AppSense

AppSense Professional (ILT-AMS-100)

Design Document v1.0

Contents

Executive Summary

This instructor-led course provides the necessary foundation to deploy, administer and maintain user virtualization solutions using the AppSense Management Suite. Formal instructor-led training quickly familiarizes administrators with the features and functionality of the four components of the AppSense Management Suite; Application Manager, Environment Manager, Performance Manager and Management Center. This course prepares administrators to perform AppSense Management Suite installations and administrative tasks such as:

- Managing user behavior across multiple sites and platforms with policy and personalization
- Managing user rights for corporate application and network access control
- Managing entitlement of system resources based on user, group and application
- Performing basic troubleshooting

This is the introductory curriculum and will serve as the entry point for other AppSense technology courses. This course also contains the subject matter for the AppSense Certified Professional exam (APP-102).

Methodology

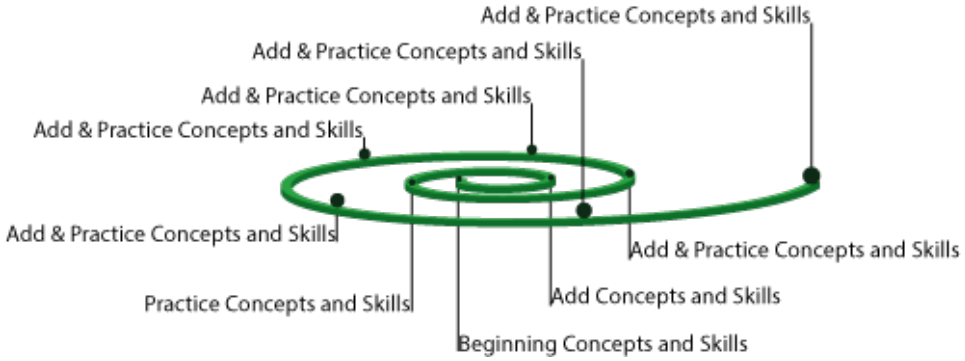
The ultimate goal of any training course is the acquisition of new skills. As such, the goal of the AppSense Professional Course is to acquire the skills necessary to administer and perform basic troubleshooting of the AppSense Management Suite.

Traditional Method

Traditional course design tends to adopt a linear approach to course delivery. Each topic is covered in one or two free standing modules, taking students through introductory to advanced concepts and tasks without revisiting concepts and tasks once they have been dealt with.

Spiral Method

Spiral course design is a technique where, first, the basic concepts and tasks are introduced without worrying about the details. Then, as learning and skill transfer progresses, more and more concepts and tasks are introduced while constantly revisiting and reemphasizing the concepts and skills covered thus far, helping to commit them into long-term memory. We are implementing the Spiral Method to better facilitate the retention of desired skills.



Scenario Based

Training with scenarios creates an atmosphere that is far more conducive to skills retention than relying heavily on lectures, videos and other widely used methods, and it provides measurable results. By combining scenarios with a spiral course design, students become more engaged. Students practice performing tasks in a context that relates those tasks back to real world situations.

Course Prerequisities

Learners should possess moderate to advanced Microsoft Windows administrative skills including:

- Performing administrative tasks associated with Windows Server 2008, Windows 7, Windows Server 2003, and Windows XP
- Familiarity with Active Directory including Group Policy Objects, sites, and group/user accounts, and familiarity with the fundamentals of Microsoft SQL Server administration.
- An understanding of Windows troubleshooting techniques and tools such as Task Manager, Performance Monitor, Event Viewer, etc.
- Ability to create and manage user accounts, profiles, security groups, and service accounts

Delivery Method

Instructor-led in either a physical or virtual classroom.

Project Deliverables

Deliverable	Audience	Medium
Course Description Document	Prospective Learners	PDF File
Student Guide	Learners	PDF File
Student Exercise Guide	Learners	PDF File
PowerPoint Slide-Decks	Instructors	PPT Files
Instructor Guide	Instructors	PDF File
Instructor Exercise Guide	Instructors	PDF File
Lab Setup Guide	Instructor/Lab Managers	PDF File

Course Length

5 days

Detailed Course Objectives Outline

Module 0: Introduction and Course Overview

Overview of the course learning objectives, course and classroom logistics, introductions and student expectations.

Course Scenario

To enhance the learner experience, the hands-on and discussion activities of this course will be designed around a course scenario meant to contextualize the learning objectives around real world situations. This module will describe and define the scenario used in the course.

The exact scenario is TBD and will be created and fully defined during the development phase of this project, but given the business requirements and criteria of the scenario, students will install, design, configure, deploy and troubleshoot a user virtualization solution using AppSense technologies.

An overview of the entire scenario will be discussed in this module. It will then be broken down and revisited in each subsequent module as appropriate – always tying back to the complete scenario through the end of the course.

