



State Data Center Security Shared Services Architecture Project

Technical Forum Notes and Handouts

11/09/07

Table of Contents

1.	MESSAGE FROM ARCHITECTURE TEAM.....	3
2.	TECHNICAL FORUM NOTES/Q&A.....	4
3.	SECURITY ARCHITECTURE TECHNICAL FORUM – PRESENTATION SLIDES	8
4.	SDC ARCHITECTURE TEAM WEBSITE – HANDOUT.....	12
5.	CA MIGRATION STRATEGY FOR DISTRIBUTED SYSTEMS – HANDOUT	13

1. Message from Architecture Team

The SDC architecture team wants to thank all the customers who came to the Security Shared Service Architecture Technical Forum on October 25, 2007. We appreciate the candid feedback and remain committed to sharing information about architecture strategy and direction as early as possible with our customers. We ask that customers be patient with our ability to answer detailed questions about how we will deploy specific technology in each agency.

As mentioned at the forum, the SDC intends to introduce architecture concepts by each domain area (server, network, storage, etc). Agency specific technical implementation planning sessions will follow these general introduction sessions as the state rolls out projects for each technology architecture deployment.

You should feel free to contact any member of the architecture team if you have questions about the materials contained in this packet.

Sarah Miller:	Business Architect	503-373-0765
Kurtis Danka:	Technical Architect	503-373-2043
Claudia Light:	Project Manager	503-373-2091

We look forward to continued partnership as we work together to build the future.

2. Technical Forum Notes/Q&A

**Security Shared Services Architecture Overview
Technical Forum Notes
Thursday, October 25, 2007 9:00 AM - 11:00 AM
State Data Center, Room 104**

Presenters:

Kurtis Danka	Technical Architect	503-373-2043
Sarah Miller	Business Architect	503-373-0765
Marshall Wells	Security Manager	503-373-0949

Security Team Members:

Shawn Dawson	Team Lead	503-378-2173
--------------	-----------	--------------

Architecture Team Members:

Claudia Light	Project Manager	503-373-2091
Sherrie Looper	Technical Writer	503-373-2136

Attendance: 31

Agencies Represented: DAS, DHS, Employment, ODVA, Lottery, DOJ DCS, OPRD, SDC, ESO, SOS, ODF, ODOT DMV, OMD, ODOC, OHCS, DCBS

Agenda

Introductions/Overview - Sarah Miller

This is the fourth in a series of technical forums being held at SDC in regards to the architecture planning efforts to form a shared services environment. This session will cover some general information about the current state of security systems and projects going on at the SDC and how we are currently leveraging these security systems.

Sessions have been previously held for Distributed Systems (Server), Network and Storage Architecture. These forums are an attempt to provide a general overview of the consolidated architecture strategy in regards to each domain area (server, network, security etc.). Individual Agency planning meetings will also be held to discuss strategies and agency business requirements.

Security Architecture Overview - Marshall Wells

[Security Technical Forum Architecture Presentation.ppt](#)

This presentation provides an overview of the current and planned security architecture at the SDC. It also discusses key features and highlights of the technical security infrastructure which is driven by the customers' business requirements. This includes the goals of being Cost effective and Business-driven, maintaining a Supportable infrastructure, and being Standards-based in all technology and supporting processes.

SDC Architecture Team Website – Sarah Miller

The SDC has put together a website to provide a single source of information for their customers. We can't stop the sharing of information, nor do we want to, but we can provide an authoritative source of information that will contain all approved communications regarding the efforts of the State Data Center.

Website address: http://oregon.gov/DAS/SDC/initiatives/arch_index.shtml

Q&A – These are listed in the order they occurred during the forum.

Standardization – General:

Q. The presentation is mainly referring to overall technology, but will supporting processes be discussed as well?

A. The individual processes that will support the implementation of the technology will be built along with them.

Q. Does the SDC use a data base to track changes?

A. We have a support request process in place and are working toward an enterprise Configuration Management system, in which we will work with our customers to build the appropriate processes that will support it. In the non-security realm, we are in the process of building a CMDB product as well as the standardized processes to support it (we use Remedy right now). This project is still in development.

Q. Do you have certificate services at the edge?

A. If this business need comes through the request process we will work with the customer to identify the best technology & build the appropriate process as needed, but an enterprise solution will be sought after first. One on one solutions can be used where appropriate, but enterprise-wide answers are the top priority.

