Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 5/19

(Certification No.)

Prodotto: **Dell EMC VxRail Appliance 4.5**
(Product)

Sviluppato da: **Dell Technologies, Inc.**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+
(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

Roma, 16 luglio 2019

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Dell EMC VxRail Appliance 4.5

OCSI/CERT/CCL/10/2018/RC

Versione 1.0

16 luglio 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	16/07/2019

2 Indice

3 Elenco degli acronimi

API Application Programming Interface

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DNS Domain Name Service

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

GUI Graphical User Interface

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

NTP Network Time Protocol

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto Della Valutazione

PP Protection Profile

REST Representational State Transfer

RFV Rapporto Finale di Valutazione (Evaluation Technical Report)

SAN Storage Attached Network

SAR Security Assurance Requirement

SDDC Software-Defined Data Center

SFR Security Functional Requirement

SOGIS Senior Officials Group Information Systems Security

SSD Solid State Device

SSO Single Sign-On

TDS Traguardo di Sicurezza (Security Target)

TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
2U	Two rack Units
VM	Virtual Machine
vSAN	Virtual Storage Attached Network

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Documenti tecnici

[ADM] Dell EMC VxRail Appliance, Version 4.5.x, Administration Guide, Rev. 04, April 2018

[CONF] VxRail Application, Version 4.5.x, Security Configuration Guide, Rev. 01, March 2018

[DEL] Dell EMC VxRail Appliance 4.5 Secure Delivery Document, v0.2, 7 January 2019

[RFV] Dell EMC VxRail Appliance 4.5, Evaluation Technical Report, v1, 3 June 2019

[TDS] Dell EMC VxRail Appliance 4.5, Security Target, v0.6, 22 May 2019

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su http://www.sogisportal.eu.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL 2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "Dell EMC VxRail Appliance 4.5", sviluppato dalla società Dell Technologies, Inc.

L'ODV è un'appliance hardware per infrastrutture *hyper-converged* che fornisce un data center definito dal software, in grado di supportare centinaia di macchine virtuali e i relativi dati associati. Più appliance possono essere raggruppate insieme per estendere le risorse di archiviazione e fornire opzioni ad alta disponibilità per i dati archiviati.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2, in conformità a quanto indicato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione riassume l'esito della valutazione di sicurezza del prodotto "Dell EMC VxRail Appliance 4.5" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

I potenziali acquirenti sono quindi tenuti a consultare il presente Rapporto di Certificazione congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	Dell EMC VxRail Appliance 4.5
Traguardo di Sicurezza	"Dell EMC VxRail Appliance 4.5" Security Target, v0.6, 22 May 2019
Livello di garanzia	EAL2 con aggiunta di ALC_FLR.2
Fornitore	Dell Technologies, Inc.
Committente	Corsec Security, Inc.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	4 dicembre 2018
Data di fine della valutazione	3 giugno 2019

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono riassunte le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV è un'appliance hardware per infrastrutture *hyper-converged* che fornisce un data center definito dal software, in grado di supportare centinaia di macchine virtuali e i relativi dati associati. Più appliance possono essere raggruppate insieme per estendere le risorse di archiviazione e fornire opzioni ad alta disponibilità per i dati archiviati.

Le appliance VxRail sono progettate per fornire tutti i servizi mission-critical per un SDDC (Software-Defined Data Center), inclusi virtualizzazione, elaborazione e archiviazione. Le appliance sono distribuite in cluster che vanno da 3 a 32 nodi. Un nodo fornisce il calcolo per l'appliance e contiene più processori. Ad eccezione delle appliance E Series, ogni appliance è un fattore di forma a due rack (2U) che supporta da un nodo (V, P e S Series) fino a quattro nodi (G Series). La serie E è un fattore di forma 1U che supporta un nodo. Una singola appliance E, G, V, P o S Series può supportare fino a 200 macchine virtuali (VM). L'infrastruttura *hyper-converged* di VxRail offre alle VM dei clienti la potenza di un'intera SAN in un'unica appliance.

La *hyper-convergence* è una tecnologia emergente che fa riferimento a sistemi completi che forniscono risorse di calcolo per l'esecuzione di un'infrastruttura VM e di uno storage condiviso per l'utilizzo da parte delle VM. Le soluzioni *hyper-converged* vengono eseguite interamente su server x86 con unità a stato solido e unità disco rigido interne per lo storage. I clienti distribuiscono il sistema come appliance che si adattano in modo lineare; ogni nodo aggiunto a un cluster VxRail contribuisce a una quantità fissa di potenza di calcolo e capacità di archiviazione. Questa memoria definita dal software consente di condividere lo storage all'interno dei singoli server su ogni nodo in un cluster VxRail.