Module 1: Introducing the AppSense User Virtualization Platform

Recognize the AppSense Management Suite

The purpose of this section is to identify the applications that make up the suite and provide a high level “C level” explanation of their roles/purpose.

- List the four components of the AppSense Management Suite
- Provide a “C” level explanation of the role of the Applications that make up the AppSense Management Suite

Describe the Challenges That Surround Managing the User Environment

Use this section to create a common understanding of what the user environment is and what specifically needs to be manipulated to manage that environment. Instructor materials will be designed to have the students provide the challenges of managing the user environment based on their experience with supporting information to provide discussion points for the main challenges we want to highlight.

- Describe the different types of Windows user profiles
- Identify the components of a Windows user profile
- Discuss the challenges of managing the components of a Windows user profile across multiple operating systems, devices, desktop delivery methods, and application delivery methods
- Describe the challenges of managing system resources for users
- Identify difficulties in locking down the user environment while allowing flexibility when required
- Describe the use of GPO’s and login scripts to manage the user’s environment
    - Both desktop and application settings

  - Controlling entitlements to execute processes and access internal network locations

Identify how the AppSense Management Suite Addresses the Challenges of Managing the User Environment

This section will show how AM, EM and PM help ease and can even remove the challenges that surround managing the user environment. This section should provide examples of where AM, EM and PM deal with the challenges raised in the previous section WITHOUT discussing how they work in detail. The real purpose of this section is to introduce key features and functionality of the products that will be expanded on in detail throughout the course. By tying the revelation of features and functionality to a discussion around solving common business challenges/problems, they will resonate with students much better than bulleted lists on a series of slides.

- Describe the benefits of the Management Center
- List the key features of the Management Center
- Using examples of solutions to previously stated challenges:
  - Describe the challenges that EM addresses
  - List the key features of EM
  - Define, compare, contrast Policy and Personalization
  - Recognize that EM is a solution to manage policy AND personalization
  - List reasons for using EM for application of Policy
  - List reasons for using EM for Personalization
- Using examples of solutions to previously stated challenges:
  - List the key features of AM
  - Describe the benefits of using AM
  - Explain how AM monitoring and auditing enforces software licensing in terminal server environments
  - Describe how AM replaces scripts and lists to control application access
- Using examples of solutions to previously stated challenges:
  - List and describe the key features and benefits of PM
  - List and describe the resources tuned by PM (disk CPU, memory)
  - Discuss some of the challenges addressed by PM
- For students: Identify one or two pain points in your current environment you would like to see how EM, AM or PM could address

Module 2: Installing the AppSense Management Suite

Identify and Define Components and Their Role

This is a terminology and definition section. We'll recognize that each application has a console, agent and policy configuration file, and we'll define their role within each application.

- Identify the main components of the AppSense Management Center
  - Recognize the elements of the three tier architecture
  - State the role of the management server

  - State the role of the database
  - State the role of the CCA
  - State the role of the management console
  - Define endpoints
  - Identify the requirements and role of IIS and BITS
  - Identify the role of the Server Configuration Utility (SCU)
- Identify the common elements of AM, EM and PM
  - Recognize that all three applications have a console, agent and configuration file
  - In general terms, discuss the purpose and function of the applications' consoles, agents and configuration files
- State the role of the personalization server
  - Identify the role of the personalization server database
  - Identify the requirements and role of IIS
  - Identify the role of the Server Configuration Utility (SCU)
  - State the role of the database

Lab

Locate the Pre-requisites for an Enterprise Installation

- Using the product documentation and www.myappsense.com:
  - Locate the system requirements and prerequisites for each of the servers
  - Locate the system requirements and prerequisites for each of the agents
  - Locate the system requirements and prerequisites for each of the consoles
  - List the required accounts for connecting to the database

Perform and Verify an Enterprise Installation

- Perform an enterprise installation of the AppSense Management Suite on AppSense-DC
- Use the Server Configuration Utility (SCU) to setup, configure and maintain the servers
  - Use the management server SCU to configure the server, connect to a MS SQL database and create the data tables
  - Use the personalization server SCU to configure the server, connect to a MS SQL database and create the data tables
  - Identify and repair any variances using the SCU
  - Use the SCU to verify that prerequisites, database, web site and services for each of the servers are operating error free
  - List the configurable IIS, DB, accounts, and support options available in the MC SCU

Module 3: Package Deployment

Diagram the Infrastructure

This section will provide an overview of how the components of each application communicate and work with each other. It will also provide an overview of the workflow of creating policy configurations and deploying them to endpoints via the management center.