Q. Digital certificate project – is the SDC working with this?

A. Yes we are involved and we will implement the technology to support it. Marshall is on the statewide board for this so he is aware of the current developments for it.

Firewalls:

Q. Are there tools that you can recommend that will help us understand the logs and information you send us?

A. In the near future we will be using SolSoft internally and looking at giving read access to SolSoft for monitoring of traffic. This will give a map that shows a customers' devices and a snapshot of the rules for traffic, but it will not reflect a complete rule set. A complete rule set will still need to go through complete analysis.

Q. Is there any interest in blocking protocols that aren't implemented within a business process for any agency?

A. We don't really have the capability to do this. We can respond to each incident only where we can block them out through the process of dealing with that incident, but in the low security zone we

don't have the legal right to block this kind of traffic. We aren't pursuing this at this time because we don't have the scope of control within this zone.

Q. If the perimeter is being hammered and the process is to shut it down, is this an automated response or a manual one?

A. This is a manual response, to actually shut down the system, although the Network Intrusion Prevention technology by design alerts to the situation and recommends a course of action in response. But, the decision on how to respond will be manual.

Standardization - Where we are now:

Q. As new projects are undertaken, are there SDC standards that we can validate proposals against. Will standards be available to the customer to validate and follow?

A. We have a process that the customer can validate against, and if an exception arises we can look at this individually to see where gaps may exist to find a solution. Our standards are proprietary but not secret and we are glad to give support through the support process.

Q. Are there processes that exist for Incident Management? If servers are being placed by one part of the SDC, will someone be reviewing the process & technology risks for those servers and provide them to the customer?

A. Yes, we will be involved with this... there is an effort behind anything we put in place through the standardized procedures, and risk analysis is part of that effort.

Q. There is an effort toward controlling identity theft (Senate Bill 583), is the SDC in compliance with this effort and to what extent?

A. Yes, there is an ongoing effort. The SDC is engaged in an internal analysis where we will form a workgroup with customers to discuss and analyze the specific requirements needed for this effort. This will include the DCBS because they are the ones enforcing it. There are two options to address: 1) a full featured security program, and 2) the redaction or encryption of personally identifiable information. The problem we're encountering is that we don't know specifically where the data is located, but we're working on an answer to where we will outline the infrastructure for the customers' data and they will identify what that data is & where it is specifically located. Discussion on this needs to happen further to ensure that compliance is achieved but that the customers' needs are also served. A cost impact is anticipated.

Q. For out of scope/non-SDC managed servers, are you encouraging use of the SDC secure server build? Can the agencies leverage tools that the SDC uses in their server build for non-SDC servers?

A. We encourage using the standardized build process that we use in the SDC, and we are happy to share that documentation with other agencies. But, we may not be able to offer use of licensed tools because it would encroach on contract issues. We will need to research this further.

Standardization - Where are we going:

Q. As a part of the community of practice for data classification, can we include an option for Host Intrusion Protection, or associate use of tools with a particular data level?

A. The SDC is putting the Host-based protection on all of the servers, but the controls that are enforced will vary based on the sensitivity of the information. i.e. For a standard server, this can be

set on a network and talk to other servers on the network, but cannot cross connect to outside servers. But there may be a case where a specific server won't be able to go on all of the network lines because of the data it is holding. We must weigh the individual risks, data, and many other variables to decide this. The development of process to support each situation is growing and will be in place as each new technology is implemented.

Configuration Management:

Q. Will the SDC share the plans for CM within Security with customers?

A. Always.

Timeframes:

Q. As we look at workstation builds and software applications for VPN & Remote Access, do we need to make sure that they will run properly with Cisco?

A. If you are using our client then yes. If you're using your own VPN, then it's a harder question to answer. Citrix remote will be a factor in this as well.

Q. How much firewall structure has moved from last year's diagram to the one shown today?

A. We've moved a few agencies to central firewalls, but the major effort has been to get the firewalls up that are supportable, and our next effort is to move to a single brand to be more manageable. After this, we will be about 50% integrated.

Q. Are you building in rules & having discussions as to re-engineering processes - will the agencies need to initiate this?

A. We will be including customers in all of the process discussions, but if a customer is proactive in this it would get us that much further ahead once the discussions take place. We need to look at what is most appropriate for the situation, including what processes may be already in place. Accountability and controls are being built within the process to determine the need to review the rules as things change in the future. We are doing our best to get the justification down at the beginning in order to know down the road why rules were put in place, and then determine if those reasons are still valid.

