



ESPDS Scalable and Secure Infrastructure

Ensuring the NOAA/NESDIS Environmental Satellite Processing and
Distribution Capabilities Meet the Growing User and Data Demands of Today
and Tomorrow

Rich Baker
Solers, Inc.

ESPDS Development Chief Architect
2013 AMS Annual Meeting

What is ESPDS?

- **ESPDS: Environmental Satellite Processing and Distribution System**
 - Developed by the NESDIS Office of Systems Development (OSD), with Solers (“Team Solers”) as the development contractor
 - Will be operated by the NESDIS Office of Satellite and Product Operations (OSPO)
- **Modernizes the NESDIS Environmental Satellite Processing Center (ESPC)**
 - Single enterprise solution that meets the needs of existing (legacy), Suomi NPP, JPSS, and GOES-R, *with scalability to meet future environmental satellite needs*
 - *No more stovepipes!*
 - Includes modernization of the Ingest, Product Generation (PG), Product Distribution (PD), and Infrastructure segments of the ESPC
 - Provides environmental satellite data and services to a growing user community including:
 - NOAA Line Offices (NWS, NMFS, NOS, NIC, NESDIS, etc.)
 - DoD (AFWA, NAVO, etc.)
 - Other U.S. and international users (government agencies, universities, foreign partners, etc.)
- **Will be implemented at the primary and backup ESPC sites:**
 - Primary ESPC site is the NOAA Satellite Operations Facility (NSOF) in Suitland, MD
 - Future ESPC backup site is the Consolidated Back-Up (CBU) facility in Fairmont, WV
- **Provides a *scalable and secure infrastructure* as a foundational building block upon which all other system functions reside**

Traits of a Scalable Infrastructure

- **No Single Point of Failure**
 - Redundancy and fault tolerance as key design tenants throughout
- **Line Replaceable Units**
 - Can upgrade or replace existing hardware and software components without impacting operational availability
- **Business Process Flexibility and Extensibility**
 - Can change existing business processes within the system, and integrate new business processes into the system, without impacting operational availability
- **Horizontal Scalability**
 - Can add additional hardware resources (computing, network, storage) and software business processing instances without impacting operational availability