7.3.1 Architettura dell'ODV

Per una descrizione maggiormente dettagliata dell'ODV, consultare il capitolo 1.5 del [TDS]. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti (vedi Figura 1).

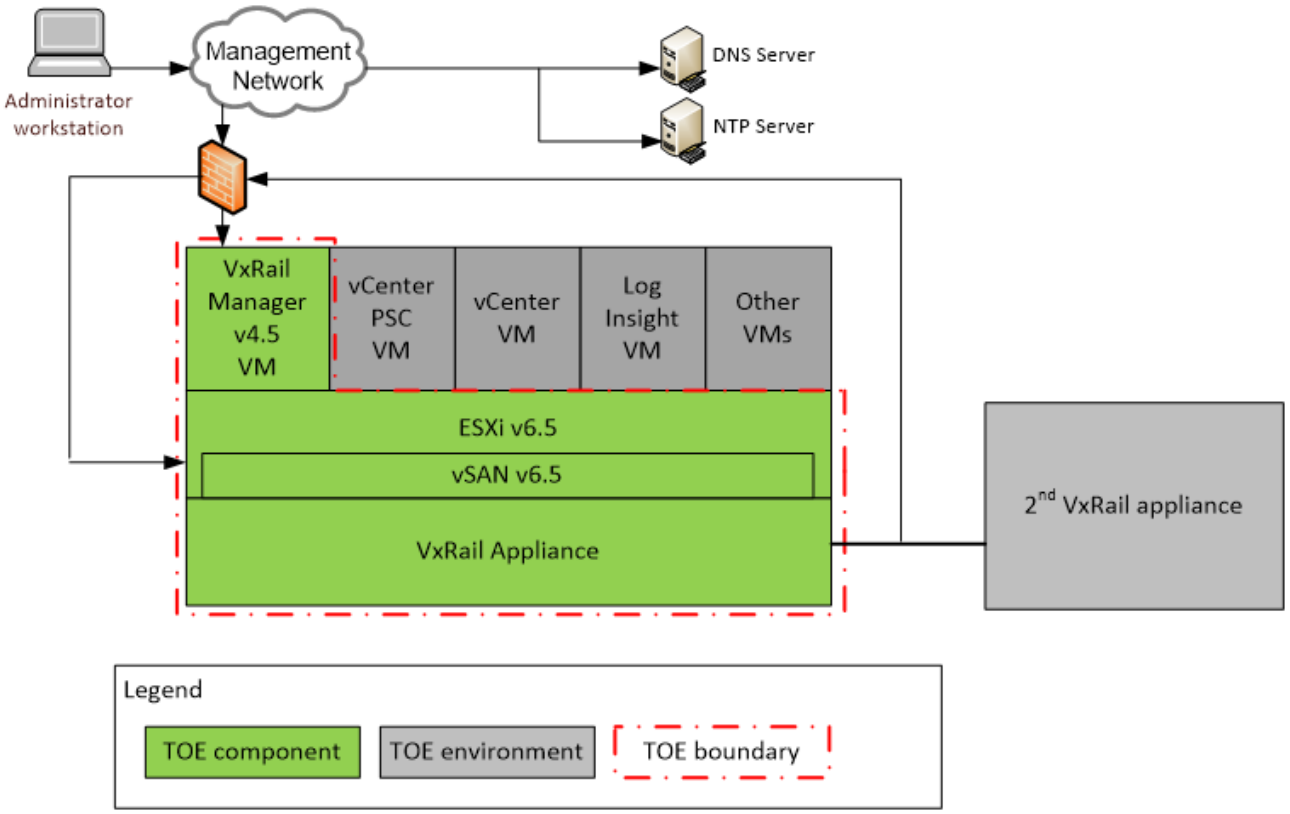

Figura 1 – Configurazione dell'ODV

L'ODV è costituito dai seguenti componenti:

- VxRail Appliance – VxRail E560, E560F, P570, P570F, V570, V570F, S570, G560, or G560F appliance

- VMware ESXi v6.5 EP 9 build-10175896 – ESXi è l'hypervisor in esecuzione nell'appliance VxRail. ESXi include VMware vSAN v6.5 EP 9 build-10175896 nel suo kernel

- VxRail Manager v4.5.225-10233140 – VxRail Manager VxRail Manager è il software che monitora nodi, dischi, alimentatori e VM per avvisare un Administrator di potenziali problemi. Il software VxRail include:

    - VxRail Manager application – presenta la VxRail Manager GUI e VxRail REST API

    - SUSE Linux operating system (OS) – sistema operativo host su VxRail VM

Il confine dell'ODV non include le VM fornite dal cliente o alcun componente esterno come un server DNS o NTP o un'infrastruttura di rete. Anche VMware vCenter è escluso dal confine. Sebbene non siano inclusi nel confine dell'ODV, tutti i componenti sono richiesti nell'ambiente operativo dell'ODV.