3. *Security Architecture Technical Forum – Presentation Slides*



Security Architecture Principles

Technical Security must be:

- Cost Effective and Business Driven
- Supportable
- Standards Based

Cost Effective and Business Driven

- Flexible architecture provides for granularity of controls
- Ability to accommodate agency business requirements
- Consolidation of security controls to reduce administrative overhead

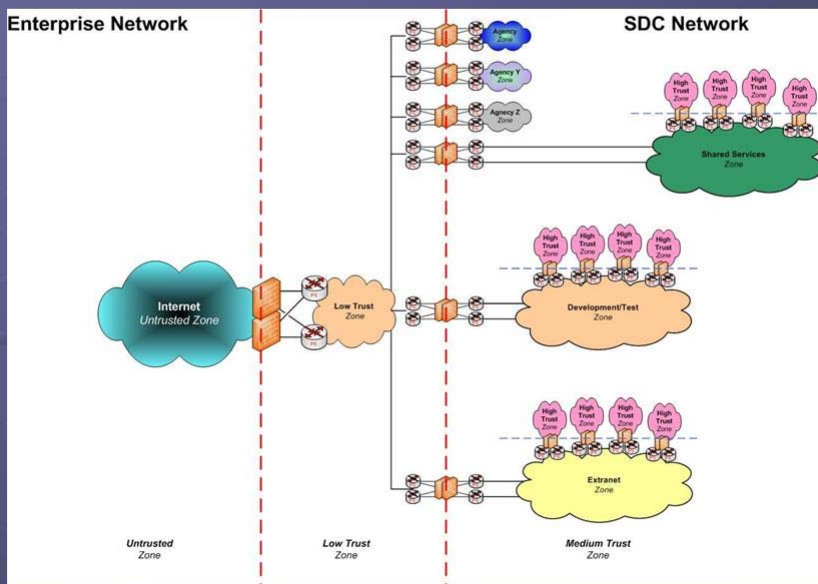
Supportable

- Standard processes and procedures in support of security controls
- Centralized management of security controls
- Increased logging and monitoring
- Integration permits greater security enforcement and intelligence
- Standard equipment allows for easier implementation and for replacement in the event of a failure

Standards Based

- Use standards-based technologies to provide security (e.g. AES, 802.1x, etc.)
 - Increases the likelihood that security technologies are interoperable
 - Ensures that implemented technologies have been subjected to the process review necessary to achieve the status of “standard”

Zoned Network Security



Where we are...

- Secure Server Builds
- Site-to-site encryption availability
- Network Access Control
 - Firewalls
 - VLANs/MPLS
- Anti-Virus / Patch standardized
- Network Intrusion Detection
- Email Firewalls
- Log Aggregation

Standardization

Where we are going...

- Wireless Network Security
- Network Admission Control
- Host Intrusion Protection
- Consolidated Remote Access VPN
- Firewall Consolidation
- Increased Use of Log Aggregation
- Replace Network Intrusion Detection
- Configuration Management

4. SDC Architecture Team Website – Handout

State Data Center – Architecture Team website :: http://oregon.gov/DAS/SDC/initiatives/arch_index.shtml

OREGON.gov
Enter search term(s) [Find](#)
Text Size: A+ A A Text Only Site Accessibility

State Data Center

Department ▾

Search

About Us

Contact Us

Services


PCTV Video Streaming

Voice Services

State Data Center Home

SDC Architecture Team

About Us



Here you will find the authoritative source for SDC architecture information. The SDC provides a consolidated shared service environment for customers across all service delivery areas including: network, server, storage, security, voice, and enterprise. Information posted here is official communication to SDC customers.

Contact Information
Department of Administrative Services
State Data Center
Architecture Team
530 Airport Road
Salem, OR 97301

Team Members

Kurtis Danka Technical Architect (503) 373-2043	Sarah Miller Business Architect (503) 373-0765	Claudia Light Process Architect (503) 373-2091
---	--	--

Architecture Resources (pdf)

[Arch. RFP Guidelines](#)
[Arch. Governing Principles](#)

Project Documentation

Project Documentation will include documents that relate to the Architecture Project specific deliverables.

[Architecture Project Charter \(pdf\)](#)

Architecture Resources

Architecture Resources will include various documents and deliverables that relate to the overall SDC Consolidation Architecture effort.

