ANGARA
Professional Assistance

ОТЧЕТ ПРОВЕДЕНИЯ SECURITY HEALTH CHECK

СИСТЕМА ВИРТУАЛИЗАЦИИ НА БАЗЕ VMWARE

Заказчик:
Дата проведения:

WWW.ANGARAPRO.RU

Оглавление

Цели услуги Security Health Check

1. Получение «вендоро-независимой» оценки реального состояния настроек безопасности и самозащиты критичной системы.
2. Выявление «дыр» в процессах эксплуатации и использования компонентов самозащиты системы и критичных данных, описание и экспертная оценка вероятности наступления последствий недостаточной настройки параметров самозащиты.
3. Оценка соответствия процессов защиты лучшим практикам, рекомендованным производителями.

Описание объекта обследования

1.1. Обследуемая система

В рамках работ по оценке состояния настроек безопасности и самозащиты производилось обследование Системы виртуализации Заказчика, построенной на базе продуктов компании VMware:

- VMware ESXi
- VMware vCenter

1.2. Цели и решаемые задачи системы

Система виртуализации развернута с целью запускать изолированные и безопасные виртуальные машины на одном физическом узле, выделяя ограниченное количества ресурсов для каждой из них. Тем самым аппаратные ресурсы физических серверов используются более рационально.

Система выполняет следующие задачи:

- Централизованное управление виртуальной инфраструктурой
- Разграничение ресурсов для виртуальных машин
- Разграничение доступа к виртуальным машинам

1.3. Текущая архитектура

Текущая архитектура обследованной системы представляет собой кластер из двух серверов гипервизоров, одного сервера управления и одной системы хранения данных.

1.4. Состав компонентов

Обследованная система состоит из следующих компонентов, размещенных на соответствующих объектах эксплуатации:

Название	Назначение	Кол-во
Сервер ESXi	Аппаратный гипервизор	2
Сервер vCenter	Централизованное управление виртуальной инфраструктурой	1
СХД	Система хранения данных	1

Результаты обследования

1.5. Методология

В настоящем разделе приведен методологический подход к оценке результатов обследования «состояния самозащиты». Качественные значения параметров приведены к количественным с использованием таблиц референсных (нормальных) значений. Все количественные и качественные параметры оценены на соответствие рекомендациям производителя.

Взвешенная оценка статусов параметров производилась на основе таблицы возможных значений с учетом их веса (степени влияния). Взвешенный статус параметра *(S)* вычисляется по формуле $S = (V*P)$, где V – вес параметра, P – значение параметра по результатам обследования. Метрики вычисляются на основе взвешенных статусов параметров, оказывающих влияние на каждую метрику. Количественное значение метрики *(M)* вычисляется по формуле $M = \sum S_i/i$, где S_i – взвешенный статус каждого параметра, влияющего на метрику, i – количество параметров влияющих на метрику.

Качественная оценка метрик производится на основе полученных количественных значений:

- $M < 0{,}33$ – Значение метрики «Плохо»
- $0{,}33 \geq M \leq 0{,}66$ – Значение метрики «Удовлетворительно»
- $M > 0{,}66$– Значение метрики «Хорошо»

Результаты обследования сгруппированы и визуализированы для трех фокусных групп потребителя. Уровень детализации данных различен для каждого уровня. Максимальная детализация приведена для фокусной группы потребителей «Инженеры эксплуатации и администрирования».

Общий методологический подход к оценке приведен на схеме:

1.6. Результаты для фокусной группы «Бизнес»

1.6.1. «Состояние самозащиты»

Удовлетворительно

«Состояние самозащиты»

Выявленные недочеты повышают риск недоступности системы при авариях на объектах эксплуатации и делают невозможным быстрое восстановление работоспособности, что может повлиять на непрерывность бизнеса, учитывая критичность данной системы для функционирования всех ИТ систем и сервисов.

Управлению доступом к системе уделено недостаточное внимание.

1.6.2. Документирование и организационные меры

Хорошо

Документирование и организационные меры

Документы, описывающие систему разработаны, незначительным недочетом является отсутствие процессного документа, описывающего действия персонала в случае сбоев для восстановления работоспособности, что может увеличить длительность простоя при недостаточно скоординированной работе обслуживающего персонала.

1.7. Результаты для фокусной группы «Руководство ИТ/ИБ»

1.7.1. Текущие статусы

В Табл. № 1 приведены метрики, статус которых не требует внесения каких-либо изменений в систему для улучшения их состояния. Значения параметров, входящих в метрику, в большинстве случаев соответствуют рекомендациям производителя.

Табл. № 1 Метрики со статусом «Хорошо»

Метрика	Статус
Документирование и организационные меры	

В Табл. №2 указаны метрики, требующие внимания для улучшения значения их статуса.