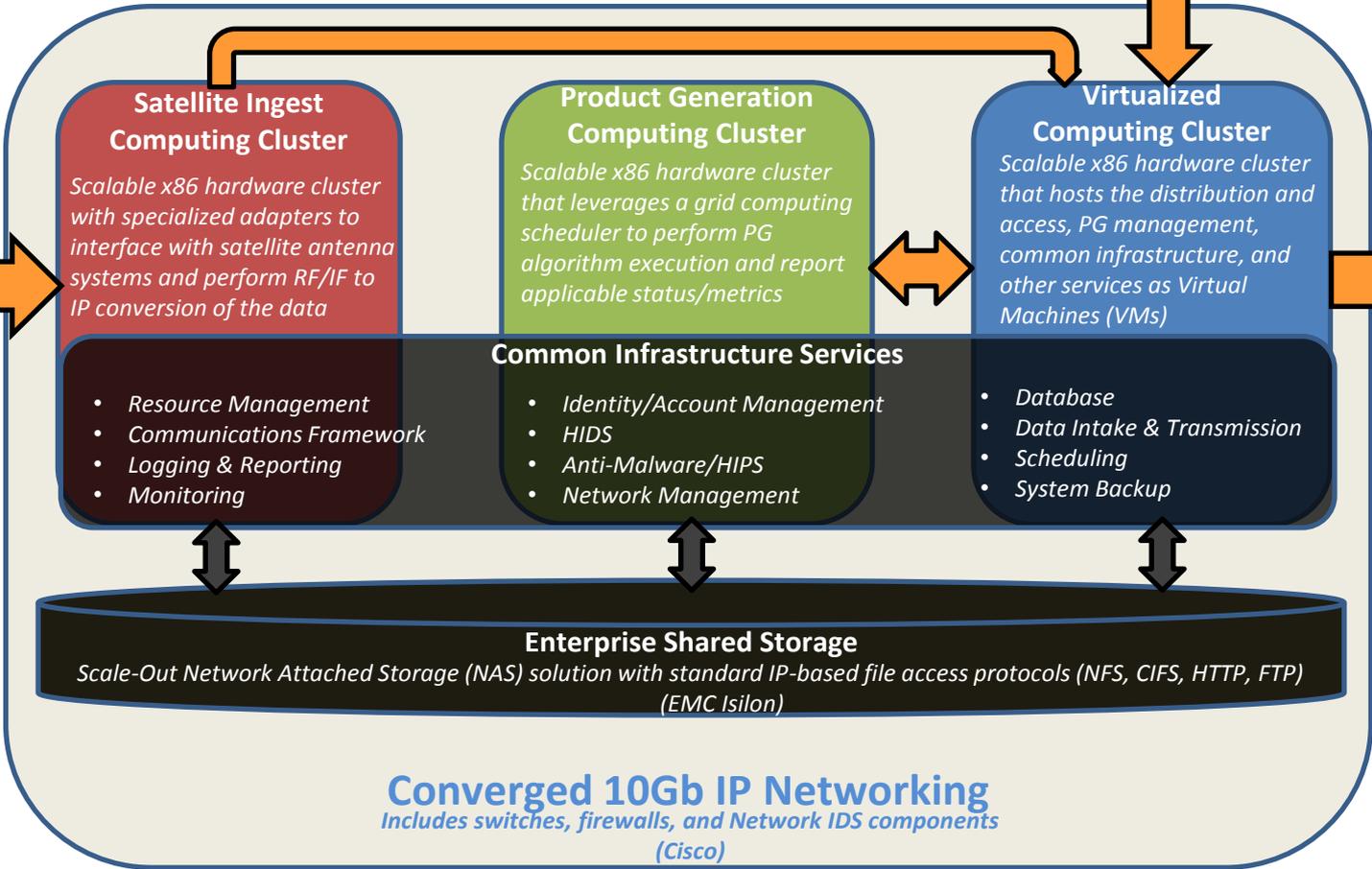
Traits of a Secure Infrastructure

- **Complies with applicable IT security policies, procedures, and controls:**
 - NIST SP 800-53
 - DOC/NOAA IT Security Handbook
 - Center for Internet Security (CIS) Benchmarks
 - DISA STIG
 - Etc.
- **Provides a “defense-in-depth” foundation for securing the system that includes:**
 - Network security
 - Centralized identity/account management, authentication, and authorization