Gli amministratori dell'ODV possono accedere ai servizi di sicurezza attraverso le seguenti interfacce:

- VxRail Manager GUI – La GUI di VxRail Manager fornisce statistiche e avvisi su hardware, reti e VM monitorati, nonché funzionalità per spegnere l'appliance e distribuire VM.

- VxRail REST API – L'API REST VxRail fornisce funzionalità limitate che possono essere utilizzate per visualizzare le informazioni sull'ODV utilizzando le chiamate REST per ottenere e impostare i dati.

- Linux Shell Interface – L'interfaccia shell di Linux fornisce accesso limitato al sistema operativo host sulla VM VxRail Manager. Gli amministratori autorizzati possono accedere ai registri di controllo attraverso questa interfaccia e spegnere la VM VxRail Manager.

- vSphere API – La vCenter VM nell'ambiente dell'ODV utilizza l'API vSphere per comunicare i criteri di archiviazione e le configurazioni della macchina virtuale all'hypervisor ESXi. VSphere Web API è anche un servizio Web esposto in esecuzione su vCenter VM e su ciascun host ESXi. Nella configurazione valutata si consiglia di utilizzare solo l'API vSphere su vCenter Server per mantenere la coerenza su tutti gli host ESXi.

- VMware Host Client – Ciascun host ESXi gestisce un'interfaccia client host VMware che può essere utilizzata per gestire il singolo host ESXi. Nella configurazione valutata si consiglia di utilizzare questa interfaccia solo per la gestione delle emergenze quando vCenter Server non è disponibile.

Ciascun nodo ESXi offre un'interfaccia utente Web vSphere e l'accesso all'API di vSphere, ma questi non devono essere utilizzati per le azioni amministrative. I nodi dovrebbero essere amministrati tramite vCenter. L'ODV può essere distribuito in varie configurazioni da una singola appliance a più appliance raggruppate in cluster di data center fisicamente separati. Nella configurazione valutata sono state considerate un'unica appliance e con due appliance raggruppate insieme.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il par. 7.1 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito.

- **Security Audit**. L'ODV genera record di controllo e li memorizza nel filesystem di VxRail Manager. Ogni tipo di registro ha una dimensione massima del file e il numero massimo di file che vengono salvati. Se tutti i file si riempiono, il file più vecchio viene sovrascritto con un nuovo file di registro. Gli eventi di controllo comprendono l'avvio e l'arresto dell'appliance, i guasti del disco, i guasti del nodo e gli eventi di autenticazione. Il file di registro è protetto da cancellazioni e modifiche non autorizzate. Solo un amministratore autorizzato può modificare o eliminare questi file.

- **User Data Protection**. L'ODV utilizza un approccio di accesso ai dati definito dalla politica di sicurezza Virtual Disk Access SFP. Alle macchine virtuali viene assegnato un disco virtuale quando viene creato. L'ODV garantisce che le macchine virtuali possano accedere solo ai file memorizzati nel loro disco virtuale assegnato. L'ODV monitora i dati memorizzati per errori di integrità utilizzando un checksum end-to-end. Se viene rilevato un errore, l'ODV tenterà di riparare i dati, aggiornare le statistiche del disco e registrare un evento nel registro eventi.

- **Identification and Authentication**. L'ODV richiede agli amministratori di identificarsi e autenticarsi prima di accedere alle TSF, tranne quando riceve l'output dall'host API. L'ODV si affida al servizio Single Sign-On (SSO) di vCenter per autenticare gli amministratori. Le regole per la creazione di nomi utente e password sono determinate dalle politiche stabilite in vSphere. Quando un amministratore immette la propria password, la TSF fornisce feedback oscurati sulle sue interfacce.