- Diagram the Management Center Infrastructure
    - Define Deployment Groups
    - Describe what AppSense means by the term package
    - Identify the communication sequence and protocols between the management console, management server, database, and CCA on the endpoints
- Diagram the Environment Manager Infrastructure
    - Identify the communication sequence and protocols between the EM console, the management server, and the CCA and EM Agent on the endpoints with regards to policy
    - Identify the communication sequence and protocols between the EM console, the personalization server, database, and EM Agent on the endpoints with regards to personalization
- Diagram the Application Manager Infrastructure
    - Identify the communication sequence and protocols between the AM console, the management server, and the CCA and AM agent on the endpoints
- Diagram the Performance Manager Infrastructure
    - Identify the communication sequence and protocols between the PM console, the management server, and the CCA and PM agent on the endpoints

Describe how deployment groups are used to manage endpoints

- List and define the purpose of the default deployment group
- Describe the methods of assigning endpoints to deployment groups
- Recognize inheritance as it applies to configurations, deployment creds, failover servers, etc.
- Explain the best practice of using deployment groups
- Describe CCA communication with management server(s)
- Recall that the CCA must be deployed on all managed endpoints
- Describe scheduling of agents and configuration installs
- Describe the purpose and requirements of, the deployment credentials for the CCA

Describe how packages are managed and deployed

- Explain how version numbers are used for version control of packages
- Use MC to view packages, versions, and availability in a deployment group
- Recall that packages and perquisites may be manually added or deleted from the MC
- Recall that installation schedules should be considered when installing agents
- Recall that unassigned packages are removed at the next CCA polling time

- Recall that locked configurations may be unlocked with changes saved or not saved (changes lost)
- Compare and contrast product configuration and storage in the MC
- Recall that agents can be deployed by any system that supports the MSI format
- Describe why an administrator might export configurations in MSI format

Labs

- Deploy CCA
    - Set the CCA Credentials and deploy the CCA from the Management Server
    - Install the CCA manually from the Management Center download page
    - Check the CCA installation log to verify it successfully installed
- Create a Deployment Group
    - Set membership rules for the deployment group and automatically add computers by discovering them
    - Manually add a computer to the deployment group
    - Set the installation schedule
        - Allow user postponement for agent installs
        - Set the retry interval
    - Set the polling periods
- Deploy and install application agents to the endpoints
- Create blank policies from the application consoles
    - Save blank EM Policy to AMC
    - Save blank AM Policy to AMC
    - Save blank PM Policy to AMC
- Assign the application policies to the deployment group
- Verify successful installation of agents and policies from the AMC and from the endpoints

Module 4: Management – Tier 1

The overall structure of this class is to gradually introduce concepts, features and functionality. So don't get hung up on the name "Tier 1". From a management/administrative point of view, we're starting tier 1 now and will move students through multiple tiers of complexity as we introduce new concepts, features and functionality while reviewing and re-enforcing those already covered.

AppSense Management Center

Configure security to control access to and of the management server

- Recall that Role Based Security is used to define user access to MC objects
- List and describe the 4 default MC security roles

Utilize alerts and event auditing for monitoring and troubleshooting

At this stage, per scenario, we will be turning on events for successes because we're testing our initial policies. In Tier 2, we'll run reports to see success/failure of our policies and then turn off success events and set the events that would normally be captured in production.

- List the feature functionality available from the MC Alerts tab
- Define Alerts in the context of the AppSense management server
- List the configuration options for management server alerts
- List the options for configuring alert notification
- Recall that alerts are configurable on a deployment group basis
- List the tasks that may be performed from the MC Reports tab
- Configure event auditing
- Recall which event ID's are useful for troubleshooting

Recall the effect of expired licenses

- Locate and list the functionality of the Enterprise Licensing screen in MC
- Describe AppSense License
- Recognize Licensing as a prime source of support calls
- Use MC to verify AppSense licenses

Labs

- From the Management Console, enable enterprise event auditing for AM, EM and PM events
- Configure a user account to have view only access to a specified object in the management server
- Create a custom object role and assign it to a user
- Create a customer server role and assign it to a user
- Configure an alert rule and SMTP notification
- Verify licensing

Application Manager

Trusted Ownership

- Describe the functionality of Trusted Ownership
- Identify how trusted ownership is enabled by default as the "out of the box" configuration

Labs

- Identify how trusted ownership is enabled in the default policy configuration
- Test trusted ownership

Describe the General Functionality of Application Manager

- Describe the 3 pillars of AM: ANAC, Application Access Control, URM
- Describe how AM can supplement, but not replace AV
- Describe the concepts of user rights, group membership, and privileges

- Recognize the AM Rules section as the location for further configs beyond the out of the box config
- Define the role of rule management groups, users, devices, custom, scripted, process
- Explain the role and function of the AM agent and configuration.aamp