 - Host-based intrusion detection and prevention
 - Anti-malware
 - Integrated monitoring, logging, and reporting (Security Incident and Event Management [SIEM])

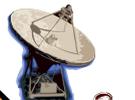
ESPDS Scalable and Secure Infrastructure



- *Suomi NPP and JPSS (via IDPS)*
- *GOES-R GS PD*
- *Non-NOAA Satellites (MSG, MTSAT, INSAT)*
- *Ancillary Data Providers*



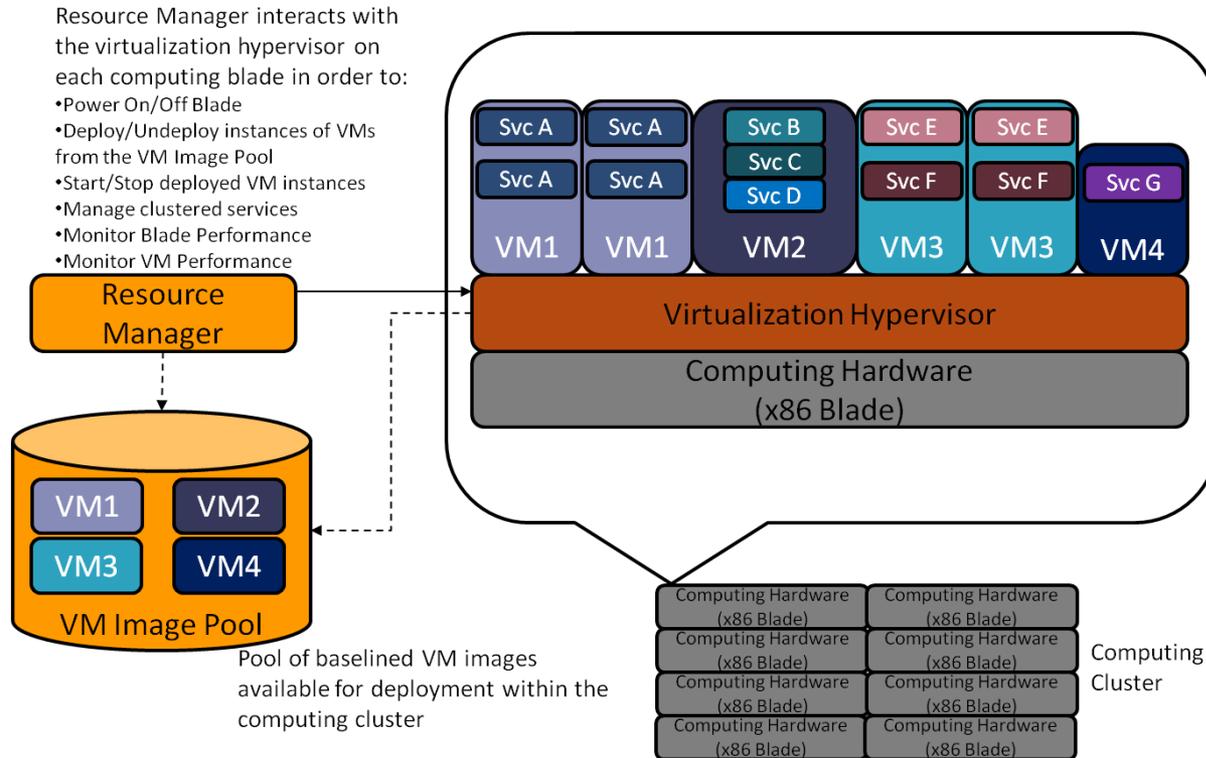
- *Legacy GOES*
- *Legacy POES*
- *Future Missions*