- **Security Management**. L'ODV fornisce i ruoli di Amministratore, vCenter System, ESXi Root e CLI Root. I ruoli di Amministratore hanno accesso alla GUI di VxRail Manager e all'API REST VxRail per eseguire varie attività, tra cui monitoraggio del sistema, distribuzione di una VM e spegnimento regolare delle VM. Il ruolo Root CLI ha accesso all'interfaccia shell di Linux per visualizzare informazioni e inviare comandi e può accedere ai file di registro. VCenter Server fornisce il ruolo del sistema vCenter all'interno di ESXi per comunicare le politiche di archiviazione e le configurazioni della macchina virtuale. I criteri di archiviazione sono restrittivi per impostazione predefinita e possono essere modificati solo in vCenter e inviati all'ODV utilizzando l'account proxy. Sia l'account proxy Administrator che vCenter

possono modificare un nome VM. Il ruolo ESXi Root viene utilizzato per accedere ai singoli host ESXi a scopo di manutenzione e risoluzione dei problemi.

- **Protection of the TSF**. L'ODV manterrà uno stato sicuro quando gli errori di lettura del disco causano il malfunzionamento di vari dischi su un nodo. È possibile impostare diverse politiche di archiviazione per ogni VM, consentendo al livello di protezione da variare per ciascuna VM. VxRail controlla gli alimentatori, i nodi e i dischi delle appliance per assicurarsi che siano operativi e mostrerà un avviso nella GUI di VxRail Manager se viene rilevato un errore. I dati TSF vengono inviati da vCenter VM all'hypervisor ESXi per l'applicazione dei criteri di archiviazione e delle configurazioni della macchina virtuale. L'ODV interpreta coerentemente questi dati assicurando che CPU, storage e dati di rete disponibili vengano inviati a vCenter. L'ODV verifica che vCenter non assegni più delle risorse disponibili per questi componenti quando riceve gli aggiornamenti. Quando viene inviato un aggiornamento, l'ODV sostituirà tutti i dati precedenti con i dati aggiornati.

- **Resource Utilization**. L'ODV fornisce funzionalità continue quando errori di lettura del disco causano errori su vari dischi su un nodo. È possibile assegnare maggiore tolleranza agli errori alle singole macchine virtuali. La TSF può imporre restrizioni sulle dimensioni massime per le macchine virtuali.

- **TOE Access**. Le interfacce dell'ODV forniscono agli amministratori un'opzione per disconnettersi e terminare la sessione. Ciò impedisce alla sessione di essere aperta quando l'amministratore non si trova sulla loro workstation.

- **High Availability**. L'ODV monitora dischi, reti e nodi sottostanti per determinare lo stato generale e le statistiche su questi componenti. Gli avvisi vengono visualizzati sulla GUI di VxRail Manager se un componente non funziona o si trova in uno stato degradato. Inoltre, se un disco è stato rimosso in modo errato viene visualizzato un avviso.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita ai clienti insieme al prodotto. La documentazione indicata contiene tutte le informazioni richieste per l'installazione, l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali (SFR) sono stati derivati direttamente o per estensione dai CC Parte 2 [CC2]. In particolare, è stato definito il componente esteso FHA_TST.1: System Testing, che fornisce all'ODV la capacità di eseguire test sulle funzioni assegnate per

garantirne il corretto funzionamento. Per una descrizione dettagliata delle proprietà del componente esteso, consultare la sez. 5.2 del Traguardo di Sicurezza [TDS].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 3 giugno 2019 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV], che è stato approvato dall'Organismo di Certificazione il 25 giugno 2019. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Dell EMC VxRail Appliance 4.5" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con aggiunta di ALC_FLR.2.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Security-enforcing functional specification	ADV_FSP.2	Positivo
Basic design	ADV_TDS.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Use of a CM system	ALC_CMC.2	Positivo
Parts of the TOE CM coverage	ALC_CMS.2	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Flaw reporting procedures	ALC_FLR.2	Positivo

Classi e componenti di garanzia		Verdetto
Test	**Classe ATE**	Positivo
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Dell EMC VxRail Appliance 4.5" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte nel TDS.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata; in particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto include una serie di raccomandazioni relative alla consegna, all'inizializzazione e all'utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([ADM], [CONF]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per i potenziali acquirenti del prodotto.

9.1 Consegna

Per mantenere la sicurezza dell'ODV durante la fase di distribuzione al cliente, sono seguite da parte del fornitore Certes diverse procedure.

Prima della spedizione sono svolye alcune attività preliminari:

- attività di pre-distribuzione per software, hardware e documentazione dell'ODV;
- etichettatura dell'ODV, che include il numero di serie, il numero del modello e logo;
- imballaggio dell'ODV.