Discuss Application Access Control

- Compare and contrast application execution with and without Application Manager
- Define unauthorized executable
- Describe the functionality of digital signatures
- Describe the functionality of trusted vendor
- Compare and contrast digital signatures, trusted vendor, and trusted ownership
- List and define rule security levels; restricted, self-authorizing, audit only, and unrestricted
- Explain AM rule precedence

Discuss Network Access Control

- Compare and contrast ANAC with firewalls (outgoing only) and web filtering
- Summarize the features of ANAC

Labs

- Create a digital signature group for an application that is also a trusted application by scanning running processes
- Update the signature group (we'll need to make it necessary some how)
- Demonstrate that a digital signature takes precedence over trusted ownership
    - Create a group rule and make the previously created signature group a prohibited item
    - Test that a user from the group cannot launch the application while a user who is not from the group can still launch it
- Demonstrate that the more narrowly focused rule wins
    - Add a folder to the prohibited items for the previously created group rule
    - Test that a user in the group cannot launch an executable in that folder
    - Create a user rule for the user and add the specific exe file to the Accessible Items for the user
    - Test that the user can now launch the executable while another user from the group still cannot
- Demonstrate Application Network Access Control
    - Add a network connection item to the group rule
    - Configure it to dis-allow RDP access to a training lab server
    - Create a device rule that allows RDP access to the same training lab server from a specific desktop
    - Test to see if a user from the denied group can RDP to the training server
- Enable Rights Discovery Mode and configure it to start collecting data (we will let it run and circle back to it during the next tier

Environment Manager

Policy

- Define Triggers
- Identify Computer and User triggers
- Discuss the purpose and functionality of nodes
- Discuss the purpose and functionality of conditions
- Discuss the purpose and functionality of actions
- Describe the multi-threaded nature of EM Policy
- Given a policy, identify the order in which the nodes, conditions and actions will run
- Explain the role and function of the EM agent and configuration.aemp with regards to policy

Personalization

- Discuss how personalization is enabled
- Describe the purpose of the virtual cache and what goes in it
- Describe the pros and cons of creating application groups
- Discuss the advantages and disadvantages of application groups
- Describe how personalization group membership works
- Explain the significance of the order personalization groups are listed in
- Describe how personalization is applied on the endpoints (TBD based on EM 8.4 functionality):
    - Identify the EM Services and their function with regards to policy
    - Describe the purpose and functionality of EMLoader.dll and PVC.dll
    - Locate and describe the contents of the personalization cache
    - Compare and contrast virtual file system and physical file system
    - Compare and contrast virtual registry and physical registry
    - Describe what happens when a user logs on
    - Describe what happens when an application is launched
    - Describe what happens when and application is closed
    - Describe what happens when a user logs off
    - Describe the purpose of the profileconfig.xml file

Labs

- Given a policy, identify the order in which the nodes, conditions and actions will run
- Create a base/generic policy for testing
- Create basic logon conditions and actions based on a scenario
- Deploy and test the policy
- Enable personalization in the policy and follow the wizard
    - Connect to the personalization server
    - Create a single personalization group
    - Create a single application group assigned to the personalization group
- Test personalization of the applications in the application group with the men in the group

Performance Manager

Discuss Performance Manager Functionality

- Describe how performance manager deals with perceived performance
- State the role and function of the PM Agent and the configuration.apmp file
- Explain how to manage CPU entitlements with performance manager
- Discuss the purpose and functionality of share factors
- Explain how to manage memory entitlements
- Define share factors and smart scheduling
- Discuss the attributes of the out of the box configuration
- Explain thread throttling
- Define and describe Application groups and their types
- List the attributes used to configure application groups
- Describe the relationship between application groups and resources
- Describe the relationship between Application Groups and User Groups and individual users
- Explain the order in which groups are evaluated and matched
- Describe how to launch PM console and identify the console areas
- Explain default PM configuration and benefits
- Recognize that PM allows resource management based on application and session state

Labs

- Test the default policy configuration
- Configure an application group
    - Change resource allocation when different users launch the applications
    - Change resource allocation based on application state
- Modify the thread throttling settings
- Deploy and test the policy

Module 5: Management – Tier 2

AppSense Management Center

Reporting

- Utilize reporting for monitoring and troubleshooting
- Using the report templates, verify which parts of the policies are working correctly and which parts are not working correctly

Describe how packages are managed and deployed

- Explain how version numbers are used for version control of packages
- Use MC to view packages, versions, and availability in a deployment group
- Recall that packages and perquisites may be manually added or deleted from the MC
- Recall that installation schedules should be considered when installing agents

- Recall that unassigned packages are removed at the next CCA polling time
- Recall that locked configurations may be unlocked with changes saved or not saved (changes lost)
- Compare and contrast product configuration and storage in the MC

Labs

- Using the report templates, verify which parts of the policies deployed in the previous sections are working correctly and which parts are not working correctly
- Add a package to the Management Server database using the Management Center's Console
- Delete packages from the Management Server database
- Unlock a package that was locked by a different user