- *NOAA Line Offices*
- *DoD*
- *CLASS*
- *Other U.S. and International Users*
- *Ancillary Data Users (PG Systems)*

- **The following slides provide an overview of the Common Infrastructure Services depicted in the previous diagram**
 - Resource Management
 - Communications Framework
 - Logging & Reporting
 - Monitoring
 - Identity/Account Management
 - HIDS
 - Anti-Malware/HIPS
 - Network Management
 - Database
 - Data Intake & Transmission
 - Scheduling
 - System Backup

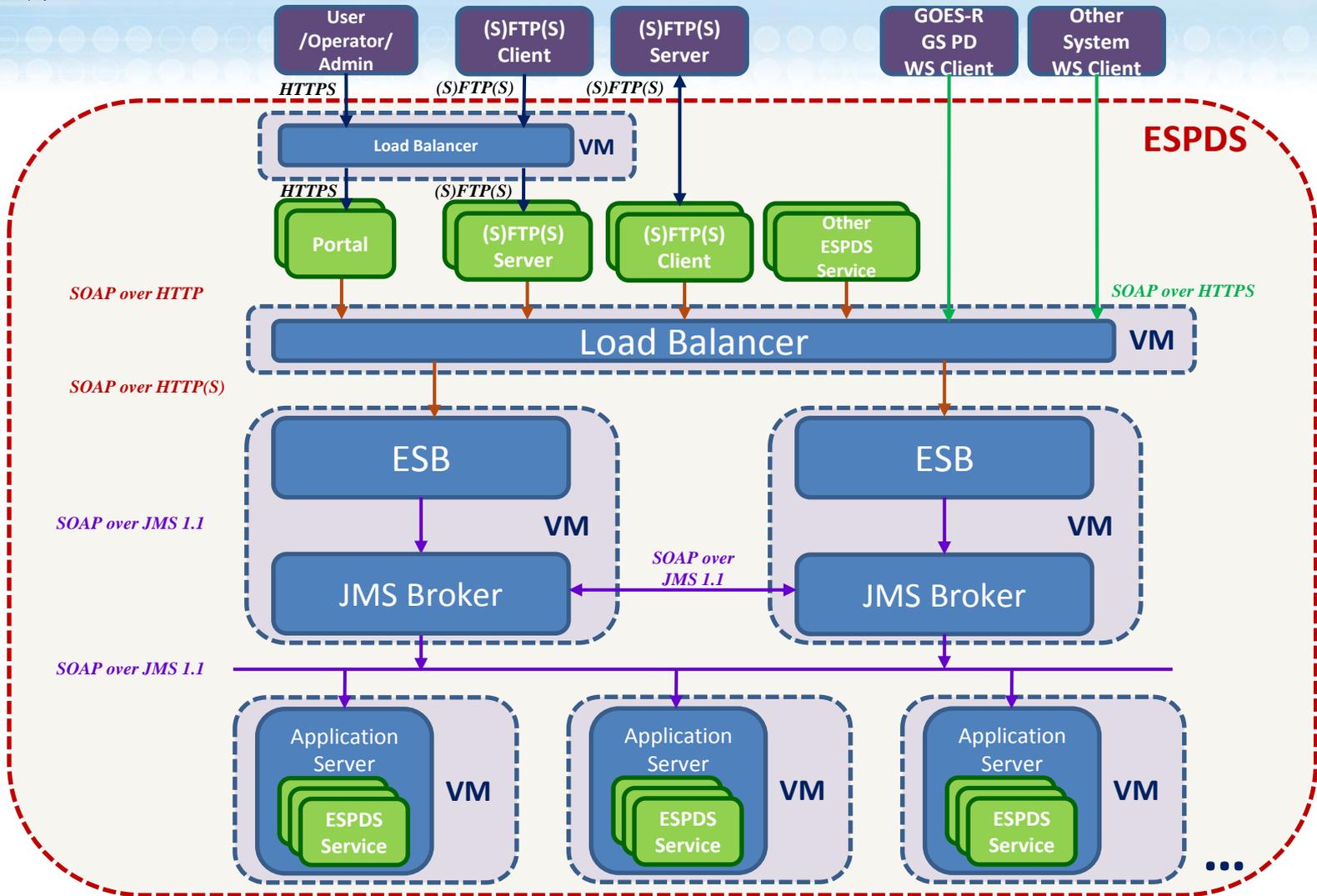
Resource Management



● Technologies Used

- VMware vSphere/ESXi, vCenter, and Orchestrator

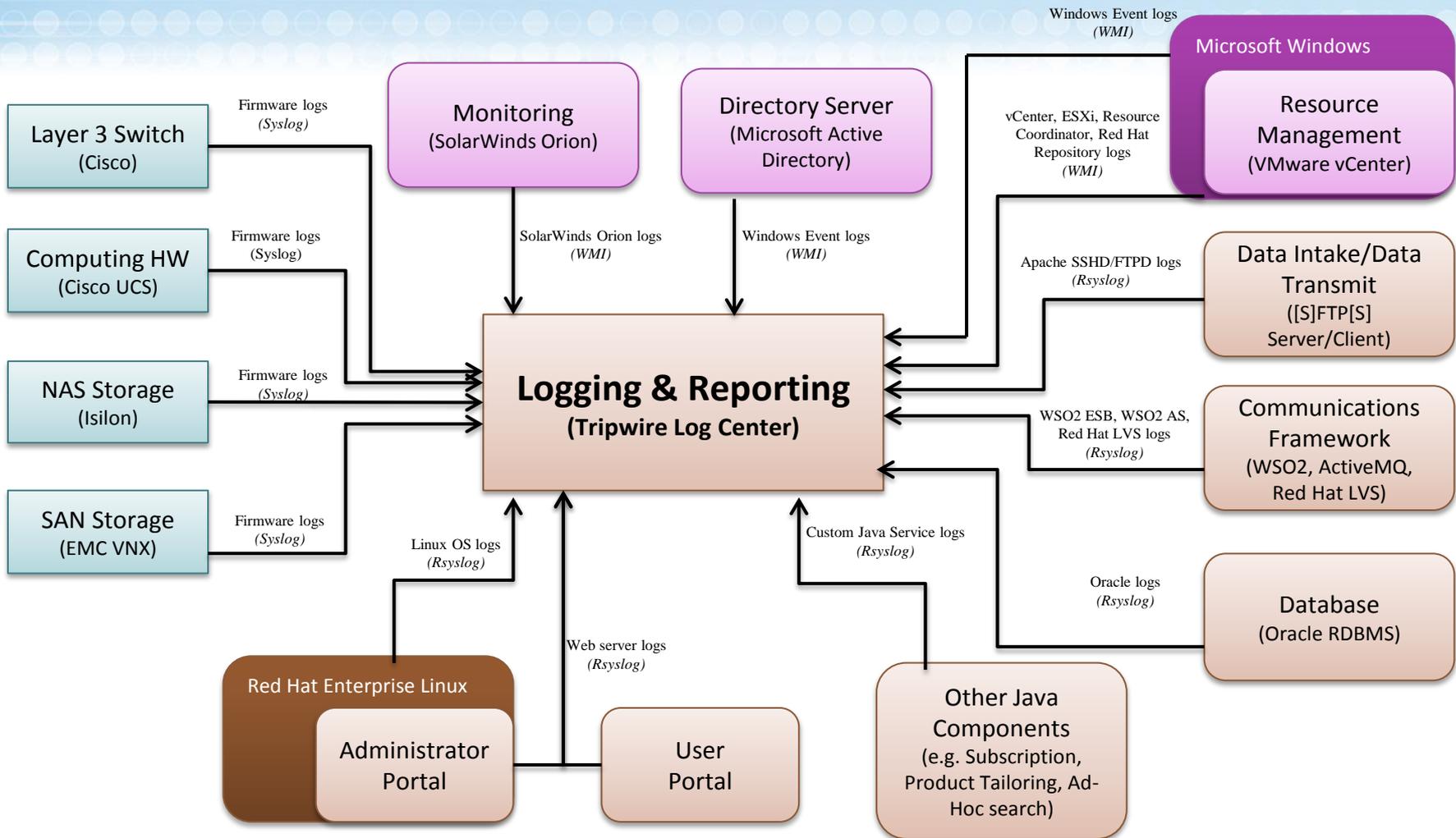
Communications Framework



Technologies Used

- WSO2 ESB and Application Server
- Apache ActiveMQ Java Message Service (JMS) Broker
- Red Hat Linux Virtual Server (LVS) Load Balancer