Per la spedizione ai clienti, Dell EMC utilizza corrieri commerciali internazionali con sistema di tracciamento della spedizione stessa.

Maggiori dettagli su tale procedura sono contenuti in "Secure Delivery Document" [DEL].

9.2 Installazione, inizializzazione ed utilizzo sicuro dell'ODV

Una volta che l'ODV viene consegnato al cliente, un membro del team di servizio Dell EMC autorizzato deve installare fisicamente l'appliance sul posto. Se è necessaria l'installazione del software in loco, il membro del team di servizio Dell EMC verificherà i download del software con un hash fornito sul sito di supporto Dell EMC. Inoltre, il software dell'ODV può essere installato sul diapositivo prima della spedizione.

I membri del team di servizio Dell EMC possono verificare il contenuto della spedizione dell'ODV esaminando l'elenco di imballaggio, incluso nella confezione, e l'etichetta di spedizione, apposta sul lato della confezione in cui viene spedito l'ODV, e la corrispondenza dei numeri di modello interni con i rispettivi numeri esterni Dell EMC.

Tutte le istanze dell'ODV vengono installate per conto del cliente da un membro del team di servizio Dell EMC che segue la seguente documentazione di distribuzione:

- "Dell EMC VxRail Appliance, Version 4.5.x, Administration Guide" [ADM], che contiene I passi dettagliati su come configurare correttamente l'ODV;
- "VxRail Application, Version 4.5.x, Security Configuration Guide" [CONF], che fornisce una panoramica delle impostazioni di configurazione della sicurezza per l'appliance VxRail e le migliori pratiche per garantire l'utilizzo sicuro del prodotto.

Una volta completata l'installazione, i clienti possono verificare le versioni del software dell'ODV effettuando il login all'interfaccia grafica utente (GUI) VxRail Manager con un nome utente e una password e navigando nella scheda Generale.

10 Appendice B – Configurazione valutata

L'oggetto della valutazione (ODV) è il prodotto "Dell EMC VxRail Appliance 4.5", sviluppato dalla società Dell Technologies, Inc.

Le appliance devono essere configurate in un cluster che includa almeno 3 nodi. Una singola appliance può supportare fino a 200 VM. Tutti i componenti software sono preinstallati sull'appliance prima della spedizione ai clienti.

Le funzionalità dell'ODV sono le stesse indipendentemente dall'appliance hardware su cui sono installate. Il software varia solo in base alle differenze di driver di basso livello necessarie per i diversi modelli di appliance.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 4.5. Il nome e il numero di versione identificano univocamente l'ODV e l'insieme dei suoi componenti, costituenti la configurazione valutata dell'ODV, verificata dai Valutatori all'atto dell'effettuazione dei test e a cui si applicano i risultati della valutazione stessa.

Per maggiori dettagli, consultare anche il par. 1.5 del [TDS].

10.1 Ambiente operativo dell'ODV

Per il suo funzionamento l'ODV si basa su hardware/software. Sebbene questo hardware/software sia necessario per il funzionamento dell'ODV, non fa parte dell'ODV. Il seguente hardware/software è richiesto per il funzionamento dell'ODV:

- VMware vCenter Server – L'ODV viene fornito con vCenter preinstallato nell'appliance VxRail. L'ODV si affida a vCenter per l'autenticazione, la creazione di criteri di archiviazione e per mantenere l'elenco di VM installate sull'appliance. Il componente vCenter è composto da due VM sull'appliance.

- Log Insight VM – v4.3.0 build 5084751 – Log Insight raccoglie e analizza i dati di registro su VM installate dal cliente.

- DNS server – per la risoluzione degli indirizzi di rete è necessario un server DNS.

- NTP server – è richiesto un server NTP per determinare l'origine dell'ora.

- Customer installed VMs – L'ODV offre virtualizzazione e storage per le VM dei clienti per soddisfare le loro esigenze aziendali. Un numero arbitrario di VM può essere distribuito, non superando le risorse fisiche fornite dall'ODV.

- Firewall – Un firewall protegge le interfacce dell'ODV.

- Switch – Almeno uno switch di rete 10GbE con otto porte switch è necessario anche per fornire la commutazione di rete per l'ODV.