Application Manager

Describe User Rights Management

- Describe the problem that user rights elevation solves
- Describe the problem that user rights removal solves
- Recognize the limitation of Windows session security (all or nothing) URM
- Recognize that privileges can be enabled, disabled, removed via AM policy with URM
- Describe Windows security tokens
- Use process explorer to view security tokens for processes to determine if URM rules have been applied
- Recall that URM manipulates Windows security tokens
- Describe the process of implementing URM
- Describe user rights policies

Discuss Active-X Controls

- Compare and contrast Active-X Controls and Web Downloads
- Describe the process of implementing ActiveX
- Define Active-X control installation

Discuss Web Downloads

- Describe the process of implementing Web Downloads
- Describe what web installation is
- Describe the problem that web installation solves
- Recall that web installation allows installation as a trusted user
- Define Web Downloads

Explain Snippets

- Describe the use of configuration snippets
- Download and install configuration snippets
- Locate configuration snippets on the local machine

- Describe the implementation of configuration snippets
- Create a user defined snippet
- Describe how to create a user defined snippet

Rights Discovery Mode

- Describe the purpose and functionality of Rights Discovery
- Explain the function of the Analysis Service
- Configure Rights Discovery
- Analyze the results
    - Create a configuration file for distribution to multiple endpoints
    - Generate reports

Labs

- Configure Active-X rules using the AM Console
- Configure and test Web Downloads rules using the AM Console
- Configure URM rules using the AM Console
- Configure AM using snippets
- Configure Rights Discovery
- Create a configuration file and distribute it to multiple endpoints
- Generate reports and analyze the results

Environment Manager

Policy & Personalization

- Discuss how EM policy and personalization can be used to replace or, at least, simplify complicated GPOs and logon scripts
- Note that EM policy and personalization can be used to replace pre-launch scripts for XenApp Published Applications and App-V – this was a comment added by James Simpson to the previous bullet … maybe wait and include this when we talk about App-V???

Policy

- List and describe condition matching logic
- Describe the behavior of the "run once" and "Count" values
- Describe the tabs in the Action dialog box
- Recognize that all Actions have a common General tab
- Recognize that all Actions have a context specific tabs
- Describe the use of the Run As library
- Recall that all actions have computer or user contexts
- Describe the function of the quick setup wizard
- Recognize that actions in the quick setup wizard are converted to native EM actions
- Recognize that some functions presented in the quick setup wizard may not apply in the context in which it is used (computer or user nodes)

- Discuss the purpose and functionality of the EM Browser Interface

Personalization

- Identify the options in the personalization global settings dialog
- Describe the role of default locations to monitor in the context of personalization settings
- Recognize that registry keys and folders to be monitored may be specified at the global level
- List and describe the fields available in the Application Properties dialog
- Recognize that registry keys and folder monitoring may be defined on a per-application basis
- Recognize that the default applications list is read only
- Define the contents and role of the Default applications list, what is in this list, and why
- Describe the relationship between the default application list and the default blacklist
- Describe the role of the User Applications list
- Compare and contrast Default Applications and User Applications
- Recognize that applications may be added to the user list via the personalization tree
- Explain when and how personalization settings are created
- Recognize that settings defined on an application group will override any settings on individual apps in the group (for consistency)
- Explain the role of application groups, and what problem they solve
- Recognize that child processes called by personalized apps are personalized
- Recognize the implications of blacklisted child processes called by whitelisted apps
- Recognize that registry keys and folders to be monitored may be specified at the application group level
- Describe the load and save behavior of application groups vs. single applications
- Describe how a user's personalization settings are controlled and stored in the database according to the personalization group they belong to
- Recognize that a user will only receive the settings from one personalization group
- Discuss how membership in a personalization group is decided
    - Personalization group settings may be setup so that user belongs to multiple personalization groups (i.e. match computer condition for group1 while matching user group condition for group2), however user will "belong" to the first group with which they match the membership rules for that session
- Describe the purpose and functionality of the white list and the black list
- Recognize that blacklists beats whitelists
- Define the available selections on the personalization group properties tab

Describe the functionality of Desktop Settings and Session Data

- Describe the contents of the desktop settings dialog
- Compare and contrast desktop settings and session data
- Explain the inheritance model for desktop settings and session data and how each personalization group can have customized desktop settings and session data

- Recognize that desktop settings are common to all users and may be disabled for specific groups
- Recognize that desktop settings manipulate the HKCU registry
- Explain what the Manage Desktop Settings option does
- Explain how session data settings are applied (to real reg and set as global exclusions)
- Describe the contents of the session data dialog
- Recognize that registry settings may be added/removed from the session data
- Recognize that session data are common to all users and may be disabled for specific groups
- Recognize that session data manipulate the HKCU registry
- Explain what the Enable Session Data option does
- Discuss how session data, desktop settings and personalization interact with each other