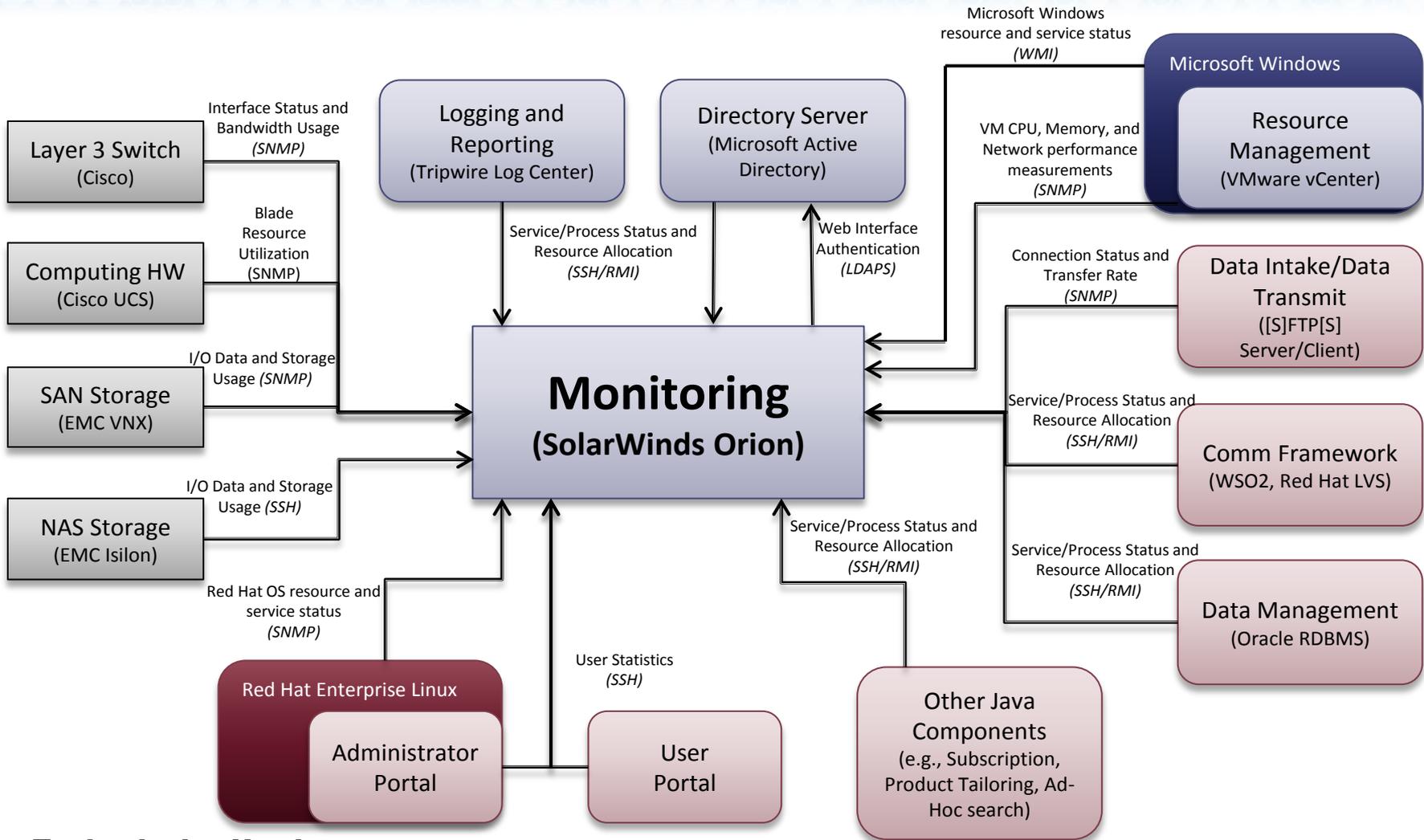
Logging & Reporting



Technologies Used

- Tripwire Log Center
- Rsyslog (Linux-based syslog client)
- Windows Management Interface (WMI)

Monitoring



● **Technologies Used**

- SolarWinds Orion Network Performance Monitor (NPM) and Application Performance Monitor (APM)
- Red Hat Simple Network Management Protocol (SNMP) Agent and Secure Shell (SSH) Server
- Windows Management Interface (WMI)

- **Centralized identity and account management solution**
- **Manages human user accounts (internal and external users, operators, administrators)**
- **Manages machine and operating system accounts**
- **Provides Kerberos and web services-based authentication and authorization services**
- **Compatible with NOAA/NESDIS HSPD-12 solution (DoD CAC PIV token, X509 PKI certificates)**
- **Technologies Used**
 - Microsoft Active Directory
 - Centrify
 - ForgeRock OpenAM

- **Centralized Host-based Intrusion Detection System (HIDS) solution**
- **Ensures integrity of critical system and configuration files across the infrastructure, including:**
 - Computing device firmware
 - Networking device firmware
 - Storage device firmware
 - Operating systems
 - Applications and services
- **Technologies Used**
 - Tripwire Enterprise

- **Provides virus scanning and Host-based Intrusion Prevention System (HIPS) capabilities across all machines and operating systems**
- **Centralized virus signature and HIPS policy management (automated deployments and updates)**
- **Technologies Used**
 - McAfee VirusScan Enterprise, HIPS, and ePolicy Orchestrator

- **Domain Name Service (DNS) Server**
- **Dynamic Host Configuration Protocol (DHCP) Server**
- **Network Time Protocol (NTP) Server**

- **Technologies Used**
 - Microsoft Windows DNS and Time Services (integrated with Active Directory)
 - Red Hat DHCP Server
 - Red Hat NTP Server

- **Highly Available Relational Database Solution**
 - Two Oracle Database 11gR2 Enterprise Edition Database Server instances
 - One primary instance providing client access
 - One identical standby instance to receive/apply redo operations from primary database
 - Oracle Data Guard configuration established between primary & standby database servers to maintain duplicate copy of operational database
 - Supports high database availability and fast start failover
- **Technologies Used**
 - Oracle Database 11gR2 Enterprise Edition with Data Guard
 - Hibernate (database client access)

- **FTP, FTPS, and SFTP client and server solutions**
- **Used to obtain product and ancillary data from providers (intake), and deliver product and ancillary data to consumers (transmission) via push or pull**
- **Technologies Used**
 - Apache FtpServer (FTP and FTPS Server)
 - Apache SSHD (SFTP Server)
 - Apache Commons Library (FTP, FTPS, and SFTP Client)

- **Schedules periodic operations to be performed within the infrastructure**
 - Product and ancillary data inventory cleanup (expired files)
 - Subscription-specific product and ancillary data acquisition
 - Extensible to accommodate future scheduling needs
- **Technologies Used**
 - Terracotta Quartz Scheduler

System Backup

- **Performs periodic backup of specific system data and files to support on-site archive and recovery**
- **Backups include:**
 - VM image files
 - Database contents
 - Log files
 - Configuration files
- **Technologies Used**
 - EMC NetWorker

ESPDS Scalable and Secure Infrastructure Benefits

- **To End Users**

- Ensures highly available and reliable access to human and machine interfaces that scales to accommodate the growing user and data demands
- Provides flexibility to quickly adapt to changes in end user requirements

- **To System Operators/Administrators**

- Easily scalable hardware and software
- Provides automated operations
- Compliant with IT security requirements for a High Impact system

- **To NOAA/NESDIS As A Whole**

- Scalable and secure foundation to support enterprise environmental satellite services across NOAA/NESDIS
- Removes mission-specific stovepiping
- Paving the path toward modernized data centers

Questions