[Architecture RFP Guidelines for Customers \(pdf\)](#)
[Initial Strategies and Action Plan \(pdf\)](#)
[Governing Principles \(pdf\)](#)
[SDC Tier1 Standards \(doc\)](#)
[Consolidation Architecture Migration Strategy for Distributed Systems \(pdf\)](#)

Architecture Forum Resources

Upcoming Meetings

Security Architecture Forum - New Date
October 25, 2007, 9 a.m. - 11 a.m.
SDC Room 104


Previous Meeting Notes and Handouts (most recent first)

- [Secure NW Arch. Forum Notes and Handouts – August 28, 2007 \(pdf\)](#)
- [Server Arch. Forum Notes and Handouts – August 14, 2007 \(pdf\)](#)
- [Storage Architecture Technical Forum Info Packet \(pdf\)](#)

Architecture Team Communications

Check back for the latest news.

[Text Only](#) | [State Directories](#) | [Agencies A to Z](#) | [Site Map](#) | [About Oregon.gov](#) | [Oregon.gov](#)
[File Formats](#) | [Oregon Administrative Rules](#) | [Oregon Revised Statutes](#) | [Privacy Policy](#) | [Web Site Feedback](#)



Adobe Reader is required to view PDF files. Click the "Get Adobe Reader" image to get a free download of the reader from Adobe.

5. CA Migration Strategy for Distributed Systems – Handout

Consolidation Architecture Migration Strategy for Distributed Systems

One key goal of the SDC is to provide good stewardship of the state’s computing resources by fully utilizing all hardware & consolidating to reduce cost. The new standard architecture for Distributed Systems is being implemented, so it is time to plan the consolidation of existing server workload & requests for new capacity into the new standard environment.

The migration of systems from older equipment to the new environment will take place in phases. The following chart shows the proposed phases & what needs to be in place before each phase can start.

Phase	Description	Dependencies	Time Frame for Roll Out
1	Pilot phase includes: <ul style="list-style-type: none"> • Creation of test/dev environment (14 blades; 60 virtual; 3 standalone) • OSP blade & virtual test in test/dev environment • Servers used for SDC internal management tools (~14 servers today) • Servers at high risk of failure (~40 servers have been identified) 	<ul style="list-style-type: none"> • Shared server environment set up & tested • Environment documented • Monitoring in place & operations trained • Metrics defined 	10/3/2007 – 11/15/2007
2	Forestry & Housing servers in test/dev/production environments (including all Phase 1 dependencies)	For each customer agency being migrated: <ul style="list-style-type: none"> • Develop roll out plan including communication & change management requirements • Complete capacity analysis of existing hardware & software usage & licensing • Hierarchical Storage Management (HSM) & Tivoli Storage Manager (TSM) are implemented & ready to manage customer storage & backup/recovery • Intrusion detection monitoring & Network Access Control in place • Virtualized partition allocations can be captured for billing • Capacity & performance tracking & reporting is operational 	11/15/2007 – 01/15/2008
3	Citrix Farm build out (14 blades & 180 virtual servers to start)	<ul style="list-style-type: none"> • Project readiness & Phase 1 dependencies 	1/2/2008 – 2/29/2008
4	Low risk candidates for migration	<ul style="list-style-type: none"> • Implementation of Tivoli Application Dependence Discovery manager (TADDM) • Phase 2 dependencies 	2/1/2008 – 5/31/2008
5	Remaining Customers <ul style="list-style-type: none"> • Customers volunteering to migrate • All remaining systems in the old environment 	<ul style="list-style-type: none"> • Phase 2 dependencies 	TBD

Consolidation Architecture Migration Strategy for Distributed Systems

Concurrently with migration of the existing environment, requests for new distributed systems processing capacity will be assessed for placement in the new standard environment. When a Support Request is received by the SDC Distributed Systems team, it is reviewed against a set of criteria to determine which platform it will reside on. The following platforms are available (in preferred order):

1. Virtual server environment

The Virtual Server environment is preferred because it represents the most efficient use of computing resources. A physical server is logically separated into many virtual servers, each running its own operating system and logically separate from the other environments. Virtual servers are highly redundant and standardized to provide the highest available uptime.

2. Blade server environment

Blade servers are independent physical servers housed in an environment (a Bladecenter) to provide optimum manageability and redundancy. Blade servers are used when requirements dictate that a virtual server environment can not be used.

3. Stand-alone server environment

A stand-alone server environment will only be considered when neither a virtual server nor blade server environment can be utilized.