Labs

- Create personalization groups
- Configure applications for personalization
- Test personalization on multiple endpoints
- Configure application groups for personalization and observe how applications within the groups are personalized on endpoints
- Enable and disable desktop settings
- Add items to session data
- Set global includes and excludes
- Enable offline mode based on set of conditions

Module 6: Management – Tier 3

Application Manager

- Recall that there is a default template available
- Recognize that the default template is available to extend the oobe
- Recognize that configuration beyond the ootb config is recommended
- Recognize that content may be allowed only when called from a specific parent app
- Define the role of rule management groups, users, devices, custom, scripted, process
- Describe implementing scripted rules
- Describe the use of Application Termination
- List the triggers for Application Termination
- List the options for Application Termination
- Describe the purpose and function of Auditing

Labs

- Configure and test auditing on a group rule
- Given a set of business requirements and objectives, create an AM policy

- For this lab, we will give the students a scenario with a set of goals and objectives that can be solved with Application Manager. We will not tell them what to create or how to create it … they'll have to put what they've learned so far to practice.
- Have them test their policy to make sure it works
- Pick one or two students to walk the class through their policy and explain why they did it that way. Solicit comments from other students about how what they did compares.

Environment Manager

Policy

Discuss the purpose and functionality of Lockdown

- Describe what lockdown does
- List the Windows controls to which lockdown applies
- Explain why lockdown cannot be used to hide controls when MSAA is used
- Explain why MSAA cannot be enabled and allow bypass of lockdown
- Describe what the general lockdown wizard does and how to use it
- Describe the general lockdown wizard advanced settings window
- Describe the usage of the Keyboard Wizard in locking down machines
- Describe what the office wizard does
- list the office versions supported by the office wizard
- Recognize the requirement of having the office version to be locked installed on the machine that is using the office lockdown wizard
- Describe how to select office features to lockdown when using the office wizard
- Describe when and how to use the blocked text library
- Describe the role of the blocked message library

Discuss the purpose and functionality of Self Heal

- Explain the purpose and functionality of Self Heal
- Recognize that the self healing action can have conditions applied
- Describe the self healing feature as it applies to a service, files, processes and the registry
- Recognize that self heal supports path, file name, and command line

Expanding on Actions

- Describe how action execution may be ordered, and the execution relationship between parent and child actions
- Describe the behavior of EM when actions fail
- Describe the behavior of EM when an action with "stop if fails" enabled fails
- Identify when to use custom actions
- Recognize valid custom action languages
- Identify success/failure return values in custom actions

- Recall that command line options, parameters, and working directory may be specified when using custom actions
- Recognize custom action timeouts will honor the timeout specified in the action

Expanding on Nodes

- List and describe the rules regarding timings and timeouts for nodes and triggers
- List and describe the contents of reusable nodes and conditions
- Locate library nodes in the EM console
- Describe how to reference library nodes
- Explain why to use reusable nodes and conditions
- Explain how the execution order of nodes takes advantage of multi-threading
- Explain when to use library nodes, reusable nodes, and reusable conditions
- Explain the execution rules of nodes within a node group
- Describe how to use node groups
- Explain when and why to use node groups

Labs

- Using the Management Center's download page, install the EM Console on AppSense-PC1 and AppSense-PC2
- Use the console on PC1 and PC2 to create lockdown actions for XP and Win7 respectively. Utilizing conditions to differentiate between them, create lockdown actions for the following:
    - Use Microsoft Office Lockdown to disable specified office features
    - Use the general lockdown wizard to disable specific menu items of a given application
    - Lockdown a user's ability to use keyboard commands
    - Lockdown a user's ability to enter specific text
- Configure a self-heal action on the hosts file
- Based on a set of criteria, create an if/else condition
- Create reusable nodes and conditions
- Given a series of scenarios, recognize when to use stop if fails
- Create a custom action
- Merge two policies together (we will work the scenario and lab so that at this point, they will have two policies they've been testing that they can now merge together)

Personalization

Configuration Assistant

- Describe the purpose and functionality of Configuration Assistant
- Explain what the Configuration Assistant tick box does (Passive database, pvc.dll)
- Describe when data is synced to the Passive database
- Navigate the user interface
- Analyze and interpret the data collected by Configuration Assistant

Labs

- Enable data collection and view data in Configuration Assistant
- Given a scenario and set of data, use Configuration Assistant to analyze the data and configure personalization
    - Based on config assistant output, configure includes and excludes for specific applications
    - Determine what should go into session data
    - Determine what should be captured in desktop settings
    - Determine what should go into global exclusions

Combined Policy and Personalization Lab

- Given a scenario, use policy and personalization to replace a set of GPO's and logon scripts

Module 7: Management - Tier 4

Environment Manager

Policy

Discuss the purpose and functionality of Hiving

We will be incorporating "the hiving template" into this section.

