March/April 2010 On Technical/Security

EnterpriseOne® Security Best Practices: Looking Outside the Box

By Gregg Larkin

Editor's Note: *Think EnterpriseOne security and you're probably thinking about application security. But there's a much bigger picture that needs to be considered when reviewing your security practices with respect to your EnterpriseOne system. In this article, Gregg Larkin takes you on a tour of all of the servers and areas external to the applications that could bring unwanted exposure if they're not locked down.*

Introduction

Being the systems administrator (CNC) for a large EnterpriseOne system is a big job. One of the aspects of that job is locking down and securing the EnterpriseOne environment. Yes, application security is a big piece of that. But that's not what this article is all about. This article will focus outside the box and outline all of the other things that need to be locked down in addition to the objects and reports inside the application. At my company, I am responsible for setting up and maintaining the application security for over 300 security groups. I also have to make sure that enterprise servers, databases, web servers, transaction servers, third-party tool servers, and the like are secured and maintained as well. This article will discuss the best practices for overall system security, as well as some tips from the field.

This article will focus outside the box and outline all of the other things that need to be locked down in addition to the objects and reports inside the application.

This article will be useful for the following audiences:

- New customers setting up EnterpriseOne
- Existing customers migrating to E1 9.0, or updating part of their technical environment
- CNCs performing a systems audit or doing a periodic "sanity check"
- IT auditors
- IT Management charged with ultimate responsibility for system security

This article will provide you with a high level overview of what you need to look for to make sure your EnterpriseOne environment is locked down and as secure as possible. Most of the tips listed will be generic enough for all releases of E1 from XE to 9.0. I will hit on some new items found in Tools Release 8.98 / E1 9.0.

Copyright © 2010 by Klee Associates, Inc.
www.JDEtips.com

Common System-Wide Security Practices

This first section focuses on general server best practices.

Stay Current with Patches

One principle of good security and system maintenance is to establish a regular schedule for applying patches. In our shop, we have a monthly and quarterly patch and maintenance cycle.

Each month, we have two evenings scheduled during which we patch production servers. All of the servers in our environment are kept to the latest patch levels for their appropriate operating system and firmware. Application owners are also encouraged to use the outage window to apply their patches. The monthly outages occur after regular working hours for the majority of our users, with exceptions for systems that require 24/7 uptime.

Once a quarter, we take a day-long outage on a Saturday. During the quarterly outages, more complex maintenance is applied. This may include activities like firmware updates, SAN maintenance, OS service pack upgrades, telecom and router updates, and more. Again, application owners like the JDE® team are encouraged to use this window for their large maintenance projects such as disaster recovery testing, database patches, application updates, etc.

For example, an IT organization needs to maintain the following:

- Server Operating System patches
- Server/SAN/Networking firmware
- Database hotfixes, patches, and service packs
- Application hotfixes, patches, and service packs
- Anti-Virus and Malware detection updates and patches
- Oracle® Critical Patch Updates (www.oracle.com/technology/deploy/security/alerts.htm)

Monitor System Activity

This sounds simple, but is actually a complex topic. Each component in your system has some degree of monitoring capability, either natively baked in, or through a third-party add-on tool. An IT organization needs to have a system and a policy in place to monitor its systems and applications. Decisions also need to be made and revisited periodically to determine what to monitor and how actively and/or proactively.

Some examples of monitoring tools include:

- Monitor drive space utilization that alert us when certain disk thresholds are crossed.
- Monitor if an application or server goes down, and if so, send out an alert to the Network Operations team.
- Monitor batch processing and send alerts when batch jobs (EnterpriseOne and other applications) fail.
- For certain key nightly processes, we have set up expected time parameters for completion. If the process exceeds the time parameter, it will trigger alerts to the operators and text messages to the administrators (that's always a fun way to be woken up at 2 am).

JDEtips Knowledge Express

This Article Continues…

Subscribers, log in from our main search page to access the full article:

www.JDEtips.com/MyAccess.html

Not a Subscriber? Gain access to our full library of JDE topics:

www.JDEtips.com/JD-Edwards-Library

Visit **www.JDEtips.com** for information on the JDEtips University schedule, private training and consulting, and our Knowledge Express Document Library.

License Information: The use of JDE is granted to JDEtips, Inc. by permission from J.D. Edwards World Source Company. The information on this website and in our publications is the copyrighted work of JDEtips, Inc. and is owned by JDEtips, Inc.

NO WARRANTY: This documentation is delivered as is, and JDEtips, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. JDEtips, Inc. reserves the right to make changes without prior notice.

Oracle and J.D. Edwards EnterpriseOne and World are trademarks or registered trademarks of Oracle Corporation. All other trademarks and product names are the property of their respective owners.

Copyright © by JDEtips, Inc.