Табл. №2 Метрики со статусом «Удовлетворительно» или «Плохо»

Метрика/статус	Вес параметра	Оказывающий негативное влияние параметр
Управление резервным копированием  Плохо	5	Не проводится резервное копирование vCenter
	4	Не проводится резервное копирование виртуальных машин
Управление доступом к системе  Удовлетворительно	3	Не проводится разграничение ресурсов в пулах
	4	Нет разделения сетей консоли управления и виртуальных машин
	2	Не включен запрет локального входа на ESX-сервер
	1	Не настроен таймаут бездействия пользователя в консоли

Метрика/статус	Вес параметра	Оказывающий негативное влияние параметр
	1	Служба SSH не отключена
	2	Не включен Strict Lockdown Mode на хостах (запрет на изменение настроек хоста локально, если он подключен к vCenter)
Управление обновлениями и уязвимостями  Удовлетворительно	2	Используются неактуальные версии ПО
	4	Обновлены не все клиенты Vmware
Управление журналированием и мониторинг  Удовлетворительно	3	Не настроено оповещение администраторов
	2	Нет документа "план восстановления после сбоя"
Управление резервированием и отказоустойчивостью  Удовлетворительно	3	Не настроен DPM (балансировка нагрузки питания)
	4	Недостаточное количество каналов подключения к СХД
	4	Недостаточное количество каналов электропитания
	3	Отсутствует резервирование БП серверов
	3	Нет распределения питания БП по различным фазам
Управление конфигурацией и изменениями  Удовлетворительно	2	Не включен Strict Lockdown Mode на хостах (запрет на изменение настроект хоста локально, если он подключен к vCenter)
	3	Не установлен пароль загрузчика ESX-сервера

1.8. Результаты для фокусной группы «Инженеры эксплуатации и администрирования»

В Табл. №3 приведены параметры, значения которых не соответствуют рекомендациям производителя и действия, которые необходимо выполнить для улучшения значения статусов метрик и общего «состояния самозащиты» системы.

Табл. №3 Параметры не соответствующие рекомендация производителя

Параметр	Вес параметра	Ожидаемое значение	Фактическое значение	Рекомендация по устранению
Наличие документа "реакция на инциденты"	4	Есть	Нет	Разработать документ и провести моделирование инцидента
Наличие документа "план восстановления после сбоя"	2	Есть	Нет	Разработать документ и провести моделирование сбоя
Распределение питания БП по различным фазам	3	Да	Нет	Подключить дополнительную фазу питания в серверной
Количество каналов подключения к СХД	4	2	1	Подключить дополнительный канал к СХД
Используются актуальные версии ПО	2	Да	Нет	Обновить ПО до актуальной версии
Обновлены все клиенты Vmware	4	Да	Нет	Обновить все клиенты VMware
Резервное копирование виртуальных	4	Да	Нет	Проводить резервное копирование

Параметр	Вес параметра	Ожидаемое значение	Фактическое значение	Рекомендация по устранению
машин производится				
Служба SSH отключена	1	Да	Нет	Отключить службу SSH
Включен Strict Lockdown Mode на хостах (запрет на изменение настроект хоста локально, если он подключен к vCenter)	2	Да	Нет	Включить Strict Lockdown Mode
Настроен таймаут бездействия пользователя в консоли	1	Да	Нет	Настроить таймаут бездействия
Настроено оповещение администраторов	3	Да	Нет	Настроить оповещение на почту
Резервное копирование vCenter производится	5	Да	Нет	Проводить резервное копирование
Разграничение ресурсов в пулах используется	3	Да	Нет	Применять разграничение ресурсов в пулах
vApp (Порядок запуска виртуальных машин после запуска сервера виртуализации) настроен	4	Да	Нет	Создать vApp и настроить его на запуск виртуальных машин после загрузки сервера

Параметр	Вес параметра	Ожидаемое значение	Фактическое значение	Рекомендация по устранению
Кластер FT настроен и используется	3	Да	Нет	Настроить кластер FT
DPM (балансировка нагрузки питания) включена и настроена	3	Да	Нет	Настроить функции DPM
Разделение сетей консоли управления и виртуальных машин	4	Да	Нет	Разделить сеть на сегмент управления и сегмент для использования виртуальных машин

1.9. Прочие рекомендации по модернизации, оптимизации и повышению уровня доступности

Кроме перечисленных рекомендаций в таблице №3, рекомендуем обратить внимание на необходимость своевременно обновлять систему и устанавливать последние патчи.

1.10. Оценка рисков и рекомендации

В таблице приведены основные угрозы, ущерб от реализации которых, по экспертным оценкам, является наиболее значительным.

Угроза	Вероятность реализации	Ущерб от реализации	Рекомендации
Несанкционированный доступ к серверу ESXi через ssh	Низкий	Значительный	Отключить SSH службу
Потеря данных в случае выхода из строя СХД	Средняя	Значительный	Настроить резервное копирование
Несанкционированный доступ к виртуальной инфраструктуре	Средняя	Значительный	Настроить разграничение доступа для пользователей

ANGARA

Professional Assistance

Контакты

121096, г. Москва, ул. Василисы Кожиной, д.1, к.1.
БЦ «Парк Победы»
Телефон/факс: +7 (495) 269 26 06
E-mail: info@angarapro.ru