- Describe the purpose and functionality of Hiving.
- Explain how registry hiving can be used in place of personalization settings.
- Describe a situation where registry hiving can be used in conjunction with personalization settings.

Labs

- Given a scenario, use policy hiving in preference to personalization setting.
- Given a scenario , use policy hiving to complement personalization settings. (Nb need to be careful about this can see people getting touchy)

Personalization

Describe Personalization Sites

- Describe the requirements and configuration for deploying servers in multiple sites.
- Describe personalization server sites and their dependency of SQL replication
- Discuss the considerations for deploying multiple servers to multiple sites
- Describe site membership
- Discuss the considerations for deploying multiple servers to a single site
- Explain how network load balancers can be used to control the connections to multiple servers

Labs

- Install a second personalization server on AppSense-TS

- Use the personalization server SCU to configure the server and connect it to the personalization server database on AppSense-DC
- Export the settings from one server and import them to another server
- Add an additional server to the default site and configure endpoints accordingly
- Design a deployment of servers across multiple sites sufficient to meet the detailed business requirements

Create complex configurations

- Discuss how mandatory profiles can be used with personalization to replace roaming profiles
- Describe what the App-V Wizard does
- List the personalization items available in the App-V wizard
- Manage personalization settings of App-V delivered applications

Labs

- Construct a Hybrid user profile by creating a mandatory profile and personalizing using EM.
- Personalize App-V delivered applications

AppSense Management Center

Install additional servers

- Describe how to install a stand-a-lone server
- Use the SCU to connect to the existing database

Labs

- Install a second management server on AppSense-TS
- Use the management server SCU to configure the server and connect it to the management server database on AppSense-DC
- Given a scenario, design a deployment of servers across multiple sites sufficient to meet the detailed business requirements

Module 8: Maintenance and Troubleshooting

AppSense Management Centre

Recall the management center architecture and component communication

- Recall that the CCA installs a watchdog service
- Explain the role of the watchdog service
- Recall that the CCA does not have a configuration package (stored in registry)
- List and describe communication timeouts

Event Auditing

Utilize alerts, event auditing and reporting for monitoring and troubleshooting

- List the feature functionality available from the MC Alerts tab
- Define Alerts in the context of the AppSense management server
- List the configuration options for management server alerts
- List the options for configuring alert notification
- Recall that alerts are configurable on a deployment group basis
- List the tasks that may be performed from the MC Reports tab
- Configure event auditing
- Recall which event ID's are useful for troubleshooting

Labs

- Configure event Auditing
- Need list of events to audit for more common ones taken from the instructional part (practice what we preach)ie Do event audit for no licence etc?

Configure Diagnostics

- List the reasons for enabling Diagnostics as opposed to Auditing
- Configure Diagnostics
- List and explain the the diagnostic results shown in the console.

Lab

- Enable diagnostics from the server and request diagnostics from an endpoint
- Review the findings

Environment Manager

Personalization

Discuss the functionality of Archives and Rollback

- Recognize application rollback as a method to restore individual application settings
- Recognize that PS creates archives automatically on a per application/group basis
- Recall that PS archives are taken at 1AM each day (by default) only if application was accessed - based on usage count
- Recall that applications may be manually archived from the EM console
- Describe the user and administrator activities involved in rolling back application settings from an archive
- Manage archive retention using settings available in the Global Settings dialog
- Recognize that when an archive is created, a purge is automatically run as well, retaining the last 5 archives (by default)
- Describe the behavior and process of taking archives

- Set expiry date for PS data
- Manage archive data for deleted applications
- Manage retention of PS Archives in Global Settings

Lab

- Use the EM console to create an archive of the personalization settings for a given user.
- Roll back and test the application of rolled back settings for a specific application in a given user account.

Discuss Using the EM Browser Interface for Archive and Rollback

- Recall the role and function of the EM Browser Interface

Labs

- As a regular user, use the EM Browser Interface to:
    - Create a backup of an application's settings
    - Restore their backups – create, protect and delete backups
    - Delete an application's settings and return them to their default

Discuss Personalization Analysis

- List the features available from the Personalization Analysis dialog
- Explain what personalization analysis does and give examples of the types of data collected
- Recognize that using personalization analysis, files and registry settings may be manipulated
- Recognize that whitelist application usage can be analyzed and that analysis can be limited to a given date range by using personalization analysis for up to 6 months
- Recognize that personalization analysis can be used to display discovered applications, those applications may then be converted to personalized applications, and application versions may need to be edited
- Describe the "Automatically discover user applications" checkbox, when to use it, and what it records

Labs

- Use personalization analysis to edit a whitelisted application registry and observe the effects on an endpoint

