all you need to do to secure your systems
- Our main goal is to minimize the attack surface as much as possible while maintaining functionality

Deltek INSIGHT 2014

The Basics

OPTIMIZE
YOUR POTENTIAL

The Basics

- Securing the different tiers
  - Database
  - App tier
  - Web tier
- Windows
  - Patching
- Network

- The upgrade from Costpoint 6 to 7 is an ideal time to put these practices in place
  - Take advantage of the extended testing and make sure that everything is working and performing as you would expect it to
  - If you're already on Costpoint 7, making these changes to test systems first is strongly recommended
- Deltek's Costpoint 7.0.1 Post-Installation Hardening Guide covers some of these topics, a few others and contains many links to other resources

Database

- The database is the foundation of your system, the “Keys to the Kingdom” so to speak
- A person with malicious intent can wreak havoc if they gain access to the database, even if it’s read-only access
- Set strong passwords for each of the users and change them regularly
- End-users no longer require database accounts for Costpoint access
  - Disable and/or remove accounts that are no longer needed
- Control who has administrator level access to database servers and individual databases
- Audit privileged account use
- For all accounts, grant the minimum required rights needed for running the software

App Tier

- Change the password for the Weblogic system account and other Weblogic acccounts
- Minimize rights of the service account running the Costpoint services
  - This user should only be a regular domain user with admin rights on the app servers locally
  - Only grant this account file and share access to the bare minimum that it needs for operation
- Only install the bare minimum of software and Windows Roles/Features required for operation
- If using Active Directory Authentication, secure the connection using SSL if possible

Web Tier

- Don’t expose the application directly to the internet unless you have to
  - Remote access is usually best handled using a VPN or other methods to remotely connect to your network resources
- Use and enforce SSL, even if Costpoint is only available on your LAN
- Only install the IIS Role Services that you need

Windows Server

- Only install the roles, features and 3rd party applications needed to run the software and manage your systems
- Ensure that the systems are fully patched when you put them into service and patched on a regular schedule
- Use the Windows firewall to minimize what ports are available
  - Ports required for management and ports for services like database listeners, web server ports, etc.

Network

- If you must expose Costpoint to the internet, the Web Tiers should be non-domain members, set up in a DMZ zone on your network
  - Set rules on your firewall to only allow the ports needed
    - TCP 443,80 in to IIS
    - TCP 7009 from IIS server to Weblogic
- Use SSL to secure the connection to Active Directory if possible
  - Weblogic performs an LDAP ‘simplebind’ when connecting to Active Directory
  - If you are connected to the AD over the standard TCP port of 389 and not using SSL (port 636) your AD usernames and passwords are traveling over the network **in the clear**
  - Active Directory must be set up for secure communications and the certificate that signed your AD servers certificate needs to be imported into the cacerts certificate store in Weblogic

Network (cont.)

- Configuring trust for your Active Directory Server
  - Oracle's documentation for this process is very detailed
  - Export the certificate of your CA
  - The Java 'keytool' command is what's used to import the certificate, the command would be similar to:
    - `keytool -import -alias ALIAS -file CA_CERT_FILE -keystore KEYSTORE -storepass KEYSTORE_PASSWORD –trustcacerts`
  - Once imported, you can go into the Costpoint configuration Utility and set your configured AD server(s) to use SSL and connect over TCP port 636
  - After restarting Weblogic, you should be connecting securely

Patching

- Keep your Operating Systems as up to date as possible
- Keep up with the patches for your Database platform
- Subscribe to the emails from Deltek regarding your products, monitoring them for any security related patches and apply as soon as feasible
  - Ideally apply them in a test environment first
- Deltek delivers patches for products that are bundled with the applications, such as Weblogic, I would not recommend obtaining those directly from Oracle or the other vendors

Deltek INSIGHT 2014

Costpoint 7 Changes

OPTIMIZE
YOUR POTENTIAL

Costpoint 7 Authentication Options

- You now have many new authentication options for Costpoint 7
  - Costpoint Database
  - Active Directory
  - Single Sign-on
  - Single Sign-on or Active Directory
  - Windows Domain and Active Directory
  - Windows Domain and Costpoint Database
  - Client Certificate

Costpoint 7 Authorization Changes

- Groups are now additive
  - Users can be members of multiple groups, with rights adding up to a resultant set of rights
- Deny always takes precedence
- WAY more flexible than Costpoint 6
- Segregation of Duties
  - Allows for configuration and enforcement of Segregation of Duties rules

Deltek INSIGHT 2014

Questions?

OPTIMIZE
YOUR POTENTIAL

Contact Us

Drew Roman
IT Solutions Director
Drew.roman@wjtechnologies.com
703-885-8160
http://linkedin.com/in/drewroman

13665 Dulles Technology Drive
Herndon, VA 20171
www.WJTechnologies.com