- Cablaggio – Per ciascun tipo di porta sono necessari i seguenti cavi o equivalenti:

  - Porte RJ45 Network Interface Cards (NIC) – 2 cavi CAT6 o superiori per nodo che sono forniti con l'ODV
  - Porte SFP + NIC – 2 cavi DAC twinax compatibili per nodo o 2 cavi in fibra ottica per nodo

- Administrator workstation – Questa workstation viene utilizzata per accedere alla GUI VxRail tramite un browser standard e API REST VxRail tramite un client REST.

Per maggiori dettagli, consultare anche i par. 1.4.2 e 1.5.1.1 del [TDS].

11 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie.

L'installazione dell'ambiente di test è avvenuta seguendo le istruzioni contenute nella documentazione di supporto ([ADM], [CONF]), come indicato in Appendice A – Indicazioni per l'uso sicuro del prodotto. Dopo la configurazione dell'ODV i valutatori hanno verificato che l'ODV è stato installato correttamente e tutti i servizi previsti funzionavano correttamente.

L'ambiente di test così realizzato è lo stesso utilizzato dal Fornitore per testare le TSFI.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Copertura dei test

I valutatori hanno esaminato il piano di test presentato dal Fornitore e hanno verificato la completa copertura dei requisiti funzionali (SFR) e delle TSFI descritte nelle specifiche funzionali.

11.2.2 Risultati dei test

I Valutatori hanno eseguito una serie di test, scelti a campione tra quelli descritti nel piano di test presentato dal Fornitore, verificando positivamente il corretto comportamento delle TSFI e la corrispondenza tra risultati attesi e risultati ottenuti per ogni test.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Non sono stati utilizzati strumenti di test particolari, oltre ai componenti dell'ODV che hanno permesso di sollecitare tutte le TSFI selezionate per i test indipendenti.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione.

Tutti i test indipendenti eseguiti dai Valutatori hanno dato esito positivo.

11.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali (cfr. par. 11.1). I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quella indicata nel [TDS], par. 1.2.

In una prima fase, i Valutatori hanno effettuato delle ricerche utilizzando varie fonti di pubblico dominio, quali internet, libri, pubblicazioni specialistiche, atti di conferenze, ecc., al fine di individuare eventuali vulnerabilità note applicabili a tipologie di prodotti simili all'ODV. In questa ricerca è stato considerato anche il sistema operativo Linux, facente parte dell'ambiente operativo, ma comunque necessario al corretto funzionamento dell'ODV. Sono state così individuate alcune vulnerabilità potenziali.

In una seconda fase, i Valutatori hanno esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) ed utilizzato lo strumento di scansione automatica Burp Suite, al fine di evidenziare eventuali ulteriori vulnerabilità potenziali dell'ODV. Da questa analisi, i Valutatori hanno effettivamente determinato la presenza di altre vulnerabilità potenziali.

I Valutatori hanno analizzato nel dettaglio le potenziali vulnerabilità individuate nelle due fasi precedenti, per verificare la loro effettiva sfruttabilità nell'ambiente operativo dell'ODV. Quest'analisi ha portato a individuare alcune effettive vulnerabilità potenziali.

I Valutatori hanno quindi progettato dei possibili scenari di attacco, con potenziale di attacco Basic, e dei test di intrusione per verificare la sfruttabilità di tali vulnerabilità potenziali candidate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi. Per l'esecuzione dei test i Valutatori hanno utilizzato il già citato strumento Burp Suite.

L'esecuzione dei test di intrusione ha confermato la presenza di vulnerabilità potenzialmente sfruttabili da un attaccante con potenziale di attacco Basic. Tali risultati sono stati prontamente segnalati al Fornitore, tramite un Rapporto di Osservazione. Il Fornitore ha replicato, recependo le osservazioni dei Valutatori e rilasciando una nuova versione del Traguardo di Sicurezza in cui i requisiti funzionali SFR relativi all'identificazione e autenticazione sono meno stringenti (FIA_UAU.1 e FIA_UID.1 invece di FIA_UAU.2 e FIA_UID.2). I Valutatori hanno quindi sottoposto a test questa nuova versione dell'ODV, e hanno potuto verificare che la soluzione proposta dal Fornitore ha risolto tutti i problemi sollevati con le precedenti osservazioni.

I Valutatori hanno così concluso che nessuno degli scenari di attacco ipotizzati con potenziale Basic può essere portato a termine con successo nell'ambiente operativo dell'ODV. Pertanto, nessuna delle vulnerabilità potenziali precedentemente individuate può essere effettivamente sfruttata. Sono state invece individuate tre vulnerabilità residue; tali vulnerabilità potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a Basic.