Basic Troubleshooting Techniques for Personalization

- Recall EM Architecture
    - Recall the communication sequence and protocols between the EM console, the management server, and the CCA and EM Agent on the endpoints with regards to policy
    - Recall the communication sequence and protocols between the EM console, the personalization server, database, and EM Agent on the endpoints with regards to personalization
- Test end-to-end communications
- Use the SCU to identify problems

- Use Persinfo to identify problems

Labs

- Given a series of scenarios, use the various tools and techniques previously discussed to troubleshoot why a user is not able to personalize an application

Policy

Basic Troubleshooting Techniques for Policy

- Recall the structure of an EM policy
- Use the configuration profiler to validate a deployed configuration
- Use the EM Console to configure audit events to be sent to a syslog for monitoring and alerts

Labs

- Given a series of scenarios, use the various tools and techniques previously discussed to troubleshoot why a policy in not being applied to a user

SQL Maintenance

- Recognize things to be aware of on the SQL back end and what should be done to keep the database running, transaction logs from getting out of control, etc.

Labs

Need to get more info from Andrew Silva, Ian Bray and Travis McGee for this section

Application Manager

Basic Troubleshooting Techniques for AM

- Recall the structure of an AM policy
- Recall the purpose and functionality of:
    - Endpoint Analysis
    - Auditing
    - Configuration Profiler
    - Rules Analyzer
    - Rights Discovery
    - Archiving

Labs

- Given a series of scenarios, use the various tools and techniques previously discussed to troubleshoot why an AM policy is not being applied to a user

Performance Manager

Basic Troubleshooting Techniques for PM

- Recall the structure of a PM policy
- Use the configuration profiler to validate a deployed configuration

Labs

- Given a series of scenarios, use the various tools and techniques previously discussed to troubleshoot why an AM policy is not being applied to a user

Module 9: Upgrades

In this module, we'll first cover upgrading Environment Manager and Application Manager independently. Then, we'll cover upgrading the suite.

Environment Manager

Server

- Discuss the considerations for upgrading the Personalization Server
- List the steps to upgrade the server

Agent

- Discuss the considerations for upgrading the EM Agent
- List the steps to upgrade the agent

Config

- Discuss the considerations for upgrading the EM Policy
- List the steps to upgrade the policy

Labs

- Upgrade the personalization server, including any necessary prerequisites
- Using the SCU, update the database
- Import the new EM Agent into the Management Center and deploy it
- Upgrade the policy and deploy it

Application Manager

Agent

- Discuss the considerations for upgrading the AM Agent
- List the steps to upgrade the agent

Config

- Discuss the considerations for upgrading the AM Policy
- List the steps to upgrade the policy

Labs

- Import the new AM Agent into the Management Center and deploy it
- Upgrade the policy and deploy it

AppSense Management Suite

- Discuss the considerations for upgrading the suite

- List the steps to upgrade the suite

Labs

- Perform the necessary tasks to successfully upgrade the AppSense Management Suite

Hardware & Software Equipment Requirements

Overview

A pod for this course is defined as a set of Windows machines of various configurations in a single AD domain. These machines may be physical or virtual, however for ease of setup and manageability it is most likely that a virtual environment will be used. The contents of a course pod are outlined in the Detail section. A comprehensive Lab Setup Doc will be provided as part of the deliverables for this project. This Lab Setup Doc will detail configuration, shares, user accounts/groups, etc.

All machines require KVM access beyond RDP to the individual machines for power cycling and other out of band tasks.

Detail

The detailed hardware and software requirements are currently TBD and will be finalized during the development and testing phases of this project. Estimated requirements at this time are:

Machine Name	OS	HD	RAM
AppSense-DC	Windows Server 2008 (64-bit)	40 GB	2 GB
AppSense-TS	Windows Server 2008 (32-bit)	20 GB	2 GB
AppSense-PC1	Windows XP (32-bit)	20 GB	2 GB
AppSense-PC2	Windows 7 (64-bit)	20 GB	2 GB
AppSense-RS	Windows Server 2008 (64-bit)	40 GB	2 GB

Additional Software

All machines in the pod will have Microsoft Office 2010 installed and licensed. AppSense software will be made available uninstalled and unlicensed. Additionally, a directory of course-specific software as detailed in the Lab Setup Doc will be installed as per that document.

Project Timeline

Milestone	Date	Comments/Status
Analysis & Design phases start	3/19	
Analysis & Design phases complete	7/3	
Development phase starts	7/4	
Development phase complete		
Implementation phase start		
Implementation phase complete		
Go Live		

Project Team

Name	Role
Dmitry Shkliarevsky	Executive Sponsor
Raj Saklikar	Education Project Lead
Damian Entwistle	Education Developer
Keith Hart	Project Manager
List of SME's TBD	